ivanti

NMDM Admin Guide ES

ivanti

CONTENTS

1. **Acerca de Ivanti Neurons for MDM** **9**
2. **Resumen de nuevas funciones** **10**
3. **Vídeos** **14**
4. **Introducción** **17**
   - 4.1. Configuración de dispositivos macOS 24
   - 4.2. Configuración y uso de los correos electrónicos de confirmación de registro 27
   - 4.3. Configuración y uso de los correos electrónicos de notificación de cumplimiento de políticas 28
   - 4.4. Características a petición 29
   - 4.5. Preparación para la compatibilidad con un dispositivo de Android Enterprise 32
5. **Panel** **33**
   - 5.1. Trabajar con widgets 34
   - 5.2. Datos sobre aplicaciones 40
   - 5.3. Uso de Informes programados 45
   - 5.4. Uso de Informes personalizados 52
6. **Usuarios** **60**
   - 6.1. Añadir usuarios 61
   - 6.2. Grupos de usuarios 65
   - 6.3. Ajustes del usuario 70
   - 6.4. Marca del usuario 81
   - 6.5. Inscripción de usuarios en el Apple Business Manager 82
   - 6.6. Licencias de usuario 91
   - 6.7. Administrar usuarios 92
     - 6.7.1. Añadir el usuario de una API para operaciones de Cisco ISE 93
     - 6.7.2. Asignar funciones a usuarios 94
     - 6.7.3. Funciones del usuario 96
     - 6.7.4. Encontrar y filtrar usuarios 99
     - 6.7.5. Asignar usuarios a grupos de usuarios 102
     - 6.7.6. Invitar a usuarios 103
     - 6.7.7. Activar y desactivar usuarios 104
     - 6.7.8. Gestionar múltiples inicios de sesión del administrador 106
     - 6.7.9. Cambiar una contraseña 107
     - 6.7.10. Enviar un mensaje 109
     - 6.7.11. Quitar usuarios de grupos de usuarios 111
     - 6.7.12. Eliminar a un usuario 112
     - 6.7.13. Exportar usuarios 113
     - 6.7.14. Asignar atributos personalizados a los usuarios 114
     - 6.7.15. Eliminar atributos personalizados de los usuarios 115
     - 6.7.16. Cambiar la configuración regional del usuario 116
     - 6.7.17. Editar un nombre de usuario 117
     - 6.7.18. No participar en la obtención de datos sobre localización 118
     - 6.7.19. Información de tiempo de espera 119
     - 6.7.20. Cancelar las analíticas sobre el uso del sistema 120
     - 6.7.21. Registro de dispositivo por generación de PIN 121
7. **Dispositivos** **122**
   - 7.1. Introducción a los dispositivos 123
   - 7.2. Grupos de dispositivos 138
   - 7.3. Dispositivos no administrados 144
   - 7.4. Inventario de aplicaciones 145
   - 7.5. Administrar dispositivos 148
     - 7.5.1. Despliegue de dispositivos Apple 150
     - 7.5.2. Desplegar dispositivos de Windows 159
     - 7.5.3. Configurar Apple Remote Desktop en dispositivos macOS 163
     - 7.5.4. Registro de dispositivos (iOS, macOS y Android) 164
     - 7.5.5. Registro de dispositivos (PC con Windows 10+ y Microsoft HoloLens 2) 168
     - 7.5.6. Solución de contraseña del administrador local (LAPS, por sus siglas en inglés) 171
     - 7.5.7. Inscripción de paquete de aprovisionamiento con PIN 173
     - 7.5.8. Uso de la Inscripción en masa para dispositivos Windows 177
       - 7.5.8.1. Inscripción en masa de Ivanti 179
     - 7.5.9. Cambiar ajustes del código de acceso 181

7.5.10. Cambiar nombre del dispositivo ... 182
7.5.11. Encontrar y filtrar dispositivos ... 183
7.5.12. Uso del modo Propietario del dispositivo ... 186
7.5.13. Dispositivo administrado con perfil profesional ... 193
7.5.14. Uso de la inscripción en masa para Android ... 194
7.5.15. Inscripción masiva mediante carga de archivos CSV ... 197
7.5.16. Device_to_User_BulkEnrollment ... 200
7.5.17. Uso de la inscripción móvil de Samsung Knox ... 201
7.5.18. Inscribir dispositivos de Oculus ... 202
7.5.19. Activar Bluetooth en un dispositivo ... 205
7.5.20. Programar actualización de iOS ... 206
7.5.21. Reinstalar aplicaciones del sistema iOS ... 207
7.5.22. Asignar un dispositivo a un nuevo usuario ... 208
7.5.23. Reasignar un dispositivo Android ... 209
7.5.24. Forzar el ingreso de un dispositivo ... 210
7.5.25. Encontrar un dispositivo ... 211
7.5.26. Bloquear un dispositivo ... 212
7.5.27. Administrar dispositivos en el modo Perdido de Apple ... 213
7.5.28. Administración de dispositivos Android en modo Perdido ... 215
7.5.29. Solicitar registros de depuración ... 217
7.5.30. Apple_Enhanced_Logging ... 218
7.5.31. Retirar un dispositivo ... 219
7.5.32. Renuncia de la propiedad de un dispositivo ... 220
7.5.33. Borrar un dispositivo ... 221
7.5.34. Eliminar dispositivos ... 223
7.5.35. Desbloquear un dispositivo ... 224
7.5.36. Reiniciar o apagar dispositivos ... 226
7.5.37. Borrar la contraseña de las restricciones (solo iOS) ... 228
7.5.38. Eliminar la asociación de Sentry de un dispositivo ... 229
7.5.39. Asignar atributos personalizados a los dispositivos ... 230
7.5.40. Eliminar atributos personalizados de los dispositivos ... 231
7.5.41. Sincronizar y obtener comentarios de aplicaciones ... 232
7.5.42. Establecer la contraseña del firmware ... 234
7.5.43. Volver a emitir una nueva clave de recuperación personal ... 235
7.5.44. Configurar o cambiar el bloqueo de recuperación ... 237
7.5.45. Administración de acceso de Apple ... 238
7.5.46. Inscripción de políticas de grupos ... 239
8. Aplicaciones ... 240
8.1. Catálogo de aplicaciones ... 241
8.2. Gestión de aplicaciones mediante Declarative Device Management (DDM) ... 261
8.2.1. Ajustes de la gestión de aplicaciones mediante DDM ... 263
8.3. Apps@Work (iOS, Android, Windows y macOS) ... 266
8.4. Funciones de la tienda de aplicaciones de Apps@Work en iOS ... 269
8.5. Funciones avanzadas de iOS Go ... 272
8.6. Ver Detalles de la aplicación ... 279
8.7. Configuración de aplicaciones ... 282
8.8. Asignar atributos personalizados a las aplicaciones ... 299
8.9. Configuraciones administradas para Android ... 301
8.10. Administrar aplicaciones de Google Play ... 307
8.11. Eliminar aplicaciones del App Catalog ... 309
8.12. Actualizar aplicaciones internas ... 310
8.13. Encontrar el nombre del paquete de una aplicación de Android ... 311
8.14. Categorías ... 312
8.15. Filtros de distribución ... 313
8.16. Excluir o distribuir aplicaciones ... 316
8.17. Opiniones ... 317
8.18. Apps and Books de Apple ... 319
8.19. Ajustes del catálogo ... 329
8.20. Instalar dependencias de aplicaciones ... 332
8.21. Desplegar Divide Productivity con Android Enterprise ... 335
8.22. Configurar la aplicación Provisioner ... 338
8.23. Administración de aplicaciones de Windows ... 341

8.24. Ivanti Bridge ... 344
9. Contenido ... 350
9.1. Gestión de contenidos ... 351
9.2. Categorías ... 353
10. Configuraciones ... 354
10.1. Trabajar con configuraciones ... 355
10.2. Creación de una configuración del portal de autoservicio para usuarios ... 368
10.3. Configuración personalizada ... 370
10.4. Insertar SyncML en dispositivos mediante la configuración personalizada ... 372
10.5. Configuración del diseño de la pantalla de inicio ... 373
10.6. Configuración del control de aplicaciones: controle qué aplicaciones pueden instalarse en cada dispositivo ... 375
10.7. Configuración de las notificaciones de la aplicación ... 377
10.8. Exportar configuraciones ... 379
10.9. Priorizar configuraciones ... 380
10.10. Administrar configuraciones ... 381
10.10.1. Tipos de configuración ... 382
10.10.2. Variables ... 398
10.10.3. Configuraciones de App Connect ... 403
10.10.3.1. Introducción a AppConnect ... 404
10.10.3.2. Código de acceso de AppConnect ... 405
10.10.4. Configuración de seguridad ... 407
10.10.4.1. Android Enterprise ... 409
10.10.4.2. Atestación de Claves de Acceso de Apple ... 412
10.10.4.3. Valores predeterminados de privacidad de las aplicaciones ... 413
10.10.4.4. Editar la configuración predeterminada de Android Enterprise ... 416
10.10.4.5. Configurar Android Enterprise ... 418
10.10.4.6. Android Enterprise: modo no GMS para el dispositivo administrado en el trabajo (AOSP) ... 425
10.10.4.7. Desafío de acceso (Work Challenge) de Android ... 426
10.10.4.8. Configuración del certificado ... 431
10.10.4.9. Transparencia del certificado ... 434
10.10.4.10. Configuración de comprobación de revocación de certificados ... 435
10.10.4.11. Crear configuración en modo autónomo de una única aplicación ... 436
10.10.4.12. Creación de una configuración de proxy de DNS ... 437
10.10.4.13. Configuración del registro de dispositivos ... 438
10.10.4.14. Configuración del administrador de discos ... 440
10.10.4.15. Cifrado en Android ... 441
10.10.4.16. DNS cifrado ... 442
10.10.4.17. Ajustes de inteligencia externa ... 445
10.10.4.18. Defensa contra amenazas ... 446
10.10.4.19. FileVault 2 ... 447
10.10.4.20. Clave de recuperación de FileVault ... 448
10.10.4.21. Configuración de opciones de FileVault ... 449
10.10.4.22. Certificado de identidad ... 450
10.10.4.23. Configuración del Bloqueo de activación de Apple ... 456
10.10.4.24. Configuración personalizada iOS ... 460
10.10.4.25. Ajustes de inteligencia ... 461
10.10.4.26. Restricciones de iOS ... 464
10.10.4.27. Visualización de la sala de conferencias ... 484
10.10.4.28. Ajustes del teclado ... 485
10.10.4.29. Bloqueo y kiosco: modo de administrador de dispositivos de Android ... 487
10.10.4.30. Configurar el modo kiosco para Android ... 490
10.10.4.31. Configurar el kiosco del dispositivo compartido Android ... 492
10.10.4.32. Bloqueo y kiosco: Android Enterprise ... 493
10.10.4.33. Bloqueo y kiosco: Samsung KNOX Standard ... 522
10.10.4.34. Configuración de la solución de contraseñas de administrador local ... 526
10.10.4.35. Firewall de macOS ... 527
10.10.4.36. Restricciones de macOS ... 529
10.10.4.37. Restricciones de la AppStore de macOS ... 536
10.10.4.38. Restricciones de grabación en disco de macOS ... 537
10.10.4.39. Control multimedia permitido (obsoleto) ... 538
10.10.4.40. Ajustes del Finder de macOS ... 542
10.10.4.41. Política de extensiones del kernel de macOS ... 543

10.10.4.42. Mobile@Work para macOS ... 544
10.10.4.43. Configuración de las reglas de actualización de software macOS ... 550
10.10.4.44. Preferencia de certificado ... 551
10.10.4.45. Active Directory (macOS) ... 552
10.10.4.46. Preferencia de identidad ... 555
10.10.4.47. Creación automática de cuentas en Office 365(macOS) ... 556
10.10.4.48. Autenticar ... 558
10.10.4.49. App Catalog de Apple ... 560
10.10.4.50. Dominios administrados ... 561
10.10.4.51. Configuración del código de acceso ... 562
10.10.4.52. Preferencias de privacidad (macOS) ... 566
10.10.4.53. Configuración de privacidad ... 568
10.10.4.54. Información de Declaración de la privacidad del cliente ... 571
10.10.4.55. Ajustes del cliente de Ivanti Go ... 572
10.10.4.56. Ajustes de Siri ... 574
10.10.4.57. Configuración de archivos de configuración de servicios ... 576
10.10.4.58. Actualizaciones de software ... 578
10.10.4.59. Configuración de los ajustes de actualización del software ... 585
10.10.4.60. Configuración de Preferencias de Seguridad ... 589
10.10.4.61. Servidor de zona horaria ... 590
10.10.4.62. Filtro de contenido web ... 591
10.10.4.63. Firewall de Windows ... 594
10.10.4.64. Protección de la información de Windows ... 597
10.10.4.65. Restricciones de Windows ... 602
10.10.4.66. Restricciones de Windows Desktop ... 608
10.10.4.67. Ajustes de escritorio para Windows 10 ... 611
10.10.4.68. Configuración predeterminada de Windows Hello para empresas ... 613
10.10.4.69. Configuración del administrador de IA de Windows ... 614
10.10.4.70. Play Integrity (antes SafetyNet Attestation) ... 616
10.10.4.71. Código de acceso y pantalla de bloqueo avanzados de Android ... 617
10.10.4.72. Microsoft Defender for Endpoint ... 618
10.10.4.73. Autenticación basada en certificado ... 619
10.10.5. Configuraciones de recursos del usuario ... 621
10.10.5.1. Configuración de CalDAV ... 622
10.10.5.2. Configuración de CardDAV ... 623
10.10.5.3. Configuración de Google ... 624
10.10.5.4. Configuración de correo electrónico ... 626
10.10.5.5. Configuración de Exchange ... 630
10.10.5.6. Configuración de fuente ... 634
10.10.5.7. Configuración del calendario suscrito ... 635
10.10.5.8. Crear una configuración de Web Clip ... 636
10.10.5.9. Instalación de Office 365 ... 638
10.10.5.10. Ajustes de GPO de Windows ... 640
10.10.5.11. Configuración de cifrado de BitLocker ... 642
10.10.6. Configuración de acceso a la red de la empresa ... 647
10.10.6.1. Configuración de AirPlay ... 648
10.10.6.2. Configuración de AirPrint ... 649
10.10.6.3. Configuración de VPN siempre activa ... 650
10.10.6.4. Permisos predeterminados del tiempo de ejecución de las aplicaciones ... 654
10.10.6.5. Educación ... 656
10.10.6.6. Configuración de proxy global ... 657
10.10.6.7. Configuración de proxy global (Android) ... 658
10.10.6.8. Configuración de LDAP ... 659
10.10.6.9. Configuración del servidor de macOS ... 660
10.10.6.10. Tunnel ... 661
10.10.6.11. Configurar AppTunnel ... 662
10.10.6.12. Configuración de VPN por aplicación ... 667
10.10.6.13. Configuración de inicio de sesión único ... 677
10.10.6.14. Configuración del relé de red ... 689
10.10.6.15. Inicio de sesión seguro multiusuario para iOS ... 691
10.10.6.16. Configuración de ajustes de la APN de Android ... 693
10.10.6.17. Configuración de VPN ... 697

10.10.6.18. VPN a petición ... 709
10.10.6.19. Configuración de Wi-Fi ... 717
10.10.7. Configuración de la red móvil ... 726
10.10.7.1. Configuración de APN ... 727
10.10.7.2. Móvil ... 728
10.10.7.3. Configuración de la red móvil privada ... 731
10.10.7.4. Configuración de preajustes de iOS para Telecom ... 732
10.10.7.5. Configuración mejorada de segmentación de red 5G ... 733
10.10.7.6. Configuración de eSIM ... 735
10.10.8. Otra configuración ... 738
10.10.8.1. Configuración de dominios asociados ... 740
10.10.8.2. Configuración de la transferencia de archivos de Android ... 741
10.10.8.3. Configuración de Apple TV ... 745
10.10.8.4. Duplicación AirPlay ... 746
10.10.8.5. Ajustes del navegador ... 748
10.10.8.6. Configurar el modo Single App para iOS ... 751
10.10.8.7. Configurar un perfil de MDM en iOS ... 754
10.10.8.8. Configurar un perfil de MDM en macOS ... 756
10.10.8.9. Caché de contenidos ... 757
10.10.8.10. Crear un acceso directo de Android ... 761
10.10.8.11. Creación de configuraciones de ajustes de accesibilidad ... 762
10.10.8.12. Crear configuración de salva pantallas ... 765
10.10.8.13. Configurar el salvapantallas del usuario ... 766
10.10.8.14. Ajustes del nombre del dispositivo ... 767
10.10.8.15. Configuración del fondo de pantalla del dispositivo ... 768
10.10.8.16. Configuración de la integración de servidores EMA ... 771
10.10.8.17. Configuración de ahorro de energía ... 772
10.10.8.18. Configuración de Ethernet (macOS) ... 778
10.10.8.19. Configuración de Google BeyondCorp ... 782
10.10.8.20. Configuración del mensaje de la pantalla de bloqueo ... 786
10.10.8.21. Configuración de la ventana de inicio de sesión: macOS ... 788
10.10.8.22. Configuración de las extensiones del sistema de macOS ... 789
10.10.8.23. MAM solo ... 790
10.10.8.24. Configuración Google Play administrada ... 792
10.10.8.25. Ajustes del asistente de migración ... 793
10.10.8.26. Configuración de las notificaciones ... 794
10.10.8.27. Ajustes de la impresora ... 795
10.10.8.28. Configuración para eliminar el «bloatware» ... 798
10.10.8.29. Configuración de ajustes y extensión de Safari ... 799
10.10.8.30. Configuración de las restricciones de teléfonos Samsung ... 803
10.10.8.31. Configuración predeterminada del navegador: iOS y visionOS ... 804
10.10.8.32. Configuración de los ajustes del host de Compartir pantalla ... 805
10.10.8.33. Configuración del modo Single-App ... 807
10.10.8.34. Configuración de la cadencia de recomendación de actualizaciones de software ... 810
10.10.8.35. Menú Inicio y Barra de tareas ... 811
10.10.8.36. Configuración de la actualización del sistema ... 813
10.10.8.37. Administración de actualización de Windows 10 ... 819
10.10.8.38. Programación de aplicaciones Windows ... 822
10.10.8.39. Configuración del BIOS de Windows ... 823
10.10.8.40. BitLocker de Windows ... 831
10.10.8.41. Configuración del kiosco de Windows ... 832
10.10.8.42. Configuración de la licencia de Windows ... 837
11. Políticas ... 838
11.1. Trabajar con políticas ... 839
11.2. Política personalizada ... 845
11.3. Supervisar y controlar las aplicaciones permitidas ... 870
11.4. Priorizar políticas ... 878
11.5. Política de hardware de Windows ... 879
12. Administración ... 880
12.1. Sistema ... 881
12.1.1. Atributos ... 882
12.1.2. Ajustes de borrado del dispositivo ... 889

12.1.3. Perfiles GDPR ... 895
12.1.4. Correos electrónicos de notificación ... 897
12.1.5. Administración de funciones ... 898
12.1.6. Espacios ... 906
12.1.6.1. Espacios ... 907
12.1.6.2. Administrar espacios ... 909
12.1.6.3. Ejemplos de espacios ... 914
12.1.6.4. Delegar dispositivos ... 916
12.1.6.5. Delegar aplicaciones ... 917
12.1.7. Administradores de asistencia técnica ... 919
12.1.8. Administrador > Notificación de uso del sistema ... 920
12.2. Infraestructura ... 922
12.2.1. Acceso ... 923
12.2.2. Listas de aplicaciones (plists) ... 924
12.2.3. Exportar trazas de auditorías ... 925
12.2.4. Gestión de certificados ... 928
12.2.5. Configuración de SCEP para Entidades de Certificación externas ... 936
12.2.6. Proveedores de credenciales derivadas ... 938
12.2.7. Conector ... 939
12.2.8. Uso del comando httpproxy para Conector ... 942
12.2.9. Help@Work ... 943
12.2.10. Identidad de la infrastructura ... 946
12.2.10.1. Configurar el proveedor de identidades ... 947
12.2.10.2. Aprovisionamiento de usuarios con SCIM ... 951
12.2.10.2.1. Aprovisionamiento de usuarios para IdP de Entra ID ... 954
12.2.10.2.2. Aprovisionamiento de usuarios para Okta IdP ... 960
12.2.11. Configuración del servidor LDAP ... 963
12.2.12. Sentry ... 972
12.3. Ajustes de Apple ... 973
12.3.1. Configurador de Apple ... 974
12.3.2. Inscripción basada en cuentas ... 976
12.3.3. Inscripción de dispositivos ... 979
12.3.4. Inscripción Beta ... 995
12.3.5. Configuración del asistente de configuración ... 996
12.3.6. Instalación del Certificado MDM ... 997
12.3.7. Dispositivos iPad compartidos para empresas ... 998
12.3.8. Director de la escuela ... 1003
12.3.9. Ajustes (Apple) ... 1006
12.4. Trabajar con dispositivos Windows ... 1009
12.4.1. Configuración de los perfiles de Windows Autopilot ... 1010
12.4.2. Audit Trails en los perfiles de Windows Autopilot ... 1016
12.4.3. TenantLockdown CSP ... 1017
12.4.4. Explorador ADMX (GPO) ... 1018
12.4.5. Configuración de los intervalos del inventario de aplicaciones ... 1019
12.4.6. Inventario de hardware ... 1020
12.5. Configuración con Microsoft Azure ... 1021
12.5.1. Uso de Microsoft Azure ... 1022
12.5.2. Configuración de la gestión del endpoint unificado de Entra ID de Windows 10 ... 1025
12.5.3. Asignación de la aplicación Entra ID UEM ... 1026
12.5.4. Conecte Ivanti Neurons for MDM con Entra ID User Source ... 1027
12.5.5. Inquilino de Azure ... 1029
12.5.5.1. Azure Tenant Requirements ... 1030
12.5.5.2. Aplicar la licencia de Intune a usuarios de dispositivos ... 1032
12.5.5.3. Para añadir MobileIron como socio de cumplimiento ... 1033
12.5.5.4. Creación de una directiva de acceso condicional en Microsoft Endpoint Manager ... 1034
12.5.5.5. Conexión de Microsoft Azure con Ivanti Neurons for MDM ... 1035
12.5.5.6. Creación de una directiva de cumplimiento de los dispositivos de los socios ... 1036
12.5.5.7. Estado del dispositivo que notifica desde Ivanti Neurons for MDM a Azure ... 1038
12.5.5.8. Cancelar el aprovisionamiento del inquilino de Azure ... 1040
12.5.6. Administrador > Microsoft Azure > Office 365 App Protection ... 1041
12.6. Conectar con Google Apps ... 1050
12.6.1. Cuentas administradas de Google Play (cuentas con Android Enterprise) ... 1051

12.6.2. Registro de dispositivos Android ... 1055
12.6.3. API de administración de Android ... 1056
12.6.4. API de Google Apps ... 1062
12.6.5. Administrador- Android Enterprise ... 1063
12.7. Trabajar con dispositivos de ChromeOS ... 1065
12.7.1. ChromeOS e Ivanti Neurons for MDM ... 1066
12.7.2. Distribuir aplicaciones de Android en dispositivos de ChromeOS ... 1068
12.7.3. Agregar y distribuir aplicaciones de extensión de ChromeOS ... 1069
12.7.4. Configuración de ChromeOS Blueprint ... 1070
12.7.5. Acciones de dispositivos ... 1071
12.7.6. Preguntas más frecuentes ... 1072
12.7.7. Pasos recomendados para la evaluación ... 1074
12.8. Administración del firmware ... 1075
12.8.1. Inscripción al servicio Zebra OTA ... 1076
12.8.2. Administración de licencias de Samsung E-FOTA (Retirado) ... 1077
12.9. Gestionar secuencias de comandos y archivos ... 1078
12.9.1. Todas las secuencia de comandos ... 1079
12.9.2. Archivos ... 1084
12.10. Personalización de marca ... 1085
12.10.1. Administrador > Catálogo de aplicaciones Apple (personalización de marca) ... 1086
12.10.2. Personalizar el App Catalog de Android ... 1087
12.10.3. Administrador > Personalización de marca del kiosko de Android ... 1088
12.10.4. Cómo personalizar las plantillas de correo electrónico ... 1089
12.10.5. Portal de autoservicio ... 1098
12.10.6. Portal de autoservicio (personalización) ... 1100
12.10.7. Personalización del inicio de sesión multiusuario (clip web) ... 1101
12.10.8. Organización ... 1102
12.11. Añadir la administración de dispositivos que no sean iOS ... 1103
13. Paquetes ... 1104
13.1. Actualización ... 1108
14. Licencias de dispositivo ... 1110
14.1. Suspensión del abonado ... 1111
15. Abrir un tique de asistencia ... 1112
16. Atributos de terceros ... 1113
17. Apps@Work ... 1114
18. Activación de la autenticación de Kerberos entre Ivanti Neurons for MDM y el servidor SCEP ... 1117
19. Guía de administración de Ivanti Neurons for MDM 127 ... 1120
20. Welcome ... 1121
21. Welcome CSH ... 1122
22. Administración de actualización de Windows ... 1123

1. Acerca de Ivanti Neurons for MDM

Como método moderno para la seguridad de dispositivos móviles, Ivanti Neurons for MDM proporciona soluciones de Administración unificada de extremos (UEM) en una infraestructura sumamente escalable, segura y fácil de actualizar que es compatible con millones de dispositivos en el mundo.

- Actualizaciones instantáneas: obtenga actualizaciones automáticas de software y seguridad, y acceso a nuevas funciones en el momento en que estén disponibles.
- Escalabilidad a demanda: escale su implementación a medida que las necesidades de la empresa cambian sin tener que preocuparse por planificar la capacidad.
- Minimizar los costes del hardware: al eliminar la necesidad de mantener el hardware de forma local, los servicios basados en la nube no requieren de ninguna huella para su gestión.
- Alto tiempo de funcionamiento y alta disponibilidad.
- Maximizar las inversiones existentes: reasigne los recursos informáticos para que dejen de dedicarse al mantenimiento de hardware y se dediquen a tareas más estratégicas que aporten valor al negocio.

Puede consultar los resúmenes de **Resumen de nuevas funciones** disponibles en esta versión.

2. Resumen de nuevas funciones

Esta sección ofrece un resumen de las nuevas funciones y mejoras disponibles en esta versión. También se proporcionan referencias a la documentación que describe estas características y mejoras, cuando están disponibles.

Características y mejoras generales

Características de Android

Funciones de iOS, macOS, watchOS, visionOS y tvOS

Características de Windows

Características y mejoras generales

- **Gestión de id. de paquete de macOS mejorada**:?Se mejoró la implementación de la aplicación PKG interna de macOS al detectar y completar de manera automática el id de paquete correcto durante la carga de la aplicación y garantizar que se envíe el mismo id de paquete a los dispositivos. Esto mejora la precisión de la identificación de la aplicación, resuelve los desajustes de estado de dispositivo instalación del dispositivo servidor y mejora los informes de estado de la instalación. Las ID de paquete se pueden revisar y editar durante la carga antes de bloquearse después del despliegue.
- **Visibilidad de id de paquete para aplicaciones instaladas**: la sección Aplicaciones instaladas de la página Detalles del dispositivo ahora incluye una columna de id de paquete, que se puede habilitar u ocultar desde la configuración de la página.
- **Reintento automático para instalaciones fallidas de aplicación Android**: las instalaciones de aplicación Android que entren en un estado de instalación de error ahora se reintentan de forma automática a partir de una hora después del registro del dispositivo. Los comandos de instalación se vuelven a enviar cada 30 minutos durante un máximo de cinco intentos para mejorar el éxito de la implementación de la aplicación.
- **Seguimientos de auditoría de movimiento de dispositivo para espacios**: se agregó el ajuste Habilitar seguimientos de auditoría para inscripción y cancelación de inscripción de dispositivo en espacios para rastrear el movimiento del dispositivo entre espacios. Para más información, véase Exportar trazas de auditorías.
- **¿SO?Filtro de plataforma para la configuración de limpieza del dispositivo**:?Los administradores ahora pueden filtrar las acciones de limpieza de dispositivo por plataforma de SO al eliminar pendiente dispositivos retirados y dispositivos pendientes. Por defecto, todas las plataformas compatibles permanecen seleccionadas, preservando el comportamiento existente. Los administradores pueden modificar la selección y restringir las operaciones de limpieza a plataformas específicas según sea necesario. Para más información, consulte Ajustes de limpieza del Ajustes de borrado del dispositivo.
- **Sincronización de la política de protección de la aplicación de Office 365**:?Anteriormente, los administradores podían seleccionar aplicaciones directamente en Ivanti Neurons for MDM mientras creaban o modificaban políticas de protección de aplicación. Microsoft ha obsoleto la API que se utilizó para recuperar la lista de aplicaciones disponibles, lo que hace que las listas de aplicación protegidas aparezcan vacías en Ivanti Neurons for MDM. La administración de la política de protección de la aplicación de Microsoft Office 365 se actualiza para alinearse con los cambios en Microsoft Intune. Las aplicaciones configuradas en Intune ahora se sincronizan automáticamente con Ivanti Neurons for MDM, lo que garantiza una visibilidad continua de las aplicaciones protegidas. Aunque la eliminación de aplicación sigue siendo compatible con Ivanti Neurons for MDM, las nuevas asignaciones de aplicación deben configurarse en Microsoft Intune y se reflejarán de forma automática.
- **Registro de auditoría de movimiento del dispositivo para espacios**:?Los administradores ahora pueden realizar un seguimiento del movimiento del dispositivo entre espacios a través de los registros de auditoría. Cuando se habilita, la nueva configuración de auditoría registra los eventos siempre que un dispositivo se elimina de un espacio y se agrega a otro, lo que proporciona mayor

visibilidad de las asignaciones de espacio automatizadas y basadas en reglas. Para obtener más información, consulte **Exportar trazas de auditorías**.

- **Asignación automática de atributos personalizados mediante Grupos de dispositivo**:?Los administradores ahora pueden asignar atributos personalizados a nivel de grupo de dispositivos. Los dispositivos que son miembros de un grupo de dispositivos heredan de forma automática los valores de atributo configurados, reduciendo la configuración manual y ayudando a garantizar una categorización coherente del dispositivo. Para obtener más información, consulte **Grupos de dispositivos**.
- **Restricciones de registro del dispositivo a nivel de SO**:?Restringir el registro del dispositivo por plataforma, lo que permite inscribir solo **dispositivos**Apple **,**Android **y** Windows aprobados. Para Para más información, consulte Configuración del **Ajustes del usuario**.

Características de Android

- **Prevenir actualizaciones de aplicación mientras la aplicación está en uso**:?Los administradores ahora pueden evitar que las aplicaciones Android administradas se actualicen mientras están en uso activo. Cuando **la opción No actualizar mientras la aplicación está en uso** está habilitada, las actualizaciones de la aplicación se aplazan hasta que el usuario cierra la aplicación o la mueve al segundo plano, lo que ayuda a minimizar las interrupciones durante las sesiones activas. Para obtener más información, consulte **Configuración de aplicaciones**.
- **Mantener el modo de kiosco en los cambios de política de bloqueo**: se agregó soporte para mantener el modo de kiosco en los cambios de política de bloqueo. Los dispositivos vuelven al modo de quiosco de forma automática después de una actualización de la política de confinamiento, lo que reduce la intervención manual y minimiza las interrupciones en los dispositivos con fines específicos. Para obtener más información, consulte **Bloqueo y kiosco: Android Enterprise**.
- **Habilitar notificaciones sin editar**:?Se ha añadido soporte para configurar la visibilidad de la notificación de la pantalla de bloqueo en los dispositivos del propietario del dispositivo. Los administradores pueden mostrar, ocultar o redactar el contenido de la notificación en la pantalla de bloqueo para ayudar a proteger la información confidencial mientras mantienen la funcionalidad de notificación. Para más información, consulte Contraseña **Código de acceso y pantalla de bloqueo avanzados de Android**.
- **soporte con la asignación de dispositivo a usuario durante la inscripción masiva de perfiles**: se agregó soporte con la asignación de dispositivo a usuario en perfiles de inscripción masiva. Los administradores pueden asignar un usuario específico a cada dispositivo a través del archivo CSV de inscripción masiva o durante la adición manual de dispositivo, lo que permite la asignación automática de usuarios durante la inscripción y reduce las tareas administrativas posteriores a la inscripción. Los administradores también pueden actualizar las asignaciones de usuarios antes de la inscripción del dispositivo. Para más información, consulte Asignación de **dispositivo a usuario en Perfiles de inscripción masiva**.

Funciones de iOS, macOS, watchOS, visionOS y tvOS

- **Nuevas claves de omisión para los perfiles de inscripción de dispositivos:**: los administradores ahora pueden utilizar las siguientes claves para omitir determinadas pantallas al crear perfiles de inscripción de dispositivos:
  - Omitir el panel de Liquid Glass (iOS 27.0+ y macOS 27.0+)
  - Omitir el panel de aspecto de accesibilidad (iOS 27.0+)
    Estas claves de omisión agilizan el proceso de inscripción al permitir a los administradores ocultar determinados paneles de configuración durante la inscripción de dispositivos. Para obtener información, consulte **Inscripción de dispositivos**.
- **Compatibilidad con el estado operativo del sistema del dispositivo mediante DDM**: Ivanti Neurons for MDM ahora es posible consultar el estado de salud del sistema del dispositivo mediante DDM en la página **Detalles del dispositivo**. Los administradores pueden consultar este estado en **Estado de los componentes del dispositivo** para monitorizar el estado del sistema que notifican los dispositivos supervisados. Para obtener más información, consulte **Introducción a los dispositivos**.

- **Nuevos campos de Detalles del dispositivo para dispositivos Apple:** : se han añadido **nuevos campos** que permiten consultar con mayor detalle el estado de la gestión de dispositivos Apple. Los administradores ahora pueden consultar los siguientes datos:
  - **Modo multiusuario** para dispositivos con iOS 27.0 o posterior. Este campo indica si un iPad está configurado como dispositivo compartido.
  - **Tipo de inscripción de MDM** en dispositivos con iOS 27.0+, macOS 27.0+, tvOS 27.0+, visionOS 27.0+ y watchOS 27.0+.
  - **Retorno al servicio de MDM** con conservación de aplicaciones en dispositivos con iOS 27.0+ y visionOS 27.0+.
    Estos campos ayudan a los administradores a consultar directamente desde la página Detalles del dispositivo la información de configuración e inscripción del dispositivo. Para obtener más información, consulte **Introducción a los dispositivos**.
- **Compatibilidad con la configuración de valores predeterminados de privacidad de las aplicaciones**: los administradores ahora pueden configurar los **valores predeterminados de privacidad** de una o varias aplicaciones mediante Apple Device Declarative Management (DDM). Al iniciar una aplicación por primera vez, los usuarios reciben una única solicitud de consentimiento que les permite aceptar o posponer los permisos recomendados para componentes de privacidad compatibles, como la cámara, el micrófono, la ubicación, Bluetooth y el acceso a la red local. Para Para más información, consulte Valores predeterminados de privacidad de la **Valores predeterminados de privacidad de las aplicaciones**.

> La configuración de valores predeterminados de privacidad de la aplicación ahora es compatible con los dispositivos supervisados de macOS 27.0+.

- **Se agregó un nuevo atributo de Administración de la aplicación DDM**: se agregó el **campo Administración de la aplicación DDM del atributo aplicación DDM de** Apple habilitada a las páginas de 'Búsqueda avanzada' y lista de dispositivo. Muestra qué dispositivos tienen aplicaciones distribuidas a través de DDM. Los administradores pueden activarlo a través de Configuración del usuario. Para obtener más información, consulte **Introducción a los dispositivos**.
- **Configuración de SSO extensible de macOS mejorada: se actualizó**la configuración de SSO extensible de macOS para asignar correctamente atributos de token como nombre de usuario **y** nombre preferidos. Esto resuelve los errores de configuración causados por asignaciones de token a usuario no válidas y permite que los perfiles SSO se implementen correctamente en los dispositivos.
- **Registro mejorado**de Apple:?Los administradores pueden iniciar la recopilación mejorada de registros de Apple en dispositivos Apple compatibles mediante un token proporcionado por AppleCare. Los detalles del dispositivo muestran el estado de la sesión, la información del token y la marca de tiempo, y las sesiones activas se pueden cancelar si es necesario. Para más información, consulte Registro mejorado de **Apple**.
- **estado del modo de bloqueo** (iOS 27+, macOS 27+): se agregó soporte para ver y filtrar dispositivos por estado del modo de bloqueo mediante el nuevo **campo Modo de bloqueo de** seguridad en la **página Detalles del** dispositivo, Búsqueda **avanzada**y reglas del grupo de dispositivos. Este campo indica si el modo de bloqueo está habilitado (**verdadero**) o deshabilitado (**falso**) en un dispositivo. Para más información, consulte **Introducción a los dispositivos** , Grupos de **Grupos de dispositivos** y política **Política personalizada**.
- **Ajustes de actualización de software de macOS Actualización**de soporte : la **configuración** de ajustes de actualización de software de macOS ya no es compatible con macOS 27 y dispositivos posteriores. Esta configuración ahora solo se aplica a versiones compatibles hasta macOS 26.x. Para más información, consulte Configuración de reglas de actualización de software de **Configuración de las reglas de actualización de software macOS**.
- **Actualización del soporte de restricciones** (iOS 27+, macOS 27+): Se actualizaron las **restricciones** Permitir mejoras de seguridad en segundo plano **e** Permitir mejoras de seguridad en segundo plano Eliminación para indicar que ya no son compatibles con iOS 27 y posterior y dispositivos macOS 27 y posteriores. Para más información, consulte Restricciones de **Restricciones de iOS** y Restricciones de **Restricciones de macOS**.

- **Actualizaciones de la configuración de ajustes de Siri** (iOS 27.0+, macOS 27.0+, tvOS 27.0+ y visionOS 27.0+):?Se ha añadido soporte con nuevos ajustes de restricción en la configuración de Ajustes de Siri . Para más información, consulte Ajustes de **Ajustes de Siri**.
- **Actualizaciones de la configuración de ajustes de Intelligence** (iOS 27.0+, macOS 27.0+ y visionOS 27.0+):?Se ha añadido soporte con nuevos ajustes de restricción en la configuración de ajustes de Intelligence. Para más información, consulte Ajustes de **Ajustes de inteligencia**.
- **Ajustes de privacidad de Safari** (iOS 27.0+, macOS 27.0+): se ha añadido soporte con los ajustes de privacidad de Safari en la configuración de la extensión y ajustes de Safari, lo que permite a los administradores configurar permisos predeterminados de cámara y micrófono para sitios web específicos mediante la administración de dispositivo declarativos (DDM) de Apple. Para más información, consulte Extensión de **Configuración de ajustes y extensión de Safari**

Características de Windows

- **¿AI de Windows?Configuración de gestión**:?Windows AI Management ahora admite políticas CSP de Windows AI adicionales para administrar las funciones de Microsoft Copilot, Windows Recall y Microsoft Paint AI. Los administradores pueden deshabilitar la clave de hardware de Copilot, eliminar la aplicación de Microsoft Copilot, deshabilitar el análisis de datos de IA para Recall, configurar los límites de almacenamiento de instantáneas de Recall y deshabilitar Image Creator, Cocreator y Generative Fill in Paint. También se ha añadido soporte con políticas tanto bajo el alcance del usuario como bajo el alcance del dispositivo, lo que permite un control más granular de las funciones de IA en dispositivos Windows. Para más información, consulte Configuración de administración de IA de **Configuración del administrador de IA de Windows**.

Características de Mobile Threat Defense

Mobile Threat Defense (MTD) protege los dispositivos administrados de las amenazas y vulnerabilidades móviles que afectan a dispositivos, redes y aplicaciones. Para obtener información sobre las funciones relacionadas con la MTD, según la versión actual, consulte la Guía de la solución de Mobile Threat Defense para su plataforma, disponible en la sección MOBILE THREAT DEFENSE en la página de **documentación de productos** de Ivanti.

> Cada versión de la «Guía de MTD» contiene todas las características de Mobile Threat Defense que se han probado totalmente a día de hoy y que están disponibles para su uso tanto en entornos de servidor como de cliente. Debido al desfase entre las versiones del servidor y del cliente, las nuevas versiones de la Guía de MTD están disponibles con la última versión de la serie cuando las características son totalmente funcionales.

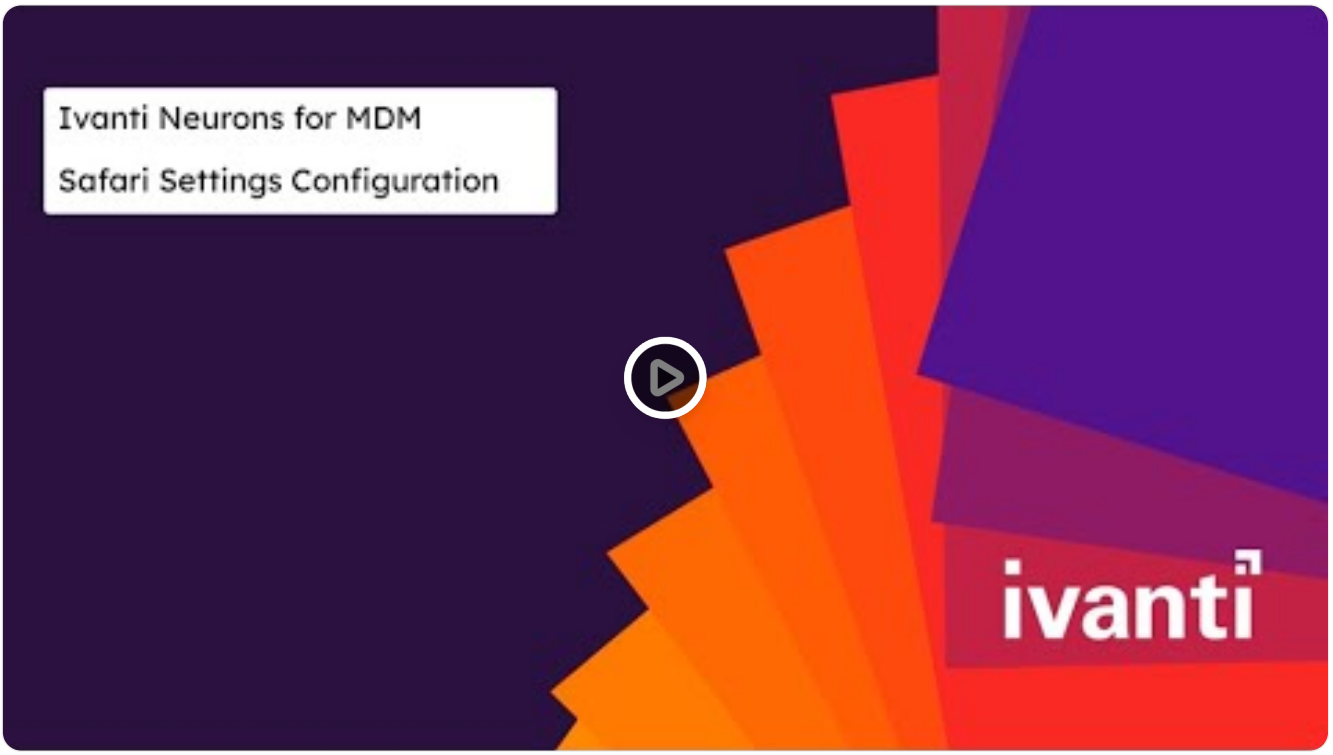
3. Vídeos

Vídeos destacados




Neurons for MDM R120
Appending the
Organization Name to the
Subject of System-
generated Emails
ivanti
Copyright © 2025 Ivanti. All rights reserved.


Neurons for MDM R119
Block App Uninstall for In
House Apps
ivanti
Copyright © 2025 Ivanti. All rights reserved.



¿Busca un vídeo sobre una función o funcionalidad específica en Ivanti Neurons for MDM? Comparta su opinión a través de la sección "**¿Le ha resultado útil este artículo?**" disponible en cualquier página de este documento.

4. Introducción

Esta sección proporciona una visión general de la configuración y el uso de las funciones que requieren la interacción a través del portal de Ivanti Neurons for MDM. Esta sección contiene los siguientes temas:

- Visión general de la solución
  - Características clave
  - Diagrama de arquitectura
  - Ivanti Neurons for MDM aplicaciones
  - Funciones
  - Cómo empezar
- Ajuste del idioma preferido en un navegador
- Interfaz de navegación unificada para Ivanti Neurons for MDM y Access
- El modo Administrador del dispositivo (AD) de gestión de dispositivos Android va a quedar obsoleto.

Visión general de la solución

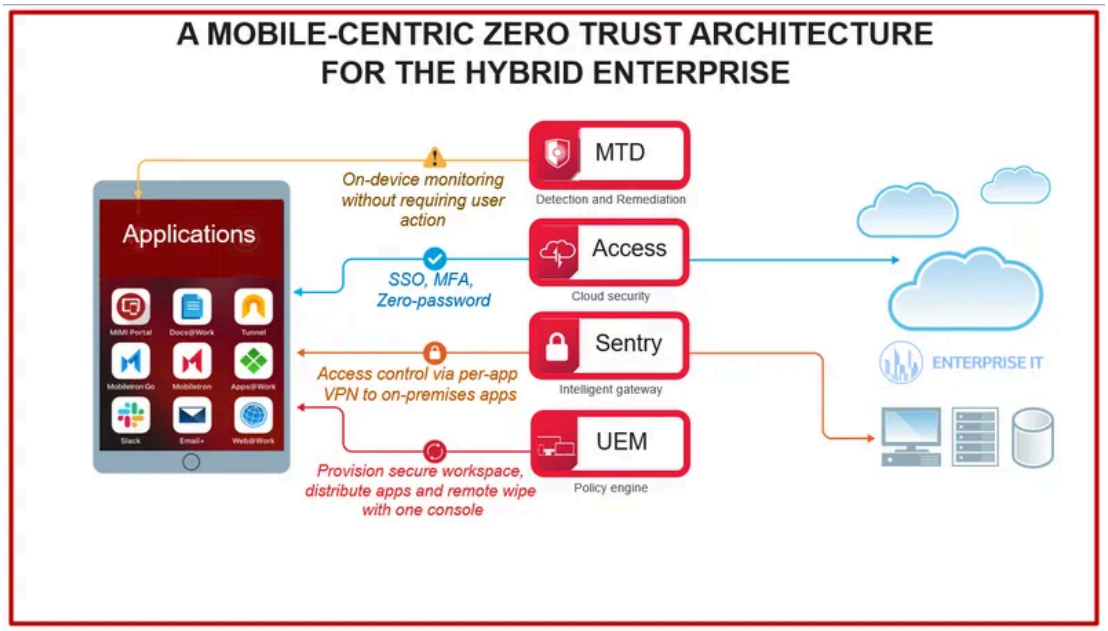
El acceso continuo a los datos de la empresa en dispositivos móviles y otros puntos finales fuera de la red corporativa requiere un enfoque dedicado a la seguridad. Para estar a la altura de las necesidades de seguridad actuales, las empresas deben considerar cómo pueden:

- Aprovisionar puntos finales como teléfonos móviles y ordenadores portátiles
- Conceder acceso basado en un conjunto de datos imperativos
- Proteger los datos en reposo y en movimiento
- Aplicar las medidas necesarias

La solución de Ivanti a este moderno problema responde a todos los retos. Puede supervisar los puntos finales y activar políticas adaptables para remediar las amenazas, poner en cuarentena los dispositivos y mantener el cumplimiento. Juntos, los siguientes componentes ayudan a su organización a realizar el marco de redes de confianza cero centrado en los móviles:

- Ivanti Neurons for MDM le ayuda a crear un espacio de trabajo seguro en cualquier dispositivo con aplicaciones, configuraciones y políticas para el usuario según su rol. Los usuarios obtienen un acceso fácil y seguro a los recursos que necesitan para su productividad
- **Sentry** :Una pasarela inteligente en línea que ayuda a su acceso seguro a los recursos locales
- **Access** :Le ayuda a verificar el usuario, el dispositivo, la aplicación, el tipo de red y la presencia de amenazas. La verificación de control de acceso adaptable es la base del modelo de confianza cero. Access proporciona un inicio de sesión único y seguridad en Cloud
- **Mobile Threat Defense**:La combinación de Ivanti Neurons for MDM y Mobile Threat Defense (MTD) protege los datos en el dispositivo y en la red con un cifrado de última generación y una supervisión de las amenazas para detectar los ataques a nivel de dispositivo, red y aplicación.

La siguiente ilustración muestra la visión general de la solución:



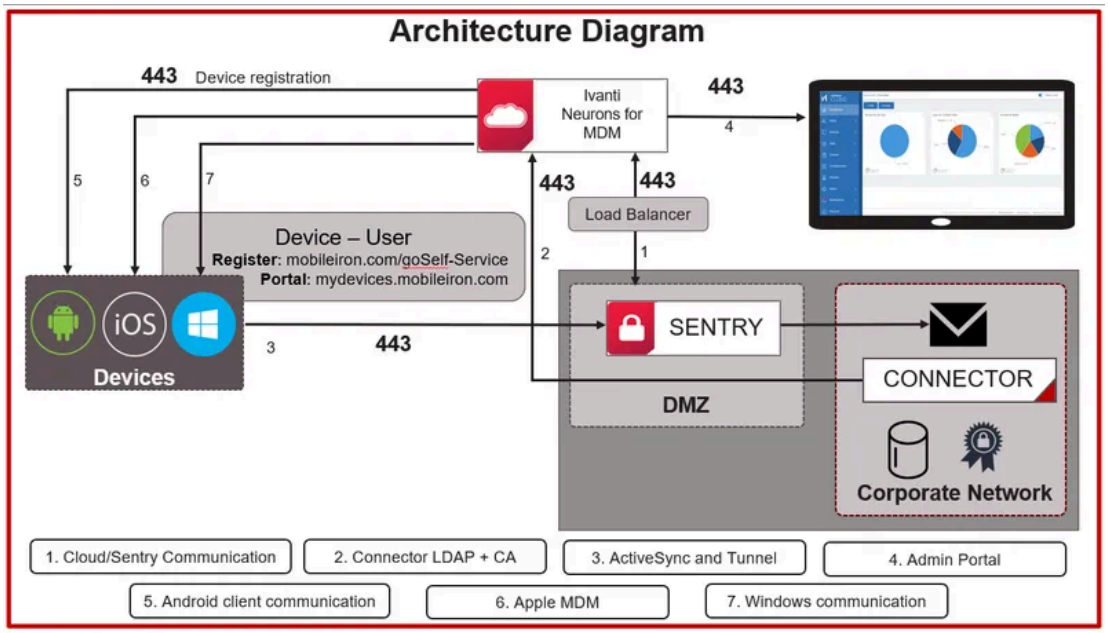
Características clave

La plataforma de Ivanti Neurons for MDM proporciona la visibilidad fundamental y los controles informáticos necesarios para asegurar, administrar y supervisar cualquier dispositivo móvil o de escritorio corporativo o propiedad de los empleados que acceda a datos críticos para la empresa. Ivanti Neurons for MDM La plataforma Ivanti Neurons for MDM permite que las organizaciones aseguren una amplia gama de dispositivos para empleados que se usan dentro de la organización mientras se administra el ciclo de vida completo del dispositivo, lo que incluye:

- Gestión y aplicación de la configuración de políticas
- Distribución y administración de aplicaciones
- Gestión y distribución de guiones para dispositivos de escritorio
- Acciones de dispositivos
- Control de acceso y autenticación multifactorial
- Detección y corrección de amenazas

Diagrama de arquitectura

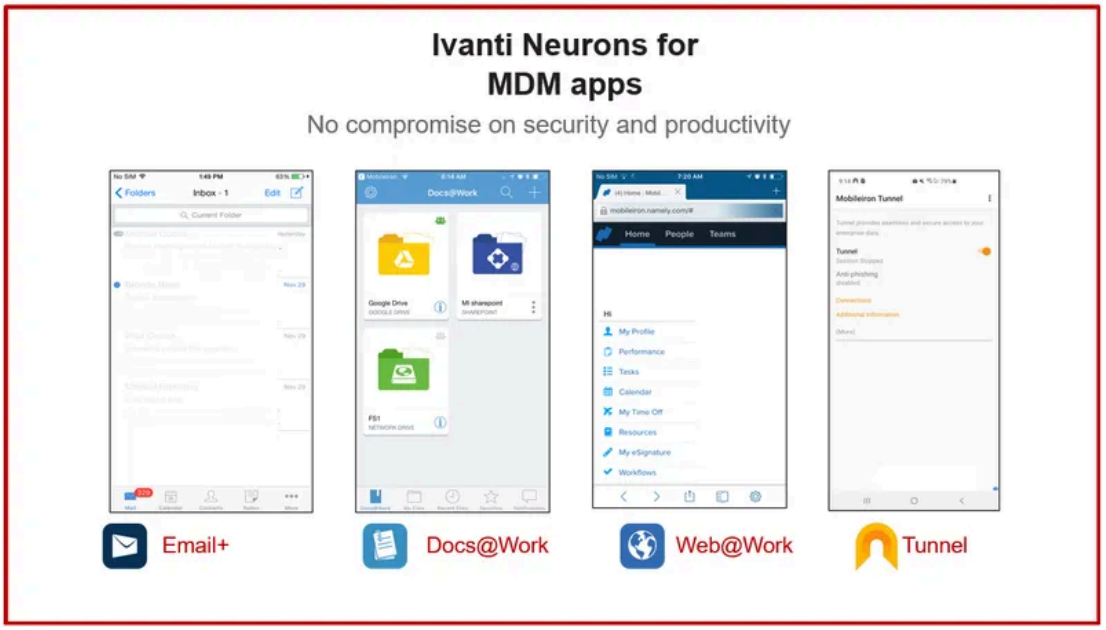
El siguiente diagrama muestra la visión general de la arquitectura de la plataforma Ivanti Neurons for MDM UEM:



Ivanti Neurons for MDM aplicaciones

- **Catálogo de aplicaciones** :El catálogo de aplicaciones es un escaparate de aplicaciones empresariales personalizable. Los administradores de TI pueden publicar directamente aplicaciones privadas o internas en los dispositivos de sus usuarios finales. El App Catalog también puede combinarse con el Programa de Compras por Volumen de Apple para facilitar la distribución segura de aplicaciones móviles en dispositivos iOS. Además, Ivanti puede aprovechar las capacidades que se encuentran en las aplicaciones gestionadas de iOS y Android Enterprise. Esto permite una configuración fácil dentro de la plataforma Ivanti Neurons for MDM UEM de ajustes de nivel aplicación y políticas de seguridad para ambas funciones de seguridad de aplicaciones avanzadas.
- **Email+** :De es una aplicación de gestión de información personal (PIM) segura y multiplataforma para iOS y Android. Email+ proporciona correo electrónico, calendario, contactos y tareas seguras en los dispositivos personales y de la empresa mediante la comunicación con un servidor ActiveSync en su empresa.
- **Docs@Work**: permite a los usuarios acceder, crear, editar, marcar y compartir contenidos de forma segura desde repositorios como Microsoft Share Point, y servicios en la nube como Box y Dropbox. Esto es importante para que los usuarios puedan maximizar la productividad sobre la marcha.
- **Web@Work** :Es un navegador seguro que permite a los usuarios de la empresa acceder de forma segura al contenido web de su intranet corporativa. Con Web@Work se puede limitar el acceso a los datos de la empresa a los usuarios autorizados. Cuando Web@Work se despliega junto con App Tunnel, se aseguran los datos de la empresa en movimiento. Con Web@Work los usuarios pueden acceder a los recursos web internos de forma rápida y sencilla.

La siguiente imagen muestra las aplicaciones en Ivanti Neurons for MDM:



Funciones

Administrador :Como administrador de empresa, es responsable de las siguientes tareas:

- Proporcionar a los usuarios de la empresa un acceso perfecto y seguro a los correos electrónicos, las aplicaciones, las configuraciones y la conectividad del espacio de trabajo, como Wi-Fi y VPN.
- Separar los datos personales de los datos empresariales en los dispositivos de los empleados para que los datos empresariales no se filtren en las aplicaciones personales y los datos personales no sean accedidos inadvertidamente por el departamento de TI.

Usuario :Como usuario de la empresa, puede acceder sin problemas a las aplicaciones empresariales y a los datos personales desde dispositivos móviles, ordenadores de sobremesa y servicios en la nube modernos y seguros. Para obtener más información sobre las distintas tareas que puede realizar como usuario, consulte **Usuarios**. y **Administración de funciones**.

Cómo empezar

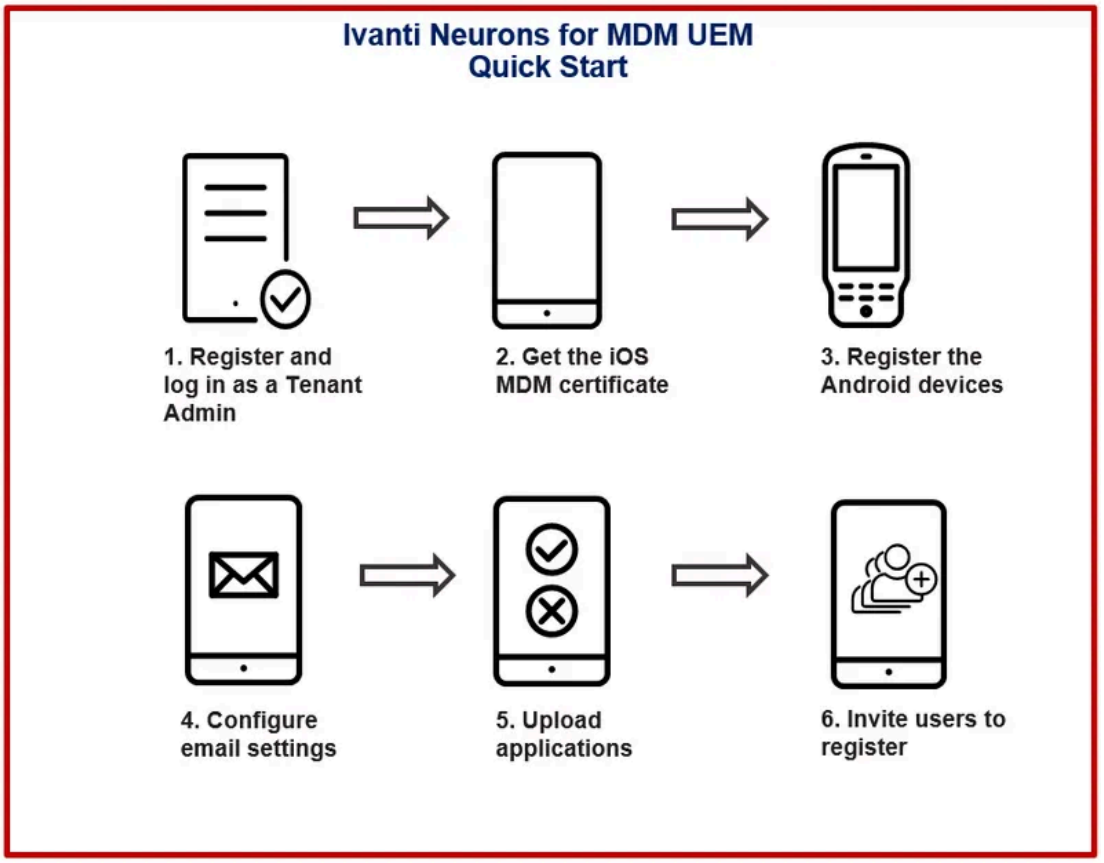
Si es un nuevo usuario registrado, siga los pasos indicados en esta sección para incorporarse rápidamente a los servicios en Ivanti Neurons for MDM.

Luego de suscribirse a la plataforma Ivanti Neurons for MDM, Ivanti le crea un abonado de Ivanti Neurons for MDM. Recibirá un correo electrónico a la dirección de correo electrónico registrada y el correo contiene un PDF con la siguiente información sobre el abonado creado para su empresa:

- Información sobre el paquete de software que ha adquirido
- La URL y las credenciales de inicio de sesión del super administrador del abonado
- Cómo acceder a la comunidad de soporte y a las preguntas frecuentes sobre Ivanti Neurons for MDM
- Dónde acceder a la documentación técnica y descargar el software

> Ivanti, Inc no proporciona claves de software. Al iniciar sesión en su abonado de Ivanti Neurons for MDM con las credenciales del superadministrador y aceptar los términos de servicio, se activa el producto Ivanti Neurons for MDM.

El siguiente diagrama muestra los pasos para comenzar con Ivanti Neurons for MDM:



Procedimiento

1. Haga clic en la URL proporcionada en el correo electrónico de registro de los abonados. Aparece el aviso de restablecimiento de la contraseña.
2. Cambie su contraseña.
3. Inicie sesión en la cuenta del abonado con el ID y la contraseña. Aparece el asistente de bienvenida.
4. Complete los detalles en el formulario de**Bienvenida**, acepte los términos y el acuerdo, y haga clic en **Continuar**.
5. Para instalar el certificado MDM de iOS, consulte **Instalación del Certificado MDM**.

> Si desea gestionar sus dispositivos iOS en un momento posterior, puede omitir la instalación del certificado MDM de iOS. A continuación, el asistente le pedirá que registre los dispositivos Android de su empresa. Tenga en cuenta que si omite la instalación del certificado MDM de iOS, los dispositivos iOS no podrán registrarse. Los usuarios verán un mensaje que indica que la inscripción de dispositivos iOS no se ha habilitado.

6. Para registrar los dispositivos Android en el modo Android Enterprise (AE), consulte **Cuentas administradas de Google Play (cuentas con Android Enterprise)**. A continuación, el asistente le pedirá que configure las cuentas de correo electrónico.

> Si desea administrar sus dispositivos Android en un momento posterior, puede omitir la inscripción de cuentas de Google Play administradas de Android. Si omite la inscripción de cuentas gestionadas de Google Play, no podrá registrar los dispositivos empresariales Android. Los dispositivos Android se pueden seguir registrando con el administrador del dispositivo, pero las características principales como Google Play administrado y la Configuración de aplicaciones no estarán disponibles para usarse.

7. Para configurar las opciones de correo electrónico y ActiveSync, consulte **Configuración de Exchange** y **Configuración de correo electrónico**.
8. Haga clic en **Continuar**. Aparece el aviso de creación de código de acceso.
9. Seleccione un tipo de código de acceso y haga clic en **Continuar**.
10. Seleccione las aplicaciones que desea cargar y haga clic en **Continuar**.
11. Especifique las direcciones de correo electrónico de los usuarios y haga clic en **Continuar**. Los usuarios recibirán un correo electrónico para registrar sus dispositivos móviles. Se muestra un resumen de la configuración.
12. Haga clic en **Finalizado**. Se muestra la página del panel de control.
13. Para seguir explorando, haga lo siguiente:
    - Vaya a **Usuarios**. Todos los usuarios invitados aparecen en la lista.
    - Vaya a **Aplicaciones**. Todas las aplicaciones que has subido aparecen en la lista.
    - Vaya a **Configuraciones**. Se enumeran todas las configuraciones que usted impulsó durante el registro.

Para obtener más información sobre las distintas tareas que puede realizar como administrador, consulte la sección **Administración**.

Ajuste del idioma preferido en un navegador

Si un usuario ha configurado el idioma de su navegador como uno que no es compatible, el usuario puede establecer en_US (inglés de Estados Unidos) como el idioma predeterminado para el portal.

Para establecer la preferencia de idioma en el navegador Safari que se ejecuta en dispositivos macOS 10.15+, los usuarios pueden establecer el idioma preferido de la siguiente manera:

1. En el dispositivo macOS, vaya a **Preferencias del sistema**.
2. Vaya a **Idioma y región > General.**
3. Configure la opción **en_US** (o cualquier otra opción de idioma) como el **Idioma preferido**.

Interfaz de navegación unificada para Ivanti Neurons for MDM y Access

Para clientes nuevos en algunos clústeres, Access está disponible como interfaz de navegación unificada con Ivanti Neurons for MDM . Inicie sesión con sus credenciales de administrador de Ivanti Neurons for MDM. Las opciones de Access están disponibles en el panel de navegación izquierdo en forma de pestaña independiente. Visite la **Documentación del producto** y haga clic en Access para obtener más información sobre Access y cómo configurarlo.

La interfaz de navegación unificada incluye las siguientes características:

- Inicio de sesión unificado tanto para Ivanti Neurons for MDM como para Access.
- Selector de productos en el panel de navegación izquierdo para cambiar entre los productos de Ivanti Neurons for MDM y Access.

- Memoria de selección de productos: una vez que haya iniciado sesión por primera vez, aparecerá el portal de administración de Ivanti Neurons for MDM. En los siguientes inicios de sesión, aparecerá Ivanti Neurons for MDM o Access, según el producto que se seleccionó la primera vez que se inició sesión.
- Panel de navegación izquierdo tanto para Ivanti Neurons for MDM como para Access.
- Panel de configuración de cuenta unificado con enlaces a opciones como Opciones de actualización, Documentación, Portal de asistencia, Cambiar contraseña y Cerrar sesión.

El modo Administrador del dispositivo (AD) de gestión de dispositivos Android va a quedar obsoleto.

Se está dejando de usar el modo de administrador del dispositivo (DA) para administrar dispositivos Android de manera gradual desde Ivanti Neurons for MDM 78 en adelante.

Todos los nuevos usuarios con un abonado nuevo creado en Ivanti Neurons for MDM 78 no podrán registrar ningún dispositivo (Android 6 y posterior) en modo DA. Los nuevos abonados que necesiten habilitar el registro de AD para Android 6 a Android 9 deben ponerse en contacto con la asistencia técnica de Ivanti.

- Los dispositivos con Android 10 y posteriores seguirán teniendo bloqueado el registro en el modo AD.
- Para los usuarios existentes (con o sin implementaciones en modo AD), no hay cambios en términos de gestión de los dispositivos en modo AD existentes (Android 6 a Android 11). No obstante, al actualizar a Ivanti Neurons for MDM 78, los dispositivos recién registrados que ejecuten Android 10+ en abonados existentes tampoco podrán funcionar en modo DA. Dichos abonados existentes solo podrán inscribir dispositivos de las versiones Android 6 a Android 9 en modo AD.
- Si algún usuario tiene previsto migrar dispositivos DA de una instancia Core a Ivanti Neurons for MDM R78, asegúrese de que Android Enterprise está habilitado y de que al menos una configuración del sistema se distribuye al conjunto de destino: PO, DO o COPE antes de activar la migración. Este paso es esencial para evitar la retirada de dispositivos tras la migración.

Tipo de registro AD	Abonado existente (actualizado a 78)	Nuevo abonado
Nuevo registro AD del dispositivo con OS >=10	No permitido	No permitido
Nuevo registro AD del dispositivo con OS <10	Permitida	No permitido
Dispositivos AD existentes con OS >=10	Permanecerá activo	N/A
Dispositivos AD existentes con OS <10	Permanecerá activo	N/A
Dispositivos AD migrados con OS >=10	Se retirará	Se retirará
Dispositivos AD migrados con OS <10	Permanecerá activo	Se retirará

4.1. Configuración de dispositivos macOS

Este es un resumen que ofrece una lista de procedimientos frecuentes y otro contenido relacionado con la configuración de dispositivos macOS en Ivanti Neurons for MDM Puede acceder a todos los temas de macOS en la *Guía para el administrador de* Ivanti Neurons for MDM.

Contenido

- Registro de dispositivos
- Configuración de la plantilla de invitación de usuarios
- Configuración de funciones Zero Sign-on
- Configuración de Mobile@Work para el cliente macOS
- Configuración de secuencias de comandos de shell en macOS
- Configuración de ajustes de macOS
- Configuración de directivas de macOS

Registro de dispositivos

La mayoría de los usuarios comienzan por registrar un dispositivo. Para iniciar el proceso de registro, puede hacerlo de cualquiera de las siguientes formas:

- Envíe una invitación a uno o más usuario (registro de iReg). Para obtener más información, consulte el tema *Registro de dispositivos de macOS* en la sección **Registro de dispositivos**.
- **Inscripción de dispositivos** e **Inscripción de usuarios en Apple Business Manager**

Para obtener más información, consulte en Registro de dispositivo.

Configuración de la plantilla de invitación de usuarios

Puede personalizar la invitación por correo electrónico del usuario final para que la apariencia le resulte más familiar a sus usuarios finales. Para obtener más información, consulte **Plantillas de correo electrónico de personalización de marca**.

Puede personalizar el proceso de registro del dispositivo con nombres y logotipos que sus usuarios reconocerán. Para obtener más información, consulte **Personalización de marca dispositivos**.

Para obtener más información, consulte **Configuración y uso de correos electrónicos de confirmación del registro**.

Configuración de funciones Zero Sign-on

Para la documentación relacionada con Zero Sign-on, consulte «Zero Sign-on con Access» en la *Guía de Access*.

Para la inscripción automática de Zero Touch, consulte el paso 13 del tema Ajustes de usuario en la sección Configurar los ajustes para registrar dispositivos nuevos.

Configuración de Mobile@Work para el cliente macOS

Mobile@Work para macOS proporciona lo siguiente:

- Prestaciones de secuencia de comandos en dispositivos macOS

- Catálogo de aplicaciones para usuarios finales
- Notificaciones «push»
- Pantalla de Incorporación del usuario (bienvenido/estado) para los registros de la inscripción de dispositivos automatizada

Antes de forzar Mobile@Work en los usuarios finales, asegúrese de que **Mobile@Work for macOS Configuration.htmMobile@Work para macOS** se ha creado y de que está ajustado para que se distribuya en los equipos de macOS de destino.

Puede habilitar la incorporación de usuarios a los dispositivos macOS durante el proceso automatizado de **Inscripción de dispositivos**. Tan pronto como se completa la Inscripción de dispositivos, Mobile@Work para macOS se inserta en el dispositivo junto con los perfiles, configuraciones y aplicaciones.

Configuración de secuencias de comandos de shell en macOS

Ivanti Neurons for MDMle permite crear sus propias secuencias de comandos de shell de macOS que luego pueden cargarse y Ivanti Neurons for MDMejecutarse en dispositivos macOS administrados. Se pueden configurar las secuencia de comandos utilizando la configuración de secuencia de comandos de Mobile@Work para macOS. Mobile@Work para macOS regresa los resultados de ejecución de la secuencia de comandos a Ivanti Neurons for MDM, y estos se muestran en los registros del dispositivo. Puede verificar los registros del dispositivo desde la página de detalles del dispositivo macOS, en la pestaña **Registros**. Para obtener más información sobre cómo crear, cargar y administrar el repositorio de secuencias de comandos, consulte **Todas las secuencias de comandos**.

Antes de poder ejecutar las secuencias de comandos de shell en dispositivos macOS, asegúrese de que los usuarios dispongan de la aplicación Mobile@Work para macOS en sus dispositivos y tengan una configuración de Mobile@Work para macOS insertada en sus dispositivos. Las secuencias de comandos se pueden ejecutar una vez o de manera recurrente. Las secuencias de comando de Ivanti Neurons for MDM también permiten que los administradores recopilen información de un dispositivo y, a continuación se la almacene en Ivanti Neurons for MDM como atributo personalizado. Por ejemplo, si necesita saber cuál es la versión de Java de un dispositivo macOS, puede recopilar esta información y almacenarla individualmente por cada dispositivo en un atributo personalizado del dispositivo. Para obtener más información, consulte *Cómo crear una configuración de secuencia de comandos Mobile@Work para macOS* en **Mobile@Work para macOS.**

Configuración de ajustes de macOS

Las **Configuraciones** son conjuntos de ajustes que se envían a los dispositivos. Por ejemplo, se pueden usar configuraciones para establecer los ajustes VPN y los requisitos del código de acceso en estos dispositivos. Utilice la página **Configuraciones** para seleccionar, configurar y distribuir configuraciones. Hay muchos **tipos de configuraciones** disponibles. En esta **página**, puede ver una lista de las configuraciones disponibles de macOS, incluidas las siguientes:

- **Wi-Fi**
- **Código de acceso**
- **VPN**
- **DNS cifrado**
- **FileVault 2**
- **Clave de recuperación de FileVault**
- **Firewall de macOS**
- **Restricciones de macOS**
- **Restricciones de la AppStore de macOS**

- Ajustes del Finder de macOS
- Política de extensiones del kernel de macOS
- Active Directory (macOS)
- Creación automática de cuentas en Office 365(macOS)

Puede utilizar configuraciones predeterminadas para importar y distribuir un archivo de configuración predeterminada.

Configuración de directivas de macOS

Las Directivas definen los requisitos para los dispositivos, así como lo que pasará si un dispositivo no cumple con los requisitos. Cada política cuenta con una regla y una medida de cumplimiento (lo que sucede si se infringe la regla). Utilice la página **Políticas** para seleccionar, configurar y distribuir políticas. La protección de datos/cifrado desactivado y Aplicaciones permitidas son directivas relacionadas con macOS. Puede utilizar Directivas personalizadas según el dispositivo y los atributos del usuario, los criterios de la sección, los valores y las medidas de cumplimiento que se especifiquen.

Distribución de aplicaciones para macOS

Ivanti Neurons for MDM es compatible con la distribución de aplicaciones macOS mediante el protocolo MDM de Apple y la aplicación Mobile@Work. Los administradores pueden optar por utilizar uno o ambos de los siguientes enfoques:

- Protocolo MSM de Apple: Los administradores pueden cargar únicamente formatos PKG específicos (formato de distribución) como aplicaciones internas y también pueden distribuir aplicaciones desde Mac App Store (se incluye el soporte para licencias de Apps and Books de Apple). Sin embargo, este enfoque no permite que los administradores distribuyan DMG y otros formatos PKG.
- Mobile@Work for macOS app - As a way to distribute apps to users, administrators can use MobileIron Packager (MIP) app to convert any PKG, DMG or .app files to an MIP file. Cargue el archivo MIP a Ivanti Neurons for MDM como aplicación interna.

> Puede descargar el servicio Mac Packager de Ivanti Neurons for MDM desde las descargas de software de MobileIron.

Los administradores pueden utilizar Mobile@Work para distribuir aplicaciones internas que están en formato DMG, PKG o .app. Para las aplicaciones que solo están disponibles en Mac App Store, los administradores pueden continuar usando las prestaciones de MDM, que incluyen las prestaciones de las licencias de Apps and Books de Apple.

4.2. Configuración y uso de los correos electrónicos de confirmación de registro

Los administradores pueden configurar y activar los correos electrónicos para los usuarios una vez que hayan completado el registro. Este correo electrónico puede contener, por ejemplo, instrucciones adicionales para los usuarios después de haberse registrado con éxito. Los administradores pueden activar el envío de este correo electrónico durante la invitación del usuario.

El proceso:

- **Configuración de la función:**
  - Configure la plantilla de correo electrónico: la plantilla de correo electrónico en inglés tiene este aspecto por defecto, pero se puede revisar para que se adapte mejor a sus necesidades siguiendo las instrucciones que hay en **Personalización de una plantilla de correo electrónico** en **Cómo personalizar las plantillas de correo electrónico**.



  - Active el correo electrónico de confirmación de registro. Consulte **Configuración de los correos electrónicos de confirmación de registro del usuario** en **Ajustes del usuario**.
- **Cómo usar esta función:**
  - Envíe al usuario la invitación para registrarse, según se describe en **Invitar a usuarios**. Cuando el usuario se registra correctamente, Ivanti Neurons for MDM enviará a ese usuario el correo electrónico de confirmación de registro.

4.3. Configuración y uso de los correos electrónicos de notificación de cumplimiento de políticas

Los administradores pueden ajustar en una plantilla de correo electrónico de notificación de cumplimiento de políticas los correos electrónicos enviados por las acciones de envío de correos «políticas de aplicaciones personalizadas y permitidas» para los usuarios cuyos dispositivos hayan infringido el cumplimiento. Los siguientes procesos describen la configuración:

- **Configuración de la función:**
  - **Configure la plantilla de correo electrónico**.
    La plantilla de correo electrónico en inglés tiene este aspecto por defecto, pero se puede revisar para que se adapte mejor a sus necesidades siguiendo las instrucciones que hay en **Personalización de una plantilla de correo electrónico** en **Cómo personalizar las plantillas de correo electrónico**

    
  - **Active la plantilla de notificación de cumplimiento de políticas**. Esta plantilla funciona junto con el mensaje que se elabora mediante las acciones de envío de correo electrónico de «políticas de aplicaciones personalizadas y permitidas» . Ivanti Neurons for MDM inserta la información que usted especifica en esas acciones de correo electrónico en la plantilla de notificación de cumplimiento de políticas. Se puede activar la plantilla de correo electrónico de cumplimiento de políticas al crear o editar una política de aplicaciones personalizadas o permitidas. Para obtener más información sobre las instrucciones para habilitar la plantilla de notificación de cumplimiento de políticas para una política Personalizada o una política de Aplicaciones permitidas, consulte **Añadir una política personalizada** y **Crear una Política de aplicaciones permitidas** respectivamente.
- **Cómo usar esta función:**
  - Cuando un dispositivo no cumple con una política de aplicaciones personalizadas o permitidas con la plantilla de notificación de políticas activada, Ivanti Neurons for MDM envía un correo electrónico al propietario del dispositivo, y ajusta primero el correo electrónico en la plantilla de notificación de políticas. Su interacción con esta función consiste en configurarla como se ha resumido anteriormente, mientras que Ivanti Neurons for MDM es quien hace uso de esta función.

4.4. Características a petición

Ivanti Neurons for MDM incluye determinadas funciones a pedido que, de forma predeterminada, están deshabilitadas. Dichas características podrían tener algún impacto en el rendimiento y podrían no estar completamente listas para su implementación en la producción.

Los administradores pueden contactar con la **Asistencia técnica** si están interesados en activar una o más de las características a petición en los dispositivos de los abonados que estén desactivados por defecto.

En el siguiente cuadro se incluye la lista de características documentadas a petición:

Característica	Descripción	Plataforma(s)	Licencia
Características de Windows 10	Características aplicables a los dispositivos con Windows 10.	Windows 10	• Antiguo: Gold • Actual: Secure EUM Consulte **Paquetes** para obtener más información sobre las ofertas antiguas y actuales.
Copiar URL del catálogo de aplicaciones al portapapeles	Permite a los administradores copiar la URL del catálogo de aplicaciones al portapapeles para las aplicaciones. Esta URL puede distribuirse a los usuarios por correo electrónico. Si el usuario hace clic en el vínculo desde un dispositivo registrado, el catálogo de aplicaciones con la aplicación se abrirá en el navegador. Aquí, el usuario podrá elegir instalar la aplicación. Los administradores son responsables de restringir la distribución de esta URL a los usuarios deseados.	• iOS • macOS	N/A (Específico para abonados)
Configurar un clip web como aplicación	Configure un **clip web** como aplicación en el catálogo de aplicaciones para que la aplicación web esté disponible para los usuarios en el catálogo de aplicaciones. El clip web se puede definir como una configuración, pero esta solo la puede insertar el administrador. Los usuarios pueden optar por instalar la aplicación web en sus dispositivos o no hacerlo, mientras que no pueden rechazar la configuración del clip web.	iOS	N/A (Específico para abonados)
Activar el registro de dispositivos de la lista de permitidos	Permita el registro de dispositivos en función de los números de serie de la lista de permitidos en Usuarios > **Ajustes del usuario** > Configuración predeterminada de registro de dispositivos.	• iOS • macOS	N/A (Específico para abonados)
Autenticación basada en certificados	**La autenticación basada en certificados** permite a los administradores iniciar sesión utilizando certificados digitales y un nombre de host especificado por el abonado o un nombre de host mnemónico. Esta configuración de autenticación se puede configurar mediante la configuración del host mnemónico en la pestaña **Administrador**.	Esta función no es específica de la plataforma.	N/A (Específico para abonados) Esta función solo está disponible en los entornos de clústeres NA3 y solo si está habilitada por la Asistencia técnica.

Característica	Descripción	Plataforma(s)	Licencia
Crear una configuración de dispositivos dedicados (de un solo uso propiedad de la empresa, o COSU)	Los administradores pueden configurar dispositivos exclusivos que se pueden usar con una finalidad específica mediante Android Enterprise con la configuración de dispositivos exclusivos (propiedad de la empresa y uso único, o COSU). La **configuración de COSU** se distribuye a los dispositivos administrados para el trabajo (modo propietario del dispositivo) para proporcionar solo una aplicación disponible a los usuarios en modo kiosco.	Android Enterprise	Licencia
Periodo de inactividad del tablero de resultados	Por defecto, el periodo de inactividad del tablero de resultados se ajusta para 15 días. Esto se puede actualizar según las necesidades del abonado y hasta un máximo de 30 días. Si necesita un periodo de inactividad más largo, contacte con el equipo de **Soporte técnico**.	Esta función no es específica de la plataforma.	

4.5. Preparación para la compatibilidad con un dispositivo de Android Enterprise

Esta sección describe los requisitos de red mínimos para dispositivos de Android Enterprise. Los dispositivos Android generalmente no requieren que abra puertos de entrada en el cortafuegos para funcionar correctamente. No obstante, hay una serie de conexiones de salida que los administradores deben conocer cuando ajustan sus entornos de red para los dispositivos de Android Enterprise.

La lista de cambios en la red que figura en el siguiente cuadro no es exhaustiva y puede cambiar. Cubre los puntos finales conocidos para las versiones actuales y pasadas de las aplicaciones de gestión empresarial API y GMS.

> Además de los puestos que se listan en la tabla siguiente, los dispositivos de Android Enterprise requieren acceso a Ivanti Neurons for MDM.

Para obtener información sobre los requisitos de los dispositivos Android Enterprise, consulte **Requisitos de red para Android Enterprise** de la Ayuda de Android Enterprise.

Google no proporciona IP específicas, por lo que debe permitir que su cortafuegos acepte conexiones salientes a todas las direcciones IP contenidas en el bloque IP que aparece en el ASN de Google de 15169 que se enumera aquí: **http://bgp.he.net/AS15169#_prefixes**.

> Las IP de los puntos de Google y los nodos de Edge no aparecen en los bloques AS15169. Consulte **https://peering.google.com/** para obtener más información sobre la red Edge de Google.

5. Panel

El panel muestra importantes estadísticas sobre los dispositivos registrados y los usuarios. Cada sección del panel se llama widget. En cada widget se define:

- la categoría de los datos mostrados (por ej. «dispositivos» o «usuarios»)
- cómo se agrupan los datos (por ej., por versión del SO o por modelo)
- cómo se filtran los datos (por ej., mostrar solo dispositivos iOS o muestra la versión de SO)
- cómo se muestran los datos (por ej., en un gráfico circular o gráfico de barras)

Verificación de informes y otra información

El **Panel** muestra importantes estadísticas sobre los dispositivos registrados y los usuarios. Cada sección del panel se llama widget.

Puede verificar la información adicional de la siguiente manera:

- **Revisar las notificaciones**: vaya a la página **Panel > Notificaciones** (o haga clic en el icono de la campana, en la esquina superior derecha) para consultar las notificaciones y realizar las acciones necesarias.
- **Informes**: vaya a la página **Panel > Informes** para consultar los datos de su sistema de gestión unificada de endpoints (UEM).
- **Rastros de auditoría**: vaya a la página **Panel > Rastros de Auditoría** para consultar el registro cronológico de las actividades realizadas en todas las entidades de Ivanti Neurons for MDM. Para habilitar esta función, vaya a la página **Administrador > Infraestructura > trazas de auditorías** y haga clic en **Habilitar trazas de auditoría**.
- **Información sobre aplicaciones**: vaya a la página **Panel > Información sobre aplicaciones** para consultar y analizar la distribución de las aplicaciones y otros datos relacionados.

Esta sección contiene los siguientes temas:

- **Trabajar con widgets**
- **Datos sobre aplicaciones**
- **Uso de Informes programados**
- **Uso de Informes personalizados**

5.1. Trabajar con widgets

Esta sección contiene los siguientes temas:

- Añadir un widget
- Organizar los widgets
- Editar un widget
- Revisar notificaciones
- Informes
- Audit Trails

El panel muestra importantes estadísticas sobre los dispositivos registrados y los usuarios. Cada sección del panel se llama widget. En cada widget se define:

- la categoría de los datos mostrados (por ej. «dispositivos» o «usuarios»)
- cómo se agrupan los datos (por ej., por versión del SO o por modelo)
- cómo se filtran los datos (por ej., mostrar solo dispositivos iOS)
- cómo se muestran los datos (por ej., en un gráfico circular o gráfico de barras)

Añadir un widget

1. Haga clic en **Añadir** (arriba a la derecha).
2. Asigne un nombre al widget.
3. Seleccione una categoría de datos.
4. Complete las opciones de filtrado a medida que se muestran.
5. Seleccione el tipo de visualización predeterminada (gráfico circular, gráfico de barras, gráfico de líneas).
6. Haga clic en **Hecho**.

Organizar los widgets

Los widgets siempre se muestran en filas de tres. Sin embargo, pueden cambiar el orden en que aparecen:

1. Haga clic en **Organizar** (arriba a la derecha).
2. Arrastre los cuadros en el orden en que quiere que aparezcan los widgets.
3. Haga clic en **Aceptar**.

Editar un widget

1. Haga clic en el icono de ajustes del widget (arriba a la derecha).
2. Seleccione **Editar**.
3. Realice los cambios.
4. Haga clic en **Hecho**.

Revisar notificaciones

Haga clic en el icono de la campana (arriba a la derecha) o vaya a la página **Panel > Notificaciones** para revisar las notificaciones y tomar medidas cuando sea necesario en función de los siguientes criterios:

- Tipo de componente
  - APP
  - LDAP
  - Entra ID
  - Lista de permitidos de dispositivos
  - Apps and Books
  - iOS
  - Android
  - macOS
  - visionOS
  - watchOS
  - tvOS
  - Abonado
  - EC
  - Conector
  - Sentry
  - Token del servidor de inscripción de dispositivos

Tipo de notificación

  - Caducidad
  - Sincronización de datos
  - Límite de uso
  - Acción administrativa
  - Error de autenticación del servidor
  - Error de validación
  - Cambio de estado

Gravedad

  - Borrado
  - Información
  - Crítica
  - Advertencia

Los administradores pueden seleccionar el componente APP para revisar rápidamente todas las notificaciones específicas para la aplicaciónen la página de Notificaciones y también en la sección notificaciones de campana. Si hay que aceptar algún nuevo permiso para las aplicaciones de Google Play, los administradores podrán aceptarlos después de hacer clic en las notificaciones en lugar de visitando la página de cada aplicación para revisar y aceptar los permisos.

> Ivanti Neurons for MDM los clientes/abonados obtendrán notificaciones de aprobación de la aplicación de Android Go aunque la aplicación no se haya importado al Catálogo de aplicaciones.

Revisar la caducidad de la contraseña del usuario y las notificaciones de cambio de ID

Los administradores pueden revisar la próxima caducidad de las contraseñas en la página **Notificaciones**. También se les notifica de la caducidad de las contraseñas desde las dos semanas anteriores hasta el día anterior, incluidos enlaces a los archivos con informes CSV que contienen las listas de los usuarios correspondientes. Una vez que la contraseña expire, ya no se generarán más notificaciones.

Asimismo, los administradores pueden revisar una notificación que enumera los usuarios cuyas ID (UID) se han detectado que han sufrido cambios durante la última sincronización de LDAP.

Borrar una notificación

Puede borrar manualmente las notificaciones de cualquier gravedad siempre que sea necesario desde la página **Notificaciones**.

1. En la página **Notificaciones**, haga clic en el icono de la columna **Acciones** para ver la notificación que desea borrar. Aparecerá la ventana **Confirmar borrado de la notificación**.
2. Haga clic en **Borrar notificación**. Una vez borrada, el estado de la notificación cambiará a **Borrada** en la columna **Estado**.

> El recuento total de las notificaciones que se borran se muestra en la página **Notificaciones**.

Informes

En la página **Panel > Informes**, puede acceder a los datos de su sistema de administración unificada de puntos de conexión (UEM, Unified Endpoint Management). Por ejemplo, los administradores pueden agregar información, como Nombre de espacio del dispositivo y Atributos personalizados del dispositivo, a los informes mediante la opción de filtro correspondiente, al mismo tiempo que crear informes de dispositivos y de dispositivos bloqueados. Por consiguiente, estos informes tienen columnas para el Nombre del espacio del dispositivo y los Atributos personalizados del dispositivo, respectivamente. Los Atributos personalizados del dispositivo están disponibles en las opciones de filtrado mientras se crea un informe. Los administradores pueden elegir de la lista de claves de atributos de dispositivos personalizados que se utilizan para los dispositivos y seleccionar los operadores disponibles.

A partir de Ivanti Neurons for MDM 76, los operadores de todas las plantillas de informes tienen operadores estándar. Los operadores de las siguientes plantillas están estandarizados en esta versión:

- Panel de control > Informes > Crear informe

A continuación se describe el flujo de trabajo de un informe:

1. Elegir - seleccionar de una plantilla de informes predefinidos.
2. Definir alcance - establecer el período de tiempo de los datos del informe.
3. Establecer detalles - nombrar y personalizar su informe.
4. Ejecutar o programar - ejecutar el informe inmediatamente o crear una programación.
5. Compartir - especificar quién recibirá el informe.

Temas relacionados:

- Panel > Informes (programados)

- Panel > Informes (personalizados)

Búsqueda rápida: vaya a la pestaña Informes. El campo de búsqueda rápida le permite buscar a partir de las siguientes columnas, incluso si incluye espacios o caracteres especiales:

- NOMBRE
- DESCRIPCIÓN
- NOMBRE DE LA PLANTILLA

Audit Trails

Rastros de auditoría ofrecen un registro cronológico de las actividades realizadas en Ivanti Neurons for MDM. Estos registros incluyen las acciones realizadas por administradores, usuarios finales y componentes del sistema.

Los administradores utilizan **Rastros de auditoría** para revisar cambios, comprobar las acciones realizadas, solucionar problemas y respaldar las comprobaciones de conformidad. **Los rastros de auditoría** permiten realizar un seguimiento de acciones como la adición, actualización y eliminación de entidades administradas, incluidos los dispositivos. Para obtener más información, consulte Registro de dispositivos (iOS, macOS y Android).

Activar trazas de auditorías

Debe habilitar la opción **Rastros de auditoría** para poder registrar las actividades realizadas en Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Administración** > **Infraestructura** > **Rastros de auditoría**.
   Aparecerá el panel **Rastros de auditoría**.
2. Active el botón **Exportación de rastros de auditoría**.

> Después de habilitar la opción Registros de auditoría, no podrá desactivarla. Si necesita desactivarla, póngase en contacto con Soporte de Ivanti.

Consultar los registros de auditoría

Siga estos pasos para consultar más detalles sobre los **Rastros de auditoría**:

Procedimiento

1. Vaya a **Panel**> **Rastros de auditoría**.

Aparecerá el panel **Rastros de auditoría**.

2. En la siguiente tabla se muestran los detalles que aparecen en el panel **Rastros de auditoría**:

Ajuste	Descripción
Icono	Muestra el icono de actividad correspondiente al evento de auditoría..
Actividad	Muestra la acción realizada, como el registro de entrada del dispositivo o el inicio de sesión del administrador.
Estado	Indica si la actividad se completó correctamente o si falló. Si un informe no se genera correctamente, puede volver a ejecutar la tarea desde **Historial de informes**. Utilice esta opción para volver a ejecutar la tarea fallida sin crear una nueva programación de informes.
Realizado por	Muestra el administrador o usuario que realizó la actividad.
Realizado en	Muestra la fecha y hora en que se produjo la actividad.
Realizado el	Muestra el dispositivo, la cuenta u objeto afectados por la actividad.
Detalles	Muestra información adicional sobre la actividad.
Tipo	Muestra el tipo de actividad, como Acción del dispositivo o Cuenta.
Categoría	Indica el área funcional a la que pertenece la actividad, como Gestión de dispositivos o Acceso al portal de administración.

3. Haga clic en el botón **Acciones** para acceder a las siguientes opciones:

- **Configurar los ajustes de los rastros de auditoría**: seleccione esta opción para acceder a la configuración de **Rastros de auditoría** en **Administración** > **Infraestructura** > **Rastros de auditoría**.
- **Exportar a CSV**: seleccione esta opción para exportar y descargar los **rastros de auditoría**.

4. (Opcional) Puede utilizar los **Filtros** para consultar determinados **rastros de auditoría**.

Vista de detalles de la actividad

El icono **Cambios: antes y después** aparece en la columna **Panel** > **Rastros de auditoría** > **Detalles**. Permite a los administradores comparar los valores de los atributos antes y después de una acción auditada. Esta comparación facilita identificar qué ha cambiado, verificar las actividades de los usuarios o del sistema y solucionar problemas relacionados con las actualizaciones de configuración.

Haga clic en el icono para consultar los detalles de la comparación de los rastros de auditoría en el panel **Cambios de los rastros de auditoría: antes y después,** donde se muestra la siguiente información:

Ajuste	Descripción
Atributo	Aparece el nombre del atributo modificado. Por ejemplo, `createdAt`.
Antes de	Muestra el valor del atributo antes de realizar la acción. Se resalta en rojo.
Después de	Muestra el valor del atributo después de realizar la acción. Se resalta en verde.

Búsqueda avanzada de rastros de auditoría

Utilice la opción Búsqueda avanzada para buscar rastros de auditoría en función de reglas. Defina criterios específicos para identificar y consultar actividades. Puede utilizar los siguientes atributos para realizar una búsqueda avanzada:

- **Actividad**
- **Categoría**
- **Creado el**
- **Realizado por**
- **Realizado el**
- **Nombre del espacio**
- **Estado**
- **Tipo**

Creación de informes de rastros de auditoría

Puede programar los **informes de auditoría** para que se ejecuten cada 12 o 24 horas, o crear informes personalizados. Además, puede ejecutar informes de **rastros de auditoría** bajo demanda. Los informes bajo demanda no siguen una programación e incluyen los **rastros de auditoría** correspondientes a las últimas 24 horas.

Puede generar un informe de rastros de auditoría en uno de los siguientes formatos:

- CSV
- JSON
- CEF

Además, al crear un informe en **Rastros de auditoría** > **Distribución de informes**, puede seleccionar la opción **Exportación SFTP** para exportar y cargar toda la información de los registros de auditoría en una ubicación específica del servidor. La exportación de registros de auditoría utiliza Secure Shell File Transfer Protocol (SFTP). El servidor debe estar accesible mediante el puerto predeterminado. Puede configurar **Exportación de rastros de auditoría** para que los archivos de auditoría se carguen automáticamente en una ubicación específica. Para más información, véase **Exportar trazas de auditorías**.

Para obtener más información sobre la creación de informes, consulte **Uso de Informes programados** e **Uso de Informes personalizados**.

5.2. Datos sobre aplicaciones

Esta sección contiene los siguientes temas:

- Ver la distribución de aplicaciones
- Ver detalles de la aplicación
- Añadir gráficos de una sola distribución de aplicaciones
- Añadir un gráfico de aplicaciones iOS no administradas
- Añadir las 10 principales aplicaciones administradas instaladas
- Añadir las 5 aplicaciones internas mejor valoradas

Los datos sobre aplicaciones son una característica del Panel que le ayudará a ver y analizar la siguiente distribución de aplicaciones:

- Distribución de aplicaciones internas que requieren instalación
- Distribuciones de aplicaciones públicas que requieren instalación
- Aplicaciones iOS no administradas
- Las 10 principales aplicaciones administradas instaladas
- Las 5 aplicaciones internas mejor valoradas

Análisis de las 5 aplicaciones principales que requieren instalación: estas son aplicaciones internas o públicas que se han distribuido a un gran número de usuarios pero que tienen, en proporción, tasas bajas de instalación. El gráfico de Aplicaciones iOS no administradas proporciona información sobre las aplicaciones no administradas en los dispositivos. Podrá ver la lista de aplicaciones no administradas, en qué dispositivos están instaladas y, además, tomar medidas para convertir la aplicación en una aplicación administrada. Estas son las distribuciones de aplicaciones que requieren la atención del administrador o que este tome medidas al respecto para mejorar la distribución. Estas tablas representan los dispositivos que ya tienen la aplicación instalada. El gráfico circular ofrece un resumen completo de la distribución de aplicaciones tanto públicas como internas, lo cual no solo ayuda a analizar el número de dispositivos que requieren instalación de aplicaciones sino que, además, le permite seguir indagando para obtener más información específica sobre las aplicaciones haciendo clic en una sección específica del gráfico. Además, también puede añadir una sola tabla de distribución que represente la distribución de una versión específica para una sola aplicación.

> El tablero solo muestra información sobre los dispositivos que se verificaron en los últimos 15 días.

Ver la distribución de aplicaciones

En la página **Aplicaciones**, en **Panel**, puede ver los siguientes gráficos:

- La distribución de aplicaciones internas que requiere instalación
- La distribución de aplicaciones públicas que requiere instalación
- Aplicaciones iOS no administradas

De forma predeterminada se muestran los gráficos de 5 aplicaciones internas y de 5 aplicaciones iOS públicas y no administradas. Las tablas están ordenadas de izquierda a derecha, empezando por la aplicación con la tasa más alta de desinstalación.

Los gráficos circulares tienen dos colores para representar el estado de la instalación. El color azul representa el número de dispositivos en los que se ha instalado la aplicación. El color rojo representa el número de dispositivos que requieren instalación. Si pone el cursor sobre cada sección de color, aparece el recuento de dispositivos.

Puede eliminar un gráfico haciendo clic en la opción de borrado que hay en la esquina superior derecha del gráfico.

Ver detalles de la aplicación

El centro de gráfico circular también muestra el número de dispositivos que requieren instalación. Ejemplo: 750/1000 significa que 750 de los 1000 dispositivos requieren instalación.

Los gráficos circulares tienen 3 colores para representar la distribución de la aplicación.

- El color azul representa el número de dispositivos en los que se ha instalado la aplicación. Al hacer clic en la sección azul del gráfico, se navega hasta la página **Dispositivos**. En la página **Dispositivos**, la columna **Versión de la aplicación** indica la versión instalada de la aplicación y la fecha en la que se instaló la aplicación.

> También puede ver los dispositivos según las versiones de la aplicación instaladas si selecciona las opciones de la sección de **Versiones** en el panel izquierdo.

- El color rojo representa el número de dispositivos que requieren que se instale la aplicación. Al hacer clic en la sección roja del gráfico, se navega hasta la página **Dispositivos**. En la página **Dispositivos**, se pueden ver los dispositivos que requieren que se instale la aplicación.

En el centro del gráfico aparece el icono de la aplicación. Cuando el icono está marcado, lleva hasta la página detalles de la aplicación en **Aplicaciones > App Catalog**.

Esta página, haga clic en la pestaña **Dispositivos con la aplicación instalada** para ver la lista de dispositivos para la aplicación seleccionada.

Haga clic en la pestaña **Dispositivos sin la aplicación instalada** para ver la lista de dispositivos que no han instalado la aplicación seleccionada.

Añadir gráficos de una sola distribución de aplicaciones

Se pueden añadir gráficos circulares de una sola distribución para la versión específica de una aplicación en la página Aplicaciones. El color rojo representa la lista de dispositivos aptos que deberían tener instalada la aplicación. Estas tablas representan gráficamente los siguientes detalles de la distribución de las aplicaciones:

- Dispositivos instalados con una versión específica de la aplicación
- Dispositivos instalados con otras versiones de la aplicación
- Dispositivos que no tienen la aplicación instalada

Procedimiento

1. Haga clic en **+Añadir** en la página **Aplicaciones**. Aparecerá la ventana **Añadir gráfico de aplicaciones**.
2. En la lista desplegable **Tipo de gráfico**, seleccione **Una sola distribución de aplicaciones**.
3. Seleccione la casilla de la lista de aplicaciones para la que desea ver el gráfico de una sola distribución.

> Como alternativa, también puede buscar una aplicación específica escribiendo su nombre en el campo de búsqueda de aplicaciones.

4. Haga clic en **Añadir gráfico**. Los gráficos de una sola distribución de aplicaciones aparecen en la página Aplicaciones.

> Puede seleccionar un máximo de 9 aplicaciones de la lista.

El centro del gráfico muestra el número de dispositivos que están instalados con la versión específica de la aplicación.

Ejemplo: 5/10 indica que 5 de cada 10 dispositivos tienen instalada la versión específica de la aplicación.

Los gráficos circulares tienen 3 colores para representar la distribución de la aplicación.

- El color azul representa el número de dispositivos en los que se ha instalado la versión específica de la aplicación. Al hacer clic en la sección verde del gráfico, se navega hasta la página **Dispositivos**, donde aparece la lista de dispositivos instalados con la versión específica de la aplicación. También se pueden ver los dispositivos en función de otras versiones instaladas la aplicación seleccionando las opciones en la sección **Versión de la aplicación** que hay en el panel izquierdo.
- El color azul claro representa el número de dispositivos en los que se han instalado otras versiones de la aplicación. Al hacer clic en la sección verde del gráfico, se navega hasta la página **Dispositivos**, donde aparece la lista de dispositivos instalados con otras versiones de la aplicación. También se pueden ver los dispositivos en función de otras versiones instaladas la aplicación seleccionando las opciones de versión en la sección **Versión de la aplicación** que hay en el panel izquierdo.
- El color rojo representa el número de dispositivos en los que no se ha instalado la aplicación. Si pone el cursor sobre cada sección de color, aparece el recuento de dispositivos. Al hacer clic en la sección roja del gráfico, se navega hasta la página **Dispositivos**, donde se pueden ver los dispositivos que no han instalado con la aplicación. El panel de la izquierda también muestra la fecha a partir de la cual aplicación está disponible en el catálogo de aplicaciones.

En el centro del gráfico aparece el icono de la aplicación. Cuando el icono está marcado, lleva hasta la página detalles de la aplicación en **Aplicaciones > App Catalog**. Esta página, haga clic en la pestaña **Dispositivos con la aplicación instalada** para ver la lista de dispositivos para la aplicación seleccionada. Haga clic en la pestaña **Dispositivos sin la aplicación instalada** para ver la lista de dispositivos que no han instalado la aplicación seleccionada.

Puede eliminar un gráfico haciendo clic en la opción de borrado que hay en la esquina superior derecha del gráfico.

Añadir un gráfico de aplicaciones iOS no administradas

Puede identificar y visualizar la lista de aplicaciones no administradas mediante un gráfico de aplicaciones iOS exclusivas no administradas en la página de aplicaciones. Este gráfico aparece automáticamente cuando un administrador añade una aplicación de iOS no administrada al catálogo. El administrador puede eliminar o añadir este gráfico según lo necesite.

Procedimiento

1. Haga clic en **+Añadir** en la página **Aplicaciones**. Aparecerá la ventana **Añadir gráfico de aplicaciones**.
2. En la lista desplegable **Tipo de gráfico**, seleccione **Aplicaciones no administradas**.
3. Haga clic en **Añadir gráfico**. El gráfico de Aplicaciones iOS no administradas aparecerá en la página **Aplicaciones** .

El gráfico muestra el número de aplicaciones que no están administradas en el catálogo de aplicaciones. La parte inferior del gráfico muestra tres columnas con los siguientes detalles:

- **Dispositivos con aplicaciones iOS no administradas**: indica el número de aplicaciones iOS no administradas. Haga clic en el enlace para ver la lista de dispositivos con aplicaciones no administradas en la ventana Dispositivos con aplicaciones iOS no administradas.
- **Total de aplicaciones en el catálogo de aplicaciones**: muestra el número total de aplicaciones disponibles en el catálogo de aplicaciones.
- **Aplicaciones iOS no administradas (%)**: indica el porcentaje de aplicaciones iOS no administradas.

Si ya se ha instalado una aplicación desde la iTune App Store, puede convertir la aplicación y sus datos en una aplicación administrada. Para convertir dicha aplicación en una aplicación administrada:

1. Haga clic en el enlace del número de la **columna de dispositivos con aplicaciones iOS no administradas**. Aparecerá la ventana **Aplicaciones iOS no administradas**.
2. Seleccione una o más aplicaciones no administradas de la lista y haga clic en el enlace de número de aplicaciones iOS no administradas. Las aplicaciones seleccionadas se convertirán en aplicaciones administradas y su estatus se actualizará la próxima vez que ingrese el dispositivo.

> Puede exportar los datos sobre las aplicaciones no administradas en formato CSV haciendo clic en el vínculo **Exportar a CSV**.

Añadir las 10 principales aplicaciones administradas instaladas

Puede identificar y visualizar la lista de las 10 aplicaciones instaladas administradas más usadas mediante un gráfico de aplicaciones iOS instaladas administradas en la página de aplicaciones. El administrador puede eliminar o añadir este gráfico según lo necesite.

De forma predeterminada, el gráfico de las 10 aplicaciones instaladas administradas más usadas está disponible en la página **Aplicaciones**. Si el gráfico se elimina, el administrador puede añadirlo desde la página **Aplicaciones**.

Procedimiento

1. Haga clic en **+Añadir** en la página **Aplicaciones**. Aparecerá la ventana **Añadir gráfico de aplicaciones**.
2. En la lista desplegable **Tipo de gráfico**, seleccione **10 aplicaciones instaladas administradas más usadas**.
3. Haga clic en **Añadir gráfico**. El gráfico con las 10 aplicaciones instaladas administradas más usadas aparecerá en la página **Aplicaciones**.

Puede ver las 10 aplicaciones instaladas administradas más usadas según la categoría seleccionada en la lista desplegable **Mostrar**. Las categorías disponibles son:

- **Todas las aplicaciones** (seleccionada de forma predeterminada)
- **Aplicaciones internas**
- **Aplicaciones públicas**

Cada barra del gráfico representa cada aplicación específica y también se muestra el nombre de la aplicación. Pase el cursor sobre cada barra para ver la plataforma (Android, iOS o Windows) y el número de dispositivos instalados con la aplicación.

Al hacer clic en la barra de una aplicación en particular, navegará hasta la página **Dispositivos** que muestra los detalles de los dispositivos que tienen la aplicación instalada. El panel de la izquierda en la página de dispositivos indica el número de dispositivos con la aplicación instalada. Al hacer clic en el botón de la X en el panel de la izquierda, regresará a la página **Aplicaciones** del Panel.

Puede eliminar el gráfico haciendo clic en la opción de eliminar que hay en la esquina superior derecha del gráfico.

Añadir las 5 aplicaciones internas mejor valoradas

Puede identificar y visualizar la lista de las 5 aplicaciones internas mejor valoradas desde el gráfico de las 5 aplicaciones internas mejor valoradas en la página de aplicaciones. El administrador puede eliminar o añadir este gráfico según lo necesite.

De forma predeterminada, el gráfico de las 5 aplicaciones instaladas internas mejor valoradas está disponible en la página **Aplicaciones**. Si el gráfico se elimina, el administrador puede añadirlo desde la página **Aplicaciones**.

Procedimiento

1. Haga clic en **+Añadir** en la página **Aplicaciones**. Aparecerá la ventana **Añadir gráfico de aplicaciones**.
2. En la lista desplegable **Tipo de gráfico**, seleccione **5 aplicaciones internas mejor valoradas**.
3. Haga clic en **Añadir gráfico**. El gráfico con las 5 aplicaciones internas mejor valoradas aparecerá en la página **Aplicaciones**.

Este gráfico representa los datos mediante los logos de las aplicaciones, acompañados de estrellas que indican la calificación para esa aplicación. La calificación mediante estrellas está representada por imágenes de estrellas y números enteros (la calificación máxima es 5). También se muestra el número de usuarios que han valorado la aplicación.

> El número de valoraciones para una aplicación no está restringido a los dispositivos de ese administrador y espacio, sino que se basa en las valoraciones de todos los usuarios de la aplicación. La calificación es el promedio de todas las calificaciones de esa aplicación dadas por los diferentes usuarios que vieron esa aplicación desde Apps@Work en sus dispositivos inscritos.

Al hacer clic en una aplicación concreta, nos redirige a la página de **Detalles de la aplicación** que muestra los detalles específicos de la aplicación.

Puede eliminar el gráfico haciendo clic en la opción de eliminar que hay en la esquina superior derecha del gráfico.

5.3. Uso de Informes programados

Licencia: Silver

La función Informes programados le permite programar y generar informes, con diferentes métricas y plantillas previamente empaquetadas, listos para usarse. Debe tener la función de Administrador del sistema o Solo lectura del sistema para acceder a esta función. Actualmente puede crear un máximo de 40 informes.

> El informe de infracciones de políticas puede tener varios registros para el mismo dispositivo si a este se le han creado varias instancias de Tunnel. Esto es aplicable tanto a los informes estándar como a los informes personalizados.

Generar un informe

Puede programar y generar un informe.

Procedimiento

1. Vaya a **Panel** > **Informes**.
2. Haga clic en **Crear un informe** para visualizar la página Elija una plantilla para informes.
3. Elija una plantilla para su informe de la opciones que ha configurado.
   - **Dispositivos bloqueados**: informe sobre los dispositivos cuyo acceso está bloqueado actualmente por Sentry.
   - **Dispositivos**: informe sobre los dispositivos de todas las particiones del sistema.
   - **Incumplimiento de políticas**: informe sobre las infracciones de políticas del sistema.
   - **Usuarios**: informe sobre los usuarios del sistema
   - **Estado de caducidad de la contraseña del usuario**: informe sobre el estado de caducidad de la contraseña de los usuario del sistema.
   - **Aplicaciones más instaladas**: informe sobre todas las aplicaciones del sistema, ordenadas por número de instalaciones.
   - **Aplicaciones no administradas**: informe sobre las aplicaciones no administradas del sistema.
   - **Todas las aplicaciones**: informe sobre todas las aplicaciones de los dispositivos administrados por usted.
   - **Rastros de auditoría**: informe de todas las actividades realizadas en las distintas entidades de Ivanti Neurons for MDM.
4. Haga clic en **Siguiente**.
   Se muestra la página **Detalles del informe**.
   - Introduzca un **Nombre del informe**.
   - (Opcional) Introduzca una **Descripción** para el informe.

Seleccione **Rango de eventos** en las opciones siguientes:
Para informes existentes:

- **Todos los eventos**
- **Día anterior**
- **Semana anterior**
- **Mes anterior**
- **Rango anterior**: muestra el informe que se creó con el control deslizante de rangos desde la versión anterior del portal administrativo de Ivanti Neurons for MDM. Si el administrador selecciona y guarda alguna de las opciones anteriores para un

informe, no se mostrará la opción Rango anterior. El valor de rango se puede ver en la página Resumen de informes.

Para nuevos informes:

- **Todos los eventos**
- **Día anterior**
- **Semana anterior**
- **Mes anterior**

Haga clic en **Siguiente**. Se muestra la página Datos del informe.

6. Haga clic en **Personalizar columnas** para agregar, eliminar o cambiar el orden de las columnas en la sección **Columnas de informes**. También puede hacer clic sobre el nombre de la columna para eliminar la columna agregada.
7. (Opcional) utilice la casilla **Seleccionar todas las columnas** para seleccionar todas las columnas visualizadas de la lista.
8. Haga clic en **Restaurar valores predeterminados** para volver a las columnas generadas anteriormente. Para volver a las columnas sin ninguna personalización, puede elegir una de las plantillas de la página **Elija una platilla para informes**.
9. Cree filtro basados en reglas específicas de la sección **Filtro avanzado**.

> Todas las opciones de filtros no está disponible para todos los informes. Para obtener más información sobre la lista de filtros disponibles, consulte el tema **Filtros** bajo este proceso.

> Los siguientes atributos de nuevo hardware están disponibles para dispositivos de Windows cuando se crean informes: cifrado de BitLocker, Edición de SO, Versión del sistema, Fabricante de placa base, Producto de placa base, Estado de placa base, Fabricante de BIOS, Versión de BIOS, Particiones de disco duro, Tupo de unidad óptica, Nombre de CPU y Estado de CPU.

10. (Opcional) haga clic en el icono **+** para agregar otra regla o en el icono **Agregar grupo** para agregar otro grupo de reglas.
11. Haga clic en **Siguiente**. Se muestra la página Programa del informe.
12. Seleccione *uno* de los siguientes formatos para descargar el informe:
    - CSV
    - PDF
    - **CSV y PDF**
      Para archivos de informes en PDF, se permiten hasta 10 columnas. En la sección Gráficas de informes, se mostraránincluirán los dos tipos de gráficas que se incluirán en los informes en PDF.
      El informe de **Todas las aplicaciones** es compatible solo con el formato CSV.

Haga clic en **Programación automática** para configurar un informe que se ejecutará automáticamente mediante la configuración de la periodicidad. También puede hacer clic en **Manual** para ejecutar el informe una vez y que se envíe en un correo electrónico.

- Seleccione *una* de las opciones de **Informes recurrentes**:
  - **Diario**
  - **Semanal**
  - **Mensualmente**
  - **Programa anterior**: para informes existentes
- Seleccione la **Fecha de inicio** y la **Fecha final** (opcional).

14. Haga clic en **Siguiente**. Se muestra la página Distribución del informe. Seleccione los destinatarios del informe.

15. (Opcional) agregue ID de correos electrónicos externos haciendo clic en el enlace **Agregar correo electrónico externo**.
16. Haga clic en **Hecho**. Aparece el **Resumende distribución de informes**.
17. (Opcional) haga clic en **Editar** para modificar su informe.
18. Haga clic en **Guardar**.
19. Haga clic en el icono de descarga para seleccionar el formato del informe. El destinatario del informe recibe un correo electrónico que contiene un botón de **Descargar informe** para descargar el informe.

Filtros

Opciones de reglas	Descripción
Bloqueo de activación habilitado	Reglas basada en el bloqueo de activación activada como **Sí** o **No**. Ejemplo de regla: 'El bloqueo de activación habilitado es igual a Sí'.
Estado de la aplicación Tunnel	Regla para el estado de la aplicación Tunnel como **BLOQUEAR** o **PERMITIR**. Ejemplo de regla: 'El estado de la aplicación Tunnel es igual a Bloquear'.
Nivel de batería	Valor del nivel de batería del dispositivo. Ejemplo de regla: 'El nivel de batería es igual a 1080'. El valor introducido para el nivel de la batería debe ser en segundos.
Último ingreso del cliente	Regla basada en el último ingreso del cliente dentro del rango de fecha. Ejemplo de regla: '«Último ingreso del cliente» está en el rango 02/04/2019 6:00:00 hasta el 05/04/2019 17:00:00'.
Estado del cumplimiento	Regla basada en el estado del cumplimiento como **Sí** o **No**. Ejemplo de regla: 'El estado del cumplimiento es igual a Sí'.
Nombre del país actual	Introduzca el nombre del país actual. Ejemplo de regla: 'El estado del cumplimiento es igual a Francia'.
MMC actual	Regla basada en el código móvil del país. Ejemplo de regla: 'El MCC actual es igual a 410'.
MNC actual	Regla basada en el código de red móvil actual. Ejemplo de regla: 'El MNC actual es igual a 06'.
Inscripción de dispositivos activada	Regla basada en la inscripción de dispositivos activada como **Sí** o **No**. Ejemplo de regla: '«Inscripción de dispositivos activada» es igual a Sí'.
Estado nativo de antiphishing	Seleccione cualquiera de las siguientes opciones de Estado nativo de antiphishing: • es igual a • no es igual a Los valores posibles son: • No activado • N/A • Activado • Desconocido
Estado de la VPN de antiphishing	Seleccione cualquiera de las siguientes opciones de Estado de la VPN de antiphishing: • es igual a • no es igual a Los valores posibles son: • No activado • N/A • Activado

Opciones de reglas	Descripción
	• Desconocido
Inscrito en la Inscripción de dispositivos	Regla basada en «inscrito en la Inscripción de dispositivos» como **Sí** o **No**. Ejemplo de regla: «Inscrito en la inscripción de dispositivos es igual a Sí»
Protección de datos **Itinerancia de datos activada**	Indica si la protección de datos está habilitada en el dispositivo. Los valores posibles son **Sí** y **No**. Ejemplo de regla: 'La protección de datos es igual a Sí'. Regla basada en la itinerancia de datos activada como **Sí** o **No**. Ejemplo de regla: 'La itinerancia de datos activada es igual a Sí'.
Estado del bloqueo del dispositivo	Regla basada en el estado del bloqueo del dispositivo. Ejemplo de regla: 'El estado de bloqueo del dispositivo es igual a Bloqueo'.
Id. de dispositivo **MCC de origen**	Regla para una Id. específica del dispositivo dentro de un rango de varias Id. de dispositivos. Ejemplo de regla: 'La Id. del dispositivo es superior a 45'. x Regla basada en el código móvil del país de origen. Ejemplo de regla: 'El MCC de origen es igual a 310'.
MNC de origen	Regla basada en el código de red móvil de origen. Ejemplo de regla: 'El MNC de origen es igual a 510'.
IMEI	Regla para un valor de IMEI específico. Ejemplo de regla: 'El IMEI comienza por 9900'.
Estado de la invitación	Seleccione cualquiera de las siguientes opciones de Estado de la invitación: • Ninguno • Pendiente • Caducado • **Completado** Ejemplo de regla: 'El estado de la invitación es igual a Pendiente'.
Servicio de Localizador habilitado	Regla basada en el servicio de localización activado como **Sí** o **No**. Ejemplo de regla: 'El servicio de localización activado es igual a Sí'.
Estado de activación del MTD	Seleccione cualquiera de las siguientes opciones de Estado de la activación del MTD: • es igual a • no es igual a Los valores posibles son: • N/A • Error • Pendiente • Protegido

Opciones de reglas	Descripción
Estado de cuarentena	Regla basada en el servicio de localización activado como **Sí** o **No**. Ejemplo de regla: 'El estado de cuarentena es igual a Sí'.
Registrado en	Regla para seleccionar el rango de fecha y hora desde que se registró el dispositivo. Ejemplo de regla: '«Registrado el» está en el rango 03/10/2017 09:00:00 hasta el 20/10/2017 17:00:00'.
Itinerancia	Regla basada en la itinerancia como**Sí** o **No**. Ejemplo de regla: 'La itinerancia es igual a Sí'.
Estado	Seleccione cualquiera de las siguientes opciones de Estado de la invitación: • Activo • Retirada pendiente • Retirada enviado • Retirado • Retirada cancelada • Borrado pendiente • Borrado enviado • Borrado • Borrado cancelado Ejemplo de regla: 'El estado es igual a «Retirada pendiente».
Itinerancia de voz activada	Regla basada en la itinerancia de voz activada como **Sí** o **No**. Ejemplo de regla: 'La itinerancia de voz activada es igual a Sí'.
Dirección MAC de Wi-Fi	Introduzca un valor de dirección Mac específico. Ejemplo de regla: 'La dirección Mac Wi-Fi no es igual a 00-14-22-01-23-45'.
Copia de seguridad de iCloud habilitada	Regla basada en la copia de seguridad de iCloud activada como **Sí** o **No**. Ejemplo de regla: 'La copia de seguridad de iCloud activada es igual a Sí'.
Estado de activación de la cuenta de iTunes Store.	Regla basada en el estado de activación de la cuenta de iTunes Store como **Sí** o **No**. Ejemplo de regla: 'El estado de activación de la cuenta de iTunes Store no es igual a No'.
Tipo de plataforma	Aplicable para el informe de Todas las aplicaciones.
Origen	Aplicable para el informe de Todas las aplicaciones.
Atributos personalizados	Aplicable para el informe de Todas las aplicaciones.
Administrado	Aplicable para el informe de Todas las aplicaciones y de Aplicaciones más usadas.
Identificador de la aplicación	Informe de todas las aplicaciones por defecto.
Meid	Aplicable para el informe de Aplicaciones sin administrar.

Llevar a cabo acciones en un informes desde la página Informes programados

Puede llevar a cabo varias acciones desde la página Informes programados.

Procedimiento

1. Vaya a **Panel** > **Informes**.
2. En la página **Mis informes programados**, haga clic en el menú desplegable de **Acciones**, y seleccione una de las opciones siguientes:

Opciones de acciones	Acción llevada a cabo
Ver	Le permite ver el informe.
Editar	Le permite editar el informe. El informe también le permite visualizar el rango que se seleccionó en la última versión como Rango anterior.
Ejecutar ahora	Ejecuta el informe.
Descargar CSV	Descarga el informe en formato CSV.
Descargar PDF	Descarga el informe en formato PDF.
Eliminar	Elimina el informe.

Ver información de los informes

Puede ver la información del informe y llevar a cabo algunas acciones en el informe creado.

Procedimiento

1. Vaya a **Panel** > **Informes**.
2. En la página **Mis informes programados**, haga clic en el nombre del informe para ver los detalles. Se abre la página del informe.
3. Puede ver el Resumen del informe y el Historial de informes en esta página.

Temas relacionados:

- Para asignar una función personalizada a un usuario, consulte **Asignar funciones**.
- Consulte **Funciones de usuario** para ver una lista de funciones predeterminadas.
- **Administración de funciones**
- **Uso de Informes personalizados**

5.4. Uso de Informes personalizados

Licencia: Gold

La función Informes personalizados le permite personalizar y generar informes con diferentes métricas y plantillas listas para usarse. Debe tener la función de Administrador del sistema o Solo lectura del sistema para acceder a esta función. Actualmente puede crear un máximo de 40 informes.

Esta sección contiene los siguientes temas:

Generación de un informe

Llevar a cabo acciones en un informe

Ver información de los informes

Generación de un informe

Puede programar y generar un informe desde el portal administrativo de Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Panel** > **Informes**.
2. Haga clic en **Crear un informe** para visualizar la página Elija una plantilla para informes.
3. Elija una plantilla para su informe de la opciones que ha configurado.
    - **Dispositivos bloqueados**: informe sobre los dispositivos cuyo acceso está bloqueado actualmente por Sentry.
    - **Dispositivos**: informe sobre los dispositivos de todas las particiones del sistema.
    - **Incumplimiento de políticas**: informe sobre las infracciones de políticas del sistema.
    - **Usuarios**: informe sobre los usuarios del sistema
    - **Estado de caducidad de la contraseña del usuario**: informe sobre el estado de caducidad de la contraseña de los usuario del sistema.
    - **Aplicaciones más instaladas**: informe sobre todas las aplicaciones del sistema, ordenadas por número de instalaciones.
    - **Aplicaciones no administradas**: informe sobre las aplicaciones no administradas del sistema.
    - **Todas las aplicaciones**: informe sobre todas las aplicaciones de los dispositivos administrados por usted.
    - **Rastros de auditoría**: informe de todas las actividades realizadas en las distintas entidades de Ivanti Neurons for MDM.
4. Haga clic en **Siguiente**. Se muestra la página Detalles del informe.
5. Introduzca un **Nombre del informe**.
6. (Opcional) Introduzca una **Descripción** para el informe.
7. Seleccione **Rango de eventos** en las opciones siguientes:
   Para informes existentes:
    - **Todos los eventos**
    - **Día anterior**
    - **Semana anterior**
    - **Mes anterior**

- **Rango anterior**: muestra el informe que se creó con el control deslizante de rangos desde la versión anterior del portal administrativo de Ivanti Neurons for MDM. Si el administrador selecciona y guarda alguna de las opciones anteriores para un informe, no se mostrará la opción Rango anterior. El valor de rango se puede ver en la página Resumen de informes.

Para nuevos informes:

- **Todos los eventos**
- **Día anterior**
- **Semana anterior**
- **Mes anterior**

Haga clic en **Siguiente**. Se muestra la página Datos del informe.

9. Haga clic en **Personalizar** para generar un informe personalizado:

> En la página **Panel > Informes**, la columna Nombre de plantilla mostrará "personalizado" entre paréntesis para indicar que se trata de un informe personalizado.

10. Haga clic en **Personalizar columnas** para agregar, eliminar o cambiar el orden de las columnas en la sección **Columnas de informes**. También puede hacer clic sobre el nombre de la columna para eliminar la columna agregada.
11. (Opcional) utilice la casilla **Seleccionar todas las columnas** para seleccionar todas las columnas visualizadas de la lista.
12. Haga clic en **Restaurar valores predeterminados** para volver a las columnas generadas anteriormente. Para volver a las columnas sin ninguna personalización, puede elegir una de las plantillas de la página **Elija una platilla para informes**. Las columnas predeterminadas se indican con un icono de candado.
13. Cree filtro basados en reglas específicas de la sección **Filtro avanzado**.

> Todas las opciones de filtros no está disponible para todos los informes. Para obtener más información sobre la lista de filtros disponibles, consulte el tema **Filtros** bajo este proceso.

> Los siguientes atributos de nuevo hardware están disponibles para dispositivos de Windows cuando se crean informes: cifrado de BitLocker, Edición de SO, Versión del sistema, Fabricante de placa base, Producto de placa base, Estado de placa base, Fabricante de BIOS, Versión de BIOS, Particiones de disco duro, Tupo de unidad óptica, Nombre de CPU y Estado de CPU.

14. (Opcional) haga clic en el icono **+** para agregar otra regla o en el icono **Agregar grupo** para agregar otro grupo de reglas.
15. Haga clic en **Siguiente**. Se muestra la página Programa del informe.
16. Seleccione *uno* de los siguientes formatos para descargar el informe:
    - **CSV**
    - **PDF**
    - **CSV y PDF**
      Para archivos de informes en PDF, se permiten hasta 10 columnas. En la sección Gráficos de informes, aparecerán los dos tipos de gráficos que se incluirán en los informes en PDF.
      El informe de **Todas las aplicaciones** es compatible solo con el formato CSV.

Haga clic en **Programación automática** para configurar un informe que se ejecutará automáticamente mediante la configuración de la periodicidad. También puede hacer clic en **Manual** para ejecutar el informe una vez y que se envíe en un correo electrónico.

- Seleccione *una* de las opciones de **Informes recurrentes**:
  - **Diario**
  - **Semanal**
  - **Mensualmente**
  - **Programa anterior**: para informes existentes
- Seleccione la **Fecha de inicio** y la **Fecha final** (opcional).

> La opción Ejecutar ahora generará un informe puntual. Puede usar la misma plantilla para generar informes programados. En la página **Panel > Informes**, en las columnas Frecuencia y Próximo programado aparecerá el estado no programado de estos informes.

18. Haga clic en **Siguiente**. Se muestra la página Distribución del informe. Seleccione los destinatarios del informe.
19. (Opcional) agregue ID de correos electrónicos externos haciendo clic en el enlace **Agregar correo electrónico externo**.
20. Haga clic en **Hecho**. Aparece el **Resumende distribución de informes**.
21. (Opcional) haga clic en **Editar** para modificar su informe.
22. Haga clic en **Guardar**.
23. Haga clic en el icono de descarga para seleccionar el formato del informe. El destinatario del informe recibe un correo electrónico que contiene un botón de **Descargar informe** para descargar el informe.

Filtros

Opciones de reglas	Descripción
Bloqueo de activación habilitado	Reglas basada en el bloqueo de activación activada como **Sí** o **No**. Ejemplo de regla: 'El bloqueo de activación habilitado es igual a Sí'.
Estado de la aplicación Tunnel	Regla para el estado de la aplicación Tunnel como **BLOQUEAR** o **PERMITIR**. Ejemplo de regla: 'El estado de la aplicación Tunnel es igual a Bloquear'.
Nivel de batería	Valor del nivel de batería del dispositivo. Ejemplo de regla: 'El nivel de batería es igual a 1080'. El valor introducido para el nivel de la batería debe ser en segundos.
Último ingreso del cliente	Regla basada en el último ingreso del cliente dentro del rango de fecha. Ejemplo de regla: '«Último ingreso del cliente» está en el rango 02/04/2019 6:00:00 hasta el 05/04/2019 17:00:00'.
Estado del cumplimiento	Regla basada en el estado del cumplimiento como **Sí** o **No**. Ejemplo de regla: 'El estado del cumplimiento es igual a Sí'.
Nombre del país actual	Introduzca el nombre del país actual. Ejemplo de regla: 'El estado del cumplimiento es igual a Francia'.
MMC actual	Regla basada en el código móvil del país. Ejemplo de regla: 'El MCC actual es igual a 410'.
MNC actual	Regla basada en el código de red móvil actual. Ejemplo de regla: 'El MNC actual es igual a 06'.
Inscripción de dispositivos activada	Regla basada en la inscripción de dispositivos activada como **Sí** o **No**. Ejemplo de regla: '«Inscripción de dispositivos activada» es igual a Sí'.
Estado nativo de antiphishing	Seleccione cualquiera de las siguientes opciones de Estado nativo de antiphishing: • es igual a • no es igual a Los valores posibles son: • No activado • N/A • Activado • Desconocido
Estado de la VPN de antiphishing	Seleccione cualquiera de las siguientes opciones de Estado de la VPN de antiphishing: • es igual a • no es igual a Los valores posibles son: • No activado • N/A • Activado

Opciones de reglas	Descripción
	• Desconocido
Inscrito en la Inscripción de dispositivos	Regla basada en «inscrito en la Inscripción de dispositivos» como **Sí** o **No**. Ejemplo de regla: «Inscrito en la inscripción de dispositivos es igual a Sí»
Protección de datos **Itinerancia de datos activada**	Indica si la protección de datos está habilitada en el dispositivo. Los valores posibles son **Sí** y **No**. Ejemplo de regla: 'La protección de datos es igual a Sí'. Regla basada en la itinerancia de datos activada como **Sí** o **No**. Ejemplo de regla: 'La itinerancia de datos activada es igual a Sí'.
Estado del bloqueo del dispositivo	Regla basada en el estado del bloqueo del dispositivo. Ejemplo de regla: 'El estado de bloqueo del dispositivo es igual a Bloqueo'.
Id. de dispositivo **MCC de origen**	Regla para una Id. específica del dispositivo dentro de un rango de varias Id. de dispositivos. Ejemplo de regla: 'La Id. del dispositivo es superior a 45'. x Regla basada en el código móvil del país de origen. Ejemplo de regla: 'El MCC de origen es igual a 310'.
MNC de origen	Regla basada en el código de red móvil de origen. Ejemplo de regla: 'El MNC de origen es igual a 510'.
IMEI	Regla para un valor de IMEI específico. Ejemplo de regla: 'El IMEI comienza por 9900'.
Estado de la invitación	Seleccione cualquiera de las siguientes opciones de Estado de la invitación: • Ninguno • Pendiente • Caducado • **Completado** Ejemplo de regla: 'El estado de la invitación es igual a Pendiente'.
Servicio de Localizador habilitado	Regla basada en el servicio de localización activado como **Sí** o **No**. Ejemplo de regla: 'El servicio de localización activado es igual a Sí'.
Estado de activación del MTD	Seleccione cualquiera de las siguientes opciones de Estado de la activación del MTD: • es igual a • no es igual a Los valores posibles son: • N/A • Error • Pendiente • Protegido

Opciones de reglas	Descripción
Estado de cuarentena	Regla basada en el servicio de localización activado como **Sí** o **No**. Ejemplo de regla: 'El estado de cuarentena es igual a Sí'.
Registrado en	Regla para seleccionar el rango de fecha y hora desde que se registró el dispositivo. Ejemplo de regla: '«Registrado el» está en el rango 03/10/2017 09:00:00 hasta el 20/10/2017 17:00:00'.
Itinerancia	Regla basada en la itinerancia como**Sí** o **No**. Ejemplo de regla: 'La itinerancia es igual a Sí'.
Estado	Seleccione cualquiera de las siguientes opciones de Estado de la invitación: • Activo • Retirada pendiente • Retirada enviado • Retirado • Retirada cancelada • Borrado pendiente • Borrado enviado • Borrado • Borrado cancelado Ejemplo de regla: 'El estado es igual a «Retirada pendiente».
Itinerancia de voz activada	Regla basada en la itinerancia de voz activada como **Sí** o **No**. Ejemplo de regla: 'La itinerancia de voz activada es igual a Sí'.
Dirección MAC de Wi-Fi	Introduzca un valor de dirección Mac específico. Ejemplo de regla: 'La dirección Mac Wi-Fi no es igual a 00-14-22-01-23-45'.
Copia de seguridad de iCloud habilitada	Regla basada en la copia de seguridad de iCloud activada como **Sí** o **No**. Ejemplo de regla: 'La copia de seguridad de iCloud activada es igual a Sí'.
Estado de activación de la cuenta de iTunes Store.	Regla basada en el estado de activación de la cuenta de iTunes Store como **Sí** o **No**. Ejemplo de regla: 'El estado de activación de la cuenta de iTunes Store no es igual a No'.
Tipo de plataforma	Aplicable para el informe de Todas las aplicaciones.
Origen	Aplicable para el informe de Todas las aplicaciones.
Atributos personalizados	Aplicable para el informe de Todas las aplicaciones.
Administrado	Aplicable para el informe de Todas las aplicaciones y de Aplicaciones más usadas.
Identificador de la aplicación	Informe de todas las aplicaciones por defecto.
Meid	Aplicable para el informe de Aplicaciones sin administrar.

Llevar a cabo acciones en un informe

Puede llevar a cabo varias acciones desde la página Informes programados.

Procedimiento

1. Vaya a **Panel** > **Informes**.
2. En la página **Mis informes programados**, haga clic en el menú desplegable de **Acciones**, y seleccione una de las opciones siguientes:

Opciones de acciones	Acción llevada a cabo
Ver	Le permite ver el informe.
Editar	Le permite editar el informe.
Ejecutar ahora	Ejecuta el informe.
Descargar CSV	Descarga el informe en formato CSV.
Descargar PDF	Descarga el informe en formato PDF.
Eliminar	Elimina el informe.

Ver información de los informes

Puede ver la información del informe y llevar a cabo algunas acciones en el informe creado.

Procedimiento

1. Vaya a **Panel** > **Informes**.
2. En la página **Mis informes programados**, haga clic en el nombre del informe para ver los detalles. Se abre la página del informe.
3. Seleccione una de las siguientes opciones

Opciones de acciones	Acción llevada a cabo
Alternar	Le permite habilitar o deshabilitar el informe.
Ejecutar ahora	Ejecuta el informe.
Ver	Le permite ver los detalles del informe. Utilice el menú desplegable de Acciones para llevar a cabo cualquiera de las tareas siguientes: • **Desactivar** • **Descargar el CSV/PDF más reciente** (basado en el tipo de informe seleccionado, ya sea CSV, PDF o CSV & PDF, muestra la opción de Descargar) • **Historial** • **Eliminar**
Eliminar	Elimina el informe.

Temas relacionados:

- Para asignar una función personalizada a un usuario, consulte **Asignar funciones**.
- Consulte **Funciones de usuario** para ver una lista de funciones predeterminadas.
- **Administración de funciones**
- **Uso de Informes programados**

6. Usuarios

Antes de invitar a alguien a registrar sus dispositivos móviles, es necesario crear una entrada de usuario para esa persona. También será necesario que cree un usuario para cualquier persona que vaya a usar Ivanti Neurons for MDM para ayudar a administrar dispositivos o publicar contenido (administradores).

Esta sección contiene los siguientes temas:

- Grupos de usuarios
- Ajustes del usuario
- Marca del usuario
- Inscripción de usuarios en el Apple Business Manager
- Inscripción de Usuario generada por cuenta
- Licencias de usuario
- Administrar usuarios

6.1. Añadir usuarios

Esta sección contiene los siguientes temas:

- Añadir usuarios
- Añadir múltiples usuarios
- Añadir múltiples usuarios cargando un archivo
- Añadir un administrador
- Usuario «nadie»
- Visualizar la información del PIN para el registro del dispositivo

Puede añadir un solo usuario o varios usuarios a la vez. Una vez que haya añadido varios usuarios, le recomendamos que filtre la visualización para mostrarle solamente los que le interesan.

A continuación mencionamos otras cosas que puede hacer con los usuarios en esta página:

- Asignarlos a un grupo de usuarios o eliminarlos de este
- enviar un mensaje
- invitarlo a registrarse
- asignar funciones
- cambiar una contraseña
- eliminar
- generar un pin

Todos los perfiles del propietario del dispositivo están asignados a una cuenta de dispositivo. Las cuentas de dispositivos no tienen ninguna restricción en el número de dispositivos asignados. Los perfiles de trabajo (propiedad del empleado) son cuentas del usuario asignadas.

Añadir a un usuario

Procedimiento

1. Vaya a **Usuarios.**
2. Haga clic en **+ Añadir** (arriba a la derecha).
3. Seleccione **Un solo usuario**.
4. Complete el formulario con la información del usuario:
    - Dirección de correo electrónico (requerido)
    - Nombre
    - Apellidos

> El campo del nombre de usuario muestra la dirección de correo electrónico que ha introducido. En la mayoría de los casos, no debe editar este campo predeterminado. Para obtener más información, consulte Cuándo editar un nombre de usuario

    - Nombre en pantalla

> Si desea cambiar el nombre en pantalla de este usuario, edite el texto predeterminado en el campo **Nombre en pantalla**.

5. Si desea asignar una contraseña, ingrésela en los campos **Contraseña** y **Confirmar contraseña**.
    - Si asigna una contraseña, debe comunicársela al usuario para que pueda registrar sus dispositivos.
    - Si no asigna ninguna contraseña, el usuario tendrá que crear una contraseña cuando registre sus dispositivos.
6. Seleccione **Configuración regional** en la lista desplegable.
7. Introduzca **ID de Apple administrada**. Puede incluir «appleid» como subdominio para la ID de Apple administrada con el fin de evitar cualquier conflicto con las ID de Apple existentes. Por ejemplo, usuario@appleid.sudominio.com. El subdominio tiene que ser un subdominio verificado válido de Apple Business Manager.

> No puede actualizarse la cuenta con una Id de Apple administrada diferente si hay un dispositivo inscrito como usuario activo con la Id de Apple administrada de la cuenta actual.

(Opcional) Asigne uno o más grupos de usuarios. La ID de Apple administrada no se puede actualizar cuando hay un dispositivo con el estado «Activo» y «Retirada pendiente».

10. Si desea configurar otras características antes de invitar a este usuario, desactive la opción **Enviar esta invitación ahora**. De lo contrario, se enviará el correo electrónico con la invitación cuando haga clic en **Hecho**.
11. Haga clic en **Hecho** para añadir al usuario.

En el caso de los dispositivos Android, las cuentas de dispositivos están diseñadas para dispositivos administrados de un solo uso, en los que una sola cuenta de servicio local puede utilizarse para inscribir un gran número de dispositivos. Al crear un nuevo usuario, debe estar activada la Cuenta de dispositivo empresarial Android disponible en **Administrador > Google > Android Enterprise**. Las cuentas de dispositivo están activadas de forma predeterminada (en lugar de las cuentas de usuario) para las inscripciones de cuentas de Google Play gestionadas por el propietario del dispositivo.

Marque la casilla **Cuenta de dispositivo con Android Enterprise** para permitir que se asigne automáticamente una Cuenta de dispositivo Google a las inscripciones de dispositivos administrados en el trabajo con Android Enterprise vinculadas a esta cuenta.

Al editar un usuario local o LDAP para dispositivos Android, a los dispositivos de la cuenta de Google Play administrada por el propietario del dispositivo de Android Enterprise asociados al usuario se les asignarán cuentas de dispositivo en el siguiente registro de dispositivos, siempre que se cumplan las siguientes condiciones:

- Que esté activada esta función seleccionando la casilla **Cuenta de dispositivo con la versión corporativa de Android**.
- Que la aplicación Go del dispositivo Android tenga la versión 47 o posterior.

Añadir múltiples usuarios

Procedimiento :

1. Vaya a **Usuarios.**
2. Haga clic en **+ Añadir** (arriba a la derecha).
3. Seleccione **Usuarios múltiples**.
4. Puede introducir direcciones de correo electrónico **Manualmente** de manera predeterminada. Escriba o peque las direcciones de correo electrónico de los usuarios separadas por comas.
5. Por ejemplo: jperez@miempresa.com, lruiz@miempresa.com, nvillalba@miempresa.com
   Si desea configurar otras características antes de invitar a este usuario, desactive la opción **Enviar esta invitación ahora**.

6. De lo contrario, se enviará el correo electrónico con la invitación cuando haga clic en **Hecho**.
   Haga clic en **Hecho** para añadir a los usuarios.

Añadir múltiples usuarios cargando un archivo

Procedimiento:

1. Vaya a **Usuarios.**
2. Haga clic en **+ Añadir** (arriba a la derecha).
3. Seleccione **Usuarios múltiples**.
4. Seleccione **Cargar CSV**.
5. Haga clic en **Descargar plantilla CSV**.
6. Edite la plantilla con la siguiente información para cada usuario:
   - Id. de usuario (obligatoria)
   - dirección de correo electrónico (obligatoria)
   - contraseña
   - nombre
   - apellidos
   - Nombre en pantalla
   - grupos de usuarios
   - atributos personalizados
7. Esta es la misma información que usted introduce al **añadir a un solo usuario**. No supere las 10 000 entradas en el archivo.
   Guarde el archivo.
8. Arrástrelo al área de cargas o seleccione **Cargar CSV** para seleccionar el archivo.
9. Una vez que aparezca la información cargada sobre el usuario, haga las modificaciones pertinentes.
10. Haga clic en **Siguiente** (abajo a la derecha).
11. Si no desea enviar invitaciones directamente, seleccione **No enviar invitaciones.**
12. Haga clic en **Hecho**.

Añadir un administrador

Procedimiento :

1. Haga clic en **Añadir** (arriba a la derecha).
2. Seleccione **Un solo usuario**.
3. Complete el formulario con la información del usuario:
   - Dirección de correo electrónico
   - Nombre
   - Apellidos
4. El campo **nombre de usuario** muestra la dirección de correo electrónico que ha introducido.
   Si desea cambiar el nombre para mostrar de este usuario, edite el texto predeterminado en el campo **Nombre para mostrar**.
5. Asigne una contraseña en el campo **Contraseña**.

6. Introduzca de nuevo la contraseña en el campo **Confirmar contraseña**.
7. Haga clic en **Hecho** para añadir al usuario.
8. Comunique la contraseña a la persona que le ayudará a administrar los dispositivos.

Usuario «nadie»

El usuario «nadie» es un usuario predeterminado que no puede eliminarse. El servicio aplica este usuario a los dispositivos que no tienen ningún usuario asociado, como por ejemplo los dispositivos retirados.

Visualizar la información del PIN para el registro del dispositivo

Mientras se añaden nuevos usuarios, a los administradores les aparecerá la información del PIN generado para el registro si el Tipo de autenticación del registro de dispositivos está establecida en Solo PIN. Esta información puede resultar útil para asistir a los usuarios con inscripciones de dispositivos.

- Para usuarios individuales, el PIN aparece a través de la acción **Usuarios > Invitar usuario a registrarse** y también en la sección Información del PIN de la página Detalles del usuario.
- Para múltiples usuarios, los PIN aparecen en forma de columna en la página Lista de usuarios además de las columnas «Estado del PIN» (válido o caducado), «PIN emitido», y «PIN caduca».

Si no puede realizar las tareas en la página **Usuarios**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración del sistema
- Administración de usuarios

6.2. Grupos de usuarios

Esta sección contiene los siguientes temas:

- Crear un grupo de usuarios administrado dinámicamente
- Crear un grupo de usuarios administrado manualmente
- Creación de un grupo de usuarios a partir de uno de los grupos de usuarios duplicados
- Crear un grupo de usuarios mediante la carga de archivos CSV

Cree un grupo de usuarios para poder asignar aplicaciones y roles a múltiples usuarios. Por ejemplo, puede necesitar crear un grupo de administradores si desea que todos los administradores de un departamento sean administradores de las aplicaciones y el contenido.

Puede crear un grupo de usuarios para administrarlo con uno de los siguientes métodos:

- **Administrado dinámicamente (lo más común):** se añaden/eliminan dinámicamente usuarios locales y de LDAP en un grupo según ciertas reglas y/o atributos.
- **Administrado manualmente (finalidad limitada):** añada/elimine manualmente usuarios en un grupo. Los grupos administrados manualmente solo se recomiendan para pruebas que requieran menos permisos.

Puede introducir texto en el campo **Buscar** para ver una lista de todos los grupos de usuarios cuyos nombres empiezan por el texto introducido.

- Los resultados de la búsqueda aparecen como una lista de posibles coincidencias en tiempo real mientras se introduce texto.
- Seleccione el nombre del grupo de usuarios deseado de la lista de posibles coincidencias para las acciones posteriores.
- La coincidencia de la búsqueda no distingue entre mayúsculas y minúsculas.

Crear un grupo de usuarios administrado dinámicamente

> El siguiente procedimiento no es aplicable a grupos de usuarios dinámicos.

Procedimiento

1. Haga clic en **+Añadir**.
2. Introduzca un nombre para el grupo de usuarios en el campo **Nombre**.
3. (Opcional) Haga clic en **Añadir descripción** para añadir una descripción para el grupo de usuarios.
4. Haga clic en la opción **Administrado dinámicamente (lo más común)**.
5. Establezca reglas o atributos según sus requisitos. La siguientes reglas corresponden a las opciones disponibles:
    - Atributo personalizado de LDAP
        - msExchPoliciesIncluded
        - msExchMailboxGrid
        - mailNickname

    Atributo predeterminado de LDAP

        - samAccountName

- userPrincipalName

Atributo predeterminado del usuario

- email_address
- distinguished_name
- last_name
- display_name
- first_name
- Grupo de usuarios
- Atributo personalizado del usuario

DN del grupo de usuarios

- GUID del grupo de usuarios
- Nombre del grupo de usuarios

6. Para cada regla, seleccione entre los usuarios locales y LDAP. Puede incluir o excluir un subgrupo utilizando los criterios de filtrado del **Grupo de usuarios**.
7. Añada más reglas haciendo clic en el icono más (+).
   Puede establecer filtros condicionales para seleccionar los que cumplan con **CUALQUIERA** o **TODAS** las reglas añadidas.
8. Cree un grupo de reglas haciendo clic en el icono jerárquico que hay junto al icono más (+).
9. Revise las reglas y atributos del grupo de usuarios en la consulta de texto que se muestra bajo la elecciones de las reglas.
10. En la sección **Resultados**, revise los detalles del (de los) usuario(s) que coinciden con los criterios configurados. Cuando añada o modifique una regla o un atributo, observará que se muestran los usuarios que coinciden, si es que existen:
11. Haga clic en **Guardar** para guardar el grupo de usuarios configurado.

Crear un grupo de usuarios administrado manualmente

1. Haga clic en **+Añadir**.
2. Introduzca un nombre de grupo.
3. (Opcional) Haga clic en **Añadir descripción** para añadir una descripción.
4. Seleccione la opción **Administrado manualmente (finalidad limitada)**.
5. En el campo **Buscar usuarios**, escriba la dirección de correo electrónico de cada usuario que vaya a incluir en el grupo.
   A medida que escribe, se encontrará y se mostrarán los usuarios que coincidan, si es que existen.
6. Seleccione los usuarios que desee añadir al grupo. Puede buscar y añadir más usuarios según sea necesario.
7. Haga clic en **Guardar**.

> Puede crear un grupo de usuarios administrados manualmente y, después, añadir este grupo a otro grupo de usuarios administrado dinámicamente. En tal escenario, editar el grupo de usuarios administrado manualmente no rompe la regla del grupo de usuarios administrados dinámicamente. No podrá eliminar un grupo de usuarios administrado manualmente si se agrega a un grupo de usuarios administrado dinámicamente.

Creación de un grupo de usuarios a partir de uno de los grupos de usuarios duplicados

Desde el Neurons for MDM 127 portal del Administrador se muestra el número de grupos de usuarios duplicados y el número de GUID correspondiente para identificar los grupos duplicados cuando se selecciona el atributo “Nombre del grupo de usuarios” en el creador de reglas. Además, una tabla bajo esta regla muestra la lista de los grupos de usuarios duplicados y sus detalles, como el Nombre del Grupo de Usuarios, el GUID, la Fuente y el nombre distinguido (DN).

Procedimiento

1. Inicie sesión en el portal del administrador de Ivanti Neurons for MDM
2. Vaya a **Usuarios**, **Grupos de usuarios**.
3. Haga clic en **+Añadir**. Se abre el asistente para crear un grupo de usuarios.
    1. Especifique el nombre en el campo **Nombre**.
    2. Seleccione **Nombre del grupo de usuarios** en el generador de reglas, seleccione **es igual a**, seleccione *uno* de los nombres de grupo duplicados.
    3. Haga clic en el icono **+** para añadir más reglas.
    4. Seleccione **Grupo de usuarios GUID**, **es igual a**.
    5. Copie y pegue el GUID de la tabla que muestra la lista de nombres de grupos de usuarios duplicados y GUIDs. El resultado muestra los usuarios asociados que se añadirán al nuevo grupo.
    6. Haga clic en **Guardar**. Los usuarios de la lista se añaden ahora al nuevo grupo de usuarios que ha creado.

Si no puede realizar las tareas en la página **Grupos de usuarios**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración del sistema
- Administración de usuarios

Crear un grupo de usuarios mediante la carga de archivos CSV

La función recién agregada permite a los administradores crear grupos de usuarios y agregar usuarios a los grupos creados mediante un archivo CSV.

Procedimiento

1. Inicie sesión en el portal del administrador de Ivanti Neurons for MDM
2. Vaya a **Usuarios**, **Grupos de usuarios**.
3. Haga clic en **+Añadir**.
4. Seleccione **Importar grupos de usuarios desde CSV**. Se abre el asistente de importación de grupos de usuarios.
    1. En la sección Descargar CSV, haga clic en **Descargar plantilla CSV** para descargar la plantilla CSV. Con la plantilla, puede editar el archivo para crear grupos de usuarios y agregar usuarios a los grupos de usuarios nuevos/existentes.
    2. Después de editar y guardar el archivo CSV, haga clic en **Elegir un archivo** para cargar el archivo CSV.
    3. Haga clic en **Cargar**. Aparecerá una confirmación si se ha cargado correctamente.

Propiedad	Descripción
Límite del tamaño del archivo CSV	El tamaño máximo del archivo CSV para importar está limitado a 2 MB.
Requisitos de formato de archivo CSV	Los archivos CSV deben contener exactamente 2 columnas: accountUid y groupName. • Tanto el valor accountUid como el groupName son obligatorios. • Los registros que no cumplan con estos criterios se descartarán durante la importación. Los administradores pueden descargar un archivo CSV de muestra desde la sección de importación como referencia.
Gestión de errores durante la importación	Si se producen errores o fallos durante la importación CSV, se generará un archivo de error. • Ahora los administradores pueden descargar este archivo de error para revisar las filas de CSV fallidas y comprender los motivos del error. • El archivo de error incluye la fila CSV específica que falló y proporciona una explicación del error.
Condiciones de importación correctas	La importación de usuarios a grupos de usuarios solo se realiza correctamente cuando el grupo de usuarios es local y se administra manualmente. • El usuario debe existir en el sistema para que la importación se realice correctamente.

Condiciones para crear un grupo de usuarios y agregar un usuario con un archivo CSV de muestra

Detalles del archivo CSV de muestra

accountUid: test_user_1@org.com

groupName: test_group_1

Condiciones	Descripción
Grupo existente	Si el grupo test_group_1 ya existe, el usuario test_user_1@org.com se asociará con el grupo.
Grupo inexistente	Si el grupo test_group_1 no existe, se creará un nuevo grupo con el nombre test_group_1 y el usuario test_user_1@org.com se asociará con el grupo.
Grupo no local	Si el grupo test_group_1 existe pero no es un grupo local, este registro se incluirá en el archivo CSV de error con el motivo "El grupo no es local".
Grupo no administrado manualmente	Si el grupo test_group_1 existe pero no es un grupo administrado manualmente, este registro se incluirá en el archivo CSV de error con el motivo "El grupo no es un grupo administrado manualmente".
Usuario inexistente	Si el usuario test_user_1@org.com no existe, este registro se incluirá en el archivo CSV de error con el motivo "Usuario no encontrado".
Usuario o grupo inexistente	Si tanto el usuario test_user_1@org.com como el grupo test_group_1 no existen, se creará un nuevo grupo con el nombre test_group_1 y este registro se incluirá en el archivo CSV de error con el motivo "Usuario no encontrado".

6.3. Ajustes del usuario

Esta sección contiene los siguientes temas:

- Editar el ajuste predeterminado
- Añadir un ajuste personalizado
- Eliminar un ajuste personalizado
- Configurar los ajustes para registros de nuevos dispositivos
- Configurar el límite de dispositivos por usuario
- Configurar el límite de borrado de dispositivos
- Ajustes del usuario
- Configurar la autenticación del Portal de autoservicio
- Establecer la complejidad de la contraseña
- Definir los Términos del servicio
- Configurar los correos electrónicos con los recordatorios de invitaciones para el usuario
- Configuración de los correos electrónicos de confirmación de registro del usuario
- Configurar el ajuste del horario de trabajo del usuario
- Configurar el ajuste de autenticación del Portal de administración

Los ajustes del usuario definen las opciones de registro de los dispositivos. Hay diferentes tipos:

- **Ajuste de registro de dispositivos**: establece la autenticación por contraseña, PIN o ambos; tipo de Apple Enrollment y propiedad del dispositivo.
    - Anteriormente, si se configuraba SAML auth/IdP, la autenticación SAML se utilizaba tanto para el registro de dispositivos como para la autenticación del portal.
    - **Configuración de registro de dispositivo de plataforma** : los administradores ahora pueden controlar la inscripción de dispositivo a nivel del sistema operativo restringiendo el registro de plataformas específicas de Apple, Android y Windows con el sistema. Esta nueva configuración de restricción a nivel de SO se aplica como control de inscripción principal y, cuando se habilita para una plataforma, las restricciones de registro relacionadas para esa plataforma se desactivan de forma automática. Esto ayuda a las organizaciones a aplicar políticas de inscripción y evitar que se registren plataformas de dispositivo no compatibles.

Ajuste de Límite de dispositivos: establece el número de dispositivos que puede registrar un usuario.

- **Ajuste de límite de borrado**: establece el límite del número máximo de dispositivos que se pueden borrar de una vez.
- **Ajuste de autenticación del portal de autoservicio:** Establezca el tipo de autenticación de la contraseña para el portal de autoservicio.
- **Ajuste de complejidad de la contraseña**: establece parámetros sobre complejidad de la contraseña y políticas para las cuentas locales que se utilizan para registrar dispositivos y acceder a los portales de autoservicio y del administrador.
- **Ajuste de las Condiciones del servicio:** establece las condiciones de servicio que se muestran al usuario en cada registro del dispositivo.
- **Ajuste del Recordatorio de invitación para el usuario:** establece las fechas y frecuencia para enviar correos electrónicos con recordatorios de invitaciones para el usuario.

- **Ajuste de confirmación del registro del usuario:** controla la capacidad de enviar el correo electrónico de confirmación de registro del usuario. Consulte **Configuración y uso de los correos electrónicos de confirmación de registro**para ver una descripción general de la solución y **Configuración de los correos electrónicos de confirmación de registro del usuario** a continuación, para ver instrucciones específicas sobre los ajustes del usuario.
- **Ajuste del horario de trabajo del usuario:**controla la capacidad de configurar un horario de trabajo del usuario que bloquee toda la comunicación de Sentry con los dispositivos administrados durante las horas prescritas no laborables. Muy útil para usuarios en regiones con leyes de desconexión laboral.
- **Ajustes de autenticación del portal de administración:** controla si Ivanti Neurons for MDM le solicita al administrador solo la contraseña o la contraseña y el PIN.

Puede editar los ajustes predeterminados para el grupo **Todos los usuarios** o añadir ajustes personalizados y asignarlos a otros grupos de usuarios.

Editar el ajuste predeterminado

Haga clic en el vínculo **Editar** en el ajuste que tiene el icono de bloqueo. No se puede eliminar un ajuste predeterminado.

Añadir un ajuste personalizado

Haga clic en el vínculo **Añadir ajuste para grupos específicos de usuarios**.

Eliminar un ajuste personalizado

Haga clic en el icono x.

Configurar los ajustes para registros de nuevos dispositivos

Puede configurar la versión mínima de SO, el tipo de autenticación y la propiedad del dispositivo para registros de nuevos dispositivos. La URL de inscripción de dispositivos generada en las versiones anteriores de Ivanti Neurons for MDM dejará de funcionar en la versión actual. El administrador deberá regenerar la URL de inscripción de dispositivos para el registro el dispositivo.

Registro de dispositivos de la lista de permitidos

La opción de registrar un dispositivo en una lista de permitidos solamente está disponible en la configuración de usuario predeterminada y no en la configuración de usuario personalizada. Puede cargar un archivo CSV utilizando la plantilla que contiene los números de serie y los atributos de dispositivo personalizados que se utilizan para incluir en la lista de permitidos algunos dispositivos. Puede incluir uno o más atributos de dispositivo personalizados existentes para crear la lista de permitidos. Esto le permitirá asignar atributos a grupos de dispositivos o espacios después del registro.

Para crear atributos personalizados, vaya a **Administrador > Atributos**. Los dispositivos iOS y macOS no pueden registrarse a través de iReg si la función de lista de permitidos está activada y el número de serie del dispositivo no se menciona en el archivo CSV. Si el archivo CSV contiene un número de serie duplicado, se considerará la última entrada del archivo CSV y los atributos de dispositivo personalizados asociados con esa entrada se considerarán para la asignación de dispositivo durante el registro.

Si la opción **Lista de dispositivos permitidos** está activada, solo los dispositivos incluidos en dicha lista podrán registrarse en Ivanti Neurons for MDM. Esta función solo es aplicable a los dispositivos que se registran a través del proceso de registro basado en web. Esto no afectará a los dispositivos que ya estén registrados en Ivanti Neurons for MDM. Después del registro, si el número de serie del dispositivo se elimina del archivo CSV, el dispositivo no se retirará. El usuario mencionado en el archivo CSV es opcional y se asignará solamente si el usuario se menciona en el archivo CSV y es un usuario válido.

Si desea cargar un nuevo archivo CSV, puede eliminar el archivo CSV existente y cargar el nuevo archivo. Las listas de permitidos solo son compatibles con iReg y si en caso de que se requiera el cliente Go, opte por el registro sin contacto. Para que funciones como AppConnect y Threat Defense funcionen, el cliente Go debe estar instalado en el sistema. Como no se admite el registro en la aplicación, el usuario puede primero registrar el dispositivo a través de iReg, y más tarde, se puede insertar la aplicación Go en los dispositivos desde el catálogo de aplicaciones. Cuando el usuario acepte la instalación de la aplicación, el dispositivo será un dispositivo gestionado y todas las funciones seguirán funcionando después del registro. La configuración «zero-touch» no puede utilizarse en los dispositivos en que el estado de AppConnect es Activo o Inactivo. Solo puede utilizarse cuando el estado de AppConnect es Ninguno. El estado de AppConnect se mantiene como Ninguno hasta que se inicia el cliente Go en el dispositivo después de registrarse a través de iReg.

Procedimiento

1. Inicie sesión en Ivanti Neurons for MDM.
2. Vaya a **Usuarios** > **Ajustes de usuario.**
3. En **Ajustes del registro de dispositivos**, haga clic en **+agregar ajuste para grupos de usuarios específicos**.
4. Edite el ajuste predeterminado **Tipo de autenticación del registro de dispositivos** o añada uno nuevo.
5. Introduzca un nombre en el campo **Nombre**.
6. (Opcional) Introduzca una descripción del ajuste.
7. En la sección **Ajustes de SO**, defina la versión mínima del SO para iOS, macOS o Windows:
8. Seleccione el botón de alternar **Habilitar la versión mínima** y seleccione una versión de SO de la lista desplegable.

> El ajuste Habilitar la versión mínima no es aplicable para registros del dispositivo DEP.

Para **Android**:

- Active la opción **Revisión de seguridad mínima** (solo Android) y especifique el período seleccionando el tipo de duración de las siguientes opciones de la lista desplegable:
  - **día(s)**
  - **mes(es)**
  - **año(s)**

  Active la opción **Lista de permitidos/lista de bloqueados del fabricante** y seleccione cualquiera de las siguientes opciones:
  - **Crear una lista de permitidos**- para permitir que solo se registren los dispositivos de estos fabricantes.
  - **Crear una lista de bloqueados**- para impedir que se registren los dispositivos de estos fabricantes.
    Para añadir a un fabricante:
    1. Haga clic en **Añadir fabricante**.
    2. Escriba el nombre del fabricante en el campo **Nombre del fabricante**.
    3. Haga clic en **Guardar**. El nombre del fabricante añadido aparecerá en la tabla.

    > El nombre del fabricante distingue entre mayúsculas y minúsculas. Para editar o borrar el nombre de un fabricante añadido, haga clic en la opción **Editar** o **Eliminar** del fabricante.

En la sección Inscripción de Apple, seleccione el Tipo de inscripción de Apple:

- **Inscripción de dispositivos**

- **Inscripción de usuarios**- predeterminado, la inscripción de usuarios se aplica a los dispositivos iOS y iPadOS.
- (Opcional) **Incluir dispositivo macOS (macOS 10.15+)**: seleccione esta opción para que la Inscripción de usuarios sea aplicable también a los dispositivos macOS.

En la sección **Método de invitación de registro (solo iOS y Android)**, habilite **Registro solo MAM**.

> Esta opción debería estar habilitada para los registros de dispositivos «MAM only» y, cuando se habilita, los usuarios son redirigidos a la App Store pública para que descarguen la aplicación del cliente de AppStation.

11. En la sección **Tipo de autenticación de registro de dispositivos**, seleccione una de las opciones siguientes de tipo de registro desde el desplegable **Seleccionar tipo de registro**. Si utiliza la Inscripción de dispositivos, asegúrese de que la configuración de Inscripción de dispositivos coincide con su elección.
    - **Solo contraseña**
    - **Solo PIN** Cuando selecciona esta opción, se bloquea el botón de alternar Omitir la autenticación de registro de dispositivos IdP.
    - **Contraseña y PIN**

      > Los usuarios todavía pueden recibir un PIN para completar la activación de la cuenta.

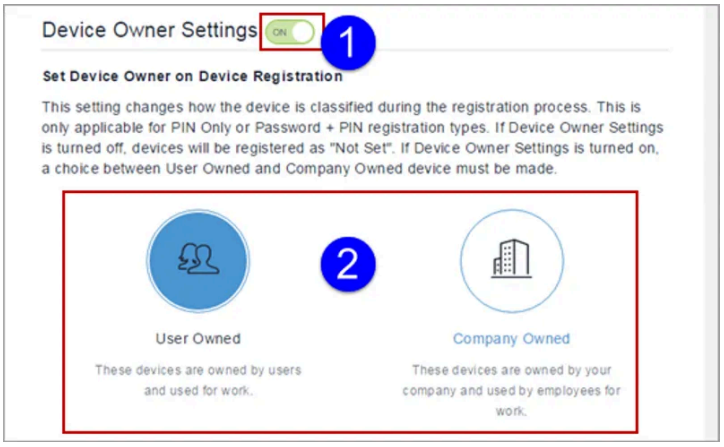
> Esta configuración afecta tanto al registro normal como al registro de Inscripción de dispositivos.

Para PIN, especifique lo siguiente. Durante el registro del dispositivo, el usuario puede hacer clic en **Reenviar PIN** si fuera necesario.

- **Vigencia del PIN**: durante cuánto tiempo será válido el PIN (1-30 días)
- **Longitud del PIN**: el número de caracteres (4-12)
- **Permitir que el usuario solicite un nuevo PIN**: (cuando lo olvide o caduque)

Opcionalmente, también puede activar los **Ajustes del propietario del dispositivo** y, a continuación, hacer clic en **Propiedad del usuario** o **Propiedad de la empresa**. Este ajuste cambia la clasificación del dispositivo durante el proceso de registro.

- Si los **Ajustes del propietario del dispositivo** están activados y el administrador ha marcado el dispositivo como Propiedad del usuario, el usuario tendrá la opción de marcar el dispositivo como Propiedad del usuario o Propiedad de la empresa durante la inscripción de dispositivos y también desde el portal de autoservicio. Para los dispositivos con inscripción de usuarios, los ajustes predeterminados de propietario del dispositivo serán «Propiedad del usuario», independientemente de lo que elija el administrador.
- Para dispositivos supervisados, el ajuste de propietario del dispositivo será «Propiedad de la empresa».



Haga clic en **Añadir+** para un grupo de usuarios, como mínimo, en el que desee distribuir el ajuste.

15. (Características a pedido solo para dispositivos iOS y macOS). También puede activar la opción **Lista de permisos de dispositivos** para permitir el registro del dispositivo basado en los números de serie de la lista de permisos.
16. Haga clic en **Siguiente**. Se abre la página de Distribución de ajustes del usuario.
17. Seleccione la distribución del grupo de usuarios.
18. Haga clic en **Hecho**.
19. Enviar una invitación a los usuario. Para obtener más información, consulte Invitar a usuarios.

Tenga en cuenta los puntos siguientes:

> Si el dispositivo de un usuario se registra solo mediante la opción PIN, el usuario recibe un correo electrónico con la confirmación del registro con un PIN de autenticación.

- Se envía un PIN a la Id. de correo electrónico del usuario.
- El usuario introduce el PIN en la página de registro del dispositivo.
- Si el PIN es correcto, el usuario es redirigido para completar el proceso de registro.

Para usuarios configurados con Proveedor de identidad (IdP) basado en SAML, Ivanti Neurons for MDM es compatible con la autenticación basada en PIN mientras registra el dispositivo. El Tipo de autenticación del registro de un dispositivo debe ser PIN y contraseña. La característica de PIN y contraseña actúa como autenticación de dos factores para mayor seguridad. En este caso, cuando un usuario intenta registrar un dispositivo:

- Se envía un PIN a la Id. de correo electrónico del usuario.
- El usuario introduce el PIN en la página de registro del dispositivo.
- Si el PIN es correcto, el usuario será redirigido a la página de inicio de sesión de IdP, donde el usuario debe introducir el nombre de usuario y la contraseña de IdP.
- Si las credenciales de IdP son correctas, el usuario es redirigido al dispositivo para completar el proceso de registro.

Configurar el límite de dispositivos por usuario

Procedimiento

1. Edite el ajuste predeterminado **Límite de dispositivos** o añada uno nuevo.

2. (Opcional) Haga clic en **+ Agregar configuración para grupos de usuarios específicos** para configurar el límite de dispositivos para grupos de usuarios específicos.
3. Edite o asigne un nombre para identificar el ajuste.
4. Escriba una descripción opcional del ajuste.
5. En el menú desplegable **Número máximo de dispositivos activos**, seleccione el límite de dispositivos Apple activos.
6. En el menú desplegable **Número máximo de dispositivos Apple watchOS para emparejar con un iPhone**, seleccione el límite de dispositivos Apple watchOS activos para emparejar con el iPhone.
7. (Opcional) Si **+ Agregar configuración para grupos de usuarios específicos** está seleccionado, haga clic en **Siguiente** y seleccione al menos un grupo de usuarios para la distribución de esta configuración.
8. Haga clic en **Hecho**.

Configurar el límite de borrado de dispositivos

Procedimiento

1. Edite el ajuste predeterminado del **Límite del borrado de dispositivos**.
2. Active la opción **Habilitar el límite de borrado para todos los usuarios (incluidas las funciones predeterminadas)**.
3. En el campo **Número máximo de dispositivos que un usuario puede borrar a la vez**, escriba el número máximo de dispositivos que se pueden borrar a la vez. El valor predeterminado es 1. Puede establecer un valor máximo de 200 como límite de borrado de dispositivos.
4. Haga clic en **Hecho**.

Configurar la autenticación del Portal de autoservicio

Procedimiento

1. Edite el ajuste predeterminado **autenticación del Portal de autoservicio** o añada uno nuevo haciendo clic en el **ajuste +Añadir para grupos de usuarios específicos**.
2. Edite o asigne un nombre para identificar el ajuste.
3. Escriba una descripción opcional del ajuste.
4. Seleccione un **Tipo de autenticación del Portal de autoservicio** del menú desplegable. Puede ser una de las siguientes opciones:
    - Contraseña
    - Certificado
5. Haga clic en **Siguiente**.
6. Seleccione uno o más grupos de usuarios para los que se puede distribuir esta configuración.
7. Haga clic en **Hecho**.

Establecer la complejidad de la contraseña

Puede establecer parámetros sobre complejidad de la contraseña y políticas para las cuentas locales que se utilizan para registrar dispositivos y acceder a los portales de autoservicio y del administrador.

> La longitud, características y políticas de la contraseña establecidas a continuación definen la seguridad de una contraseña.

También definen la dificultad que tendrá el usuario para seleccionar una contraseña válida. Si usa una cuenta local para sus usuarios finales y desea tener contraseñas seguras para acceder al portal del administrador, considere la posibilidad de emplear un PIN para registrar el dispositivo con el objetivo de que la complejidad de la contraseña no interfiera con el registro del dispositivo. Utilice el ajuste de tipo «Autenticación del registro de dispositivos» para seleccionar el modo de autenticación para el registro del dispositivo en **Ajustes del usuario > Ajuste del registro de dispositivos**.

Procedimiento

1. Edite los ajustes predeterminados de la **Complejidad de la contraseña**.
2. Defina los siguientes ajustes de complejidad de la contraseña:

Ajuste	Qué hacer
Longitud mínima de la contraseña	Mueva el control deslizante para especificar la longitud mínima de una contraseña con el objetivo de impedir que el usuario cree contraseñas breves e inseguras. El número oscila entre 8 y 32.
Características obligatorias	Especifique la cantidad de caracteres de la contraseña que deben cumplirse al seleccionar una contraseña. El mínimo de características que deben cumplirse es 3 (4 para los clientes federales).
Caracteres especiales (símbolos) obligatorios	Especifique la cantidad de caracteres no alfanuméricos que debe contener una contraseña.
Caracteres en mayúscula obligatorios	Especifique la cantidad de caracteres alfabéticos en mayúscula que debe contener una contraseña.
Caracteres en minúsculas obligatorios	Especifique la cantidad de caracteres alfabéticos en minúscula que debe contener una contraseña.
Caracteres numéricos obligatorios	Especifique la cantidad de caracteres numéricos minúscula que debe contener una contraseña.
Validaciones de la contraseña	
Secuencia numérica permitida	Seleccione la cantidad de números repetidos en una secuencia. Por ej.: 123.
Repetición de caracteres permitida	Seleccione la cantidad de caracteres alfabéticos repetidos. Por ej.: bbc.

3. Establezca las siguientes políticas sobre contraseñas para personalizar el comportamiento.

Ajuste	Qué hacer
Historial de contraseñas conservado	Mueva el control deslizante para seleccionar la cantidad de contraseñas nuevas que deben asociarse a la cuenta de un usuario antes de poder usar una contraseña antigua. El número oscila entre 3 y 36.
Período de caducidad de la contraseña	Mueva el control deslizante para seleccionar la duración de la caducidad de la contraseña en días. El número oscila entre 30 y 365 días.
Tiempo de espera por inactividad	Mueva el control deslizante para especificar el tiempo que un usuario puede estar inactivo antes del tiempo de sesión de un portal de administración o de un portal de autoservicio. El número oscila entre 5 y 60 (minutos).
Hubo un error en el umbral de inicios de sesión	Mueva el control deslizante para seleccionar la cantidad de intentos de inicio de sesión fallidos que se pueden hacer antes de que el bloqueo de cuenta tenga lugar a los 5 minutos. El número oscila entre 2 y 5. Cuando el número de intentos fallidos esté dentro del límite, se le muestra un mensaje al usuario sobre el bloqueo e indicándole que intente iniciar sesión más tarde. Cuando el número de intentos fallidos supere el límite, se le muestra un mensaje al usuario sobre el bloqueo e indicándole que intente iniciar sesión después de un tiempo determinado (en minutos).

4. Haga clic en **Hecho**. Si ha cambiado el ajuste predeterminado de Complejidad de la contraseña, la contraseña antigua de la cuenta local existente seguirá siendo la misma. Una vez que caduque, se solicitará al usuario que renueve la contraseña. Para los administradores que estén intentando iniciar sesión en el Portal de administración, pueden contactar con el Soporte técnico, que les dará pautas para restablecer la contraseña.

> Al registrar un dispositivo, el enfoque recomendado es usar el modo de registro solo PIN.

Definir los Términos del servicio

Procedimiento

1. Cree un nuevo ajuste de los **Términos de servicio**.
2. Asigne un nombre para identificar el ajuste.
3. Escriba una descripción opcional del ajuste.
4. Seleccione **Avisar al usuario**... opción.
5. Escriba un título y el texto para mostrar.
6. Haga clic en **Añadir+** para un grupo de usuarios, como mínimo, en el que desee distribuir el ajuste.
7. Haga clic en **Guardar**.

> Una vez que acepte, las condiciones de servicio no se pueden eliminar. No obstante, puede desactivar los avisos para un nuevo registro si desmarca la opción **Avisar al usuario**... opción.

Configurar los correos electrónicos con los recordatorios de invitaciones para el usuario

Los administradores pueden fomentar las inscripciones a los dispositivos utilizando este ajuste para enviar correos electrónicos con los recordatorios de invitaciones para usuarios.

Procedimiento

1. Edite un **ajuste de recordatorio de invitación para el usuario** existente o añada uno nuevo.
2. Edite o asigne un nombre para identificar el ajuste.
3. Escriba una descripción opcional del ajuste.
4. Asegúrese de que la opción **Recordatorios de invitación para el usuario** esté activada.
5. E el campo Definir fechas de inicio y fin, elija cuando quiere empezar a enviar recordatorios por correo electrónico y dejar de hacerlo.

> La cantidad máxima de correos electrónicos que se pueden enviar es de 30. Para restablecer este límite, el administrador debe volver a enviar la invitación.

6. En el campo Definir la frecuencia, elija la frecuencia con la que desea enviar recordatorios por correo electrónico.
7. Haga clic en **Siguiente**.
8. Seleccione una distribución para esta configuración.
9. Haga clic en **Hecho**.

Configuración de los correos electrónicos de confirmación de registro del usuario

Los administradores pueden enviar correos electrónicos a los nuevos usuarios que hayan completado el registro.

Procedimiento

1. Edite un **ajuste de confirmación de registro del usuario** existente o añada uno nuevo.
2. Edite o asigne un nombre para identificar el ajuste.
3. Escriba una descripción opcional del ajuste.
4. Asegúrese de que esté activada la opción **Enviar un correo electrónico de confirmación cuando el registro de usuario se realice correctamente**.
5. Haga clic en **Siguiente**.
6. Seleccione una distribución para esta configuración.
7. Haga clic en **Hecho**.

Configurar el ajuste del horario de trabajo del usuario

Los administradores pueden configurar un horario de trabajo del usuario para usuarios que bloquee toda la comunicación de Sentry con los dispositivos administrados durante las horas prescritas no laborables. Es muy útil para usuarios en regiones con leyes de desconexión laboral.

Procedimiento

1. Seleccione **Usuarios**.
2. Seleccione **Ajustes del usuario**.
3. En la sección, **Ajuste para grupos específicos de usuarios** seleccione **+Añadir ajuste para grupos específicos de usuarios**.

4. Introduzca un nombre para el ajuste.
5. Active el ajuste.
6. Seleccione la zona horaria.
7. Configure las horas durante las cuales Ivanti Neurons for MDM bloqueará el protocolo de Exchange ActiveSync, las aplicaciones habilitadas para AppConnect para AppConnect y las aplicaciones administradas.
8. Haga clic en **Siguiente**.
9. Configure la distribución y, a continuación, haga clic en **Hecho**.

> Los cambios aplicados pueden tardar hasta 1 hora y 15 minutos en tener efecto en el dispositivo.

Configurar el ajuste de autenticación del Portal de administración

Los administradores pueden ajustar el tipo de autenticación para autenticar el inicio de sesión del usuario. Este ajuste controla si al administrador se le pedirá solo la contraseña o la contraseña y el PIN.

Procedimiento

1. Edite un **Ajuste de autenticación del portal de administración** existente o añada uno nuevo.
2. Edite o asigne un nombre para identificar el ajuste.
3. Escriba una descripción opcional del ajuste.
4. En el **Tipo de autenticación del portal de administración**, seleccione cualquiera de las siguientes opciones:

Opción	Descripción
Contraseña	Seleccione esta opción para autenticar el inicio de sesión solo mediante contraseña. Los usuarios todavía pueden recibir un PIN para completar la activación de la cuenta.
Contraseña y PIN	Seleccione esta opción para autenticar el inicio de sesión mediante contraseña y PIN. Al seleccionar esta opción se muestran los siguientes campos: • **Vigencia del PIN**: seleccione de la lista desplegable la duración en minutos de la vigencia del PIN. Los minutos deben estar en un intervalo de 1 a 15. • **Longitud del PIN**: seleccione de la lista desplegable la longitud de caracteres del PIN. La longitud del PIN debe estar en un intervalo de 4 a 12. Esta opción es aplicable solo para las cuentas locales y no para las cuentas de administrador de LDAP.
Permitir que el usuario solicite un nuevo PIN	Seleccione esta opción para permitir a los usuarios que soliciten un nuevo PIN.

5. Haga clic en **Siguiente**.
6. Seleccione una distribución para esta configuración.
7. Haga clic en **Hecho**.

Para usuarios configurados con **Identity Provider** (IdP),Ivanti Neurons for MDMbasado en SAML, admite la autenticación mediante PIN en el portal de administración. El Tipo de autenticación del portal de administración debe ser PIN y contraseña. Esta característica

actúa como autenticación de dos factores para mayor seguridad. En este caso, cuando dicho usuario intente iniciar sesión en el portal:

- Se envía un PIN a la Id. de correo electrónico del usuario.
- El usuario introduce el PIN en la página de inicio de sesión del portal de administración.
- Si el PIN es correcto, el usuario será redirigido a la página de inicio de sesión de IdP, donde el usuario debe introducir el nombre de usuario y la contraseña de IdP.
- Si las credenciales de IdP son correctas, el usuario será redirigido al portal del administrador.

Al iniciar sesión en el portal del administrador, el usuario puede hacer clic en **¿Olvidó su contraseña?** para restablecerla. En la siguiente pantalla, el usuario puede introducir una nueva contraseña y el PIN (que se le pedirá en función de la configuración del modo de autenticación de usuario anterior) enviado a la dirección de correo electrónico del usuario. Haga clic en **Reenviar PIN** si fuera necesario. El usuario debe esperar 15 minutos entre solicitudes de contraseña olvidada.

> Cuando esta configuración se distribuye a los dispositivos, un intento de inicio de sesión consecutivo sin éxito (valor predeterminado: 5 intentos) por parte de un usuario que utilice una contraseña o un PIN provocará el bloqueo de la cuenta y se mostrará un mensaje al usuario durante el bloqueo.

6.4. Marca del usuario

La marca del usuario le permite personalizar el proceso de registro del dispositivo con nombres y logotipos que sus usuarios reconocerán. Puede personalizar la marca a nivel de usuario de las siguientes maneras:

- Establezca un nombre de host personalizado para la URL de registro.
- Muestre su logotipo en el correo electrónico y en la pantalla de registro.
- Muestre un icono de favoritos personalizado durante las actividades de registro.

> Actualizar los ajustes anteriores cambia el valor de referencia de **$**.

Licencia: Gold

Requisito previo:

- Decida qué nombre de host desea usar en su URL personalizada. Debe cumplir los siguientes requisitos:
  - No contener espacios
  - No contener caracteres especiales

Obtenga un archivo de logotipo que cumpla los siguientes requisitos:

  - Formato PNG
  - 580 x 80 pixeles

Obtenga un icono de favoritos que cumpla los siguientes requisitos:

  - Formato PNG
  - 64 x 64 pixeles

Procedimiento:

1. Vaya a **Usuarios > Marca de usuario**.
2. Haga clic en **Personalizar** (arriba a la derecha).
3. En el campo **Nombre de host**, escriba un nombre breve para usarlo como nombre de host en su URL.
4. Haga clic en **Comprobar disponibilidad** para confirmar que el nombre de host que ha introducido no ha sido usado por una tercera persona.
5. Si el nombre de host no está disponible, introduzca un nombre diferente.
6. Compruebe la URL de registro resultante en **Vista previa de la URL**.
7. Haga clic en **Siguiente**.
8. En **Logotipo**, haga clic en **Elegir archivo** para cargar el logotipo que va a usar en el correo electrónico y la pantalla de registro.
9. Haga clic en **Siguiente**.
10. En **Icono de favoritos**, haga clic en **Elegir archivo** para cargar el icono de favoritos que se va a mostrar en lugar del icono de favoritos de Ivanti Neurons for MDM durante las actividades de registro.
11. Haga clic en **Hecho**.

6.5. Inscripción de usuarios en el Apple Business Manager

Esta sección contiene los siguientes temas:

- Requisitos para habilitar la inscripción de usuarios
- Prioridad de los registros
- Diferencia entre la inscripción de MDM estándar y la Inscripción de usuarios
- Diferencia entre la Inscripción de usuarios y la Inscripción de dispositivos
- Conectar Ivanti Neurons for MDM con Apple Business Manager

Disponible para:

- Los dispositivos no supervisados con iOS 13.0 hasta la última versión admitida por Ivanti Neurons for MDM.
- Dispositivos con macOS 10.15 o versiones más recientes compatibles Ivanti Neurons for MDM.

Apple Business Manager es un lugar donde los equipos informáticos automatizan la implementación de dispositivos, compran y distribuyen contenido y gestionan las funciones en sus organizaciones. Apple Business Manager implementa la Inscripción de Usuarios; una opción de inscripción diseñada para las empresas que quieren pasarse al modelo «BYOD» (Bring Your Own Device). La Inscripción de usuarios es una versión modificada del protocolo MDM con un enfoque mucho mayor en la privacidad del usuario, implementada con el nivel de seguridad que las empresas necesitan.

Inscripción de usuarios permite a los administradores hacer lo siguiente:

- Instalar y desinstalar aplicaciones administradas
- Instalar y desinstalar las configuraciones de red
- Instalar una VPN parcial con alcance para las aplicaciones y cuentas administradas
- Requerir el uso de una contraseña

Requisitos para habilitar la inscripción de usuarios

A continuación figuran los requisitos para permitir la inscripción de usuarios. Si alguna de estas no se cumple, el tipo de inscripción será «inscrito en el dispositivo».

- Un dispositivo no supervisado con iOS 13.0 hasta la última versión compatible con Ivanti Neurons for MDM o un dispositivo con macOS 10.15 o versiones más recientes compatibles Ivanti Neurons for MDM.
- El ajuste del usuario para el campo Tipo de inscripción de Apple debe establecerse como «Inscripción de usuarios».
- Una cuenta de Apple Business Manager.
    - La cuenta de licencia de aplicaciones de Apple debe ser parte de la misma cuenta de Apple Business Manager.
    - Dentro de Apple Business Manager, si tiene un cuenta en Ubicaciones, debe tener Apps y Books que coincida con la misma ubicación. Puede que deba añadir una nueva ubicación (p. ej.: Costa Oeste).

ID de Apple administrada: la ID de Apple administrada que se asociará a cada dispositivo inscrito.

    - Esta ID de Apple administrada proporciona autenticación para la gestión y licencias de MDM.
    - Cuando la MDM rechaza aplicaciones y medios, las licencias de Apple necesarias se asignan a la ID de Apple administrada asociada al dispositivo.

- Como parte del cumplimiento con el RGPD, las ID de Apple administradas ahora se enmascaran en la lista de usuarios y en las páginas de detalles de usuario considerando el ID de Apple como los datos de usuario.
- Las ID de Apple administradas las usó por primera vez Apple School Manager y ahora las usa Apple Business Manager para la inscripción de usuarios.

> El ID de Apple administrada del dispositivo y el token de ubicación de Apps and Books deben ser de la misma organización de la cuenta de Apple Business Manager.

Si son diferentes, se muestra una notificación en el Portal de Administración de Ivanti Neurons for MDM cuando se produce un error en la asignación de licencia para una aplicación.

Microsoft Entra ID configurado para autenticación federada o un ID de Apple creado manualmente en Apple Business Manager con un dominio validado.

- Para obtener instrucciones sobre el uso de la Autenticación federada, consulte la **Guía del usuario de Apple Business Manager** en el sitio web de Apple. Es necesario iniciar sesión.

Los usuarios de dispositivos que estén sincronizados con LDAP deben asignarse a una función de administración de dispositivos y asociarse a una ID de Apple administrada.

En la página de la lista **Usuarios** y en la página de la lista **Dispositivos**, se puede agregar la columna ID de Apple administrada para que se muestre a todos los usuarios. En la página de la lista **Dispositivos**, puede agregar la columna Inscripción de usuarios inscritos para mostrar el estado de los dispositivos con Inscripción de usuarios. Además, las exportaciones de usuarios y dispositivos incluyen estas columnas en los archivos CSV.

Prioridad de los registros

- La inscripción de usuarios se admite a través del cliente Go para iOS e iReg. Apple ya no admite la inscripción de usuarios a través de Ivanti Go para iOS e iReg. **Inscripción de usuario basada en cuenta** solo está disponible en la cuenta profesional o educativa del dispositivo.
- La Inscripción de dispositivos automatizada y Apple Configurator siempre estarán inscritos en el dispositivo.
- Si se aplica la configuración MAM a un dispositivo, el registro MAM tiene prioridad sobre la Inscripción de usuarios.
- Si se cumplen tanto los requisitos de auth-only como de Inscripción de usuarios, la Inscripción de usuarios tiene prioridad.
- Si usted vuelve a inscribir un dispositivo desde Go para el cliente iOS, el tipo de inscripción será la misma que el tipo del registro del dispositivo, independientemente del cambio en el tipo de inscripción de Ivanti Neurons for MDM. Por ejemplo, si se inscribió un dispositivo por el usuario, cambie el tipo a Inscripción de dispositivos en Ivanti Neurons for MDM y vuelva a inscribir el dispositivo desde el cliente Go. El dispositivo seguirá estando inscrito por el usuario y no por el dispositivo.

Diferencia entre la inscripción de MDM estándar y la Inscripción de usuarios

En esta sección se explica la diferencia entre la inscripción estándar de MDM y la inscripción de usuarios en el Apple Business Manager.

Inscripción de MDM estánda

La siguiente lista indica lo que un servidor Ivanti Neurons for MDM puede hacer en una inscripción estándar de MDM, pero no podrá hacer en el modo Inscripción de usuarios.

El servidor MDM:

- No puede borrar el dispositivo.
- No ve las aplicaciones personales que el usuario del dispositivo ha instalado en el mismo.
- No puede convertir las aplicaciones instaladas por el usuario en aplicaciones gestionadas por MDM.
- No es posible borrar la clave de acceso del dispositivo (por ej. desbloquear el dispositivo).
- No puede establecer un largo y complejo requisito de código de acceso al dispositivo.
- No puede configurar un dispositivo VPN o proxy Wi-Fi, ni puede hacer ninguna gestión de la funcionalidad móvil.
- No puede ver los identificadores del dispositivo como el UDID, el número de serie o el IMEI.
- No puede aplicar muchas restricciones en todo el dispositivo (como la restricción de la clasificación del contenido de la aplicación), bloquear iCloud y aplicar cualquiera de las restricciones supervisadas.

Inscripción de usuarios en el Apple Business Manager

En la Inscripción de usuarios, el servidor MDM puede hacer todo lo necesario para administrar las aplicaciones, cuentas y datos de la empresa.

Con la Inscripción de usuarios se puede:

- Instalar aplicaciones internas o aplicaciones a través de licencias de Apps and Books del usuario (Apple).
  - Las licencias se aplican por orden de llegada y las consumen las ID de Apple administradas.
  - La licencia consumida por una aplicación instalada en un dispositivo con Inscripción de usuarios será diferente de la licencia consumida por la misma aplicación instalada en el dispositivo con inscripción de dispositivos.
  - Compruebe el tipo de licencia para las aplicaciones de Apple Apps y Books en una página de detalles del usuario a través de la pestaña Uso de licencia; se mostrará el Tipo de inscripción como Inscripción de usuario o Inscripción de dispositivo.

Aplicar los ajustes de la carga útil del código de acceso. Por ejemplo,

  - allowSimple = false
  - forcePIN = true
  - minLength = 6

Consultar datos relacionados con aplicaciones, certificados y perfiles gestionados por la empresa.

- Configurar una VPN por aplicación para aplicaciones, correo, contactos y calendarios que han sido instalados por MDM.
- Aplicar algunas restricciones, como «abrir en» administrado, contactos administrados, datos administrados en la pantalla de bloqueo y otras tantas.

Los datos de la empresa se almacenan en un volumen separado del Sistema de Archivos de Apple (APFS), que se crea en el momento de la inscripción, y se codifica por separado de los datos de usuario del dispositivo. Este volumen contiene datos almacenados por aplicaciones gestionadas; notas de la empresa; documentos de la unidad iCloud Drive de la empresa; entradas del Llavero de la empresa; adjuntos y cuerpos de correo gestionados y adjuntos del calendario. Anular la incripción de MDM destruye el volumen y las claves.

Todas las aplicaciones de terceros solo pueden ser aplicaciones personales o aplicaciones administradas a través de Ivanti Neurons for MDM. El servicio MDM no puede empezar a administrar aplicaciones que el usuario del dispositivo ya ha instalado. En este caso, el administrador deberá solicitar al usuario del dispositivo que elimine la aplicación personal antes de instalar la aplicación a través de MDM. El servicio MDM no puede empezar a administrar aplicaciones que el usuario ya ha instalado. Sin embargo, algunas aplicaciones de sistema como Notas y Archivos serán compatibles tanto con las cuentas de trabajo como con las personales.

Inscripción de usuarios para dispositivos macOS

La inscripción del usuario es compatible con dispositivos con macOS 10.15 o versiones más recientes compatibles Ivanti Neurons for MDM.

- Mobile@Work para macOS no es compatible con los dispositivos inscritos en la Inscripción de usuarios de macOS.
  - Incluso si la aplicación se distribuye al dispositivo con Inscripción de usuarios de macOS, la aplicación no se insertará al dispositivo desde MDM.
  - Por lo tanto, las funciones de Mobile@Work, como la administración de secuencias de comandos y la gestión de aplicaciones para las aplicaciones de Packager (MIP) no son compatibles con los dispositivos inscritos en la Inscripción de usuarios de macOS.

Dependencia de las aplicaciones y cambios de comportamiento en los dispositivos macOS con Inscripción de usuarios.

  - En los dispositivos macOS con Inscripción de usuarios, la dependencia de las aplicaciones funciona en base al mejor esfuerzo, ya que la MDM no conoce (no puede confirmar) el estado de la instalación de las aplicaciones con requisitos previos antes de distribuir la aplicación principal.
  - Las aplicaciones y configuraciones se pueden distribuir a los usuarios y grupos de usuarios que pertenezcan a los dispositivos macOS con Inscripción de usuarios. Sin embargo, las aplicaciones siempre muestran el botón **Instalar** en lugar de «Instalado» porque la MDM no puede mostrar el estado de la instalación de las aplicaciones en los dispositivos macOS inscritos en la Inscripción de usuarios.
  - Las aplicaciones instaladas se indican como Aplicaciones solicitadas en la página **Dispositivos > Inventario de aplicaciones**, ya que los dispositivos macOS inscritos en la Inscripción de usuarios no notifican al servidor Ivanti Neurons for MDM si las aplicaciones están instaladas o no en el informe del inventario.

En el filtro de distribución para las aplicaciones, los atributos Inscrito en la Inscripción de dispositivos e Inscrito en la Inscripción de dispositivos automatizada se pueden utilizar para la distribución personalizada, según sea necesario.

- Las licencias basadas en el usuario se admiten mediante ID de Apple administradas para instalar aplicaciones de Apple Apps y Books. No se permiten las licencias basadas en dispositivos. El catálogo de aplicaciones solo muestra las aplicaciones de Apple Apps y Books.
- No todas las configuraciones, políticas y acciones están permitidas. Véase la lista completa de las configuraciones y políticas que figuran a continuación de este procedimiento.
  - Si se distribuyen configuraciones no admitidas a un dispositivo macOS inscrito en la Inscripción de usuarios, no se distribuirán ni se aplicarán al dispositivo y pueden mostrar un mensaje como «Restricciones - este no es un tipo de solicitud válida».
  - Del mismo modo, las acciones de los dispositivos de administración no admitidas se informarán en la IU de Ivanti Neurons for MDM.
  - Los informes no admitidos no los enviará Ivanti Neurons for MDM.

A continuación se indican las configuraciones y políticas no admitidas para ser distribuidas a los dispositivos macOS inscritos en la Inscripción de usuarios:

- Código de acceso
- Túnel
- Tunnel (a petición)
- Configuraciones de VPN

- Creación automática de cuentas en Office 365
- Política de extensiones del kernel de macOS
- Preferencia de privacidad
- Restricciones de macOS
- Actualizaciones de software
- AirPrint
- Privacidad del cliente de MI
- FileVault 2
- Clave de recuperación de FileVault
- Cortafuegos
- Regla de políticas del sistema
- Preferencia de certificado
- Control de políticas del sistema
- Políticas del sistema administradas
- Restricciones de la AppStore de macOS
- Restricciones de grabación en disco de macOS
- Ajustes del Finder de macOS
- Mobile@Work para macOS
- Mobile@Work para secuencias de comandos de macOS
- Control multimedia permitido
- Servidor de zona horaria
- Política de aplicaciones permitidas

Diferencia entre la Inscripción de usuarios y la Inscripción de dispositivos

En esta sección se explica la diferencia entre la Inscripción de usuarios y la Inscripción de dispositivos.

La Inscripción de usuarios se aplica a los dispositivos con iOS 13.0 y macOS 10.15 hasta la última versión compatible. Los dispositivos anteriores a iOS 13.0 y macOS 10.15 se considerarán con «inscripción de dispositivos» independientemente de si el usuario del dispositivo ha sido habilitado para la Inscripción de usuarios o no.

> La inscripción de usuarios para Apple Business Manager no permite borrar o desbloquear. Sin embargo, el portal del usuario seguirá teniendo esas opciones disponibles aunque no funcionen.

Inscripción de usuarios comparada con la Inscripción de dispositivos			
Funcionalidad	Inscripción de usuarios	Mobile Application Management (Gestión de Aplicaciones Móviles, MAM)	Inscripción de dispositivos
Borrar el dispositivo y ver las aplicaciones personales del usuario	✗	✗	✓
Convertir de administrado a no administrado o viceversa	✗	✗	✓
Borrar el código de acceso del dispositivo, configurar una VPN en todo el dispositivo o el proxy Wi-Fi o gestionar la funcionalidad móvil	✗	✗	✓
Ver los identificadores del dispositivo como el número de serie, IMEI	✗	✗	✓
Aplicar restricciones supervisadas	✗	✗	✓ (Solo dispositivos supervisados)
Puede instalar y configurar aplicaciones y cuentas	✓	✓	✓
Puede configurar una VPN por aplicación, correo, contactos y calendarios que se hayan instalado por MDM	✓	✗	✓
Puede aplicar algunas restricciones, como «abrir en» administrado, contactos administrados, datos administrados en la pantalla de bloqueo y otras tantas.	✓	✗	✓
Puede consultar datos relacionados con aplicaciones, certificados y perfiles gestionados por la empresa.	✓	✗	✓

Conectar Ivanti Neurons for MDM con Apple Business Manager

En esta sección se describe cómo activar la Inscripción de usuarios para Apple Business Manager.

Requisitos previos

- Debe tener una cuenta de Apple Business Manager. Véase **https://business.apple.com/**.
- Debe solicitar e instalar un **certificado MDM** de Apple para administrar los dispositivos iOS.

Creación de usuarios locales para permitir la Inscripción de usuarios

En esta sección se explica la creación de usuarios locales y LDAP y la configuración de la Inscripción de usuarios para los dispositivos de Apple sin supervisión. La Inscripción de usuarios no funcionará en dispositivos supervisados o en dispositivos inscritos en la Inscripción de dispositivos de Apple.

Crear un grupo de usuarios administrado manualmente (estático)

Este es un procedimiento de una sola vez. Si ya ha creado este grupo, pase a la sección «Crear usuarios para la Inscripción de usuarios».

Procedimiento

1. Vaya a **Usuarios >** **Grupos de usuarios**.
2. Cree un grupo de usuarios (estático) administrado manualmente, como el Grupo de Inscripción de usuarios, para añadir usuarios con el tipo de registro del dispositivo como Inscripción de usuarios.
3. Haga clic en **Guardar**.

Crear un ajuste de tipo de registro de dispositivos

Este es un procedimiento de una sola vez. Si ya ha creado este grupo, pase a la sección «Crear usuarios para la Inscripción de usuarios». Para los dispositivos inscritos en la inscripción de usuarios, la configuración predeterminada del Propietario del dispositivo será «Propiedad del usuario».

Procedimiento

1. Vaya a **Usuarios >** **Ajustes del usuario**.
2. En la sección Ajuste del registro de dispositivos, haga clic en el ajuste **+ Añadir para grupos de usuarios específicos**.
3. Cree un nuevo ajuste, como el Registro IU, para los usuarios con el tipo de registro del dispositivo como Inscripción de usuarios.
4. En la sección Inscripción de Apple, seleccione **Inscripción de usuarios** como el Tipo de inscripción de Apple.
5. Haga clic en **Siguiente**.
6. En la página Distribución de ajustes del usuario, seleccione el grupo de usuarios recién creado, como el Grupo de Inscripción de usuarios.
7. Haga clic en **Hecho**.

Crear un usuario local para la Inscripción de usuarios

Como requisito previo, cree un grupo de usuarios administrado manualmente y un ajuste de registro de dispositivos para la Inscripción de usuarios.

Procedimiento

1. Vaya a **Usuarios**.

2. Haga clic en + **Añadir** > **Un solo usuario**.
   Introduzca la nueva información de usuario y añádala al grupo de usuarios recién creado, como el Grupo de Inscripción de usuarios. Para más información, consulte *Agregar un usuario* en el tema **Usuarios** .

Importación de usuarios LDAP para habilitar la Inscripción de usuarios

Requisitos previos

- Como requisito previo, establezca un conector Ivanti Neurons for MDM para acceder a los recursos de **LDAP**.
- Asegúrese de que el ajuste **ID administrador de Apple** está establecido en **Patrón** (dirección de correo electrónico del usuario). Asegúrese de que el patrón de la ID de Apple administrada sea único. De lo contrario, la cuenta no se actualizará con la ID de Apple administrada si ya existe la misma ID de Apple administrada en otra cuenta.
- (Opcional), incluir el subdominio "appleid" para evitar conflictos con los ID de Apple existentes.
- Puede importar usuarios desde LDAP e invitarlos a la Inscripción de usuarios. Los usuarios de LDAP importados tendrán sus ID de Apple administradas sincronizadas con Ivanti Neurons for MDM, lo cual es un requisito para la inscripción de usuarios.

Procedimiento

1. Vaya a **Usuarios.**
2. Haga clic en **+Añadir > Invitar a usuarios de LDAP.**
3. Haga clic en **Seleccionar usuarios** en la entrada del servidor LDAP.
4. En la página Añadir usuarios de LDAP, introduzca el nombre del usuario, grupo u OU en el campo de búsqueda.
5. Para añadir nuevos usuarios o grupos, haga clic en **+Añadir** junto a la entrada que desee añadir.
6. Haga clic en **Hecho**.

Importación de usuarios de Entra ID para habilitar la Inscripción de usuarios

Como requisito previo, conecte Ivanti Neurons for MDM con Microsoft Entra ID (Entra ID).

Puede invitar a usuarios de Entra ID para la Inscripción de Usuarios. Los usuarios de Entra ID importados tendrán sus ID de Apple administradas sincronizadas con Ivanti Neurons for MDM, lo cual es un requisito para la inscripción de usuarios.

Procedimiento

1. Vaya a **Administrador > Fuente de usuario de Entra ID**.
2. Edite los ajustes.
3. Seleccione **Activar este Entra ID**.
4. En el ajuste de ID administrada de Apple, seleccione una o más de la siguientes opciones:
   - **Patrón**
     - **Dirección de correo electrónico del usuario**: asegúrese de que el patrón de la ID de Apple administrada sea único. De lo contrario, la cuenta no se actualizará con la ID de Apple administrada si ya existe la misma ID de Apple administrada en otra cuenta.
     - Como alternativa, seleccione **userUPN**.
5. (Opcional), incluir el subdominio "appleid" para evitar conflictos con los ID de Apple existentes.
6. Seleccione **Invitar automáticamente a los usuarios importados desde Entra ID**. A los usuarios importados desde Entra ID a Ivanti Neurons for MDM se les invita automáticamente a registrarse por correo electrónico.

7. Haga clic en **Guardar**.

Instrucciones del usuario del dispositivo para registrarse mediante la inscripción de usuarios

En esta sección se describen las acciones que el usuario del dispositivo debe realizar para registrar la Inscripción de usuarios de Apple.

Procedimiento

1. En el dispositivo iOS que desee registrar, abra el correo electrónico de invitación que contiene el enlace y un texto que guía al usuario final a un enlace de registro como mobileiron.com/go.
2. Abre el enlace de registro en Safari.
3. Aparecerá la página de inicio de sesión. El usuario del dispositivo debe iniciar la sesión con sus credenciales de usuario local o LDAP.
   Aparecerá la página de registro aparece con un mensaje que dice que ya se descargó el perfil.
   Pulse Ajustes. Aparecerá la página Ajustes.
4. Pulse Inscribirse en [nombre de su empresa].
5. Aparecerá la página Inscripción del usuario.
6. Pulse Inscribir mi [Su dispositivo]. Por ejemplo, pulse Inscribir mi iPhone.
   Si pulsa Cancelar y eliminar perfil, tendrá que empezar de nuevo el proceso de registro.
   Se le presentará un inicio de sesión para la cuenta de Apple o su cuenta Federada. Introduzca la contraseña de su ID de Apple administrada. (La ID de Apple administrada aparecerá en la parte superior de su página de inicio de sesión).
   Puede que se le presente la opción de seguir con la sesión iniciada, haga una selección.
   Una página mostrará el mensaje «Inscripción correcta».

Uso de registros de dispositivos para la resolución de problemas

Para solucionar los errores o problemas de un dispositivo con Inscripción de usuarios, comience por revisar los registros del dispositivo.

Procedimiento

1. Vaya a Dispositivos.
2. Haga clic en el dispositivo para visualizar la página de detalles del dispositivo. Puede verificar los campos Inscrito en la inscripción de usuarios e ID de Apple administrada registrado.
3. Seleccione la pestaña Registros.
4. En la región Filtros, limite los registros del dispositivo utilizando filtros basados en nombres de acciones (como Finalizar la compra, Nombre del dispositivo, Definir token de arranque, Obtener token de arranque, etc.), estado, fecha de inicio y fecha de fin.
5. En la columna Acciones, haga clic en el icono del ojo para mostrar los detalles del registro del dispositivo, como la ID de inscripción.
6. Haga clic en **Aceptar**.

6.6. Licencias de usuario

Ivanti Neurons for MDM las licencias basadas en el usuario definen el número de usuarios que puede registrar, el número de dispositivos que se permite por licencia de usuario, la cantidad de contenido que puede configurar para la distribución a los dispositivos y qué funciones están disponibles. Si alcanza el límite de usuarios, aparece un triángulo rojo en la página del administrador. Si alcanza el límite de contenido, el servicio impedirá que pueda añadir más y mostrará un mensaje indicándole que ha llegado al límite.

Para determinar cuántas licencias de usuario debe planificar, tenga en cuenta los siguientes puntos:

- Cada licencia de usuario adquirida bajo el paquete Secure UEM o Secure UEM Premium permite el registro de hasta cinco dispositivos.
- Una vez que el usuario registra más de cinco dispositivos, se notifica otra licencia de usuario.
- No hay límite obligatorio en el número de licencias de usuario que un usuario puede notificar.
- Cuando los dispositivos se retiran o se borran, las licencias se anulan.

Por ejemplo, cuando la Usuaria1 registra su teléfono de empresa el primer día de trabajo, estará notificando una licencia de usuario. Una semana después, registra dos teléfonos personales y una tableta bajo la misma licencia. Cuando registre otra tableta, ya tendrá cinco dispositivos, de modo que estará notificando una segunda licencia de usuario. Si le roban su teléfono personal, borrará el dispositivo, lo cual anulará la segunda licencia de usuario.

Visualizar el número de dispositivos/licencias de un usuario

Procedimiento:

1. Vaya a **Usuarios.**
2. Haga clic en el vínculo del usuario.

En el panel izquierdo aparecen los detalles del usuario, incluidos el uso de la licencia.

6.7. Administrar usuarios

Esta sección contiene los siguientes temas:

- Añadir el usuario de una API para operaciones de Cisco ISE
- Asignar funciones a usuarios
- Funciones del usuario
- Encontrar y filtrar usuarios
- Asignar usuarios a grupos de usuarios
- Invitar a usuarios
- Activar y desactivar usuarios
- Gestionar múltiples inicios de sesión del administrador
- Cambiar una contraseña
- Enviar un mensaje
- Quitar usuarios de grupos de usuarios
- Eliminar a un usuario
- Exportar usuarios
- Asignar atributos personalizados a los usuarios
- Eliminar atributos personalizados de los usuarios
- Cambiar la configuración regional del usuario
- Editar un nombre de usuario
- No participar en la obtención de datos sobre localización
- Información de tiempo de espera
- Cancelar las analíticas sobre el uso del sistema
- Registro de dispositivo por generación de PIN

6.7.1. Añadir el usuario de una API para operaciones de Cisco ISE

Puede agregar un usuario de API con el rol "Operaciones de Cisco ISE" que permite a Cisco ISE interactuar con la API de Cisco ISE en Ivanti Neurons for MDM. Después de crear este usuario, se utilizan sus credenciales de Cisco ISE para autenticar las llamadas API en Ivanti Neurons for MDM. Estas API permiten a Cisco ISE obtener información sobre el dispositivo, realizar acciones sobre el dispositivo (como por ejemplo un borrado total, borrado corporativo y bloqueo del PIN) y enviar mensajes a los dispositivos.

> el usuario de la API no podrá acceder al portal de administración. Este usuario es solo para habilitar el uso de la API.

> solo al Superadministrador de un abonado se le asigna la función de Operaciones de Cisco ISE de forma predeterminada. El Superadministrador debe elegir explícitamente a los demás usuarios del sistema que deben tener esta función y asignársela. Los usuarios asignados a la función de Operaciones de Cisco ISE pueden, por su parte, asignar la función a otros usuarios adecuados en el sistema.

Procedimiento

1. Vaya a **Usuarios** > **Usuarios**.
2. Haga clic en **Añadir**.
3. Seleccione **Usuario de API**.
4. Complete el formulario resultante con la información del usuario:
    - Dirección de correo electrónico
    - Nombre
    - Apellidos

> El campo del nombre de usuario muestra la dirección de correo electrónico que ha introducido. En la mayoría de los casos, no debe editar este campo predeterminado. Consulte **Cuándo editar un nombre de usuario**.

Si desea cambiar el nombre en pantalla de este usuario, edite el texto predeterminado en el campo **Nombre en pantalla**.

6. Asigne una contraseña introduciéndola en los campos **Contraseña** y **Confirmar contraseña**.
7. Deje seleccionada la función **Operaciones de gestión de API de Cisco ISE** en la sección **Asignar funciones**.
8. Haga clic en **Hecho** para añadir al usuario.

Si no puede realizar las tareas en la página **Usuarios**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración del sistema
- Administración de usuarios

6.7.2. Asignar funciones a usuarios

Puede dar a los usuarios acceso a datos de Ivanti Neurons for MDM y funciones mediante la asignación de **roles**. Puede asignar funciones directamente a los usuarios o a grupos de usuarios. Al asignar una función a un {{grupo de usuarios}}, se da esa función a todos los usuarios de ese grupo.

> El rol de usuario de solo lectura no se asigna por defecto a los usuarios.
> La página Roles y las opciones asociadas están ocultas para los abonados que tienen acceso a Ivanti Neurons for UEM y Ivanti Neurons for MDM.

Los usuarios no pueden asignar los permisos que ya no tienen. Los permisos y las funciones que no están asignados a los usuarios no se muestran para su selección. En este caso, se mostrará un mensaje de error. Cuando un administrador de Ivanti Neurons for MDM o un administrador asociado intenta asignar roles a un administrador socio, Ivanti Neurons for MDM muestra un mensaje que indica que un administrador asociado debe llevar a cabo esta operación en el Portal del proveedor de servicios.

Para obtener más información sobre las funciones, consulte **Roles_Management.htm**.

Procedimiento:

1. Vaya a:
   - **Usuarios > Usuarios** *o*
   - Usuarios > Grupos de usuarios.

Seleccione uno o más usuarios o grupos de usuarios.

3. Haga clic en **Acciones**.
4. En la página de detalles del Usuario o la página de detalles del Grupo de usuarios, haga clic en **Asignar funciones** *o*
   En la página Lista de usuarios o Lista de grupos de usuarios, seleccione **Anexar funciones**.
5. Seleccione una o más de las siguientes funciones que desee asignar:
   - Administración del sistema | Multiespacio
   - Sistema de solo lectura | Multiespacio
   - Gestión de usuarios | Multiespacio
   - Solo lectura del usuario | Multiespacio
   - Importación del usuario e invitación de LDAP | Multiespacio
   - Administración de dispositivos | Específico del espacio
   - Dispositivo de solo lectura | Específico del espacio
   - Administración de aplicaciones y contenidos | Específico del espacio
   - Solo lectura de aplicaciones y contenidos | Específico del espacio
   - Acciones de dispositivos | Específico del espacio
   - Operaciones ISE de Cisco | Multiespacio
   - Administración de tareas programadas | Multiespacio
   - Servicios de plataformas comunes (CPS) | Multiespacio
   - Gestión de la migración de bajo impacto en los usuarios | Multiespacio
   - Inscripción de dispositivos personalizados | Multiespacio

- Editar Editar Microsoft Graph | Multiespacio
- Enviar/Cancelar borrado | Multiespacio
- Ver Microsoft Graph | Multiespacio
- Administrar integración de Access | Multiespacio

Haga clic en **Siguiente**.

7. Si los roles seleccionados están unidos por Espacio, entonces los Espacio seleccione todos los roles unidos a Espacios.

> Si solo hay un espacio (Espacio predeterminado), el paso Especificar espacio se omitirá cuando se asigne una función vinculada al espacio.

La página de resumen mostrará el nombre del espacio para el turno vinculado al espacio como espacio predeterminado.
Revise el resumen de las funciones que va a asignar y haga clic en **Hecho**.

Dar permiso al personal de soporte técnico para que usen las acciones básicas de los dispositivos

Las funciones de soporte técnico, por lo general, permiten al personal visualizar datos. No obstante, algunas organizaciones prefieren incluir las acciones básicas de los dispositivos:

- Forzar ingreso
- Bloquear
- Desbloquear
- Enviar mensaje
- Retirar
- Borrar

Procedimiento

Puede dar permiso a las acciones.

1. Vaya a **Usuarios > Usuarios*** o**** Usuarios > Grupos de usuarios**.
2. Seleccione uno o más usuarios o grupos de usuarios.
3. Haga clic en **Acciones**.
4. En la página de detalles del usuario o la página de detalles del grupo de usuarios, seleccione **Asignar funciones** *o*
   Desde la página de Lista de usuarios o Lista de grupos de usuarios, seleccione **Anexar roles**.
5. Seleccione **Solo lectura del dispositivo**.
6. Seleccione **Acciones de dispositivos**.
7. Haga clic en **Hecho**.

> Asegúrese de que ha seleccionado Dispositivo de solo lectura antes de seleccionar las Acciones del dispositivo para los usuarios que tengan permisos inesperados.

6.7.3. Funciones del usuario

Los roles de usuarios determinan las páginas que los usuarios pueden ver en Ivanti Neurons for MDM y las cosas que pueden realizar los usuario. La siguiente tabla enumera las funciones que se pueden asignar y que significa cada una.

Función	Descripción	Específica para el espacio
Administración del sistema	Permite a un administrador gestionar ajustes a nivel de inquilino como los certificados MDM, los ajustes de App Catalog, etc.	No
Sistema de solo lectura	Permite a un administrador visualizar los ajustes a nivel de inquilino como los certificados MDM, los ajustes de App Catalog, etc.	No
Administración de usuarios	Permite a un administrador añadir y eliminar usuarios, asignar funciones y añadir usuarios a los grupos de usuarios.	No
Usuario de solo lectura	Permite a un administrador ver usuarios y grupos de usuarios, así como las aplicaciones y catálogos de contenido.	No
Administración de dispositivos	Permite a un administrador gestionar grupos de dispositivos, configuraciones y políticas, además de realizar todas las acciones de los dispositivos.	Sí
Dispositivo de solo lectura	Permite a un administrador visualizar grupos de dispositivos, configuraciones y políticas.	Sí
Administración de aplicaciones y contenido	Permite a un administrador añadir, distribuir y eliminar aplicaciones y contenido.	Sí
Aplicaciones y contenidos de solo lectura	Ver datos en Usuarios, Aplicaciones, Contenido, incluidas las tareas de AppConnect	Sí
Acciones de dispositivos	Permite a un administrador iniciar acciones de dispositivos, como: • Forzar ingreso • Bloquear • Desbloquear • Enviar mensaje • Retirar • Borrar debe seleccionar «Solo lectura del dispositivo» antes de seleccionar «Acciones de dispositivos». De lo contrario, los usuarios no tendrán los permisos necesarios.	Sí
Importación e invitación de usuarios LDAP	Permite a un administrador registrar a otros usuarios LDAP y enviar invitaciones para que registren sus dispositivos.	No
Operaciones Cisco ISE	Permite a un administrador invocar las API necesarias para la integración de Cisco ISE.	No
Administración de tareas programadas	Permite a un administrador crear y administrar las tareas programadas para diferentes operaciones administrativas.	No
Servicios de plataformas comunes (CPS, por sus siglas	Permite a un administrador utilizar los Servicios de plataformas comunes.	No

Función	Descripción	Específica para el espacio
en inglés)		
Gestión de la migración de bajo impacto para el usuario	Permite a un administrador gestionar los ajustes de migración de bajo impacto para el usuario.	No
Inscripción de dispositivos personalizados	Permite a un administrador inscribir un dispositivo utilizando la inscripción de dispositivos personalizados.	No
Editar Microsoft Graph	Permite a un administrador editar los ajustes de Microsoft Graph API utilizados para la protección de aplicaciones de Office 365.	No
Ver Microsoft Graph	Permite a un administrador ver los ajustes de Microsoft Graph API utilizados para la protección de aplicaciones de Office 365.	No
Enviar/Cancelar Borrado	Permite a un administrador enviar un comando de borrado a un dispositivo o cancelar un comando de borrado emitido antes de que se ejecute.	No
Administrar integración de Access	Permite a un administrador gestionar la integración de Access.	No

Para obtener más información, consulte **Asignar funciones**.

6.7.4. Encontrar y filtrar usuarios

Esta sección contiene los siguientes temas:

- Buscar a un usuario
- Uso de la Búsqueda avanzada para los usuarios
- Cargando las consultas de Búsqueda para los usuarios
- Filtrar usuarios

Buscar a un usuario

Una vez que haya añadido muchos usuarios, puede ser útil usar filtros o búsquedas para encontrar rápidamente la entrada de un usuario.

Procedimiento

1. Vaya a **Usuarios.**
2. Escriba los caracteres en el cuadro cuadro de búsqueda.

Uso de la Búsqueda avanzada para los usuarios

Puede utilizar la opción de Búsqueda avanzada para buscar usuarios en función de reglas para identificar y ver los usuarios con criterios específicos. Las opciones de reglas se pueden anidar juntas utilizando las opciones CUALQUIERA (O) o TODOS (Y). Los usuarios que coinciden con las reglas se muestran debajo de la sección. Las regla se pueden crear con los operadores siguientes:

- comienza con
- termina con
- contiene
- no contiene
- no comienza con
- no termina con
- es menor que
- es mayor que
- se encuentra en el intervalo
- es igual a
- no es igual a

Desde Neurons for MDM 127ellvanti Neurons for MDM portal del Administrador se muestra el número de grupos de usuarios duplicados y el número de GUID correspondiente para identificar los grupos duplicados cuando se selecciona el atributo Nombre del grupo de usuarios en el creador de reglas. Además, una tabla bajo esta regla muestra la lista de los grupos de usuarios duplicados y sus detalles, como el Nombre del Grupo de Usuarios, el GUID, la Fuente y el nombre distinguido (DN).

Procedimiento

1. En la página Usuarios, haga clic en el enlace **Búsqueda avanzada**.

2. Haga clic en **Cualquiera** si los usuarios deben coincidir con al menos una de las reglas o en **Todas** si los usuarios deben coincidir con todas las reglas.
3. Crear una regla que defina los criterios de búsqueda, como Grupo de usuarios, Atributo de usuario personalizado y Atributo LDAP personalizado.
4. (Opcional) Haga clic en + para crear reglas adicionales, si fuera necesario.
5. (Opcional) Haga clic en **Guardar** para guardar la consulta.
6. Haga clic en **Buscar**. En la página se muestran la lista de usuarios que coinciden con los criterios de búsqueda.

Cargando las consultas de Búsqueda para los usuarios

Procedimiento

1. En la página Usuarios, haga clic en el enlace **Búsqueda avanzada**.
2. Haga clic en el icono «Carpeta». Aparecerá la ventana **Búsqueda avanzada**. La lista de las consultas de búsqueda creadas se muestra en la sección **Cargar consulta**. En esta sección se muestran los siguientes detalles:
   - **Nombre de la consulta**: el nombre de la consulta cargada.
   - **Contenido de la consulta** muestra el contenido de las reglas que definen la consulta de búsqueda.
   - **Acciones**: seleccione la acción que se realizará en la consulta.
3. Haga clic en **Cargar consulta** en la columna **Acciones** para ver la lista de usuarios que coinciden con los criterios definidos en la consulta cargada.
   Para borrar una consulta cargada, haga clic en el icono «Borrar».

Filtrar usuarios

La barra de navegación lateral de Filtros tiene una lista con varias secciones que le ayudan a buscar un usuario concreto en la lista total de usuarios. El asistente de Administrar filtros contiene la lista de todas la secciones que puede seleccionar para que se muestren en la barra de navegación de Filtros.

Procedimiento

1. Vaya a **Usuarios.**
2. Haga clic en las casillas relevantes de las secciones que se listan en el asistente de Administrar filtros. Puede buscar las siguientes opciones:
   - Administradores
   - Estado de Google
   - Estado de la invitación
     - Completa (el usuario la recibió y respondió).
     - Caducada (el usuario no respondió a tiempo).
     - No invitado (no ha invitado a este usuario).
     - Pendiente (Pendiente de la respuesta del usuario).

   Caducidad de la contraseña

     - Caduca el (la opción de usuarios con caducidad de la contraseña está ajustada en una fecha concreta).
     - Nunca (la opción de usuarios con caducidad de la contraseña está ajustada en «nunca»).

- Grupo de usuarios (Seleccione los {{grupos de usuarios}} de su interés).
- Fuente de usaurio
  - LDAP
  - Entra ID
  - Lista
  - Salesforce
  - Local
- Sincronización
  - Sincronización directa: lista los usuario que se sincronizaron de manera directa desde el servidor de LDAP
  - Sin sincronización: lista los usuario que se eliminaron del servidor LDAP
  - Sincronización indirecta: lista los usuario que se sincronizaron de manera indirecta desde el servidor de LDAP
  - N/A

3. (Opcional) Haga clic en **Restablecer valores predeterminados** para restablecer la selección a los filtros predeterminados. La barra de navegación de Filtros muestra las secciones seleccionadas. Si desmarca todas las casillas del asistente de Administrar filtros, la barra de navegación lateral de Filtros mostrará todas las secciones.
4. Haga clic en cualquier lugar fuera del asistente de Administrar filtros para salir del asistente.
5. Haga clic en el icono x para cerrar la barra de navegación lateral del Filtros y haga clic en **Filtros** para volver a abrir la barra de navegación lateral.

6.7.5. Asignar usuarios a grupos de usuarios

Esta sección contiene los siguientes temas:

- Asignar usuarios desde la página usuarios
- Asignar usuarios desde la página grupos de usuarios

Asignar usuarios a grupos de usuarios es una forma estupenda de reducir al mínimo la cantidad de veces que tiene que repetir tareas como las siguientes:

- distribuir aplicaciones
- asignar funciones

Asignar usuarios desde la página usuarios

1. Vaya a **Usuarios.**
2. Seleccione los usuarios con los que desea trabajar.
3. Haga clic en **Acciones**.
4. Seleccione **Asignar al grupo**.
5. Seleccione los grupos o haga clic en **Crear nuevo** para iniciar un grupo nuevo.
6. Haga clic en **Guardar**.

Asignar usuarios desde la página grupos de usuarios

1. Vaya a **Usuarios > Grupos de usuarios**.
2. Seleccione los grupos de usuarios con los que desea trabajar.
3. Haga clic en **Acciones** (arriba a la derecha).
4. Seleccione **Asignar usuarios**.
5. Escriba la dirección de correo electrónico de cada usuario.
6. Haga clic en **Asignar usuarios**.

6.7.6. Invitar a usuarios

Cuando añade a un usuario, tiene la posibilidad de invitar a ese usuario a que inscriba sus dispositivos. De hecho, esta opción está seleccionada de forma predeterminada. El usuario invitado recibe un mensaje de correo electrónico que contiene la información necesaria para inscribirlos. También puede invitar (o volver a invitar) a un usuario desde la página **Usuarios > Usuarios**.

Procedimiento

1. Vaya a **Usuarios.**
2. Seleccione los usuarios a los que desea invitar.
3. Seleccione **Acciones > Enviar invitación**. Aparece la vista previa de la invitación, junto con una opción para establecer la propiedad del dispositivo en **UsuarioPropiedad** o **Propiedad de la empresa**.

4. Opcionalmente, encienda **Configuración del propietario del dispositivo**.
5. Haga clic en **propiedad del usuario** o **propiedad de la empresa**. Este ajuste cambia la clasificación del dispositivo durante el proceso de registro. Esto solo es aplicable a los tipos de registro Solo PIN o Contraseña y PIN. Si los **Ajustes del propietario del dispositivo** están desactivados, los dispositivos se registrarán como "No ajustados". Para los dispositivos supervisados, el ajuste del propietario del dispositivo será "Propiedad de la empresa".
6. Haga clic en **Enviar**. Si se llevó a cabo un registro de dispositivos basados en PIN, el usuario recibirá un PIN en la dirección de correo electrónico que registró. Si se ajusta un registro basado en código QR, el usuario recibirá un código QR.
7. Haga clic en **Aceptar**.

> Si la función de correo electrónico de confirmación de registro está activada como se describe en **Configuración y uso de los correos electrónicos de confirmación de registro**, también verá un recordatorio de que el usuario va a recibir un correo electrónico de confirmación de registro una vez que se realice correctamente el registro. Para recibir el correo electrónico, el usuario debe formar parte de la lista de distribución que se especifica en **Configuración de los correos electrónicos de confirmación de registro del usuario** en **Ajustes del usuario**.

Para obtener más información, consulte **Importar usuarios LDAP**.

6.7.7. Activar y desactivar usuarios

Esta sección contiene los siguientes temas:

- Activar y desactivar usuarios locales
- Activar y desactivar usuarios LDAP

Los usuarios locales y de LDAP pueden estar en estado activado o desactivado. En función de su estado, puede crear políticas personalizadas utilizando la condición «Usuario activado» y configurando una acción para esa condición en el creador de normas. Por ejemplo, puede existir la regla de política personalizada para retirar los dispositivos que pertenecen a los usuarios locales/LDAP desactivados.

Activar y desactivar usuarios locales

De forma predeterminada, cuando se crea un usuario local, el usuario está en estado activado.

Procedimiento

1. Vaya a **Usuarios.**
2. Haga clic en el nombre en pantalla del usuario local.
3. Haga clic en **Editar**. Aparecerá la ventana **Autenticación obligatoria**.
4. Introduzca su contraseña de administrador y haga clic en **Autenticar**.

> cuando se introducen varias entradas incorrectas de la contraseña y si se supera el «Límite del umbral de inicio de sesión fallido» establecido en los «Ajustes de complejidad de la contraseña», la cuenta se bloqueará y se cerrará la sesión actual.

5. Seleccione o deseleccione la opción **Activado** para activar o desactivar, respectivamente, al usuario local.
6. Haga clic en **Guardar**.

Activar y desactivar usuarios LDAP

Puede activar o desactivar usuarios LDAP solo para Microsoft Active Directory. En Microsoft Active Directory, al abrir las propiedades de la cuenta de un usuario, haga clic en la pestaña **Cuenta** y, a continuación, seleccione o deseleccione las casillas del cuadro de diálogo con las opciones de **Cuenta**. Entonces se asignarán valores numéricos al atributo **UserAccountControl**. El valor que se asigne al atributo indicará a Windows qué opciones se han activado. Luego de asignar un valor al atributo UserAccountControl, el estado del usuario lo reflejará después de la sincronización de LDAP con Ivanti Neurons for MDM.

A continuación se indican los posibles valores que se pueden asignar:

- 512 - Habilitado.
- 514 - Desactivado.
- 66048 - Activado, la contraseña no caduca nunca.
- 66050 - Desactivado, la contraseña no caduca nunca.

Ver las cuentas del usuario

Procedimiento

1.	Haga clic en **Iniciar**.

	2.	Vaya a **Programas**.

3.	Vaya a **Herramientas administrativas**.

	4.	Haga clic en **Usuarios y equipos de Active Directory**.

Para obtener más información, consulte **https://support.microsoft.com/en-in/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-pro**.

Puede ver y editar los atributos usando la herramienta Ldp.exe o el complemento Adsiedit.msc. Solo los administradores con experiencia debe usar estas herramientas para editar Active Directory. Ambas herramientas están disponibles después de haber instalado las herramientas de la Asistencia técnica desde sus soportes de instalación originales de Windows.

6.7.8. Gestionar múltiples inicios de sesión del administrador

Múltiples sesiones del portal del administrador de Ivanti Neurons for MDM son compatibles de manera que el administrador puede ver distintas páginas del portal de manera simultánea. Si usted es administrador, puede ver la fecha del último inicio de sesión para ayudarle hacer un seguimiento de los múltiples inicios de sesión.

Ver los datos de inicio de sesión del último administrador

Procedimiento

1. Haga clic en **Cuenta**
2. Lea la entrada **Último inicio de sesión:**.

6.7.9. Cambiar una contraseña

Esta sección contiene los siguientes temas:

- Cambiar contraseña desde la pestaña Usuarios
- Aplicar contraseña que nunca caduque
- Eliminar el ajuste para que no caduque nunca la contraseña

> Si un usuario tiene un rol de Administración del sistema, solo un Súperusuario o un usuario que tenga la sesión activa podrá ver la opción **Cambiar contraseña**.

Puede cambiar su contraseña de Ivanti Neurons for MDM. También puede cambiar la contraseña para otro usuario si tiene permiso.

Procedimiento

1. Haga clic en el icono Cuenta (arriba a la derecha).
2. 
   Seleccione **Cambiar contraseña** en el menú desplegable.
3. Introduzca su contraseña actual.
4. Introduzca su nueva contraseña.
5. Introduzca otra vez su nueva contraseña.
6. Para definir una contraseña que no caduque, seleccione **Establecer contraseña para que nunca caduque**.

> al establecer la contraseña para que nunca caduque, se anula el **Período de caducidad de la contraseña** definido en Usuarios > Ajustes del usuario > Ajuste de complejidad de la contraseña.

7. Haga clic en **Hecho**.

> para restablecer la contraseña de la cuenta local y que caduque, desactive la opción **Establecer contraseña para que nunca caduque**. Una vez que esta opción deje de estar seleccionada, una ventana emergente mostrará la fecha de caducidad anterior de la contraseña aplicada al usuario.

Cambiar contraseña desde la pestaña Usuarios

Procedimiento

1. Vaya a **Usuarios.**
2. Haga clic en el nombre en pantalla del usuario.
3. Haga clic en **Editar** (arriba a la izquierda). Se abre la ventana **Autenticación obligatoria**. Los administradores (que son usuarios locales o usuarios de LDAP) deben autenticarse introduciendo la contraseña del administrador antes de editar el usuario.
4. Introduzca su contraseña de administrador y haga clic en **Autenticar**.

> cuando se introducen varias entradas incorrectas de la contraseña y si se supera el «Límite del umbral de inicio de sesión fallido» establecido en los «Ajustes de complejidad de la contraseña», la cuenta se bloqueará y se cerrará la sesión actual.

5. Introduzca la contraseña actual en el campo **Contraseña actual**.

> este campo no se mostrará cuando cambie la contraseña de otro usuario.

6. Introduzca la nueva contraseña en el campo **Cambiar contraseña**.
7. Confirme la nueva contraseña.
8. Haga clic en **Guardar** (arriba a la izquierda).

Aplicar contraseña que nunca caduque

1. Vaya a **Usuarios.**
2. Seleccione uno o más usuarios.
3. Haga clic en **Acciones**.
4. Seleccione **Asignar contraseña para que no caduque nunca**. Aparece la ventana **Establecer contraseña de la cuenta local para que nunca caduque**.
5. Haga clic en **Enviar**.

Eliminar el ajuste para que no caduque nunca la contraseña

1. Vaya a **Usuarios.**
2. Seleccione uno o más usuarios.
3. Haga clic en **Acciones**.
4. Seleccione **Eliminar la opción de que la contraseña no caduque nunca**. Aparece la ventana **Eliminar la contraseña de la cuenta local para que nunca caduque**.
5. Haga clic en **Enviar**. Una vez que se haya eliminado este ajuste, se aplicará a los usuarios la fecha de caducidad anterior de la contraseña.

6.7.10. Enviar un mensaje

Esta sección contiene los siguientes temas:

- Enviar un mensaje a los usuarios
- Enviar un mensaje a los dispositivos

Puede enviar un mensaje a cualquier usuario conocido. Los mensajes pueden ser correo electrónico o {{notificaciones push}}. Solamente los usuarios con dispositivos inscritos pueden recibir notificaciones push.

Requisitos previos

- Para dispositivos de iOS, asegúrese de que está instalado el cliente de Go.
- Para dispositivos de macOS, asegúrese de que está instalado el cliente de Mobile@Work.

Enviar un mensaje a los usuarios

1. Vaya a **Usuarios > Usuarios**.
2. Seleccione los usuarios a los que desea enviar un mensaje.
3. Haga clic en **Acciones** (arriba a la derecha).
4. Haga clic en **Enviar mensaje**.
5. Si no desea enviar ningún mensaje de correo electrónico, quite la marca de verificación en la casilla **Enviar un mensaje por correo electrónico**.
6. Si va a enviar un mensaje de correo electrónico, introduzca un asunto y el texto del mensaje.
7. Si va a enviar una notificación push, seleccione la casilla **Enviar una notificación push** e introduzca el texto del mensaje.
8. Haga clic en **Enviar**.

Enviar un mensaje a los dispositivos

1. Vaya a **Dispositivos > Dispositivos**.
2. Seleccione los dispositivos a los que desea enviar un mensaje.
3. Haga clic en **Acciones** (arriba a la derecha).
4. Haga clic en **Enviar mensaje**.
5. Opcionalmente, también puede hacer clic en el enlace del nombre del dispositivo para ir a la página de detalles del Dispositivo y hacer clic en el icono **Enviar mensaje** .
6. Si no desea enviar ningún mensaje de correo electrónico, quite la marca de verificación en la casilla **Enviar un mensaje por correo electrónico**.
7. Si va a enviar un mensaje de correo electrónico, introduzca un asunto y el texto del mensaje.
8. Si va a enviar una notificación push, seleccione la casilla **Enviar una notificación push** e introduzca el texto del mensaje.

> El mensaje de notificación push también puede incluir URL a las que pueden acceder los usuarios.

9. Haga clic en **Enviar**.
   Cuando se envía una notificación push al usuario, este podrá ver el icono de una campana en la barra de herramientas de la

pantalla del dispositivo. Al pulsar en el icono de la campana, el usuario podrá ver el historial de notificaciones recibido y llevar a cabo una acción o eliminar una notificación.

Disponibles tanto en las páginas de **Dispositivos** como de **Usuarios** , los administradores pueden incorporar atributos específicos de dispositivos o usuarios en los mensajes, que posteriormente se ponen en cola para su envío a los usuarios finales.

6.7.11. Quitar usuarios de grupos de usuarios

Esta sección contiene los siguientes temas:

- Quitar usuarios desde la página usuarios
- Quitar usuarios desde la página grupos de usuarios

Quitar a un usuario de un grupo de usuarios implica que:

- cualquier función asignada a ese grupo queda eliminada del usuario
- cualquier aplicación asignada a ese grupo deja de estar disponible en el {{catálogo de aplicaciones}}
- las aplicaciones que se configuraron para ser eliminables se eliminan de los dispositivos del usuario

Quitar usuarios desde la página usuarios

1. Seleccione el usuario con el que desea trabajar.
2. Haga clic en **Acciones** (arriba a la derecha).
3. Seleccione **Quitar del grupo**.
4. Seleccione los grupos.
5. Seleccione **Quitar**.

Quitar usuarios desde la página grupos de usuarios

1. Haga clic en el grupo de usuarios para mostrar los detalles.
2. Haga clic en **Editar** (arriba a la derecha).
3. Haga clic en el vínculo **Eliminar** que hay junto al usuario que desea eliminar.
4. Haga clic en **Guardar** (arriba a la derecha).

6.7.12. Eliminar a un usuario

Esta sección contiene los siguientes temas:

- Qué ocurre cuando se elimina a un usuario local
- ¿Qué ocurre con los usuarios de LDAP?

Procedimiento

1. Vaya a **Usuarios > Usuarios.**
2. Seleccione la entrada del usuario.
3. Haga clic en **Acciones** (arriba a la derecha).
4. Seleccione **Eliminar**.

Cuando un administrador de Ivanti Neurons for MDM o un administrador asociado intenta eliminar a un administrador socio, Ivanti Neurons for MDM muestra un mensaje que indica que un administrador asociado debe llevar a cabo esta operación en el Portal del proveedor de servicios.

> Si un usuario tiene algunos dispositivos asociados a su cuenta, primero debe retirar y eliminar los dispositivos y luego eliminar el usuario. Si el usuario no tiene dispositivos, la información del usuario se puede eliminar cuando se elimina el usuario.

Qué ocurre cuando se elimina a un usuario local

- Toda la información relacionada con un usuario eliminado se elimina también del sistema.
- Se retiran los dispositivos asociados con el usuario.
- Se mantiene el contenido cargado por el usuario.
- No se permiten más registros de dispositivos para la cuenta del usuario.

¿Qué ocurre con los usuarios de LDAP?

- Si el servidor LDAP se ha desactivado, el usuario LDAP no puede eliminarse permanentemente. La siguiente sincronización de datos LDAP restaurará a un usuario LDAP eliminado.
- Si el servidor o grupo LDAP se ha eliminado, los usuarios LDAP se convierten en usuarios locales y sí pueden eliminarse.
- Cuando se elimina un usuario desde LDAP, no se eliminará de la nube. El estado de sincronización cambiará a "NO_SYNC", pero no se eliminará el usuario.

6.7.13. Exportar usuarios

Como administrador, puede exportar una lista de usuarios desde Ivanti Neurons for MDM.

> Por motivos de seguridad, cuando se exporta el PIN de registro del dispositivo del usuario a un archivo CSV, el PIN se enmascarará como '' en lugar del PIN real.

Procedimiento

1. Vaya a **Usuarios > Usuarios**.
2. Seleccione uno o más usuarios de la lista.
3. Haga clic en **Exportar a CSV**.

Verá una ventana emergente que le informará de que el informe exportado tardará un tiempo en procesarse. Una vez enviada la solicitud, debe esperar a que se complete la solicitud para enviar otra solicitud. Cuando el informe esté listo, recibirá un mensaje que le indicará que debe descargar o eliminar el informe generado. Usted también recibirá un correo electrónico con un enlace para descargar el informe.

> Los detalles de los atributos **Usuario personalizado** y **LDAP** también se pueden exportar a un archivo CSV junto con otros detalles.

> Cuando se agrega un usuario con un valor de campo que contiene los caracteres +,-,= o @, los datos del usuario del archivo CSV exportado añadirán automáticamente un prefijo al campo con una comilla única (') o un símbolo de barra (|) además de una barra diagonal inversa (\). Esto se hace para evitar la vulnerabilidad de inserción en Excel.

6.7.14. Asignar atributos personalizados a los usuarios

Se pueden asignar atributos personalizados a los usuarios, como el departamento, a uno o más usuarios. Cada atributo tiene un valor correspondiente que puede usar para tareas como la creación de configuraciones y grupos de usuarios. Puede asignar atributos personalizados a uno o más usuarios.

Procedimiento

1. Vaya a **Administrador > Sistema >Atributos** para crear nuevos atributos personalizados en caso necesario.
2. Vaya a **Usuarios.**
3. Seleccione uno o más usuarios.
4. Haga clic en **Acciones**.
5. Seleccione **Asignar atributos personalizados**.
6. Seleccione una de las siguientes opciones:
    - Forzar la asignación (sobreescritura) de todos los atributos aunque se encuentre algún valor existente.
    - Sobrescribir solo si el valor está vacío y omitir atributos con valores existentes.

Seleccione los atributos que desea asignar e introduzca sus valores (no se permiten valores vacíos).

8. Haga clic en **Asignar**.

Temas relacionados:

- Atributos
- Variables

6.7.15. Eliminar atributos personalizados de los usuarios

Puede eliminar atributos personalizados de uno o más usuarios.

> Tenga precaución, ya que esta acción no es reversible.

Procedimiento

1. Vaya a **Usuarios.**
2. Seleccione uno o más usuarios.
3. Haga clic en **Acciones**.
4. Seleccione **Eliminar atributos personalizados**.
5. Seleccione los atributos que desea eliminar.
6. Seleccione **Quitar**.

Temas relacionados:

- Atributos
- Variables

6.7.16. Cambiar la configuración regional del usuario

Por defecto, la configuración regional del usuario está ajustada como la región del abonado. En caso necesario, puede cambiar la configuración regional para cada usuario.

Procedimiento

1. Vaya a **Usuarios.**
2. Haga clic en el nombre en pantalla del usuario.
3. Haga clic en **Editar**. Aparecerá la ventana **Autenticación obligatoria**.
4. Introduzca su contraseña de administrador y haga clic en **Autenticar**.

> cuando se introducen varias entradas incorrectas de la contraseña y si se supera el «Límite del umbral de inicio de sesión fallido» establecido en los «Ajustes de complejidad de la contraseña», la cuenta se bloqueará y se cerrará la sesión actual.

5. En el campo Configuración regional, haga clic en **Cambiar**.
6. En la ventana **Cambiar configuración regional del usuario**, seleccione la configuración regional en la lista desplegable **Cambiar configuración local a:**.
7. Haga clic en **Hecho**.
8. Haga clic en **Guardar**.

6.7.17. Editar un nombre de usuario

Cada vez que añade un usuario, el texto que introduce para la dirección de correo electrónico también queda automáticamente registrado para el nombre de usuario. En la mayoría de los casos, debe dejar el nombre de usuario predeterminado porque:

- Es obligatorio un nombre de usuario con formato de dirección de correo electrónico.
- Es conveniente utilizar la **variable** nombre de usuario en las configuraciones, aunque también se puede utilizar la dirección de correo electrónico.

El único momento en que se puede editar un nombre de usuario es en el caso poco frecuente de que se produzca un conflicto con un nombre de usuario ya existente, ya que los nombres de usuario deben ser exclusivos en todo el sistema de administración de dispositivos. Puede darse un conflicto, por ejemplo, si dos departamentos de una organización se inscriben en el sistema de administración de dispositivos.

Si se produce un conflicto de nombres de usuario:

Si no puede añadir a un usuario debido a un conflicto de nombres de usuario, introduzca un nombre de usuario diferente utilizando el formato de dirección de correo electrónico. No es necesario que la dirección de correo electrónico se corresponda con una cuenta de correo electrónico real. Por ejemplo, puede cambiar la siguiente dirección de correo electrónico:

Lruiz@miempresa.com

a

LauraRuiz@miempresa.com

Si edita el nombre de usuario, cualquier configuración que incluya el nombre de usuario como variable dejará de funcionar para este usuario. Para evitarlo, cree configuraciones alternativas que utilicen la variable del correo electrónico.

6.7.18. No participar en la obtención de datos sobre localización

Esta sección contiene los siguientes temas:

- Para dispositivos iOS
- Para dispositivos Android

Si se aplica una configuración de privacidad para habilitar la recopilación de datos sobre localización el usuario del dispositivo puede reemplazar la configuración.

Para dispositivos iOS

Los usuarios de dispositivos iOS pueden desactivar los servicios de ubicación para evitar que se envíen datos de ubicación al sistema de administración de dispositivos desde los ajustes siguientes:

Ajustes > Privacidad > Servicios de localización

Para dispositivos Android

Los usuarios de los dispositivos Android pueden desactivar el ajuste de ubicación para evitar la recopilación de datos de ubicación. La ubicación de este ajuste varía según el fabricante. A los usuarios de Android también se les pide que acepten la solicitud de datos sobre localización.

6.7.19. Información de tiempo de espera

El tiempo de inactividad del portal administrativo es de 5 a 60 minutos y el tiempo de espera es de 24 horas.

Procedimiento

1. Vaya a **Usuarios > Ajustes del usuario**.
2. Edite los ajustes predeterminados de la **Complejidad de la contraseña**.
3. En la sección Políticas sobre contraseñas, mueva el control deslizante **Tiempo de espera por inactividad** para especificar el tiempo que un usuario puede estar inactivo antes del tiempo de sesión de un portal de administración o de un portal de autoservicio. El número oscila entre 5 y 60 (minutos).
4. Haga clic en **Hecho**.

6.7.20. Cancelar las analíticas sobre el uso del sistema

Se recogen datos anónimos de diagnóstico y uso de los productos para ayudar a mejorarlos.

Si desea mantener la propiedad de los datos de uso, puede rechazar el envío de analíticas de uso del sistema.

Procedimiento

1. Haga clic en el enlace de **Datos de uso** en la parte inferior de la página del portal administrativo de Ivanti Neurons for MDM. Aparecerá la ventana **Datos de uso**.
2. Desmarque la casilla **Enviar diagnósticos y datos de uso**.
3. Haga clic en **Guardar**.

6.7.21. Registro de dispositivo por generación de PIN

Esta sección contiene los siguientes temas:

- Para usuarios únicos o múltiples desde la página de inicio de usuarios
- Para un solo usuario desde Detalles de usuario

Puede generar PIN de registro de dispositivos para los usuarios sin enviar un correo electrónico de invitación, lo que agiliza el proceso de registro del dispositivo.

Para usuarios únicos o múltiples desde la página de inicio de usuarios

1. Vaya a **Usuarios** > **Usuarios**.
2. Seleccione los usuarios para quienes desea generar un PIN de registro. Puede seleccionar uno o varios usuarios.
3. Haga clic en el botón **Acciones**.
4. Seleccione **Generar PIN** en el menú desplegable.
5. Los PIN generados se mostrarán en la columna **PIN DE REGISTRO** .
6. Para ver los PIN, haga clic en **Ver PIN**.

Para un solo usuario desde Detalles de usuario

1. Vaya a **Usuarios** > **Usuarios**.
2. Haga clic en el nombre de usuario para quien desee generar un PIN de registro para abrir los detalles del usuario.
3. En la sección Información del usuario, haga clic en **Generar PIN**.
4. Haga clic en **Ver PIN** para ver el PIN generado.

> Asegúrese de que tiene los permisos adecuados para generar PIN de registro para los usuarios. La opción Generar PIN está habilitada solo para usuarios cuyo estado de registro del dispositivo es "PIN de contraseña".

7. Dispositivos

Esta sección contiene los siguientes temas:

- Introducción a los dispositivos
- Grupos de dispositivos
- Inventario de aplicaciones
- Administrar dispositivos

7.1. Introducción a los dispositivos

Esta sección contiene los siguientes temas:

- Administrar dispositivos
- Llevar a cabo acciones en un dispositivo
- Ajustar la zona horaria de un dispositivo
- Enumerar los dispositivos por criterios
- Mostrar información detallada sobre los dispositivos
- Asigne en masa o cambie los usuarios o atributos personalizados en los dispositivos
- Exportación de dispositivos a un archivo CSV
- Buscar registros de un dispositivo

Cada entrada de la página **Dispositivos** representa un dispositivo móvil que se registró en Ivanti Neurons for MDM y muestra información importante acerca de este. La página de la lista de dispositivos muestra los dispositivos con información como:

- Nombre
- Dirección de correo electrónico
- N.º de teléfono
- SO
- Tipo de dispositivo
- Estado
- Último ingreso
- Recuento de infracciones
- Espacio
- Propietario legal (para iPad compartidos)

La dirección IP de Wi-Fi se comunica al servidor de Ivanti Neurons for MDM. Cualquier cambio en la dirección IP se comunica en cada registro. La dirección IP conforme al RGPD está disponible como opción en la página de la lista de dispositivos y en la página de detalles del dispositivo. Esta función requiere que los dispositivos se registren a través de Go 5.5 para iOS o versiones posteriores y Go 72 o versiones posteriores para Android, según lo admita Ivanti Neurons for MDM.

> A medida que se añaden nuevos campos del RGPD (como la dirección IP y la ID de eSIM) a lo largo de las versiones de Ivanti Neurons for MDM, los administradores que han configurado el RGPD tendrán que editar el perfil del RGPD si desean ocultar los nuevos campos.

El identificador de equipos (EID) se muestra como atributo de iOS cuando una lista de dispositivos se exporta al formato de hoja de cálculo (CSV). El EID y el EID móvil (MEID) (cuando están presentes) están prefijados por una cadena EID o MEID, respectivamente.

> El servidor de Ivanti Neurons for MDM no puede gestionar el procesamiento del mismo dispositivo con identificadores de diferentes clientes y registrados en distintos abonados. El servidor solamente puede gestionar la instancia donde está el mismo dispositivo con diferentes identificadores de clientes y registrados en el mismo abonado.

Administrar dispositivos

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Vaya a **Dispositivos**.
3. Seleccione uno o más dispositivos.
4. Seleccione una acción en la lista desplegable de **Acciones**.

La siguiente tabla detalla las acciones disponibles desde la página Dispositivos:

Categoría	Acción
Común	• Añadir al grupo • Desbloqueo de AppConnect> • Asignar atributos personalizados • **Asignar al usuario** • Sincronización con el estado de compatibilidad del dispositivo • Desactivar Escritorio remoto • Activar Escritorio remoto • Activar/desactivar Bluetooth • **Forzar ingreso** • **Bloquear** • Eliminar atributos personalizados • Reiniciar/apagar • Sincronización con el estado de compatibilidad del dispositivo • **Eliminar un dispositivo** • **Enviar mensaje** • Establecer propiedad • **Desbloquear** • **Borrar**
iOS	• **Asignar al propietario legal** (Solo para iPad compartidos) • Reinstalar aplicaciones del sistema iOS • Establecer zona horaria
macOS	• Establecer contraseña automática del administrador de macOS • Establecer/cambiar contraseña del firmware • Configurar/cambiar el bloqueo de recuperación
Android	• Entrar en modo kiosko • Salir del modo Pantalla completa
Windows	Secuencias de comandos y Acciones a través de Ivanti Bridge

Llevar a cabo acciones en un dispositivo

El menú Acciones (botón de elipsis) le permite llevar a cabo varias acciones en un dispositivo seleccionado.

Procedimiento

1. Haga clic en el nombre del dispositivo. Se abre la página de información del dispositivo.
2. Haga clic en Acciones (menú elipsis) para realizar una de las siguientes acciones de dispositivos:
    - Cambiar nombre del dispositivo

- Eliminar dispositivo
- Editar Pertenencia al grupo
- Activar/desactivar Bluetooth
- Secuencias de comandos y Acciones a través de Ivanti Bridge
- Extraer el registro de Ivanti Bridge
- Renunciar a la propiedad
- Solicitar registros de depuración
- Reiniciar/apagar dispositivo
- Retirar
- Establecer propiedad
- Configurar/cambiar el bloqueo de recuperación
- Borrar
- Sincronización con el estado de compatibilidad del dispositivo

Ajustar la zona horaria de un dispositivo

Aplicable a: dispositivos iOS 14.0+ y tvOS 14.0+

Esta acción no requiere servicios de localización. La acción del dispositivo de zona horaria también se muestra en la página de detalles del dispositivo. Los cambios de zona horaria realizados en el dispositivo también se reflejarán en el servidor de Ivanti Neurons for MDM.

> Esta acción del dispositivo desencadena un error si la restricción **Forzar fecha y hora automáticos** está habilitada en la **Configuración de restricciones para iOS.**

Procedimiento

1. Seleccione uno o más dispositivos.
2. Haga clic en **Acciones** > **Establecer la zona horaria** para los dispositivos seleccionados.
3. Ingrese la cadena de zona horaria con el formato de identificación de zona horaria de Olson. Por ejemplo, Pacífico/A mitad de camino.
4. Haga clic en **Establecer zona horaria**.

Enumerar los dispositivos por criterios

Puede usar la barra de navegación lateral de Filtros para buscar y ver dispositivos específicos de toda la lista de dispositivos. Utilice la lista desplegable Espacio para seleccionar todos los espacios o espacios específicos para ver los dispositivos y la información relacionada. También puede buscar dispositivos utilizando la versión de visualización o la versión del paquete. La página Dispositivos muestra tanto la versión del paquete como la versión de visualización de los dispositivos.

> Cuando se navega por la página de Grupos de dispositivos y hace clic en el número que se lista en **N.º de dispositivos** o bien, desde la página **Inventario de aplicaciones** haciendo clic en el enlace del recuento instalado en la columna **N.º instalado**, se muestra un mensaje que indica el nombre del espacio para el que se enumeran los dispositivos en la página.

Mostrar información detallada sobre los dispositivos

Haga clic en el enlace de la columna Nombre de una entrada para visualizar la página Detalles del dispositivo: la página Detalles del dispositivo contiene varias pestañas donde se organiza la siguiente información:

- **Descripción general**: en la siguiente tabla se enumeran todos los detalles que aparecen en la pestaña Descripción general:
- **Configuraciones**: muestra los detalles de las configuraciones aplicadas. Para obtener más información, consulte **Trabajar con configuraciones**

Nombre de la sección	Descripción
General	• Ubicación del dispositivo • Fabricante • Dirección MAC de Wi-Fi • Dirección WiFi-IP (dispositivos Android) • Anclado a la red - (dispositivos iOS) • Tiene batería: (solo para macOS 13.3+) • Dirección IP • Dirección IP pública: muestra la dirección IP del dispositivo para Android o ChromeOS. Si el dispositivo se conecta a una VPN o a un servidor proxy, muestra la dirección IP de la proxy WAN. • Número de modelo: (macOS 13.3+ e iOS 16.4+) • Número de serie • Número alternativo de serie (dispositivos Android): número de serie específico del fabricante aplicable a dispositivos Samsung en modo Administrador del dispositivo o Propietario del dispositivo. • Bloquear PIN: los administradores pueden bloquear remotamente un dispositivo gestionado y generar un PIN único para desbloquearlo manualmente. Seleccione **Ver** para mostrar el PIN en la página **Detalles del dispositivo** a los usuarios con privilegios de administrador. Solo compatible con dispositivos macOS. • Uso del almacenamiento - Almacenamiento utilizado (excepto Windows) y almacenamiento interno disponible en los dispositivos • Batería disponible (Android) • Estado de batería (Android): cargando, descargando, completa y no cargando • Carga restante estimada de la batería (Windows) • Tiempo de ejecución estimado de la batería (Windows) • Actualización disponible (macOS) • Nombre de la actualización disponible (macOS) • Versión de SO • Versión de compilación del SO • Versión de generación suplementaria • Suplemento SO/Versión Extra • Dispositivo Apple Silicon • Versión de firmware • Origen del dispositivo • Propietario legal • Modo multiusuario • Zona horaria

Nombre de la sección	Descripción
	• Último código de acceso de desbloqueo del dispositivo conocido • Modo de bloqueo de seguridad • Actualización del sistema (dispositivos Android) • Versión de la revisión de Zebra (dispositivos Android) • Última Id. de Hotfix (dispositivos Windows) • Última instalación de Hotfix el (dispositivos Windows) • Tipo de inscripción mediante MDM • Retorno al servicio mediante MDM (iOS 27.0+ y visionOS 27.0+)
Ajustes	• Nombre del dispositivo • Identificador del dispositivo • GUID de dispositivo • Dispositivo de la Inscripción de dispositivos (dispositivos Apple) • Inscrito en la inscripción de dispositivos (dispositivos Apple) • Inscripción de dispositivos automatizada activada • Inscrito en la Inscripción de dispositivos automatizada • Inscrito en la inscripción de usuarios (dispositivos Apple) • ID de Apple administrada registrada (dispositivos Apple) • Grupos de dispositivos • Idioma • Identificadores de dispositivos MDM • Id. del cliente del dispositivo • Versión de la aplicación del cliente • Id. de paquete de la aplicación del cliente • Registrado con el cliente • Identificadores de dispositivos EAS • Bloqueo de activación habilitado • Gestión declarativa de Apple activada • Aplicación DDM de Apple aplicación habilitada • Código de derivación del Bloqueo de activación • Condiciones del servicio • Propiedad • Cuenta de iTunes activa • Servicio de localización de dispositivo activado • En cuarentena

Nombre de la sección	Descripción

	• Sentry bloqueado
	• Acceso bloqueado
	• Medida de cumplimiento bloqueada
	• Compatible con APNS
	• Modo supervisado (dispositivos iOS y macOS): identifica un dispositivo supervisado. El dispositivo mantiene el control directo del equipo informático. El modo supervisado permite funciones adicionales de los dispositivos (por ejemplo, implementaciones de servicios de campo, dispositivos de puntos de venta al por menor), dispositivos «en préstamo» utilizados en la hostelería y servicios, y dispositivos compartidos entre los alumnos de un aula de laboratorio.
	• Borrar PIN: haga clic en **Ver** para mostrar el PIN.
	• Usuario administrador de macOS gestionado (dispositivos macOS)
	• Contraseña de administrador local de macOS (dispositivos macOS): seleccione **Ver** para consultar la información de **Contraseña de administrador**, la **Última rotación de la contraseña**, la **Próxima rotación** y la **Causa** relacionadas con dispositivos inscritos y gestionados mediante Registro automatizado de dispositivos.
	Después de que el administrador visualice la contraseña, podría transcurrir hasta una hora adicional (próxima comprobación) para que la contraseña se rote desde la hora indicada en **Próxima rotación**.
	• Estado del cifrado del dispositivo (dispositivos macOS)
	  ◦ Cifrado de FileVault habilitado
	  ◦ Clave de recuperación personal utilizada
	  ◦ Clave de recuperación institucional utilizada
	• Token de Bootstrap disponible
	• Protección de la integridad del sistema habilitada
	• Contraseña del firmware
	  ◦ Contraseña
	  ◦ Cambio pendiente
	  ◦ Estado del comando
	  ◦ Permitir la opción ROM
	• Bloqueo de recuperación
	  ◦ Contraseña
	  ◦ Bloqueo de recuperación habilitado
	• Secuencias a través de Mobile@Work para macOS
	• Detalles de los ajustes de cortafuegos (dispositivos macOS)
	  ◦ Firewall habilitado
	  ◦ Bloquear todo lo entrante
	  ◦ Modo sigiloso

Nombre de la sección	Descripción
	• Estado del cortafuegos de la aplicación (dispositivos macOS) • Estado del firewall (dispositivos Windows) • Última copia de seguridad en iCloud (dispositivos iOS) • Período de gracia del bloqueo del código de acceso (dispositivos iOS) • Id. de Android • Nivel de revisión de la seguridad de Android (dispositivos Android) • Modo kiosco (dispositivos Android) • Tipo de certificación SafetyNet de Android (dispositivos Android) • Compatible con Android Enterprise (dispositivos Android) • Habilitado para la versión corporativa de Android (dispositivos Android) • Compatible con Samsung SAFE (dispositivos Android) • Dispositivos Android administrados en el trabajo (Propietario del dispositivo) habilitados • Perfil de trabajo de Android en el Dispositivo propiedad de la empresa habilitado • Estado nativo de antiphishing • Estado de antiphishing • Estado de la VPN de antiphishing • Dispositivo administrado de Android con perfil profesional • Se habilitó el bloqueo del Perfil de trabajo de Android en el Dispositivo propiedad de la empresa • Help@Work disponible • Compatible con Zebra • Estado de Secure Apps • Estado del cifrado de Secure Apps • Modo de cifrado de Secure Apps • Compatible con FCM • Estado de activación del MTD
Protección de la información de Windows (dispositivos Windows)	• WIP • Bloqueador de aplicaciones configurado • Ajustes de EDP obligatorios
Telefonía	**Suscripciones a servicios para dispositivos** • Teléfono • Tecnología de telefonía móvil • IMSI • ICCID

Nombre de la sección	Descripción
	• IMEI • IMEI 2 - (solo en dispositivos Android con un puerto SIM doble. Aplicable a Android 8.0 o posterior) • MEID • Ubicación del dispositivo • Operador • MCC de origen • MNC de origen • Nombre del país actual • Nombre del país de origen • Tecnología de telefonía móvil • Itinerancia • Operador actual • MMC actual • MNC actual • Itinerancia de datos • Itinerancia de voz • EID - (aplicable a dispositivos Android compatibles) **Suscripciones al servicio SIM** (aplicable a dispositivos iOS compatibles) En los dispositivos iOS compatibles estas propiedades se muestran para varias suscripciones de servicio activo eSIM. • Versión de ajuste del operador • Red de ajuste del operador • MMC actual • MNC actual • EID • ICCID • IMEI • Datos preferidos • Voz preferida • Etiqueta • ID de etiqueta • Número de teléfono • Ranura SIM • En itinerancia • Abonado Red portadora **Suscripciones al servicio SIM** (aplicable a dispositivos Android compatibles)

Nombre de la sección	Descripción
	En los dispositivos Android compatibles, estas propiedades se muestran para varias suscripciones de servicio activas. • Versión de ajuste del operador • MMC actual • MNC actual • ICCID • Datos preferidos • Voz preferida • Id de suscripción • Número de teléfono • Ranura SIM • Integrado • Gestionado
Cumplimiento de los dispositivos Azure	• Identificador del dispositivo Azure • Estado de cumplimiento del dispositivo Azure • Código de estado del cliente de Azure • Hora del informe de cumplimiento del dispositivo Azure • UPN del usuario del dispositivo de Azure Intune
Conformidad de dispositivos de Google BeyondCorp	• Identificador del dispositivo • Estado del compatibilidad • Hora del informe de compatibilidad • Usuario
Información de batería	• Nivel de batería: muestra el nivel de carga actual de la batería, tal y como ha informado el SO de Android • Condición de la batería: como han informado los dispositivos Android, Mac e iOS. • Estado de carga de la batería: como ha informado SO de Android • Porcentaje de integridad de la batería (específico de OEM): la integridad de la batería en porcentaje para los fabricantes de los dispositivos compatibles, como Zebra • Fecha de fabricación de la batería (OEM): la fecha de fabricación de la batería de los fabricantes de dispositivos compatibles, como Zebra • Ciclos de carga de la batería (OEM): número de ciclos completados en total para los fabricantes de dispositivos compatibles, como Zebra
Estado de los componentes del dispositivo	• **Banda base**: indica el estado de la banda base del dispositivo. • **Cámara**: indica el estado de la cámara del dispositivo. • **Pantalla**: indica el estado de la pantalla del dispositivo.

Nombre de la sección	Descripción
(dispositivos supervisados iOS 27.0+ y macOS 27.0+)	• **Face id**: indica el estado de Face id del dispositivo. • **Comunicación de campo cercano**: indica el estado de NFC del dispositivo. • **Touch id**: indica el estado de Touch id del dispositivo. • **Banda ultraancha**: indica el estado de la banda ultraancha del dispositivo.

- **Aplicaciones instaladas**: Muestra los detalles de las aplicaciones que están instaladas en el dispositivo. La fecha de instalación de la versión actual de la aplicación instalada se muestra en la columna **Fecha de la aplicación notificada** . Busque las aplicaciones instaladas para el dispositivo de la siguiente manera:
- Nombre de la aplicación
- ID de conjunto o paquete

> La fecha de instalación de las aplicaciones de los dispositivos que salen de la cuarentena es la fecha en que el dispositivo se retira de la cuarentena.

> En el caso de los dispositivos Android Enterprise, también puedes ver los detalles de uso de las aplicaciones instaladas ordenadas por Día, Semana, Mes o Año. Para ver esta información, debe haber seleccionado la opción **Activar la recopilación de datos de uso de la aplicación** disponible en la sección **Configuración** , y luego puede seleccionar las opciones **Uso de la aplicación: Día**, **Uso de la aplicación: Semana**, **Uso de la aplicación: Mes**, **Uso de la aplicación: Año** para ver los detalles de uso de la aplicación.

- **Aplicaciones disponibles**: muestra los detalles de las aplicaciones que están disponibles para el dispositivo. Buscar a las aplicaciones disponibles para el dispositivo de la siguiente manera:
- Nombre de la aplicación
- ID de conjunto o paquete

En la columna **Configuración de aplicaciones**, al seleccionar **Nombre de configuración**, se le dirigirá a la pestaña **Configuración de aplicaciones** del catálogo de aplicaciones para que revise las opciones de configuración de la aplicación. Si es necesario, puede modificar la configuración de la aplicación para el dispositivo en la página **Resumen de configuración de la aplicación** . Para obtener más información sobre cómo configurar una aplicación, consulte Configuración de aplicaciones.

En la columna **Configuración de aplicaciones**, al seleccionar **Nombre de configuración**, se le dirigirá a la pestaña **Configuración de aplicaciones** del catálogo de aplicaciones para que revise las opciones de configuración de la aplicación. Si es necesario, puede modificar la configuración de la aplicación para el dispositivo en la página **Resumen de configuración de la aplicación** . Para obtener más información sobre cómo configurar una aplicación, consulte Configuración de aplicaciones.

> Asegúrese de recordar el nombre y el tipo de la configuración de la aplicación específica para el dispositivo asignado en la página **Configuración de aplicaciones**.

> La columna **Estado** indica el estado de instalación de la aplicación en el dispositivo. El estado de instalación de la aplicación solo se captura para las aplicaciones gestionadas. El estado de instalación de las aplicaciones no gestionadas se muestra como No instalado. Debe convertir la aplicación en Gestionada para ver el estado correcto de la instalación.

- **Aplicaciones de AppConnect**: información de las aplicaciones AppConnect instaladas.
- **Políticas**: detalles de las {{políticas}} aplicadas . Para los dispositivos en riesgo, compruebe el motivo de la infracción en la columna Infracción. Si se accedió a la raíz del dispositivo, el sistema mostrará el motivo en la columna **Infracción**:

Prioridad (1 = la más alta)	Infracción
1	Plugin en riesgo
2	Cliente manipulado
3	Fabricante de dispositivos desconocido: desconocido
4	Carpeta sospechosa detectada: [ruta]
5	Se ha encontrado un binario sospechoso en: [ruta]
6	La carpeta /data es navegable o la carpeta /data/data es navegable
7	Se encontró /system/app/Superuser.apk
8	El administrador del paquete ha sido vulnerado
9	Se ha encontrado una aplicación sospechosa: [package]

- **Certificados**: detalles de los certificados instalados.
  Para ver el uso del certificado, vea la columna Tipo de uso. Si el certificado es específico para el dispositivo, mostrará el tipo de uso como 'dispositivo'. Si el certificado es específico para el usuario, mostrará el tipo de uso como 'usuario'.
- **Sentry** - información sobre Sentry (asociaciones ActiveSync)
- **Atributos** - atributos personalizados y atributos del dispositivo
- **Usuarios**: muestra la lista de usuarios activos para el dispositivo MacOS supervisado.

> La pestaña **Usuarios** se ha mejorado y se muestra la identificación de Apple administrado como un hipervínculo, y al hacer clic se redirige a la página de detalles de la cuenta de usuario en el iPad compartido.

- **Registros**: consulte y personalice los filtros de los dispositivos. Puede hacer lo siguiente desde Filtros:
  - Seleccione el nombre de la acción para filtrar los dispositivos en función de las acciones de la aplicación.
  - Seleccione Estado.
  - Especifique la Fecha de inicio y la Fecha final.
- **Hardware** - detalles del inventario de hardware (sistema, placa base, BIOS, disco duro, CD ROM, procesador y memoria física)

Asigne en masa o cambie los usuarios o atributos personalizados en los dispositivos

Puede utilizar la función Asignación en masa a través del icono de carga para cargar un archivo CSV para asignar o cambiar los usuarios y/o los atributos personalizados en los dispositivos en masa.

Procedimiento

1. Desde la página Dispositivos, haga clic en el icono **Asignación en masa a través de la carga** (junto al botón Acciones).
2. (Opcional) Haga clic en **Descargar plantilla** para guardar un archivo de plantilla CSV que puede editar y cargar.

3. Cuando el archivo CSV esté listo, haga clic en **Elegir archivo** para explorar la localización del archivo CSV o arrastre y suelte el archivo CSV en la sección Datos del archivo.
4. Seleccione una de las siguientes opciones:
    - **Forzar la asignación (sobrescritura) de todos los atributos aunque se encuentre algún valor existente.**
    - **Sobrescribir solo si el valor está vacío y omitir atributos con valores existentes.**

Haga clic en **Cargar**.

Exportación de dispositivos a un archivo CSV

Puede exportar la información del dispositivo de un dispositivo específico mediante la opción **Exportar a CSV** desde la página **Dispositivos**.

Procedimiento

1. Vaya a **Dispositivos**.
2. Seleccione todos o múltiples espacios para ver la información relacionada con espacios específicos.
3. Haga clic en el enlace del número de dispositivos. Se muestra la página Lista de dispositivos relacionada con el espacio seleccionado.
4. Haga clic en la opción **Exportar a CSV** para exportar la lista de dispositivos y detalles relacionados a un archivo CSV. Aparece un mensaje emergente que informa de que el informe de exportación tardará un tiempo en procesarse. Espere a que se complete la solicitud para enviar otra solicitud. Cuando el informe está listo, recibirá un mensaje que le indicará que debe descargar o eliminar el informe.
5. Haga clic en **Descargar**. Usted también recibirá un correo electrónico con un enlace para descargar el informe.
6. (Opcional) Haga clic en **Eliminar** para eliminar el informe.

Buscar registros de un dispositivo

Procedimiento

1. Vaya a **Dispositivos** > **Dispositivos**, haga clic en el enlace de la columna **Nombre** de una entrada.
2. Haga clic en la pestaña **Registros**.
3. Utilice los filtros Acción, Estado, Fecha de inicio y Fecha de fin para restringir los dispositivos mostrados. Puede hacer lo siguiente desde Filtros:
    1. Seleccione el nombre de la acción para filtrar los dispositivos en función de las acciones de la aplicación.
    2. Seleccione Estado.
    3. Especifique la Fecha de inicio y la Fecha final.
4. La columna Detalles del dispositivo muestra el estado de la aplicación de la siguiente manera:
   Para todos los dispositivos, el estado muestra los siguientes detalles:
    - Nombre de la aplicación, versión de la aplicación, paquete o ID del paquete
    - Estado de la instalación
    - Cualquier error y la razón del error
      Por ejemplo - appOrConfigName=Nombre:<app name>;Identificador=<bundleid>;iTunesStoreId:<itunesid>;Estado:<status or error reason from Apple>versión: <app version>

Para los dispositivos Windows, el estado muestra los siguientes detalles:

- Incluye el ID del paquete, el estado y los errores.
  Por ejemplo:
- Para el tipo: inventario y estado de la aplicación: reconocer. Muestra: appType
- Para el tipo: inventario y estado de la aplicación: envío. No muestra nada
- Para el tipo: instalación/desinstalación y el estado: correcto/incorrecto/envío: muestra Incluir ID de paquete o ID de paquete, estado, nombre, versión y errores.

Si no puede ver la página **Dispositivos**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración de dispositivos
- Dispositivo de solo lectura

7.2. Grupos de dispositivos

Esta sección contiene los siguientes temas:

- Añadir un grupo de dispositivos
- Eliminar un grupo de dispositivos
- Exportación de dispositivos a un archivo CSV
- Asignar atributos personalizados a grupos de dispositivo

En la página **Grupos de dispositivos**, puede crear listas de dispositivos que desee tratar de la misma manera. Puede definir y asignar políticas y configuraciones en los grupos de dispositivos. Los siguientes grupos son los grupos de dispositivos predeterminados creados por Ivanti Neurons for MDM:

- Todos los dispositivos
- Dispositivos Android
- Dispositivos con Android Enterprise
- Dispositivos iOS
- Tipo de dispositivo (Apple)
- Dispositivos tvOS
- Dispositivos macOS
- Dispositivos de visionOS
- Dispositivos watchOS
- Dispositivos Windows

Los detalles de las aplicaciones asignadas a un grupo de dispositivos concreto se muestran en la pestaña **Aplicaciones** para el grupo de dispositivos específico.

Añadir un grupo de dispositivos

> Agregar un grupo de dispositivos no es aplicable a grupos de usuarios dinámicos.

Según el tipo de licencia que tenga, puede agregar un nuevo grupo de dispositivos basado en reglas para identificar los dispositivos con los criterios específicos. Los dispositivos que coinciden con las reglas se muestran bajo de la sección del generador de reglas. Las reglas se pueden anidar juntas utilizando las opciones CUALQUIERA (O) o TODOS (Y). Las regla se pueden crear con los operadores siguientes:

- comienza con
- termina con
- contiene
- no contiene
- no comienza con
- no termina con
- es menor que

- es mayor que
- se encuentra en el intervalo
- es igual a
- no es igual a
- no está en blanco
- está en blanco

El Ivanti Neurons for MDM administrador muestra un número de grupos de usuarios duplicados y el número correspondiente de GUID para identificar los grupos duplicados, cuando se selecciona el atributo Nombre del grupo de usuarios en al generador de reglas. Además, una tabla bajo esta regla muestra la lista de los grupos de usuarios duplicados y sus detalles, como el Nombre del Grupo de Usuarios, el GUID, la Fuente y el nombre distinguido (DN).

Licencia Bronze:

Las funciones pueden identificar dispositivos siguiendo los siguientes criterios:

- Tipo de dispositivo
- SO - el sistema operativo (prerrellenado)
- Versión de SO
- SO con versión
- Grupo de usuarios

Licencia Silver:

Las funciones pueden identificar dispositivos siguiendo los siguientes criterios:

- Entra ID Inscrito
- Número alternativo de serie (Solo Android: aplicable a dispositivos Samsung en modo Administrador del dispositivo o Propietario del dispositivo)
- Dispositivo Android dedicado
- Compatible con Android Enterprise
- Dispositivo administrado de Android con perfil profesional
- Tipo de certificación SafetyNet de Android
- Android for Work habilitado
- Nivel de revisión de la seguridad de Android (dispositivos Android)
- Dispositivos Android administrados en el trabajo (Propietario del dispositivo) habilitados
- Perfil de Android for Work habilitado
- Perfil de trabajo de Android en el Dispositivo propiedad de la empresa habilitado
- Estado nativo de antiphishing
- Estado de antiphishing
- Estado de la VPN de antiphishing
- Preparado para APNS
- Dispositivo Apple Silicon
- Inscripción de dispositivos automatizada activada

- Inscrito en la Inscripción de dispositivos automatizada
- Identificador del dispositivo Azure
- Estado de cumplimiento del dispositivo Azure
- Código de estado del cliente de Azure
- Hora del informe de cumplimiento del dispositivo Azure
- Estado operativo de la banda base
- Cifrado de BitLocker
- Sentry bloqueado
- Acceso bloqueado
- Token de Bootstrap disponible
- Tipo de aprovisionamiento masivo (configurador de Apple o ninguno)
- Operador
- Estado operativo de la cámara
- Último ingreso del cliente
- Registrado con el cliente
- Cumplimiento
- Medida de cumplimiento bloqueada
- Nombre del país actual (seleccione el nombre del país actual de la lista desplegable)
- MMC actual
- MNC actual
- Atributo personalizado del dispositivo
- Atributo personalizado de LDAP
- Atributo personalizado del usuario
- Itinerancia de datos
- Nombre del dispositivo
- Dispositivo registrado
- Origen del dispositivo
- Tipo de dispositivo
- Nombre en pantalla
- Estado operativo de la pantalla
- Cifrado habilitado
- Estado operativo de Face ID
- Particiones del disco duro
- Nombre del país de origen (seleccione el nombre del país de origen de la lista desplegable)
- MCC de origen
- MNC de inicio
- IMEI

- IMEI2 (solo en dispositivos Android con doble puerto SIM y aplicable para dispositivos Android 8.0 o superior)
- Clave de recuperación institucional habilitada
- Dirección IP
- Modo pantalla completa
- Último ingreso
- Solo MAM
- Fabricante
- Tipo de inscripción mediante MDM
- Retorno al servicio mediante MDM (iOS 27.0+ y visionOS 27.0+)
- Modo multiusuario (iOS 27.0+)
- Estado de activación del MTD
- Estado operativo de NFC
- SO
- Versión de compilación del sistema operativo
- Edición de SO
- Versión de SO
- SO con versión
- Propiedad
- N.º de teléfono
- Dirección IP pública (dispositivos Android o ChromeOS)
- Clave de recuperación personal habilitada
- En cuarentena
- Bloqueo de recuperación habilitado
- Itinerancia
- Estado de Secure Apps
- Modo de bloqueo de seguridad
- Número de serie
- Estado
- Supervisado
- Versión del sistema
- Capacidad total del dispositivo
- Memoria total MB
- Versión de TPM
- Estado operativo de Touch ID
- Desbloquear token disponible (iOS)
- Inscripción de usuarios activada
- Grupo de usuarios

- Estado operativo de la radio de banda ultraancha
- Itinerancia de voz
- Clave de recuperación personal de macOS en custodia
- Tipo de clave de recuperación de macOS

Procedimiento

1. Haga clic en **Añadir**.
2. Introduzca un nombre para el grupo.
3. Introduzca una descripción opcional para el grupo.
4. Seleccione el tipo de grupo de dispositivos que desea crear:
   - **Gestionado dinámicamente**: Utiliza reglas para definir qué dispositivos están en el grupo.
     - **Cargar desde búsqueda avanzada**: seleccione esta opción para acceder a una biblioteca de búsquedas guardadas. Al elegir una consulta, se completarán automáticamente el nombre del grupo de dispositivos y los criterios de la regla según la búsqueda seleccionada.

     > Puede crear y guardar estas consultas desde **Dispositivos** > **Dispositivos** > **Búsqueda avanzada**. Todas las consultas guardadas allí estarán disponibles automáticamente para su carga.

   Gestionado manualmente: Introduzca cada usuario cuyos dispositivos deben incluirse en el grupo.
5. Para grupos administrados dinámicamente:
   1. Cree una regla que defina el grupo.
   2. **Ejemplo**: SO es iOS
      Haga clic en **+** para crear reglas adicionales, si fuera necesario.
   3. **Ejemplo**: El dispositivo es el iPhone 5S
      Haga clic en **Cualquiera** si los dispositivos tienen que cumplir al menos una de las reglas.
   4. Haga clic en **Todas** si los dispositivos tienen que cumplir todas las reglas.
6. Para grupos administrados manualmente:
   1. Escriba el nombre de un usuario cuyo dispositivo desee añadir.
   2. Seleccione el dispositivo de la lista que se muestra.
   3. Repita los pasos «a» y «b» hasta que todos los dispositivos aparezcan en la lista.

Haga clic en **Guardar**.

Eliminar un grupo de dispositivos

Procedimiento

1. Ir a **Dispositivos**>**Grupos de dispositivos**.
2. Marque la casilla del grupo de dispositivos que desea eliminar.
3. Haga clic en **Eliminar Grupo de dispositivos**.

Exportación de dispositivos a un archivo CSV

Puede exportar la información del dispositivo de un grupo de dispositivos específico mediante la opción **Exportar a CSV** desde la página **Grupos de dispositivos**.

Procedimiento

1. Ir a **Dispositivos**>**Grupos de dispositivos**.
2. Seleccione todos o múltiples espacios para ver la información relacionada con espacios específicos.
3. Haga clic en el enlace del número de grupos de dispositivos. Se muestra la página Lista de dispositivos relacionada con el espacio seleccionado.
4. Haga clic en la opción **Exportar a CSV** para exportar la lista de dispositivos y detalles relacionados a un archivo CSV. Aparece un mensaje emergente que informa de que el informe de exportación tardará un tiempo en procesarse. Espere a que se complete la solicitud para enviar otra solicitud.
5. Haga clic en **Descargar**. Recibirá un correo electrónico con un enlace para descargar el informe.
6. (Opcional) Haga clic en **Eliminar** para eliminar el informe.

Si no puede ver la página **Grupos de dispositivos**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**

- Administración de dispositivos
- Dispositivo de solo lectura

Asignar atributos personalizados a grupos de dispositivo

Ahora los administradores pueden asignar atributos personalizados directamente a grupos de dispositivo. Cualquier dispositivo que se convierta en miembro de un grupo de dispositivos hereda de forma automática los valores de atributo personalizados configurados, eliminando la necesidad de asignar manualmente atributos a dispositivos individuales después de la inscripción. Utilice grupos de dispositivo para asignar valores de atributos personalizados a los dispositivos que se convierten en miembros del grupo.

Procedimiento

1. Ir a **Dispositivos**>**Grupos de dispositivos**.
2. Seleccione un grupo existente o cree uno.
3. En la página Detalles del grupo de dispositivos, haga clic en **Atributos**.
4. Haga clic en **Agregar nuevo**.
5. Elija el atributo personalizado y especifique el valor requerido.

7.3. Dispositivos no administrados

Esta sección contiene los siguientes temas:

- Bloquear un dispositivo
- Desbloquear un dispositivo
- Borrar un dispositivo de la lista de dispositivos

Licencia: Silver

Si ha configurado el control de acceso al correo electrónico Sentry, cualquier dispositivo no registrado que acceda a su sistema de correo electrónico será considerado un dispositivo no administrado. Usted define si los dispositivos no administrados pueden tener acceso al correo electrónico de forma predeterminada al configurar un Sentry. A continuación, puede permitir o bloquear manualmente el acceso al correo electrónico para estos dispositivos.

> La página Dispositivos no administrados se actualiza cada cinco minutos. Por lo tanto, los cambios en la administración no se ven reflejados inmediatamente.

Bloquear un dispositivo

Procedimiento

1. Seleccione el dispositivo.
2. Seleccione **Acciones > Bloquear.**

El dispositivo se mantiene bloqueado hasta que seleccione **Acciones > Permitir** o **Acciones > Eliminar**.

Desbloquear un dispositivo

Procedimiento

1. Seleccione el dispositivo.
2. Seleccione **Acciones > Permitir.**

El dispositivo sigue teniendo acceso al correo electrónico hasta que seleccione **Acciones > Bloquear** o **Acciones > Eliminar**.

Borrar un dispositivo de la lista de dispositivos

Procedimiento

1. Seleccione el dispositivo.
2. Seleccione **Acciones > Eliminar**.

La próxima vez que el dispositivo intente acceder a su sistema de correo electrónico, volverá a aparecer en esta lista y usted tendrá que repetir cualquier acción de Bloquear o Permitir que haya aplicado previamente en el dispositivo.

7.4. Inventario de aplicaciones

Esta sección contiene los siguientes temas:

- Filtrar cómo se muestran las aplicaciones
- Mostrar los dispositivos instalados para una aplicación
- Visualizar la lista de aplicaciones
- Visualización de las aplicaciones Win32 o Win32 Store instaladas en un dispositivo
- Creación de un permiso de vista personalizada
- Exportar un inventario de aplicaciones

El inventario de aplicaciones es la lista de aplicaciones detectadas en los dispositivos inscritos. Como administrador, puede usar esta página para obtener información sobre las aplicaciones que se están utilizando en los dispositivos inscritos. Puede responder preguntas como las siguientes:

- ¿Qué aplicaciones son las más populares?
- ¿Los dispositivos iOS obtienen las aplicaciones directamente desde la App Store?
- ¿Cuántos usuarios de Android han descargado una {{aplicación interna}} opcional?
- ¿Cuántos dispositivos están utilizando una versión obsoleta de una aplicación?

Filtrar cómo se muestran las aplicaciones

Al mostrar la página **Dispositivos > Inventario de aplicaciones**, aparecen enumeradas todas las aplicaciones. Para reducir esta lista a ciertas aplicaciones, utilice los filtros (panel izquierdo). Por ejemplo, para limitar la lista y que aparezcan solo las aplicaciones privadas de Google Play, seleccione **Privadas** en la sección **Origen**.

Se puede ver el inventario de aplicaciones en todos o en varios dispositivos espaciales seleccionando varios espacios de la lista desplegable. Al pasar el cursor sobre las aplicaciones mostradas, se muestran los recuentos de los dispositivos. Se puede hacer clic en el recuento de una aplicación para que muestre todos los dispositivos que contienen la aplicación. Cada registro del inventario de la aplicación se agrupará por espacios.

Puede buscar mediante el nombre de la aplicación o el ID del paquete.

Si ha seleccionado varios espacios, al pasar el ratón por el valor **Total** de la columna **# Instalado**, se muestra el número de instalaciones por espacio de dispositivo.

Mostrar los dispositivos instalados para una aplicación

Haga clic en el número **Gestionado**, **No gestionado** o **Total** que aparece en la columna **# Instalado**.

Visualizar la lista de aplicaciones

Haga clic en el **n.º solicitado** que hay junto a la aplicación en el inventario de aplicaciones para ver los dispositivos que solicitaron la aplicación. Esto solo es aplicable a dispositivos solo MAM.

Visualización de las aplicaciones Win32 o Win32 Store instaladas en un dispositivo

El inventario de aplicaciones muestra las aplicaciones Win32 o Win32 Store en un dispositivo si la **configuración de privacidad** para ese dispositivo permite la recopilación de información para todas las aplicaciones del mismo. Puede configurar la política de privacidad del dispositivo.

Procedimiento

1. Determine qué configuración de privacidad es aplicable al dispositivo deseado siguiendo las indicaciones de **Dispositivos**.
2. Vaya a **Configuraciones**.
3. Para la configuración de privacidad que anotó en el paso 1:
    1. Seleccione la configuración.
    2. Haga clic en Editar.
    3. En **Recopilar inventario de aplicaciones,** seleccione **Para todas las aplicaciones del dispositivo**.
    4. Haga clic en **Hecho**.

> El CSP Win32AppInventory devuelve la lista de todas las aplicaciones Win32 y Win32 Store instaladas en el dispositivo cada 24 horas tras la ejecución de los análisis de inventario en el dispositivo.

Creación de un permiso de vista personalizada

Puede especificar permisos de vista personalizados para los usuarios.

Procedimiento

1. Vaya a **Administrador**.
2. Vaya a **Administración de funciones**.
3. Haga clic en **Añadir función personalizada**.
4. Seleccione la opción **Función específica para espacios** .
5. Introduzca el nombre de usuario en el campo **Nombre**.
6. En el menú **Dispositivos**, haga clic en **Inventario de aplicaciones**.
7. Seleccione la casilla **Vista**.
8. En el menú **Dispositivos**, haga clic en **Acciones del dispositivo**.
9. Haga clic en **Guardar**.
10. Vaya a **Usuarios** en el menú principal.
11. Haga clic en el nuevo usuario que ha creado.
12. Haga clic en **Asignar funciones**.
13. Seleccione la casilla **aplicación | Específica para el espacio** y haga clic en **Siguiente**.
14. La página **Resumen** mostrará los permisos asignados a la función creada.
15. Haga clic en **Hecho**.
16. Inicie la sesión como nuevo usuario.
17. Haga clic en **Dispositivos** en el menú principal.
18. Haga clic en **Inventario de aplicaciones**.
19. La página **Inventario de aplicaciones** mostrará ahora solo las aplicaciones permitidas para el usuario.

Exportar un inventario de aplicaciones

Como administrador, puede solicitar informes del Inventario de aplicaciones mediante la opción **Exportar a CSV**.

Procedimiento

1. Vaya a **Dispositivos > Inventario de aplicaciones**.
2. Seleccione un inventario de la lista.
3. Haga clic en **Exportar a CSV**.
4. Seleccione una de las siguientes opciones:

- **Exportar aplicaciones a CSV** para exportar todas las aplicaciones del inventario de aplicaciones.
- **Exportar dispositivos a CSV** para exportar una aplicación específica según la tabla siguiente:

Opción	Descripción
ID de paquete	Introduzca el ID de paquete de la aplicación.
¿Desea exportar	Seleccione una de las siguientes opciones: • Total instalado • Administrado • Sin administrar • Solicitado (para dispositivos MAM-Only)

5. Haga clic en **Exportar**.

El administrador verá una ventana emergente que le informará de que el informe exportado tardará un tiempo en procesarse. Una vez enviada la solicitud, el administrador debe esperar a que se complete la solicitud para enviar otra solicitud. Cuando el informe está listo, el administrador recibirá un mensaje para que descargue o elimine el informe que se ha generado. El administrador también recibirá un correo electrónico con un enlace para descargar el informe.

Si no puede ver la página **Inventario de aplicaciones**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración de dispositivos
- Dispositivo solo lectura

7.5. Administrar dispositivos

Esta sección contiene los siguientes temas:

- Desplegar dispositivos de Windows
- Configurar Apple Remote Desktop en dispositivos macOS
- Registro de dispositivos (iOS, macOS y Android)
- Registro de dispositivos (PC con Windows 10+ y Microsoft HoloLens 2)
- Inscripción de paquete de aprovisionamiento con PIN
- Uso de la Inscripción en masa para dispositivos Windows
- Cambiar ajustes del código de acceso
- Cambiar nombre del dispositivo
- Encontrar y filtrar dispositivos
- Uso del modo Propietario del dispositivo
- Dispositivo administrado con perfil profesional
- Uso de la inscripción en masa para Android
- Inscripción masiva mediante carga de archivos CSV
- Uso de la inscripción móvil de Samsung Knox
- Inscribir dispositivos de Oculus
- Activar Bluetooth en un dispositivo
- Programar actualización de iOS
- Reinstalar aplicaciones del sistema iOS
- Asignar un dispositivo a un nuevo usuario
- Reasignar un dispositivo Android
- Forzar el ingreso de un dispositivo
- Encontrar un dispositivo
- Bloquear un dispositivo
- Administrar dispositivos en el modo Perdido de Apple
- Solicitar registros de depuración
- Retirar un dispositivo
- Renuncia de la propiedad de un dispositivo
- Borrar un dispositivo
- Eliminar dispositivos
- Desbloquear un dispositivo
- Reiniciar o apagar dispositivos
- Borrar la contraseña de las restricciones (solo iOS)
- Eliminar la asociación de Sentry de un dispositivo
- Asignar atributos personalizados a los dispositivos

- Eliminar atributos personalizados de los dispositivos
- Sincronizar y obtener comentarios de aplicaciones
- Establecer la contraseña del firmware
- Volver a emitir una nueva clave de recuperación personal
- Configurar o cambiar el bloqueo de recuperación
- Administración de acceso de Apple
- Inscripción de políticas de grupos

7.5.1. Despliegue de dispositivos Apple

Ivanti Neurons for MDM es compatible con la gestión de todos los dispositivos de Apple. Se trata de una solución integral para aprovisionar, gestionar, actualizar y proteger su flota, de manera que el usuario final vive la mejor experiencia de uso.

Esta sección contiene los siguientes temas:

- Instalación del certificado MDM de Apple
- Inscripción de dispositivos Apple
- Ivanti Go para clientes de iOS
- Gestión de aplicaciones para dispositivos Apple
- Administrar configuraciones
- Administración de actualizaciones de software
- Configuración de dispositivos de iOS/iPadOS
- Configuración de dispositivos de watchOS
- Acciones de dispositivo compatibles con dispositivos watchOS
- Configuración de dispositivos visionOS
- Acciones de dispositivo compatibles con dispositivos visionOS
- Configuración de dispositivos de macOS
- Configuración de dispositivos TvOS
- Soporte para la gestión de dispositivos declarativos (DDM)

Instalación del certificado MDM de Apple

Para administrar dispositivos de Apple, empiece por solicitar e instalar un certificado de Apple MDM para administrar dispositivos iOS. Renueve el certificado MDM de Apple una vez al año. (La cuenta de Apple que se usó para crear el certificado recibe una notificación de la web de Apple cuando se acerca la fecha de caducidad). Utilice la página Certificado de MDM para agregar o renovar este certificado.

Siga los pasos descritos en Instalar certificado MDM

Inscripción de dispositivos Apple

Puede elegir cualquiera de los métodos siguientes para inscribir dispositivos:

- Inscripción de dispositivos automatizada
- Director de la escuela de Apple
- Configurador de Apple

Ivanti Go para clientes de iOS

El siguiente paso es seleccionar el tipo de inscripción que su empresa permite para los dispositivos. Ivanti Neurons for MDM actualmente es compatible con:

- Registro de dispositivos (iOS, macOS y Android)

- Inscripción de usuarios en el Apple Business Manager
- Inscripción de Usuario generada por cuenta
- Ajustes (Apple)

Gestión de aplicaciones para dispositivos Apple

La página Catálogo de aplicaciones de Ivanti Neurons for MDM sirve como interfaz para que los administradores rijan su catálogo de aplicaciones de manera eficaz. Esta función abarca la organización de las aplicaciones móviles disponibles para los usuarios finales, y abarca tanto las tiendas de aplicaciones públicas como las destinadas a la distribución a través de Ivanti Neurons for MDM.

Aplicaciones compatibles:

La página Catálogo de aplicaciones agrega varios tipos de aplicaciones, incluidas aplicaciones de la AppStore pública, aplicaciones personalizadas, aplicaciones desarrolladas internamente, aplicaciones habilitadas para AppConnect, GoClient para iOS y M@W para macOS, de manera que agilizan el proceso de importación para su posterior configuración y distribución.

En los dispositivos que funcionan con configuraciones de solo gestión de aplicaciones móviles (MAM), se pide a los usuarios de iOS que seleccionen un certificado de autenticación al acceder al catálogo de aplicaciones. Este paso de autenticación es crucial para garantizar el acceso a las aplicaciones de la lista y ajustarse a unas prácticas de seguridad sólidas.

> Los MacBooks con chipset M1 de Apple ofrecen compatibilidad especializada con las aplicaciones VPP para iPhone y iPad dentro de [Su producto de software]. En concreto, únicamente los administradores tienen autoridad para forzar aplicaciones VPP compatibles para iPhone y iPad, lo que impide que los usuarios las instalen directamente desde la aplicación.

Para obtener instrucciones de implementación detalladas y opciones de configuración, consulte la documentación completa disponible en la Guía del administrador y los recursos que figuran a continuación:

- Gestión de aplicaciones
- Ajustes del catálogo de aplicaciones
- Configurar Apps y Books de Apple
- Tienda de aplicaciones corporativas de Apps@Work
- Restricciones de la AppStore de macOS

Administrar configuraciones

Las configuraciones son conjuntos de ajustes que usted, como administrador, envía a los dispositivos. Por ejemplo, se pueden utilizar configuraciones para establecer los ajustes VPN y los requisitos del código de acceso en los dispositivos. Las configuraciones existentes en su sistema aparecerán en la página Configuraciones. Puede seleccionar varias configuraciones desde la página de Configuraciones y empujarlas a varios dispositivos a la vez. Estas configuraciones se pueden enviar a los spaces de dispositivos específicos y los dispositivos de otros spaces no se verán afectados. Las configuraciones se pueden enviar a un único espacio, a varios espacios o a todos los espacios a la vez.

La mayoría de las configuraciones en Ivanti Neurons for MDM son comunes a todas las plataformas. Para obtener más detalles sobre cómo trabajar con configuraciones, consulteTrabajar con configuraciones.

Algunas configuraciones solo son compatibles con plataformas específicas. Puede consultar la lista por plataforma compatible en Tipos de configuración

Administración de actualizaciones de software

Puede empezar por establecer la configuración de Actualización de software para sus dispositivos iOS y macOS.

> Al configurar una ventana programada para la actualización de software, el comando de actualización del sistema operativo se enviará cada hora al dispositivo para asegurarse de que la actualización no pierda la ventana. Según el comportamiento de Apple, cada vez que el dispositivo reciba la orden de actualización del sistema operativo, una ventana emergente notificará al usuario de la necesidad de actualizar. El usuario puede aplazarlo hasta tres veces. A la tercera vez, según el comportamiento de Apple, el dispositivo forzará la actualización.

Los dispositivos MacOS tienen algunas reglas específicas que se pueden aplicar. Consulte la configuración de las reglas de actualización de software macOS

Comando de actualización del SO para iOS

También puede enviar una orden única de actualización a uno o varios dispositivos desde la Lista de dispositivos o desde la Página de dispositivos. Consulte el comando Programar actualización del SO.

Configuración de dispositivos de iOS/iPadOS

Las siguientes configuraciones son compatibles con iOS/iPadOS:

- **Restricciones de iOS/iPadOS**
- **Configuración eSIM**
  - **Plan de conservación de datos**
- **Configuración de red móvil**
- **Activar Modo perdido**
- **Configurar un perfil de MDM en iOS**
- **Modo Single-App**
  - **Modo aplicación única autónoma**
- **iPad compartido para negocios.**
- **Configuración de educación**
- **Configuración personalizada de iOS**
- **Mensaje de la pantalla de bloqueo**

Configuración de dispositivos de watchOS

Ahora puede inscribir dispositivos Apple watchOS en Ivanti N-MDM mientras los vincula con los dispositivos iOS.

Esta función actualmente es compatible con: watchOS 10+.

ProcedureProcedimiento

1. Debe inscribir el dispositivo iOS 17+ supervisado.
2. Asigne la configuración de inscripción del Apple Watch al dispositivo iOS.
3. Ya puede emparejar su Apple Watch con el iPhone.

> Puede emparejar el Apple Watch después de enviar la configuración del reloj al iPhone. No puede activar la gestión remota para un Apple Watch si la configuración del reloj se transfiere al iPhone después de que el Apple Watch se sincronice con él.

Las configuraciones siguientes son compatibles con los dispositivos watchOS:

- Cellular_Configuration
- Configuración del certificado
- Transparencia del certificado
- Identity_Certificate_Configuration
- Restricciones de iOS
- Passcode_Settings
- Per-App_VPN_Configuration
- Wi-Fi_Configuration

Acciones de dispositivo compatibles con dispositivos watchOS

Las acciones siguientes del dispositivo son compatibles con los dispositivos watchOS:

- Borrar contraseña
- Bloquear el reloj de Apple
- Borrar Apple Watch
- Dar de baja el reloj Apple desde Ivanti Neurons for MDM

> Al desvincular el dispositivo iOS emparejado, el reloj se reiniciará y se desvinculará del dispositivo iOS.

Configuración de dispositivos de macOS

Las siguientes configuraciones son compatibles con macOS:

- Restricciones de macOS
- Configuración de dispositivos macOS
- Trabajar con scripts y el cliente Mobile@Work
- Configurar un perfil de MDM en macOS
- Configurar la contraseña del firmware
- Activar FileVault
  - Clave de recuperación de FileVault
  - Configuración de opciones de FileVault
- Plataforma y SSO extensible
- Active Directory macOS
- Cortafuegos
- Ethernet
- Creación de cuentas en Office 365

- Extensiones del sistema de macOS
- Restricciones de grabación en discos multimedia
- Ajustes de privacidad

Configuración de dispositivos TvOS

Las siguientes configuraciones son compatibles con tvOS:

- Configuración de Apple TV
- Restricciones de Apple TV
- Visualización de la sala de conferencias
- Duplicación AirPlay

Configuración de dispositivos visionOS

Ahora puede inscribir dispositivos Apple visionOS en Ivanti Neurons for MDM.

Esta función actualmente es compatible con: visionOS 1.1+

Puede inscribir dispositivos visionOS utilizando uno de los siguientes métodos:

- Inscripción de dispositivos basada en cuenta
- Inscripción de Usuario generada por cuenta
- Inscripción de dispositivos

Las configuraciones siguientes son compatibles con los dispositivos visionOS:

- Configuración de CalDAV
- Configuración de CardDAV
- Configuración del certificado
- Configuración de comprobación de revocación de certificados
- Transparencia del certificado
- Creación de una configuración de proxy de DNS
- DNS cifrado
- Configuración de correo electrónico
- Configuración de Exchange
- Configuración de Google
- Certificado de identidad
- Restricciones de iOS
- Configuración de LDAP
- Dominios administrados
- Configuración del relé de red
- Configuración de VPN por aplicación
- Configuración de inicio de sesión único

- Configuración del calendario suscrito
- Configuración de VPN
- Filtro de contenido web
- Configuración de Wi-Fi

Acciones de dispositivo compatibles con dispositivos visionOS

Las acciones siguientes del dispositivo son compatibles con los dispositivos visionOS:

- Borrar Apple Vision Pro
- Retirar Apple Vision Pro
- Desbloquear Apple Vision Pro

Soporte para la gestión de dispositivos declarativos (DDM)

La gestión declarativa de dispositivos de Apple es un protocolo moderno de gestión que permite a los dispositivos gestionados aplicar de forma proactiva y autónoma sus propios ajustes de gestión con menos comunicación. La gestión declarativa de dispositivos se activa en los dispositivos recién inscritos durante la inscripción o durante el registro de los dispositivos ya inscritos.

La gestión declarativa de dispositivos se activa automáticamente en los dispositivos elegibles siguientes:

- Equipos con macOS 13 o posterior
- Dispositivos con iOS 16 o iPadOS 16 o posterior
- Los dispositivos inscritos a través de la inscripción de usuarios son compatibles con Administración declarativa de dispositivos de iOS o iPadOS 16 o posterior.
- Dispositivos Apple TV con tvOS 16 o posterior
- Dispositivos Apple Watch con watchOS 10 o posterior
- Dispositivos Apple Vision Pro con visionOS 1.1 o posterior

Funciones de gestión declarativa compatibles actualmente:

- **Canales de estado**:
  - Cambios en la versión del SO
  - Cumplimiento del código de acceso
  - Código de acceso presente
- **Configuraciones**:
  - Configuración de gestión declarativa

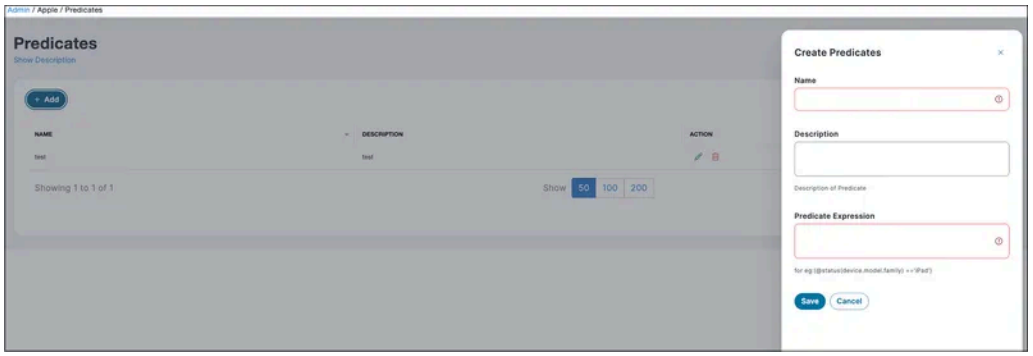
Predicados en configuraciones DDM

Los predicados son expresiones en lenguaje Cocoa que pueden proporcionar flexibilidad y granularidad a la activación de una configuración un dispositivo. La expresión reside en el dispositivo y se aplicará cuando se cumplan las condiciones de este predicado. Hemos añadido una nueva función que permite crear, guardar y aplicar predicados a cualquier configuración de DDM.

La configuración de DDM muestra una nueva opción en la página Distribución para aplicar un Predicado. Puede encontrar los Predicados ya creados en la lista desplegable de esta sección.

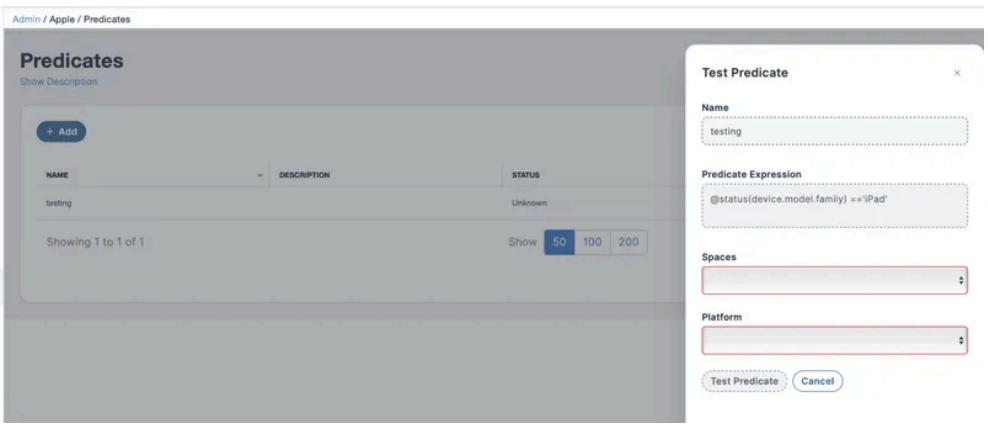
Creación de un predicado

1. Vaya a **Administrador** > **Apple** > **Predicados**.
2. Haga clic en **Añadir**. Aparece en pantalla la ventana Crear predicados.
3. Introduzca la siguiente información:
   - **Nombre**: nombre del predicado
   - **Descripción**: agregar alguna descripción relevante.
   - **Expresión de predicado**: expresión de predicado. Por ejemplo, @status(device.model.family) ==’iPad’.



4. Haga clic en **Guardar**. Aparece un diálogo en la pantalla que confirma la creación del predicado.
5. Verifique la validez de la sintaxis de predicado actualizando la página y observando valores en el campo de estado (con valores: **Desconocido**, **En curso**, **Válido**, **No válido**).
   1. Haga clic en **Probar**. La ventana de **Probar predicado** aparece en la pantalla.
   2. Introduzca la siguiente información:
      - **Nombre**: predeterminado
      - **Expresión de predicado**: predeterminado
      - **Espacios**: espacio predeterminado
      - **Plataforma**: iOS/macOS
      - **Nombre del dispositivo**: relacionado con la expresión de predicado.

      > El campo **Nombre del dispositivo** aparecerá bajo el campo **Plataforma** solo después de que se hayan seleccionado los campos **Espacios** y **Plataforma** en los desplegables.



3. Haga clic en **Probar predicado**.
4. Aparece un diálogo en la pantalla que confirma el inicio del predicado de prueba.
5. Actualice la página para encontrar el estado de la sintaxis de predicado.
    - Para una expresión de predicado correcto, el estado cambia de **Desconocido** > **En curso** > **Válido**.
    - Para una expresión de predicado incorrecto, el estado cambia de **Desconocido** > **En curso** > **No válido**.
6. Repita el procedimiento si desea crear varios predicados utilizando diferentes expresiones de predicado.

Distribución de predicados para una configuración DDM

1. Cree una configuración compatible con DDM.
2. Configure el interruptor de palanca “Activación con predicados” en ON y use el botón para incluir los predicados (según sea necesario).



Para editar o eliminar un predicado, vaya a **Administrador** > **Apple** > **Predicados**. En esta página encontrará la lista de predicados disponibles. Haga clic en **Editar** para realizar cualquier cambio en el predicado existente y guardarlo. Del mismo modo, para eliminar un predicado existente, selecciónelo y haga clic en **Eliminar**.

> No puede eliminar un predicado si está asociado a alguna configuración.

Propiedades de administración para una configuración DDM

El administrador puede usar lo siguiente para crear predicados:

- Variables de usuario y dispositivo
- Atributos del usuario
- Atributos del dispositivo

Ejemplo del uso de propiedades de gestión en predicados (atributos personalizados):

Predicado para verificar si el nombre del usuario es "Prueba" @Property (UserFirstName) == 'Test'

Más ejemplos

- Familia de hardware de un dispositivo: (Mac, iPhone, iPad, etc.)
  @status(device.model.family) =='iPad'
  Si cierto, el código de acceso está presente en el dispositivo. Si Falso, el código de acceso no está presente en el dispositivo.
  @status(passcode.is-present)==true
- La familia del sistema operativo en uso en el dispositivo, como macOS o iOS.
  @status(device.operating-system.family)=='iPadOS'

- La versión del sistema operativo en uso en el dispositivo, como 15.0
  @status(device.operating-system.version)=='18.2'
  @status(device.operating-system.version)<'18.3'
  @status(device.operating-system.version)>='18.2'
- Valor booleano que especifica el estado habilitado para la bóveda del archivo en el dispositivo
  @status(diskmanagement.filevault.enabled)==true
- Ejemplo de propiedades de gestión (atributos personalizados):
  El predicado para verificar el nombre del usuario es "prueba"
  @property(userFirstName)=='test'

7.5.2. Desplegar dispositivos de Windows

Esta sección contiene los siguientes temas:

- Información general
- Administración de dispositivos
- Inscripción y registro de dispositivos Windows
- Administración de actualización de Windows
- Administración y distribución de aplicaciones
- Control de aplicaciones
- Configuración del administrador de dispositivos Windows
- Cumplimiento de los dispositivos de Windows
- Inventario de aplicaciones y hardware de Windows

Información general

Ivanti Neurons for MDM le ayuda a administrar todos los equipos portátiles y de escritorio de Windows, incluida la administración del ciclo de vida de los dispositivos HoloLens 2 end-end: desde configuración, inscripción, aprovisionamiento, seguridad, aplicación, administración, monitorización, actualización de software y SO, hasta la retirada.

Administración de dispositivos

Dispositivos Windows compatibles:

- Windows PC 10+
- Microsoft HoleLens 2

Para obtener más información sobre las funciones de Administración de dispositivos y de informes, consulte Dispositivos

Inscripción y registro de dispositivos Windows

Ivanti Neurons for MDM es compatible con todos los métodos de registro de dispositivos estándar para dispositivos de Windows:

- Registro manual
- Inscripción en masa
- a través de SCCM y de Ivanti EPM
- Windows Autopilot
- Registro Entra ID

Para obtener más información sobre métodos de registro, consulte Uso de Microsoft Azure

Para obtener información sobre compatibilidad multiusuario, consulte Compatibilidad con varios usuario para dispositivos de Windows.

Administración de actualización de Windows

- Configuración y programación de las actualizaciones de Windows: para configurar y programar las actualizaciones de Windows, cree una configuración mediante Configuración - **Actualizaciones de software**.
- Windows Update Management: puede ver y aprobar las actualizaciones notificadas por los dispositivos Windows que desee actualizar mediante Windows Update Management. Mediante esta característica, puede evitar que las actualizaciones innecesarias o no probadas se instalen en los dispositivos. Para obtener más información, consulte **Administración de actualización de Windows**.

Administración y distribución de aplicaciones

Los usuarios pueden administrar ciclos de vida de aplicaciones completos (Importar, configuración, programar, distribución, actualizar y eliminación) de las aplicaciones de Windows.

Tipos de aplicaciones compatibles:

- Interno
- MSB
- Almacenamiento público

Extensiones de aplicaciones compatibles:

- MSI
- MSIX
- APPX
- Agrupaciones de APPX
- EXE (Bridge)

Para obtener más información sobre cómo administrar las aplicaciones de Windows, consulte **Configuración de aplicaciones**. Para automatizar las actualizaciones de las aplicaciones, consulte **Programación de aplicaciones Windows** y **Trabajar con configuraciones**.

Control de aplicaciones

La configuración del control de aplicaciones le permite categorizar las aplicaciones como lista de permitidos o lista de bloqueados a nivel de dispositivo. Las aplicaciones que ya estén instaladas no serán visibles y no podrán iniciarse. Las aplicaciones seguirán siendo visibles en la App Store, pero no se podrán descargar ni iniciar. Cualquier dispositivo al que se distribuya esta configuración de Control de aplicaciones la empleará e ignorará cualquier otro ajuste de Políticas de aplicaciones permitidas. La configuración de control de aplicaciones sustituye a cualquier política relacionada con la aplicación que haga referencia a las mismas aplicaciones en los dispositivos de destino.

Para obtener más información, consulte **Configuración del control de aplicaciones: controle qué aplicaciones pueden instalarse en cada dispositivo**.

Configuración del administrador de dispositivos Windows

La compatibilidad para Windows 10+ PC y Microsoft HoloLens 2 incluye las capacidades siguientes:

- **Registro de dispositivos (PC con Windows 10+ y Microsoft HoloLens 2)**
- **Configuración del código de acceso**
- **Configuración de Exchange**

- Configuraciones
- Dispositivos
- Aplicaciones
- Programación de aplicaciones Windows
- Configuración del control de aplicaciones: controle qué aplicaciones pueden instalarse en cada dispositivo
- Administración de actualización de Windows
- Estado del dispositivo que notifica desde Ivanti Neurons for MDM a Azure
- Configuración de los perfiles de Windows Autopilot
- Insertar SyncML en dispositivos mediante la configuración personalizada
- Políticas
- Restricciones de Windows
- Certificados de identidad
- Windows Hello para empresas
- Perfiles de Wi-Fi y de VPN

> Las configuraciones que se han distribuido a los dispositivos de HoloLens que no son compatibles con este tipo de dispositivo, no se notificarán como configuraciones distribuidas en la pestaña Configuración en los Detalles del dispositivo.

Funciones de Windows (compatible solo para PC de Windows):

- Ivanti Bridge
- Configuración del BIOS de Windows
- BitLocker de Windows
- Configuración del kiosco de Windows
- Configuración de la licencia de Windows
- Configuración de la integración de servidores EMA
- Ajustes de la impresora
- Configuración para eliminar el «bloatware»
- Explorador ADMX (GPO)

Cumplimiento de los dispositivos de Windows

Ivanti Neurons for MDM se puede configurar con Microsoft Azure para una inscripción perfecta de los usuarios en sus dispositivos de escritorio de Windows y tabletas con Windows 10+. Para configurar la integración del abonado de Azure para habilitar el Cumplimiento de dispositivos, consulte Uso de Microsoft Azure.

Inventario de aplicaciones y hardware de Windows

Inventario de aplicaciones de Windows

El Inventario de aplicaciones es una lista de aplicaciones detectadas en los dispositivos inscritos. Utilice esta página para obtener información sobre las aplicaciones que se están utilizando en los dispositivos inscritos. Para obtener más información, consulte Inventario de aplicaciones.

El inventario de aplicaciones muestra las aplicaciones Win32 o de Win32 Store en un dispositivo si la configuración de privacidad del mismo permite la recopilación de información para todas las aplicaciones del dispositivo.

Configuración de los intervalos del inventario de aplicaciones

Puede establecer intervalos de recopilación de inventario de aplicaciones de Windows 10 para varios inventarios de tipos de origen de aplicaciones. Los intervalos se usan cuando la política de privacidad se ha ajustado para que se obtengan todas las aplicaciones del dispositivo.

Para obtener más información, consulte **Configuración de los intervalos del inventario de aplicaciones**.

Inventario de hardware de Windows

Puede habilitar la recopilación de información sobre el hardware de dispositivos Windows 10+. Estos detalles se recuperan usando Bridge. Para obtener más información, consulte el **Inventario de hardware**.

7.5.3. Configurar Apple Remote Desktop en dispositivos macOS

Esta sección contiene los siguientes temas:

- Activar Apple Remote Desktop en dispositivos macOS
- Deshabilitar el escritorio remoto de Apple en dispositivos macOS

Activar Apple Remote Desktop en dispositivos macOS

La función de escritorio remoto de Apple permite compartir pantallas y le permite administrar los dispositivos de manera remota. La función de Apple Remote Desktop está disponible para los dispositivos macOS 10.14.4+ supervisados.

Procedimiento

1. Vaya a **Dispositivos**, seleccione uno o más dispositivos macOS supervisados.
2. Haga clic en **Acciones** > **Activar Remote Desktop** para los dispositivos.
3. Haga clic en **Remote Desktop** para confirmarlo.

Deshabilitar el escritorio remoto de Apple en dispositivos macOS

Procedimiento

1. Vaya a **Dispositivos**, seleccione uno o más dispositivos macOS supervisados.
2. Haga clic en **Acciones** > **Deshabilitar escritorio remoto** para los dispositivos. La función de compartir pantalla se deshabilita y no puede administrar dispositivos de manera remota.

7.5.4. Registro de dispositivos (iOS, macOS y Android)

Esta sección contiene los siguientes temas:

- **Instalar el perfil de administración manualmente**
- **Enviar una invitación (iOS, macOS, and Android)**
- **Pedir a los usuarios finales que se descarguen la aplicación (iOS y Android)**

La mayoría de los usuarios comienzan por registrar un dispositivo. Para iniciar el proceso de registro, puede hacerlo de cualquiera de las siguientes formas:

- Envíe una invitación a uno o más usuarios finales (registro de iReg)
- Pida a los usuarios finales que descarguen Go (registro en la aplicación)

> Si la inscripción en MDM de dispositivos iOS y macOS falla con el mensaje Error en la instalación del *perfil El servidor SCEP ha devuelto una respuesta no válida.*. error, el usuario del dispositivo debe reiniciar el proceso de inscripción del dispositivo desde el principio. Esto ocurre sobre todo cuando el usuario del dispositivo tarda más de lo esperado en completar el proceso de inscripción en MDM de dispositivos iOS y macOS después de descargar el perfil en el dispositivo. Póngase en contacto con el servicio de asistencia de Ivanti para obtener más información.

Ivanti Neurons for MDM es compatible con la gestión a nivel de usuario de un solo usuario (usuario local o usuario registrado en Active Directory (AD)) en dispositivos macOS. Los administradores pueden gestionar dispositivos para los usuarios, aplicar perfiles de dispositivos y de usuarios y, por ende, usar la App Store, la distribución de aplicaciones, configuraciones y políticas (como Apps@Work, restricciones y seguridad).

Para administrar dispositivos macOS con un usuario de AD, el usuario de AD tiene que ser el usuario que ha iniciado sesión durante el registro. Cualquier otro usuario no registrado no podrá ver los perfiles específicos para los usuarios registrados (por ejemplo, las certificaciones de identidad o la VPN). Sin embargo, las configuraciones a nivel de dispositivo sí podrán verlas y usarlas cualquier usuario que haya iniciado sesión.

> El usuario **final debe tener una cuenta** en Ivanti Neurons for MDM antes de poder iniciar el proceso de registro del dispositivo. Para los usuarios de LDAP, esto significa que deben tener configurados un **Connctor** y un **servidor LDAP** y que el usuario debe importarse del servidor LDAP. Para los usuarios locales, esto implica **añadir un usuario**.

> La URL de inscripción de dispositivos generada en las versiones anteriores de Ivanti Neurons for MDM dejará de funcionar en la versión actual. El administrador deberá regenerar la URL de inscripción de dispositivos para el registro el dispositivo.

Instalar el perfil de administración manualmente

Aplicable a:

- iOS 12.2 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- macOS 11.0 hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Registro de dispositivos de iOS

Durante el registro en la aplicación en dispositivos iOS:

- Durante el registro del dispositivo con Go app aparece una página con instrucciones para instalar el perfil.
- Haga clic en la opción **Instalar el perfil descargado** y haga clic en **Entendido**.
- El perfil descargado es válido durante algunos minutos, después de los cuales será obligatorio volver a registrarse.

Registro del dispositivo macOS

Para el registro del dispositivo macOS en el portal de autoservicio, el usuario debe realizar los siguientes pasos:

Procedimiento

1. Iniciar sesión con sus credenciales.
2. En la página Instalar perfil de administración, el perfil se descarga en el sistema local del usuario.
3. Haga doble clic en el perfil descargado para hacerlo visible en las Preferencias del sistema del usuario.

> Hay un tiempo limitado para que el usuario instale el perfil antes de que quede invalidado.

4. Abra **Perfiles** en Preferencias del sistema. Cuando el perfil se descarga en el dispositivo, los usuarios pueden ver una página web con el enlace Perfiles. Haga clic en **Perfiles** para abrir la aplicación Ajustes.
5. Haga clic en **Instalar** para instalar el perfil de administración.
6. Continúe y termine el procedimiento de instalación. Introduzca la contraseña del sistema cuando se le solicite.

Enviar una invitación (iOS, macOS, and Android)

Comience el proceso de registro enviando una invitación. Ivanti Neurons for MDM Cloud ofrece las siguientes formas de enviar una invitación a los usuarios finales para que registren un dispositivo:

- En el **Asistente de inicio**
- al **añadir uno o más usuarios**
- en la página Usuarios (**Acciones > Enviar invitación**)

> Si el usuario final pierde la invitación, puede compartir la URL que se listó en la invitación. Asegúrese de que agrega **/go** al final de la URL.

Los usuarios finales que tengan una cuenta de Ivanti Neurons for MDM con una contraseña no necesitan una invitación para iniciar el proceso de registro. Puede enviarles la URL que se lista en la invitación.

Pedir a los usuarios finales que se descarguen la aplicación (iOS y Android)

La aplicación Go está disponible para dispositivos de Android y de iOS. Puede proporcionar instrucciones a los usuario finales sobre cómo descargar la aplicación desde una tienda de aplicaciones pública e iniciar el proceso de registro desde la aplicación. La invitación del correo electrónico contiene la información siguiente:

- Un vínculo a la página de registro
- Un PIN de un solo uso (si lo ha ajustado el administrador)
- Instrucciones básicas para los pasos siguientes

Si ya ha establecido una contraseña para la cuenta, ahora puede enviar la contraseña a la dirección de correo electrónico corporativo del usuario final. Si está utilizando LDAP para la autenticación, informe al usuario final de que son necesarias credenciales de red.

Si el usuario no completa la instalación del perfil de MDM durante el registro, Ivanti Neurons for MDM enviará periódicamente notificaciones push al dispositivo para pedir al usuario que complete el proceso de registro.

El usuario puede usar el nombre de usuario y la constraseña o escanera el código QR para iniciar el registro del dispositivo desde Go app. Los detalles son los siguientes:

- **Nombre de usuario**: dirección de correo electrónico
- **Contraseña**: si se especifica en los **Ajustes de usuarios** y el administrador define una contraseña temporal
- **Código QR**: genere el código QR desde el portal de autoservicio de Ivanti Neurons for MDM. Cuando intenta escanear el código QR mediante la opción **Escanear código QR**, aparece un aviso en la pantalla que solicita al usuario que dé permiso de acceso a la cámara del dispositivo. Después de dar permiso, la cámara escanea el código QR y se registra el dispositivo. Esta opción es compatible con Android 9 o posterior, iOS 14 y versiones posteriores.

Como usuario final, si recibe un correo electrónico de registro en su dispositivo móvil, pulse el enlace para empezar el proceso de registro. Si recibe un correo electrónico en un equipo de sobremesa o portátil, introduzca la URL en el navegador del dispositivo móvil para iniciar el proceso de registro.

Si aun no tiene definida una contraseña para su cuenta de usuario de Ivanti Neurons for MDM o si **Ajustes de usuario** requieren un PIN de registro, se incluye un PIN de un solo uso. Después de ingresar el PIN, al usuario final se le pedirá que establezca una contraseña para la cuenta si no existe ya una.

> Para dispositivos de Android Enterprise, cuando se completa el registro, se desinstalan los certificados de CA instalados manualmente en un perfil de trabajo de los dispositivos de la empresa o de los dispositivos administrados de trabajo.

Reinscripción de dispositivos iOS

Si desea volver a inscribir su dispositivo, puede hacerlo de la siguiente manera:

1. Iniciar el cliente Go en el dispositivo.
2. Vaya a **Configuración** > **Solución de problemas** > **Vuelva a registrar el dispositivo**. El proceso de reinscripción se inicia y muestra algunas solicitudes de confirmación.
3. Pulse **Sí** en las indicaciones.

> Si pulsa **Cancelar** durante la instalación del perfil, el proceso de inscripción se detiene y el servidor Ivanti Neurons for MDM desactiva el MDM del dispositivo.

Para reiniciar el proceso de reinscripción debe volver a instalar el perfil ya descargado. El perfil descargado solo es válido durante unos minutos, después debe realizar la reinscripción desde el cliente Go.

Re-registrando dispositivos Android

El administrador puede volver a registrar un dispositivo mediante las operaciones de retirar, borrar o eliminar sin borrar manualmente la entrada activa existente. Este método es más útil, concretamente, para re-registros donde la nueva entrada y la entrada existente pertenecen al mismo abonado. La página de Dispositivos muestra el estado de los dispositivos en el portal administrativo de Ivanti Neurons for MDM de la manera siguiente:

- **Activo**: el dispositivo se ha registrado correctamente

- **Retirado**: el dispositivo se restablece y se mostrará el estado retirado
- **Borrado**: el dispositivo se restablece y se mostrará el estado borrado
- **Restablecer**: se restablece el dispositivo y quedará en estado activo en el servidor hasta el próximo registro

La página de Audit Trails lista el registro del dispositivo, el re-registro y los estados retirados de dispositivos Android. Para obtener más información, consulte **Trabajar con widgets**.

> Para Android 9.x y versiones anteriores, se mostrará una única entrada después de volver a registrarse. En el caso de Android 10.x y versiones posteriores, se mostrarán múltiples entradas. No obstante, solo la entrada más reciente estará activa y las anteriores quedarán en estado retirado.

7.5.5. Registro de dispositivos (PC con Windows 10+ y Microsoft HoloLens 2)

Esta sección contiene los siguientes temas:

- Registro manual
  - Enviar una invitación
  - Completar el proceso de registro del usuario final
- Windows Autopilot
- Registro estándar de Entra ID

Hay dos tipos de proceso de registro de dispositivos:

- Registro manual
  - Invitación
  - Registro de usuario final
- Windows Autopilot
- Con SCCM e Ivanti EPM, a través de la inscripción de paquetes de aprovisionamiento con PIN. Consulte **Inscripción de paquete de aprovisionamiento con PIN**.
- **Inscripción en masa**

Registro manual

La mayoría de los usuarios comienzan por registrar un dispositivo. Para iniciar el proceso de registro, puede hacerlo de cualquiera de las siguientes formas:

- Invitación por correo electrónico
- Dirigir a los usuarios la URL para su implementación
- El **usuario final debe tener una cuenta** en Ivanti Neurons for MDM antes de poder iniciar el proceso de registro del dispositivo. Para los usuarios de LDAP, esto significa que deben tener configurados un **Conector** y un **servidor LDAP** y que el usuario debe importarse del servidor LDAP. Para los usuarios locales, esto implica **añadir un usuario**.
- La URL de inscripción de dispositivos generada en las versiones anteriores de Ivanti Neurons for MDM dejará de funcionar en la versión actual. El administrador deberá regenerar la URL de inscripción de dispositivos para el registro el dispositivo.

Enviar una invitación

En la mayoría de los casos, comenzará el proceso de registro enviando una invitación. Ivanti Neurons for MDM ofrece las siguientes formas de enviar una invitación a los usuarios finales para que registren un dispositivo:

- en el **Asistente de inicio**
- al **añadir uno o más usuarios**
- en la página Usuarios (**Acciones > Enviar invitación**)

Si los usuarios finales pierden la invitación, la reciben en un ordenador de escritorio o un portátil o si, por cualquier motivo, no la reciben, puede enviarles la URL que se incluía en la invitación. Solo tiene que añadir **\go** al final de la URL del servicio.

Los usuarios finales que tienen una cuenta de Ivanti Neurons for MDM con una contraseña establecida no necesitan una invitación para iniciar el proceso de registro. Puede enviarles la URL que aparecería en la invitación.

Completar el proceso de registro del usuario final

Dígale a los usuarios de sus dispositivos cómo completar el proceso de registro. Puede usar las siguientes instrucciones como plantilla y realizar cualquier cambio necesario:

Procedimiento

1. Abra un navegador en su PC con Windows 10+.
2. Navegue hasta mobileiron.com/go.
   Será redirigido a una página nueva que contiene una URL de inscripción.
3. Copie esa URL de inscripción en el portapapeles.
4. Pulse **añadir cuenta** en la parte inferior de la página **Ajustes**.
5. Introduzca la dirección de correo electrónico asociada con la invitación recibida.

> Si el nombre de usuario de Ivanti Neurons for MDM no coincide con la dirección de correo electrónico que este ingresó en Ivanti Neurons for MDM, dígale al usuario que ingrese su nombre de usuario cuando se le solicite la dirección de correo electrónico.

Copie la URL del servidor del lugar de trabajo que copió en el siguiente campo de texto.

7. Pulse **iniciar sesión**.
8. Introduzca su contraseña en el siguiente campo.
9. Deje en blanco los demás campos.
10. Pulse **iniciar sesión**.
11. Haga clic en **hecho** en la pantalla **CUENTA AÑADIDA**.
    La pantalla de inicio del lugar de trabajo muestra que se ha añadido una cuenta.

Windows Autopilot

Windows Autopilot es una característica de Microsoft que ayuda a los administradores a configurar y pre-configurar nuevos dispositivos para que estén listos para la empresa. La función de Autopilot ayuda a un aprovisionamiento rápido, fiable y sin problemas de los dispositivos Windows Desktop o HoloLens 2. Además, la función Autopilot ayuda a realizar las siguientes tareas:

- Unir automáticamente dispositivos a Entra ID (Entra ID)
- Inscribir automáticamente los dispositivos en los servicios MDM
- Crear y auto-asignar dispositivos a grupos de configuración basados en el perfil del dispositivo
- Personalizar la experiencia de inscripción
- Aplicar configuraciones y políticas
- Instalar aplicaciones esenciales

Ivanti es compatible con todos los modos de perfiles Autopilot:

- Impulsado por el usuario
- Proveído previamente impulsado por el usuario (anteriormente White Glove)

- Modo de auto-despliegue

Para obtener más información, consulte **Configuración de los perfiles de Windows Autopilot**.

> Por motivos de seguridad y uso no autorizado del dispositivo, todos los dispositivos Windows de Autopilot se pueden bloquear para un arrendatario mediante la función TenantLockdown CSP. Para utilizar esta función, los dispositivos deben estar inscritos mediante la opción Autopilot. Esta configuración se aplica a nivel de dispositivo. Ver **TenantLockdown CSP**.

Registro estándar de Entra ID

Cuando los usuarios se añaden al abonado de Entra ID, pueden inscribir directamente sus dispositivos a través de la Cuenta de Trabajo.

Procedimiento

1. En un dispositivo Windows, vaya a **Ajustes > Cuentas > Acceder al trabajo o escuela**.
2. Seleccione Agregar cuenta de trabajo o escuela y haga clic en **Conectar**.
3. Proporcione una dirección de correo electrónico desde su cuenta de trabajo.

El dispositivo se inscribe automáticamente a Ivanti Neurons for MDM.

7.5.6. Solución de contraseña del administrador local (LAPS, por sus siglas en inglés)

La **Solución de contraseña del administrador local (LAPS)** automatiza el manejo seguro de las contraseñas de los dispositivos Windows. LAPS aplica cambios de contraseñas aleatorios y regulares y almacena estas contraseñas de forma segura en un directorio, de manera que se reduce el riesgo de movimiento lateral en caso de compromiso.

La versión moderna de LAPS se integra con Azure y las últimas plataformas de administración de dispositivos Windows, lo que permite almacenar, recuperar y configurar las políticas de contraseñas de manera segura con Ivanti Neurons for MDM y el portal de Azure. Esto asegura que las credenciales de los administradores permanezcan protegidas y auditables en ambos tipos de puntos de conexión de Windows: los heredados y los administrados en la nube.

> Para usar LAPS con Ivanti Neurons for MDM, los administradores de Azure deben asegurarse de que la aplicación N-MDM se agregue a su entorno de Azure con el permiso de LAPS requerido (**DeviceLocalCredential.Read.All**).

> La configuración de LAPS puede especificar qué cuenta de administrador local se aplica mediante la configuración de la directiva **Nombre de la cuenta de administrador**. Si el nombre de cuenta especificado en la configuración no está presente en el dispositivo, no se podrá gestionar dicho nombre de cuenta. No obstante, cuando el **Nombre de la cuenta de administrador** se deja en blanco, la política, por defecto, se establece como la cuenta del administrador local integrada del dispositivo, la cual se identifica mediante su identificador relacional (RID) conocido.

> Cuando se aplica la configuración LAPS, la contraseña de la cuenta de administrador local del dispositivo será administrada por el administrador y se generará la contraseña en Azure Active Directory.

Otras funciones de LAPS

- Almacenamiento de contraseñas en Azure: ahora se pueden almacenar de forma segura las contraseñas de los administradores locales en el objeto de dispositivo de Azure.
- Recuperación de contraseñas: Los administradores pueden recuperar las contraseñas de los dispositivos directamente a través del portal de Azure.
- Ajustes configurables: Ajustes de LAPS configurables que se pueden gestionar en el portal de Ivanti Neurons for MDM.
- Rotación de contraseñas bajo demanda: Los administradores pueden rotar manualmente las contraseñas de los dispositivos desde el portal de Ivanti Neurons for MDM.
- Restablecimiento automático de contraseña al usarla: las contraseñas se pueden restablecer automáticamente una vez que se hayan utilizado.

Cree la configuración de LAPS

Requisitos previos

- La solución LAPS debe estar activada en los dispositivos. Esta solución NO está disponible para todos por defecto. Póngase en contacto con el equipo de soporte para recibir ayuda.
- Los dispositivos deben estar inscritos en Operaciones de dispositivos de Azure (ADO).

Procedimiento

1. En su plataforma de administración de configuración, inicie la creación de la configuración LAPS.
2. **Establecer parámetros obligatorios**:
    - **Directorio de respaldo**: seleccione la contraseña de respaldo solo para Microsoft Entra ID.
    - **Nombre del administrador local**: especifique el nombre de cuenta del administrador de su sistema (por ej., Administrador).
3. **Configurar ajustes adicionales**: establezca estos ajustes según la política de seguridad de su organización. Se usarán los valores predeterminados a menos que se determine lo contrario.
    - **PasswordAgeDays**: Número de días hasta que la contraseña de administrador local se rota automaticamente.
    - **PasswordComplexity**: Especifique los requisitos de complejidad de la contraseña (por ej., alfanumérica, caracteres especiales).
    - **PasswordLength**: Establezca la longitud deseada de la contraseña del administrador local.
    - **PostAuthenticationActions**: Defina las acciones que deben realizarse después de la autenticación.
    - **PostAuthenticationResetDelay**: Establezca un retraso (en horas/minutos) para restablecer la contraseña después de la autenticación.
4. **Distribuir configuración LAPS**
    - Asignar el perfil de configuración LAPS a usuarios/dispositivos inscritos en ADO.
    - Cuando haya aplicado la configuración, se creará una contraseña de administrador local aleatoria y se almacenará de forma segura en Microsoft Entra ID en:
      Dispositivos → Administrar dispositivos → Recuperación de la contraseña del administrador local.
5. **Rotación de contraseña**
    - La contraseña se rota automáticamente según el valor establecido en: **PasswordAgeDays**.
    - Puede revisar el estado de rotación de contraseña en los registros del dispositivo.

Rotación de contraseña

Para forzar la rotación inmediata de la contraseña del administrador local, siga los pasos a continuación:

1. **Navegue hasta el dispositivo**: vaya a la página de detalles del dispositivo de la consola de administración.
2. **Inicie la rotación de contraseña**
    - Haga clic en el menú de elipsis (...).
    - Seleccione **Rotar la contraseña local del administrador**.
    - Confirme la acción cuando se le solicite. Esto enviará una solicitud de rotación de contraseña.
3. **Registro y confirmación**
    - El dispositivo procesa el cambio de contraseña la siguiente vez que se fuerce el contacto.
    - Actualice la página en Microsoft Entra ID para ver la contraseña actualizada en la sección de recuperación de contraseñas.

7.5.7. Inscripción de paquete de aprovisionamiento con PIN

El administrador puede inscribir los dispositivos administrados por SCCM o Ivanti Endpoint Manager a Ivanti Neurons for MDM. La herramienta Paquete de despliegue permite a las organizaciones simplificar la transición de los dispositivos de Windows a Ivanti Neurons for MDM Modern Management, sin tiempo de inactividad ni interrupción para el usuario final. La transición sin fisuras se archiva mediante la descarga de un único paquete de despliegue desde la consola de Ivanti Neurons for MDM, a continuación, se despliega a través de la herramienta de administración o del dominio existente. Una vez que se ejecuta el paquete, inscribirá silenciosamente el punto final en Ivanti Neurons for MDM para la administración continua. El enfoque permite a los administradores primero migrar fácilmente los dispositivos y luego tener la flexibilidad de configurar los dispositivos más tarde de forma inalámbrica. Cuando un dispositivo completa la inscripción silenciosa en Ivanti Neurons for MDM, se une a MDM y es coadministrado por las dos autoridades de administración. Una vez que un administrador ha configurado la experiencia de Windows deseada dentro de Ivanti Neurons for MDM, la plataforma de administración heredada se puede retirar, dejando Ivanti Neurons for MDM como la única autoridad de administración del dispositivo.

> Hay una excepción a esta regla si un dispositivo va a transicionar de Microsoft Endpoint Manager (MEM) o era anteriormente SCCM. El Cliente MEM existente continuará funcionando en Modo de Coexistencia (opuesto al modo de Co-Administración), hasta que la plataforma MEM sea desmantelada. Cuando está habilitado el Modo de coexistencia, el cliente de MEM deshabilita automáticamente determinadas funciones en favor de que Ivanti Neurons for MDM proporcione esas cargas de trabajo. Para obtener más información, consulte la **documentación de coexistencia de Microsoft**.

Para obtener información sobre comportamientos más exactos al usar MEM y otras plataformas de administración de terceros, Ivanti sugiere probar primero la herramienta Paquete de implementación de Ivanti Neurons for MDMen su entorno.

Requisitos previos

- Las cuentas de usuario deben importarse en Ivanti Neurons for MDM mediante LDAP, Entra ID (Entra ID), carga local de usuarios u otras integraciones de identidad.
- Todos los dispositivos deben tener instalado **Windows Configuration Designer**.
- Habilitar el registro basado en PIN en Ivanti Neurons for MDM
- Los usuarios no deben tener espacios en su nombre de usuario, esto podría provocar el fallo de la transición del dispositivo del usuario.
- Esta herramienta puede desplegarse en entornos que no aprovechan Entra ID.
- Los elementos principales de Ivanti Neurons for MDM Modern Windows Management Suite no requieren Entra ID. Para evitar el impacto durante la transición, es posible que la coadministración o coexistencia requieran el despliegue de determinadas cargas de trabajo / configuraciones en la inscripción en segundo plano.
- Actualmente, el paquete de despliegue únicamente es compatible con SCCM e Ivanti Endpoint Manager.

Procedimiento

1. Vaya a **Administrador>Windows>Paquete de despliegue**.
2. Seleccione el **Usuario** o los **Grupos de usuarios** para generar los PIN y haga clic en **Descargar paquete de implementación** (archivo .zip).
3. El paquete de despliegue se proporciona a los administradores de SCCM / Ivanti Endpoint Manager para que lo extraigan y transfieran los archivos a sus respectivos dispositivos administrados por estos administradores. Para obtener información sobre

cómo llevar a cabo este paso, consulte **Paquetes y programas en Administrador de la configuración**.

4. Después de la transferencia, los administradores desencadenan de manera remota la secuencia de comandos de setup.ps1 enlos dispositivos. Para obtener información sobre cómo desencadenar la secuencia de comandos, consulte **Crear y desplegar secuencias de comandos desde el Administrador de configuración**.
5. Los dispositivos se inscriben en Ivanti Neurons for MDM.

El PIN generado para los usuarios es válido solo por 24 horas. Una vez que el PIN caduca, se debe generar un nuevo PIN.

El archivo que contiene los PIN se elimina del dispositivo después de completar el intento de inscripción.

Inscribir dispositivos de SCCM a Ivanti Neurons for MDM

Procedimiento

1. Descargue todos los archivos relacionados con el despliegue desde Ivanti Neurons for MDM para los usuarios seleccionados.
2. Seleccione las cuentas o grupos que se deberán inscribir.
3. Desplegar archivos del paquete en los dispositivos del cliente mediante SCCM:
    1. Verifique si los clientes necesarios están presentes en SCCM. Si el diseñador de configuración de Windows no se encuentra en el cliente, el administrador deberá enviar el diseñador y desplegarlo en el cliente.
    2. En el servidor SCCM, cree una carpeta y copie el archivo zip de despliegue y extraiga el contenido del archivo.
    3. Cree un archivo .bat que copie el contenido de la carpeta donde se extraen los archivos en el dispositivo del cliente.
    4. En SCCM, vaya a **Biblioteca de Software > Administración de aplicaciones > Paquetes** y cree un paquete para copiar el contenido de la carpeta en el cliente. Introduzca la carpeta de destino en la que desee copiar el contenido.
    5. Desplegar el paquete en el dispositivo o la ubicación del dispositivo.
    6. En la sección Monitorización puede monitorizar el estado de despliegue y confirmar que los archivos se copian en la carpeta de destino del cliente.
4. Ejecute la secuencia de comandos para inscribir un dispositivo:
    1. Vaya a **Biblioteca de Software > Secuencias de comandos** y cree una secuencia de comandos.
    2. Introduzca un nombre para la secuencia de comandos y importe la secuencia de comandos de PowerShell **setup.ps1** desde la carpeta descomprimida.
    3. Aprobar la secuencia de comandos y ejecutarla en el dispositivo de destino.
    4. Seleccione **Iniciar ahora** y haga clic en **Guardar**. Las tareas programadas empiezan a ejecutar la secuencia de comandos. Si la ejecución es correcta, el estado se volverá Verde.
5. Para verificar la inscripción del dispositivo, **Ajustes** > **Agregue o elimine un paquete de aprovisionamiento** > **Detalles**.

Inscripción de dispositivos de Ivanti Endpoint Manager en Ivanti Neurons for MDM

Procedimiento

1. Descargue todos los archivos relacionados con el despliegue desde Ivanti Neurons for MDM para los usuarios seleccionados.
2. Seleccione las cuentas o grupos que se deberán inscribir.
3. **Caso 1**: se tiene en cuenta un nombre de dispositivo para inscribirlo con el mismo nombre de usuario. En este caso, la dirección de correo electrónico no es una dirección de usuario correcta. Como dirección de correo de inscripción se utiliza un correo

electrónico con el nombre del dispositivo concatenado con el dominio de AD. El administrador debe ajustar la Cuenta como LocalSystemAccount y usar setup.ps1 como archivo principal para iniciar la ejecución de PowerShell.
Caso 2: se tiene en cuenta una dirección de correo electrónico de usuario para inscribir el dispositivo y no hay restricciones para modificar los archivos en la ubicación del dispositivo. Utilice la dirección de correo electrónico del usuario de la sesión activa para la inscripción. Para habilitar esta inscripción, el administrador debe ajustar la Cuenta como Cuenta de usuario actual y usar setup.ps1 como archivo principal para iniciar la ejecución de PowerShell.
Caso 3: se tiene en cuenta una dirección de correo electrónico válida para inscribir el dispositivo con restricciones para modificar los archivos en la ubicación del dispositivo. Utilice la dirección de correo electrónico de la sesión activa para la inscripción. Este caso tiene dos subcasos:

- Usar dos o más secuencias de comandos para la inscripción: cree un paquete de distribución con **setupEPMCopyContentsToTempFolderStep1.ps1** y ejecútelo como Cuenta de usuario actual. Los archivos se copian en una ubicación temporal: Cree otro paquete de distribución **setupEPMCopyContentsToTempFolderStep2.ps1** y ejecútelo como Cuenta del sistema local.

  > Si el usuario del dispositivo tiene restricciones para modificar la carpeta que contiene los archivos del paquete, copie los archivos en una carpeta temporal, compruebe la id del usuario y cree un paquete de PowerShell. El paquete de PowerShell se ejecuta con el script **setupEPMCopyContentsToTempFolderStep2.ps1**. Después de la instalación, se eliminará la carpeta temporal.

Deshabilitar/Habilitar UAC

1. Actualizar la entrada de registro para deshabilitar el control de UAC y reiniciar el equipo
2. Ejecute el paquete de PowerShell como cuenta del Cliente actual y usando setup.ps1
3. Actualizar la entrada de registro para habilitar el control de UAC y reiniciar el equipo

Crear paquete de PowerShell:

1. Verifique si los clientes necesarios están presentes en el Administrador de puntos terminales.
2. Copie los archivos en C:\Program Files\LANDesk\ManagementSuite\LANDesk\files\. Cree una subcarpeta en esta carpeta y extraiga los archivos.
3. Crear un paquete: **Distribución > Paquetes de distribución > Nuevo > Windows > PowerShell**.

   > El administrador puede distribuir los paquetes a distintos dispositivos basándose en el nivel de restricciones que tengan ajustados los dispositivos.

4. En la sección Archivo principal, introduzca el nombre del paquete y cargue setup.ps1 desde la carpeta donde se han copiado los archivos
5. En la sección Archivos adicionales, copie los archivos restantes (menos la secuencia de comandos setup.ps1) mediante **Agregar**.
6. Seleccione la cuenta del usuario actual en la sección Cuentas.
7. Haga clic en **Guardar**.

4. Crear tarea programada:
   1. Seleccione el paquete creado, haga clic con el botón derecho y seleccione **Crear tareas programadas**. Se crea una tarea programada.
   2. Arrastre el dispositivo y agréguelo a la sección del paquete programado.

3. En el Paquete programado, haga clic con el botón derecho y seleccione **Propiedades**.
4. Verifique el paquete.
5. En Tipo de tarea, seleccione **Enviar**.
6. Seleccione **Iniciar ahora** y haga clic en **Guardar**. Las tareas programadas empiezan a ejecutar la secuencia de comandos. Si la ejecución es correcta, el estado se volverá Verde.

5. Para verificar la inscripción del dispositivo, **Ajustes** > **Agregue o elimine un paquete de aprovisionamiento** > **Detalles**. Como alternativa, el administrador puede verificar la inscripción de un dispositivo en los Registros de diagnóstico del dispositivo.

7.5.8. Uso de la Inscripción en masa para dispositivos Windows

La función de registro en bloque le permite registrar rápidamente múltiples dispositivos Windows con Ivanti Neurons for MDM.

Requisitos previos:

- Las cuentas de usuario deben importarse en Ivanti Neurons for MDM utilizando Entra ID (Entra ID) Cuenta Premium.
- Todos los dispositivos deben tener instalado **Windows Configuration Designer**.

Procedimiento:

1. Enlace el Ivanti Neurons for MDM y los abonados de Entra ID. Consulte **Conexión de Entra ID a UEM para dispositivos Windows 10.**
2. Abra la aplicación de **Windows Configuration Designer** y seleccione **Aprovisionar dispositivos de escritorio**. Aparece una nueva ventana de proyecto en la pantalla.
3. Ingrese los siguientes detalles:
    - Nombre: un nombre único para su proyecto
    - Carpeta de proyecto: ubicación del dispositivo donde desee guardar el proyecto
    - Descripción: descripción opcional del proyecto

Haga clic en **Finalizar** para cerrar la ventana del nuevo proyecto y lleve a cabo una secuencia de pasos.

5. **Ajuste del dispositivo**
   Introduzca un nombre único para sus dispositivos. El nombre puede incluir un número de serie (%SERIAL%) o un conjunto aleatorio de caracteres.
6. También puede introducir una clave de producto si va a actualizar Windows, si va a configurar el dispositivo para un uso compartido o si va a eliminar un software preinstalado.
7. **Ajuste de la red**
   Además, puede configurar la red Wi-Fi a la que se conectarán los dispositivos la primera vez que se inicien. Si los dispositivos de red no están configurados, será necesaria una conexión de red con cable la primera vez que se inicie el dispositivo.
8. **Gestión de la cuenta**
   Seleccione **Inscribir en Entra ID**, introduzca una fecha de caducidad **Caducidad masiva de Token** y, a continuación, haga clic en **Obtener token en masa**.
9. Introduzca sus credenciales de Entra ID para obtener un token masivo.
10. En la página **Mantener la sesión en todas las aplicaciones**, haga clic en **No, iniciar sesión solo en esta aplicación**.
    - Haga clic en Siguiente cuando se obtenga correctamente el Token en masa y cree el paquete.
    - Se crea un usuario con un paquete de aprovisionamiento en el portal de Azure: nombre principal del usuario (like package_0ea893a5-1e93-4d21-a6b1-dc788946fd1d@miwinqe.onmicrosoft.com). Copie el archivo (herramienta ppkg de tiempo de ejecución) en un dispositivo de almacenamiento.

> El usuario Entra ID para crear el token masivo, y el usuario del paquete no deben tener MFA activado. Para verificarlo, debe realizar la unión OOBE + Entra ID en ese usuario.

Recree o sincronice el usuario del paquete (creado en Azure) para Ivanti Neurons for MDM.

Inscriba en masa un dispositivo con una unidad flash dentro del paquete de aprovisionamiento. También puede hacer doble clic en el dispositivo existente para llevar a cabo la experiencia posterior a OOBE. Si el paquete no se instaló correctamente en el primer intento, el segundo intento también fallará. Compruebe si el nuevo dispositivo se ha creado en Ivanti Neurons for MDM y Entra ID pertenece al usuario del paquete.

7.5.8.1. Inscripción en masa de Ivanti

El administrador puede inscribir múltiples dispositivos de Windows con un usuario genérico (a través de ppkg) que comienza con el prefijo **windows-bulkenroll**, y luego realiza la asignación del usuario.

Requisitos previos:

- En el Ivanti Neurons for MDM, cree una cuenta de usuario con prefijo como **windows-bulkenroll**. Por ejemplo, **windows-bulkenroll**-user1@abc.com, **windows-bulkenroll**-user2@abc.com.

Creación del paquete PPKG con Diseñador de configuración de Windows

1. Descargue e instale el **Ddiseñador de configuración de Windows**.
2. Crear nuevo proyecto.
3. Haga clic en **Aprovisionar escritorio**.
4. Introduzca el nombre del proyecto y seleccione una ruta.
5. En la sección **configurar el dispositivo**, introduzca el nombre del dispositivo.
6. En la sección **Configuración de red**, introduzca el nombre de la red (para configurar la red, si es necesario o se puede deshabilitar).
7. En la sección **Gestión de la cuenta**, seleccione **Inscribirse en el administrador local**. Introduzca **Nombre de usuario** y **Contraseña**, y haga clic en **Siguiente**.
8. En la sección **Agregar aplicaciones**, haga clic en **Siguiente**.
9. En la sección **Agregar certificados**, seleccione **Switch al editor avanzado** y haga clic en **proceder** > **Sí**.
10. Vaya a **RuntimeSettings** > **Inscripciones en el lugar de trabajo**. Introduzca **UPN** (el mismo usuario creado en Ivanti Neurons for MDM en la sección de requisitos previos). Seleccione las siguientes opciones:
    - AuthPolicy: OnPremise
    - DiscoveryServiceFullUrl: https://login.mobileiron.com
    - Secreto: introduzca la contraseña

Haga clic en **Archivo** > **Guardar**.

12. Haga clic en **Exportar** > **Paquete de aprovisionamiento**.
13. Haga clic en **Siguiente** en las pantallas siguientes y haga clic en **Generar**.
    El archivo ppkg se guarda en la ubicación especificada.

Dispositivo de provisión en modo OOBE con PPKG

Provise los dispositivos con el archivo del paquete PPKG recién creado de la sección anterior. Una vez que el dispositivo se inscribe y el registro sea exitoso, encontrará la entrada del dispositivo en el servidor MDM con el usuario que tiene prefijo como **windows-bulkenroll**.

Asignar dispositivo al usuario

1. En la página de dispositivos, haga clic en el usuario que tiene un prefijo como **windows-bulkenroll**.
2. Haga clic en **Asignar a usuario**. Se abre la ventana Asignación a la ventana de usuario.
3. Seleccione o busque el dispositivo de la lista.
4. Seleccione el dispositivo requerido.

5. Haga clic en **Asignar a usuario**. El dispositivo seleccionado se asignará al usuario.

Cuando el usuario inicia sesión en el dispositivo por primera vez, el cambio de contraseña es imprescindible.

> La opción de asignación a la opción de usuario solo está disponible para los dispositivos inscritos a granel Ivanti.

> Solo las configuraciones y aplicaciones de alcance del dispositivo funcionarán para los dispositivos inscritos en esta categoría. Las configuraciones y aplicaciones de alcance del usuario no son compatibles.

7.5.9. Cambiar ajustes del código de acceso

Esta sección contiene los siguientes temas:

- Cambiar la configuración asignada del código de acceso
- Cómo asignar una configuración diferente del código de acceso

Utilice la configuración del código de acceso asignada a un dispositivo para cambiar los ajustes del código de acceso. Usted puede:

- Cambiar los ajustes de la configuración asignada

O

- Asignar una configuración diferente del código de acceso

Los cambios que realice en la configuración afectarán a todos los dispositivos a los que esté asignada esa configuración.

Cambiar la configuración asignada del código de acceso

Procedimiento

1. Vaya a **Dispositivos**.
2. Encuentra la entrada del dispositivo en la lista.
3. Haga clic en el vínculo que aparece en la columna **Nombre**.

> Si se ha asignado alguna configuración del código de acceso, aparecerá en la pestaña Configuraciones.

En la pestaña Configuraciones, haga clic en el vínculo **Configuración de código de acceso**.

5. Haga clic en **Editar** (arriba a la derecha).
6. Realice los cambios.

Cómo asignar una configuración diferente del código de acceso

Procedimiento

1. Asegúrese de que alguien haya creado la configuración que usted necesita.
2. Vaya a **Dispositivos**.
3. Encuentra la entrada del dispositivo en la lista.
4. Haga clic en el vínculo que aparece en la columna **Nombre**.

7.5.10. Cambiar nombre del dispositivo

Los administradores pueden cambiar manualmente el nombre del dispositivo (es decir, no usando la configuración de 'Editar nombre del dispositivo').

Aplicable a:

- Dispositivos iOS supervisados
- Dispositivos tvOS supervisados
- Dispositivos macOS 10.10+

Procedimiento

1. Vaya a **Dispositivos**.
2. Encuentra la entrada del dispositivo en la lista.
3. Dé uno de los siguientes pasos:
    - Añada la columna **Nombre del dispositivo** si no está ya añadida haciendo clic en el icono del engranaje de Ajustes que hay a la derecha y seleccionando **Nombre del dispositivo**.
    - Haga clic en el enlace de la columna **Nombre** para ir a la página de detalles del dispositivo.
4. Junto al nombre del dispositivo, haga clic en el icono del lápiz para **Editar**.
5. Introduzca un nuevo nombre para el dispositivo y haga clic en el icono de la marca.
6. En el cuadro de visualización 'Sobrescribir nombre del dispositivo', revise las notas y haga clic en **Aceptar**.

El nombre cambiado se enviará al dispositivo la próxima vez que se conecte. Esta acción no podrá deshacerse.

> Si anteriormente ya se había configurado un Nombre del dispositivo predeterminado, esta acción sobrescribirá el conjunto de nombres de la configuración.

7.5.11. Encontrar y filtrar dispositivos

Esta sección contiene los siguientes temas:

- Buscar un dispositivo
- Filtrar dispositivos
- Uso de la búsqueda avanzada
- Carga de las consultas de búsqueda

Buscar un dispositivo

El Administrador de Ivanti Neurons for MDM muestra el número de grupos de usuarios duplicados y el número correspondiente de GUID para identificar los grupos duplicados, cuando se selecciona el atributo Nombre del grupo de usuarios en el generador de reglas. Además, una tabla bajo esta regla muestra la lista de los grupos de usuarios duplicados y sus detalles, como el Nombre del Grupo de Usuarios, el GUID, la Fuente y el nombre distinguido (DN).

Procedimiento

1. Vaya a **Dispositivos**.
2. Escriba el nombre del dispositivo en el campo **Buscar**. Se enumeran todos los dispositivos que contienen los caracteres.

Filtrar dispositivos

La barra de navegación lateral de Filtros tiene una lista con varias secciones que le ayudan a buscar un dispositivo concreto en la lista total de dispositivos. El asistente de Administrar filtros contiene la lista de todas la secciones que puede seleccionar para que se muestren en la barra de navegación de Filtros.

Procedimiento

1. Vaya a **Dispositivos**.
2. Haga clic en las casillas relevantes de las secciones que se listan en la barra de navegación lateral de Filtros.
   Ejemplo:
   - Desde la sección **Usuario activo**, seleccione **Sí** para que aparezcan solo los dispositivos en los que los usuarios están en estado activo.
   - Si ha asignado atributos personalizados a los dispositivos, puede filtrar los dispositivos en función de dichos atributos haciendo clic en el icono de ajustes (cog).
   - Desde la sección **Estado**, seleccione **Retirado** y **iOS** para que se muestren solo los dispositivos iOS retirados.

(Opcional) Haga clic en **Restablecer valores predeterminados** para restablecer la selección a los filtros predeterminados. La barra de navegación de Filtros muestra las secciones seleccionadas. Si desmarca todas las casillas del asistente de Administrar filtros, la barra de navegación lateral de Filtros mostrará todas las secciones.

4. Haga clic en cualquier lugar fuera del asistente de Administrar filtros para salir del asistente.
5. (Opcional) Haga clic en el icono x para cerrar la barra de navegación lateral del Filtros y haga clic en **Filtros** para volver a abrir la barra de navegación lateral.
   - Si utiliza alguna de las palabras de parada que se listan en el archivostopwords.txt, que forma parte de la configuración del servidor de Apache SOLR, las palabras no se indexarán, como resultado, las entidades que contienen las palabras de parada, no se mostrarán en los resultados de búsqueda.

- Entre los ejemplos de entidades, se incluyen dispositivos, usuarios, grupos, atributos, aplicaciones, certificados, registros de auditorías, contenido y módulos de notificación.
- Ejemplos de palabras de parada: a, un, si, ser, en, entre otras.

Uso de la búsqueda avanzada

Puede utilizar la opción de Búsqueda avanzada para buscar un dispositivo en función de reglas para identificar y ver los dispositivos con criterios específicos. Estas reglas se pueden crear usando los operadores correspondientes, como «comienza con», «termina con», «contiene», «no contiene», «no comienza con», «no termina con», «es menor que», «es mayor que», «está en el intervalo», «es igual a» y «no es igual a». Las opciones de reglas se pueden anidar juntas utilizando las opciones CUALQUIERA (O) o TODOS (Y). Los dispositivos que coinciden con las reglas se muestran debajo de la sección.

El Administrador de Ivanti Neurons for MDM muestra el número de grupos de usuarios duplicados y el número correspondiente de GUID para identificar los grupos duplicados, cuando se selecciona el atributo Nombre del grupo de usuarios en el generador de reglas. Además, una tabla bajo esta regla muestra la lista de los grupos de usuarios duplicados y sus detalles, como el Nombre del Grupo de Usuarios, el GUID, la Fuente y el nombre distinguido (DN).

Procedimiento

1. En la página Dispositivos, haga clic en el enlace **Búsqueda avanzada**. Se abre el asistente de Búsqueda avanzada.
2. Haga clic en una de las siguientes opciones:
   - **Cualquiera**: si los dispositivos tienen que cumplir al menos una de las reglas.
   - **Todas**: si los dispositivos deben cumplir todas la regla

Cree una regla que defina los criterios de búsqueda. **Por ejemplo**: "Preparado para APNS equivale a Sí".

4. (Opcional) Haga clic en **+** para crear reglas adicionales, si fuera necesario.
5. Haga clic en **Buscar**. En la página se muestran la lista de dispositivos que coinciden con los criterios de búsqueda.
   - Para los dispositivos iOS 14.0+, la ID de eSIM (EID) de un dispositivo estará disponible en la página de detalles del dispositivo. La ID de eSIM (EID) permite a los operadores asignar la SIM a un dispositivo específico. El campo de la ID de eSIM (EID) cumple con el RGPD.
   - Dado que se añaden campos de GDPR nuevos (como Dirección IP e ID de eSIM) a las versiones de Ivanti Neurons for MDM, los administrados que ya tienen GDPR configurado deben editar el perfil de GDPR si desean ocultar los campos nuevos.
   - La búsqueda avanzada muestra el estado del bloqueo de recuperación de un dispositivo.

Carga de las consultas de búsqueda

Puede ver la lista de consultas de búsqueda guardadas.

Procedimiento

1. Haga clic en Búsqueda avanzada y luego en el icono de la carpeta. La lista de las consultas de búsqueda creadas se muestra en la sección **Cargar consulta** y se muestran los detalles siguientes:
   - **Nombre de la consulta**: el nombre de la consulta cargada.
   - **Contenido de la consulta** muestra el contenido de las reglas que definen la consulta de búsqueda.
   - **Acciones**: seleccione la acción que se realizará en la consulta.
2. Haga clic en **Cargar consulta** en la columna **Acciones** para ver la lista de dispositivos que coinciden con los criterios definidos en la consulta cargada.

3. Haga clic en **Eliminar** para borrar una consulta guardada.

7.5.12. Uso del modo Propietario del dispositivo

Esta sección contiene los siguientes temas:

- Aprovisionamiento de dispositivos Android Enterprise mediante un código QR o NFC Bump
- Aprovisionamiento de dispositivos Android Enterprise mediante token de cliente

Licencia: Gold

Una vez que los dispositivos se hayan registrado, los puede designar como Propiedad de la empresa o Propiedad del empleado. Esta designación ayuda a administrar las políticas basadas en si el usuario tiene un dispositivo personal o un dispositivo propiedad de la empresa. Con la licencia correcta, podrá usar la propiedad en reglas para crear grupos de dispositivos.

Empezando con un dispositivo nuevo o con el restablecimiento de los valores de fábrica, utilice la aplicación **Provisioner** para aprovisionar el modo del propietario del dispositivo mediante una de las siguientes opciones:

- Intercambio de datos NFC (Near Field Communication)
- Escaneo de código QR

Para realizar el intercambio de datos NFC, es necesario que el dispositivo maestro o la plantilla entre en contacto físico con un dispositivo nuevo o con la configuración de fábrica para aprovisionarlo.

Para realizar un escaneo del código QR, es necesario pulsar la pantalla de un dispositivo nuevo o con la configuración de fábrica, configurar una red Wi-Fi y escanear el código cuando dispositivo esté listo para ser aprovisionado.

Durante el aprovisionamiento del modo propietario del dispositivo utilizando el código NFC o QR code, la aplicación Provisioner acepta un token de inscripción. En el registro, el token de inscripción se envía al servidor. Si está presente en el servidor y el dispositivo se asigna a un usuario, el dispositivo está correctamente registrado.

El cliente Go controlará el dispositivo una vez que esté en el modo Propietario del dispositivo y bloqueará la pantalla hasta que el dispositivo esté registrado con Ivanti Neurons for MDM para evitar que los usuarios salgan del proceso de aprovisionamiento. El modo Propietario del dispositivo también es compatible con el modo Kiosco. Para ver información sobre la configuración, vaya a: **Bloqueo y configuración de kiosco**.

Importante

- Si retira un dispositivo en el modo Propietario del dispositivo, se restablecerá la configuración de fábrica del dispositivo.
- Todos los dispositivos del modo Propietario del dispositivo pueden tener opcionalmente todas las aplicaciones del sistema habilitadas.
- Un dispositivo solo puede tener un propietario del dispositivo activo a la vez.
- Solo los dispositivos compatibles con Android Enterprise se pueden aprovisionar en modo propietario.
- Para los dispositivos Samsung KNOX Standard que estén en modo Propietario del dispositivo, se pedirá a los usuarios que activen la licencia Samsung ELM. Este aviso aparecerá también en los dispositivos Samsung que estén en modo Propietario del dispositivo cuando la aplicación de cliente Go se actualice desde una versión anterior a la versión lanzada más recientemente compatible con Ivanti Neurons for MDM. Después de la activación, se muestra el número de serie en la página de detalles del Dispositivo, que debe coincidir con el campo Dispositivo > Ajustes > Número de serie.

Aprovisionamiento de dispositivos Android Enterprise mediante un código QR o NFC Bump

Para aprovisionar dispositivos Android Enterprise mediante código QR o NFC bump, deberá descargar e instalar la aplicación Provisioner de Google Play en el dispositivo maestro.

Componentes compatibles

Versión de Provisioner: 1.3.0.

Provisioner es compatible o funciona con lo siguiente:

Elemento	Versión
SO de Android (el dispositivo que se va a aprovisionar)	• Es necesaria la versión 5.0 o versiones más recientes compatibles, si se utiliza NFC. • Es necesaria la versión 7.0 o versiones más recientes compatibles si se utiliza un código QR. El dispositivo debe ser compatible con Android Enterprise.
SO de Android (en el dispositivo maestro)	5.1 hasta la versión lanzada más recientemente. Para usar el intercambio de datos NFC, el dispositivo debe contar con NFC. No es necesario para el código QR.
Producto de servidor UEM, habilitado para Android Enterprise	Uno de los siguientes: Ivanti Neurons for MDM, o permitir Ivanti Neurons for MDM etiquetado.
Aplicación del cliente Android	Provisioner instalará automáticamente la última versión de la aplicación del cliente en el dispositivo aprovisionado.

Requisitos previos

Para aprovisionar un dispositivo de Android Enterprise para que sea un dispositivo administrado en el trabajo, debe:

- Asegúrese de que la configuración necesaria relacionada con Android Enterprise está definida y se aplicará al dispositivo registrado.

> La configuración por defecto de Android Enterprise: Work Managed Device debe estar habilitada para el dispositivo.

Habilitar Android Enterprise en el servidor.

- Tenga un dispositivo Android compatible con NFC (solo si se va usar NFC) para que sirva como dispositivo maestro, con la aplicación Provisioner instalada.
- Disponga de dispositivos compatibles con Android Enterprise para aprovisionar.

Para habilitar la transferencia Android con el fin de usarla con el intercambio de datos NFC:

Procedimiento

1. Vaya a los **Ajustes** del dispositivo.
2. Vaya a **Redes > Redes inalámbricas**.
3. En la sección **Conectividad**, seleccione **Compartir y conectar**.
4. Ponga el interruptor **NFC** en **Activado (On)**.
5. Ponga el interruptor de **Transferencia Android** en **Activado (On)**.

Los pasos para activar la transferencia Android y NFC pueden variar según cada dispositivo.

Aprovisionamiento de dispositivos de Android Enterprise para que sea un dispositivo administrado en el trabajo

Procedimiento

1. Utilizando el dispositivo maestro Android, descargue de Google Play la aplicación Provisioner e instálela.
2. Inicie Provisioner en el dispositivo maestro.
3. Seleccione el método de aprovisionamiento: NFC o código QR.
4. Pulse **Aplicación a aprovisionar** y elija la aplicación del cliente que va a instalar en el dispositivo aprovisionado:

Seleccione esta aplicación de cliente:	Para registrarse con este servidor UEM:
Ir	Ivanti Neurons for MDM
En el UEM de trabajo	(Permitir etiquetados) Ivanti Neurons for MDM

5. Rellene los campos restantes en la aplicación Provisioner. Algunos campos podrían autorrellenarse si existe un tipo de Wi-Fi compatible. Los campos de Wi-Fi no aparecen si se selecciona el código QR. Siga estas pautas:

Campo	Valor
Seleccione la aplicación que va a aprovisionar	Go o At Work
Zona horaria	Introduzca la zona horaria que se va configurar en el dispositivo
Configuración regional	Introduzca la configuración regional que se va configurar en el dispositivo
Activar todas las aplicaciones del sistema	Haga clic en la casilla para activar todas las aplicaciones del sistema
SSID de la red Wi-Fi	Introduzca la SSID de la Wi-Fi que va a usar el dispositivo de destino
Tipo de seguridad Wi-Fi	Introduzca el tipo de seguridad Wi-Fi
Contraseña Wi-Fi	Introduzca la contraseña para la Wi-Fi
Inscripción en masa	La función de inscripción en masa es opcional. Para usar la inscripción en masa, es necesario un nombre de host. Opcionalmente, también se puede introducir un nombre de usuario y seleccionar la opción de inicio rápido. Para omitir la función de inscripción en masa, estos campos se deben dejar en blanco.

6. Pulse **Continuar**.
7. Si se seleccionó **NFC**, pulse **Continuar**. La pantalla **Subir los dispositivos** aparece en el dispositivo maestro. Continúe con la sección **Intercambio de datos NFC** que aparece a continuación.
8. Si seleccionó **Código QR**, aparece la pantalla **Escanear este código QR** en el dispositivo maestro. Continúe con la sección **Código QR** que aparece a continuación.

Siga los siguientes pasos al para el intercambio de datos NFC

Confirme que el dispositivo de destino esté mostrando la pantalla de bienvenida de Android.

9. Haga «chocar» la parte posterior del dispositivo maestro con la del dispositivo destino para iniciar la transferencia NFC. Si la transferencia NFC se produce correctamente, el dispositivo de destino hará un sonido y, a continuación, comenzará a descargar la aplicación de cliente. Si no se puede establecer una conexión Wi-Fi o si el dispositivo no puede descargar la aplicación el cliente, este realizará automáticamente un restablecimiento a la configuración de fábrica.
10. Si oye un sonido o ve una pantalla que no sea la de bienvenida, puede desacoplar los dispositivos. Esto suele tardar algunos segundos. Si el dispositivo no está cifrado, comenzará el proceso de cifrado antes de continuar.
11. Puede seguir aprovisionando dispositivos adicionales «haciéndolos chocar» con el dispositivo maestro. El dispositivo de destino debe mostrar la pantalla de Bienvenida y el dispositivo maestro debe mostrar la pantalla "Subir los dispositivos".

Siga los siguientes pasos al para el aprovisionamiento con código QR.

Confirme que el dispositivo de destino esté mostrando la pantalla de bienvenida de Android.

12. Pulse la pantalla de Bienvenida de Androud en el dispositivo de destino 6 veces en el mismo punto de la pantalla.
13. Se le pedirá que configure una red Wi-Fi para que el asistente de configuración pueda descargar un lector de códigos QR en el dispositivo de destino.
14. Una vez que se haya descargado el lector de códigos QR, se habrá iniciado la cámara.
15. Sujete el dispositivo de destino algunos centímetros por encima del dispositivo maestro hasta que se haya escaneando correctamente el código QR. A continuación, el asistente de configuración procederá a descargar la aplicación del cliente. Si no puede descargar la aplicación de cliente, realizará automáticamente un restablecimiento a la configuración de fábrica.
16. Puede seguir aprovisionando dispositivos adicionales escaneando el código QR en el dispositivo maestro. El dispositivo de destino debe tener una cámara lista para escanear y el dispositivo maestro debe mostrar la pantalla "Escanee este código QR".
17. El código QR también se puede exportar pulsando el botón Compartir. Las opciones de exportación que se ofrecen variarán según el dispositivo.

Aprovisionamiento de dispositivos Android Enterprise mediante token de cliente

Puede aprovisionar un dispositivo Android Enterprise en modo Propietario del dispositivo mediante un token de cliente de marca en lugar de utilizar los métodos de NFC bump o código QR. Este método le permite iniciar sesión en un dispositivo con un token, lo cual facilita la instalación automática del cliente Go o At Work y el aprovisionamiento en el modo Propietario del dispositivo:

> Los tokens de cliente de marca son compatibles con los dispositivos aprovisionados con cuentas gestionadas de Google Play, que utilizan Android 6 o versiones más recientes compatibles. Para obtener más detalles, consulte la guía para desarrolladores de UEM de Android. https://developers.google.com/android/work/prov-devices#Key_provisioning_differences_across_android_releases.

Requisitos para usar este método:

- Debes estar registrado con una cuenta Android Enterprise.
- El dispositivo debe ser compatible con Android Enterprise.
- El dispositivo debe usar desde Android 6 hasta la versión lanzada más recientemente.
- Debe tener dispositivo nuevo o con la configuración de fábrica.

Para configurarlo (para dispositivos con Android 5.0+):

Procedimiento

1. En ellvanti Neurons for MDMportal de , vaya a **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Seleccione **Bloqueo y kiosco: Android Enterprise**.
4. Se muestra la página **Crear configuración de bloqueo y kiosco: para Android Enterprise**.

Introduzca un nombre y descripción para la configuración.

5. Elija un tipo de bloqueo.

Haga clic en **Dispositivos administrados en el trabajo (Propietario del dispositivo)**.

6. Aparecerán las opciones de ajustes de bloqueo de Propietario del dispositivo.

Opcionalmente, también puede

- Desactivar la Wi-Fi o los ajustes de Wi-Fi
- Desactivar cámara
- Desactivar Bluetooth
- No permitir ajustes de Bluetooth
- Desactivar captura de pantalla
- Silenciar volumen principal
- No permitir el Control de aplicaciones
- No permitir credenciales
- No permitir emisiones de emergencia
- No permitir redes móviles
- No permitir tethering
- No permitir VPN
- No permitir configuración predeterminada de fábrica
- Activar protección de restablecimiento de valores de fábrica.

> Opcionalmente, puede especificar una lista de Id. de cuentas Google autorizadas (un valor entero) que pueda aprovisionar el dispositivo después del restablecimiento de fábrica o dejar el cursor sobre el icono de ayuda para ver ayuda sobre cómo recuperar Id. de cuentas autorizadas).

No permitir Modificar cuentas

- Desactivar NFC (transferencia de salida)

- No permitir llamadas salientes
- No permitir arranque seguro
- No permitir Compartir localización
- No permitir características de depuración
- Asegurar Verify Apps
- No permitir SMS
- No permitir Silenciar micrófono
- No permitir hora automática
- No permitir zona de hora automática
- Desactivar itinerancia de datos
- No permitir suspensión de Wi-Fi
- Restringir métodos de entrada
- Restringir servicios de accesibilidad
- Desactivar transferencia de archivos USB
- Desactivar elementos multimedia externos
- Desactivar el protector de teclado (no tendrá efecto si está configurado el PIN/código de acceso)
- Mantener la pantalla encendida mientras esté conectada a la corriente
- No permitir la creación de ventanas
- Saltar consejos para el primer uso

En la sección **Activar/desactivar aplicaciones del sistema**, puede optar opcionalmente por desactivar las siguientes aplicaciones del sistema:

7. También puede elegir habilitar el **Modo kiosco**.

Elemento	Versión
Aplicaciones del sistema predefinidas	
Cámara integrada	Haga clic en el botón de alternar para **ENCENDER** o **APAGAR** la aplicación de Cámara integrada.
Teléfono integrado	Haga clic en el botón de alternar para **ENCENDER** o **APAGAR** la aplicación de Teléfono integrada.
Nombre del paquete de la aplicación del sistema	Para activar o desactivar cualquier otra aplicación del sistema que no sean las aplicaciones del sistema predefinidas, haga clic en el icono + (más) y añada el nombre del paquete de aplicaciones del sistema. Para eliminar la aplicación del sistema, haga clic en el icono - (menos).

Aparecerán los siguientes ajustes:

- Activar el modo de Bloqueo de tarea
- Entrar en el modo kiosko automáticamente (solo en la configuración inicial)

- Desactivar los ajustes rápidos
- Permitir al usuario acceder a los ajustes Wi-Fi
- Permitir al usuario acceder a los ajustes Bluetooth
- Permitir al usuario acceder a los ajustes de localización
- Permitir al usuario retrasar las actualizaciones de la aplicación
- Permitir al usuario acceder a los ajustes de fecha y hora
- Permitir al usuario acceder a los ajustes de red móvil
- Permitir al usuario seleccionar el idioma
- Activar dispositivo compartido (seleccione cualquiera de las siguientes opciones)
  - Activar inicio de sesión
  - Activar cierre de sesión (proporcione el ajuste de tiempo de espera por inactividad en horas)

Opcionalmente, seleccione las opciones de imagen de marca personalizada o predeterminada de la lista desplegable.

8. También puede crear un PIN de salida del kiosco para salir del modo kiosco.
9. También puede crear una lista de permitidos de aplicaciones que estarán disponibles para los usuarios en el modo kiosco.

Aprovisionar el dispositivo

Procedimiento

1. Encienda el dispositivo e introduzca su contraseña Wi-Fi. Es posible que su dispositivo le solicite una contraseña diferente.
2. En la pantalla **Verificar cuenta** introduzca el token de Android Enterprise. Haga clic en **Siguiente**.
3. En la pantalla **Servicios de Google**, haga clic en **Instalar**.
4. Acepte de los Términos y condiciones.
5. En la pantalla Configurar dispositivo de trabajo, haga clic en **Siguiente**. Se descargará el cliente Go o At Work y se instalará en el dispositivo. Ahora, el dispositivo entrará en modo Propietario del dispositivo.

Temas relacionados

- Uso de la inscripción en masa para Android
- Grupos de dispositivos

7.5.13. Dispositivo administrado con perfil profesional

Dispositivo administrado con Perfil de trabajo en el Dispositivo propiedad de la empresa es un modo en el que el dispositivo con Android Enterprise es un Dispositivo propiedad de la empresa en el que los datos personales están separados del resto. Este modo admite dos perfiles en los que se pueden desplegar aplicaciones de trabajo dentro del perfil administrado al mismo tiempo que el usuario sigue manteniendo su parte personal. El modo Dispositivo administrado con Perfil de trabajo en el Dispositivo propiedad de la empresa se crea distribuyendo una configuración de Dispositivo administrado con Perfil de trabajo a un dispositivo que se aprovisiona en modo propietario de dispositivo.

Para más información sobre el Dispositivo administrado con opciones de bloqueo del perfil profesional, consulte **Bloqueo y kiosco: Android Enterprise**.

> Este modo requiere Android 8.0 hasta la versión más reciente.

Las configuraciones de aplicaciones, las aplicaciones que comparten widgets entre varios perfiles, los alias de certificados de cliente y los certificados de ID se pueden aplicar al Dispositivo administrado con Perfil de trabajo.

Las siguientes configuraciones se pueden aplicar a los Dispositivos administrados con perfil profesional:

- Código de acceso avanzado
- VPN siempre activada
- Certificado
- Certificado de identidad
- Cuenta de Google
- Código de acceso
- Restricción para teléfonos Samsung
- Defensa contra amenazas
- Wi-Fi
- Permisos predeterminados del tiempo de ejecución de las aplicaciones
- Certificación SafetyNet
- Código de acceso
- Medidas locales de Threat Defense

7.5.14. Uso de la inscripción en masa para Android

La función de inscripción en masa le permite registrar rápidamente múltiples dispositivos Android con Ivanti Neurons for MDM.

Licencia: Silver

Realice las siguientes tareas antes de utilizar la inscripción masiva:

1. Instalar Android SDK, que incluye Android Debug Bridge (adb), en el ordenador que se está usando para registrar los dispositivos. Para obtener más información acerca de Android Debug Bridge, visite: **http://developer.android.com/tools/help/adb.html.**
2. Habilitar la depuración de USB.
   el procedimiento para habilitar la depuración de USB en dispositivos Android varía dependiendo de la versión de Android. Consulte: **http://developer.android.com/tools/device.html** para obtener más información sobre cómo habilitar la depuración de USB.
3. Instalar el cliente Go en cada dispositivo.
4. Conectar los dispositivos mediante el cable USB al ordenador de aprovisionamiento que se usará para registrarlos.

Se puede iniciar y registrar Go en un servidor utilizando el shell de Android Debug Bridge (adb). Android Debug Bridge es una herramienta que se puede utilizar desde la línea de comandos de Windows o en la utilidad Terminal de iOS. Le permite comunicarse con un dispositivo Android conectado. Desde el shell de adb, el formato de comandos es el siguiente:

> adb shell

$ am start -a android.intent.action.MAIN -d "mirp://na1.mobileiron.com?key=value&key=value" -n com.mobileiron.anyware.android/com.mobileiron.polaris.manager.ui.StartActivity

> El Protocolo de registro (**mirp**) se usa para codificar los datos relevantes para el registro.

Las claves y valores válidos son los siguientes:

Clave	Valor
usuario	Dirección de correo electrónico del usuario que se habría escrito en el campo de nombre de usuario si se usara iReg. Obligatorio.
contraseña	Contraseña del usuario
pin	PIN de registro para el usuario
quickStart	**Cuando se establece en TRUE:** aparece la pantalla de presentación, pero durante menos tiempo. En la pantalla de bienvenida, cuando el control de número cambia al botón Continuar, la pantalla avanzará automáticamente sin tener que pulsar Continuar. Además, este flujo de aprovisionamiento simplificado se produce en todos los dispositivos: • Las indicaciones de privacidad y acceso directo para el usuario se omitirán. • En los dispositivos de Zebra, el cliente debe conceder privilegios de administrador a sí mismo sin un aviso al usuario. Requiere una versión mínima de Zebra MX 4.3. **Cuando se establece en FALSE:** aparece la pantalla de presentación como siempre y el usuario tendrá que pulsar Continuar en la pantalla de bienvenida. Opcionalmente, se puede poner de forma predeterminada en FALSE.

> Para usar la inscripción en masa, es obligatorio utilizar una contraseña, PIN o token.

Este comando de ejemplo especifica un servidor, un usuario, una contraseña, un PIN y un inicio rápido:

am start -a android.intent.action.MAIN -d "mirp://ppp183.auto.mobileiron.com?user=miadmin@auto0001.mobileiron.com&password=P@$$W0R3&pin=12345&quickStart=true" -n com.mobileiron.anyware.android.qa/com.mobileiron.polaris.manager.ui.StartActivity

Ejemplo de secuencia de comandos de inscripción en masa

puede utilizar esta secuencia de comandos como ejemplo a la hora de diseñar su propia secuencia de comandos de inscripción en masa. Esta secuencia de comandos de ejemplo registra todos los dispositivos conectados al equipo de aprovisionamiento con el mismo usuario y contraseña.

for i in `adb devices | grep -v devices |

do

eco "Registering $i"

adb -s $i shell "am start -a android.intent.action.MAIN -d \"mirp://<nombre_de_servidor?user=dirección_de_correo_electrónico_del_usuariopassword=contraseña

done

Posibles mensajes de error

Aquí le mostramos algunos errores potenciales que podría encontrarse al usar la inscripción en masa.:

Error	Solución
mirp scheme not found (no se encontró el esquema mirp)	Comando de ejemplo usando un esquema mirp: am start -a android.intent.action.MAIN -d "xxxmirp://?
La URL no es válida	Aparece si no se envía ninguna cadena de datos. Verifique que la URL es correcta.
No server information found (No se encontró información sobre el servidor)	Falta información sobre el servidor o se introdujo incorrectamente.
No user information found (No se encontró información sobre el usuario)	Verifique que se introdujo la clave del usuario.
No password/pin information found (no se encontró información sobre la contraseña/PIN)	Verifique que se introdujo un PIN O una contraseña.

Cuando hay varios perfiles creados para la inscripción masiva:

- Un dispositivo Android Enterprise totalmente gestionado e inscrito de forma nativa recibe el atributo personalizado que se creó con el primer perfil.
- Al migrar dispositivos, si el dispositivo está presente en un perfil de inscripción masiva, los atributos personalizados definidos para el dispositivo migrante del perfil de inscripción masiva se aplicarán al dispositivo en la migración. Este comportamiento es el mismo para los dispositivos Android Enterprise migrados totalmente gestionados porque recibe el atributo personalizado del primer perfil.

Además, todos los perfiles creados para ese dispositivo en particular se ven como activos.

7.5.15. Inscripción masiva mediante carga de archivos CSV

La inscripción en masa permite registrar varios dispositivos Android utilizando identificadores de dispositivos. Puede cargar el archivo CSV para añadir dispositivos en masa.

Procedimiento

1. En la página **Dispositivos**, haga clic en la pestaña **Inscripción en masa**. Aparecerá la página **Inscripción en masa**.
2. Haga clic en **Añadir**.
3. En el campo de texto **Nombre del perfil**, introduzca el nombre del Perfil. Opcionalmente, también puede clic en **+Añadir descripción** para proporcionar una descripción para el archivo CSV.
4. En la sección **Cargar CSV**, haga clic en **Descargar plantilla de CSV** para descargar la plantilla CSV. Con el formato existente, se puede editar el archivo para añadir dispositivos.

> Permite hasta 200000 fila simultáneamente en el CSV de inscripción en masa.

5. Después de haber editado y guardado el archivo CSV, haga clic en **Cargar CSV** para cargar el archivo CSV. Aparecerá una confirmación si se ha cargado correctamente.

> Las filas con información incorrecta pueden resultar en un error de carga del CSV. Cada registro deberá incluir, al menos, el número de serie y la información del fabricante o el valor IMEI.

> para eliminar el archivo CSV añadido, haga clic en el icono 'menos'. Para elegir un archivo CSV diferente para cargar, haga clic en el enlace **Elegir un archivo diferente**.

6. Opcional: seleccione **Asignación de atributos personalizados sin token** para inscribir en masa todo tipo de dispositivos sin generar un token. Esta opción no está seleccionada de forma predeterminada.

La inscripción masiva sin token también se puede aplicar cuando se proporciona el IMEI o la combinación de número de serie y fabricante (con o sin atributos personalizados) en el archivo CSV cargado. Sin embargo, el registro del dispositivo depende de la corrección de los valores de los atributos cargados en el archivo CSV. En el siguiente cuadro se explican los escenarios sobre el resultado basados en la combinación de atributos y valores introducida para la inscripción en masa:

Situación	**Valores de los atributos introducidos**			**Estado del registro del dispositivo**
	IMEI	**Número de serie**	**Fabricante**	
1	Correcto	Incorrecto	Incorrecto	El dispositivo está registrado
2	Incorrecto	Correcto	Correcto	El dispositivo está registrado
3	Incorrecto	Incorrecto	Correcto	El dispositivo no está registrado
4	Incorrecto	Correcto	Incorrecto	El dispositivo no está registrado

> El nombre del fabricante distingue entre mayúsculas y minúsculas.

7. En el campo **Seleccionar usuario**, debe seleccionar un usuario.
   El token de inscripción aparecerá en la columna Token de inscripción. Para actualizar la ficha de inscripción, haga clic en **Actualizar**.
   La fecha de caducidad del token se muestra en la sección **Caducidad del token** . Para ampliar el período de caducidad del token, haga clic en **Ampliar**. En el campo **Ampliar hasta**, introduzca el número de días en el que quiere ampliar el token.

> El número de días especificado debe estar comprendido entre 7 y 999. El token predeterminado caducará en un plazo de 7 días. Esta página no se mostrará si ha seleccionado la opción **Asignación de atributos personalizados sin token**.

8. Haga clic en **Hecho**.

Después de la carga, se muestran los siguientes detalles del archivo CSV cargado en una tabla en la página **Perfiles de registro en bloque**.

Ajuste	Descripción
Nombre del perfil	El nombre del perfil.
Descripción	Alguna descripción sobre el perfil.
Última modificación	La fecha de la última vez que se modificó el archivo CSV.
TIPO	Para perfiles autogestionados → Autogestionado
N.º de dispositivos	El número de dispositivos en la inscripción en masa.
Usuario asociado	El nombre del usuario asociado.
Nombre de usuario	Especifica el usuario asociado con el dispositivo. Necesario cuando la asignación de dispositivo a usuario está habilitada. El usuario debe existir en Ivanti Neurons for MDM.
Acciones	Puede llevar a cabo cualquiera de las siguientes acciones: **Descargar inventario existente**: haga clic en este botón para descargar los detalles de todos los dispositivos disponibles en el perfil. **Ver**: haga clic en este enlace para ver los detalles de los perfiles cargados en masa para el registro. **Editar**: haga clic en este botón para editar los detalles del perfil. Esta opción solo está disponible cuando se selecciona la opción de dispositivo único. **Eliminar**: haga clic en este vínculo para eliminar el perfil. En la ventana de confirmación, haga clic en **Sí** para confirmar que desea borrar el perfil cargado.

> para el registro debe usarse el token generado mientras se cargaba el archivo CSV. Si se introduce el token incorrecto, se redirigirá al proceso IReg normal, donde debe introducirse la Id./contraseña.

Acciones

Al visualizar los perfiles de Inscripción masiva desde la sección Ver detalles del perfil, puede realizar otras tareas desde la pestaña Acciones, presente en la página Ver detalles del perfil.

- **Agregar más dispositivos**: utilice esta opción para agregar más dispositivos a un perfil. Debe proporcionar bien **Número IMEI** o **Número de serie**, o ambos, **Fabricante**, y opcionalmente la información de **Atributos personalizados** y, a continuación, hacer clic en **Guardar**.
- **Modificar configuración**: utilice esta opción para modificar una configuración existente. Puede agregar **teclas específicas de Ivanti**, hacer cambio a **teclas predefinidas adicionales del sistema de Android** o **teclas del sistema personalizadas de Android** y a continuación haga clic en **Actualizar**.
- **Generar código QR**: utilice esta opción para generar un código QR para la inscripción en masa de perfiles.
- **Actualizar Token**: utilice esta opción para actualizar un token o ampliar su validez. La validez puede fijarse entre 7 y 999 días o puede fijarse en **Nunca caduca**.
- **Cambiar usuario asociado**: utilice esta opción para cambiar un usuario asociado. Es necesario buscar y seleccionar el usuario en la ventana emergente **Cambiar Usuario Asociado**, y luego hacer clic en **Aplicar**.
- **Editar**: utilice esta opción para editar los dispositivos del perfil seleccionado. Debe seleccionar los dispositivos y hacer clic en el botón **Editar**.
- **Eliminar**: utilice esta opción para eliminar dispositivos del perfil seleccionado. Después de seleccionar los dispositivos y de hacer clic en el botón Eliminar, aparecerá una ventana de confirmación en la pantalla. Haga clic en **Eliminar**.

> Los dispositivos autogestionados tienen estados de dispositivo distintos. Puede encontrar más detalles **Uso de la inscripción móvil de Samsung Knox**.

7.5.16. Device_to_User_BulkEnrollment

File not found!

7.5.17. Uso de la inscripción móvil de Samsung Knox

La inscripción móvil de Samsung Knox permite a los administradores registrar dispositivos Samsung cualificados en Ivanti Neurons for MDM. Mediante la Inscripción móvil de Knox, se puede enviar un dispositivo directamente desde un vendedor autorizado a un usuario final, y el cliente de Go Android se descargará automáticamente con los datos de inscripción precargados. Para obtener más información, consulte **Inscripción móvil de Samsung Knox para Android Enterprise**.

Requisitos

- Lista de dispositivos por IMEI
- Archivo CSV que contiene una lista de dispositivos con un IMEI o número de serie y, opcionalmente, un nombre de usuario y una contraseña de inscripción.
- Neuronas Ivanti for MDM (versión actual).
- Cuenta Samsung Knox aprobada para la inscripción móvil
- Dispositivos compatibles de Samsung: La lista de dispositivos Samsung compatibles está disponible en **aquí**.

7.5.18. Inscribir dispositivos de Oculus

Ivanti Neurons for MDM ahora puede administrar dispositivos de Quest for Business (dispositivos Oculus). Actualmente, Meta es compatible con dispositivos de Oculus for Business (OFB) y Quest for Business (QFB) para MDM. Debe llevar a cabo algunas tareas básicas en la consola Meta para hacer que los dispositivos estén listos para MDM y, a continuación, registrarse con Ivanti Neurons for MDM.

Puede inscribir la flota de dispositivos Oculus en el Gestor de dispositivos de la consola de Meta Workplace. Debe iniciar sesión en el Oculus Business Workplace mediante las credenciales compartidas con el correo electrónico registrado. En la página de Inicio, se mostrará la información de Todos los dispositivos en la sección de Flota de dispositivos. La sección de Flota de dispositivos proporciona una vista general de todos los dispositivos disponibles en Administración de dispositivos. Estos detalles incluyen el Nombre de dispositivo, Estado de dispositivo, SO (Sistema operativo), Modelo, etc.

Esta sección contiene los siguientes temas:

- Requisitos previos para inscribir los dispositivos Oculus
  - Cómo ajustar una aplicación de MDM en el Administrador de dispositivos
  - Cómo ajustar el dispositivo Oculus

Registre un dispositivo OFB con MobileIron Go

  - En la consola de Ivanti Neurons for MDM
  - En clientes de Go

Requisitos previos para inscribir los dispositivos Oculus

Cómo ajustar una aplicación de MDM en el Administrador de dispositivos

Los dispositivos/auriculares se proporcionan y actualizan con, al menos, la versión **28** de **Oculus for Business**. En la consola de Meta, el administrador debe ajustar un MDM en el Administrador de dispositivos y asignar los dispositivos Oculus al servicio MDM específico.

Procedimiento

1. En la página de inicio de **Oculus Business Workplace** , seleccione **Aplicaciones**.
2. En la **Biblioteca de aplicaciones**, haga clic en la aplicación MDM de terceros que desee instalar y, a continuación, haga clic en **Actualizar**.
3. Seleccione el MDM correcto para la aplicación en la lista de **Administración de dispositivos móviles** y, a continuación, haga clic en **Actualizar aplicación**.
4. Haga clic en el auricular del dispositivo Oculus en el que desee instalar el MDM. La información del dispositivo aparecerá en pantalla.
5. En la pestaña **Acerca de**, baje hasta **Administrador de dispositivos móviles**.
6. Haga clic en el botón **Editar** que hay junto a la opción **Autoridad de MDM**.

> Por defecto, se seleccionará la opción Administrador de dispositivos de Oculus. Debe seleccionar la aplicación MDM Authority y seleccionar **MobileIron Go** en la lista de aplicaciones de MDM Authority.

Haga clic en **Guardar**. El dispositivo se restablece automáticamente y, a continuación, deberá configurar el dispositivo Oculus mediante la aplicación de configuración.

Cómo ajustar el dispositivo Oculus

Puede agregar dispositivos de auriculares de Oculus Quest 2 mediante la aplicación de Configuración del dispositivo. Esta aplicación debe compartirse con los usuarios necesarios para que estos puedan descargar e instalar la aplicación en sus dispositivos Android.

Procedimiento

1. En la sección **Flota de dispositivos**, haga clic en **Dispositivos sin configurar**.
2. Haga clic en **Obtener la aplicación de configuración**. La página **Enviar enlace de descarga** aparece en la pantalla.
3. Seleccione uno o más miembros del equipo en la lista o haga clic en **Agregar destinatario** para seleccionar en la lista.
4. Haga clic en **Enviar enlace**. Los usuarios seleccionados recibirán un correo electrónico con un enlace para instalar la aplicación de **Configuración del dispositivo**.
5. Haga clic en el enlace **Descargar la aplicación de configuración del dispositivo** en el correo electrónico para instalar la **Aplicación de configuración del dispositivo** en su dispositivo Android.

> Después de descargarla, esta aplicación no aparecerá en la tienda de aplicaciones de su dispositivo. Debe obtenerlo desde la sección de Descargas del dispositivo e instalarlo.

Abra la aplicación **Oculus for Business** desde su dispositivo Android.

7. ENCIENDA los dispositivos Oculus pulsando el botón de encendido durante 2 segundos.
8. Active el Bluetooth y coloque el dispositivo Android cerca de los dispositivos Oculus hasta que se complete la configuración.
9. Busque dispositivos Oculus mediante el Bluetooth de su dispositivo Android.
10. Cuando se encuentre el dispositivo Oculus necesario, debe conectarlo a una red WiFi para completar la configuración.
11. Haga clic en **Introducir información de Wi-Fi** y proporcione el Nombre de la red y la contraseña y haga clic en **Guardar**. Ahora, el dispositivo Oculus está conectado a la red WiFi.
12. Haga clic en **Iniciar configuración**. Aparece una notificación en pantalla indicando el progreso de la configuración, y no debe cerrar la aplicación ni manipular los auriculares durante la configuración.
    Aparece una confirmación en pantalla. Puede seguir buscando más dispositivos mediante el botón **Encontrar más dispositivos**.

Registrar un dispositivo OFB con MobileIron Go

En la consola de Ivanti Neurons for MDM

Se puede registrar un dispositivo OFB con MobileIron Go en la consola de Ivanti Neurons for the MDM. No obstante, la configuración del modo Work Managed Device Non-GMS (AOSP) (en **Configuraciones**) debe distribuirse a estos grupos de dispositivos OFB.

En clientes de Go

Se puede registrar un dispositivo OFB en el cliente de MobileIron Go. Debe llevar a cabo las tareas siguientes para registrar el dispositivo OFB:

- Después de completar la configuración mediante la aplicación de configuración de OFB, continúe con las instrucciones en pantalla del auricular de OFB y complete la configuración del dispositivo.

- La aplicación MobileIron Go se inicia automáticamente y debe proporcionar las credenciales de inicio de sesión para completar el registro siguiente las instrucciones de MDM.

Ahora, el dispositivo está aprovisionado en modo DO y está ajustado para administrarse con MDM.

7.5.19. Activar Bluetooth en un dispositivo

Aplicable a:

- iOS 11,3+
- macOS 10.13.4+

Se puede activar o desactivar Bluetooth en un dispositivo.

Procedimiento

1. Navegue hasta el dispositivo en la **página de Dispositivos**.
2. Lleve a cabo una de las siguientes acciones:
    - Seleccione los dispositivos de la lista.
    - Haga clic en el nombre del dispositivo para visualizar la página de detalles del Dispositivo.
3. Desde el menú **Acciones** haga clic en **Activar/desactivar Bluetooth**.
4. Haga clic en **Aceptar**.

Se insertarán los cambios en el dispositivo la próxima vez que ingrese.

7.5.20. Programar actualización de iOS

Aplicable a:

- Dispositivos de Inscripción de dispositivos iOS 9.0+ supervisados
- Dispositivos iOS 10.3+ supervisados.

Programa una actualización de un dispositivo iOS para la última versión disponible de iOS. El menú **Dispositivo** > **Acciones** opción **Actualizar la versión de SO** para dispositivos de iOS supervisados muestra una lista con solo aquellas versiones de iOS que se aplican al dispositivo.

Procedimiento

1. Navegue hasta el dispositivo en la página **Dispositivos**.
2. Haga clic en el nombre del dispositivo para visualizar la página de detalles del Dispositivo.
3. Desde el menú **Acciones**, haga clic en **Actualizar la versión del SO**.
4. En el asistente de **Actualizar la versión de SO**, revise la versión de iOS y seleccione la versión de SO en la lista desplegable de **Actualizar a versión**.

> Si introduce una versión igual o anterior, aparecerá un mensaje de error que indicará que al versión iOS de destino debe ser superior a la versión actual.

5. Haga clic en **Actualizar**.

Cuando el dispositivo iOS se conecte, se programará para actualizar la versión de iOS más reciente disponible. Si el dispositivo tiene un código de acceso, después de que MDM envíe la actualización al dispositivo, este pone en cola la actualización y se pide al usuario que introduzca su código de acceso para iniciar la instalación. Para más información, consulte las **Actualizaciones de software**.

7.5.21. Reinstalar aplicaciones del sistema iOS

Aplicable a:

- Dispositivos iOS 11.3+.

Vuelva a instalar las aplicaciones del sistema iOS borradas en dispositivos iOS.

Procedimiento

1. Navegue hasta la **Página de dispositivos**. Como alternativa, también puede hacer clic en el nombre del dispositivo y realizar esta acción desde la página Detalles del dispositivo.
2. Seleccione uno o más dispositivos iOS.
3. Desde el menú **Acciones**, haga clic en **Volver a instalar aplicaciones iOS del sistema**.
4. En el cuadro de visualización «Volver a instalar aplicaciones iOS del sistema», seleccione una o más aplicaciones disponibles del sistema para instalar en los dispositivos.
5. Haga clic en **Reinstalar aplicaciones**.

Las aplicaciones se instalarán en los dispositivos de iOS seleccionados y compatibles cuando los dispositivos se conecten. Las aplicaciones del sistema instaladas de este modo no se considerarán aplicaciones administradas. Si no se ha seleccionado ningún dispositivo compatible, usted recibirá un mensaje de que las aplicaciones del sistema no se instalarán en dichos dispositivos.

Para más información, consulte las **Actualizaciones de software**.

7.5.22. Asignar un dispositivo a un nuevo usuario

Es posible que sea necesario volver a aprovisionar un dispositivo registrado existente para un nuevo usuario, si ha habido un cambio de funciones del usuario o si ha cambiado la relación del usuario anterior con la empresa. Estos pasos ayudan a evitar que haya que retirar y volver a registrar el dispositivo.

Procedimiento:

1. Navegue hasta el dispositivo en la **página de Dispositivos**.
2. Haga clic en el nombre del dispositivo para visualizar la página de detalles del Dispositivo.
3. Haga clic en el icono **Asignar al usuario** .

> También puede seleccionar un dispositivo en la página **Dispositivos** y hacer clic en la opción **Asignar a usuario** del menú **Acciones** .

Empiece a introducir los nombres de usuarios en **Buscar usuario**... .

5. Seleccione al usuario deseado.
6. Haga clic en **Asignar al usuario**.
   El dispositivo se aprovisionará para ese usuario.

> Quizá se dé cuenta de que en los casos basados en el usuario y basados en licencias, puede asignar un dispositivo a un usuario que ha excedido el límite de dispositivos asignados. Esto ocurre porque la intención de la función de límite de dispositivos es limitar el registro de dispositivos para admitir los casos de BYOD («Bring Your Own Device»).

En ambas licencias, las basadas en el dispositivo y las basadas en el usuario, la consecuencia es la imposición de un límite de dispositivos. Para las licencias basadas en dispositivos, el coste para el consumidor final no cambia porque el número total de dispositivos del sistema se mantiene igual. Para las licencias basadas en el usuario, la ausencia de esta comprobación beneficia al cliente. Por ejemplo, imagine a cinco usuarios, del U1 al U5, con cinco dispositivos cada uno. Con el sistema de licencias basadas en el usuario, se consumirían cinco licencias. Si, de lo contrario, dos de los dispositivos del U4 y el U5 se pasan al U1y al U2, el consumo de licencias se REDUCIRÁ de cinco a tres.

7.5.23. Reasignar un dispositivo Android

El administrador puede transferir la propiedad de un dispositivo Android de un usuario a otro. Durante el proceso de reasignación, el perfil de gestión del dispositivo se reconfigurará o reasignará del usuario actual al nuevo usuario en modo Android Enterprise. La reasignación se puede realizar en todos los dispositivos de Android Enterprise excepto en los dispositivos de Android Management API (AMAPI) y no se puede realizar en los dispositivos de Android Enterprise de Google Domain.

> La reasignación de dispositivos solo puede realizarse con los dispositivos en el mismo modo. Por ejemplo, un dispositivo en modo Dispositivo gestionado por el trabajo puede reasignarse a otro usuario en el mismo modo.

El proceso de reasignación de dispositivos tendrá los estados siguientes:

- Iniciado
- Éxito
- Error
- Pendiente

Puede ver el estado de la última reasignación de un dispositivo en la página **Detalles del dispositivo** > pestaña **Información general** > **Estado de la última reasignación**.

Procedimiento

1. Vaya a **Dispositivos**.
2. Seleccione uno o más dispositivos de la lista.
3. En la lista **Acciones**, haga clic en **Asignar al usuario**.
4. También puede hacer clic en el nombre de cualquier dispositivo. Se abre la **página de información del dispositivo**. Haga clic en el icono **Asignar a usuario** para acceder a la pantalla Asignar a usuario y seleccionar el usuario deseado.
5. Haga clic en **Asignar al usuario**. Las opciones seleccionadas se validarán para comprobar si los dispositivos seleccionados pueden reasignarse a los usuarios seleccionados o no.
   Tras la validación y reasignación correctas, aparece un mensaje de confirmación en la pantalla.

> Si ha seleccionado un número máximo de 10 dispositivos, aparecerá en pantalla el mensaje "Asignación iniciada". Si ha seleccionado 11 o más dispositivos, aparecerá en pantalla la ventana emergente "Validación en curso".

> La reasignación de dispositivos Android es una solución innovadora creada exclusivamente para eliminar los datos sobrantes del usuario registrado anterior y solo está disponible en la SKU SUEM-Premium.

7.5.24. Forzar el ingreso de un dispositivo

Los dispositivos deben comunicarse con Ivanti Neurons for MDM (ingresar) para proporcionar y recibir información. Los ingresos se programan a intervalos regulares. También se puede pedir a un dispositivo que ingrese a petición. Forzar el ingreso del dispositivo puede acelerar el proceso de aplicación de configuraciones, actualizar {{políticas}}, etc.

Procedimiento

1. Vaya a **Dispositivos > Dispositivos**.
2. Seleccione los dispositivos.
3. Haga clic en **Acciones**.
4. Seleccione **Forzar ingreso**.
5. Opcionalmente, también puede hacer clic en el enlace del nombre del dispositivo para ir a la página de detalles del Dispositivo, hacer clic en el icono **Forzar ingreso**  y, luego, clic en **Aceptar**.

> Si hay un error en el extremo del dispositivo mientras se procesa el comando de instalación de configuración durante el ingreso, Ivanti Neurons for MDM no reintentará instalar la configuración del dispositivo durante los siguientes ingresos automáticamente. El administrador tendrá que volver a intentar instalar la configuración manualmente desde la página de detalles del dispositivo. Para ello, vaya a la pestaña Configuración, seleccione la configuración del error y haga clic en **Reintentar la instalación**.

7.5.25. Encontrar un dispositivo

Si ha habilitado la característica Encontrar para un dispositivo, puede mostrar la última localización para dicho dispositivo. Debe editar la **configuración de privacidad** para habilitar la obtención de datos sobre localización y aplicar la configuración al dispositivo para que el dispositivo habilite esta característica. También es necesario que el dispositivo admita esta característica y los usuarios deben aceptar compartir sus datos sobre localización.

Procedimiento

1. Navegue hasta el dispositivo en la página **Dispositivos**.
2. Haga clic en el vínculo que aparece en la columna **Nombre**.
3. En la pestaña **Información general**, haga clic en el enlace que aparece en **Localización del dispositivo**.

Se mostrarán los siguientes detalles en la página:

Nombre del campo	Descripción
Ubicado por última vez en	Muestra la fecha y le hora en la que se localizó por ultima vez al dispositivo.
Coordenadas	Muestra la latitud (posición norte-sur) y longitud (posición este-oeste) del dispositivo.

También podrá encontrar en la página el mapa con la localización del dispositivo.

7.5.26. Bloquear un dispositivo

Puede provocar el bloqueo de pantalla de un dispositivo. El bloqueo funciona de forma algo diferente dependiendo del dispositivo.

Procedimiento

1. Vaya a **Dispositivos > Dispositivos**.
2. Seleccione el dispositivo.
3. Haga clic en **Acciones**.
4. Seleccione **Bloquear**.
5. También puede hacer clic sobre el enlace del nombre del dispositivo para acceder a la página Detalles del dispositivo y hacer clic en el icono **Candado**  y en **Aceptar**.
6. Para las aplicaciones Android AppConnect, el comando Bloquear bloquea al usuario fuera del contenedor y también bloquea el dispositivo. Los usuarios pueden volver a iniciar sesión en el dispositivo y en la aplicación AppConnect mediante el código de acceso del dispositivo y el código de acceso de AppConnect, respectivamente.
7. En dispositivos iOS 7, puede introducir un mensaje para mostrar y un número de teléfono (opcional).
   Estas opciones pueden ofrecer a los usuarios de los dispositivos información sobre por qué se ha bloqueado el dispositivo y el número al que pueden llamar para desbloquearlo.
8. En dispositivos macOS, se solicita al usuario un PIN de 6 dígitos como código de acceso para acceder al dispositivo. Para continuar con el bloqueo de pantalla, el usuario del dispositivo debe:
   1. Introducir el PIN.
   2. Seleccionar la casilla para confirmar el bloqueo del dispositivo.
   3. Hacer clic en **Sí, enviar comando de bloqueo**.

> En macOS, el usuario puede añadir un mensaje opcional en la pantalla de bloqueo y un número de teléfono durante la configuración del código de acceso del dispositivo.

9. Para dispositivos de ChromeOS, cuando se lleva a cabo una operación de Bloqueo, es posible aparezca en la pantalla la ventana emergente "Bloquear un dispositivo puede requerir que el usuario introduzca un código de acceso para acceder al dispositivo". Haga clic en **Bloquear** y el estado del dispositivo se actualizará a **Desactivar enviado**, y el estado actualizado del dispositivo será visible después de la sincronización periódica del dispositivo.

Métodos alternativos para bloquear un dispositivo:

- El usuario de un dispositivo puede realizar la acción de bloqueo desde el Portal de autoservicio.
- El administrador puede realizar la acción de bloqueo desde el Portal del administración.

7.5.27. Administrar dispositivos en el modo Perdido de Apple

Esta sección contiene los siguientes temas:

- Activar el modo Perdido
- Realizar acciones del modo Perdido
- Desactivar el modo Perdido

Aplicable a: dispositivos iOS 10.3+ supervisados

Con Ivanti Neurons for MDM, puede poner un dispositivo supervisado en modo Perdido. Esto significa que usted comunica el dispositivo como perdido a los servidores de Apple y esto le permite recuperar la última localización registrada del dispositivo, además de desactivar el modo Perdido si encuentra el dispositivo.

Activar el modo Perdido

Puede comunicar que ha perdido un dispositivo a los servidores de Apple poniendo el dispositivo en modo Perdido. Una vez que haya puesto el dispositivo en modo Perdido:

- Si se retira el dispositivo, no podrá desactivar el modo Perdido.
- Si se borra el dispositivo, no podrá localizar ni hacer un seguimiento del dispositivo.

Procedimiento

1. Vaya a **Dispositivos**.
2. Seleccione la casilla del dispositivo.
3. Seleccione **Acciones** > **Común** > **Activar Modo Perdido**.
4. También puede acceder a la página **Detalles del dispositivo** seleccionando el enlace del nombre del dispositivo. Haga clic en el icono de acción del dispositivo y seleccione **Activar modo perdido**.

Realizar acciones del modo Perdido

Una vez se haya activado el modo Perdido, puede realizar las siguientes acciones desde la sección Modo dispositivo perdido:

- Insertar mensaje/número de teléfono en iPhone
  - Introducir un mensaje que aparecerá en la pantalla bloqueada del dispositivo perdido.
  - Introducir un número de contacto que aparecerá en la pantalla bloqueada del dispositivo perdido. Si alguien encuentra el dispositivo, podrán llamar a ese número para comunicárselo.

Bloquear dispositivo

- **Actualizar localización del dispositivo**

> Si el dispositivo se ha borrado, no podrá localizarlo.

- **Reproducir sonido del modo perdido**

> El sonido se reproducirá hasta que el dispositivo se elimine del modo Perdido o hasta que un usuario desactive el sonido del dispositivo.

- **Actualizar localización**
  La opción **Actualizar ubicación** se añade a **Modo perdido** para ver la ubicación del dispositivo. Se muestran los siguientes detalles:
  - **Latitud**: la latitud de la ubicación del dispositivo.
  - **Marca horaria**: se muestra la marca de fecha y hora de la carga útil.
  - **Longitud**: la longitud de la ubicación del dispositivo.

Desactivar el modo Perdido

Si se recupera un dispositivo que estaba en modo Perdido o se habilitó el modo Perdido por error, puede desactivar el modo Perdido.

> Si el dispositivo perdido se retira de Ivanti Neurons for MDM, la desactivación del modo perdido no funcionará.

Procedimiento

1. Vaya a **Dispositivos**.
2. Seleccione la casilla del dispositivo.
3. Seleccione **Acciones** > **Común** > **Desactivar Modo Perdido**.
4. Como alternativa, vaya a la página **Detalles del dispositivo** seleccionando el enlace del nombre del dispositivo y seleccione **Modo de dispositivo perdido: Activado** > **Desactivar Modo Perdido**.

7.5.28. Administración de dispositivos Android en modo Perdido

Esta sección contiene los siguientes temas:

- Activar el modo Perdido
- Desactivar el modo Perdido

Activar el modo Perdido

Aplicable a: dispositivos Android 8+

Puede colocar múltiples dispositivos Android simultáneamente en modo Perdido a través de Ivanti Neurons for MDM. Esto significa que puede informar de un dispositivo perdido a Ivanti Neurons for MDM colocando los dispositivos en modo Perdido, lo que le permite mostrar un mensaje personalizado, número de teléfono y nota al pie de página en la pantalla, junto con una opción para reproducir un sonido.

> Esta función solo es compatible con los dispositivos totalmente gestionados, incluidos los dispositivos no GMS.

Procedimiento

1. Vaya a **Dispositivos**.
2. Seleccione la casilla de los dispositivos.
3. Seleccione **Acciones > Activar modo perdido**.
4. Alternativamente, también puede hacer clic en el enlace del nombre del dispositivo para ir a la página de detalles del Dispositivo y hacer clic en el icono ⋮. Seleccione **Activar modo perdido**.
5. Introduzca un mensaje en la pantalla de bloqueo o un número de teléfono, o ambos, para que aparezca en la pantalla de bloqueo del dispositivo o dispositivos perdidos. Los administradores también pueden seleccionar la nota al pie y las opciones **Reproducir sonido en modo perdido**. Si alguien encuentra los dispositivos, podrán llamar a ese número para comunicárselo.

> Se debe introducir un mensaje o un número de teléfono en los campos respectivos para activar la opción **Activar modo perdido**.

> El sonido del Modo Perdido se reproducirá durante 5 minutos a menos que el teléfono se desbloquee, se pulse el botón de llamada o el Administrador desactive el Modo Perdido dentro de ese tiempo. Para reproducir un sonido, vuelva a activar el Modo Perdido en los dispositivos.

6. Seleccione **Activar el modo Perdido** para colocar los dispositivos Android en modo Perdido.

La activación del modo perdido deshabilitará las acciones siguientes:

- Desbloquear
- Entrar/Salir de kiosco
- Fuerza inicio de sesión para el kiosco compartido
- Asignar al usuario
- Enviar mensaje

- Establecer propiedad

> Una vez que se activa el modo Perdido en un dispositivo, se desactivará la opción del modo Perdido en el servidor.

Desactivar el modo Perdido

Si se recupera un dispositivo en modo Perdido o el modo Perdido se activó por error, puede desactivarlo.

> Si los dispositivos perdidos se borran de Ivanti Neurons for MDM, no funcionará la desactivación del Modo perdido.

Procedimiento

1. Vaya a **Dispositivos**.
2. Seleccione la casilla de los dispositivos.
3. Seleccione **Acciones > Desactivar modo perdido**.
4. También puede hacer clic en el enlace del nombre del dispositivo para ir a la página de detalles del dispositivo y seleccionar **Modo dispositivo perdido: Activado > Desactivar Modo Perdido**.

> En la sección **Detalles**, **Desactivar modo perdido** se vuelve visible solo después de activar **Activar modo perdido**. Una vez activado **Desactivar modo perdido**, desaparece el campo **Modo dispositivo perdido: Activado**, que incluye la opción **Desactivar Modo Perdido**.

> Los dispositivos que estaban previamente en Modo Kiosko tendrán que volver a entrar en Kiosko después de desactivar el modo Perdido.

7.5.29. Solicitar registros de depuración

Puede enviar una solicitud a los dispositivos iOS, macOS y Android administrados en el trabajo para recuperar registros de depuración para solucionar problemas con los dispositivos. Mediante el comando «Solicitar registros de depuración» de la página de Dispositivos, las acciones y el éxito o fracaso de un evento se capturan en los registros de depuración

Esta función requiere los siguientes clientes:

- Los dispositivos iOS requieren Go 5.3.0 para iOS o versiones más recientes compatibles. Para los dispositivos migrados de Ivanti EPMM a Ivanti Neurons for MDM, esta función requiere Mobile@Work 12.2.0 para iOS o versiones más recientes compatibles.
- Los dispositivos macOS requieren Mobile@Work 1.5 para macOS o versiones más recientes compatibles.
- Los dispositivos Android gestionados por trabajo requieren Go 65 para Android o una versión más reciente compatible.

Procedimiento

1. Vaya a **Dispositivos > Dispositivos**.
2. Seleccione el dispositivo y haga clic en el enlace con el nombre del dispositivo para ir a la página de detalles del Dispositivo.
3. Haga clic en el icono ⋮.
4. Seleccione **Solicitar registros de depuración** y haga clic en **Aceptar**.

Una vez que se envíe la solicitud y los registros estén listos en el dispositivo, se enviará una notificación al administrador y aparecerá en los registros del dispositivo. Los registros del dispositivo también se pueden descargar haciendo clic en el enlace.

7.5.30. Apple_Enhanced_Logging

File not found!

7.5.31. Retirar un dispositivo

La retirada de un dispositivo termina su relación con Ivanti Neurons for MDM. Puede retirar un dispositivo si:

- el usuario se va de la empresa
- el usuario ha reemplazado el dispositivo
- tiene que deshacer las tareas de administración que ha completado (volver a empezar)

Procedimiento

1. Vaya a **Dispositivos > Dispositivos**.
2. Seleccione el dispositivo.
3. Haga clic en **Acciones** (arriba a la derecha).
4. Seleccione **Retirar**.
5. Opcionalmente, también puede hacer clic en el enlace del nombre del dispositivo para ir a la página de detalles del Dispositivo y hacer clic en el icono ⋮
6. Seleccione **Retirar** y haga clic en **Aceptar**.

> Cuando se realiza una operación de Retirada en un dispositivo que está en estado Activo, el dispositivo se retirará inmediatamente.

7.5.32. Renuncia de la propiedad de un dispositivo

Aplicable a dispositivos Android en el modo Perfil de trabajo en el Dispositivo propiedad de la empresa.

Renunciar a la propiedad de un dispositivo en modo Perfil de trabajo en el Dispositivo propiedad de la empresa elimina el perfil de trabajo y retira el dispositivo de Ivanti Neurons for MDM sin afectar a las aplicaciones ni a los datos personales. Así, el usuario final puede utilizar el dispositivo como dispositivo personal, con acceso total a todos los controles y ajustes del dispositivo.

> Es necesario eliminar el dispositivo del portal Google Zero Touch o Knox Mobile Enrollment.

Es posible que renunciar a la propiedad de un dispositivo si:

- el usuario se va de la empresa
- el usuario ha reemplazado el dispositivo

Procedimiento

1. Vaya a **Dispositivos > Dispositivos**.
2. Seleccione el dispositivo.
3. Haga clic en la página **Detalles del dispositivo** y haga clic en el icono ⋮.
4. Seleccione **Renunciar a la propiedad**.

7.5.33. Borrar un dispositivo

Borrar un dispositivo elimina todos los datos y devuelve el dispositivo a los ajustes predeterminados de fábrica.

Procedimiento

1. Vaya a **Dispositivos > Dispositivos**.
2. Seleccione el dispositivo.
3. Haga clic en **Acciones** (arriba a la derecha).
4. Seleccione **Borrar.**
5. Alternativamente, también puede hacer clic en el enlace del nombre del dispositivo para ir a la página de detalles del Dispositivo y hacer clic en el icono ⋮. Seleccione **Borrar** y haga clic en **Aceptar**.
6. Por defecto, se selecciona la opción **Preservar plan de datos**.
   (Opcional, aplicable a dispositivos iOS 11.3+) Seleccione la opción **Omitir configuración de proximidad**.
7. Seleccione la opción **Retorno al servicio** para volver a registrar automáticamente el dispositivo después de borrar los datos, de modo que no tenga que volver a registrar el dispositivo manualmente después de un borrado. Aplicable solo para dispositivos de iOS 17+ registrados en modo DEP.
   1. Seleccione la **Configuración Wi-Fi** en el menú desplegable. El usuario debe desactivar todos los bloqueos de activación. Aplicable solo para dispositivos de iOS 17+ registrados en modo DEP.
   2. (opcional) Seleccione la opción **Preservar aplicaciones**, si desea que los dispositivos vuelvan al servicio preservando la aplicaciones existentes. Únicamente se conservarán las aplicaciones instaladas mediante Ivanti N-MDM con prioridad alta. Aplicable solo para dispositivos iOS 26.
8. Para dispositivos macOS, puede enviar un PIN de 6 dígitos al dispositivo como código de acceso. En el dispositivo, se solicita al usuario que introduzca el PIN para acceder al dispositivo. Para continuar con la acción de borrado, el usuario del dispositivo debe:
   1. Introducir el PIN.
   2. Seleccionar la casilla para confirmar la acción de borrado del dispositivo.
   3. Hacer clic en **Sí, borrar este dispositivo**.
9. Para dispositivos de ChromeOS, cuando se lleva a cabo una operación Borrar desde la página **Detalles del dispositivo** o **Lista de dispositivos**, aparece una ventana con el mensaje "Borrar un dispositivo lo devuelve a los ajustes de fábrica, que puede resultar en pérdida de datos. La acción Borrar es distinta según la plataforma" aparece en la pantalla.
   1. Marque la casilla "Entiendo que Borrar no se puede deshacer" para confirmar la acción de borrar el dispositivo.
   2. Haga clic en **Borrar** para borrar el dispositivo.

El estado del dispositivo cambia a "**Borrar enviado**". El estado del dispositivo actualizado será visible después de una sincronización de dispositivo periódica.

En dispositivos de Android Enterprise, puede llevar a cabo la acción **Borrar** dispositivo incluso después de que se reinicie el dispositivo y que permanezca bloqueado.

Los dispositivos de Android que se encuentran en estado **Pendiente de borrar** se pueden eliminar mediante la opción **Eliminar dispositivo** que se encuentra en la página **Detalles del dispositivo**. Cuando se ha eliminado el dispositivo, éste pierde la conexión con el servidor y deja de ser compatible. El usuario debe volver a inscribir el dispositivo después de llevar a cabo el restablecimiento de los valores de fábrica.

7.5.34. Eliminar dispositivos

Después de retirar un dispositivo, puede eliminarlo. Al eliminarlo, se quita de todas las páginas. Puede eliminar un dispositivo solo si su estado es Retirado, Retiro pendiente, Borrado o Borrado pendiente.

Procedimiento

1. Vaya a **Dispositivos > Dispositivos**. La lista de dispositivos aparece en la pantalla.
2. Seleccione el dispositivo que desee eliminar.
3. Haga clic en **Acciones**.
4. En la sección **Común**, seleccione la opción **Eliminar dispositivos**. Aparece una ventana emergente en la pantalla.
5. Seleccione la opción "Entiendo que no se puede anular la eliminación" y, a continuación, haga clic en **Eliminar dispositivo(s)**.
6. También puede eliminar un dispositivo siguiendo los pasos que se indican a continuación:
    - Vaya a **Dispositivos** >**Dispositivos**.
    - En la columna **Nombre en pantalla del usuario**, haga clic en cualquier enlace. Aparece en pantalla la página **Detalles del dispositivo**. Haga clic en **Detalles del dispositivo**. Aparecerá una ventana emergente en la pantalla, y si reconoce la advertencia y hace clic en **Aceptar**, se eliminará el dispositivo específico.

Eliminar múltiples dispositivos

Puede eliminar varios dispositivos seleccionando todos los dispositivos que desee eliminar.

Procedimiento

1. Vaya a **Dispositivos > Dispositivos**.
2. Seleccione los dispositivos de la lista de dispositivos disponibles.
3. Haga clic en la pestaña **Acciones**, bajo el encabezado **Común**, seleccione la opción **Eliminar dispositivos**.
4. En la ventana **Eliminar dispositivos**:
    1. Seleccione la casilla de verificación **Entiendo que la eliminación no se puede revertir**.
    2. Haga clic en **Eliminar dispositivos válidos**, para eliminar los dispositivos seleccionados.

7.5.35. Desbloquear un dispositivo

Esta sección contiene los siguientes temas:

- Desbloquear dispositivos Android
- Desbloquear AppConnect para aplicaciones Android
- Desbloquear un dispositivo iOS
- Desbloquear dispositivos de ChromeOS

Para desbloquear un dispositivo:

Puede eliminar el bloqueo de pantalla de un dispositivo. El desbloqueo funciona de forma algo diferente dependiendo del dispositivo.

Procedimiento

1. Vaya a **Dispositivos > Dispositivos**.
2. Seleccione los dispositivos.
3. Haga clic en **Acciones**.
4. Seleccione **Desbloquear**.
5. También puede hacer clic sobre el enlace del nombre del dispositivo para acceder a la página Detalles del dispositivo y hacer clic en el icono **Desbloquear** y en **Aceptar**.

Desbloquear dispositivos Android

Cuando se recibe el comando Desbloquear, la aplicación Android intenta restablecer el código de acceso. En los modos Administrador del dispositivo y Propietario del dispositivo, el código de desbloqueo se restablece, mientras que en los modos Personal habilitado en el Propietario del perfil y Propietario de la empresa, se restablece el código de desbloqueo del perfil de trabajo.

El comando de desbloqueo proporciona una opción para que el administrador establezca el código de desbloqueo con una combinación de caracteres alfanuméricos. La opción predeterminada, que establece el código de desbloqueo en "0000", se puede realizar en varios dispositivos. Sin embargo, la nueva opción, Código de desbloqueo personalizado para Android, se puede realizar en un dispositivo de cada vez. El número mínimo de caracteres debe ser 6 y el máximo 8. Esta opción está disponible en la pestaña **Acciones**, así como en la página **Detalles del dispositivo**. Cuando selecciona la opción Desbloquear en la pestaña **Acciones** o en la página **Detalles del dispositivo**, puede ver las dos opciones siguientes.

- Predeterminada
- (Solo Android) Proporcionar un código de desbloqueo: puede proporcionar un código de desbloqueo de esta sección y hacer clic en **Desbloquear**.
    - Omitir solicitud de restablecimiento del código de acceso en el dispositivo: seleccione esta opción para omitir el restablecimiento del código de acceso si la configuración del código de acceso se envía a un dispositivo.

Después de configurar el código de desbloqueo, el administrador puede encontrarlo en las páginas **Pruebas de auditoría** y **Registros del dispositivo**.

> El desbloqueo Directboot solo funciona para la opción de desbloqueo por defecto, código de desbloqueo '0000'. El código de desbloqueo personalizado para el arranque directo no es compatible.

Desbloquear AppConnect para aplicaciones Android

En las aplicaciones AppConnect, el comando **Desbloqueo de AppConnect** ayuda a desbloquear contenedores que hayan sido bloqueados porque los usuarios estaban intentando iniciar sesión varias veces con códigos de acceso incorrectos. Este desbloqueo no desbloqueará el dispositivo en sí.

Desbloquear un dispositivo iOS

Cuando se recibe el comando Desbloquear, la aplicación iOS elimina el código de acceso de dispositivo. Si la **configuración del código de acceso** especifica que es necesario un nuevo código de acceso, se solicitará al usuario del dispositivo que establezca un nuevo código de acceso que cumpla con las reglas definidas en la configuración de códigos de acceso. El usuario debe realizar este cambio en los 60 minutos posteriores. De lo contrario, la aplicación forzará al usuario a que establezca un nuevo código de acceso.

Desbloquear dispositivos de ChromeOS

Cuando un dispositivo de ChromeOS se selecciona y se hace clic en la opción **Desbloquear**, aparece una ventana en la pantalla con el mensaje : "Desbloquear puede borrar un código de acceso existente para habilitar el acceso de un usuario al dispositivo. Desbloquear es distinto según la plataforma". Haga clic en **Desbloquear** y el estado del dispositivo se actualizará a "Desbloquear enviado", y el estado actualizado se visualizará después de la sincronización periódica del dispositivo.

7.5.36. Reiniciar o apagar dispositivos

Esta sección contiene los siguientes temas:

- Reiniciar un dispositivo
- Apagar un dispositivo

Aplicable a: dispositivos Android 7.0+ (dispositivos administrados), iOS 10.3+ supervisado, tvOS 10.3+ supervisado, macOS 10.13+ y Windows 10+.

Los administradores pueden reiniciar o apagar un dispositivo supervisado de iOS individualmente desde la página de detalles del dispositivo o en masa desde la página de la lista de dispositivos.

Reiniciar un dispositivo

Procedimiento

1. Vaya a **Dispositivos**.
2. Navegue hasta el dispositivo.
3. Haga clic en el vínculo que aparece en la columna **Nombre**.
4. Haga clic en el botón **Acciones**.
5. Haga clic en **Reiniciar/apagar el dispositivo**.

> Los dispositivos no compatibles no se pueden reiniciar.

6. Lea la advertencia que se muestra.
7. (Opcional) Seleccione esta opción para borrar el código de acceso del dispositivo al reiniciarlo. Si no se borra el código de acceso, el dispositivo pedirá un código de acceso y no estará conectado a la Wi-Fi después del reinicio.
8. Seleccione **Reiniciar dispositivo** si no está seleccionado ya.
9. Si todavía desea reiniciar el dispositivo, haga clic en **Enviar a dispositivo**. De lo contrario, haga clic en **Cancelar**.

> Para los dispositivos Android, los administradores pueden ver la información sobre cuándo se reinició el dispositivo en **Tiempo de actividad** en la página Detalles del dispositivo.

Puede reiniciar varios dispositivos compatibles desde la página de la lista de **Dispositivos**. Para ello, seleccione los dispositivos en cuestión, haga clic en **Acciones> Reiniciar/apagar dispositivo** y siga las instrucciones que aparecen en pantalla.

Apagar un dispositivo

Procedimiento

1. Vaya a **Dispositivos**.
2. Navegue hasta el dispositivo.
3. Haga clic en el vínculo que aparece en la columna **Nombre**.
4. Haga clic en el botón **Acciones**.
5. Haga clic en **Reiniciar/apagar el dispositivo**.

> Los dispositivos no compatibles no se pueden reiniciar.

6. Lea la advertencia que se muestra.
7. Seleccione **Apagar dispositivo**.
8. Si todavía desea apagar el dispositivo, haga clic en **Enviar a dispositivo**. De lo contrario, haga clic en **Cancelar**.

Puede apagar varios dispositivos compatibles desde la página de la lista de **Dispositivos**. Para ello, seleccione los dispositivos en cuestión, haga clic en **Acciones> Reiniciar/apagar dispositivo** y siga las instrucciones que aparecen en pantalla.

7.5.37. Borrar la contraseña de las restricciones (solo iOS)

Puede borrar una contraseña de restricciones establecida por los usuarios en dispositivos iOS 8 supervisados. Esta acción solo está disponible para dispositivos activos.

Procedimiento

1. Vaya a Dispositivos > Dispositivos.
2. Seleccione la entrada del dispositivo.
3. Seleccione Acciones > Borrar la contraseña de las restricciones.
4. Confirme la acción cuando se le solicite.

7.5.38. Eliminar la asociación de Sentry de un dispositivo

La asociación de Sentry se aplica a los dispositivos para el túnel de aplicaciones o un sistema de correo electrónico habilitado para ActiveSync que controla el acceso a los correos electrónicos de los dispositivos. Si es necesario, puede eliminarse la asociación de cualquier dispositivo que esté asociado con Sentry de la siguiente manera:

Procedimiento

1. Vaya a **Dispositivos.**
2. En la columna **Nombre**, haga clic en el enlace del dispositivo para el que desee eliminar la asociación de Sentry.
3. Haga clic en la pestaña **Sentry** .
4. En la columna **Acciones**, haga clic en **Eliminar**.

7.5.39. Asignar atributos personalizados a los dispositivos

Se pueden asignar atributos personalizados a los dispositivos, como una Id. interna, a uno o más dispositivos. Cada atributo tiene un valor correspondiente que puede usar para tareas como la creación de configuraciones y grupos de dispositivos. Después de crear atributos personalizados, puede asignarlos a dispositivos. Para obtener más información sobre cómo administrar atributos, consulte **Atributos**.

Procedimiento

1. Inicie sesión en el portal administrativo.
2. Vaya a **Dispositivos**.
3. Seleccione uno o más dispositivos.
4. Haga clic en **Acciones**.
5. Seleccione **Asignar atributos personalizados**.
6. Seleccione *una* de las siguientes opciones:
    - Forzar la asignación (sobreescritura) de todos los atributos aunque se encuentre algún valor existente.
    - Sobrescribir solo si el valor está vacío y omitir atributos con valores existentes.

Seleccione los atributos que desea asignar e introduzca sus valores (no se permiten valores vacíos).

8. Haga clic en **Asignar**.

> Se pueden exportar los **Atributos de dispositivos personalizados** con sus valores al formato CSV desde la página **Detalles de dispositivos**.

7.5.40. Eliminar atributos personalizados de los dispositivos

Tenga precaución, ya que esta acción no es reversible. Para eliminar los atributos personalizados de uno o más dispositivos:

Procedimiento

1. Vaya a **Dispositivos**.
2. Seleccione uno o más dispositivos.
3. Haga clic en **Acciones**.
4. Seleccione **Eliminar atributos personalizados**.
5. Seleccione los atributos que desea eliminar.
6. Seleccione **Quitar**.

7.5.41. Sincronizar y obtener comentarios de aplicaciones

Puede enviar una solicitud a una aplicación instalada en dispositivos Android para obtener información detallada sobre el estado de configuración actual de la aplicación. Cuando se envía una solicitud, se recibe un informe de comentarios de configuración de la aplicación para el dispositivo.

Procedimiento

1. Vaya a **Dispositivos**.
2. Haga clic en el dispositivo para el que desea enviar la solicitud.
3. Haga clic en **Acciones**.
4. Seleccione **Sincronizar y recuperar los comentarios de la aplicación**. La petición se envía para sincronizar y recuperar los comentarios de configuración de la aplicación. Se actualizará el campo «Última sincronización de comentarios sobre la aplicación» que hay junto a «Último ingreso del cliente».
5. En la pestaña **Aplicaciones instaladas**, haga clic en el vínculo **Ver detalles** para la aplicación en la columna **Comentarios sobre aplicaciones**. Aparecerá la ventana **Comentarios sobre la aplicación**.
   Clave: proporciona información detallada y la ubicación de los ajustes notificados (en la configuración de la aplicación administrada de la aplicación) basándose en los comentarios que se han recibido desde las aplicaciones.
   Sello temporal: hora y fecha de la clave.
   Gravedad: indica la importancia de la clave. Ejemplo: 'Info', 'Error'.
   Mensaje: el tipo de mensaje recibido de los comentarios sobre configuración de la aplicación. Ejemplo: ‘Error’.
   Datos: detalles de los datos recibidos de los comentarios sobre configuración de la aplicación.

Visualizar los comentarios sobre la configuración de aplicaciones desde el App Catalog

Se puede ver el informe de comentarios sobre la configuración de la aplicación para cada aplicación en particular desde el App Catalog.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Seleccione la aplicación de la que desea ver los detalles.
3. Haz clic en la pestaña **Comentarios sobre configuración de aplicaciones**. La columna **Recuento de dispositivos** muestra el número de dispositivos (hipervínculo) para cada clave del informe de comentarios sobre la configuración de la aplicación.
4. Haga clic en el hipervínculo de número de dispositivos para ver los detalles de los dispositivos. Por ejemplo, al hacer clic en el hipervínculo 5, se muestran los detalles de 5 dispositivos. Se muestran los siguientes detalles para la combinación de 'Clave' y 'Gravedad', que aparece encima de la tabla:
   Dirección de correo electrónico: especifica el nombre de usuario. Al hacer clic en el enlace del nombre de usuario, se accede a la pestaña **Aplicaciones instaladas** en **Dispositivos > Detalle del dispositivo**.
   Tipo de dispositivo: especifica el modelo del dispositivo.
   OS: número de versión del OS Android.
   Número de serie: número de serie del dispositivo.
   Sello temporal: hora y fecha en que se actualizó por última vez.
   Mensaje: el tipo de mensaje recibido de los comentarios sobre configuración de la aplicación. Ejemplo: ‘Error’.
   Datos: detalles de los datos recibidos de los comentarios sobre configuración de la aplicación.

Se pueden ver las notificaciones de errores de los comentarios sobre configuración de la aplicación para el dispositivo Android haciendo clic en el icono de la campana (arriba a la derecha) o desde la página **Panel > Notificaciones**. Al hacer clic en el enlace de notificación, se accede a la pestaña **Comentarios sobre configuración de la aplicación** y se puede ver el informe de comentarios de la aplicación.

> El informe de comentarios sobre configuración de la aplicaciones se eliminará y no se mostrará cuando el dispositivo se borre o se retire. Esta tarea en segundo plano que se ejecuta cada 24 horas purga los datos de más de 7 días de antigüedad.

7.5.42. Establecer la contraseña del firmware

Aplicable a: macOS 10.13 o versiones más recientes compatibles.

El administrador puede establecer o actualizar la contraseña del firmware (EFI) para un dispositivo macOS. La contraseña del firmware evita que el dispositivo macOS se inicie desde cualquier dispositivo de almacenamiento interno o externo que no sea el disco de inicio seleccionado por el usuario del dispositivo. Como resultado, también bloquea la posibilidad de usar la mayoría de las combinaciones de claves de inicio.

Procedimiento:

1. Vaya a **Dispositivos**.
2. Para establecer o cambiar la contraseña del firmware para un solo dispositivo:
    1. Haga clic en el nombre de usuario con el que está asociado el dispositivo para ver la página de detalles del dispositivo.
    2. En la sección General, amplíe **Contraseña del firmware** y haga clic en **Establecer contraseña** o en **Establecer/cambiar contraseña del firmware** desde el menú de Acciones del dispositivo.
    3. En esta sección se muestra la siguiente información:
        1. **Contraseña:** la contraseña o una lista de posibles contraseñas.

            > Cuando un administrador establece la contraseña del firmware, se envía el comando al dispositivo. Si el dispositivo no responde a tiempo, la contraseña se almacena temporalmente y de muestra en este campo. La nueva contraseña no entrará en vigor hasta que el dispositivo la reconozca y el dispositivo se reinicie. Hasta entonces, se mostrarán todas las posibles contraseñas. Una vez que el dispositivo se reinicie y el cambio de contraseña se reconozca, todas las contraseñas no deseadas se borrarán.

        2. **Cambio pendiente:** indica si el cambio de contraseña está pendiente.
        3. **Estado del comando:** indica si el cambio de contraseña fue un éxito o un fracaso.
        4. **Permitir ROM opcionales:** indica si las ROM opcionales se deben habilitar. Por defecto, está configurado como No.

Para establecer o cambiar la contraseña del firmware para más de un dispositivo:

1. Seleccione los dispositivos.
2. Desde el menú Acciones, haga clic en **Establecer/cambiar contraseña del firmware**.

Introduzca la contraseña actual y la nueva.

Si es la primera vez, la contraseña actual se puede dejar vacía.

Para restablecer la contraseña, deje vacío el campo de la contraseña nueva.

5. Haga clic en **Guardar**.

> Solo los dispositivos con versiones de macOS compatibles se actualizarán con la nueva contraseña. Los dispositivos no compatibles se omitirán.

7.5.43. Volver a emitir una nueva clave de recuperación personal

Aplicable a: dispositivos macOS con Mobile@Work para macOS 1.66 o versiones más recientes compatibles.

Al migrar desde otras soluciones MDM a Ivanti Neurons for MDM, los administradores pueden solicitar al sistema operativo que vuelva a emitir una nueva clave de recuperación personal (PRK, en inglés) en el momento de la inscripción, si ya se emitió una PRK previamente antes de la inscripción. Esto permite almacenar la clave en Ivanti Neurons for MDM.

Puede ver las entradas del registro de Trazas de auditoría para las actividades PRK de la siguiente manera:

1. Vaya a **Panel de control > Audit Trails**.
2. El filtro Tipo, seleccione **Clave personal de recuperación.** Las entradas de PRK aparecerán en la categoría de Administración de dispositivo y actividades como "Clave personal de recuperación vista".

Requisito previo

Distribuya las siguientes configuraciones a los dispositivos antes de realizar este procedimiento:

- Configuración de Mobile@Work para macOS.
- Configuración de la Clave de recuperación de FileVault.

Procedimiento

1. Póngase en contacto con la asistencia técnica para solicitar la secuencia de comandos para generar una nueva PRK en el dispositivo.
2. Cree un atributo personalizado del dispositivo con el nombre «deviceprk» que se utilizará en la secuencia de comandos.
3. Suba la secuencia de comandos al repositorio en **Administrador > Secuencias de comandos y archivos > Todas las secuencias de comandos**. Mientras lo hace, seleccione el atributo personalizado «deviceprk».
4. Cree un grupo de dispositivos dinámico para los dispositivos en los que no se ha recuperado la PRK de la antigua solución de MDM. Seleccione las reglas del grupo de dispositivos de la siguiente manera: «**Platform=macOS** and **Encryption Enabled is equal to Yes** and **macOS Personal Recovery Key escrowed is equal to No** and **macOS Recovery Key Type is equal to Personal**» («Plataforma=macOS y Cifrado habilitado es igual a Sí y Clave de recuperación personal de macOS en custodia es igual a No y Tipo de clave de recuperación de macOS es igual a Personal»).
5. Cree una configuración de secuencia de comandos de Mobile@Work para macOS en la que se pueda seleccionar la secuencia de comandos de la PRK del repositorio. Distribuya la configuración al nuevo grupo de dispositivos.
6. Programe la secuencia de comandos para que se ejecute una vez al día o según desee. Esta secuencia de comandos pedirá la contraseña de usuario cada vez que se ejecute. De forma predeterminada, el período de tiempo de espera para la ejecución de la secuencia de comandos es de 60 segundos. Se recomienda ampliar el periodo de tiempo de espera en la configuración correspondiente de Mobile@Work para macOS estableciendo el campo **Max Run Time** en 300 segundos.

- La clave descifrada está disponible en la página de detalles del dispositivo de un dispositivo de la sección Estado de cifrado del dispositivo. Haga clic en **Ver** junto al campo Cifrado de FileVault habilitado.
- Al obtener la PRK, el dispositivo se sale del grupo de dispositivos. Por lo tanto, la configuración de la secuencia de comandos ya no será aplicable y se eliminará del dispositivo.

- Una vez que MDM recupere la clave de recuperación de un dispositivo utilizando la secuencia de comandos, este se desinstalará del dispositivo.

Temas relacionados:

- **Atributos**
- **Todas las secuencia de comandos**
- **Grupos de dispositivos**
- **Mobile@Work para macOS**
- **Clave de recuperación de FileVault**

7.5.44. Configurar o cambiar el bloqueo de recuperación

Se aplica a: macOS 11.5+

El administrador puede establecer o cambiar el bloqueo de recuperación para el reinicio del dispositivo para el dispositivo macOS que se ejecuta en la silicona de Apple. Un bloqueo de recuperación impide el arranque de los dispositivos macOS en modo de recuperación, a menos que se introduzca el código de acceso.

Procedimiento:

1. Vaya a **Dispositivos**.
2. Para establecer o cambiar el bloqueo de recuperación para el reinicio:
    1. Haz clic en el nombre de visualización del usuario al que está asociado el dispositivo para ver la página de detalles del dispositivo. Dé uno de los siguientes pasos:
    2. En la sección **Descripción general**,expanda **Bloqueo de recuperación** y haga clic en **Establecer contraseña** o en **Cambiar contraseña**. O haga clic en la elipsis **Acciones** y, luego, en **Establecer/cambiar bloqueo de recuperación**.
    3. En el cuadro de diálogo **Establecer/Cambiar bloqueo de recuperación** haga lo siguiente:
        1. **Contraseña actual**: introduzca aquí la contraseña actual. Manténgala vacía si es la primera vez que la establece.
        2. **Contraseña**: ingrese la contraseña que desea establecer.
        3. **Confirmar contraseña**: vuelva a introducir la contraseña que desea establecer.

Haga clic en **Establecer/cambiar bloqueo de recuperación**.

> En la Descripción general, el **Bloqueo de recuperación habilitado** muestra el estado del código de acceso de bloqueo de recuperación.

> Los administradores también pueden suprimir el código de acceso al eliminar el código de acceso existente y hacer clic en **Establecer/cambiar bloqueo de recuperación**.

7.5.45. Administración de acceso de Apple

Requisitos previos:

- Verifique y bloquee el dominio en Apple Business Manager o Apple School Manager.
- Configure al menos un servidor MDM desde las organizaciones de Apple Business Manager o Apple School Manager, donde las ID gestionadas de Apple se presentan en el Ivanti Neurons for MDM.

Iniciar sesión con un ID de Apple administrado permite a las empresas controlar los servicios y funciones de Apple que pueden utilizar los usuarios.

En Apple Business Manager o Apple School Manager, la configuración **Permitir cuentas de Apple administradas** controla dónde los usuarios pueden iniciar sesión con sus ID de Apple administrados. Los administradores pueden configurar esta opción para restringir el inicio de sesión a dispositivos gestionados o supervisados, o permitirlo en cualquiera de los dispositivos.

- **Cualquier dispositivo** (predeterminado): los usuarios pueden iniciar sesión con su ID administrada de Apple en cualquier dispositivo, independientemente de que la gestione una solución MDM.
- **Solo dispositivos administrados**: los usuarios solo pueden iniciar sesión en dispositivos gestionados por una solución MDM que admita el endpoint de Get Token.
- **Solo dispositivos supervisados**: los usuarios solo pueden iniciar sesión en dispositivos que estén supervisados (y gestionados) por una solución MDM que sea compatible con el endpoint Get Token.

Estas configuraciones forman parte de la gestión más amplia de "Administración de acceso" para los Servicios de Apple dentro de Apple Business Manager y Apple School Manager.

> Con mayor seguridad, restringir el inicio de sesión a dispositivos gestionados o supervisados puede mejorar la seguridad de los datos al garantizar que la información relacionada con el trabajo solo sea accesible en dispositivos controlados.

El inicio de sesión en una Cuenta de Apple Administrada fallará si hay cero o múltiples organizaciones de servidores MDM de **Inscripción de Dispositivos** presentes en la pestaña de Inscripción de Dispositivos, y el administrador configura la opción **Permitir Cuenta de Apple Administrada** (disponible en **Gestión de Acceso** > **Servicios de Apple**) en "Solo Dispositivos Supervisados" o "Solo Dispositivos Administrados" en Apple Business Manager o Apple School Manager.

> Los dispositivos no podrán iniciar sesión si la cuenta de **Apple Administrada** no está presente en el servidor MDM de Inscripción de Dispositivos Ivanti Neurons for MDM.

7.5.46. Inscripción de políticas de grupos

Los dispositivos Windows 10/11 se pueden inscribir en Ivanti Neurons for MDM mediante una política de grupo. Crear un grupo de políticas inscribirá automáticamente todos los dispositivos que tengan una unión híbrida con Azure AD.

ProcedurePara inscribir dispositivos con una política de grupo

1.	**Asegúrese de que sus dispositivos tienen enlace híbrido con Azure AD. Para obtener más información, consulte la documentación de Microsoft: dispositivos de enlace híbrido de Azure AD.**
2.	**Cree un objeto de política de grupo. Para más información, consulte la documentación de Microsoft: Configurar la inscripción automática para un grupo de dispositivos.**
3.	**Cree un grupo de seguridad que incluya los dispositivos que desee inscribir. Para más información, consulte la documentación de Microsoft: Grupos de seguridad de Active Directory.**
4.	**Enlace el objeto de la política de grupo con el grupo de seguridad. Para obtener más información, consulte la documentación de Microsoft: Enlace al GPO del dominio.**

Experiencia de usuario

Cuando un usuario inicia sesión en el dispositivo con credenciales de Azure AD, Microsoft identifica la configuración de MDM basada en Azure AD que pertenece a su organización. El dispositivo está inscrito en Ivanti Neurons for MDM y puede recibir políticas y comandos.

8. Aplicaciones

Esta sección contiene los siguientes temas:

- Catálogo de aplicaciones
- Apps@Work
- Funciones de la tienda de aplicaciones de Apps@Work en iOS
- Ver Detalles de la aplicación
- Configuración de aplicaciones
- Asignar atributos personalizados a las aplicaciones
- Configuraciones administradas para Android
- Administrar aplicaciones de Google Play
- Eliminar aplicaciones del App Catalog
- Actualizar aplicaciones internas
- Encontrar el nombre del paquete de una aplicación de Android
- Categorías
- Filtros de distribución
- Excluir o distribuir aplicaciones
- Opiniones
- Apps and Books de Apple
- Ajustes del catálogo
- Instalar dependencias de aplicaciones
- Desplegar Divide Productivity con Android Enterprise
- Configurar la aplicación Provisioner
- Administración de aplicaciones de Windows
- Ivanti Bridge

8.1. Catálogo de aplicaciones

Esta sección contiene los siguientes temas:

- Licencias para las características de las aplicaciones
- Alternar entre la vista de lista y de cuadrícula
- Añadir una aplicación de la Google Play Store para Android Enterprise
- Añadir una aplicación desde una store pública
- Añadir una aplicación interna
- Delegar permisos de dispositivos delegados para aplicaciones internas de Android Enterprise
- Mostrar el estado del perfil de aprovisionamiento para las aplicaciones internas de iOS
- Actualizar el perfil de aprovisionamiento para las aplicaciones internas de iOS
- Implementar aplicaciones internas en Google Play
- Añadir una aplicación web para dispositivos con Android Enterprise
- Añadir una aplicación web para dispositivos iOS
- Uso de la búsqueda avanzada
- Exportación de aplicaciones a un archivo CSV

Utilice la página del catálogo de aplicaciones para administrar su catálogo de aplicaciones. El catálogo de aplicaciones enumera las aplicaciones móviles que ha puesto disponibles para sus usuarios. Estas incluyen aplicaciones que los usuarios pueden descargar desde tiendas de aplicaciones públicas y aplicaciones que pretende distribuir mediante de Ivanti Neurons for MDM (aplicaciones internas). Las aplicaciones con AppConnect activado, GoClient para iOS y M@W para macOS también están disponibles como aplicaciones de empresa en la página Catálogo de aplicaciones, de manera que se simplifica el proceso de importación para configuración y distribución. En dispositivos «MAM only», a los usuarios de iOS se les solicitará que seleccionen el certificado para autenticar el acceso a estas aplicaciones cuando abran el Catálogo de aplicaciones.

Los MacBooks con chipset M1 de Apple admiten aplicaciones VPP para iPhone y iPad. Solo el administrador puede enviar las aplicaciones VPP de iPhone y iPad compatibles. Esta opción no está disponible para que los usuarios la instalen desde el Catálogo de aplicaciones.

En el caso de los abonados de Ivanti Neurons for MDM con dispositivos Android, si Android Enterprise no está habilitado a finales de marzo de 2021, los administradores no podrán buscar aplicaciones con los nombres. La comunicación sobre este cambio se muestra con un mensaje de banner cuando se accede a la página del App Catalog. Este mensaje de banner se seguirá mostrando hasta que se active Android Enterprise en estos abonados y hasta que no se seleccione la opción "No volver a mostrar esto".

- el método de instalación silenciosa de aplicaciones no está disponible para las aplicaciones macOS públicas. Las aplicaciones macOS también se pueden implementar a través del Apps and Books de Apple mediante licencias basadas en dispositivos y mediante el método de instalación silencioso de aplicaciones en las inscripciones.
- Al cargar la aplicación Ivanti Go al servidor Ivanti Neurons for MDM, si es necesario seleccionar la opción **Convertir en aplicación gestionada,** también deberá habilitar la opción **Instalar en dispositivo** .
- App Catalog y la instalación de aplicaciones no son compatibles con dispositivos Sonim XP5S.
- Android no permite desinstalar las aplicaciones con privilegios de administrador activos. Para desinstalar la aplicación, vaya a **Ajustes del dispositivo > Seguridad > Administradores de dispositivos**, y desactive los privilegios del Administrador del dispositivo. A continuación, desinstale la aplicación.

- Si una aplicación de Android Enterprise se instala manualmente desde Google Play Store de Android Enterprise en el dispositivo y, más adelante, el administrador retira su distribución, la aplicación deberá desinstalarse también de forma manual.
- Si la aplicación está comprimida u oculta, no se podrán cargar las aplicaciones internas de Android.
- Las aplicaciones públicas no son compatibles con **iPads compartidos**.
- Debido a una limitación de Apple, para las aplicaciones Business-to-Business (B2B) disponibles en el Catálogo de aplicaciones, las descripciones y capturas de pantalla de las aplicaciones no están disponibles en la pestaña **Detalles**.
- Cuando se busca una aplicación en el Catálogo de aplicaciones o en el portal administrativo, los resultados de la búsqueda se basan en el **Nombre de la aplicación**, **Comentario**, **Descripción**, **Versión en pantalla** y **Novedades**. Si los datos de la aplicación buscada coinciden con cualquiera de estos campos, se mostrarán como resultado de búsqueda.

Licencias para las características de las aplicaciones

Las siguientes características del catálogo de aplicaciones requieren licencias adicionales:

- Instalación/desinstalación silenciosa de aplicaciones: licencia Silver
- Configuración por aplicación: licencia Gold
- Configuración personalizada de AppConnect: licencia Gold
- Configuración personalizada de **Android Enterprise**: Silver license

Si el dispositivo Android está en modo kiosco:

Solo pueden instalarse aplicaciones internas mientras el dispositivo esté en modo kiosco. Puede instalar aplicaciones públicas, pero el dispositivo debe salir del modo kiosco antes de que puedan instalarse las aplicaciones. Además, se pueden limitar la cantidad de aplicaciones disponibles para usarse en dispositivos en el modo kiosco a solamente las aplicaciones que su empresa haya aprobado o puesto en la lista de permitidos. En dispositivos que usen Android 4.1, si una aplicación aprobada inicia una aplicación no incluida en la lista de permitidos, esa aplicación se iniciará y después se minimizará rápidamente. En dispositivos que usen Android 5,0, la aplicación no aprobada iniciada desde una aplicación que está en la lista de permitidos seguirá sin estar disponible.

Alternar entre la vista de lista y de cuadrícula

Haga clic en el icono Lista o Cuadrícula en la parte derecha de la pantalla del catálogo de aplicaciones.

Añadir una aplicación de la Google Play Store para Android Enterprise

- Se puede agregar una aplicación desde Google Play Store al catálogo de aplicaciones y ponerla a disposición de los usuarios. Para añadir una aplicación desde la Google Play Store en Android Enterprise, es necesario aprobar la aplicación para que pueda incluirse en el catálogo de aplicaciones.
- El diseño de Google Play Store para los dispositivos Android Enterprise tiene una página de inicio -para los dispositivos migrados- que se gestiona desde el Core y tiene un enlace rápido a Ivanti Neurons for MDM, que muestra todas las aplicaciones que se gestionan desde Ivanti Neurons for MDM. Al migrar dispositivos Android Enterprise de Core a Ivanti Neurons for MDM, solo las aplicaciones comunes entre el catálogo de aplicaciones de Core e Ivanti Neurons for MDM aparecen en el perfil de trabajo de Google Play Store del dispositivo. Puede hacer clic en el botón Ivanti Neurons for MDM para ver la lista de todas las aplicaciones que están disponibles en el catálogo de aplicaciones de Ivanti Neurons for MDM.

El diseño de Google Play Store para los dispositivos Android Enterprise tiene una página de inicio -para los dispositivos migrados- que se gestiona desde el Core y tiene un enlace rápido a Ivanti Neurons for MDM, que muestra todas las aplicaciones que se gestionan desde Ivanti Neurons for MDM. Al migrar dispositivos Android Enterprise de Core a Ivanti Neurons for MDM, solo las aplicaciones comunes entre el catálogo de aplicaciones de Core e Ivanti Neurons for MDM aparecen en el perfil de trabajo de Google Play Store

del dispositivo. Puede hacer clic en el botón de Ivanti Neurons for MDM para ver todas las aplicaciones que hay disponibles en el catálogo de aplicaciones de Ivanti Neurons for MDM.

Requisito previo

- Se debe habilitar Android Enterprise para acceder y añadir aplicaciones de Google Play store al App Catalog.

ProcedureProcedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Haga clic en **Añadir** (arriba a la izquierda).

> Seleccione Google Play de la lista desplegable para buscar una aplicación en la Google Play Store. Google Play iFrame se muestra cuando Android Enterprise está inscrito.

3. Busque la aplicación en el campo de búsqueda y haga clic en la aplicación.
4. Haga clic en **Hecho**.

> Una aplicación aprobada se puede desaprobar más adelante haciendo clic en **DESAPROBAR**.

Opción	Descripción
Ajustes de aprobación Mantener la aprobación cuando la aplicación solicite nuevos permisos	Permite a los usuario instalar aplicaciones actualizadas
Revocar la aprobación de la aplicación cuando esta aplicación solicite nuevos permisos **Ajustes de aprobación** Añadir suscriptor	**Desinstala la aplicación de la store hasta que se vuelva a aprobar.** Introduzca la dirección de correo electrónico para añadir suscriptores a las notificaciones por correo electrónico cuando las aplicaciones que haya aprobado soliciten nuevos permisos.

Añadir una aplicación desde una store pública

Se puede añadir una aplicación desde una store pública al catálogo de aplicaciones y ponerla disponible para los usuarios.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Haga clic en **Añadir**.
3. Elija la aplicación que desea:
4. Seleccione la app store pública.
5. Introduzca el nombre de la aplicación.
6. Seleccione la aplicación de la lista.

7. Haga clic en **Siguiente**.
8. Describa la aplicación para los usuarios:
9. Añada o elimine categorías.
10. Introduzca una descripción opcional.
11. Haga clic en **Siguiente**.
12. Defina la distribución de aplicaciones:
13. Seleccione una opción de distribución.
14. Amplíe la sección **Opciones avanzadas y configuración de aplicaciones**.
15. Siga las siguientes pautas para completar las opciones:

Ajuste	Qué hacer
Instalar en dispositivo	Seleccione esta opción para iniciar la instalación inmediatamente después del registro. Se solicitará al usuario que confirme la instalación de la aplicación, excepto en las siguientes situaciones: • El dispositivo es un dispositivo iOS supervisado para las instalaciones de nuevas aplicaciones y actualizaciones de aplicaciones. • El dispositivo es un dispositivo iOS no supervisado para actualizaciones de aplicaciones. • Los usuarios que se hayan inscrito en el programa Apps and Books. • El dispositivo es un dispositivo Samsung Knox y se ha seleccionado la opción de instalación silenciosa que aparece a continuación. En el caso de aplicaciones públicas iOS, cuando se instalan por primera vez en el dispositivo, App Catalog muestra el botón 'Reinstalar', que permite al usuario volver a instalar la aplicación. la reinstalación se realiza si la versión de la aplicación es diferente a la versión de la app store de iOS.
No mostrar la aplicación en el App Catalog del usuario final	Seleccione esta opción si no desea que el usuario vea la aplicación en el catálogo de aplicaciones del dispositivo.
Establecer la prioridad de instalación de las aplicaciones	Seleccione Alta, Media o Baja para establecer la prioridad de la instalación de la aplicación durante la incorporación del usuario. Solo se instalan las aplicaciones de alta prioridad durante la incorporación del usuario.
Suspender una segunda inserción de la aplicación después de un número determinado de intentos fallidos (solo iOS)	Ponga el interruptor de conmutación en ON para suspender la segunda inserción de la aplicación después de un número determinado de intentos fallidos de reinserción pulsación utilizando los siguientes ajustes: **Dejar de insertar después de**: introduzca el número de intentos fallidos de reinserción después de los cuales debe dejarse de intentar la inserción. Los valores introducidos deben estar entre **1** y **999** **intentos fallidos y volver a intentarlo después**: introduzca el número de horas necesarias después de la reinserción fallida para volver a intentarlo. Los valores introducidos deben ser estar entre **3** y **48** horas.
(Solo Android) Instalar de forma silenciosa en dispositivos Samsung Knox	Esta opción no es aplicable a las aplicaciones públicas.
(Solo iOS y macOS) Activar la VPN por aplicación para esta aplicación	Seleccione esta opción para usar una **Configuración de VPN por aplicación** con esta aplicación. Seleccione la configuración VPN por aplicación para usarla de la lista desplegable. Para macOS, seleccione solo la configuración de VPN por aplicación de Tunnel.
(Solo iOS) Impedir la copia de seguridad de iCloud e iTunes	Seleccione esta opción para evitar que se haga una copia de seguridad en iCloud e iTunes de los datos relacionados con esta aplicación.
(Solo iOS) Eliminar aplicaciones dadas de baja	Seleccione esta opción para eliminar esta aplicación una vez que el dispositivo ya no esté siendo administrado por Ivanti Neurons for MDM.

Ajuste	Qué hacer
(Solo iOS) Configuración personalizada AppConnect	En la aplicación habilitada para AppConnect, introduzca las claves y valores que especifican sus preferencias de configuración personalizada. Consulte la documentación de la aplicación para ver las claves disponibles.
iOS 7+ Ajustes de la aplicación administrada	Introduzca las claves y valores definidos para esta aplicación a modo de aplicación administrada por iOS 7+. Consulte la documentación de la aplicación para ver información sobre las claves compatibles.

> Las aplicaciones de **Android Enterprise** tendrán opciones distintas.

Haga clic en **Siguiente**.

4. Seleccione una opción de promoción:
5. Haga clic en **+ Añadir descripción** para introducir una breve descripción de la configuración.

- No destacadas
- Lista de destacadas
- Banner destacado
- Si selecciona Banner destacado especifique los siguientes detalles:
    1. **Título**: especifique el título de la aplicación
    2. **Descripción**: especifique los detalles de la aplicación
    3. **Estilo de banner**: seleccione un color de banner

6. Opcionalmente, puede cambiar la distribución de la configuración.
7. Haga clic en **Hecho** para guardar la configuración de la aplicación.
8. Haga clic en **Hecho**.

> Cuando se busca una aplicación de Windows en el Catálogo de aplicaciones, se puede buscar la aplicación que más coincide mediante las opciones **Nombre de la aplicación** o **ID de AppStore** en la lista desplegable:

- **Nombre de la aplicación**: seleccione esta opción para proporcionar el nombre de la aplicación
- **ID de AppStore**: seleccione esta opción para proporcionar la ID de AppStore

La búsqueda de aplicaciones de Windows Store admite aplicaciones de Win32 Store.

Asegúrese de que la herramienta Winget está disponible en el dispositivo para gestionar las aplicaciones de Win32 Store.

Añadir una aplicación interna

Puede cargar una aplicación interna al catálogo de aplicaciones con los siguientes formatos de archivo. Si el archivo es grande puede tardar varios minutos en cargarse. El número de versiones de aplicaciones internas está limitado a 100. Si se supera ese número, el sistema Ivanti Neurons for MDM purga las versiones más antiguas de la aplicación. El estado de la carga y purga de la aplicación aparece en una lista y es visible desde la página de Registros de Auditoría.

El inventario de aplicaciones MIP devuelto por Mobile@Work puede ser incorrecto para algunas aplicaciones. Mobile@Work puede fallar al detectar el estado de instalación de las aplicaciones que no están instaladas en la ubicación predeterminada. Para tales aplicaciones, agregar la secuencia de comandos de detección ayudará a identificar el estado correcto de la aplicación en el dispositivo. Mobile@Work determina la presencia de la aplicación si el código de salida de la secuencia de comandos de detección es 0. Para cualquier otro código de salida, la aplicación se determinará como no instalada. En función de las aplicaciones detectadas, Mobile@Work prepara el informe de inventario para el dispositivo.

- IPA (iOS)
- MIP (aplicación Packager de macOS)
- PKG (macOS)
- APK (Android)
- APPX, APPXBUNDLE, EXE y MSI (Windows)

> Mobile@Work para macOS solo puede detectar solicitudes de instalación correctas en las aplicaciones PKG con secuencias de comandos o DMG con PKG con secuencias de comandos. No informará si la aplicación ha sido borrada o si las secuencias de comandos instalados han sido eliminados. Por tanto, el servidor Ivanti Neurons for MDM no podrá reenviar un comando de instalación. Si se pierde la conexión mientras descarga las aplicaciones, vuelva a intentarlo y haciendo un ingreso. Para las aplicaciones MIP, aun en el caso de que la aplicación se haya eliminado del dispositivo instalado a través de las PKG con secuencias de comandos o DMG con PKG con secuencias de comandos, Mobile@Work no instalará la aplicación MIP si el acceso a las PKG existe en la carpeta de entradas del dispositivo del cliente.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Haga clic en **Añadir** (arriba a la izquierda).
3. En **Seleccione las plataformas para cargar el archivo**, elija la categoría de su plataforma (p. ej., **Apple Apps**) y seleccione el SO específico (p. ej., iOS o macOS en el menú desplegable de Apple Apps).

> Si un usuario selecciona una plataforma e intenta cargar un tipo de archivo en conflicto (p. ej., selecciona Apple pero carga un archivo .apk), el sistema activará un error de "Formato de archivo no válido".

4. Arrastre el archivo de la aplicación hasta el cuadro punteado o haga clic en **Elegir archivo** para seleccionarlo del sistema de archivos y haga clic en **Confirmar**.
5. Haga clic en **Siguiente** (abajo a la derecha).
6. Describa la aplicación para usuarios y configure los requisitos previos de la misma:
7. Añada categorías.
8. Al añadir un paquete macOS, si el archivo del paquete contiene más de una aplicación (por ejemplo, paquetes de Microsoft Office y Cisco AnyConnect), se usarán las aplicaciones principales seleccionadas para identificar que el paquete se ha instalado. La VPN por aplicación, si está configurada, se aplicará a estas aplicaciones.
9. Introduzca una descripción opcional.
10. **Código de producto MSI**: cuando cargue aplicaciones MSI, el código de producto de la aplicación MSI se rellena automáticamente en este campo.

> Debe seleccionar la opción "He marcado el código de producto MSI" para asegurarse de que el GUID correcto esté relleno.

URL de anulación: introduzca una anulación de URL de origen de la aplicación opcional para permitir la descarga de la aplicación desde un origen diferente o para permitir la obtención de archivos grandes, como archivos multimedia para instalar Microsoft Office desde una red local (HTTP y HTTPS). Esta opción requiere acceso a una red interna segura y la sincronización manual de un servidor alternativo donde estén almacenadas las aplicaciones. No introduzca un valor a menos que haya establecido la infraestructura necesaria. Puede editar este valor mientras se editan los ajustes de la aplicación para esa aplicación específica.

- Para aplicaciones de iOS, las URL de reemplazo de aplicaciones debe tener formato HTTP o HTTPS.
- Para aplicaciones de Android y macOS, las URL de reemplazo de aplicaciones solo deben tener formato HTTPS.
- Para aplicaciones de macOS, la URL debe terminado con la extensión .pkg.

6. **Línea de comandos** (Solo aplicaciones MSI Windows de 32 bits): introduzca un conmutador de línea de comandos opcional para especificar la información adicional que no sea parte del paquete mientras se implementan los archivos MSI. Por ejemplo, para escribir registros de la instalación en un archivo de salida, se puede introducir "/log output.txt" en este campo. De este modo, se creará el archivo output.txt en la carpeta C:\Windows\System32. Por defecto, la opción de la línea de comandos /qn para la instalación silenciosa se rellena automáticamente durante la carga de la aplicación MSI.

> El nombre del paquete de la aplicación MSI que se va a cargar no se debe añadir como parte de los argumentos de la línea de comandos. Si se añade, la carga se restringirá hasta que el nombre del paquete de la aplicación se elimine de los argumentos de la línea de comandos. En el enlace adicional se proporciona una lista de todas las opciones admitidas de la línea de comandos. Este enlace será visible en el modo Visualización y Edición de la aplicación.

.EXE for Win32: se instalan a través de Bridge mediante el modo de administrador de PowerShell. La función de Bridge se usará automáticamente si está disponible.

- Actualice la versión para mantener la coherencia entre la **Versión en pantalla** y la **Versión del paquete**
- Ubicación del instalador (.EXE)
- Parámetros de la línea de comandos del instalador: el obligatorio un argumento para ejecutar de forma silenciosa al archivo (por ejemplo, /SILENT o /VERYSILENT).
- Ejecutar instalador como usuario: para instalar usando las credenciales del usuario, seleccione la opción «Ejecutar como usuario».

Para aplicaciones de Win32 Store: se instalan a través de Bridge mediante el modo de administrador de PowerShell.

9. Configure las aplicaciones con requisitos previos para las aplicaciones Packager de macOS (opcional). Consulte Comprender las aplicaciones internas de Packager para macOS para conocer información general acerca de la funcionalidad de las aplicaciones con requisitos previos.
10. **URL de inicio**: ingrese en la URL personalizada para iniciar la aplicación en AppStation. Solo es necesario cuando agregue aplicaciones que no son de AppConnect en un entorno «MAM only» con AppStation y solo es aplicable en aplicaciones iOS.
11. Configure la pestaña **delegación de aplicaciones**.

> Una vez que delega una aplicación con requisitos previos y esta se convierte en aplicación con requisitos previos del espacio no predeterminado, no se puede dejar de delegar esa aplicación a menos que elimine primero la relación de requisito previo.

Haga clic en **Siguiente**.

13. Haga clic en **Siguiente**.
14. (Opcional) Añada capturas de pantalla de la aplicación.

15. (Opcional) Añada o sustituya los iconos de la aplicación (aplicaciones para iOS, macOS y Windows).
16. Haga clic en **Siguiente**.
17. Para las aplicaciones Packager de macOS, defina o seleccione las secuencias de comandos de instalación que se ejecutarán antes y/o después de la instalación de la aplicación. Seleccione uno o ambos de los siguientes secuencias de comandos escribiendo en el cuadro de búsqueda o haciendo clic en el enlace para ver la lista de secuencias de comandos. Haga clic en **Siguiente**.
18. Puede crear las secuencias de comandos en la página **Administración > Secuencias de comandos y archivos > Todas la Secuencias de comandos**. Si actualiza la aplicación, puedes elegir copiar las secuencias de comandos de la aplicación anterior y ejecutar las secuencias de comandos de la aplicación actualizada. Si omite esta sección, puede configurar las secuencias de comandos editando la aplicación más tarde.

- **Secuencias de comandos de preinstalación**: introduzca el nombre de la secuencia de comandos para seleccionar la secuencia de comandos que se ejecutará antes de la instalación de la aplicación. Las secuencia de comandos de preinstalación se ejecutarán o volverán a ejecutarse hasta que se reciba del cliente el estado de éxito de la ejecución de la secuencia de comandos. Solo después de eso, se envía el comando de instalación de la aplicación. Puede ver el estado de ejecución de ka secuencia de comandos en la página de detalles del dispositivo en la pestaña **Registros**.
- **Secuencias de comandos de preinstalación**: introduzca el nombre de la secuencia de comandos para seleccionar la secuencia de comandos que se ejecutará antes de la instalación de la aplicación.
- **Secuencias de comandos de desinstalación**: introduzca el nombre de la secuencia de comandos que el servidor envía a un dispositivo cuando detecta que una aplicación ya no se distribuye al dispositivo.
- **Secuencias de comandos de detección**: ingrese el nombre de la secuencia de comandos que el servidor envía a un dispositivo para detectar una aplicación. El resultado de la secuencia de comandos de detección de la aplicación anula el resultado del inventario predeterminado de la aplicación en el dispositivo. Independientemente de si la aplicación se distribuye al dispositivo o no, la secuencia de comandos de detección de todas las aplicaciones se enviará al dispositivo para evaluar la existencia de las aplicaciones en el dispositivo.
  A continuación se muestra una secuencia de comandos de detección de muestra:

```
#!/bin/bash
app_name="Name of the App"
count="$(system_profiler SPApplicationsDataType | grep "$app_name" -c)"
echo "$app_name count $count"
if [ $count -ge 1 ]
then
echo "$app_name is installed"
else
echo "$app_name is not installed"
exit 1
fi
exit 0
```

Defina la distribución de aplicaciones:

12. Seleccione una opción de promoción:
13. Seleccione una opción de distribución.
14. Amplíe la sección **Opciones avanzadas y configuración de aplicaciones**.
15. Siga las siguientes pautas para completar las opciones:
16. Haga clic en **Siguiente**.

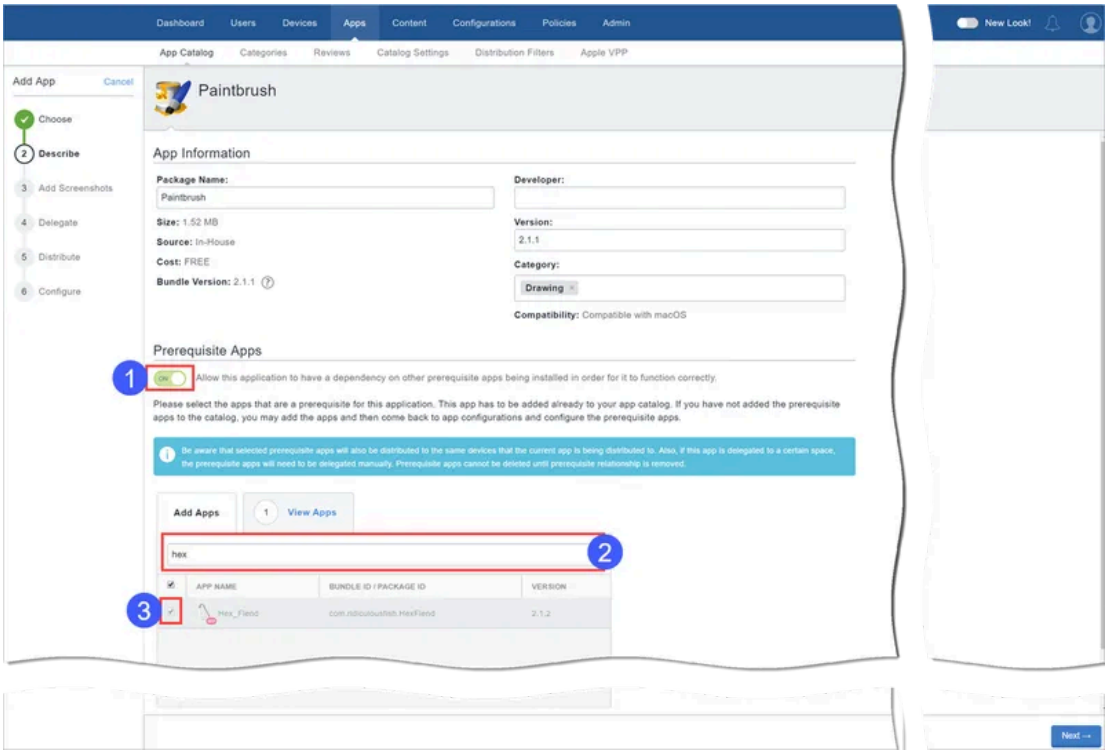
Ajuste	Qué hacer
Instalar en dispositivo	Seleccione esta opción para iniciar la instalación inmediatamente después del registro. Se solicitará al usuario que confirme la instalación de la aplicación, excepto en las siguientes situaciones: • El dispositivo es un dispositivo iOS supervisado. • El dispositivo es un dispositivo Samsung Knox y se ha seleccionado la opción de instalación silenciosa que aparece a continuación.
No mostrar la aplicación en el App Catalog del usuario final	Seleccione esta opción si no desea que el usuario vea la aplicación en el catálogo de aplicaciones del dispositivo.
Establecer la prioridad de instalación de las aplicaciones	Seleccione Alta, Media o Baja para establecer la prioridad de la instalación de la aplicación durante la incorporación del usuario. Solo se instalan las aplicaciones de alta prioridad durante la incorporación del usuario.
Suspender una segunda inserción de la aplicación después de un número determinado de intentos fallidos (solo iOS)	Ponga el interruptor de conmutación en ON para suspender la segunda inserción de la aplicación después de un número determinado de intentos fallidos de reinserción pulsación utilizando los siguientes ajustes: **Dejar de insertar después de**: introduzca el número de intentos fallidos de reinserción después de los cuales debe dejarse de intentar la inserción. Los valores introducidos deben estar entre **1** y **999** **intentos fallidos y volver a intentarlo después**: introduzca el número de horas necesarias después de la reinserción fallida para volver a intentarlo. Los valores introducidos deben ser estar entre **3** y **48** horas.
(Solo Android) Instalar de forma silenciosa en dispositivos Samsung Knox	Seleccione esta opción si no desea que se solicite al usuario que confirme la instalación en dispositivos Samsung KNOX.
(Solo iOS y macOS) Activar la VPN por aplicación para esta aplicación	Seleccione esta opción para usar una **Configuración de VPN por aplicación** con esta aplicación. Seleccione la configuración VPN por aplicación para usarla de la lista desplegable. Para macOS, seleccione solo la configuración de VPN por aplicación de Tunnel.
(Solo iOS) Impedir la copia de seguridad de iCloud e iTunes	Seleccione esta opción para evitar que se haga una copia de seguridad en iCloud e iTunes de los datos relacionados con esta aplicación.
(Solo iOS) Eliminar aplicaciones dadas de baja	Seleccione esta opción para eliminar esta aplicación una vez que el dispositivo ya no esté siendo administrado por Ivanti Neurons for MDM.
(Solo iOS) Configuración personalizada AppConnect	En la aplicación habilitada para AppConnect, introduzca las claves y valores que especifican sus preferencias de configuración personalizada. Consulte la documentación de la aplicación para ver las claves disponibles.
iOS 7+ Ajustes de la aplicación administrada	Introduzca las claves y valores definidos para esta aplicación a modo de aplicación administrada por iOS 7+. Consulte la documentación de la aplicación para ver información sobre las claves compatibles.

17. Haga clic en **Hecho**.

- No destacadas
- Lista de destacadas
- Banner

Comprender las aplicaciones internas de Packager de macOS

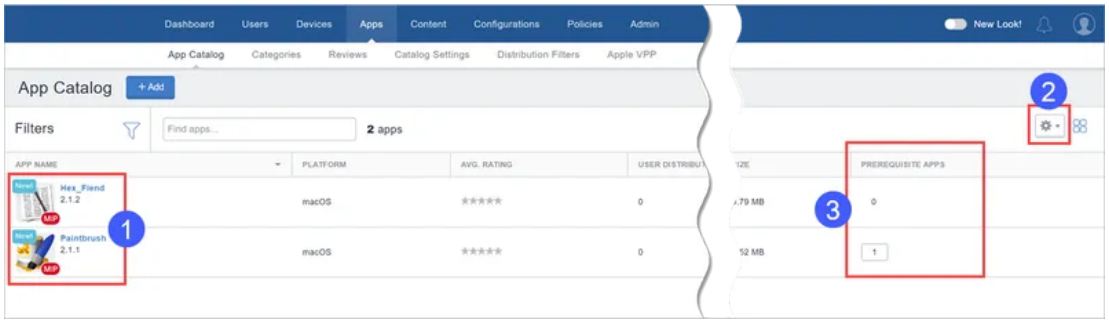
A la hora de importar aplicaciones internas de Packager de macOS, el administrador puede activar 1, la función de aplicaciones con requisitos previos, para buscar 2 y seleccionar 3, las aplicaciones con requisitos previos que deben instalarse en los clientes antes de poder instalar la aplicación que el administrador está importando.



Una vez importada, la aplicación interna Packager de macOS aparecerá en el app catalog con el MIP identificador debajo 1. A continuación podrá usar los ajustes de la columna, 2, para añadir la columna APLICACIONES CON REQUISITOS PREVIOS (PREREQUISITE APPS), 3, con el fin de ver rápidamente las aplicaciones que tienen dependencias, es decir, las que tienen requisitos previos.

- Puede buscar y seleccionar aplicaciones de tipo MIP, no MIP y aplicaciones públicas (Apps and Books y aplicaciones públicas de la App Store de macOS) como aplicaciones con requisitos previos.
- Los usuarios deben aceptar la licencia de Apps and Books para que las aplicaciones con requisitos previos de Apps and Books se instalen de forma silenciosa.
- Para las aplicaciones públicas con requisitos previos que no sean de Apps and Books, los administradores deben distribuir explícitamente las aplicaciones públicas y el usuario debe instalarlas. Hay que importar las aplicaciones públicas (de Apps and Books y que no sean de Apps and Books) en el App Catalog para que puedan aparecer en la lista de aplicaciones con requisitos previos. La columna «Origen» indica el tipo de aplicación con requisitos previos.
- El ingreso de MDM es obligatorio para instalar una aplicación interna que no sea MIP que tenga aplicaciones con requisitos previos que no sean de MIP.
- Los usuarios deben instalar manualmente aplicaciones públicas con requisitos previos que no sean de Apps and Books.

- Si se elimina el token de Apps and Books o si la licencia ha caducado, no se instalarán las aplicaciones de Apps and Books seleccionadas como aplicaciones con requisitos previos y, por ende, tampoco la aplicación principal. El administrador debe seguir la práctica recomendada para informar a los usuarios con antelación para las aplicaciones de Apps and Books en cualquiera de estos casos.

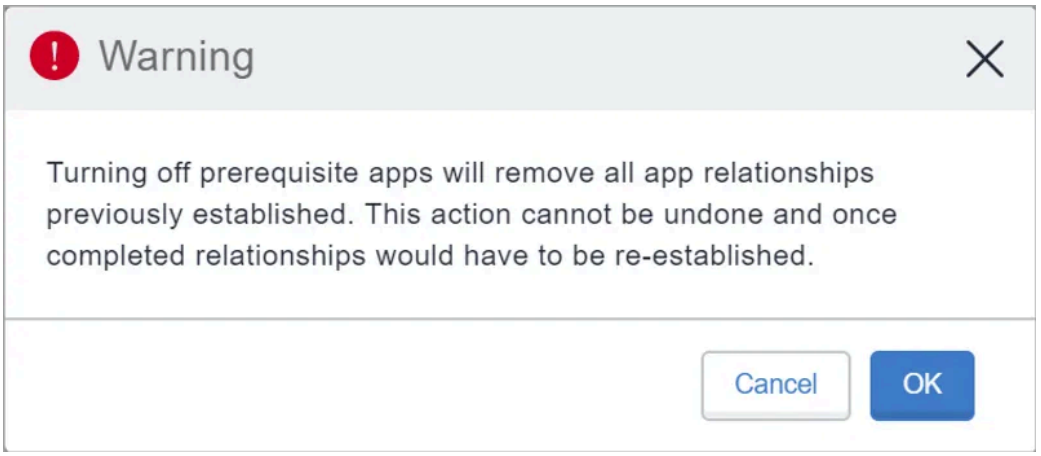


Las aplicaciones con requisitos previos también están disponibles como aplicaciones independientes para que el usuario las descargue cuando se distribuyan explícitamente. Si el usuario intenta desinstalar una aplicación con requisitos previos:

- Asegúrese de que la aplicación necesaria se instala de nuevo en el siguiente registro del dispositivo.
- La aplicación con requisitos previos se desinstalará si no hay ninguna aplicación principal dependiente en el mismo dispositivo.
- Si la aplicación con requisitos previos no se ha distribuido explícitamente, se desinstalará junto con la aplicación principal.
- Si la aplicación con requisitos previos se ha distribuido explícitamente, se mantendrá en el dispositivo.
- Si la aplicación con requisitos previos tiene una aplicación dependiente, se mantendrá en el dispositivo.

Desactivar la función de aplicaciones con requisitos previos

Cuando interactúe con aplicaciones que tienen dependencias y aplicaciones con requisitos previos, p. ej. al actualizar, borrar o delegar dichas aplicaciones, encontrará mensajes del sistema que le informarán de cómo la dependencia o el requisito previo de la aplicación puede afectar a las acciones que usted va a realizar. Por ejemplo, cuando intente desactivar la función «Aplicaciones con requisitos previos» para una aplicación, aparecerá el siguiente mensaje:



- Si desactiva la función «Aplicaciones con requisitos previos» para una aplicación, desaparecerán los detalles sobre las aplicaciones con requisitos previos. Esto incluye la delegación automática y la no delegación de las aplicaciones con requisitos previos de los subespacios.
- En Apps@Work, el botón de instalación no aparecerá para las aplicaciones dependientes cuyas aplicaciones con requisitos previos no estén ya instaladas en el cliente receptor.

- En los dispositivos de los usuarios, cuando un usuario intenta instalar una aplicación interna con dependencias, se instalarán primero las aplicaciones con requisitos previos (si no están ya instaladas) y, a continuación, la aplicación principal. Este proceso podrá tardar algunos minutos. Al usuario le aparecerá un listado de aplicaciones dependientes junto con el estado de su instalación.

Delegación y no delegación de las aplicaciones con requisitos previos de los espacios

- Las aplicaciones con requisitos previos vinculadas a una aplicación (la aplicación principal) se delegan automáticamente cuando la aplicación principal se delega a un subespacio.
- Si la aplicación principal no está delegada a un subespacio, las aplicaciones con requisitos previos tampoco lo estarán en los casos en los que las aplicaciones con requisitos previos no estén explícitamente distribuidas. De todos modos, en las aplicaciones con requisitos previos que están vinculadas a más de una aplicación principal no se podrá cancelar la delegación.
- Si las aplicaciones con requisitos previos están explícitamente delegadas, entonces no se puede cancelar su delegación automáticamente.

Delegar permisos de dispositivos delegados para aplicaciones internas de Android Enterprise

Se pueden asignar permisos delegados a aplicaciones internas que se pueden aplicar a dispositivos gestionados por Android Enterprise y dispositivos AMA.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. En el **App Catalog**, seleccione la aplicación para la que desee delegar permisos de dispositivos.
3. Haga clic en la pestaña **Configuraciones de la aplicación**.
4. En Permisos delegados (aplicación interna Android Enterprise), seleccione los permisos necesarios para las aplicaciones:

> Solo la implementación de COSU usa AMAPI. Consulte la sección AMAPI para obtener más información.

   - **Configurar permisos del tiempo de ejecución de aplicaciones de terceros**
   - **Ocultar y suspender aplicaciones de terceros**
   - **Administrar certificados**
   - **Gestionar las configuraciones de las aplicaciones**
   - **Administrar el bloqueo de la desinstalación de aplicaciones**
   - **Gestionar la habilitación de aplicaciones del sistema**
   - **Administrar la selección de certificados** (no compatible con el modo AMAPI)
   - **Administrar la retención de aplicaciones no instaladas** (no compatible con el modo AMAPI)
   - **Gestionar la recopilación de redes** (compatible solo con una aplicación a la vez)
   - **Gestión de la recopilación de registros de seguridad** (compatible solo con una aplicación a la vez)
   - **Administrar la instalación de aplicaciones existentes** (no compatible con el modo AMAPI)
   - **Instalar y eliminar paquetes** (no compatible con el modo AMAPI)

La opción Instalar y desinstalar paquetes está disponible en todos los dispositivos que admiten el modo propietario del dispositivo Android (7.0 o posterior). Hay otros permisos delegados que solamente son aplicables a Android 8.0 o posterior.

Configure las opciones de distribución seleccionando entre **A todas las personas con la aplicación**, **A nadie** o **Personalizado**.

6. Haga clic en **Guardar**.

Mostrar el estado del perfil de aprovisionamiento para las aplicaciones internas de iOS

Mostrar el perfil del estado de aprovisionamiento de la página del Catálogo de aplicaciones para las aplicaciones internas de iOS. La información sobre herramientas que hay junto al nombre del perfil muestra el número de días que quedan para que el perfil caduque. Este estado puede resultar útil para comprobar cuándo van a caducar los perfiles de aprovisionamiento para las aplicaciones internas.

Este estado es útil para solucionar problemas de aplicaciones que no se instalan porque el perfil va a caducar. Si no hay un perfil de aprovisionamiento adecuado, las aplicaciones se instalan pero no se abrirán ni se iniciarán.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Haga clic en el icono del engranaje que hay en la parte superior derecha para que aparezcan las columnas.
3. Seleccione **Perfil de aprovisionamiento** para ver la columna de la lista de aplicaciones en la página del App Catalog.

Los detalles del Perfil de aprovisionamiento también están disponibles en la página de detalles de la aplicación, bajo la sección Ajustes del perfil de aprovisionamiento.

Actualizar el perfil de aprovisionamiento para las aplicaciones internas de iOS

El perfil de aprovisionamiento se aplica a una aplicación interna específica de iOS. Los detalles del perfil de aprovisionamiento de una aplicación están disponibles en la página de detalles de la aplicación. Es necesario tener un perfil de aprovisionamiento que no haya caducado para iniciar una aplicación interna iOS en el dispositivo. Si ha caducado, se puede actualizar el perfil de aprovisionamiento cargando el perfil de la página de detalles de la aplicación.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Haga clic en la aplicación para la que es necesaria la actualización del perfil de aprovisionamiento. Aparecerá la página de detalles de la aplicación.
3. Haga clic en **Editar**.
4. En la sección **Perfil de aprovisionamiento**, haga clic en **Elegir archivo**.
5. Seleccione el archivo de perfil de aprovisionamiento (extensión de archivo .mobileprovision) que desea actualizar y haga clic en **Guardar**.

Implementar aplicaciones internas en Google Play

Cargue las aplicaciones internas en el canal privado de Google Play e impórtelas a Ivanti Neurons para MDM para su despliegue en dispositivos con Android Enterprise.

Procedimiento

1. Inicie sesión en la consola de aplicaciones privadas de Google: **https://play.google.com/apps/publish**.
2. Haga clic en **Todas las aplicaciones** en el menú de la izquierda.
3. Haga clic en **Crear nueva aplicación** e introduzca un nombre para dicha aplicación.

4. Haga clic en **Cargar APK** para cargar el archivo .apk que ha generado.
5. Haga clic en **Listado de tiendas**:
    - Introduzca una breve descripción y una descripción completa.
    - Cargue la captura de pantalla para todas las pestañas.
    - Cargue un icono de alta resolución.
    - Cargue un icono gráfico de características (graphic.png).
    - Introduzca la información obligatoria para Categorización, Detalles de contacto y Política de privacidad.
    - Complete el cuestionario de calificación de la aplicación.
6. Haga clic en **Precios y distribución**.
   Si ya ha introducido toda la información obligatoria, aparecerá «Listo para publicarse» en la parte superior de la pantalla.
7. Vaya a la pestaña Aplicaciones de Ivanti Neurons for MDM.
8. Haga clic en **Actualizar catálogos disponibles** para sincronizar sus aplicaciones privadas.

> pueden pasar varias horas hasta que su aplicación se publique.

Añadir una aplicación web para dispositivos con Android Enterprise

Una aplicación web es un enlace a cualquier sitio web, que se instala en el dispositivo en forma de acceso directo. Las aplicaciones web funcionan del mismo modo que cualquier otra aplicación, lo cual significa que se puede distribuir siguiendo los mismos criterios que una aplicación. Aparece en el catálogo de aplicaciones y la pueden instalar los usuarios del mismo modo que cualquier otra aplicación. No obstante, las aplicaciones web puede que tengan una sola versión y que no se admita la instalación silenciosa. Las aplicaciones web utilizan clips web y se instalan en el dispositivo como configuraciones, pero funcionan como aplicaciones.

Configure un clip web como aplicación en el catálogo de aplicaciones para que la aplicación web esté disponible para los usuarios en el catálogo de aplicaciones. El clip web se puede definir como una configuración, pero esta solo la puede distribuir el administrador. Los usuarios pueden optar por instalar la aplicación web en sus dispositivos o no hacerlo, mientras que no pueden rechazar la configuración del clip web.

En Android Enterprise, una aplicación web es una forma incrustada de aplicación web que se ejecuta sobre Google Chrome dentro del perfil de trabajo. Puede combinarse con una VPN o soluciones SSO en Android Enterprise. Después de crear una aplicación web, la aplicación funciona como cualquier otra aplicación de Android, que usted podrá distribuir según sea necesario. Las aplicaciones web requieren que Chrome esté instalado en el Perfil de trabajo del Dispositivo propiedad de la empresa para poder ejecutarse.

> Si hay algún problema con el uso de esta función, los administradores pueden ponerse en contacto con la **asistencia técnica**.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Haga clic en **+ Añadir**.
3. Seleccione **Google Play** de la lista desplegable para buscar una aplicación en la Google Play Store. Google Play iFrame se muestra si Android Enterprise está inscrito.
4. Haga clic en Aplicación **web**.
5. Describa la aplicación para los usuarios:
    1. Título o nombre de la aplicación.

2. URL de la aplicación.
3. Tipo de visualización para la aplicación web.
4. Icono de carga, que puede ser una imagen PNG o JPEG cuadrada de 512px.

Haga clic en **Crear**. Espere a que la aplicación se publique en iFrame. Esto puede tardar algunos minutos. Puedes cerrarla y volver más tarde.

7. Una vez que la aplicación web esté publicada, importe la aplicación al app catalog para su distribución. Haga clic en el icono de la aplicación web.
8. Desplácese hacia abajo y haga clic en **Seleccionar**.
9. Añada categorías y una descripción opcional.
10. Haga clic en **Siguiente**.
11. Seleccione una de las siguientes opciones para la delegación de aplicaciones:
    - Delegar esta aplicación a todos los espacios.
    - No delegar esta aplicación a todos los espacios.

Haga clic en **Siguiente**.

13. Seleccione una opción de distribución para la aplicación.
14. Haga clic en **Finalizar**.

Después de añadir una aplicación web, puede editarla siempre que lo necesite. Para hacerlo:

1. En la página **App Catalog**, haga clic en el nombre de la aplicación web existente.
2. Haga clic en **Editar** para editar los campos de la aplicación web.

Añadir una aplicación web para dispositivos iOS

Una aplicación web es un enlace a cualquier sitio web, que se instala en el dispositivo en forma de acceso directo. Las aplicaciones web funcionan del mismo modo que cualquier otra aplicación, lo cual significa que se puede distribuir siguiendo los mismos criterios que una aplicación. Aparece en el catálogo de aplicaciones y la pueden instalar los usuarios del mismo modo que cualquier otra aplicación. No obstante, las aplicaciones web puede que tengan una sola versión y que no se admita la instalación silenciosa. Las aplicaciones web utilizan clips web y se instalan en el dispositivo como configuraciones, pero funcionan como aplicaciones.

Configure un clip web como aplicación en el catálogo de aplicaciones para que la aplicación web esté disponible para los usuarios en el catálogo de aplicaciones. El clip web se puede definir como una configuración, pero esta solo la puede distribuir el administrador. Los usuarios pueden optar por instalar la aplicación web en sus dispositivos o no hacerlo, mientras que no pueden rechazar la configuración del clip web.

> Si hay algún problema con el uso de esta función, los administradores pueden ponerse en contacto con la **asistencia técnica**.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Haga clic en **+Añadir** (arriba a la izquierda).
3. Haga clic en **Aplicaciones web**.
4. Describa la aplicación para los usuarios:

1. Nombre de la aplicación.
2. URL de la aplicación.
3. Tipo de plataforma.
4. Icono de la aplicación.
5. Añada o elimine categorías.
6. Pantalla completa: seleccione esta opción para que la aplicación web se muestre a pantalla completa.
7. Extraíble: seleccione esta opción para hacer que la aplicación web sea extraíble.
8. Haga clic en **Siguiente**.

Seleccione una de las siguientes opciones para la delegación de aplicaciones:

- Delegar esta aplicación a todos los espacios.
- No delegar esta aplicación a todos los espacios.

Haga clic en **Siguiente**.

7. Seleccione una opción de distribución para la aplicación.
8. Haga clic en **Finalizar**.

Edición de una aplicación web

Después de añadir una aplicación web, puede editarla siempre que lo necesite.

Procedimiento

1. En la página **App Catalog**, haga clic en el nombre de la aplicación web existente.
2. Haga clic en **Editar** para editar los campos de la aplicación web.

Distribución de despliegue lento

El ajuste de **Distribución con despliegue gradual** permite a los administradores implementar automáticamente nuevas versiones de las aplicaciones en los dispositivos de forma gradual. La opción Utilizar el método de distribución de implementación lenta está disponible cuando se instala la siguiente versión de la aplicación. El portal administrativo de Ivanti Neurons for MDM le permite editar aplicaciones aun cuando la implementación lenta esté pausada.

Una vez que se establece la implementación lenta para una versión, se aplica para las siguientes con el mismo porcentaje que se estableció la última vez. Puede pausar la distribución de una aplicación si la distribución está configurada al 100 %. Sin embargo, si establece el objetivo de distribución al 100 %, debe establecer manualmente el porcentaje de objetivo de distribución para la siguiente versión, ya que la interfaz de usuario restablece el porcentaje al 0% .

Procedimiento

1.	**Vaya a App Catalog, Aplicaciones, y seleccione una de las opciones de modo de distribución.**

2.	**Seleccione la opción % de dispositivos en el resumen de la selección (implementación lenta).**

3.	**Desde la configuración de implementación lenta**, arrastre el control deslizante en **Especificar el % objetivo de distribución.**

4.	**Haga clic en Confirmar y, luego, haga clic en Hecho. Se muestra el estado de la última versión de la aplicación. La página del App Catalog indica el estado de IMPLEMENTACIÓN LENTA en la tabla.**

Si no puede realizar las tareas en la página **App Catalog**, puede ser que no tenga los permisos necesarios. Necesita el rol de Administración de aplicaciones y contenido.

Uso de la búsqueda avanzada

Puede utilizar la opción de Búsqueda avanzada para buscar una aplicación en función de reglas para identificar y ver las aplicaciones con criterios específicos. Estas reglas se pueden crear usando los operadores correspondientes, como «igual a», «es menor que», «es mayor que», «está igual que» y «no es igual que». Las opciones de reglas se pueden anidar juntas utilizando las opciones CUALQUIERA (O) o TODOS (Y). Las aplicaciones que coinciden con las reglas se muestran debajo de la sección.

> Los valores de los atributos personalizados que se usan en Buscar distinguen entre mayúsculas y minúsculas.

Procedimiento

1. Desde la página del Catálogo de aplicaciones, haga clic en el enlace **Búsqueda avanzada**. Se abre el asistente de Búsqueda avanzada.
2. Haga clic en una de las siguientes opciones:
   - **Cualquiera**: si las aplicaciones deben cumplir al menos una de las reglas
   - **Todas**: si las aplicaciones deben cumplir todas la regla

Para crear una regla que defina los criterios de búsqueda, seleccione una de las opciones siguientes y seleccione la acción asociada adecuada:

- AppConnect activado
- Valoración media
- ID de paquete
- Categoría
- Coste
- Atributos personalizados
- Fecha en que se agregó a AppCatalog
- Fecha de modificación
- Distribución de dispositivos
- Distribución de grupos de dispositivos
- Tipo de dispositivo
- Distribución de grupo
- Versión de SO mínima
- Nombre

- Plataforma de SO
- Perfil de aprovisionamiento
- Tamaño
- Fuente
- Distribución de usuarios
- Nombre de los grupos de usuarios
- Versión

4. (Opcional) Haga clic en **+** para crear reglas adicionales, si fuera necesario.
5. Haga clic en **Buscar**. Se muestra la lista de aplicaciones que coinciden con los criterios de búsqueda.

Carga de las consultas de búsqueda

Puede ver la lista de consultas de búsqueda guardadas.

Procedimiento

1. Haga clic en Búsqueda avanzada y luego en el icono de la carpeta. La lista de las consultas de búsqueda creadas se muestra en la sección **Cargar consulta** y se muestran los detalles siguientes:
   - **Nombre de la consulta**: el nombre de la consulta cargada.
   - **Contenido de la consulta** muestra el contenido de las reglas que definen la consulta de búsqueda.
   - **Acciones**: seleccione la acción que se realizará en la consulta.
2. Haga clic en **Cargar consulta** en la columna **Acciones** para ver la lista de aplicaciones que coinciden con los criterios definidos en la consulta cargada.
3. Haga clic en **Eliminar** para borrar una consulta guardada.

Exportación de aplicaciones a un archivo CSV

Puede exportar las aplicaciones mediante la opción Exportar a CSV de la página App Catalog.

Procedimiento

1. Vaya a **Aplicaciones** > **Catálogo de aplicaciones**.
2. Haga clic en la opción **Exportar a CSV** para exportar la lista de aplicaciones y detalles relacionados a un archivo CSV.

> Solo se incluyen las aplicaciones que figuran en el espacio seleccionado, y todos los resultados paginados se compilan en un único archivo.

> El uso de filtros o resultados de búsqueda exportará solo las aplicaciones relevantes.

3. Aparecerá un mensaje con los botones **Continuar** y **Cancelar** que indicará si se ha iniciado el proceso de exportación y que en breve estará disponible un informe.
4. Haga clic en **Continuar** y espere a que se complete la solicitud para enviar otra.
5. Aparecerá un mensaje que indica que **App Catalog: le informe CSV ha finalizado** con los botones **Descargar** y **Eliminar**.
6. Haga clic en **Descargar** para descargar el informe.

7. (Opcional) Haga clic en **Eliminar** para eliminar el informe.

> La opción **Exportar a CSV** se volverá a activar solo después de seleccionar la opción **Descargar** o **Eliminar**.

> Si hay varias versiones de una aplicación, se mostrará una entrada por cada versión.

Temas relacionados

- Funciones del usuario
- Eliminar aplicaciones del App Catalog
- Instalar dependencias de aplicaciones

8.2. Gestión de aplicaciones mediante Declarative Device Management (DDM)

Información general

La gestión de aplicaciones mediante Declarative Device Management (DDM) permite utilizar el marco de gestión declarativa de Apple para desplegar aplicaciones y gestionar su ciclo de vida en dispositivos iOS y iPadOS. En lugar de depender del envío continuo de comandos y de consultas periódicas, DDM permite a los dispositivos aplicar las declaraciones localmente y comunicar de forma proactiva cualquier cambio de estado.

Con DDM, el servidor solo necesita enviar la declaración al dispositivo una vez. A continuación, el dispositivo aplica la configuración, supervisa su estado y comunica al servidor cualquier cambio de estado. Este enfoque basado en el dispositivo reduce las comunicaciones con el servidor, mejora la escalabilidad y permite disponer de actualizaciones de estado más rápidas durante el despliegue de aplicaciones.

Actualmente, la gestión de aplicaciones mediante DDM se centra en las funcionalidades esenciales para gestionar aplicaciones en dispositivos Apple compatibles.

Flujo de trabajo para la gestión de aplicaciones mediante DDM

En un flujo de trabajo de DDM, el servidor envía el estado deseado al dispositivo, que pasa a ser responsable de mantenerlo y notificar cualquier cambio en su estado.

Cuando se asigna una aplicación a un dispositivo habilitado para DDM:

1. El servidor envía al dispositivo una declaración de aplicación.
2. El dispositivo procesa la declaración de forma local.
3. El dispositivo instala, actualiza o mantiene la aplicación según la configuración asignada.
4. El dispositivo supervisa de forma continua el estado de la aplicación.
5. El dispositivo notifica inmediatamente al servidor cualquier cambio en el estado de instalación o de la aplicación.

Este modelo declarativo permite consultar casi en tiempo real el progreso del despliegue de aplicaciones sin necesidad de realizar consultas periódicas.

Habilitar la gestión de aplicaciones mediante DDM

La gestión de aplicaciones mediante DDM se habilita desde Configuración de usuario y se asigna a grupos de usuarios específicos.

Para habilitar la gestión de aplicaciones mediante DDM:

1. Vaya a **Usuarios** > **Ajustes de usuario.**
2. En **Ajuste de Apple DDM**, haga clic en **+Añadir** ajuste para un grupo de usuarios específico. Abrirá la página **Ajustes de Apple DDM**.
3. Introduzca un nombre y active el control deslizante **Habilitar la gestión de aplicaciones mediante DDM**.
4. Haga clic en **Siguiente**. Abrirá la página **Distribución de ajustes de usuario**.
5. Seleccione el grupo de usuarios que utilizará la gestión de aplicaciones mediante DDM.
6. Haga clic en **Hecho**.

Una vez habilitado DDM para un grupo de usuarios, todas las aplicaciones compatibles asignadas a los usuarios de dicho grupo se gestionan mediante la gestión de aplicaciones mediante DDM. La configuración de DDM se aplica a todo el entorno, pero se despliega mediante asignaciones a grupos de usuarios, lo que permite a las organizaciones implementar DDM gradualmente para usuarios o grupos seleccionados.

Métodos de inscripción compatibles

La gestión de aplicaciones mediante DDM es compatible con dispositivos iOS/iPadOS inscritos mediante:

- iReg/cliente Ivanti Go administrado
- Perfil de inscripción de dispositivos (DEP)
- Inscripción de dispositivos basada en cuenta

Tipos de aplicaciones compatibles

La gestión de aplicaciones mediante DDM es compatible con los siguientes tipos de aplicaciones:

- Aplicaciones públicas
- Aplicaciones VPP (solo disponibles con la inscripción de dispositivos)
- Aplicaciones internas

El flujo de trabajo para asignar y desplegar aplicaciones apenas cambia con respecto al utilizado en los despliegues tradicionales de N-MDM. Los procesos actuales de distribución de aplicaciones siguen funcionando y aprovechan las capacidades mejoradas de DDM para proporcionar información sobre el estado.

8.2.1. Ajustes de la gestión de aplicaciones mediante DDM

En general, la gestión de aplicaciones incluye las siguientes configuraciones:

- Impedir la copia de seguridad en iCloud
- No instalar la aplicación en dispositivos recién inscritos
- Red móvil 5G
- Proxy DNS
- Configuración de aplicaciones administradas
- Aplicaciones empresariales: Apps@Work, Email+, etc.
- VPN por aplicación
- Relé de red
- Filtro de contenido web
- Permitir actualizaciones de App Store

Además de las configuraciones anteriores, la gestión de aplicaciones mediante DDM ofrece varias funcionalidades disponibles exclusivamente en dispositivos administrados mediante DDM.

Fijación de versiones de aplicaciones

La fijación de versiones de aplicaciones permite a los administradores desplegar una versión específica de una aplicación y mantenerla en los dispositivos administrados mediante DDM.

Cuando se habilita la fijación de versiones:

- Los dispositivos instalan la versión de aplicación especificada.
- Se impiden las actualizaciones automáticas a versiones más recientes.
- Las aplicaciones permanecen en la versión asignada hasta que un administrador selecciona de forma explícita una nueva versión.

Esta funcionalidad permite un mayor control sobre la coherencia de las versiones de las aplicaciones y los despliegues de actualizaciones por fases.

Procedimiento

1. Vaya a **Aplicaciones** > **Catálogo de aplicaciones**.
2. Haga clic en una aplicación de la lista mostrada. Abrirá la página **Detalles de la aplicación**.
3. En la pestaña **Configuraciones de aplicaciones**, haga clic en **Ajustes de aplicaciones de Apple**.
4. Haga clic en cualquiera de las configuraciones disponibles de la lista.
5. Haga clic en **Editar**.
6. En la sección **Fijar la versión de la aplicación en un dispositivo**, selecciones la opción **Fijar la versión de la aplicación**.
7. En la lista **Seleccionar versión de la aplicación**, seleccione la versión de la aplicación que desea utilizar.

> Si el dispositivo ya tiene instalada una versión de la aplicación, no puede sustituirla por una versión anterior.

8. Haga clic en **Actualizar**.

Controles automatizados de las actualizaciones de la App Store (actualización automática de aplicaciones)

Los administradores pueden configurar cómo se gestionan las actualizaciones de la App Store de las aplicaciones administradas. Esta funcionalidad permite controlar mejor las actualizaciones de las aplicaciones y ayuda a las organizaciones a adaptarlas a sus procesos internos de validación y despliegue.

Permitir descargas a través de redes móviles

DDM incorpora una configuración específica para controlar las descargas y actualizaciones de aplicaciones a través de redes móviles.

Procedimiento

1. Vaya a **Aplicaciones** > **Catálogo de aplicaciones**.
2. Haga clic en una aplicación de la lista mostrada. Abrirá la página **Detalles de la aplicación**.
3. En la pestaña **Configuraciones de aplicaciones**, haga clic en **Instalar en el dispositivo**.
4. Haga clic en cualquiera de las configuraciones disponibles de la lista.
5. Haga clic en **Editar**.
6. En la sección **Descargas permitidas a través de redes móviles**, seleccione una de las siguientes opciones:
    - **Ajustes de la tienda**: opción predeterminada. El dispositivo utiliza la configuración de la tienda correspondiente al descargar aplicaciones.
    - **Siempre activado:** se permite descargar aplicaciones incluso cuando el dispositivo no dispone de conexión Wi-Fi.
    - **Siempre desactivado:** no se pueden descargar aplicaciones cuando el dispositivo no dispone de conexión Wi-Fi.
7. Haga clic en **Actualizar**.

Flujo de instalación de aplicaciones

El proceso de distribución de aplicaciones sigue siendo similar al de la gestión tradicional de aplicaciones mediante N-MDM.

Los administradores pueden:

- Asignar aplicaciones
- Distribuir aplicaciones
- Instalar aplicaciones

Sin embargo, DDM modifica la forma en que se comunica el estado del despliegue. En lugar de depender de las consultas del servidor, los dispositivos informan de los cambios en el estado de las aplicaciones en cuanto se completa una acción. Esto permite obtener información más precisa y oportuna sobre el progreso de la instalación y los resultados del despliegue.

Notificación y monitorización del estado

Una de las principales ventajas de la gestión de aplicaciones mediante DDM es la notificación proactiva del estado.

Con DDM:

- Los dispositivos monitorizan localmente el estado de las aplicaciones.
- Los eventos de instalación y actualización se detectan inmediatamente.
- Los cambios en el estado se notifican automáticamente al servidor.
- La información sobre el despliegue está disponible sin tener que esperar a los intervalos de consulta programados.

Esto proporciona a los administradores una visibilidad más rápida sobre:

- Progreso de la instalación de las aplicaciones
- Instalaciones realizadas correctamente
- Finalización de las actualizaciones de las aplicaciones
- Cambios en el estado de las aplicaciones
- Errores de despliegue

La información en tiempo real facilita la resolución de problemas y permite una gestión de aplicaciones más ágil.

Requisitos

La gestión de aplicaciones mediante DDM solo admite:

- iOS 26 o posterior
- iPadOS 26 o posterior
- Cliente Ivanti Go administrado 126 o posterior

Los dispositivos que no cumplan estos requisitos continuarán utilizando la gestión tradicional de aplicaciones mediante N-MDM.

> Una vez que un dispositivo se procesa por la gestión de aplicaciones mediante DDM, deshabilitar o actualizar esta distribución de políticas no revierte el dispositivo a dicha gestión. Para que el dispositivo vuelva a utilizar la gestión de aplicaciones mediante MDM, elimine la asignación de la política y vuelva a registrarlo.

8.3. Apps@Work (iOS, Android, Windows y macOS)

Apps@Work es un escaparate de aplicaciones de empresa que facilita la distribución segura de software y aplicaciones. Apps@work está disponible para dispositivos iOS, Android, macOS y Windows. La appstore corporativa Apps@Work está integrada en los clientes Ivanti Go app y Mobile@Work para iOS, Android y macOS. Para dispositivos Windows es una aplicación independiente nativa. Esta sección contiene los siguientes temas:

- Apps@Work de iOS
- Android Apps@Work
- macOS Apps@Work
- Windows Apps@Work

Apps@Work de iOS

La tienda de aplicaciones nativas de Apps@work se despliega automáticamente con el cliente de Go. No es necesaria ninguna acción del administrador. La pestaña Apps@work se muestra en la barra de tareas del cliente de Go. El usuario final puede acceder a esta pestaña para ver e instalar las aplicaciones aprobadas por la empresa. Para obtener más información, consulte Funciones de la tienda de aplicaciones de Apps@Work en iOS.

Las notificaciones del usuario final de iOS Apps@Work para actualizaciones de aplicaciones están habilitadas por defecto. Si desea cambiar los ajustes, consulte el tema **Notificaciones** en Ajustes del catálogo.

Clientes existentes con webclip de Apps@Work para iOS

Los clientes que tienen desplegado webclip de Apps@Work de iOS legado, no obtendrán por defecto el catálogo de aplicaciones nativas integrado. Si quiere transicionar al catálogo nativo de Apps@Work de iOS y eliminar webclip de Apps@work de los dispositivos, lleve a cabo los pasos siguientes:

Enviar las configuraciones

El administrador debe enviar el Catálogo de aplicaciones para la configuración del cliente nativo de los dispositivos para que Apps@Work esté disponible en la experiencia de la tienda de aplicaciones nativas desde la aplicación del cliente de Go. Para obtener más información, consulte Trabajar con configuraciones.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Vaya a **Configuraciones** > Filtrar y seleccionar **Servicios del cliente**. Se listan todas las configuraciones del cliente.
3. Seleccione **Catálogo de aplicaciones para el cliente nativo**. Se abre la página de configuración del Catálogo de aplicaciones del cliente nativo.
4. Haga clic en el icono **Editar distribución**. Se abre la página Editar distribución.
5. Seleccione una de las siguientes opciones:
    - **Todos los dispositivos**
    - **Sin dispositivos**: si no quiere distribuir en ningún dispositivo
    - **Personalizar**: le permite seleccionar dispositivos, grupos de dispositivos, usuarios, grupos de usuarios

6. Después de distribuir la configuración, el usuario debe actualizar la versión del cliente de Go a 83 o superior. La pestaña de Apps@Work ahora es visible en el cliente de Go app.

> La configuración no se puede enviar a los dispositivos que se han registrado mediante iReg porque el cliente de Go no está disponible en el dispositivo. Debe instalar el cliente de Go app para obtener el catálogo de aplicaciones nativas. Para obtener más información, consulte **Registro de dispositivos (iOS, macOS y Android)**.

Eliminar webclip Apps@Work de iOS

Para clientes que tienen Webclip de Apps@Work distribuido en sus dispositivos y ya han migrado a la experiencia nativa da Apps@Work, pueden eliminar webclip de Apps@Work para iOS.

Procedimiento

1. Vaya a **Configuraciones**.
2. Filtrar la configuración: **Catálogo de aplicaciones de Apple**.
3. Haga clic en **Editar**.
4. Desde **Distribución** seleccione **Distribución a ningún dispositivo**.
5. Haga clic en **Guardar**.

Android Apps@Work

La tienda de aplicaciones nativas de Apps@work se despliega automáticamente con el cliente de MI Go. No es necesaria ninguna acción del administrador. La pestaña Apps@work se muestra en la barra de tareas del cliente de Mi Go. El usuario final puede acceder a esta pestaña para ver e instalar las aplicaciones aprobadas por la empresa. Para obtener más información, consulte **Administrador-Android Enterprise**.

macOS Apps@Work

MacOs Apps@work está integrado en el cliente de Mobile@Work de macOS. Después de registrar el dispositivo en Ivanti Neurons for MDM. el cliente cambiará y se mostrará como Apps@Work. Para nuevos abonados, la configuración de webclic del catálogo de aplicaciones de Apple no se enviará a dispositivos de macOS. En caso necesario, el administrador puede distribuir la configuración de webclip de Apps@work en los dispositivos macOS. Para obtener más información, consulte **Configuración de dispositivos macOS**.

Distribución de aplicaciones para macOS

- Ivanti es compatible con la distribución de aplicaciones de macOS a través del protocolo de Apple MDM y usando la aplicación de Mobile@Work. Los administradores pueden optar por utilizar uno o ambos de los siguientes enfoques:
  - Protocolo MSM de Apple: Los administradores pueden cargar únicamente formatos PKG específicos (formato de distribución) como aplicaciones internas y también pueden distribuir aplicaciones desde Mac App Store (se incluye el soporte para licencias de Apps and Books de Apple). Sin embargo, este enfoque no permite que los administradores distribuyan DMG y otros formatos PKG.
  - Aplicación Mobile@Work para macOS: Como una manera de distribuir aplicaciones a los usuarios, los administradores pueden utilizar la aplicación MobileIron Packager (MIP) para convertir cualquier archivo PKG, DMG o .app a un archivo MIP. Cargue el archivo MIP en Ivanti Neurons for MDM como si se tratase de una aplicación interna

Puede descargar la utilidad desde el **sitio de descargas de software**.

- Los administradores pueden utilizar Mobile@Work para distribuir aplicaciones internas que están en formato DMG, PKG o .app. Para las aplicaciones que solo están disponibles en Mac App Store, los administradores pueden continuar usando las prestaciones de MDM, que incluyen las prestaciones de las licencias de Apps and Books de Apple. Para obtener más información, consulte **Configuración de dispositivos macOS**.

Windows Apps@Work

Apps@Work es una aplicación nativa independiente que se puede descargar desde Microsoft Store o se puede enviar directamente desde Ivanti Neurons for MDM. Permite el uso de aplicaciones públicas e internas de Windows en dispositivos de Windows 10+ en Ivanti Neurons for MDM. Apps@Work se instala en segundo plano en dispositivos compatibles de Windows 10+.

Para obtener más información, consulte **Configuración de aplicaciones**.

Uso de Windows Apps@Work

Apps@Work permite el uso de aplicaciones públicas e internas de Windows en dispositivos de Windows 10 en Ivanti Neurons for MDM. Apps@Work se instala en segundo plano en dispositivos compatibles de Windows 10.

Certificado de autenticación de Apps@Work

Para usar la Autenticación de certificados con Windows Apps@Work:

1. Vaya a **Administrador > Windows > Certificado de autenticación de Apps@Work**.
2. Ajustar como **OCTIVADO**.

> Si se ajusta como **DESACTIVADO**, se fuerza el uso del nombre de usuario y la contraseña.

> SAML no es compatible con Apps@Work para Windows.

Para configurar una aplicación para Apps@Work:

1. Seleccione una aplicación de Windows.
2. Haga clic en la pestaña **Configuración de la aplicación**.
3. Haga clic en **Instalar en el dispositivo**.
   La configuración de aplicaciones Windows internas se puede establecer en la marca de instalación silenciosa o instalarse usando Apps@Work. Las aplicaciones públicas no se pueden establecer en una instalación silenciosa.
4. Opcionalmente, también puede decidir si mostrar u ocultar aplicaciones en el catálogo de Apps@Work.
   Esta opción se aplica solo a las aplicaciones internas.
5. Haga clic en la pestaña **Promoción**.

> Actualmente Apps@Work no es compatible con la promoción de banners, así que las opciones disponibles son **Destacado** y **No destacado**.
>
> para las aplicaciones públicas, solo aparece la opción **Promoción**.

8.4. Funciones de la tienda de aplicaciones de Apps@Work en iOS

La pestaña Apps@Work tiene las funciones siguientes:

- Acceda a la pestaña de Apps@Work desde la aplicación Go
- Buscar
- Instalar una aplicación: botón Estados
- Aplicaciones destacadas y banner
- Notificación de actualizaciones de las aplicaciones
- Ajustes: Mis dispositivos

Acceda a la pestaña de Apps@Work desde la aplicación Go

Procedimiento

1. Inicie sesión en Go app desde su dispositivo de iOS.
2. Pulse el icono **Apps@Work**. Hay disponibles dos pestañas predeterminadas: Todas las aplicaciones y Categorías.

3. Pulse la pestaña **Todas las aplicaciones**. La pestaña Todas las aplicaciones es una lista de todas las aplicaciones en orden alfabético.
4. Pulse la pestaña **Categorías**. La pestaña Categorías solo muestra las categorías que tienen aplicaciones en ella, como se muestra a continuación:
    - Cada categoría muestra el número de aplicaciones que contiene.
    - La fila de MyApps que hay bajo la pestaña Categorías es un elemento de la lista que contiene todas las aplicaciones instaladas. La fila de MyApps siempre será la primera categoría y el resto de categorías se listan en orden alfabético.
    - Cuando no se instalan aplicaciones, la lista de MyApps muestra Ninguna.
    - Cuando hace clic en una categoría, todas las aplicaciones que son específicas de la categoría se listan con la opción Instalar. Haga clic en **Instalar** individualmente cada aplicación o puede hacer clic en **Instalar todo** para instalar todas las aplicaciones de la categoría. Se le solicitará que permita la instalación de cada aplicación.

Buscar

Procedimiento

1. Inicie sesión en Go app desde su dispositivo de iOS.
2. Pulse el icono **Apps@Work**.
3. Pulse el icono de búsqueda (lupa) para buscar lo siguiente:
    - **Nuevas versiones**: muestra una lista de nuevas aplicaciones cuando no se escribe texto en la barra de búsqueda

    - Escriba cualquier texto y el campo de búsqueda predecirá de manera dinámica y mostrará las aplicaciones que coincidan.
    - El número de resultados de búsqueda se muestra como subtítulo

- Puede pulsar el botón **Instalar** para instalar una aplicación sin acceder a la página de detalles.



Instalar una aplicación: botón Estados

Puesto que la instalación de aplicaciones requiere que el servidor procese la solicitud y envíe la aplicación al dispositivo, el botón de instalar no se mostrará en el progreso en tiempo real. El botón de instalar cambia los estados de Instalar > Solicitado > Instalado.

Procedimiento

1. Inicie sesión en Go app desde su dispositivo de iOS.
2. Pulse el icono **Apps@Work**.
3. Pulse **Instalar** y aparecerán las notificaciones de estado como se muestra a continuación:
   - Aparece un mensaje de alerta, la primera vez, que indica que se ha solicitado una instalación.
   - Pulse el botón Solicitado. Aparece un mensaje de alerta.

> El estado Instalado no es un botón.



Aplicaciones destacadas y banner

La pestaña Destacados es visible según la configuración que haya enviado el administrador. La pestaña Destacados es la página de inicio predeterminada cuando no hay actualizaciones disponibles.



Procedimiento

1. Inicie sesión en Go app desde su dispositivo de iOS.
2. Pulse el icono **Apps@Work**.
3. Pulse la pestaña **Destacado**.
   - El banner de la aplicación destacada muestra una aplicación en el banner.
   - La Aplicación destacada contiene una lista de todas las aplicaciones destacadas.



Notificación de actualizaciones de las aplicaciones

El usuario final recibe una notificación en el dispositivo cuando hay disponibles actualizaciones de alguna aplicación. La notificación contiene el número de aplicaciones que tienen actualizaciones disponibles. Cuando el usuario hace clic sobre la notificación, se abre Apps@Work.

Procedimiento

1. Inicie sesión en Go app desde su dispositivo de iOS. El icono de Apps@Work muestra el número de aplicaciones que tienen pendientes actualizaciones.
2. Pulse la notificación de actualización de la aplicación, se verá redirigido a la página Todas la aplicaciones de Apps@Work. Aparecerán las indicaciones siguientes:

- La subsección Actualizaciones disponibles de la pestaña Todas las aplicaciones muestra el número de aplicaciones que hay disponibles para su actualización.
- Se muestra un icono de un punto rojo por cada aplicación que requiere una actualización.



Ajustes: Mis dispositivos

Procedimiento

1. Inicie sesión en Go app desde su dispositivo de iOS.
2. Pulse el icono **Ajustes**.
   - La pestaña de Mis dispositivos ahora está disponible en Ajustes.
   - Mis dispositivos ahora se lista como un elemento de línea de Autenticar.

8.5. Funciones avanzadas de iOS Go

Los pares clave-valor (KVP) son ajustes de aplicación simples compuestos por una clave (el nombre del ajuste) y un valor (la configuración que desea aplicar). En Ivanti Go for iOS, las organizaciones utilizan KVP para habilitar o deshabilitar funciones y ajustar el comportamiento de la aplicación sin requerir una actualización de la aplicación.

Cuando Ivanti Go se ejecuta en iPhones o iPads administrados por la organización, éste lee los ajustes de KVP al inicio o durante un registro. La aplicación implementa la actualización inmediatamente, lo que garantiza que los cambios de configuración se entreguen de forma rápida, coherente y a los usuarios correctos.

Uso de KVP en configuraciones de la aplicación Ivanti Go

Los KVP para personalizar mensajes de infracción son compatibles con la aplicación Ivanti Go. Puede configurar los KVP dentro de los ajustes de la aplicación Ivanti Go para personalizar la aplicación.

Procedimiento

1. Abra la aplicación **Ivanti Go** en su AppCatalog.
2. Seleccione **Configuraciones**.
3. Haga clic en **Agregar** para crear una nueva configuración de la aplicación de **Apple**.
4. Agregue sus KVP manualmente:
    - En la columna **Clave**, introduzca la clave de configuración que desee personalizar.
    - En la columna **Valor**, introduzca el valor que desee aplicar en los dispositivos.
5. (Opcional) Cargue un archivo *.plist* existente que contenga KVP predefinidos que desee aplicar.
6. **Guarde** la configuración.
7. Los KVP actualizados se aplicarán a los dispositivos durante su siguiente registro.

Agregar una lista a una aplicación específica de iOS (para varios pares clave-valor)

Los administradores pueden configurar múltiples pares clave-valor (KVP) para una aplicación iOS mediante números de serie de aplicación, identificadores de paquetes, detalles de versiones u otros metadatos. Esto se puede hacer de manera eficiente cargando un archivo .plist a través de la consola de Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Aplicaciones**.
2. Abra el **Catálogo de aplicaciones**.
3. Seleccione y abra la **aplicación específica de iOS** que desee configurar.
4. Vaya a la pestaña Configuraciones de la aplicación.
5. Seleccione **Configuración de la aplicación administrada de Apple**.
6. Haga clic en el **botón Agregar**.
7. Introduzca un **Nombre** para su configuración.
8. Haga clic en **Usar .plist**.
9. Seleccione **Elegir una de estas opciones**.

10. Vaya al archivo de plist, selecciónelo y haga clic en **Abrir**. El sistema rellenará automáticamente la tabla de configuración con los pares de valores clave de la plist.
11. Elija los grupos de usuarios o grupo de dispositivos que deben recibir la configuración.
12. Haga clic en **Distribuir esta configuración de aplicación**.
13. Haga clic en **Guardar** para completar el proceso.

> El archivo cargado debe tener una extensión .plist. Si creó manualmente el archivo (ejemplo, en un editor de texto), asegúrese de que la extensión se cambie de *.txt* a *.plist* antes de cargar.

Inicio de Ivanti Go en modo de aplicación única durante el registro

Esta función permite a los administradores utilizar pares clave-valor durante el registro del dispositivo para iniciar de forma automática Ivanti Go for iOS en modo de aplicación única (SAM). Cuando un dispositivo comienza la inscripción, los pares de clave-valor configurados activan Ivanti Go para abrirse inmediatamente. Durante este proceso, se muestra al usuario un mensaje que indica:

Espere mientras se configura su dispositivo.

Para activar este comportamiento, la configuración del modo de aplicación única debe instalarse y dirigirse explícitamente a Ivanti Go for iOS antes o durante el flujo de trabajo de registro. Una vez completada correctamente la inscripción, se sale del modo de aplicación única de forma automática. A continuación, el dispositivo se envía al usuario final para su funcionamiento normal, lo que garantiza una configuración segura sin restringir el uso posterior al registro.

Esta capacidad es compatible con entornos Ivanti Mobile@Work, lo que proporciona un flujo de registro seguro para dispositivos iOS supervisados.

Configuración de la activación Zero Touch

Para habilitar la activación Zero Touch para Ivanti Go, siga estos pasos:

1. Configure un grupo que incluya solo dispositivos donde *Cliente registrado = No*.
2. Cree una configuración de modo de aplicación única (SAM) para la aplicación Ivanti Go. Asigne esta configuración solo al grupo de dispositivos creado en el *paso 1*.
3. Añada el par de valores (KVP) de zero_touch_activation a la configuración de la aplicación Ivanti Go. Diríjase al mismo grupo de dispositivos utilizado en los pasos anteriores.

Configuración de KVP

Clave	Valor	Tipo	Descripción
zero_touch_activation	Verdadero	Booleano	Cuando el valor se establece en verdadero, la aplicación Ivanti Go reconoce que se está ejecutando en modo de aplicación única (SAM) a través de la configuración SAM. La configuración de SAM inicia la aplicación Ivanti Go, mientras que este valor actúa como ajuste adicional que permite que la aplicación funcione correctamente en modo SAM. Después de la inscripción correcta, el dispositivo sale del modo de aplicación única y pasa a estar disponible para el usuario final para su uso normal.

Habilitar el botón Volver al servicio en Ivanti Go (iOS 18+)

La función **Volver al servicio** permite al dispositivo volver a inscribirse de forma automática una vez que se borran los datos, lo que reduce la necesidad de volver a inscribir manualmente el dispositivo después de una limpieza.

Los administradores pueden activar o desactivar el botón Volver al servicio mediante un par de valores de clave (KVP) configurable. Cuando el KVP se implementa en Ivanti Go como parte de la configuración de la aplicación:

- La opción Volver al servicio se vuelve visible para el usuario final.
- El usuario puede iniciar el proceso de restablecimiento directamente desde Ivanti Go.
- El dispositivo realiza un restablecimiento de Volver al servicio administrado por Apple.
- Los perfiles de administración y las aplicaciones requeridas permanecen intactos.
- El dispositivo completa su flujo de reabastecimiento y está listo para reutilizarse.

Esta función es compatible con Ivanti Go for iOS, iOS 18 y dispositivos posteriores inscritos en el modo DEP.

Configuración de KVP

Añada el siguiente KVP a la configuración de la aplicación administrada de Ivanti Go en Ivanti Neurons for MDM:

Clave	Valor	Descripción
ReturnToServiceHabilitado	verdadero	Habilite el botón **Volver al servicio** en Ivanti Go. Cuando se establece en falso u omitido, la función permanece oculta.

Desactivar la protección de capturas de pantalla en la pantalla de autenticación SAML

Ivanti Go for iOS incluye protección de captura de pantalla integrada para mejorar la seguridad durante el registro del dispositivo. De forma predeterminada, el registro con pantallas de autenticación SAML bloquea:

- Capturas de pantalla
- Grabaciones de pantalla
- Compartir pantalla

Esta protección garantiza que los datos de autenticación confidenciales, como nombres de usuario, contraseñas y contenido de inicio de sesión basado en SAML, no se puedan capturar ni compartir sin autorización.

Los administradores pueden deshabilitar la protección de capturas de pantalla en dispositivos administrados mediante una configuración KVP. Cuando se aplica esta configuración, la aplicación Ivanti Go permitirá capturas de pantalla y grabaciones solo en la pantalla de autenticación SAML, mientras mantiene todos los demás mecanismos de seguridad en toda la aplicación.

Configuración de KVP

Para deshabilitar la protección de capturas de pantalla para la pantalla de autenticación SAML, aplique el siguiente KVP a la configuración de la aplicación Ivanti Go en su MDM:

Clave	Valor	Descripción
SCREENSHOT_PROTECTION_DISABLED	Verdadero	Desactiva la captura de pantalla, la grabación de pantalla y la protección de pantalla compartida en la pantalla Autenticación de SAML. Cuando se omite o se establece en Falso, la protección permanece habilitada por defecto.

KVP para personalizar mensajes de violación de política

Estos KVP permiten a los administradores personalizar los mensajes enviados a los usuarios finales cuando se detectan violaciones de la política.

Estos KVP para personalización describen los KVP y tipos de infracción disponibles para los administradores para personalizar el comportamiento de la aplicación Ivanti Go for iOS. Estos KVP definen el comportamiento de la aplicación, como proporcionar notificaciones detalladas a los usuarios del dispositivo y exportar contactos desde Ivanti Go para iOS.

Los tipos de infracción no son mutuamente excluyentes. Si hay un conjunto de infracciones, se mostrará una lista de mensajes en Ivanti Go for iOS.

Pares de valor clave (KVP)	Mensajes predeterminados
compliance.message.COMPROMISED	• Su dispositivo ha sido comprometido debido a un jailbreak. Devuelva correctamente su dispositivo a un estado sin jailbreak o póngase en contacto con su administrador para obtener ayuda para resolver este problema.
compliance.message.DATA_PROTECTION_DISABLED	• El acceso corporativo se ha deshabilitado para la protección de datos. Comuníquese con su administrador para obtener ayuda para resolver este problema.
compliance.message.OUT_OF_ CONTACT	• Su dispositivo iOS está fuera de contacto. Comuníquese con su administrador para obtener ayuda para resolver este problema.
compliance.message.APPS	• A su dispositivo le faltan aplicaciones que son necesarias o tiene aplicaciones que no están permitidas. Agregue/quite las aplicaciones necesarias o comuníquese con su administrador para obtener ayuda para resolver este problema.
compliance.message.MDM_DISABLED	• Su dispositivo no cumple con los requisitos porque se ha desactivado la capacidad MDM. Vuelva a inscribir su dispositivo o comuníquese con su administrador para obtener ayuda para resolver este problema.
compliance.message.ROAMING	
compliance.message.generic	• El acceso corporativo se ha deshabilitado por un motivo no especificado. Comuníquese con su administrador para obtener ayuda para resolver este problema.
compliance.message.header	Su dispositivo no cumple con los requisitos por las siguientes razónes: Cuando el tipo de infracción es CUSTOM or CUSTOM_NOTIFY_ONLY, el sistema muestra mensajes independientes sin encabezado.
compliance.message.CUSTOM	Es posible que se requiera una acción en su dispositivo. Póngase en contacto con su administrador según sea necesario.
compliance.message.CUSTOM_NOTIFY_ONLY	Su dispositivo no cumple con los requisitos y se ha enviado una notificación. Consulte la pestaña de notificaciones o su correo electrónico para obtener más detalles.

Si la lista de tipos de infracción no incluye ninguna infracción con un mensaje asignado, pero incluye al menos una infracción sin un mensaje asignado, muestre el mensaje predeterminado:

- El acceso corporativo se ha deshabilitado por un motivo no especificado. Comuníquese con su administrador para obtener ayuda para resolver este problema.

Si la lista de mensajes contiene al menos un mensaje de infracción, muestre el siguiente encabezado encima de la lista:
Su dispositivo no cumple con los requisitos por las siguientes razónes:

> Si no desea cambiar un mensaje predeterminado, no incluya un par clave-valor (KVP). Defina solo KVP para los mensajes que desee modificar.

Configure el navegador predeterminado y los clientes de correo electrónico mediante la configuración de aplicaciones administradas.

Los pares clave-valor (KVP) permiten a los administradores definir qué navegador y cliente de correo electrónico utilizará **Ivanti Go** para abrir enlaces web y redactar correos electrónicos usando la configuración de aplicaciones administradas.

Como administrador, puede utilizar los pares clave-valor (KVP) de la configuración de aplicaciones administradas para definir cómo se gestionan los enlaces en la pestaña **Soporte**:

Clave	Valores	Tipo	Descripción
default_browser	safari, edge, chrome, firefox, brave, opera, webatwork, duckduckgo	Cadena	Navegador que utiliza Ivanti Go para abrir enlaces web en la pestaña Soporte. Los enlaces http/https se redirigen al esquema correspondiente al navegador configurado. **Si no se configura,** se utiliza el navegador predeterminado del sistema.
Allow_browser_fallback	true, false	Booleano	**Comportamiento cuando el navegador predeterminado configurado no está instalado**: **True**: se utiliza el navegador predeterminado del sistema. **<Browser>False**: El enlace no se abre y se muestra al usuario una alerta que indica que " no está instalado". **Valor predeterminado si no se configura**: true
restrict_log_sharing_to_email	true, false	Booleano	Indica si el uso compartido de registros o información de soporte está restringido exclusivamente al correo electrónico (mediante default_email). La adjunción automática de registros es compatible con Email+ y Native Mail. Funbciona con **allow_email_fallback**. **True**: uso compartido exclusivamente por correo electrónico. **False**: se mantienen disponibles las opciones de uso compartido estándar. **Valor predeterminado si no se configura**: false.
default_email	nativemail, outlook, gmail, yahoo, citrixmail.emailplus, spark, protonmail	Cadena	Cliente de correo electrónico que utilizará Ivanti Go para redactar mensajes a partir de enlaces mailto en la pestaña Soporte. Los enlaces mailto se transforman en la URL de redacción del cliente de correo electrónico **Valor predeterminado si no se configura:**: aplicación de correo predeterminada. También determina el comportamiento de los enlaces y del uso compartido de registros cuando el cliente de correo electrónico configurado en default_email no está instalado.
Allow_email_fallback	True, False	Booleano	**Comportamiento cuando el correo electrónico predeterminado no está instalado**. **True**: si el correo electrónico configurado no está instalado, se utiliza la aplicación de correo predeterminada para redactar los correos electrónicos y se puede utilizar un método de envío alternativo para compartir los registros. **False**: se bloquea la redacción de correos electrónicos y, si el correo electrónico configurado no está disponible, se muestra a los usuarios una alerta de "**No instalado**". Se aplican las restricciones de uso compartido de registros sin opción de recurrir a un método alternativo. **Valor predeterminado si no se configura**: true. (el comportamiento alternativo está habilitado)

8.6. Ver Detalles de la aplicación

Puede explorar los detalles desde el App Catalog hasta la aplicación en cualquiera de las aplicaciones del catálogo. En la página de detalles de la aplicación, se muestran los detalles de las aplicaciones como «Mostrar versión» (por ejemplo, 1.5.0), «Versión del paquete» (por ejemplo, 1.5.0.42) y «Versión mínima del sistema operativo obligatoria» (por ejemplo, 5.0 para Android).

Las aplicaciones que no cumplan con la versión especificada en el campo Versión mínima del sistema operativo obligatoria no se muestran en el catálogo de Apps@Work. Por lo tanto, estas aplicaciones no están disponibles para su distribución a los dispositivos. El campo Versión mínima del sistema operativo obligatoria también se muestra como parte de las **Trazas de auditoría** para las aplicaciones.

Procedimiento

1. Haga clic en **Aplicaciones**.
2. Haga clic en **Catálogo de aplicaciones**.
3. Seleccione la aplicación.

Aparece la ventana Detalles de la aplicación.

> Para aplicaciones internas de iOS, puede comprobar la **Fecha de caducidad del perfil de aprovisionamiento** en la página de detalles de la aplicación.

> La información de la aplicación muestra **Permitir instalación de aplicaciones en dispositivos M1 tras la distribución** como opción para todas las aplicaciones VPP de iOS e iPadOS. El administrador debe habilitar la opción **Permitir la instalación de la aplicación en dispositivos M1 al momento de la distribución** solo para aplicaciones VPP de iOS o iPad que se pueden instalar en el dispositivo M1 macOS. Solo después de habilitar esta opción, el administrador puede ver los dispositivos M1 macOS durante la instalación de la aplicación. La configuración de la aplicación administrada es compatible con aplicaciones VPP de iOS en dispositivos M1 Mac.

> Para aplicaciones de la App Store de iOS y macOS, incluido Empresa-a-Empresa (B2B) **Sincronizar versión nueva** comprueba y sincroniza las actualizaciones de aplicaciones desde la App Store. La versión actualizada de la aplicación se muestra en un plazo de 12 a 24 horas en función del calendario de sincronización de la aplicación.

> Se añade un botón de activación para **Aplicaciones de requisitos previos** en detalles del Dispositivo. Los administradores pueden seleccionar esta opción y añadir aplicaciones como requisitos previos de una aplicación principal.

Tras distribuir una aplicación a distintos dispositivos, el estado de distribución de la aplicación se puede ver en la pestaña **Resumen de dispositivos**. La pestaña Resumen de dispositivos también contiene información sobre el número de dispositivos aptos, el número de dispositivos en los que se instaló la aplicación, el número de dispositivos en los que la instalación de la aplicación está pendiente y el número de dispositivos en los que falló la instalación de la aplicación. El número de dispositivos en estos cuadros se basa en los dispositivos que tienen Instalación obligatoria de aplicaciones, por lo que los administradores pueden realizar un seguimiento del despliegue inicial en las aplicaciones obligatorias.

Para conocer el número general de aplicaciones (incluidas las instaladas por el usuario), utilice la búsqueda en el Inventario de aplicaciones.

Las aplicaciones excluidas del dispositivo tienen pendiente el estado de distribución.

En la siguiente tabla se enumeran las razones por las que falla la instalación de aplicaciones en aplicaciones de iOS/OSX:

Motivo	Descripción
AppAlreadyInstalled	"Aplicación ya instalada".
AppStoreDisabled	"La tienda de aplicaciones está desactivada".
CouldNotVerifyAppID	"No se ha podido verificar el ID de la aplicación".
Error	"La instalación de la aplicación ha fallado con un error desconocido".
ManagedButUninstalled	"La aplicación está administrada, pero el usuario la ha eliminado. Cuando se instale de nuevo la aplicación (incluso por el usuario), se volverá a gestionar".
ManagementRejected	"El usuario ha rechazado la conversión de una aplicación no administrada a una aplicación administrada".
NotAnApp	"El comando InstallApplication se rechaza debido a un identificador de aplicación no válido que resuelve un activo que no es una aplicación."
NotSupported	"La aplicación no es compatible".
Otros	"Motivo para los nuevos errores añadidos".
PurchaseMethodNotSupported	"Para iOS 7 y posteriores, la aplicación no se puede instalar debido a un método de compra no válido (aplicable solo a aplicaciones VPP)."
UserInstalledApp	"El usuario ha instalado la aplicación antes de que pudiera tener lugar la instalación de la aplicación administrada".
UserRejected	"El usuario rechazó la sugerencia de instalar la aplicación".
UpdateRejected	"El usuario rechazó la sugerencia de actualizar la aplicación".

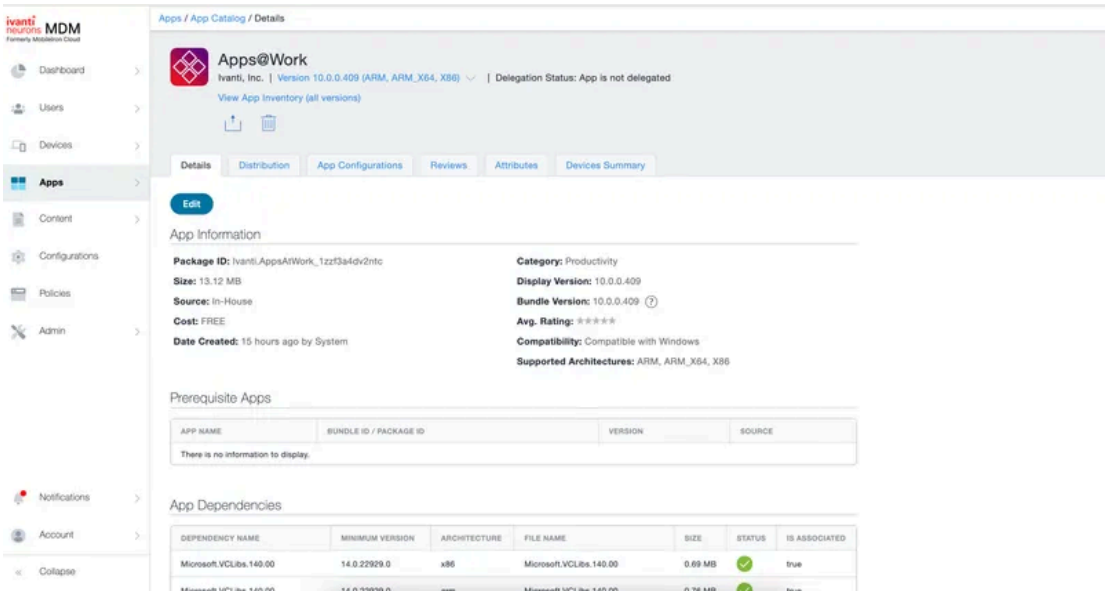
En la siguiente tabla se enumeran las razones por las que falla la instalación de aplicaciones en Android:

Motivo	Descripción
USER_INSTALLED	"Ya se ha instalado en el dispositivo (fuera de MDM)".
UNSUPPORTED	"No compatible"
USER_REJECTED_INSTALL	"El usuario ha rechazado la instalación de la aplicación".
ERROR_INSTALL	"Se ha detectado un error al intentar instalar; falló".
UNRECOGNIZED	"El artículo no se encuentra o ya no se rastrea (por ejemplo, error/desinstalado del dispositivo y eliminado del rastreo)".
UNSUPPORTED_INSTALL	"Actualizado para cliente Android 3.0/servidor 22.0.0: es necesario un estado específico para realizar un seguimiento de la instalación frente a la desinstalación."
OCULTA	"Durante la cuarentena, se enviará el estado OCULTO/DESINSTALADO. Unquarantine debería volver a "instalardo".
OTROS	"Motivo para los nuevos errores añadidos".

Para dispositivos Windows, si la aplicación está configurada para instalarse en segundo plano, en la Configuración de la aplicación, el Resumen de dispositivos muestra el número de dispositivos aptos, instalados, pendientes o fallidos para la aplicación.

Visualización de la información del inventario de aplicaciones desde la página de detalles de la aplicación

Para ver la información del inventario de aplicaciones, haga clic en **Ver inventario de aplicaciones (todas las versiones)** para ver en **Dispositivos > Inventario de aplicaciones** una lista filtrada por ID de agrupación de esa aplicación.



8.7. Configuración de aplicaciones

Esta sección contiene los siguientes temas:

- Licencias para las características de las aplicaciones
- Pasos de la configuración comunes a múltiples aplicaciones
- Ocultar o suspender aplicaciones (solo Android)
- Configuración del relé de red
- Configuración de la segmentación celular 5G
- Distribución de aplicaciones mediante la configuración del filtro de contenidos web
- Distribución de aplicaciones mediante proxy DNS
- Borrado de la caché de aplicaciones en dispositivos Android Enterprise

La configuración de aplicaciones le permite personalizar la instalación, promoción y distribución de cada aplicación que instala en sus dispositivos de usuario. Las aplicaciones pueden ser sus propias aplicaciones internas, aplicaciones de una tienda pública o aplicaciones de Ivanti Neurons for MDM. Tiene la flexibilidad de implementar las aplicaciones para muchos usuarios y grupos diferentes con nombres y configuraciones exclusivos específicamente adaptados a cada destinatario. El número de versiones de aplicaciones internas está limitado a 100. Si se supera ese número, el sistema Ivanti Neurons for MDM purga las versiones más antiguas de la aplicación. El estado de la carga y purga de la aplicación aparece en una lista y es visible desde la página de Registros de Auditoría.

> Al cambiar los valores de la configuración de aplicaciones para una aplicación en concreto en el App Catalog o en el perfil administrado de configuración de aplicaciones, será necesario introducir una o dos veces hasta que el dispositivo reciba los nuevos valores de configuración.

Licencias para las características de las aplicaciones

> Las siguientes características requieren licencias adicionales:

- Instalación/desinstalación silenciosa de aplicaciones: licencia Silver
- Configuración por aplicación: licencia Gold
- Configuración personalizada de AppConnect: licencia Gold

los paquetes de aplicaciones múltiples requieren una buena administración de grupos, ya que el sistema operativo Windows podría no definir los futuros tipos de dispositivos. En tal caso, la única forma de instalar la versión correcta de la aplicación es que el administrador utilice el grupo correcto para la aplicación correcta.

Pasos de la configuración comunes a múltiples aplicaciones

Lleve a cabo estos pasos primero y, a continuación, proceda con los pasos de la configuración para cada aplicación que desee implementar. Puede diseñar múltiples configuraciones de la misma aplicación y darle a cada una un nombre exclusivo. Cada configuración puede tener su propia distribución y niveles de promoción para adaptarse a su estrategia de implementación. El número de versiones de aplicaciones internas está limitado a 100. Si se supera ese número, el sistema Ivanti Neurons for MDM purga las versiones más antiguas de la aplicación. El estado de la carga y purga de la aplicación aparece en una lista y es visible desde la página de Registros de Auditoría. Puede instalar una aplicación en un máximo de 100 usuarios, grupos de usuarios, dispositivos o

grupos de dispositivos a la vez. Puede seleccionar una aplicación para agregarla al catálogo de aplicaciones. Ivanti Neurons for MDM tiene un proceso asincrónico para enviar comandos de solicitudes de instalación/actualización para aplicaciones de iOS. Cuando utiliza el comando Enviar instalación/Actualizar solicitud, el portal administrativo de Ivanti Neurons for MDM muestra un mensaje que el:

- el proceso continuará ejecutándose en segundo plano
- proceso completo
- estado independientemente de que el proceso se complete correctamente o con errores

Procedimiento

1. Vaya a **Aplicaciones > App Catalog** y haga clic en **+Añadir**.
2. Use el menú desplegable para seleccionar la App Store, Google Play o su app store interna y elija la aplicación que desea añadir al catálogo.
   Dependiendo de su acuerdo de licencia, es posible que también tenga disponibles aplicaciones para añadir al catálogo.
3. Opcionalmente, puede editar la Categoría de la aplicación.
4. Opcionalmente, puede añadir una breve descripción de la aplicación en el campo **Descripción**.
5. Haga clic en **Siguiente**.
6. Elija un nivel de distribución para la configuración de la aplicación:
   - **Para todo el mundo:** la aplicación se añade a los dispositivos compatibles de todos los usuarios.
   - **A nadie:** la aplicación se almacena para distribuirse posteriormente.
   - **Distribución personalizada**: seleccione cualquiera de las siguientes opciones:
     - **Usuarios/Grupos de usuarios**: la aplicación solo se distribuye a los usuarios o grupos de usuarios que usted elija.
       Haga clic en la pestaña **Usuarios** para seleccionar los usuarios.
       Haga clic en la pestaña **Grupos de usuarios** para seleccionar los grupos de usuarios.
     - **Dispositivos/Grupos de dispositivos:** la aplicación solo se distribuye a los dispositivos o grupos de dispositivos que usted elija.
       Haga clic en la pestaña **Dispositivos** para seleccionar el o los dispositivos.
       Haga clic en la pestaña **Grupos de dispositivos** para seleccionar los grupos de dispositivos.
7. Haga clic en **Siguiente**.

Configurar opciones de instalación

Puede seleccionar las opciones de configuración de la instalación.

Procedimiento

1. Haga clic en **Ajustes de instalación de la configuración de la aplicación** o haga clic en el icono **+** para añadir otra configuración para ver la página **Establecimiento de la configuración**.
2. Introduzca un nombre para la configuración en el campo **Nombre**.
3. Opcionalmente, puede añadir una breve descripción de la configuración de la instalación en el campo **Descripción**.
4. Seleccione la opción **Configuración de instalación del dispositivo**.
5. Seleccione una de las siguientes opciones:
   - **Requerir instalación en el dispositivo**
   - **Instalar solo en el momento del registro del dispositivo**

6. Seleccione la opción **No requerir una versión específica de la aplicación** para evitar degradar una aplicación ya instalada a una versión inferior. Esta opción solo está disponible para las aplicaciones modernas.
7. Seleccione las siguientes opciones:
    - **Instalar de forma silenciosa en el espacio de trabajo Samsung Knox y en dispositivos Zebra** (solo Android)
    - **No mostrar la aplicación en el Catálogo de aplicaciones del usuario final**.
    - **No instale la aplicación en dispositivos recién inscritos**: los dispositivos existentes no se verán afectados y seguirán mostrando la aplicación en el catálogo de aplicaciones del dispositivo.
        - Para cualquier dispositivo recién inscrito en esta distribución, la aplicación no aparecerá en la lista ni se enviará.
        - Si el administrador activa un comando de envío de instalación/actualización, el comando se enviará al dispositivo.
    - **Aplazar actualización de aplicación por**:?Puede utilizar esta opción para retrasar la instalación de la nueva versión de la aplicación. Este ajuste retrasa la instalación automática de nuevas versiones de la aplicación en función de la duración configurada.
    - **Modo de actualización de aplicaciones** (compatible también con dispositivos AMAPI). (Solo Android)
      Utilice esta opción para actualizar una aplicación a la última versión utilizando uno de los tres modos siguientes:
        - **Predeterminado**: se selecciona este modo una vez que selecciona la opción Modo de actualización de la aplicación. En este modo, la actualización se produce en un plazo de 24 horas desde que empieza a estar disponible la aplicación.
        - **Posponer 90 días:** si selecciona este modo de actualización, puede posponer las actualizaciones de la aplicación durante 90 días. Después de 90 días, las aplicaciones se actualizan automáticamente en función de otros ajustes realizados en la configuración de Google Play administrada.
        - **Alta prioridad**: si selecciona este modo de actualización y el dispositivo del usuario está conectado, la aplicación se actualiza inmediatamente una vez que esté disponible en la Google Play Store.
    - **Establezca la prioridad de instalación de la aplicación**: consulte el tema Configuración de la prioridad de la aplicación para obtener más información.

> En los dispositivos Android, las actualizaciones de las aplicaciones se permiten mediante la opción Actualización automática, incluso sin seleccionar la opción Instalación en segundo plano. El administrador puede controlar las actualizaciones de las aplicaciones que no son obligatorias o de las aplicaciones autoinstaladas por el usuario.

    - **No actualizar mientras la aplicación está en uso**: seleccione esta opción para evitar que una aplicación se actualice mientras el usuario está utilizando activamente la aplicación. Cuando esta opción está habilitada:
        - Las actualizaciones de aplicaciones se aplazan mientras la aplicación se ejecuta en primer plano.
        - El usuario puede continuar utilizando la aplicación sin interrupción.
        - La actualización pendiente se instala de forma automática cuando la aplicación se cierra o se mueve al segundo plano.

Eliminar aplicaciones cuando se elimina la distribución (Android)

Para las aplicaciones administradas de Google Play, Ivanti Neurons for MDM elimina de forma automática las aplicaciones de los dispositivos Android cuando la aplicación ya no está asignada al dispositivo.

Las aplicaciones se eliminan en los siguientes escenarios:

- La distribución de la aplicación se cambia a No a nadie.
- La aplicación se elimina del Catálogo de aplicaciones.
- El dispositivo se excluye de la distribución de aplicaciones.

Es posible que se encuentre con opciones adicionales de configuración, dependiendo de la aplicación que elija. Estas opciones pueden incluir la posibilidad de añadir múltiples pares de clave y valor. En dichos casos, haga clic en **+ Añadir** para introducir los pares clave/valor. Para obtener más información, consulte **Agregar una aplicación desde un almacén público** de Catálogo de aplicaciones.

9. (macOS 11+) Seleccione las opciones para instalar y configurar las aplicaciones como aplicaciones gestionadas:
    - **Instalar como aplicación administrada**
    - **Convertir en Aplicación administrada**

    > En macOS 12.0+, la compatibilidad con Managed App está disponible en los dispositivos inscritos por el usuario.

Ocultar o suspender aplicaciones (solo Android)

Para dispositivos Android en los siguientes modos: **perfil de trabajo**, **dispositivo completamente gestionado**, **dispositivo completamente gestionado con perfil de trabajo** y **perfil de trabajo en dispositivo propiedad de la empresa**, ahora es posible ocultar o suspender aplicaciones después de la instalación.

Procedimiento

	1.	**Instale una o más aplicaciones en el dispositivo para el que desee aplicar la acción Ocultar o Suspender.**
	2.	**Crear una configuración de App Control y agregar las aplicaciones gestionadas a la lista Ocultar o Suspender.**
	3.	**Aplicar los cambios al dispositivo.**

> Si una aplicación está presente tanto en la lista de Ocultar como en la lista de Suspender, entonces la aplicación será ocultada, ya que la lista de Ocultar tendrá prioridad.

Configurar la prioridad de la aplicación

Se puede definir el orden en que se reciben las aplicaciones en el dispositivo cuando se registra por primera vez (concretamente, dentro de los primeros 20 minutos después de la fecha y hora de registro) y se insertan las aplicaciones necesarias para instalarlas. Puede priorizar la descarga de aplicaciones específicas antes que otras aplicaciones. Por ejemplo, se puede priorizar la descarga de las aplicaciones Tunnel y Email antes que otras aplicaciones no tan importantes. Esta función es aplicable tanto a las aplicaciones públicas como privadas. Las aplicaciones con requisitos previos se insertan antes que las aplicaciones dependientes.

Esta función es compatible con dispositivos iOS (excepto AppStation para iOS), Android (excepto Android para empresas), macOS (aplicaciones PKG internas y aplicaciones Apple Apps y Books) y Windows.

> Esta función está disponible para los nuevos dispositivos de registro. Por defecto, todas las aplicaciones tienen prioridad Media. Durante este proceso, el usuario puede seleccionar instalar manualmente cualquier aplicación del catálogo, aunque esa aplicación competirá por los recursos para instalarse y puede ponerse en cola antes que las aplicaciones de alta prioridad.

> En cuanto a las aplicaciones de Windows, la aplicación Bridge tiene mayor prioridad que las demás aplicaciones.

Consulte la sección anterior, «Configurar opciones de instalación» para conocer el procedimiento para establecer la prioridad de una aplicación mediante la opción **Establecer la prioridad de instalación de las aplicaciones**. Puede establecer una prioridad Alta, Media o Baja para una aplicación. Las aplicaciones con la misma prioridad se instalarán sin ningún orden en particular. La prioridad de las aplicaciones no se utiliza durante las actualizaciones de la aplicación, cuando el usuario ya tiene la aplicación instalada.

Seleccionar los ajustes de configuración de Administración de aplicaciones de Apple

estos ajustes se aplicarán únicamente a esta aplicación e invalidará cualquier ajuste global seleccionado en **Aplicaciones > Ajustes del catálogo**. Para seleccionar los ajustes de **Administración de aplicaciones de Apple**:

Procedimiento

1. Haga clic en **Ajustes de aplicaciones Apple** o haga clic en el icono **+** para añadir otra configuración para ver la página **Ajustes de la configuración**.
2. Introduzca un nombre para la configuración en el campo **Nombre**.
3. Introduzca una breve descripción para la configuración en el campo **Descripción**.
4. Seleccione o cancele la selección de una o más de la siguientes opciones de los **Ajustes de administración de Apple**:
    - **Impedir la copia de seguridad de iCloud e iTunes**
    - **Eliminar aplicaciones dadas de baja**
    - (iOS 14.0+) **Permitir la eliminación y descarga de esta aplicación**: puede anular la selección de esta opción para evitar que un usuario elimine o descargue una aplicación administrada.
    - (Opcional) Agregue una **Configuración de la aplicación administrada Apple**
5. Haga clic en **Actualizar**.

Seleccionar niveles de promoción de aplicaciones

Puede establecer el nivel de promoción de la aplicación.

Procedimiento

1. Haga clic en **Ajustes de configuración de la distribución de promociones** o haga clic en el icono **+** para añadir otra configuración para ver la página **Configuración de promociones**.
2. Haga clic en **Editar**.
3. Introduzca un nombre para los ajustes de configuración de la distribución de promociones en el campo **Nombre**.
4. Opcionalmente, puede añadir una breve descripción de la configuración en el campo **Descripción**.
5. Seleccione el nivel de promoción que desea que reciba la aplicación: **No destacada**, **Lista destacada** o use un **Banner destacado**. Si elige la opción **No destacada**, la aplicación no aparecerá en la lista.
6. Si selecciona Banner destacado especifique los siguientes detalles:
    1. **Título**: especifique el título de la aplicación
    2. **Descripción**: especifique los detalles de la aplicación
    3. **Estilo de banner**: seleccione un color de banner
7. Haga clic en **+ Añadir descripción** para introducir una breve descripción de la configuración.
8. Opcionalmente, puede cambiar la distribución de la configuración.
9. Haga clic en **Hecho** para guardar la configuración de la aplicación.

Configurar reglas de tráfico de AppTunnel

Use la configuración de AppTunnel para definir las reglas de tráfico con el fin de permitir el acceso a los servicios usando Sentry:

Para obtener información acerca de cómo añadir una configuración de AppTunnel, consulte en “Cómo añadir una configuración de AppTunnel” en la *Guía de AppConnect para Ivanti Neurons for MDM*.

Configuración de una aplicación administrada

Procedimiento

1. Haga clic en el icono **+** para abrir la página de configuración.
2. Haga clic en **+ Añadir descripción** para introducir una breve descripción de la configuración.
3. Haga clic en **+ Añadir** para introducir una clave y un valor.
4. Elija un nivel de distribución.
5. Haga clic en **Siguiente**.

Configurar una VPN para cada aplicación utilizando la VPN por aplicación

Procedimiento

1. Haga clic en el icono **+** para abrir la página de configuración.
2. Introduzca un nombre para la VPN de esta aplicación en el campo **Nombre**.
3. Haga clic en **+ Añadir descripción** para introducir una breve descripción de la configuración.
4. Haga clic en la opción **Activar VPN por aplicación para esta aplicación** y seleccione una configuración de VPN por aplicación disponible.
5. (Opcional) Para las aplicaciones de macOS, introduzca la cadena **Requisito designado** en el formato, identificador "\%s\". Por ejemplo, el identificador «com.google.Chrome». Use este campo para habilitar una aplicación de paquete múltiple de macOS para usar una VPN por aplicación como Tunnel.
6. Elija cómo **Distribuir la configuración de esta aplicación**.
7. Haga clic en **Siguiente**.

Uso de la configuración de la aplicación administrada Apple

Mediante la configuración de la aplicación administrada Apple, se pueden configurar ajustes específicos para la aplicación administrada instalada. Es posible que la aplicación tenga algunos parámetros de la configuración implementados o restringidos por el desarrollador. En aplicaciones con dichas restricciones, puede ocurrir que las opciones de configuración sea limitadas. Puede configurar las aplicaciones administradas de Apple.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Seleccione una aplicación.
3. Haga clic en la pestaña **Configuraciones de la aplicación**.
4. Haga clic en **Configuración de la aplicación administrada Apple** o haga clic en el botón **+**.
   En la Configuración de la aplicación administrada Apple, ya existen algunos ajustes predeterminados de la configuración.

5. Haga clic en **Añadir** para añadir otra configuración, si fuera necesario. Opcionalmente, haga clic en el nombre de la configuración para editar la configuración.
6. En **Fuente de configuración**, seleccione cualquiera de las opciones de **Tipo de fuente**.

- **Comunidad de AppConfig**: esta opción está disponible solo para aquellas aplicaciones que tienen una especificación de la configuración de la aplicación disponible en el repositorio de la comunidad. Si esta opción está disponible, aparece seleccionada de forma predeterminada.
- **Usar especificación .xml:** seleccione esta opción para subir el esquema de la aplicación para insertar una versión concreta de la configuración de la aplicación. Haga clic en **Seleccionar archivo** para cargar el archivo .xml. Asegúrese de que el archivo .xml contenga la Id. y la versión del paquete. Se mostrará un mensaje de error si la Id. del paquete del archivo no coincide con la Id. del paquete de la aplicación.
- **Ninguno**: seleccione esta opción si no desea aplicar ningún esquema para la aplicación. Esta opción está seleccionada de forma predeterminada si la opción **Comunidad de AppConfig** no está disponible.
  El archivo .xml cargado aparece en la sección **Fuente de configuración**. Haga clic en el icono Eliminar para borrar el archivo .xml cargado.

7. En los **Ajustes de la aplicación administrada Apple**, puede configurar las opciones de configuración para introducir pares de valores clave.

- Haga clic en **Añadir** para agregar los siguientes pares de valores clave a la configuración de aplicaciones administradas para recuperar la identidad del nombre de registro por parte del cliente Go durante iReg o la Inscripción de dispositivos de Apple. Puede seleccionar los tipos de datos (String, Integer, Boolean, Long Float, Double, Date, String Array, Integer Array, Double Array, Float Array, Long Array) para los pares de valor-clave.

Añada los siguientes pares de valores clave a la configuración de aplicaciones administradas para recuperar la identidad del nombre de registro por parte del cliente Go durante iReg o la Inscripción de dispositivos de Apple:

Clave	Valor	Tipo
registration.username	$	CADENA
registration.token	$	STRING
registration.token.expirationSeconds	$	CADENA
registration.url	$	CADENA

Añada los siguientes pares de valores clave a la configuración de la aplicación gestionada para recuperar la identidad del nombre de registro por parte del agente mac (Mobile@Work) durante iReg o Inscripción de dispositivos Apple:

Clave	Valor	Tipo
ClientRegistrationUrl	$	CADENA
Token	$	CADENA
TokenExpiresAt	$	CADENA

Si el usuario final finaliza la aplicación Ivanti Go, haga clic en **Editar** para configurar la aplicación para que realice una de las siguientes acciones:

Clave	Valor	Tipo
Para mostrar la notificación por defecto utilice los siguientes valores: enableAppTerminationNotification Para Mostrar una notificación personalizada utilice los siguientes valores:	Cierto/Falso O 1/0	Booleano O Cadena
appTerminationNotificationMessage	Notificaciones personaizadas	Cadena
enableAppTerminationNotification	Cierto/Falso O 1/0	Booleano O Cadena

- **Usar .plist**:los archivos .plist contienen múltiples pares de valores clave para cargarse en masa. Haga clic en **Seleccionar archivo** para cargar el archivo .plist. Los datos .plist validados se mostrarán en la tabla **Ajustes de la aplicación administrada Apple**.

Las plists con diccionarios anidados no son válidas.

8. Haga clic en **Actualizar** para guardar los cambios.

Configuración del relé de red

Para que el tráfico de red de su aplicación sea más privado y seguro sin conectarse a una VPN. Para más información, consulte **Configuración del relé de red**.

1. Haga clic en el icono **+ Relé de red** para abrir la página de configuración.
2. Introduzca un nombre para el **Relé de red** de esta aplicación en el campo Nombre.
3. Haga clic en + **Añadir descripción** para introducir una breve descripción de la configuración.
4. Haga clic en la opción **Activar relé de red** de esta aplicación y seleccione una configuración disponible de **Relé de red**.
5. Elija cómo **Distribuir** la configuración de esta aplicación.
6. Haga clic en **Siguiente**.

Configuración de la segmentación celular 5G

La compatibilidad de la segmentación de red 5G móvil permite que las aplicaciones gestionadas individualmente se asignen a una segmentación de red que proporciona una capacidad y características de red específicas para optimizar la experiencia de la aplicación. La asignación se realiza mediante el nuevo atributo de aplicación **CellularSliceUUID** en el comando de instalación de la aplicación MDM o en la configuración declarativa de la aplicación. El valor de la cadena de la porción de red que debe introducirse en la clave lo debe proporcionar el operador de soporte.

> La segmentación de la red 5G no se utilizará si la aplicación específica o todo el dispositivo están configurados para utilizar una VPN.

ProcedureProcedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones > Configuración de aplicaciones > Segmentación 5G móvil** y haga clic en **Agregar**.
2. En la **Ajuste de la configuración**, actualice los siguientes campos:
   - Nombre
   - Seleccione la opción **Habilitar la segmentación de red 5G**
   - Elija la categoría de aplicación **DNN** o **Categoría de aplicación** (según el proveedor de red)
3. Elija un nivel de distribución para la configuración de la aplicación:
4. Haga clic en **Guardar**.

Distribución de aplicaciones mediante la configuración del filtro de contenidos web

Puede utilizar la configuración del Filtro de contenido web para distribuir una aplicación en lugar de un servidor proxy DNS. Después de crear la configuración del Filtro de Contenido Web, puede añadir la configuración a una aplicación para su distribución. Para obtener más información sobre la configuración del Filtro de contenido Web, consulte **Filtro de contenido web**.

Procedimiento

1. Vaya a **Aplicaciones** > **Catálogo de aplicaciones**.
2. Seleccione una aplicación.
3. Haga clic en **Siguiente**.
4. Seleccione la opción de delegación y haga clic en **Siguiente**.
5. Seleccione las opciones de distribución y haga clic en **Siguiente**.
6. Seleccione **Configuración del filtro de contenidos web** y haga clic en el icono **+**.
7. Especifique el **Nombre**.
8. Seleccione la casilla **Habilitar filtro de contenido web para esta aplicación**.
9. Seleccione el filtro de contenido web en el menú desplegable.
10. Elija un nivel de distribución para la configuración de la aplicación:
    1. **Para todo el mundo:** la aplicación se añade a los dispositivos compatibles de todos los usuarios.
    2. **A nadie:** la aplicación se almacena para distribuirse posteriormente.
    3. **Distribución personalizada**: seleccione cualquiera de las siguientes opciones:
       - **Usuarios/Grupos de usuarios**: la aplicación solo se distribuye a los usuarios o grupos de usuarios que usted elija.
         Haga clic en la pestaña **Usuarios** para seleccionar los usuarios.
         Haga clic en la pestaña **Grupos de usuarios** para seleccionar los grupos de usuarios.
       - **Dispositivos/Grupos de dispositivos:** la aplicación solo se distribuye a los dispositivos o grupos de dispositivos que usted elija.
         Haga clic en la pestaña **Dispositivos** para seleccionar el o los dispositivos.
         Haga clic en la pestaña **Grupos de dispositivos** para seleccionar los grupos de dispositivos.
11. Haga clic en **Siguiente**.

12. Haga clic en **Hecho**. La aplicación seleccionada se distribuye a los usuarios específicos a través de la configuración del Filtro de Contenido Web.

Distribución de aplicaciones mediante proxy DNS

Puede utilizar la configuración del proxy DNS para distribuir la aplicación. Después de crear la configuración del proxy DNS, puede añadir la configuración a una aplicación para su distribución. Para obtener más información sobre la configuración del proxy DNS, consulte Creación de una configuración de proxy de DNS.

Procedimiento

1. Vaya a **Aplicaciones** > **Catálogo de aplicaciones**.
2. Seleccione una aplicación.
3. Haga clic en **Siguiente**.
4. Seleccione la opción de delegación y haga clic en **Siguiente**.
5. Seleccione las opciones de distribución y haga clic en **Siguiente**.
6. Seleccione **Configuración del Proxy DNS** y haga clic en el icono **+**.
7. Especifique el **Nombre**.
8. Marque la casilla **Habilitar Proxy DNS para esta aplicación**.
9. Seleccione Proxy DNS en el menú desplegable.
10. Elija un nivel de distribución para la configuración de la aplicación:
    1. **Para todo el mundo:** la aplicación se añade a los dispositivos compatibles de todos los usuarios.
    2. **A nadie:** la aplicación se almacena para distribuirse posteriormente.
    3. **Distribución personalizada**: seleccione cualquiera de las siguientes opciones:
        - **Usuarios/Grupos de usuarios**: la aplicación solo se distribuye a los usuarios o grupos de usuarios que usted elija.
          Haga clic en la pestaña **Usuarios** para seleccionar los usuarios.
          Haga clic en la pestaña **Grupos de usuarios** para seleccionar los grupos de usuarios.
        - **Dispositivos/Grupos de dispositivos:** la aplicación solo se distribuye a los dispositivos o grupos de dispositivos que usted elija.
          Haga clic en la pestaña **Dispositivos** para seleccionar el o los dispositivos.
          Haga clic en la pestaña **Grupos de dispositivos** para seleccionar los grupos de dispositivos.
11. Haga clic en **Siguiente**.
12. Haga clic en **Hecho**. La aplicación seleccionada se distribuye a los usuarios específicos a través de la configuración del Proxy DNS.

Ajustes de Clonar la configuración de una aplicación

Puede clonar los Ajustes de configuración de una aplicación administrada para que los mismos ajustes se puedan aplicar en otros dispositivos. Incluso puede cambiar el nombre y realizar algunos cambios en los ajustes clonados.

Android

Puede clonar los Ajustes de configuración en dispositivos Android.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Seleccione una aplicación desde la que desee clonar los ajustes de configuración.
3. Haga clic en **Configuraciones de aplicaciones**.
4. En la sección **Resumen de configuraciones de aplicaciones**, encontrará la lista de configuraciones (**Configuraciones administradas para Android**, **Instalar en el dispositivo**, **Promoción**, **Permisos delegados del dispositivo** y **Versión de Google Play**) disponible para dispositivos de Android.
5. Haga clic en cualquiera de las configuraciones disponibles.
6. En **Acciones**, haga clic en **Clonar** para iniciar el proceso de clonación.
7. Por defecto, el nombre de la configuración clonada será <Copy of the Cloned Configuration name>. No obstante, puede modificar el nombre si introduce un nombre e su elección en el cuadro **Nombre**.
8. (Opcional) Introduzca algún texto sobre los ajustes clonados en el cuadro **Descripción**.
9. Haga clic en **Continuar**.

Aparece una ventana de confirmación que indica que se ha completado la clonación de los ajustes de configuración de la aplicación. Puede ver la versión clonada en el Resumen de configuración de aplicaciones y en la aplicación clonada.

iOS

Puede clonar los Ajustes de configuración de aplicaciones administradas en dispositivos iOS.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Seleccione una aplicación desde la que desee clonar los ajustes de configuración.
3. Haga clic en **Configuraciones de aplicaciones**.
4. En la sección **Resumen de configuraciones de aplicaciones**, encontrará la lista de configuraciones (**Instalar en el dispositivo**, **Ajustes de aplicaciones de Apple**, **Promoción**, **Configuración personalizada de AppConnect**, **Túnel de aplicaciones**, **Configuración de aplicaciones administradas de Apple** y **VPN por aplicación**) disponibles para dispositivos de iOS.
5. Haga clic en la configuración requerida que desee clonar.
6. En **Acciones**, haga clic en **Clonar** para iniciar el proceso de clonación.
7. Por defecto, el nombre de la configuración clonada será <Copy of the Cloned Configuration name>. No obstante, puede modificar el nombre si introduce un nombre e su elección en el cuadro **Nombre**.
8. (Opcional) Introduzca algún texto sobre los ajustes clonados en el cuadro **Descripción**.
9. Seleccione una fuente de configuración de la lista **Tipo de fuente**.
10. En la sección **Ajustes de aplicaciones administradas de Apple**, introduzca **Clave**, **Valor** y seleccione **Tipo** en la lista.
    Para obtener información sobre **Clave**, **Valor** y **Tipo**, consulte **Uso de la configuración de aplicaciones administradas de Apple**.
11. Haga clic en **Continuar**.
    Aparece una ventana de confirmación que indica que se ha completado la clonación de los ajustes de configuración de la aplicación. Puede ver la versión clonada en la sección **Configuración de aplicaciones administradas de Apple**.

Windows

Puede clonar los Ajustes de configuración de aplicaciones en dispositivos Windows.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Seleccione una aplicación desde la que desee clonar los ajustes de configuración.
3. Haga clic en **Configuraciones de aplicaciones**.
4. En la sección **Resumen de configuraciones de aplicaciones**, encontrará la configuración de **Instalar en el dispositivo** y **Promoción**.
5. Haga clic en la configuración requerida que desee clonar.
6. En **Acciones**, haga clic en **Clonar** para iniciar el proceso de clonación.
7. Por defecto, el nombre de la configuración clonada será <Copy of the Cloned Configuration name>. No obstante, puede modificar el nombre si introduce un nombre e su elección en el cuadro **Nombre**.
8. (Opcional) Introduzca algún texto sobre los ajustes clonados en el cuadro **Descripción**.
9. Haga clic en **Continuar**.

Aparece una ventana de confirmación que indica que se ha completado la clonación de los ajustes de configuración de la aplicación. Puede ver la versión clonada en el Resumen de configuración de aplicaciones y en la aplicación clonada.

Elegir las aplicaciones de Windows 10 para su catálogo interno

Elija las aplicaciones que va a añadir a su catálogo de aplicaciones internas. Las aplicaciones internas, de Microsoft Store y de Microsoft for Business son compatibles con Windows 10. Windows 10 implementa el cumplimiento directamente en el dispositivo de acuerdo con las aplicaciones que decida permitir o no permitir.

> El intervalo de ingresos predeterminado de Windows 10 es de una vez cada 60 minutos. Es recomendable realizar un ingreso forzado del dispositivo para obtener una actualización del estado del dispositivo y la aplicación.

Se admiten las siguientes acciones:

- Cargar nuevas aplicaciones
- Instalación silenciosa
- Instalar manualmente desde Apps@Work
- Añadir una versión nueva de la aplicación
- Eliminar una aplicación

Se admiten los siguientes formatos:

- APPX
- APPXBUNDLE
- Win32 ajustado en MSI - aplicación Win32 previamente empaquetada
- MSIX (compatible con dispositivos RS5 y posteriores a Windows 10)
- .EXE (con bridge)

> La aplicación **Ivanti Neurons Agent** está disponible en el **Catálogo de aplicaciones** de dispositivos **Windows**. El administrador puede desplegar la aplicación **Ivanti Neurons Agent** como una aplicación interna y esta aplicación se puede distribuir de igual manera en los dispositivos Windows.

Configurar aplicaciones de Windows 10

Procedimiento

1. Haga clic en **Dispositivos** en la barra de navegación principal.
2. Seleccione un dispositivo Windows 10 con el que se haya inscrito en Ivanti Neurons for MDM.
3. Haga clic en **Aplicaciones > Catálogo de aplicaciones**.
4. Seleccione una aplicación.
5. Utilice el menú desplegable **Acciones** para añadir la aplicación o eliminarla de su catálogo.
   Opcionalmente, también puede añadir una versión nueva de la aplicación.
   - Haga clic en el menú desplegable **Acciones**.
   - Seleccione **Añadir nueva versión**.
   - Vaya el catálogo y seleccione una nueva versión de la aplicación.
   - Haga clic en **Actualizar y guardar** para ver la pantalla de información de la aplicación.
6. Utilice el menú desplegable **Versión** para elegir qué versión desea utilizar.
7. Haga clic en **Editar** para comenzar a modificar los detalles.
   - Edite la **Categoría**, si fuera necesario.
   - Ingrese una **Descripción**, si fuera necesario.
   - Añada capturas de pantalla si fuera necesario.
8. Haga clic en **Guardar**.
9. Haga clic en la pestaña **Distribución** y luego en **Editar** para comenzar a modificar el nivel de distribución.
10. Haga clic en **Guardar**.
11. Haga clic en la pestaña **Configuraciones de aplicaciones** para ver un resumen de la configuración actual.
12. Introduzca, si fuera necesario, una descripción de la aplicación.
13. Haga clic en **Instalar en el dispositivo** en la página de resumen de Configuraciones de aplicaciones.
    El valor predeterminado es la instalación silenciosa y no puede modificarse
14. Haga clic en **Promoción** en el panel de navegación de la izquierda y, luego, haga clic en **Ajustes de configuración de distribución de promoción** para cambiar el nivel de promoción.
    - Haga clic en **Editar** para comenzar a modificar los ajustes del nivel de promoción.
    - Introduzca un nombre para la configuración.
    - Introduzca una descripción para la configuración.
    - Seleccione un nivel de promoción.
    - Haga clic en **Actualizar** para guardar los cambios.
15. Haga clic en la pestaña **Opiniones** para ver información sobre las opiniones.
    Exporte, si fuera necesario, los datos de las opiniones a una hoja de cálculo.

Editar los ajustes de configuración de aplicaciones de Windows 10

Procedimiento

1. Haga clic en **Políticas > Configuración**.
2. Haga clic en **+Agregar**.

3. Seleccione **Control de aplicaciones de Windows** para ver la pantalla **Crear configuración de control de aplicaciones de Windows**.
4. Ingrese un **Nombre** y una **Descripción** para la configuración.
5. Defina el tipo de aplicación del siguiente modo:
    - Permitidas (en la lista de permitidos) - solo se permiten estas aplicaciones. Estas aplicaciones se instalan de forma silenciosa si no están ya presentes en el dispositivo.
    - No permitidas (en la lista de bloqueados) - si están presentes en el dispositivo, estas aplicaciones se bloquearán cuando se inicien.
6. Especifique las definiciones de Reglas para el Tipo de aplicación e Identificador de aplicaciones.
7. Haga clic en **Buscar aplicaciones** para ver la pantalla **Buscar aplicaciones de Windows 10**.
8. Introduzca el nombre de la aplicación que desea buscar en la Windows Store.
9. Seleccione la aplicación de entre las opciones mostradas para añadirla al Identificador de aplicaciones.
10. Opcionalmente, también puede usar el menú desplegable «Tipo de aplicación» para definir una ruta en el identificador de aplicaciones con el fin de permitir o no permitir ciertas aplicaciones utilizando dicha ruta especificada o para bloquear todas las aplicaciones instaladas en dicha ruta.
    El tipo de aplicación **Editor/Iguales PFN** se aplica a dispositivos Windows 10+ y admite PFN. **EXE/Win32 es igual a**.
11. Haga clic en **Siguiente**.
12. Elija un nivel de distribución.
    - **Todos los dispositivos**.
    - **No hay dispositivos**.
    - **Personalizado** - para introducir los usuarios o grupos que recibirán la aplicación.
13. Haga clic en **Listo**.
14. Puede editar las definiciones de Regla para seleccionar un Tipo de aplicación y especificar el Identificador de aplicaciones.
    - Haga clic en el menú desplegable **Acciones**.
    - Seleccione **Añadir nueva versión**.
    - Seleccione una versión nueva de la aplicación.
    - Haga clic en **Actualizar y guardar** para ver la pantalla de **información de la aplicación**.

Configuración de Reiniciar dispositivo después de la opción de instalación de Windows.

Puede configurar un dispositivo para que se reinicie después de instalar una aplicación mediante la opción **Reiniciar dispositivo tras la instalación**.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Seleccione cualquier aplicación específica de Windows en la lista.
3. Vaya a **Configuración de aplicaciones > Instalar en dispositivo > Instalar el ajuste de configuración de la aplicación**.
4. Haga clic en **Editar** y ajuste la opción de **Reiniciar el dispositivo tras la instalación** como ACTIVO.
5. Seleccione una de las siguientes opciones de programación en la que desea reiniciar el dispositivo:

Ajuste	Qué hacer
Justo después de la instalación	Seleccione esta opción para reiniciar el dispositivo poco después de instalar la aplicación.
A determinadas horas del día	Seleccione esta opción para reiniciar el dispositivo a una hora específica después de instalar la aplicación.
Tras unos minutos	Seleccione esta opción para reiniciar el dispositivo **15**, **30**, **60** o **120** minutos después de instalar la aplicación.

6. Haga clic en **Actualizar**.

El dispositivo se reiniciará a la hora programada.

> En el caso de las aplicaciones públicas y de las aplicaciones de Microsoft Store for Business (MSB), debe establecer el ajuste **Instalar silenciosamente en dispositivos de Windows** como ACTIVO desde la sección **Configuración de aplicaciones**.

Instalación de aplicaciones con Apps@Work

Para instalar una aplicación usando Apps@Work:

1. Haga clic en la aplicación **Apps@Work**.
   La dirección de correo electrónico y la URL del servidor de su administrador está previamente rellenadas en el diálogo de inicio de sesión de Apps@Work.
2. Introduzca su contraseña y haga clic en «Iniciar sesión» para mostrar la página de las aplicaciones.
3. Seleccione una aplicación para instalarla. No podrá instalar aplicaciones con dependencias en aplicaciones con requisitos previos si estas últimas aplicaciones no están ya instaladas en el cliente.
   Para Apps@Work en dispositivos iOS, también tiene la opción de hacer clic en el botón **Instalar todo** para instalar todas las aplicaciones. Esta opción está disponible en las pantallas **Nuevos lanzamientos**, **Aplicaciones destacadas** y **Categorías**.

> las aplicaciones de Apps and Books no se instalarán si no se acepta previamente la licencia de la aplicación Apps and Books.

4. Haga clic en **Actualizar y guardar** para ver la pantalla de **información de la aplicación**.

Instalación de aplicaciones y actualizaciones para dispositivos de Android Enterprise

Los administradores pueden publicar una aplicación en el catálogo para acceso general y, al mismo tiempo, implementarla en un dispositivo específico para su uso inmediato. Esto permite a los usuarios recibir la aplicación directamente, mientras esta sigue estando disponible en el catálogo para que otros la instalen según sea necesario.

Para instalar aplicaciones y actualizaciones

1. Vaya a **Aplicaciones > Apps Catalog**.
2. Elija la aplicación que desea.
3. Haga clic en **Acciones** en la pantalla **Detalles**. Se muestra la opción **Enviar solicitud de instalación/actualización**.
4. Haga clic en Enviar solicitud de instalación/actualización. Se muestra el cuadro de diálogo **Enviar solicitud de instalación/actualización**.

5. Lleve a cabo la acción siguiente de **Enviar notificaciones de instalar y actualizar a los dispositivos de esta aplicación**:
    - Seleccione la casilla **Enviar solicitud para aplicación nueva (se aplica a los dispositivos que aún no tienen instalada la aplicación)** para instalar la aplicación nueva.
    - Seleccione la casilla **Enviar solicitud para actualizaciones (aplicable a dispositivos que tienen la aplicación instalada pero está disponible una actualización)** para actualizar una aplicación instalada.
6. Lleve a cabo la siguiente acción en **Seleccionar usuarios para enviar solicitudes**:
    - Haga clic en **Todos** para distribuir la configuración a todos los usuarios compatibles. La aplicación aparece en su App Catalog.
    - Haga clic en **Personalizado** para definir el grupo de usuarios o el usuario que verá la aplicación en App Catalog.

    > La distribución **Enviar solicitud de instalación/actualización** forma parte del proceso de distribución de aplicaciones. La configuración que elijas en la pantalla **Distribución** determinará qué dispositivos recibirán la aplicación.

Aparece una ventana de confirmación que indica que se ha completado la instalación de la aplicación.

Los cambios de nuevas instalaciones o actualizaciones se muestran en **Tablero de resultados** > **Audit Trails**.

> Para aplicaciones públicas y privadas, la opción **Enviar solicitud para actualizaciones (aplicable a dispositivos que tienen la aplicación instalada pero está disponible una actualización)** se encuentra deshabilitada. Solo se permiten solicitudes de **Enviar solicitud para una nueva aplicación**.

Temas relacionados:

- Catálogo de aplicaciones

Borrado de la caché de aplicaciones en dispositivos Android Enterprise

La **solicitud de borrado de caché** permite a los administradores eliminar de forma remota los datos almacenados en caché de una aplicación seleccionada instalada en dispositivos Android Enterprise mediante Ivanti Neurons for MDM. Esta acción ayuda a solucionar incidencias comunes de las aplicaciones, como un rendimiento lento, errores inesperados o datos temporales obsoletos, sin tener que desinstalar ni reinstalar la aplicación. La solicitud borra únicamente la caché de la aplicación y conserva los datos del usuario, la configuración de la aplicación y las configuraciones establecidas. Los administradores utilizan esta funcionalidad para restablecer rápidamente el comportamiento normal de las aplicaciones, minimizando las interrupciones en los usuarios finales.

Procedimiento

1. Vaya a **Aplicaciones** > **Catálogo de aplicaciones**.
2. Seleccione y abra la aplicación.
   Se mostrará la página **Detalles** de la aplicación.
3. Haga clic en el menú de acciones (⋮) en la página de **Detalles** de la aplicación.
4. Seleccione la opción **Solicitud de borrado de caché de aplicaciones** .
   Se mostrará el panel de **Solicitud de borrado de caché de aplicaciones** .
5. Realice una de las siguientes acciones en la sección **Seleccionar usuarios para enviar la solicitud** para distribuir la solicitud de borrado de caché de aplicaciones:
    - Seleccione **Todos** para enviar la solicitud a todos los dispositivos compatibles en los que esté instalada la aplicación.

- Seleccione **Personalizado** para enviar la solicitud a usuarios, grupos de usuarios, dispositivos o grupos de dispositivo específicos.

6. (Opcional) Busque una lista de distribución existente en **Otras opciones de filtro de distribución**.
7. (Opcional) Seleccione **+ Añadir filtro de distribución** para crear un filtro de distribución en el panel **Crear filtro de distribución** .

Utilice esta opción para enviar la **Solicitud de borrado de caché de aplicaciones** a un conjunto específico de dispositivos, como dispositivos en modo DO o EPO.

8. Haga clic en **Enviar**.
9. Haga clic en **Aceptar** en el cuadro de diálogo de confirmación de **Borrado de caché de aplicaciones** .
   Ivanti Neurons for MDM muestra una notificación con el número de dispositivos que recibieron la **Solicitud de borrado de caché de aplicaciones**.

Una vez completada la solicitud **Borrar caché de la aplicación** los datos de la aplicación (versión, nombre, platformAppId, displayVersion y bundleVersion) quedan registrados en la página **Rastros de auditoría**.

8.8. Asignar atributos personalizados a las aplicaciones

Después de crear atributos personalizados, puede asignarlos a una o más aplicaciones. Cada atributo tiene un valor correspondiente que puede usar para tareas como la creación de grupos de aplicaciones. Para obtener más información sobre cómo administrar atributos, consulte **Atributos**.

Crear y asignar un atributo personalizado para una aplicación individual

Puede asignar un atributo personalizado a una única aplicación.

Procedimiento

1. Inicie sesión en el portal administrativo.
2. Vaya a **Aplicaciones** > **Catálogo de aplicaciones**.
3. Seleccione una aplicación y haga clic en **Atributos**.
4. Haga clic en **+Agregar nuevo**, seleccione un valor en el menú desplegable de **Nombre del atributo**.
5. Especifique el valor del atributo en el campo **Valor**.
6. Haga clic en **Guardar**. El atributo personalizado se agrega a la aplicación.

Asignar un atributo personalizado a varias aplicaciones

Puede asignar atributos personalizados a una o más aplicaciones. Cuando selecciona varias aplicaciones, el atributo personalizado se aplica a cada versión de la misma. Puede seleccionar una aplicación específica, vaya a la pestaña Atributos y cambie los detalles del atributo personalizado para una versión específica de la aplicación.

Procedimiento

1. Inicie sesión en el portal administrativo.
2. Vaya a **Aplicaciones** > **Catálogo de aplicaciones**.
3. Marque las casillas de una o más aplicaciones.
4. Haga clic en **Acciones**.
5. Seleccione **Asignar atributos personalizados**. Aparece el asistente Asignar atributos personalizados a aplicaciones.
6. Seleccione *una* de las siguientes opciones:
    - Forzar la asignación (sobreescritura) de todos los atributos aunque se encuentre algún valor existente.
    - Sobrescribir solo si el valor está vacío y omitir atributos con valores existentes.
7. Marque las casillas de uno o más atributos.
8. Especifique el valor en los campos Valor (no están permitidos los valores vacíos).
9. Haga clic en **Asignar**. El atributo personalizado se asigna a todas las versiones de las aplicaciones seleccionadas.
10. (Opcional)Si quiere cambiar el atributo personalizado por una única versión de la aplicación, seleccione la versión de la aplicación en el desplegable de versiones y haga clic en Editar.

Se pueden usar los **Atributos de aplicaciones personalizadas** con sus valores para crear informes y exportar al formato CSV desde la página **Detalles de dispositivos**.

8.9. Configuraciones administradas para Android

Esta sección contiene los siguientes temas:

- Utilizar las configuraciones administradas para Android Enterprise
- Restricciones y permisos de aplicaciones para aplicaciones internas
- Configuración de Gmail con Android Enterprise

Si Ivanti Neurons for MDM tiene habilitado Android Enterprise, la configuración de Android Enterprise estará disponible para usarse por aplicación.

Utilizar las configuraciones administradas para Android Enterprise

1. Haga clic en **Aplicaciones**.
2. Haga clic en **Catálogo de aplicaciones**.
3. Seleccione una aplicación para la que realizar la configuración de Android Enterprise.
4. Haga clic en **Configuraciones de aplicaciones**.
5. Haga clic en **Configuraciones administradas para Android**.
6. Introduzca un nombre para la configuración.
7. Opcionalmente, también puede añadir una descripción.
8. Utilice los campos Configuraciones administradas para configurar los comportamientos de las configuraciones administradas:
9. Utilice los **Ajustes de configuración de Tunnel** para integrar directamente Tunnel en la aplicación Ivanti Go para dispositivos Android. Seleccione **Habilitar ajustes de Tunnel** para activar esta configuración. Con esta mejora, los administradores pueden habilitar las funciones de Tunnel desde Ivanti Go y configurar una conexión segura mediante las configuraciones de Tunnel existentes. Esta función está disponible en los dispositivos Android que se inscriban a partir de ahora. Esta función está disponible en los dispositivos Android que se inscriban a partir de ahora. Sin embargo, en los dispositivos que tengan instalada la aplicación Tunnel independiente no estará disponible la funcionalidad de Tunnel integrada en Ivanti Go. Una vez desinstalada la aplicación Tunnel independiente, la funcionalidad de Tunnel integrada estará disponible en Ivanti Go. Cada dispositivo solo puede tener aplicada una configuración de Tunnel a la vez.

Ajuste	Descripción
Bloqueo de la aplicación para que no comparta widgets en los perfiles	Permite impedir que las aplicaciones compartan widgets en los perfiles solo si la aplicación no se ha instalado de forma silenciosa. Deje desactivada esta opción para permitir que las aplicaciones de confianza instaladas en el perfil de Android Enterprise muestren widgets en la pantalla de inicio, para que los usuarios puedan acceder a la información sin tener que iniciar sesión.
Bloqueo del usuario para que no pueda desinstalar la aplicación	Habilite esta opción para bloquear posibilidad de que el usuario desinstale la aplicación (pública, privada o en las instalaciones) después de que Ivanti Neurons for MDM haya instalado la aplicación de forma silenciosa.
Código de la versión mínima	Establezca un código de versión mínima necesaria para que la aplicación anule el comportamiento de actualización predeterminado. Si el código de la versión de la aplicación instalada actualmente en el dispositivo es anterior al código de la versión mínima especificada, la aplicación se actualiza inmediatamente a la última versión.
Lanzamiento automático al instalarlo	Seleccione esta opción si desea iniciar una aplicación automáticamente después de su instalación. Esta funcionalidad solo está disponible si la aplicación está recién instalada en el dispositivo y no para una actualización de versión. En el caso del Perfil de trabajo y del Perfil de trabajo en los dispositivos propiedad de la empresa, la aplicación Go debe estar activa y en primer plano. Debido a las limitaciones de Android 10+, solo se lanzará una aplicación si el usuario pulsa varias aplicaciones en el caso del Perfil de trabajo y el Perfil de trabajo en los dispositivos propiedad de la empresa.

10. El administrador puede controlar los campos de configuración de la aplicación que se pueden enviar a los dispositivos o que no se deben enviar. En general, los valores predeterminados se establecen cuando se envían las configuraciones a distintos dispositivos. En la sección Configuraciones administradas, del ajuste **Forzar en el dispositivo**, seleccione **Forzar todos los ajustes** o **Forzar solo los ajustes con valores definidos**.

Configuración de dominios administrados

Cada configuración administrada para Android Enterprise muestra un botón que habilita los certificados para cada campo de texto. Al pulsarlo, se reemplaza dicho campo por una lista desplegable de certificados. Cuando esta opción está configurada, los certificados se aplican de forma silenciosa sin interacción alguna por parte del usuario.

Un campo habilitado para certificado existente puede cambiarse a habilitado para texto, haciendo clic en el mismo botón junto al campo. Un campo habilitado para texto cambiado a campo habilitado para certificado puede volver a cambiarse a campo habilitado para texto, haciendo clic en el mismo botón. (Los campos desplegables predeterminados no pueden revertirse a campos habilitados para texto).

> Si no hay certificados de Id. configurados en el dispositivo abonado, cuando se cambia de texto a desplegable con el botón de habilitar certificados, la única opción que se mostrará en la lista desplegable será «Ninguno».

Haga clic en **Administrar permisos** para seleccionar y configurar los permisos del tiempo de ejecución para las aplicaciones creadas con API 23+ o posterior y Android 6.0+.

Solo se incluyen para seleccionar los permisos peligrosos aplicables a la aplicación específica. La lista completa de los permisos peligrosos (como leer sus contactos, encontrar cuentas en el dispositivo, escribir registros de llamadas, etc.) están enumerados en https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups.

11. Algunos de los derechos que puede asignar a cada permiso son los siguientes:
    - Los permisos se aplican solamente cuando la aplicación los solicita.
    - Los permisos no se aplican si los usuarios los han aceptado o denegado previamente.
    - Concesión automática
    - Denegación automática. Utilice este ajuste con precaución
    - Predeterminado/global

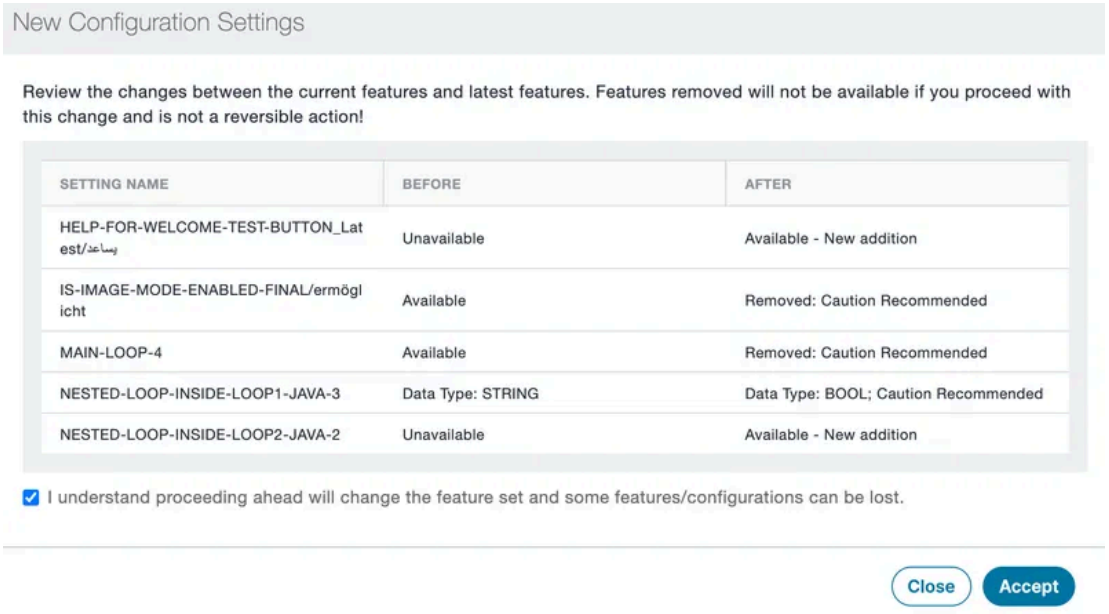
Configure las opciones de distribución seleccionando entre **A todas las personas con la aplicación**, **A nadie** o **Personalizado**.

12. Haga clic en **Guardar**.

Nuevos ajustes de configuración

Cuando se actualiza la versión de una aplicación y si hay algún cambio en las configuraciones existentes, aparece el botón **Actualizar a las funciones más recientes** después de editar la página Detalles de configuración.

1. Haga clic en **Actualizar a las funciones más recientes**.
   Aparece un mensaje de advertencia en la pantalla que indica que pasar a las funciones más recientes impedirá que los usuarios accedan a las versiones anteriores de la aplicación. El mensaje de advertencia recomienda pasos para integrar la última versión de la aplicación sin problemas.
2. Haga clic en **Siguiente**.
3. Aparece en pantalla la ventana **Ajustes de nuevas configuraciones**.



La ventana **Ajustes de la nueva configuración** enumera distintos ajustes que existían con la configuración, y el estado de cada ajuste después de la actualización. La ventana Nueva configuración enumera todas las restricciones de la base de datos y el esquema de Google enumerará el siguiente estado:

- Agregado
- Eliminado
- Modificado

Seleccione la casilla de verificación y haga clic en **Aceptar** para continuar con la actualización.
Aparece un mensaje de confirmación en la pantalla de que la configuración se ha actualizado correctamente con las últimas funciones. Ahora puede distribuir y guardar las configuraciones para que los cambios surtan efecto.

Restricciones y permisos de aplicaciones para aplicaciones internas

El administrador puede establecer algunas restricciones de aplicaciones y restringir o dar permisos para aplicaciones internas. Esta función solo estaba disponible para aplicaciones públicas. Pero esta función se ha ampliado ahora a las aplicaciones internas.

> El administrador debe volver a cargar las aplicaciones internas para que las funciones de **Restricción de aplicaciones** y **Permisos** estén disponibles en sus aplicaciones. Se recomienda eliminar la aplicación existente antes de cargar una nueva versión.

Procedimiento

1. Vaya a **Aplicaciones** > **Catálogo de aplicaciones**.
2. Seleccione una aplicación **Interna** de la lista.
3. Haga clic en **Configuraciones de aplicaciones**.
4. Haga clic en **Configuraciones administradas para Android**.
5. Haga clic en **Añadir**.
6. Aparece en pantalla la sección **Restricciones de la aplicación**.
   Introduzca los valores necesarios para las restricciones disponibles.
7. Seleccione **Administrar permisos**.
8. La ventana **Permisos seleccionados** aparecen en la pantalla.
   Seleccione los permisos necesarios de la lista y haga clic en **Seleccionar**.
9. En la sección **Permisos de tiempo de ejecución**, ajuste los valores de los permisos seleccionados.
10. En la sección **Distribuir la configuración de esta aplicación**, elija una de las opciones siguientes **Distribución de aplicaciones**:
    - **A todas las personas con la aplicación**
    - **A nadie**
    - **Personalizado**
11. Haga clic en **Guardar**.
    Las restricciones y permisos seleccionados se aplicarán en las aplicaciones internas.

Configuración de Gmail con Android Enterprise

Puede implementar Gmail en dispositivos con Android Enterprise si ha configurado Ivanti Neurons for MDM para Android Enterprise.
Para configurar Gmail con Android Enterprise

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Seleccione la aplicación de Gmail para la que realizar la configuración de Android Enterprise. Aparece la sección Establecimiento de la configuración.

3. Introduzca un nombre para la configuración.
4. Opcionalmente, también puede añadir una descripción.
5. Utilice los campos **Configuraciones administradas** para configurar los comportamientos de las configuraciones administradas:

Las opciones **Ampliar todo** y **Contraer todo** están solo disponibles para restricciones anidadas o de jerarquía.

Ajuste	Descripción
Enviar al dispositivo	Enviar todos los ajustes: seleccione esta opción para habilitar todas la alternancias, incluidas aquellas sin valores Enviar solo los ajustes con valores definidos: seleccione esta opción para habilitar todas la alternancias con los valores definidos y deshabilite las alternancias para ajustes sin valores En muchos casos, los ajustes predeterminados ya están disponibles. No obstante, el administrador puede seleccionar los ajustes de configuración de las aplicaciones requeridas o editar las variables que se deben enviar a los dispositivos.
Dirección de correo electrónico	Ingrese variables de sustitución para definir la dirección de correo electrónico. Normalmente se suele introducir $emailaddress$. Los UEM pueden usar este campo para sacar las credenciales de usuario del Active Directory.
Nombre del host o host	Introduzca el nombre de host del servidor Active Sync, como hostname.company.com:443/path.
Nombre de usuario	Utilice la variable para el nombre de usuario de Active Directory del usuario que se puede especificar como un nombre de usuario directo (janedoe) o un valor de plantilla ($username$).
Tipos de autenticación	Seleccione la lista de strings que contienen los tipos de autenticación permitidos.
SSL obligatorio	Cuando se selecciona, permite y requiere SSL en números de puerto utilizados con nombre de host.
Confiar en todos los certificados	Seleccione esta opción solamente si desea que la aplicación acepte automáticamente certificados que no sean de confianza. Utilice esta opción solo para la depuración o el desarrollo cuando trabaje en un entorno de pruebas.
Alias del certificado de inicio de sesión	Ingrese el alias para el certificado de inicio de sesión utilizado para los servidores ActiveSync.
Permitir cuentas no administradas	Seleccione esta opción para permitir a los usuarios añadir o eliminar cualquier cuenta de Exchange que no sea la cuenta especificada en esta configuración administrada.
Firma predeterminada del correo electrónico	Ingrese la secuencia que conforma la firma de correo electrónico predeterminada que se agregará al final del texto de todos los mensajes de correo electrónico salientes.
Ventana de sincronización predeterminad	Ingrese el valor de 0 a 5 que representa el período para la sincronización con EAS (Sincronización activa de Exchange).

Haga clic en **Siguiente**.

7. Configure las opciones de distribución seleccionando entre **A todas las personas con la aplicación**, **A nadie** o **Personalizado**.
8. Haga clic en **Guardar**.

8.10. Administrar aplicaciones de Google Play

Se puede definir qué binario de la aplicación Google Play debe implementarse para grupos o personas específicas. Esta implementación es aplicable a las implementaciones corporativas de Android. El desarrollador de la aplicación debe además poner su organización en la lista de permitidos para poder implementar las aplicaciones del canal alfa o beta.

1. Haga clic en **Aplicaciones**.
2. En el **App Catalog**, seleccione una aplicación en la que establecer la configuración del lanzamiento de Google Play.
3. Haga clic en la pestaña **Configuraciones de la aplicación**.
4. Haga clic en **Lanzamiento de Google Play**.

> La configuración del lanzamiento de Google solo se aplica a las aplicaciones con la versión corporativa de Android. De forma predeterminada, se aplica la opción Producción si no se selecciona la configuración del lanzamiento de Google para aplicaciones recientemente añadidas.

Haga clic en **Añadir**.

6. Introduzca un nombre para la configuración.
7. Opcionalmente, también puede añadir una descripción.
8. Seleccione una opción de la lista desplegable para seleccionar el binario que estará disponible para los usuarios y dispositivos que vayan a recibir esta aplicación. Existen las siguientes opciones:
   - Producción
   - Alfa
   - Beta

   > La opción Producción se aplica de forma predeterminada a las aplicaciones que ya están insertadas en el dispositivo.
9. Configure las opciones de distribución seleccionando entre **A todas las personas con la aplicación**, **A nadie** o **Personalizado**.
10. La opción **Personalizado** distribuye la aplicación dentro del grupo de usuarios junto con el filtro del dispositivo.
    Haga clic en **Guardar**.

Priorizar la configuración del lanzamiento múltiple

Cuando se añaden múltiples configuraciones de lanzamientos de Google, se puede priorizar el orden en que se aplica dicha configuración.

1. En **Configuraciones de aplicaciones**, haga clic en **Priorizar configuraciones**.

> Este botón solo se muestra cuando se enumeran múltiples configuraciones.

De las configuraciones enumeradas, arrastre y suelte la configuración que debe aplicarse de forma prioritaria a la parte inicial de la lista.

3. Haga clic en **Actualizar**.

Cuando se elimina la configuración prioritaria, la configuración que antes estaba enumerada en segundo lugar tendrá la prioridad máxima.

8.11. Eliminar aplicaciones del App Catalog

Puede eliminar aplicaciones públicas e internas del Catálogo de aplicaciones. No se pueden eliminar las aplicaciones con requisitos previos. Es necesario editar las aplicaciones para eliminar las relaciones de requisitos previos antes de eliminar dichas aplicaciones. Si la aplicación está instalada en dispositivos, se eliminará la próxima vez que esos dispositivos ingresen. La instalación/desinstalación silenciosa de aplicaciones es compatible con dispositivos Samsung y Zebra en el modo Administrador de dispositivos, o con todos los dispositivos en modo Propietario de dispositivos.

En el caso de las aplicaciones internas, aparece en la pantalla una ventana de confirmación. Debe seleccionar que acepta que desea continuar con la operación Eliminar y hacer clic en **Eliminar aplicación**. Cuando intenta eliminar varias aplicaciones y algunas no se pueden eliminar, aparece una ventana en la pantalla con información sobre las aplicaciones que no se pueden eliminar y el motivo.

Las condiciones siguientes se aplican cuando intenta eliminar una o más aplicaciones desde el Catálogo de aplicaciones:

- Si no se puede eliminar una versión de la aplicación interna, no es posible eliminar ninguna versión.
- Si una versión de la aplicación interna es un requisito previo, ni la aplicación ni ninguna de las versiones se pueden eliminar.
- Cuando selecciona todas o algunas de las aplicaciones internas para eliminarlas del Catálogo de aplicaciones, se eliminarán todas las versiones de las aplicaciones internas.
- Una aplicación interna delegada desde un Space no se puede eliminar.

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Haga clic en el vínculo de la aplicación.
3. Seleccione **Acciones > Eliminar del catálogo**.
4. Lea la advertencia que explica qué ocurre cuando se elimina una aplicación.
5. La advertencia explica que las licencias de Apps and Books (iOS) y las opiniones sobre las aplicaciones (todos los SO) también se eliminan.
   Marque la casilla "Entiendo la consecuencias de eliminar una aplicación" para proceder con la eliminación.
6. Haga clic en **Eliminar aplicación**.

8.12. Actualizar aplicaciones internas

Utilice el siguiente procedimiento para actualizar una aplicación interna:

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Seleccione la aplicación que desea actualizar.
3. Seleccione **Acciones > Añadir nueva versión**.
4. Arrastre y suelte la aplicación al área **Cargar aplicación** o haga clic en **Elegir archivo** para seleccionarlo del sistema de archivos.
5. Seleccione una de las siguientes opciones dependiendo de lo que desee hacer con la versión anterior de la aplicación:
    - **Mantener la descripción, las capturas de pantalla, la distribución, los requisitos previos de aplicaciones y las configuraciones de aplicaciones iguales:** sustituye la versión anterior en el App Catalog.
    - **Cambiar la descripción, las capturas de pantalla, la distribución, los requisitos previos de la aplicación o las configuraciones de la aplicación**: incluye ambas versiones en el App Catalog.
6. En **Novedades**, introduzca texto que aclare a los usuarios las diferencias que hay en la versión nueva.
7. El texto se mostrará en el dispositivo cuando el usuario seleccione la aplicación para instalar.
   Si decide cambiar las descripciones, capturas de pantalla u opciones de distribución, complete estos cambios.
8. Haga clic en **Hecho**.

Si decide mantener las versiones anteriores de la aplicación en el catálogo, solo aparecerá una entrada en **Aplicaciones > Catálogo de aplicaciones**. El panel de más a la izquierda indicará el número de aplicaciones que representa la entrada. Si después decide eliminar la versión más reciente, la versión más antigua la reemplazará automáticamente en los dispositivos instalados.

Mostrar una lista de versiones de la aplicación

Los administradores están autorizados a cargar aplicaciones con la misma versión y arquitecturas diferentes.

ProcedureProcedimiento

1. Haga clic en el vínculo de la aplicación en **Aplicaciones > App Catalog**.
2. Haga clic en la pestaña **Versión**.
   Si hay múltiples versiones de la aplicación en el catálogo, una lista desplegable mostrará todas las versiones. Si se cargan varias aplicaciones con el mismo número de versión pero con diferentes arquitecturas, el menú desplegable muestra los detalles de las arquitecturas admitidas. Las arquitecturas admitidas para las aplicaciones también se muestran en **Información de la aplicación**.

8.13. Encontrar el nombre del paquete de una aplicación de Android

Para aplicaciones públicas disponibles en la Google Play Store:

1. Utilice un explorador web para encontrar la aplicación en la Google Play Store.
2. Seleccione la aplicación.
3. Observe la URL que se muestra en el explorador.

El nombre del paquete se incluye en la URL después de id=, según se indica a continuación:

https://play.google.com/store/apps/details?id=<package name>

Para aplicaciones internas y otras aplicaciones no disponibles en la Play Store, pruebe a descargar el **Visualizador de nombres de paquetes** u otra aplicación similar en la Google Play Store.

8.14. Categorías

Esta sección contiene los siguientes temas:

- Añadir una categoría
- Quitar una categoría

Las categorías describen tipos de aplicaciones y ayudan a organizar las aplicaciones cuando los usuarios exploran el App Catalog. Cada aplicación debe tener al menos una categoría asignada. Hay disponible una lista de categorías comunes de aplicaciones cuando comience a utilizar Ivanti Neurons for MDM. Utilice esta página para administrar categorías de aplicaciones.

Añadir una categoría

Puede añadir nuevas categorías aquí o cuando añada una aplicación al catálogo de aplicaciones.

1. Haga clic en **Añadir** (abajo a la izquierda).
2. Escriba el nombre de la categoría.
3. Las categorías no diferencian entre mayúsculas y minúsculas, de forma que MÍO y Mío es lo mismo.
   Haga clic en **Guardar**.

Quitar una categoría

- Haga clic en la X que hay junto a la categoría.

Si no puede realizar las tareas en la página **Categorías de aplicaciones**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes funciones:

- Administración de aplicaciones y contenido

8.15. Filtros de distribución

Esta sección contiene los siguientes temas:

- Configurar los filtros de distribución
- Configurar los filtros de distribución para el administrador delegado

Utilice filtros de distribución para limitar las aplicaciones disponibles para instalar. Los filtros de distribución le permiten visualizar solamente las aplicaciones del catálogo de aplicaciones que sean aplicables al dispositivo.

Licencia: Silver

Estos son los filtros que están disponibles de forma predeterminada:

- **Aplicaciones compatibles con la versión corporativa de Android**: limita la distribución de aplicaciones únicamente a los dispositivos compatibles con la versión corporativa de Android.
- **Aplicaciones solo para iPad**: limita la distribución de aplicaciones solamente a dispositivos iPad.
- **Aplicaciones solo para iPhone**: limita la distribución de aplicaciones solamente a dispositivos iPhone.

Configurar los filtros de distribución

1. Vaya a **Aplicaciones > Filtro de distribución**.
   Aquí aparecerán los filtros predeterminados de aplicaciones y cualquier filtro de aplicación que se haya creado.
2. Haga clic en **+Añadir** para acceder al diálogo **Crear filtro de distribución**.
3. Introduzca un nombre y una descripción en los campos adecuados.
4. Seleccione las definiciones de reglas. Estas reglas se pueden crear usando los operadores correspondientes, como «contiene», «es menor que», «es mayor que», «está en el intervalo de», «es igual a» y «no es igual a». Las reglas se pueden anidar juntas utilizando las opciones CUALQUIERA (O) o TODOS (Y). Los filtros de distribución de aplicaciones son los siguientes:
   - Acceso bloqueado
   - Compatible con APNS
   - Dispositivo administrado de Android con perfil profesional
   - Android for Work habilitado
   - Nivel de revisión de la seguridad de Android (dispositivos Android)
   - Dispositivos Android administrados en el trabajo (Propietario del dispositivo) habilitados
   - Perfil de trabajo de Android en el Dispositivo propiedad de la empresa habilitado
   - Último ingreso del cliente
   - Registrado con el cliente
   - Cumplimiento
   - Medida de cumplimiento bloqueada
   - Nombre del país actual
   - MMC actual
   - MNC actual
   - Atributo personalizado del dispositivo

- Atributo personalizado de LDAP
- Atributo personalizado del usuario
- Atributos personalizados IDP
- Tipo de dispositivo
- Nombre del país de origen
- MCC de origen
- MNC de origen
- IMEI
- IMEI2 (solo en dispositivos Android con doble puerto SIM y aplicable para dispositivos Android 8.0 o superior)
- Modo pantalla completa
- Fabricante
- Versión de SO
- Propiedad
- N.º de teléfono
- Itinerancia
- Estado de Secure Apps
- Supervisado
- Sentry bloqueado
- Inscripción de usuarios inscritos
- Inscrito en la Inscripción de dispositivos automatizada
- Inscripción de dispositivos automatizada activada

5. Haga clic en **Crear filtro de distribución**.
6. Si fuera necesario, seleccione un filtro personalizado para actualizar.
    1. Haga clic en **Editar** para visualizar la página **Actualizar filtro de distribución**.
    2. Introduzca un nombre y una descripción en los campos adecuados.
    3. Utilice los menús desplegables para definir reglas para el filtro.
    4. Haga clic en **Crear filtro de distribución**.
7. Seleccione una aplicación.
8. En la página Detalles de la aplicación, seleccione la pestaña **Distribución**.
9. Haga clic en **Editar**.
10. Elija una opción de distribución de aplicaciones:
    - **A todo el mundo**
    - **A nadie**
    - **Personalizado**

> La sección de Filtro de distribución solo es visible si se selecciona **Todas las personas** o la opción de distribución **Personalizada**.

11. Elija una opción del filtro distribución:
    1. Introduzca un nombre de filtro en **Buscar los filtros de distribución existentes**... Para encontrar un filtro que ya se haya creado.
    2. Haga clic en **+Añadir filtro de distribución** para añadir un filtro nuevo.

> Los filtros de distribución se pueden crear o asignar a una aplicación antes de añadirla al catálogo. Los cambios realizados en los filtros de distribución afectarán a la distribución de las aplicaciones que estén usando dicho filtro (en todos los espacios).

> Cuando se configura el filtro y si el **Permitir la instalación de aplicaciones en dispositivos M1 al momento de la distribución** está habilitado, el resultado llena los dispositivos macOS M1. La aplicación iOS VPP estará disponible para todos los dispositivos mac si **Permitir la instalación de aplicaciones en dispositivos M1 al momento de la distribución** está habilitado y el filtro de distribución está en **Todos** o **Personalizado**. Los filtros de distribución de atributos relacionados con macOS no son compatibles con las aplicaciones de iOS.

Configurar los filtros de distribución para el administrador delegado

El administrador delegado puede administrar y editar los filtros creados que se añadieron a las aplicaciones individuales durante el proceso de distribución en el espacio delegado. No obstante, el administrador delegado no puede usar los filtros de distribución creados en un espacio predeterminado en cualquier otro espacio, pero sí puede usarlos para las aplicaciones delegadas.

El administrador delegado puede crear, administrar y editar filtros de distribución en espacios específicos a los que tengan acceso. El filtro de distribución está disponible solamente en el espacio en el que se creó. Los filtros de distribución de las aplicaciones no se pueden delegar.

> Cuando un administrador delegado con una función de administración de aplicaciones y del sistema añade una aplicación utilizando un filtro de distribución en un espacio delegado, podrá ver los detalles de aquellos dispositivos que estén en su espacio y de los dispositivos de otros espacios.

Los usuarios con funciones de Administración del sistema o Solo lectura del sistema no podrán crear, actualizar ni eliminar filtros de distribución en ningún espacio.

Es posible que el administrador delegado con función de administrador de aplicaciones y contenido no tenga acceso al filtro de distribución. Por eso, no podrá:

- Crear aplicaciones utilizando filtros de distribución. Esto ocurrirá cuando usted haya iniciado sesión como administrador delegado y añada una aplicación.
- El administrador delegado con función de solo lectura del sistema o superior sí podrá añadir aplicaciones con un filtro de distribución. El administrador delegado sin una función de administración del sistema podrá añadir aplicaciones sin un filtro de distribución.

El administrador delegado puede filtrar el estado de delegación en el App Catalog seleccionando las siguientes opciones:

- Delegada
- No delegada

8.16. Excluir o distribuir aplicaciones

Excluir o distribuir aplicaciones gestionadas de un dispositivo sin cambiar la configuración de distribución de aplicaciones internas y públicas en dispositivos iOS, macOS y Windows. Para todas las aplicaciones gestionadas, estas opciones están presentes en la columna **Acciones** de la sección **Aplicaciones disponibles** para todos los dispositivos.

Permisos

Para excluir o distribuir una aplicación hacia o desde un dispositivo, es necesario disponer de las siguientes autorizaciones:

- Dispositivo de acceso en space (partición)
- Accede a las aplicaciones disponibles para el dispositivo.

Excluir

La opción de exclusión de una app seleccionada desinstala y elimina del dispositivo los datos asociados. Siga el flujo de trabajo para excluir una aplicación que sea un prerrequisito. Una confirmación emergente indica que está excluyendo una aplicación prerrequisito, lo que resulta en la exclusión de la aplicación principal del dispositivo.

Si excluye aplicaciones internas con múltiples versiones, excluye todas las versiones de aplicaciones no distribuidas del dispositivo. Si excluye una aplicación del dispositivo, se elimina de Apps@Work e Ivanti Go. Si excluye y elimina una aplicación del Catálogo de aplicaciones y la vuelve a añadir, la aplicación ya no permanecerá excluida para el dispositivo. Si excluye una aplicación gestionada del dispositivo, ésta deberá estar visible en la lista **Dispositivos** > **Dispositivos** > **Aplicaciones disponibles** para que el administrador pueda distribuir la aplicación después de excluirla.

Distribuir

Cuando el administrador activa el comando **Enviar instalación** desde la aplicación, ésta no se instalará hasta que el administrador decida distribuirla desde las **Aplicaciones disponibles** del dispositivo. Aparece un nuevo mensaje de exclusión para los dispositivos que no reciben la aplicación. Cuando el administrador distribuye una aplicación disponible, la siguiente sincronización instala la aplicación distribuida en el dispositivo.

8.17. Opiniones

Esta sección contiene los siguientes temas:

- Ver las puntuaciones y opiniones
- Desactivar las puntuaciones y opiniones
- Eliminar una opinión
- Exportación de reseñas a un archivo CSV

Las opiniones son los comentarios y las calificaciones (estrellas) que los usuarios proporcionan sobre las aplicaciones en el catálogo de aplicaciones. Las opiniones proporcionan información muy valiosa para usted y los usuarios que están considerando instalar una aplicación. Utilice la página **Opiniones** para ver o eliminar puntuaciones y opiniones. Puede borrar una opinión o puntuación si está obsoleta o es inadecuada.

- Solamente los usuarios de dispositivos pueden crear y editar opiniones y puntuaciones de las aplicaciones.
- Los usuarios de dispositivos pueden editar, pero no eliminar, sus propias puntuaciones y opiniones.
- Solamente los administradores pueden eliminar opiniones sobre las aplicaciones.
- Las puntuaciones sobre las aplicaciones no se pueden eliminar. Las puntuaciones (estrellas) que se dan a las aplicaciones se mantienen en la página **Aplicaciones > App Catalog**, aunque después usted desactive la característica de puntuaciones y opiniones para los usuarios.

Ver las puntuaciones y opiniones

- Vaya a **Aplicaciones > Opiniones** para leer los comentarios de las opiniones y las puntuaciones (estrellas) de los usuarios para las aplicaciones que ha distribuido.
- Vaya a **Aplicaciones > App Catalog** y consulte la columna **Puntuación media** para ver el número total de opiniones y la puntuación media.
- Vaya a **Aplicaciones > Catálogo de aplicaciones**, haga clic en **Nombre de la aplicación** y vea la pestaña **Opiniones** para ver las puntuaciones y opiniones de una aplicación específica.

Desactivar las puntuaciones y opiniones

1. Vaya a **Aplicaciones > Ajustes de catálogo**.
2. Desactive la opción **Habilitar puntuaciones y opiniones en el catálogo de aplicaciones del usuario final**.
3. Haga clic en **Guardar**.

Eliminar una opinión

1. Vaya a **Aplicaciones > Opiniones**.
2. Seleccione la opinión.
3. Haga clic en el botón **Acciones** que hay en la parte superior derecha de la página.
4. Seleccione **Eliminar**.
5. Haga clic en **Sí** en el diálogo de confirmación **Eliminar opinión**.

Si no puede realizar las tareas en la página **Revisiones**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración de aplicaciones y contenido

Exportación de reseñas a un archivo CSV

Puede exportar las reseñas de la aplicación mediante la opción **Exportar a CSV** de la página **Reseñas**.

Procedimiento

1. Vaya a **Aplicaciones > Opiniones**.
2. Haga clic en la opción **Exportar a CSV** para exportar la lista de revisión y detalles relacionados con un archivo CSV.
3. Aparecerá un mensaje con los botones **Continuar** y **Cancelar** que indicará si se ha iniciado el proceso de exportación y que en breve estará disponible un informe.
4. Haga clic en **Continuar** y espere a que se complete la solicitud para enviar otra.
5. Aparecerá un mensaje que indica que el informe **Revisiones de aplicaciones: CSV ha finalizado** con los botones **Descargar** y **Eliminar** .
6. Haga clic en **Descargar** para descargar el informe.
7. (Opcional) Haga clic en **Eliminar** para eliminar el informe.

8.18. Apps and Books de Apple

Esta sección contiene los siguientes temas:

- Distribución de licencias de aplicaciones en varias cuentas de Apps and Books de Apple en un espacio
- Distribución de licencias basadas dispositivos y basadas en usuarios
- Uso de la opción de licencia basada en el dispositivo
- Uso de la opción de licencia basada en el usuario
- Añadir una aplicación de Apps and Books al catálogo
- Añadir cuentas de Apps and Books
- Actualización de un token seguro para Apps and Books
- Actualización de la prioridad de una cuenta de Apps and Books
- Eliminación de un token seguro de Apps and Books
- Distribuir licencias para una aplicación de Apps and Books del catálogo
- Ver licencias de aplicaciones por usuario
- Notificaciones de uso de licencias de Apps and Books
- Visualización del uso de licencias de Apps and Books
- Revocación de la licencia de Apps and Books para una aplicación
- Comportamiento de Apps and Books para dispositivos macOS y iOS
- Derecho de licencia de Apps and Books cuando un dispositivo cambia de espacio

Licencia: Silver

La pantalla **Apps and Books de Apple** solo está disponible si ha configurado Apps and Books de Apple en sus ajustes del app catalog. Esta pantalla muestra las licencias de aplicaciones que se han comprado para dispositivos Apple a través de And Books de Apple y cuántas se han usado. Utilice esta pantalla para:

- seleccionar las aplicaciones de Apps and Books que se incluirán en su catálogo
- distribuir licencias para aplicaciones de Apps and Books

Para obtener más información sobre las aplicaciones de distribución con Apps and Books, consulte el artículo Ivanti Neurons for MDM: cómo distribuir aplicaciones con VPP de la Comunidad de Ivanti.

> Es posible que Books de Apple no esté disponible en todos los países o regiones. Para distribuir licencias para las aplicaciones mediante Apps and Books de Apple, debe introducir el sToken proporcionado por Apple.

Distribución de licencias de aplicaciones en varias cuentas de Apps and Books de Apple en un espacio

- Si existe una misma aplicación en más de una cuenta de Apps and Books, la licencia se distribuirá desde la cuenta en el orden de prioridad de las cuentas.
- Si existe una misma aplicación en más de una cuenta de Apps and Books y si la licencia de la aplicación de la cuenta de Apps and Books con mayor prioridad se ha agotado, a dicha aplicación se le distribuirá una licencia desde la cuenta con la siguiente

prioridad solo si el usuario o el dispositivo están presentes en la lista de distribución de licencias de la siguiente cuenta priorizada.

- La licencia no se revocará y reasignará al cambiar la prioridad de las cuentas de Apps and Books. A la aplicación se le distribuirá una licencia desde la primera cuenta. Si se han agotado las licencias en la primera cuenta, a la aplicación se le distribuirá una licencia desde la siguiente cuenta priorizada, y así sucesivamente.
- El usuario tiene la opción de revocar todas las licencias de una aplicación desde la página del App Catalog. Esta acción revocará la licencia de dicha aplicación desde todas las cuentas disponibles de Apps and Books.
- Las licencias reservadas tienen prioridad con respecto a las cuentas de Apps and Books.

Distribución de licencias basadas dispositivos y basadas en usuarios

La licencia de una aplicación estará basada en dispositivos o en usuarios dependiendo de cómo lo asigne usted. Cuando asigna la licencia de la aplicación a un dispositivo, se convierte en una licencia basada en dispositivo. Cuando asigna la licencia de la aplicación a un usuario, se convierte en una licencia basada en el usuario.

Cuando se instala una aplicación de Apps and Books en un dispositivo, se distribuye una licencia o se publica un token para esa aplicación. Si no hay ninguna licencia disponible para la aplicación, el usuario tiene la opción de instalar y pagar la aplicación él mismo. Si ya se ha asignado a un usuario a una licencia basada en el usuario para la aplicación solicitada de Apps and Books, se instalará la aplicación utilizando la licencia existente basada en el usuario, el lugar de la licencia de Apps and Books.

> En el caso de **Shared iPads**, Apps and Books se instalan según las licencias basadas en dispositivos, independientemente de si se seleccionan o no licencias basadas en dispositivos.

Uso de la opción de licencia basada en el dispositivo

Con las licencias basadas en dispositivos, los usuarios no están obligados a inscribirse en Apps and Books. Las aplicaciones obligatorias se instalarán automáticamente. Los dispositivos corporativos supervisados no necesitan usar una Id. de Apple propiedad del departamento informático.

Durante el ingreso del dispositivo, el dispositivo es identificado por su número de serie y se instala la aplicación obligatoria si hay licencias disponibles. Si no hubiera licencias disponibles, la aplicación no se instala. Si la licencia para una aplicación está reservada, la asignación de licencia basada en dispositivo no se producirá durante la instalación de la aplicación.

> Las actualizaciones de las aplicaciones implementadas utilizando licencias de Apps and Books basadas en el dispositivo están controladas por el administrador.

Para controlar cómo se va a actualizar una aplicación, en **Aplicaciones > App Catalog**, navegue hasta la pestaña **Configuraciones de aplicaciones/Instalar en dispositivo**. Ahí podrá seleccionar una actualización inmediata que se producirá la próxima vez que se ingrese el dispositivo o bien puede elegir que la aplicación se actualice automáticamente cuando haya disponibles nuevas versiones.

Importante:antes de asignar una licencia basada en dispositivo a una aplicación «business to business» (B2B) o de productividad, confirme con el desarrollador de la aplicación que esta sea apta para las licencias basadas en dispositivos.

Uso de la opción de licencia basada en el usuario

La licencia basada en el usuario seguirá siendo válida para dicho usuario si tiene que pasar de un dispositivo a otro en caso de que el dispositivo se haya perdido o haya sido robado o si el usuario cambia a un dispositivo nuevo. Con las licencias basadas usuarios, el usuario debe inscribirse primero en Apps and Books de Apple. La inscripción es una acción manual que el usuario final debe

completar en el Catálogo de aplicaciones. Las aplicaciones obligatorias de Apps and Books no se instalarán en el dispositivo hasta que el usuario se inscriba en Apps and Books.

Si la aplicación es una aplicación obligatoria de Apps and Books y la distribución de licencias está basada en el usuario:

- Las instalaciones de aplicaciones obligatorias no se producirán si el usuario no está inscrito en el programa Apps and Books.
- Se podrán instalar las aplicaciones obligatorias si el usuario está inscrito en el programa Apps and Books y si hay una licencia disponible.
- Si el usuario está inscrito en Apps and Books pero no hay ninguna licencia disponible, la aplicación no se instalará.

Añadir una aplicación de Apps and Books al catálogo

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Seleccione una aplicación y haga clic en **Añadir al catálogo**. Haga clic en **Siguiente**.
3. Opcionalmente, puede añadir una descripción de la aplicación. Haga clic en **Siguiente**.
4. Seleccione una opción de distribución. Haga clic en **Siguiente**.
5. Haga clic en la pestaña **Configuración de la aplicación**.
6. Opcionalmente, puede seleccionar **Instalar en dispositivo**. Esta opción de configuración instalará la aplicación sin solicitar nada al usuario en dispositivos iOS supervisados.
7. Seleccione otras opciones de configuración si fuera necesario.

En la página de detalles del token seguro de Apps and Books, se muestran los siguientes detalles:

- Fecha de creación
- Ubicación (si el token contiene esta información)
- Fecha de caducidad

Añadir cuentas de Apps and Books

Ivanti Neurons for MDM permite agregar varias cuentas de Apps and Books añadiendo varios tokens seguros de Apps and Books en un solo espacio.

Lleve a cabo los siguientes pasos para agregar un token seguro de Apps and Books en un espacio:

1. Vaya a **Aplicaciones > Apps and Books de Apple**.
2. Haga clic en **+Añadir sToken de Apps and Books**.
3. Introduzca un nombre y elija un archivo del token.
4. Opcionalmente, también puede deseleccionar la opción **Distribuir automáticamente aplicaciones de Apps and Books a todos los usuarios**. Esta opción está seleccionada de forma predeterminada, en cuyo caso se usa el grupo Todos los usuarios para distribuir las licencias en orden de llegada.
5. Opcionalmente, también puede seleccionar la opción **Borrar todos los datos de la licencia de Apps and Books anterior** para borrar todas las licencias de aplicaciones asociadas a este token.
6. Haga clic en **Guardar**.

Una vez que se haya añadido la cuenta, aparecerá en la tabla una lista de todas las cuentas de Apps and Books añadidas.

Actualización de un token seguro para Apps and Books

Procedimiento

1. Vaya a **Aplicaciones > Apps and Books de Apple**.
2. Haga clic en el nombre de la cuenta de Apps and Books.
3. En la pestaña del token, haga clic en **Actualizar sToken** (archivo .stoken).
4. Introduzca el nombre del token y elija un archivo del token.
5. Opcionalmente, también puede deseleccionar la opción **Distribuir automáticamente aplicaciones de Apps and Books a todos los usuarios**. Esta opción está seleccionada de forma predeterminada, en cuyo caso se usa el grupo Todos los usuarios para distribuir las licencias en orden de llegada.
6. Opcionalmente, también puede seleccionar la opción **Borrar todos los datos de la licencia de Apps and Books anterior** para borrar todas las licencias de aplicaciones asociadas a este token.
7. Haga clic en **Actualizar**.

Desde la pestaña del token, haga clic en **Volver a sincronizar la información de uso de la licencia de Apps and Books** para realizar una sincronización completa de toda la información sobre aplicaciones y licencias del servicio de Apps and Books de Apple. Esta acción solo es necesaria si la información sobre la asignación de la licencia de Ivanti Neurons for MDM no es correcta. Esta falta de precisión puede deberse a las incoherencias de las API de Apps and Books de Apple.

Actualización de la prioridad de una cuenta de Apps and Books

Los administradores pueden asignar una prioridad a cada cuenta de Apps and Books dentro de un espacio dependiendo de dónde se vayan a consumir las licencias. Las prioridades de las cuentas de Apps and Books se utilizan para tener un sistema predecible de distribución de licencias y para resolver conflictos cuando un usuario o dispositivo es apto para recibir una licencia de varias cuentas de Apps and Books para una misma aplicación.

Procedimiento

1. Vaya a **Aplicaciones > Apps and Books de Apple**.
2. Haga clic en **Editar prioridad** junto al nombre de cuenta de Apps and Books.
3. En la ventana Editar prioridad, seleccione una nueva prioridad.
4. Haga clic en **Guardar**.

Eliminación de un token seguro de Apps and Books

La eliminación de un token seguro de Apps and Books es irreversible e implica su destrucción. Cuando se borra un token:

- Se eliminarán los tokens de las aplicaciones que tengan sus tokens reservados.
- Las aplicaciones que se pagaron se mantendrán en el catálogo y los usuarios pueden pagarlas por sí mismos.
- Las aplicaciones que instalaron los usuarios finales a través de la cuenta de Apps and Books corporativa tendrán que transferirse a cuentas personales si los usuarios desean usarlas. Los usuarios tienen un período de gracia de 30 días para hacerlo.

Procedimiento

1. Vaya a **Aplicaciones > Apps and Books de Apple**.
2. Haga clic en el nombre de la cuenta de Apps and Books.
3. En la pestaña Token, haga clic en **Eliminar**.

4. En la ventana Eliminación del token seguro de Apps and Books, seleccione la opción **Sí, eliminar el token seguro de Apps and Books** para confirmar.
5. Haga clic en **Eliminar**.

Distribuir licencias para una aplicación de Apps and Books del catálogo

1. Seleccione **Aplicaciones > Apps and Books de Apple** en el menú principal.
2. Se muestra una lista de cuentas de Apps and Books. En cada cuenta, aparecerá una lista de aplicaciones compradas a través del programa Apps and Books.
   Seleccione una aplicación y haga clic en **Distribuir licencias**.
3. Elija una opción de distribución: **En orden de llegada**, **Reservada** o **No permitida** en la sección de licencias de Apps and Books.

Ver licencias de aplicaciones por usuario

Se pueden ver las preferencias de licencias para sus usuarios usando la pestaña Uso de licencias.

1. Haga clic en la pestaña **Usuarios**.
2. Seleccione un usuario.
3. Haga clic en la pestaña **Uso de licencias**.
   Aparecerá una lista de aplicaciones con su tipo de licencia de Apps and Books y los detalles asignación de la licencia.

Para ver el uso de la licencia de cada aplicación por usuario:

1. Vaya a **Usuarios** en el menú principal de Ivanti Neurons for MDM.
2. Seleccione un usuario.
3. Aparecerá la pestaña **Dispositivos** de forma predeterminada.
   Haga clic en la pestaña **Uso de licencias**.
   Se mostrará una lista de todas las aplicaciones instaladas en el dispositivo del usuario, incluyendo el estado de la licencia. El número de serie del dispositivo aparece en la columna Tipo de licencia de Apps and Books para las licencias basadas en dispositivos.
   - Nombre de la aplicación
   - Versión de la aplicación
   - Precio de la aplicación
   - Fecha en que se asignó la aplicación
   - Tipo de licencia de Apps and Books
   - Acciones (estado de la licencia)
   - Información de la plataforma para detalles de licencia.

También puede ver el uso de la licencia de Apps and Books de cada aplicación:

1. Vaya a **Aplicación > Catálogo de aplicaciones** en el menú principal de Ivanti Neurons for MDM.
2. Seleccione una aplicación.
3. Haga clic en la pestaña **Licencias de Apps and Books** si estuviera presente.
4. Haga clic en un nombre de cuenta. En esta pestaña solamente aparecerán las aplicaciones compradas a través del programa Apps and Books.

Se muestra una pestaña independiente para cada tipo de licencia de Apps and Books.

Tipo de licencia y registro	Descripción
En orden de llegada (FCFS, por sus siglas en inglés): tiene la posibilidad de seleccionar qué grupos de usuarios recibirán este tipo de licencia.	• Aplicaciones solicitadas por el usuario: son las aplicaciones que el usuario elige instalar. La licencia pasada en el usuario es la opción predeterminada. • Aplicaciones obligatorias: son las aplicaciones necesarias y se instalan mediante la configuración del administrador utilizando el ajuste **Instalar en dispositivo**. Estas aplicaciones utilizan licencias basadas en dispositivos de forma predeterminada.
Reservada	Las licencias reservadas tienen prioridad sobre las licencias en orden de llegada. Aquí se pueden seleccionar a los usuarios o dispositivos que tendrán una licencia reservada para la aplicación.
No permitida	Introduzca los usuarios que no están autorizados a tener una licencia para esta aplicación. Estos usuarios podrán instalar la aplicación de todos modos, pero deberán comprarla.
Registro de actividad	Muestra al usuario, el tipo de licencia de Apps and Books asignada a él, la fecha en que se asignó y la última acción llevada a cabo sobre la licencia.

Para ver el uso detallado de la licencia de cada aplicación por dispositivo:

1. Vaya a **Dispositivos** en el menú principal de Ivanti Neurons for MDM.
2. Seleccione un dispositivo.
3. Haga clic en la pestaña **Aplicaciones instaladas**.
4. Se mostrará una lista de todas las aplicaciones administradas instaladas en el dispositivo seleccionado, incluyendo el estado de la licencia.
    - Nombre de la aplicación
    - Versión de la aplicación
    - Plataformas compatibles
    - Origen de la aplicación
    - Tamaño de la aplicación
    - Tipo de licencia de Apps and Books
    - Fecha de notificación (instalación) de las aplicaciones de iOS

Busque las aplicaciones instaladas para el dispositivo de la siguiente manera:

- Nombre de la aplicación
- ID de conjunto o paquete

Notificaciones de uso de licencias de Apps and Books

Las notificaciones de Apps and Books le ayudan a realizar un seguimiento del uso de la licencia de Apps and Books. Los umbrales de las notificaciones se definen del siguiente modo:

- Se emite una notificación informativa cuando se han usado más del 50 % de las licencias.
- Se emite una notificación de advertencia cuando se han usado del 70 al 80 % de las licencias.
- Se emite una notificación crítica cuando se han usado del 90 al 100 % de las licencias.
- Las notificaciones se desactivan cuando el uso disminuye por debajo del 50 %.

Para ver la información sobre licencias de cada aplicación:

1. Haga clic en **Aplicaciones > Apps and Books de Apple**.
2. Se mostrará la información sobre licencias, que incluye:
    - Nombre de la aplicación.
    - Precio de la aplicación.
    - Número de licencias disponibles.
    - Número de licencias canjeadas.

Vaya a **Panel > Notificaciones** para ver los detalles de la notificación de una licencia.

3. Aparecerá la página de notificaciones.
   Haga clic en el título de la notificación para ver los detalles. Fíjese en Panel para ver las notificaciones disponibles.

Notificaciones de uso de licencias de Apps and Books

Activación	Gravedad	Tipo de notificación	Tipo de componente
50 % canjeadas	Información	Uso de licencias	Apps and Books
70 % canjeadas	Advertencia	Uso de licencias	Apps and Books
80 % canjeadas	Advertencia	Uso de licencias	Apps and Books
90 % canjeadas	Alerta	Uso de licencias	Apps and Books
100 % canjeadas	Alerta	Uso de licencias	Apps and Books

Visualización del uso de licencias de Apps and Books

Los detalles de uso de la licencia específicos de un usuario se mostrarán en la tabla de uso de la licencia en la columna de licencias.

1. Haga clic en una aplicación.
2. Haga clic en la pestaña **Uso de licencias**.
3. Introduzca un nombre de usuario en el campo de búsqueda.

Revocación de la licencia de Apps and Books para una aplicación

Las licencias de Apps and Books se revocan cuando:

- El dispositivo está inactivo (retirado o borrado).
- La aplicación Apps and Books se elimina.
- La licencia basada en dispositivos se revoca cuando se retira el dispositivo.

- El token de Apps and Books se elimina.

Para revocar una licencia de Apps and Books para una aplicación:

1. Seleccione la aplicación en **Aplicaciones > Catálogo de aplicaciones**.
2. Haga clic en la pestaña **Licencias de Apps and Books de Apple** si está presente.
3. Lleve a cabo una de las siguientes tareas:
    1. Haga clic en **Revocar todas las licencias** para revocar todas las licencias de todos los usuarios o dispositivos.
    2. Haga clic en la pestaña **Registro de actividad**. Utilice la columna **Acciones** para revocar licencias individuales usuario a usuario o dispositivo a dispositivo.

- En dispositivos iOS, Apple permite un período de gracia de 30 días para las aplicaciones de Apps and Books una vez que se haya revocado la licencia de Apps and Books. Por lo tanto, la aplicación «Apps and Books» sigue siendo instalable.
- En dispositivos macOS, una vez que la licencia de Apps and Books haya sido revocada, la aplicación seguirá en el dispositivo.

Para revocar una licencia de Apps and Books para un usuario:

1. Haga clic en una aplicación.
2. Haga clic en la pestaña **Uso de licencias**.
3. Haga clic en el vínculo **Revocar licencia** en el usuario cuyo acceso la licencia debe eliminarse.

> Las licencias de Apps and Books se revocan automáticamente si se elimina al usuario o si este elimina el perfil MDM del dispositivo.

Notificaciones de errores de autenticación de Apps and Books

Se pueden producir algunos errores de autenticación al utilizar el servicio de And Books de Apple. Estas notificaciones de errores de autenticación de Apps and Books son las siguientes:

Notificación de error	Acción
Token de Acción no válido	Cargar un sToken válido de Apps and Books
Token caducado	Genere un nuevo token en línea utilizando la cuenta de su empresa
El sToken ha sido revocado	Cargar un Apps and Books válido
Inicio de sesión obligatorio	Inicie sesión en el servicio de Apps and Books

Comportamiento de Apps and Books para dispositivos macOS y iOS

Apps and Books para iOS

Acción	Licencia basada en el dispositivo	Licencia basada en el usuario
Eliminar la aplicación Apps and Books de la distribución para el usuario	La aplicación está desinstalada en el dispositivo del usuario	La aplicación está desinstalada en el dispositivo del usuario
Anular la delegación de Apps and Books	La aplicación está desinstalada de todos los dispositivos en espacios no predeterminados	La aplicación está desinstalada de todos los dispositivos en espacios no predeterminados
Eliminar una aplicación de Apps and Books de un espacio predeterminado o personalizado	La aplicación está desinstalada de todos los dispositivos	La aplicación está desinstalada de todos los dispositivos

Apps and Books para macOS

Acción	Licencia basada en el dispositivo	Licencia basada en el usuario
Eliminar la aplicación Apps and Books de la distribución para el usuario	La aplicación no se desinstala en el dispositivo del usuario	N/A
Anular la delegación de Apps and Books	La aplicación no se desinstala de todos los dispositivos en espacios no predeterminados	N/A
Eliminar una aplicación de Apps and Books de un espacio predeterminado o personalizado	La aplicación no se desinstala de todos los dispositivos	N/A

Derecho de licencia de Apps and Books cuando un dispositivo cambia de espacio

Cuando se mueve un dispositivo a un espacio nuevo, se revoca la licencia de Apps and Books que se asigna al dispositivo o al propietario del dispositivo. A continuación, se asignará una nueva licencia de Apps and Books dependiendo de la disponibilidad en el nuevo espacio.

A continuación se describen las situaciones de derecho de licencia de Apps and Books:

Situación	Privilegio
Una licencia de Apps and Books se asigna a un dispositivo o propietario del dispositivo en el espacio de origen y hay disponible una licencia de Apps and Books para la misma aplicación en el espacio de destino.	Asigne una licencia del token de Apps and Books en el espacio de destino.
Una licencia de Apps and Books se asigna a un dispositivo o propietario del dispositivo en el espacio de origen y no hay disponible una licencia de Apps and Books para la misma aplicación en el espacio de destino.	Revoque la licencia del token de Apps and Books en el espacio de origen.
No se asigna ninguna licencia de Apps and Books a un dispositivo o propietario del dispositivo en el espacio de origen y hay disponible una licencia de Apps and Books para cualquier aplicación de Apps and Books instalada en el espacio de destino.	Asigne una licencia del token de Apps and Books en el espacio de destino.

Si no puede realizar las tareas en la página **Categorías de aplicaciones**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración de aplicaciones y contenido

8.19. Ajustes del catálogo

Esta sección contiene los siguientes temas:

- Cambiar los ajustes de administración de aplicaciones de Apple
- Ajuste de región predeterminada de la App Store
- Activar/desactivar las actualizaciones de aplicaciones iOS
- Activar/desactivar las puntuaciones y opiniones de las aplicaciones
- Cargar o actualizar un sToken de Apps and Books de iOS/macOS (licencia: Gold)
- Eliminar un sToken de Apps and Books de iOS/macOS de su servicio de Ivanti Neurons for MDM

En la página **Aplicaciones** > **Ajustes del catálogo**, configure las preferencias que quiera aplicar en todas las aplicaciones del catálogo de aplicaciones. Puede hacer lo siguiente:

- Incluir actualizaciones de aplicaciones durante el ingreso del dispositivo
- Impedir la copia de seguridad en iCloud e iTunes (solo en iOS)
- Establecer la región predeterminada de la app store (Apple y Microsoft)
- Eliminar aplicaciones de iOS cuando el dispositivo deja de estar inscrito
- Habilitar Ivanti Neurons for MDM "Calificaciones y opiniones"
- Cargar los tokens de iOS y macOS Apps and Books (requiere licencia de Gold)

Cambiar los ajustes de administración de aplicaciones de Apple

Todos estos ajustes se aplicarán a todas las aplicaciones a no ser que se haya creado una configuración de la administración de aplicaciones para aplicaciones individuales.

1. Seleccione o quite la marca de selección de una o más de las siguientes casillas:
    - **Actualizar aplicaciones durante el ingreso del dispositivo** (opción seleccionada de forma predeterminada)
    - **Impedir la copia de seguridad de iCloud e iTunes**
    - **Eliminar aplicaciones dadas de baja**

Haga clic en **Guardar**.

Notificaciones

1. Haga clic en la lista desplegable de **Generar una notificación del sistema cuando las nuevas versiones de la aplicación estén disponibles en la tienda de Apple y en la tienda de Google**, y seleccione una de las opciones siguientes:
    - **Una vez a la semana**
    - **Una vez al día**

Haga clic en la lista desplegable de **Generar notificaciones de usuario final para las nuevas actualizaciones de la aplicación disponibles en AppCatalog**, y seleccione una de las opciones:

- **Una vez a la semana**
- **Una vez al día**

Ajuste de región predeterminada de la App Store

En los ajustes del App Catalog, establezca la región predeterminada para las app stores de Apple y Microsoft.

1. En la sección Región predeterminada de App Store:
    - Seleccione la **Región de la App Store de Apple**.
    - Seleccione la **Región de la App Store de Microsoft**.
2. Seleccione o deseleccione la opción de utilizar la última región seleccionada de la App Store como región predeterminada para cada administrador. Si se selecciona esta opción, la región de la app store se establecerá como la región que cada administrador seleccionó por última vez y anulará las configuraciones anteriores. Si es la primera vez que un administrador utiliza esta función, las regiones predeterminadas de la app store se establecerán en los ajustes anteriores de este procedimiento.
3. Haga clic en **Guardar**.

Activar/desactivar las actualizaciones de aplicaciones iOS

1. Seleccione o quite la marca de la casilla **Actualizar las aplicaciones durante la conexión del dispositivo.**
    - Esta opción está seleccionada de forma predeterminada.
    - Cuando se quita la marca de selección, los ingresos de dispositivo (incluidos los ingresos forzados por parte del administrador) no incluirán las actualizaciones de las aplicaciones.
    - No obstante, el usuario puede actualizar manualmente la aplicación haciendo clic en la acción Forzar ingreso en el catálogo de aplicaciones del dispositivo.
    - Las instalaciones de nuevas aplicaciones y todas las demás configuraciones y ajustes se actualizarán durante el ingreso del dispositivo.

Haga clic en **Guardar**.

En el caso de una aplicación administrada, el administrador puede hacer clic en el botón **Actualizar** que está en la página de detalles de la aplicación para actualizar manualmente la aplicación a la última versión de la App Store.

En el dispositivo de un usuario, el usuario puede hacer clic en el botón **Forzar ingreso** que está en el menú del App Catalog para dejar que se produzcan el ingreso del dispositivo y las actualizaciones de la aplicación a la vez que otras configuraciones y actualizaciones.

Todos estos ajustes juntos permiten que los usuarios finales puedan elegir cuándo se actualizan sus aplicaciones:

- Espere hasta estar conectado a una red Wi-Fi para evitar el consumo de datos.
- Evite quedar bloqueado, en un momento poco oportuno, mientras la aplicación se está actualizando.

Activar/desactivar las puntuaciones y opiniones de las aplicaciones

Esto permitirá a los usuarios puntuar y opinar sobre las aplicaciones y a los otros usuarios leer dichas opiniones.

1. Seleccione o quite la marca de selección en **Habilitar puntuaciones y opiniones en el catálogo de aplicaciones del usuario final**.
2. Haga clic en **Guardar**.

> El formato del sToken de Apps and Books ha cambiado. En lugar de la cadena de caracteres de versiones anteriores, ahora es una cadena de caracteres almacenada en un archivo de texto con formato de archivo vpptoken. Cargue este archivo directamente en la consola de administración para procesarlo. La página de la cuenta de Apps and Books se ha actualizado para mostrar el nombre de la organización de Apps and Books y las fechas de vencimiento.

Cargar o actualizar un sToken de Apps and Books de iOS/macOS (licencia: Gold)

1. Seleccione **Añadir sToken de Apps and Books**.
2. Introduzca un nombre para el archivo sToken en el campo **Alias**.
3. Arrastre y suelte el archivo del sToken hasta el área especificada o haga clic en **Elegir archivo** para navegar hasta el archivo del sToken.
4. Haga clic en **Guardar** o, si está actualizando un archivo de sToken, haga clic en **Actualizar**.
5. Vaya a la página **Apps and Books de Apple** para visualizar las aplicaciones asociadas a este token.

> Si los tokens de Apps y libros se reservaron para usuarios individuales en una versión anterior de Ivanti Neurons for MDM, debe verificar que sigan reservados para esos usuarios y, en caso de ser necesario, reservarlos nuevamente.

Eliminar un sToken de Apps and Books de iOS/macOS de su servicio de Ivanti Neurons for MDM

Puede revocar una aplicación que el usuario ya no necesite y volver a reasignarla según sea necesario. Si la aplicación se implementó como aplicación administrada con MDM para iOS/macOS, tendrá la opción de desinstalar la aplicación y todos los datos inmediatamente.

1. Seleccione una aplicación para desinstalarla.
2. Haga clic en **Eliminar**.
   Aparecerá un diálogo de advertencia.
3. Opcionalmente, puede conceder al usuario un período de gracia de 30 días para:
   - Guardar sus datos.
   - Comprar una copia personal de la aplicación.
   - Transferir las aplicaciones que instaló con esta cuenta de Apps and Books a sus cuentas personales para seguir usándolas.

Si no puede realizar las tareas en la página **Ajustes de catálogo**, puede ser que no tenga los permisos necesarios. Necesita tener el siguiente **rol**:

- Administración de aplicaciones y contenido

8.20. Instalar dependencias de aplicaciones

Cuando carga un paquete de aplicaciones internas, Ivanti Neurons for MDM escanea la aplicación para identificar las dependencias. Si se encuentra alguna dependencia, las enumera en el tercer paso del asistente Añadir aplicación. Para cualquier dependencia de la aplicación, los administradores pueden optar por cargar un archivo de dependencia. No obstante, es posible que algunas aplicaciones no se instalen sin cargar el archivo de dependencias.

El administrador tiene la opción de ajustar la dependencia de la aplicación cuando instala una aplicación concreta. En tal caso, puede haber una o más aplicaciones etiquetadas con la aplicación principal. Cuando un usuario intenta instalar la aplicación principal, el usuario se notificará sobre las aplicaciones dependientes que se instalarán con la aplicación principal.

> Esta función es compatible con los dispositivos iOS, Android, Windows, y macOS.

Tenga en cuenta los siguientes puntos sobre las dependencias de la aplicación y los requisitos previos:

- El administrador puede configurar las aplicaciones dependientes que son requisitos previos para que se pueda instalar una aplicación en un dispositivo. Una aplicación de requisito previo puede ser una aplicación interna, pública, privada (Android) o una VPP.
- El recuento de aplicaciones de requisitos previos ahora se muestra en la columna Aplicaciones de requisitos previos en la página Catálogo de aplicaciones. Puede pasar el ratón sobre el número para ver la lista de aplicaciones de requisitos previos.
- Una aplicación que es requisito previo se descarga directamente una vez que la aplicación principal se activa para la instalación.
- Si se delega una aplicación principal, las aplicaciones asociadas que son requisitos previos se delegan automáticamente.
- No puede eliminar una aplicación que es requisito previo del catálogo de aplicaciones hasta que se elimine la relación de requisito previo.
- Varias versiones de una aplicación pueden tener diferentes aplicaciones que son requisitos previos.
- La página Seguimiento de auditoría registra si se añaden, eliminan o se delegan automáticamente los requisitos previos de las aplicaciones de iOS, Android y macOS.
- Si el administrador o el usuario fina instala una aplicación que tiene aplicaciones de requisito previo, éstas se instalan antes que la aplicación principal. Si se realiza un registro de dispositivo antes de que se instalen todas las aplicaciones de requisitos previos, todas las aplicaciones de requisitos previos se desinstalarán.

> Si bien una aplicación necesita un archivo de dependencia, Ivanti Neurons for MDM no requiere que usted cargue ningún archivo para implementar una aplicación.

> Para dispositivos Samsung, el administrador debe agregar aplicaciones de requisito previo a la lista de aplicaciones permitidas del modo kiosko. Las aplicaciones que son prerrequisito que estén agregadas a la lista de Aplicaciones permitidas no se agregan a la lista de aplicaciones de la Lista negra.

> Para dispositivos distintos a Samsung, si la aplicación principal se agrega a la lista de aplicaciones permitidas del modo kiosko, la aplicación de requisito previo se deberá ejecutar en segundo plano. Puede ver una aplicación de requisitos previos en modo Kiosko solo si el administrador ajusta esta aplicación en modo quiosco.

Dispositivos de Windows: si la aplicación Bridge es un requisito previo que no se distribuye, y la aplicación principal es un ejecutable que se distribuye en segundo plano. Cuando se elimina la dependencia, se desinstalará la aplicación Bridge, pero después de este paso, el archivo .exe falla. El administrador debe asegurarse de que la aplicación de Bridge no esté sin distribuir por defecto.

Dispositivos de Windows: cuando la aplicación principal no se distribuye en segundo plano y la aplicación principal tiene una aplicación de requisito previo sin distribución, se instala correctamente la aplicación de requisito previo. No obstante, si la aplicación principal no se instala correctamente, inmediatamente se desinstalará la aplicación de requisito previo. El reintento de la aplicación principal fallida se produce solo cuando el usuario desencadena una solicitud de instalación.

Añadir una aplicación interna

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Haga clic en **Añadir**.
3. Arrastre el archivo de la aplicación hasta el cuadro punteado o haga clic en **Elegir archivo** para seleccionarlo del sistema de archivos y haga clic en **Confirmar**.
4. Haga clic en **Siguiente** (abajo a la derecha). Ivanti Neurons for MDM examina la aplicación para encontrar archivos de dependencias y los enumera en la tabla **Dependencias de la aplicación**.
5. Revise la información de la aplicación y verifique que ha seleccionado la aplicación correcta.
6. Haga clic en el icono de Cargar, en la columna Acciones. Aparecerá la ventana **Cargar dependencia**.
7. Haga clic en **Elegir archivo** para examinar y encontrar una copia local del archivo y, a continuación, haga clic en **Cargar**.
8. Ivanti Neurons for MDM escanea los paquetes opcionales de la aplicación, si los hay, y los enumera en la tabla de paquetes opcionales. Si aparece en la lista, haga clic en el icono de Cargar, en la columna Acciones. Aparece la ventana de carga de paquetes opcionales.
9. Revise la información de la aplicación y verifique que ha seleccionado la aplicación correcta.
10. Haga clic en **Elegir archivo** para examinar y encontrar una copia local del archivo y, a continuación, haga clic en Cargar.
11. Haga clic en **Siguiente**.
12. (Opcional) Añada capturas de pantalla de la aplicación y haga clic en **Siguiente**.
13. Si la aplicación requiere otras aplicaciones de requisitos previos.
    1. Seleccione la opción **Sobre** desde el **Aplicaciones de requisitos previos** sección.
    2. Busque la solicitud de requisitos previos bajo la pestaña **Añadir aplicaciones**.
    3. Seleccione las aplicaciones.
    4. Haga clic en **Guardar**.
14. Defina la distribución de aplicaciones y haga clic en **Siguiente**.
15. Defina la sección de Configuración de la aplicación y haga clic en **Listo**. La próxima vez que los dispositivos se sincronicen con Ivanti Neurons for MDM, la aplicación se implementa en el dispositivo junto con los archivos de dependencia.

Puede añadir dependencias adicionales haciendo clic en el botón Añadir dependencias. Una vez cargadas, estas dependencias adicionales también aparecerán enumeradas en la tabla Dependencias de la aplicación. El administrador también puede agregar manualmente un paquete opcional solo con el tipo de contenido. Este tipo de paquete no depende de la versión.

Añadir una aplicación de requisito previo

Puede agregar una aplicación de requisito previo a una aplicación principal. Puede añadir diferentes requisitos previos para diferentes versiones de una aplicación principal. La página del catálogo de aplicaciones le brinda la opción de mantener la descripción, las secuencias de comandos, las capturas de pantalla, la distribución, los requisitos previos de la aplicación y las configuraciones de la aplicación igual que la versión de la aplicación existente o cambiar las aplicaciones requeridas asociadas. No puede eliminar una aplicación de requisito previo sin eliminar la asociación con la aplicación principal.

La página Seguimiento de Auditoría ahora muestra las aplicaciones de requisitos previos admitidas en campos específicos de la siguiente manera:

La sección Prerrequisitos de aplicaciones de las aplicaciones de iOS, Android, y macOS de la página Seguimiento de auditoría muestra los campos siguientes:

appVersionId

nombre

platformAppId

Se muestran las aplicaciones de requisitos previos que se delegan automáticamente o no se delegan y que contienen los siguientes campos:

dmPartitionDistributionType

dmPartitionDistributionReason

Procedimiento

1. Seleccione una aplicación del **Catálogo de aplicaciones**.
2. Haga clic en **Editar**.
3. Desplácese hacia abajo hasta **Delegación de aplicaciones** y seleccione la opción **Delegar esta aplicación a todos los espacios**.
4. Haga clic en **Guardar**.

> Si delega varias aplicaciones y elige eliminar la delegación de la aplicación principal, la aplicación de requisito previo no se eliminará de la delegación automáticamente.

8.21. Desplegar Divide Productivity con Android Enterprise

Dividir la productividad es una aplicación PIM que puede desplegar en los dispositivos de Android Enterprise.

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. En **Aplicaciones corporativas**, haga clic en **Divide Productivity**.
3. Introduzca categorías adicionales o una descripción.
4. Haga clic en **Siguiente**.
5. Acepte los permisos mostrados.
6. Haga clic en **Siguiente**.
7. Seleccione una opción de distribución.
8. Amplíe **Opciones avanzadas y configuración de aplicaciones**.
9. Siga las siguientes pautas para habilitar las opciones:
10. Seleccione una opción de promoción.

Ajuste	Qué hacer
Bloquea al usuario para que no pueda desinstalar la aplicación	Seleccione esta opción si desea impedir que el usuario final pueda desinstalar la aplicación cuando se ha instalado de forma silenciosa.
Dirección de correo	Utilice variables para definir la dirección de correo electrónico asociada a la aplicación.
Contraseña	Utilice una variable para definir la contraseña para la cuenta de correo electrónico. Si deja este campo en blanco, se solicitará al usuario la contraseña.
Host	Introduzca el nombre de host del servidor de correo que se va a usar. Introduzca el nombre de dominio totalmente cualificado del servidor de ActiveSync. Si está usando un Sentry independiente, introduzca en su lugar su nombre de dominio totalmente cualificado (FQDN). Ejemplo: miSentry.miempresa.com
Tipo de servidor	Seleccione el tipo de servidor de correo.
Nombre de usuario	Utilice variables para definir el nombre de usuario para la cuenta de correo electrónico.
SSL es obligatorio	Seleccione esta opción si desea una comunicación segura utilizando https hacia el servidor que especificó en el campo «Host».
Confiar en todos los certificados	Seleccione esta opción solamente si desea que la aplicación acepte automáticamente certificados que no sean de confianza. Normalmente, esta opción solo se selecciona si se trabaja en un entorno de prueba.
Firma predeterminada del correo electrónico	Introduzca la firma predeterminada para todos los correos electrónicos. El usuario final puede modificar esta opción en cualquier momento. Una vez que el usuario del dispositivo lo modifique, los cambios posteriores en este campo no tendrán ningún efecto.
Tamaño máximo de adjunto en correo	Introduzca el tamaño máximo permitido para archivos adjuntos.
Habilitar tarea	Seleccione esta opción para sincronizar tareas.
Alias del certificado de inicio de sesión	Introduzca el alias para el certificado de inicio de sesión.
Alias del certificado de firma SMIME	No es compatible actualmente.
Alias del certificado de cifrado SMIME	No es compatible actualmente.
Opciones avanzadas	
Instalar en dispositivo	Seleccione esta opción para solicitar al usuario que instale la aplicación.

Ajuste	Qué hacer
Instalar de forma silenciosa en dispositivos Samsung KNOX	Seleccione esta opción para instalar la aplicación automáticamente en dispositivos Samsung KNOX.
No mostrar la aplicación en el App Catalog del usuario final	Seleccione esta opción si no desea que la aplicación aparezca en el catálogo de aplicaciones del dispositivo.

11. Haga clic en **Hecho**.

8.22. Configurar la aplicación Provisioner

Esta sección contiene los siguientes temas:

- Requisitos de aprovisionamiento
- Habilitar la transferencia Android para que use el intercambio de datos NFC
- Aprovisionar un dispositivo propiedad de la empresa
- Registrar el dispositivo
- Verificar el estado del registro del dispositivo

Proveedor es una aplicación de Ivanti Neurons for MDM que se usa para aprovisionar los dispositivos de empresa para que se puedan registrar como dispositivos administrados del trabajo y ubicados en el modo Propietario del dispositivos.

Los dispositivos propiedad de la empresa solo tienen perfil corporativo y no tienen perfil profesional. El administrador puede establecer más de 20 bloqueos en el dispositivo, que pueden restringir funciones del dispositivo como la cámara, llamadas de teléfono, SMS, redes, etc.

La aplicación Proveedor es necesaria en el dispositivo que iniciará la configuración del dispositivo de destino de Android Enterprise con separador NFC. Para aprovisionar dispositivos propiedad de la empresa, instale la aplicación Provisioner en un dispositivo maestro y utilice la opción de intercambio de datos NFC (transmisión de datos en proximidad) para aprovisionar los dispositivos nuevos. La función de intercambio de datos está conectando los dos dispositivos. Los dispositivos se pueden aprovisionar para usarse en una de estas aplicaciones del cliente:

- Go para usar con Ivanti Neurons for MDM
- At Work UEM, una aplicación de cliente sin marca, para usar con Ivanti Neurons for MDM.

Requisitos de aprovisionamiento

Para aprovisionar un dispositivo con la versión corporativa de Android y que sea un dispositivo administrado en el trabajo:

- Los dispositivos compatibles con Android Enterprise nativo propiedad de la empresa se deben restablecer a sus valores de fábrica antes del aprovisionamiento.
- La configuración de Android Enterprise se debe definir y aplicar en el grupo de dispositivos de Android.
- Un dispositivo Android compatible con NFC designado para servir como dispositivo maestro o como plantilla, con la aplicación Provisioner instalada.
- Dispositivos compatibles con Android Enterprise que se van a aprovisionar.
- Aplicación Provisioner
  Descargue la aplicación Provisioner para Android de Google Play.

Habilitar la transferencia Android para que use el intercambio de datos NFC

Procedimiento

1. Vaya a los **Ajustes** del dispositivo.
2. Vaya a **Redes inalámbricas y redes** y haga clic en **Más**.
3. Seleccione la casilla **NFC**.
4. Haga clic en **Transferencia Android** y deslice el interruptor a **On (Activado)**.

Estos pasos pueden variar ligeramente para su dispositivo.

Aprovisionar un dispositivo propiedad de la empresa

Procedimiento

1. Instale la aplicación Provisioner en el dispositivo para usarla como dispositivo Android maestro.
2. Inicie Provisioner en el dispositivo maestro.
3. Seleccione una aplicación del menú desplegable.
4. Introduzca la información solicitada por la aplicación Provisioner. Algunos campos podrían autorrellenarse si existe un tipo de Wi-Fi compatible. Siga estas pautas:

Campo	Valor
Seleccione la aplicación que va a aprovisionar	Vaya a (seleccionar para usar con Ivanti Neurons for MDM) At Work UEM (aplicación de cliente sin marca; seleccionar para utilizar con Ivanti Neurons for MDM con marca).
SSID de la red Wi-Fi	Introduzca la SSID de la Wi-Fi que va a usar el dispositivo maestro.
Tipo de seguridad Wi-Fi	Introduzca el tipo de seguridad Wi-Fi
Contraseña Wi-Fi	Introduzca la contraseña para la Wi-Fi
Zona horaria	Introduzca la zona horaria local actual
Configuración regional	Introduzca la configuración regional

5. Haga clic en **Continuar**.
   Se mostrará la pantalla **Conectar los dispositivos** en el dispositivo maestro.
6. Con el dispositivo de destino encendido y mostrando la pantalla de Bienvenida de Android, presione la parte posterior del dispositivo maestro contra la parte posterior del dispositivo de destino para iniciar la transferencia NFC.
   Si la transferencia NFC se produce correctamente, el dispositivo de destino hará un sonido y, a continuación, comenzará a descargar la aplicación de cliente elegida. Si el dispositivo no está cifrado, comenzará el proceso de cifrado antes de continuar.
7. Siga aprovisionando dispositivos adicionales intercambiando datos en los dispositivos. El dispositivo de destino debe mostrar la pantalla de Bienvenida y el dispositivo maestro debe mostrar la pantalla **Intercambio de datos en dispositivos**.

Registrar el dispositivo

Una vez que el dispositivo propiedad de la empresa se ha aprovisionado mediante el intercambio de datos NFC, tendrá instalada la aplicación de cliente seleccionada. Inicie la aplicación de cliente y registre el dispositivo.

Verificar el estado del registro del dispositivo

Procedimiento

1. Vaya a **Dispositivos > Dispositivos**.
2. Haga clic en el vínculo del dispositivo para ver los detalles.

3. El estado del dispositivo aparece en el panel izquierdo.

8.23. Administración de aplicaciones de Windows

Los usuarios pueden (Importar, configurar, programar, distribuir, actualizar y eliminar) el ciclo de vida completo de la aplicaciones de Windows. Los procesos de distribución y actualización de aplicaciones son compatibles a través de la consola MDM. Para obtener más información sobre cómo administrar aplicaciones de Windows y otras aplicaciones, consulte **Configuración de aplicaciones**, **Datos sobre aplicaciones** y **Catálogo de aplicaciones**.

Tipos de aplicaciones compatibles

- In-house (Compruebe las opciones en **Agregar una aplicación interna** de la sección **Catálogo de aplicaciones**)
- MSB (Integración con Microsoft Store for Business)
- El almacenamiento público (a través de la integración nativa con Microsoft Store) de la región de Microsoft Store se puede ajustar en Aplicaciones > Ajustes del catálogo. Para obtener más información, consulte **Agregar una aplicación desde un almacén público** de la sección **Catálogo de aplicaciones**.

Extensiones de aplicaciones compatibles

- MSI
- MSIX
- APPX
- Agrupaciones de APPX
- EXE (a través de **Ivanti Bridge**)

Control de aplicaciones

La configuración de Control de aplicaciones controla la instalación de aplicaciones por dispositivo. Para obtener más información, consulte **Configuración del control de aplicaciones: controle qué aplicaciones pueden instalarse en cada dispositivo**.

Paquetes y dependencias

Las siguientes funciones están disponibles:

1. Las aplicaciones de Windows se puede establecer como requisitos previos para todos los tipos de aplicaciones. Para obtener información sobre cómo configurar los requisitos previos de las aplicaciones, consulte **Instalar dependencias de aplicaciones**.
2. Los grupos APPX y APPX Dependencias de aplicaciones y Otras dependencias de paquetes. En la página **Ver Detalles de la aplicación**, revise la sección **Dependencias de la aplicación y otros paquetes** .
3. Las aplicaciones de Win32 son compatibles con el código de producto correcto (MSI) y líneas de comandos y variables. **Aquí** se puede encontrar una lista de opciones de línea de comandos comunes.

Secuencias de comandos

Las secuencias de comandos son compatibles a través del cliente de Ivanti Bridge. Para obtener más información sobre cómo configurar las Secuencias de comandos, consulte el **Ivanti Bridge**

Después de instalar Ivanti Bridge en los dispositivos, las secuencias de comandos se pueden distribuir de la siguiente manera:

- En el nivel de dispositivo con las secuencias de comandos y las acciones a través de la Acción de Ivanti Bridge
- A través de la configuración de Ivanti Bridge (vaya a **Configuraciones** > **Bridge**)

La **casilla de verificación** Marcar versión existente en el dispositivo, disponible en la **pestaña** Scripts y archivos para aplicaciones MSI y EXE internas, y controla cómo se instala la aplicación en dispositivos Windows. Cuando se habilita esta opción, el dispositivo ejecuta un registro para verificar si la aplicación ya está instalada e identificar su versión. Ivanti Neurons for MDM instala o actualiza la aplicación solo si no está presente o si la versión instalada es anterior a la versión requerida. Si existe la misma versión o una más reciente, la instalación se omite. Esta opción requiere que la aplicación esté instalada en al menos un dispositivo antes de habilitarla.

Secuencias de comandos y archivos previos a la instalación o posteriores

Para archivos .exe y .MSI

Puede configurar las secuencias de comandos de instalación tras PowerShell, secuencias de comandos de registro y archivos ejecutables de Windows (.exe) y descargar otros tipos de archivos para aplicaciones de Windows en el nivel de Detalles de aplicaciones.

Cuando se agrega un nuevo script o archivo anterior o posterior a la instalación, aparece la pantalla de Ivanti Bridge. Puede adjuntar el script o el archivo, agregar el argumento del script, además de proporcionar una ubicación de destino para los archivos. El script de preinstalación se debe ejecutar de manera correcta en el dispositivo antes de enviar el comando de instalación de la aplicación al dispositivo. Los scripts de pre y postinstalación y los archivos se ejecutarán/instalarán en el mismo orden en que se cargaron en la consola. Si falla la descarga o la instalación del script de preinstalación, no se puede continuar con la instalación de la aplicación.

Si falla el script tras la instalación, puede ver los errores en la página de Detalles del dispositivo, en la sección Registros del dispositivo. Además, no puede revertir los scripts/archivos descargados y ejecutables instalados antes de la instalación, en caso de que fallen las acciones después de la instalación.

Puede reordenar los scripts y archivos de preinstalación o postinstalación utilizando la opción Priorizar scripts y archivos. Esta opción solo estará disponible si hay al menos dos o más scripts o archivos disponibles. Con esta opción, puede arrastrar y soltar los archivos o scripts dentro de sus respectivas secciones previas o posteriores, y no de una sección a otra.

Comportamiento de instalación y configuraciones

Las aplicaciones de Windows son compatibles con la siguientes funciones:

- Instalaciones silenciosas
- **Programación de aplicaciones Windows**
- Opciones de reinicio

Para obtener más información sobre las opciones de comportamientos de instalación, consulte **Configuración de aplicaciones**

> Las aplicaciones MSI y EXE (instaladas mediante Bridge) admiten instalaciones con sesiones MDM sin usuario.

Por ejemplo, en los siguientes casos:

- El dispositivo se reinició y aun no ha iniciado sesión ningún usuario
- El usuario que ha cerrado sesión de Windows
- El dispositivo se inscribió en modo Autopilot sin usuario (Implementación y aprovisionamiento automático)
- Las aplicaciones se instalan a nivel de dispositivo

Permite la instalación de aplicaciones de MSI de maneras más eficientes, por ejemplo, durante la inscripción en Autopilot o por la noche, cuando nadie está trabajando en el dispositivo Windows. Cuando se usa un reembalaje sencillo para EXE en MSI, se puede instalar, pero no se puede actualizar ni eliminar. El paquete MSI real tiene una conexión con CSP. Se instalarán otros tipos de aplicaciones después de que el usuario inicie sesión.

Tunnel for Windows (por VPN de aplicación)

Tunnel es una aplicación nativa y autónoma de Windows. Actualmente está disponible en Microsoft Store para distribución a dispositivos. Crea una configuración de VPN por aplicación. Es necesario desplegar Sentry. Para configurar la aplicación de Tunnel, vaya a **Configuraciones** > **+Agregar** > Buscar Tunnel (seleccione las Configuraciones que sean compatibles con los dispositivos Windows). Seleccione el perfil Sentry y configure los ajustes para comenzar a usar el protocolo de túnel en los datos de la aplicación mediante Sentry. Para establecer un servidor de Sentry, vaya a **Admin** > **Infraestructura** > **Sentry**.

Inventario de aplicaciones

El Inventario de aplicaciones y software instalado en la flota de dispositivos Windows se puede monitorizar en dos niveles:

- Para comprobar las aplicaciones instaladas en todos los dispositivos, vaya a **Dispositivos** > **Inventario de aplicaciones**
- Para comprobar el inventario a nivel de dispositivo, vaya a Dispositivos > seleccione un dispositivo > haga clic en Aplicaciones instaladas

Los administradores pueden establecer los intervalos de recopilación del inventario de aplicaciones de Windows. Vaya a Administrador > Windows > Intervalos del inventario de aplicaciones Los intervalos se usan cuando la política de privacidad se ha ajustado para que se obtengan todas las aplicaciones del dispositivo. Para configurar la Configuración de privacidad, vaya a Configuraciones > +Agregar > busque Privacidad > Seleccione Recopilar el inventario de todas las aplicaciones del dispositivo. Seleccione los tipos de aplicaciones que desee recopilar.

Catálogo de aplicaciones corporativas (Apps@Work)

Los clientes pueden activar un Catálogo corporativo en los dispositivos Windows mediante Apps@Work. Apps@Work está disponible y se despliega a través del Catálogo de aplicaciones de Neurons for UEM. Para obtener más información, consulte **Apps@Work (iOS, Android, Windows y macOS)**.

8.24. Ivanti Bridge

Esta sección contiene los siguientes temas:

- Tipos de archivo compatibles con Bridge
- Configuración de Bridge
- Registros de Bridge
- Último ingreso de Bridge
- Recuperación de un fallo en el servicio de Bridge

Ivanti Bridge unifica las operaciones móviles y de escritorio para Windows 10 mediante una única consola y un único canal de comunicaciones. Amplía las funciones de UEM para administrar PC permite a las organizaciones sacar partido de costes considerablemente reducidos y una mayor eficiencia a la vez que se garantiza una seguridad uniforme en todos los PC y dispositivos móviles. Usando Ivanti Bridge, las empresas pueden usar un único protocolo para los dispositivos de Windows 10 Desktop, del mismo modo que hacen con dispositivos móviles compatibles con Windows, para enviar información a las aplicaciones legadas del SO.

Ivanti Bridge permite que el departamento informático modernice las operaciones de Windows en UEM sin sacrificar las funciones críticas. El departamento informático puede aplicar políticas y secuencias de comandos que ya estén implementados sin que sea necesaria una imagen del sistema, unirse al dominio o múltiples canales de comunicación con el dispositivo.

Con Ivanti Bridge, ahora las empresas pueden:

- Tener un control total sobre los PC con UEM
- Administrar los PC de forma remota e inalámbrica
- Reducir la necesidad de digitalización de equipos de sobremesa
- Hacer uso de comandos basados en GPO con secuencias de comandos Powershell implementados por UEM
- Editar y administrar fácilmente el registro
- Despliegue fácilmente aplicaciones Win32 no envueltas en MSI y aplicaciones Win32 Store
- Obtener visibilidad del sistema de archivos

> Ivanti Bridge es compatible con dispositivos Windows 11+ y procesadores ARM. Ivanti Bridge no es compatible con dispositivos de escritorio de Windows 10 Home.

Tipos de archivo compatibles con Bridge

Ivanti Bridge incluye la compatibilidad para los siguientes tipos de archivos:

- PowerShell
  Las secuencias de comando de PowerShell que se insertan en los dispositivos con Bridge admiten estos argumentos.
  Las secuencias de comandos de PowerShell de 64 bits son compatibles con los dispositivos de sobremesa Windows 10 de 64 bits.

> El tiempo de espera de Bridge en el lado del servidor para el resultado esperado tras enviar una secuencia de comandos de PowerShell es de aproximadamente 20 minutos. El tiempo de espera se registra como un Fallo. No obstante, la secuencia de comandos del dispositivo sigue funcionando.

El tiempo de espera de Bridge en el lado del dispositivo para el proceso esperado de la ejecución de una secuencia de comandos de PowerShell es de aproximadamente 60 minutos. Tras 60 minutos, el proceso se cerrará, no se guardan los resultados de la secuencia de comandos y se envía un nuevo Fallo al servidor.

Los tiempos de espera del lado del servidor y del lado del dispositivo están registrados como Errores. Si transcurre el segundo tiempo de espera y la secuencia de comandos genera algún resultado, no se registrará ningún resultado en el servidor.

Registro

- Secuencias de comandos VB
- .EXE para implementación de aplicaciones Win32
- Las aplicaciones de Win32 Store utilizan la herramienta WinGet para instalar y desinstalar las aplicaciones.

Si el administrador necesita insertar archivos Win32 (.EXE) en un dispositivo (por ejemplo, como aplicación interna Windows, se utilizará la funcionalidad de Bridge automáticamente si estuviera disponible. Es obligatorio introducir un argumento para ejecutar de forma silenciosa al archivo (por ejemplo, /SILENT o /VERYSILENT).
Las aplicaciones .EXE se instalan a través de Bridge usando el modo de administrador de PowerShell. En los dispositivos Windows, para instalar usando las credenciales del usuario, seleccione la opción «Ejecutado como usuario».

Los administradores deben seleccionar la casilla de verificación **Instalador ejecutado como usuario** en **Instalador de aplicaciones: ajustes** para instalar las aplicaciones para un usuario. No marque la casilla si desea que las aplicaciones se instalen a nivel de sistema.

Mediante Ivanti Bridge, el dispositivo se puede aumentar en las siguientes áreas clave.

- **Registro:** leer, escribir y actualizar valores del registro.
- **Archivos:** verificar, leer y actualizar contenidos de un archivo.
- **Implementación de aplicaciones:** añadir la posibilidad de instalar aplicaciones basadas en .EXE al dispositivo de sobremesa. Estas aplicaciones se pueden encontrar en los servidores de Ivanti Neurons for MDM o en una red de entrega de contenido (CDN, por sus siglas en inglés) en la nube.

Configuración de Bridge

La configuración de Ivanti Bridge requiere que los administradores completen los pasos siguientes en el orden indicado:

1. Activación de las licencias de Bridge
2. Instalación de la aplicación Bridge
3. Cargar secuencias de comandos en los dispositivos para uso permanente o único en los dispositivos

Activación de las licencias de Bridge

Ivanti Bridge forma parte del paquete Gold legado y del paquete actual de Secure UEM.

Instalación de la aplicación Bridge

Después de desactivar las licencias de Ivanti Bridge, la aplicación móvil de Bridge se puede instalar de la siguiente manera:

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Haga clic en **+Añadir**.
3. Haga clic en **Ivanti Bridge** en la sección de Aplicaciones empresariales.
4. Añada los detalles, personalice y distribuya la aplicación móvil Bridge a los dispositivos necesarios según las licencias que haya obtenido.
   Si activó la opción **Instalación silenciosa en los dispositivos Windows**, la aplicación móvil Bridge se instalará en silencio y el servicio Bridge comenzará a ejecutarse en los dispositivos.

> La aplicación Bridge se añade al Catálogo de aplicaciones por defecto, y también se distribuye por defecto a todos los dispositivos.

> Tras importar la versión más reciente de Ivanti Bridge en el catálogo del arrendatario, el administrador podrá visualizar la versión actualizada y alineada de la aplicación.

Cargar secuencias de comandos en los dispositivos

Los administradores pueden cargar secuencias de comandos en los dispositivos para usarlos de forma permanente creando una nueva configuración de Bridge:

1. Vaya a **Configuración > +Agregar**.
2. Seleccione la **configuración de Ivanti Bridge for Windows Scripts and Actions**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. En la sección Configurar Ivanti Bridge, utilice una de las dos opciones siguientes para cargar scripts:
   - Seleccionar scripts de la Biblioteca de scripts: seleccione uno de los scripts disponibles de la lista.
   - O
     Cargar scripts: especifique la configuración como se describe en la tabla del paso 7.
     - Introduzca los ajustes de la categoría **Archivo del script** para especificar un script de instalación para ser forzado o ejecutado en los dispositivos.
     - (Opcional) Introduzca los ajustes de la categoría **Deshacer archivo del script** para especificar el script de desinstalación que se forzará o ejecutará en los dispositivos. Esto es útil cuando, por ejemplo, se retira un dispositivo o se borra una configuración.
     - (Opcional) Seleccione la opción **Configurar Outlook** para configurar Microsoft Outlook en un dispositivo mediante Bridge.

       > Solo es compatible con Outlook 2000 y 2013.

Haga clic en **Siguiente**.

7. Seleccione una distribución para esta configuración.
   Para estas acciones de los dispositivos se forzará el ingreso automáticamente.

Categoría	Ajuste	Qué hacer
	Nombre	Introduzca un nombre que identifique a esta configuración.
Archivo de secuencia de comandos **Todas las versiones (equipos de sobremesa Windows 10+)**	Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
	Archivo de secuencia de comandos	Seleccione una secuencia de comandos válida o archivo ejecutable (.ps1, .reg, .exe). • El archivo de secuencia de comandos o ejecutable especificado (.ps1, .reg, .exe) se ejecutará automáticamente. • Otros tipos de archivo solamente se copiarán el la carpeta de destino.
	Argumentos de secuencia de comandos	Especifique la lista de argumentos para el archivo de la secuencia de comandos. • En archivos Win32 (.exe), introduzca un argumento para ejecutar de forma silenciosa al archivo (por ejemplo, /SILENT o /VERYSILENT). Esto es obligatorio.
Deshacer archivo de secuencia de comandos **Todas las versiones (equipos de sobremesa Windows 10+)**	Carpeta de destino	Especifique la carpeta de destino para el archivo de la secuencia de comandos. • Si no se especifica la carpeta de destino, se utilizará el valor de la variable del entorno del sistema %TEMP% como carpeta de destino.
	Archivo de secuencia de comandos	Seleccione una secuencia de comandos válida o archivo ejecutable (.ps1, .reg, .exe). • El archivo de secuencia de comandos o ejecutable especificado (.ps1, .reg, .exe) se ejecutará automáticamente. • Otros tipos de archivo solamente se copiarán el la carpeta de destino.
	Argumentos de secuencia de comandos	Especifique la lista de argumentos para el archivo de la secuencia de comandos. • En archivos Win32 (.exe), introduzca un argumento para ejecutar de forma silenciosa al archivo (por ejemplo, /SILENT o /VERYSILENT). Esto es obligatorio.
	Carpeta de destino	Especifique la carpeta de destino para el archivo de la secuencia de comandos.

Categoría	Ajuste	Qué hacer
		• Si no se especifica la carpeta de destino, se utilizará el valor de la variable del entorno del sistema %TEMP% de forma predeterminada.

Cargar secuencias de comandos a los dispositivos para un uso puntual

Los administradores pueden cargar una secuencia de comandos en los dispositivos para utilizarlos una sola vez (ad hoc).

1. Vaya a **Dispositivos > Dispositivos**.
2. Haga clic en el enlace con el nombre del dispositivo para ir a la página de detalles del Dispositivo. Este es el dispositivo de sobremesa Windows 10 donde se insertará/ejecutará la secuencia de comandos de uso puntual.
3. Haga clic en el icono ⋮ y en **Script y Acciones a través de Ivanti Bridge**.
4. Introduzca nombre.
5. En la sección Archivo de la secuencia de comandos, especifique una secuencia de comandos para insertar/ejecutar en el dispositivo tal y como se describe en la tabla anterior.
6. Haga clic en **Aplicar**.
   La ejecución de la secuencia de comandos se pondrá en la cola y puede que tarde en completarse. Vaya a la pestaña Registros para comprobar y ver el estado (mensajes de salida y error). Para estas acciones de los dispositivos se forzará el ingreso automáticamente.

Registros de Bridge

Esta función le permite extraer informes de Ivanti Bridge para dispositivos individuales, para aplicaciones de resolución de problemas y de diagnóstico. Los registros se envían la próxima vez que el dispositivo ingrese. Puede esperar a la próxima sincronización programada o realizar un registro forzado del dispositivo para obtener los registros rápidamente.

Para extraer los registros desde un dispositivo:

1. Vaya a **Dispositivos > Dispositivos**.
2. Haga clic en el enlace con el nombre del dispositivo para ir a la página de detalles del Dispositivo. Este es el dispositivo de sobremesa Windows 10 donde se insertará/ejecutará la secuencia de comandos de uso puntual.
3. Haga clic en el icono ⋮ y en **Extraer el registro de Ivanti Bridge**. Se muestra la ventana **Extraer registro de Ivanti Bridge**.
4. Seleccione una de las siguientes opciones:
   Un solo registro: solicita a Ivanti Neurons for MDM que extraiga el registro de Bridge más reciente del dispositivo.
   Todos los registros: solicita a Ivanti Neurons for MDM extraer todos los registros (hasta 30 días) en el dispositivo.
5. Haga clic en **Extraer registro**. Una vez que el dispositivo lo haya enviado a Ivanti Neurons for MDM, puede ver el registro de Bridge en la pestaña Registros en la página Detalles del dispositivo.

> Solo los registros enviados mediante la opción **Todos los registros** pueden descargarse como un archivo ZIP únicamente.

Último ingreso de Bridge

La columna última conexión de Bridge lista la fecha y hora de la última conexión del dispositivo Bridge en la página de Dispositivos. Se puede agregar la columna a la página Dispositivos mediante la opción Personalizar columnas y no es visible por defecto.

Para que esta columna sea visible, seleccione **Dispositivos** > **Personalizar columnas** > seleccione **Contacto de Bridge**.

> Los datos exportados también tendrán los detalles de la última conexión de Bridge siempre que sea de aplicación.

Recuperación de un fallo en el servicio de Bridge

Bridge Service Failure Recovery se ha introducido en Bridge 2.1.14. Por defecto, esta versión se importa al Catálogo de aplicaciones de todos los usuarios. En raras ocasiones, el Servicio de Bridge puede fallar sin un motivo conocido. En esos casos, la compatibilidad está disponible para Bridge 2.1.14 y versiones posteriores.

9. Contenido

Utilice la página Contenido para distribuir contenido alojado por una fuente externa. El contenido puede incluir archivos que los usuarios pueden descargar, como presentaciones de ventas, imágenes, hojas de cálculo y documentos.

Esta sección contiene los siguientes temas:

- **Gestión de contenidos**
- **Categorías**

9.1. Gestión de contenidos

Esta sección contiene los siguientes temas:

- Distribución de contenido alojado
- Eliminar contenido

El contenido alojado admite la distribución de contenido descargable con URLs externas. La URL externa debe llevar a un archivo descargable PDF o EPUB o IBOOK únicamente y la URL externa debe tener estas extensiones.

No se admite la distribución de licencias VPP Book, por lo que la distribución de Apple Books basada enID de iTunes Store.

Use la aplicación Books o Pages en el dispositivo para acceder al contenido enviado desde Ivanti Neurons for MDM. Puede acceder a ellos en la sección Biblioteca.

El contenido de **iBook y EPUB** puede distribuirse a los iPad iOS 8+ (licencia Gold). Estos formatos están restringidos a iPad porque Apple solo admite la distribución interna de estos formatos a iPad. Esta restricción no procede en dispositivos iOS 9.

> Las vistas previas del contenido no están disponibles para estos formatos.

Para el contenido en **PDF**, existe la opción de insertar el documento en la aplicación de iBook en los dispositivos iOS 8+.

Distribución de contenido alojado

Aunque no se pueden subir nuevos documentos a Ivanti Neurons for MDM, sí puede proporcionar una ruta (URL) donde se aloje el contenido y distribuirlo a los grupos de dispositivos.

Procedimiento

1. Vaya a **Contenido > Contenido alojado**.
2. Haga clic en **+ Añadir**.
3. Introduzca la siguiente información:
    - Título
    - Autor
    - Categoría
    - (Opcional) Descripción
4. En el campo **Ruta del contenido alojado** , introduzca una URL para el archivo que desea cargar.
5. Haga clic en **Siguiente**.
6. Realice los cambios necesarios en la distribución.
7. Haga clic en **Hecho**.

Para modificar el contenido alojado, es necesario eliminar el contenido anterior y añadir y distribuir el nuevo contenido alojado.

Para modificar otros ajustes que no sean la URL:

1. Vaya a **Contenido > Contenido alojado**.
2. Haga clic en el vínculo al documento que aparece en la columna **Nombre**.
3. Haga clic en el icono Editar.

4. Realice los cambios necesarios.
5. Haga clic en **Siguiente**.
6. Realice los cambios necesarios en la distribución.
7. Haga clic en **Hecho**.

Eliminar contenido

1. Haga clic en el vínculo al documento que aparece en la columna **Nombre**.
2. Seleccione **Acciones > Eliminar este documento**.
3. Haga clic en la casilla para confirmarlo.
4. Haga clic en **Eliminar documento**.

Al eliminar un documento:

- Se elimina del sistema.
- Deja de estar disponible en el catálogo de contenido.
- Se elimina de los dispositivos donde se ha descargado.

Si no puede realizar las tareas en la página **Contenido**, puede ser que no tenga los permisos necesarios. Necesita tener el siguiente **rol**:

- Administración de aplicaciones y contenido

9.2. Categorías

Esta sección contiene los siguientes temas:

- Añadir una categoría
- Quitar una categoría

> Como parte del fin de la asistencia técnica del contenido anunciado el 15 de abril de 2017, se ha desactivado la posibilidad de añadir nuevo contenido. El contenido cargado actualmente puede seguir distribuyéndose a través de la aplicación iBooks de Apple y es posible utilizarlo.

Las categorías describen los tipos de contenido del {{catálogo de contenido}}. Las categorías ayudan a organizar el contenido de forma que los usuarios puedan encontrar fácilmente lo que necesitan. Cada elemento añadido en el catálogo de contenido debe tener al menos una categoría asignada.

Añadir una categoría

Procedimiento

1. Haga clic en **Añadir** (abajo a la izquierda).
2. Escriba el nombre de la categoría. Las categorías no distinguen entre mayúsculas y minúsculas.
3. Haga clic en **Guardar**.

Quitar una categoría

Puede hacer clic en la X situada junto a la categoría para eliminarla.

Si no puede realizar las tareas en la página **Contenido (Contenido)**, puede ser que no tenga los permisos necesarios. Necesita tener el siguiente rol:

- Administración de aplicaciones y contenido

10. Configuraciones

Las configuraciones son conjuntos de ajustes que se envían a los dispositivos. Por ejemplo, se pueden utilizar configuraciones para establecer los ajustes VPN y los requisitos del código de acceso en los dispositivos. Las configuraciones existentes en su sistema aparecerán en la página Configuraciones.

Esta sección contiene los siguientes temas:

- Trabajar con configuraciones
- Creación de una configuración del portal de autoservicio para usuarios
- Configuración personalizada
- Insertar SyncML en dispositivos mediante la configuración personalizada
- Configuración del diseño de la pantalla de inicio
- Configuración del control de aplicaciones: controle qué aplicaciones pueden instalarse en cada dispositivo
- Configuración de las notificaciones de la aplicación
- Exportar configuraciones
- Priorizar configuraciones
- Administrar configuraciones

10.1. Trabajar con configuraciones

Esta sección contiene los siguientes temas:

- Filtrar el modo en que se muestran las configuraciones
- Añadir una configuración
- Distribución de la configuración
- Distribución de despliegue lento de configuraciones
- Enviar configuraciones a varios dispositivo
- Excluir configuraciones
- Enviar una configuración excluida
- Exportar configuraciones
- Importar configuraciones
- Editar una configuración
- Eliminar configuraciones
- Programar las actualizaciones de las aplicaciones internas
- Configuraciones de Windows que requieren una sesión de usuario activo

Las configuraciones son conjuntos de ajustes que usted, como administrador, envía a los dispositivos. Por ejemplo, se pueden utilizar configuraciones para establecer los ajustes VPN y los requisitos del código de acceso en los dispositivos. Las configuraciones existentes en su sistema aparecerán en la página Configuraciones. Puede seleccionar varias configuraciones desde la página de Configuraciones y empujarlas a varios dispositivos a la vez. Estas configuraciones se pueden enviar a los spaces de dispositivos específicos y los dispositivos de otros spaces no se verán afectados. Las configuraciones se pueden enviar a un único espacio, a varios espacios o a todos los espacios a la vez.

Hay muchos **tipos de configuraciones** disponibles. Se pueden dividir a las siguientes categorías básicas:

- seguridad
- recursos del usuario
- acceso a la red de la empresa
- red móvil
- otras (más configuraciones)

Puede llevar a cabo las siguientes acciones en la mayoría de las configuraciones:

- añadir
- editar
- duplicar
- eliminar
- excluir una o más configuraciones de un dispositivo específico
- insertar una o más configuraciones en un dispositivo específico

Algunas configuraciones tienen acciones restringidas:

- Algunas configuraciones no se pueden añadir ni duplicar. El Bloqueo de activación de iOS es un ejemplo de este tipo de configuración. Por lo tanto, estas configuraciones no estarán entre los mosaicos que aparecen al añadir una configuración. Estas configuraciones aparecerán solo en la página Configuraciones.
- Las configuraciones definidas por el sistema no pueden ser editadas ni borradas. SCEP para inscripción en iOS es un ejemplo de este tipo de configuración.
- Algunas configuraciones se pueden marcar para que no se puedan eliminar o reinstalar en un dispositivo. Estas configuraciones no se pueden excluir ni insertar en el dispositivo.

Filtrar el modo en que se muestran las configuraciones

Al mostrar la página **Configuraciones**, aparecen enumeradas todas las configuraciones. Para limitar esta lista a ciertas configuraciones, utilice el filtro (panel izquierdo) en SO y Tipo de configuración. Por ejemplo, para limitar la lista y que aparezcan solo las configuraciones de macOS, seleccione **macOS** en la sección **SO**.

Se puede ver la configuración en todos o en varios dispositivos espaciales seleccionando varios espacios de la lista desplegable. Cuando arrastra el cursor sobre las configuraciones que se muestran, aparece una ventana emergente con una lista de los espacios. Puede hacer clic en un espacio para mostrar la página de detalles de la configuración.

Aplicar el filtro **compatible** de **Apple DDM** para identificar con facilidad las configuraciones relacionadas con DDM y mejorar la diferenciación entre tipos de configuración.

Para buscar una configuración existente por su nombre, introduzca el nombre de la configuración en el campo **Buscar**.

Desde la publicación de la versión 81 de Ivanti Neurons for MDM, los administradores globales pueden delegar en los administradores de espacio la edición del Certificado de identidad generado dinámicamente para todos los dispositivos y para la opción de distribución personalizada.

Añadir una configuración

Esta opción solo se habilita si se selecciona un espacio único en la lista desplegable.

> Puede distribuir hasta un máximo de 100 archivos de configuración a la vez.

Procedimiento

1. Haga clic en **Añadir**.
2. Seleccione el tipo de configuración que desea crear.
3. Haga clic en **Siguiente**.
4. Si no desea que esta configuración quede inmediatamente habilitada, deseleccione la opción **Habilitar esta configuración**.
5. Seleccione un nivel de distribución para la configuración:
    - **Todos los dispositivos**: distribuir la configuración a todos los dispositivos disponibles. Para delegar configuraciones entre espacios, seleccione una de las siguientes opciones:
        - **No aplicar a los otros espacios**.
        - Para delegar configuraciones en los espacios, seleccione **Resumen de distribución**> **Aplicar a todos los dispositivos en los espacios de otros dispositivos**.
            - Seleccione la casilla de verificación **Permitir que el administrador del espacio edite la distribución** para permitir que los administradores del espacio delegados editen la distribución para el espacio específico.

- **Sin dispositivos** : seleccione esta configuración para la distribución en un momento posterior.
- **Predeterminada** : se definen conjuntos específicos de grupos de dispositivos a los que se enviará esta configuración. Para delegar configuraciones entre espacios, seleccione una de las siguientes opciones:
  - **No aplicar a los otros espacios**.
  - **Resumen de la distribución** > **Aplicar a los dispositivos de otros espacios**.
    - Seleccione la casilla de verificación **Permitir que el administrador del espacio edite la distribución** para permitir que los administradores delegados del espacio editen la distribución para el espacio específico.

> El administrador puede utilizar la opción de distribución Personalizada para distribuir la configuración Personalizada a Dispositivos, Grupos de dispositivos, Usuarios y Grupos de usuarios. La asignación o distribución de configuraciones a Usuarios o Grupos de Usuarios no está disponible para las siguientes configuraciones:

  - Android Enterprise: perfil de trabajo (Android for Work)
  - Android Enterprise: dispositivo administrado en el trabajo (Android for Work)
  - Android Enterprise: dispositivo administrado con perfil de trabajo/perfil de trabajo en dispositivo de la empresa
  - Dispositivos Android gestionados para el trabajo (propietario del dispositivo) para dispositivos con modo no GMS para el dispositivo administrado en el trabajo (AOSP)

6. Si su servicio tiene espacios definidos, especifique si la configuración debe aplicarse a los demás espacios y la prioridad.
7. Haga clic en **Hecho**.

> Para configuraciones que ejecutan un comando para el dispositivo en lugar de instalar un perfil en el dispositivo, los detalles de configuración no mostrarán la configuración como aplicada a ningún dispositivo.

Distribución de la configuración

Los administradores globales pueden delegar en los administradores de espacio la edición del Certificado de identidad generado dinámicamente para todos los dispositivos y para la opción de distribución personalizada. Para los certificados generados dinámicamente, puede seleccionar opcionalmente la opción **Permitir que esta configuración esté disponible en todos los** espacios. Esta opción hace que los certificados de identidad generados dinámicamente estén disponibles en todos los espacios y puedan utilizarse en Exchange, Wi-Fi, VPN y cualquier otra configuración aplicable, incluidas las configuraciones de aplicaciones gestionadas. Esta opción se puede usar en situaciones en las que solo es necesario distribuir el Certificado de identidad dinámicamente generado a los dispositivos (en espacios no predeterminados) como parte de configuraciones asociadas y no como configuración individual.

Procedimiento

1. Especifique los campos de configuración utilizando la información especificada en la tabla para la configuración individual según corresponda.
2. Haga clic en **Siguiente**.
3. Seleccione la opción **Habilitar esta configuración**.
4. (Opcional) **Permitir que esta configuración esté disponible en todos los espacios**.
5. Seleccione una de las siguientes opciones de distribución:
   - **Todos los dispositivos**. Seleccione una de las siguientes opciones:
     - **No aplicar a los otros espacios**.

        - **Aplicar a todos los dispositivos de otros espacios**.
        - **Aplicar a todos los dispositivos de otros espacios de dispositivos como prioridad más alta**. (Esto solo es puede aplicar a la configuración Wi-Fi).
        - **Aplicar a todos los dispositivos de otros espacios de dispositivos como prioridad más baja**. (Esto solo es puede aplicar a la configuración Wi-Fi).
            - Seleccione la casilla de verificación **Permitir que el administrador del espacio edite la distribución** para permitir que los administradores delegados del espacio editen la distribución para el espacio específico.
    - **Ningún dispositivo** (predeterminada)
    - **Personalizar**Seleccione una de las siguientes opciones:
        - **No aplicar a los otros espacios**.
        - **Aplicar a todos los dispositivos de otros espacios**.
        - **Aplicar a todos los dispositivos de otros espacios de dispositivos como prioridad más alta**. (Esto solo es puede aplicar a la configuración Wi-Fi).
        - **Aplicar a todos los dispositivos de otros espacios de dispositivos como prioridad más baja**. (Esto solo es puede aplicar a la configuración Wi-Fi).
            - Seleccione la casilla de verificación **Permitir que el administrador del espacio edite la distribución** para permitir que los administradores delegados del espacio editen la distribución para el espacio específico.

> Independientemente de los espacios, el certificado de identidad generado dinámicamente puede configurarse en todos los espacios, distribuirse a todos los dispositivos y aplicarse a todos los dispositivos en otros espacios de dispositivos.

6. Haga clic en **Hecho**.

Distribución de despliegue lento de configuraciones

Al distribuir configuraciones mediante la **opción** Personalizado, puede distribuir las configuraciones mediante el proceso de Despliegue lento para que las configuraciones se desplieguen en un cronograma oportuno. Puede programar la distribución de despliegue lento de forma manual o programada.

> ¿Actualmente la distribución de despliegue lento solo es compatible con VPN?y configuraciones Wi-Fi.

Procedimiento

1. Vaya a **Configuraciones** > **Añadir**.
2. Busque la configuración requerida.
3. Introduzca los detalles como **Nombre**, **Descripción**, etc. dependiendo de la configuración y haga clic en **Siguiente**.
4. Seleccione **Personalizado** para la opción de distribución. La **sección Distribución de despliegue** lento aparece en la pantalla.
5. Seleccione **Usar método de distribución de despliegue lento**. Las **opciones Despliegue** manual **y Despliegue** programado aparecen en la pantalla.
    - **Despliegue manual** : con esta opción, puede establecer manualmente el porcentaje del objetivo de distribución. Solo se realizará el porcentaje de distribución especificado. También puede seleccionar **Todos los dispositivos en el resumen de selección** para distribuir la configuración a todos los dispositivos.

- **Despliegue programado** : utilice esta opción para desplegar la distribución en cuatro etapas. Para cada etapa, puede especificar el porcentaje de despliegue, asegurándose de que cada etapa posterior tenga un porcentaje mayor que la anterior. La duración entre etapas debe ser de al menos un día y no puede superar los 30 días. La configuración guardada más recientemente se carga automáticamente como plantilla editable para configuraciones futuras.

6. Seleccione los grupos deseados a los que se debe distribuir la configuración.
7. Haga clic en **Hecho**.

Puede ver los detalles en **Configuraciones** > Configuración recién creada > **Detalles**. Desde la página Detalles, puede Pausar y reanudar el despliegue.

> Cuando crea una nueva configuración con despliegue programado, los porcentajes que ha proporcionado al crear la configuración existente se trasladan a la nueva. Puede editar los detalles o continuar con los mismos porcentajes.

Enviar configuraciones a un dispositivo

Si desea reinstalar cualquiera de las configuraciones excluidas en un dispositivo, puede insertar las configuraciones.

Procedimiento

1. Vaya a **Dispositivos** >**Dispositivos**.
2. Haga clic en el nombre del dispositivo para visualizar la página de detalles.
3. Vaya a **Configuraciones**.
4. Seleccione las casillas de verificación para seleccionar las configuraciones específicas que se enviarán al dispositivo.
5. Haga clic en **Insertar perfiles**.
6. Para insertar una sola configuración, haga clic en **Empujar** en la columna **Acciones**.

Enviar configuraciones a varios dispositivo

Puede seleccionar varias configuraciones desde la página de Configuraciones y empujarlas a varios dispositivos a la vez.

Procedimiento

1. Inicie sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Vaya a **Configuraciones**.
3. Marque las casillas para seleccionar las configuraciones específicas.
4. Haga clic en **Acciones**, seleccione **Empujar las configuraciones seleccionadas** a los dispositivos. Se abre el asistente de inserción de configuraciones y se muestran todas las configuraciones y sus estados de inserción.
5. Haga clic en **Empujar configuración(es) válida(s)**. Las configuraciones se transfieren a todos los dispositivos de forma masiva. Las configuraciones excluidas para dispositivos específicos en la pestaña **Dispositivos** > **Configuraciones** no se transfieren.

Excluir configuraciones

Algunas configuraciones previamente distribuidas se pueden eliminar manualmente de un dispositivo excluyéndolas.

Procedimiento

1. Vaya a **Dispositivos** >**Dispositivos**.
2. Haga clic en el nombre del dispositivo para visualizar la página de detalles.

3. Vaya a **Configuraciones**.
4. Marque las casillas para seleccionar las configuraciones específicas.
5. Haga clic en **Excluir perfiles**.

> Para excluir una sola configuración, haga clic en **Excluir** bajo la columna **Acciones**. Las configuraciones seleccionadas aparecen ahora en la pestaña Configuraciones excluidas.

Enviar una configuración excluida

Procedimiento

1. Vaya a **Dispositivos** >**Dispositivos**.
2. Haga clic en el nombre del dispositivo para visualizar la página de detalles.
3. Vaya a **Configuraciones** > **excluidas**.
4. Seleccione una o más configuraciones para insertarlas en el dispositivo.
5. Haga clic en **Insertar perfiles**.
6. Para insertar una sola configuración, haga clic en **Empujar** en la columna **Acciones**.

Exportar configuraciones

Puede exportar los detalles de las configuraciones seleccionadas o todas las configuraciones de los espacios seleccionados a archivos individuales.

Procedimiento

1. Vaya a **Configuraciones**.
2. Marque las casillas para seleccionar las configuraciones específicas.
3. Haga clic en **Acciones** > **Exportar todas las configuraciones seleccionadas con detalles**. Si desea exportar todas las configuraciones, seleccione **Exportar todas las configuraciones con detalles**.
   Se incluye un conjunto de archivos YAML en un archivo .ZIP. El informe incluye detalles de todas las configuraciones existentes en los espacios seleccionados.

Exportar todas las configuraciones

Exporte sus archivos de configuración para enviarlos al soporte técnico y que puedan utilizarlos como herramienta de ayuda para el diagnóstico. Puede exportar un único archivo de configuración como archivo de formato Yaml o exportar todas sus configuraciones a un archivo .zip. Puede exportar archivos de distintos puntos de la página Configuración, dependiendo de qué configuraciones desee exportar.

Procedimiento

1. Vaya a **Configuraciones**.
2. Marque las casillas para seleccionar las configuraciones específicas.
3. Haga clic en **Acciones** > **Exportar todas las configuraciones seleccionadas con detalles**. Si desea exportar todas las configuraciones, seleccione **Exportar todas las configuraciones con detalles**.
   Se incluye un conjunto de archivos YAML en un archivo .ZIP. El informe incluye detalles de todas las configuraciones existentes en los espacios seleccionados.

Exportar una configuración personalizada

Procedimiento

1. Vaya a **Configuraciones**.
2. Haga clic en **+Añadir** para seleccionar una configuración.
3. Siga los pasos para personalizar la configuración.
4. Haga clic en **Siguiente**.
5. Elija un nivel de distribución.
6. Haga clic en **Hecho**.
7. Seleccione la configuración que acaba de crear de la lista de la página **Configuración**.
8. Haga clic en el menú desplegable **Acciones** y en **Exportar.**

Se descargará un archivo con el nombre de la configuración y uno con marca de hora _aaaammdd.yaml en su dispositivo.

Exportar una configuración existente

Procedimiento

1. Vaya a **Configuraciones**.
2. Seleccione una configuración existente.
3. Haga clic en el menú desplegable **Acciones** y, a continuación, en **Exportar**.
   Se descargará un archivo con el nombre de la configuración y uno con marca de hora _yyyymmdd.yaml en su dispositivo.

Importar configuraciones

Puede importar un archivo YAML que contiene los detalles de configuración. Para editar una configuración, puede editar los detalles del archivo YAML, seleccione una configuración e importe el archivo y aparecerán los valores de actualización de la configuración. Si se selecciona más de una configuración o espacio, se deshabilita el botón Importar. Si se selecciona un tipo de archivo incorrecto, aparece un mensaje de error. Si selecciona un archivo YAML que contiene información distinta a la requerida para una configuración, aparecerá un mensaje de error.

Procedimiento

1. Vaya a **Configuraciones**.
2. Seleccione una configuración, haga clic en **Importar**, en **Seleccionar archivo**, seleccione el archivo YAML y haga clic en **Importar**. Se importa el archivo YAML con los detalles de configuración.

Configuraciones admitidas

- CERTIFICATE
- VPN
- WEBCLIP
- IDENTITY_CERTIFICATE_DG
- RESTRICTIONS
- ANDROID_WORK_DEVICE_OWNER_LOCKDOWN

- PASSCODE
- HOME_SCREEN_LAYOUT
- ANDROID_ADVANCED_PASSCODE_AND_LOCK_SCREEN
- IOS_APP_CONTROL
- SCEP
- ANDROID_SAMSUNG_SAFE_LOCKDOWN
- ANDROID_WORK_DEVICE_OWNER_WITH_WORK_PROFILE_LOCKDOWN
- ANDROID_WORK_LOCKDOWN
- DEVICE_NAME
- MOBILE_THREAT_DEFENSE
- PRIVACY
- APP_LOCK
- GOOGLE_ACCOUNT
- ANDROID_WORK_APP_RUNTIME_PERMISSION
- IDENTITY_PREFERENCE
- MAC_OS_AGENT
- MANAGED_GOOGLE_PLAY
- ANDROID_MI_TUNNEL
- ANDROID_ENCRYPTION
- ANDROID_APP_CONNECT
- APPCONNECT_DEVICE_SETTINGS
- ANDROID_WORK_DEVICE_OWNER_SYSTEM_UPDATE
- DOMAINS
- END_USER_PRIVACY
- EXCHANGE
- MI_CLIENT_PRIVACY
- APP_UPDATE_SCHEDULE
- ZERO_PASSWORD
- WINDOWS_PRINTER
- PRINTING
- AUTH_ONLY
- SAFETYNET
- OSX_RESTRICTIONS
- WATCH_OS_RESTRICTIONS
- VISION_OS_RESTRICTIONS
- ANDROID_APP_CONTROL
- WINDOWS_APP_CONTROL

- ANDROID_SAMSUNG_PHONE_RESTRICTIONS
- Mobile Application Management (Gestión de Aplicaciones Móviles, MAM)
- ANTI_PHISHING
- SETUP_ASSISTANT
- DNS_SETTINGS
- WINDOWS_KIOSK
- FIDO_AGENT
- WINDOWS_BITLOCKER
- WINDOWS_DEVICE_ADMIN_RESTRICTIONS
- TELECOM_SETTINGS
- IDENTITY_CERTIFICATE_UP
- IDENTITY_CERTIFICATE_DC
- WIFI
- NOTIFICATIONS
- WEB_CONTENT_FILTER
- WINDOWS_AI_MANAGEMENT
- WINDOWS_ENERGY_SAVER
- WINDOWS_BROWSER
- WINDOWS_DESKTOP
- WINDOWS_PHONE_RESTRICTIONS
- WINDOWS_UPDATE
- WINDOWS_GPO_ADMX
- WINDOWS_LICENSE
- WINDOWS_ATP
- WINDOWS_LAPS
- WINDOWS_EDP
- WINDOWS_BIOS
- WINDOWS_BLOATWARE_REMOVER
- WINDOWS_HELLO
- WINDOWS_START_MENU

Creación de una configuración mediante un archivo YAML

Puede crear una configuración desde un archivo YAML. Las especificaciones relacionadas con la distribución no forman parte del archivo YAML. La distribución está ajustada por defecto como Ningún dispositivo.

Procedimiento

1. Vaya a **Configuraciones**.

2. Haga clic en **Importar**, en **Seleccionar archivo**, seleccione el archivo YAML y haga clic en **Importar**. Se importa el archivo YAML con los detalles de configuración. La página de Crear configuración se abre y se muestran todos los detalles que se agregaron al archivo YAML.
3. Seleccione *uno* de los tipos de distribución:
    - **Todos los dispositivos**
    - **Ningún dispositivo**
    - **Personalizado**
4. Verifique los detalles de la configuración y seleccione *una* de las siguientes opciones de Resumen de distribución:

> El resumen de distribución no está disponible para todas las configuraciones.

    - **No aplicar a otros espacios**
    - **Aplicar a los dispositivos de otros espacios**
5. Si el nuevo nombre de la configuración coincide con el nombre de una configuración existente, aparecerá un mensaje de error, haga clic en **Aceptar**, en **Atrás** y cambie el nombre de la configuración.
6. Haga clic en **Siguiente** y, luego, haga clic en **Hecho**.

Editar una configuración

Puede abrir una configuración y editar directamente los detalles de la misma, o importar un archivo YAML con todos los detalles necesarios. Si se selecciona más de una configuración o espacio, se deshabilita el botón Importar.

Procedimiento

1. Vaya a **Configuraciones**.
2. Seleccione y abra una configuración, haga clic en el icono editar (lápiz) y edite la configuración.
3. Como alternativa, desde la página de editar configuración, haga clic en el icono **Importar**, seleccione el archivo YAML y haga clic en **Importar**. La página de Editar configuración se abre y se muestran todos los detalles que se agregaron al archivo YAML.
4. Verifique los detalles de la configuración y seleccione una de las siguientes opciones de Resumen de distribución:

> El resumen de distribución no está disponible para todas las configuraciones.

    - **No aplicar a los otros espacios**.
    - **Aplicar a los dispositivos de otros espacios**

        > La distribución está ajustada por defecto como Ningún dispositivo.
5. Haga clic en **Hecho**.

Eliminar configuraciones

Puede eliminar las configuracionesseleccionadas.

Procedimiento

1. Marque las casillas para seleccionar las configuraciones específicas.

2. Seleccione **Acciones** > **Eliminar**.

Programar las actualizaciones de las aplicaciones internas

Ivanti Neurons for MDM actualiza automáticamente las aplicaciones internas cuando se registra un dispositivo. Ahora los administradores pueden programar aplicaciones internas basándose en la zona horaria del servidor. La aplicación se actualizará solo cuando el dispositivo se registre dentro de la hora programada. De forma predeterminada, la programación de las actualizaciones de las aplicaciones está desactivada.

> Esta configuración se puede aplicar solo para las actualizaciones, no para una nueva instalación. Puede utilizar el comando Enviar instalación/actualización para anular la programación de la actualización automática de las aplicaciones de iOS. Si la actualización automática está activada a nivel de aplicación o de catálogo, tendrá prioridad frente a la Configuración de aplicaciones programada y la aplicación se actualizará inmediatamente después de su conexión.

La configuración se puede aplicar solo a los siguientes tipos de aplicaciones:

- Aplicaciones internas de iOS.
- Aplicaciones internas de Android que sólo están en modo DO.
- aplicaciones de macOS con formato .pkg y .MIP.
- Aplicaciones de Windows.

Requisitos previos

Asegúrese de que se cumplen los siguientes requisitos previos para que la configuración funcione como se espera:

- La aplicación debe estar gestionada para iOS y Android. Para macOS, la aplicación puede estar en estado gestionado o no gestionado.
- Asegúrese de que la opción Instalar en el dispositivo en la Configuración de la aplicación está activada.
- El dispositivo debe estar registrado durante la hora programada.

Procedimiento

1. Inicie sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Vaya a **Configuraciones**.
3. Haga clic en **Añadir**. Se abre la página de Añadir Configuración.
4. Busque la **Aplicación actualización automática**. Se abre la página Crear configuración de actualización automática de aplicaciones.
5. Especifique un nombre en el campo **Nombre**.
6. En la sección **Ajuste de configuración** seleccione la **zona horaria** en la lista desplegable.
7. Seleccione la **Hora de inicio** en la lista desplegable y, a continuación, seleccione la **Duración** en la lista desplegable.
8. Haga clic en **Siguiente**.
9. Seleccione el usuario y el grupo de dispositivos necesarios y, a continuación, haga clic en la casilla **Habilitar esta configuración**.
10. Haga clic en **Hecho**. La configuración se aplica, la aplicación ahora se actualizará sólo en el horario especificado.

Si no puede ver la página de Configuraciones, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración de dispositivos
- Dispositivo de solo lectura

Temas relacionados:

- Espacios
- Priorizar configuraciones

Configuraciones de Windows que requieren una sesión de usuario activo

Algunas configuraciones de Windows requieren una sesión de usuario activo (un usuario que inició sesión en el dispositivo) antes de que se puedan aprovisionar. Si ningún usuario ha iniciado sesión, estas configuraciones se aplican después de que un usuario de MDM inicie sesión en el dispositivo.

Las siguientes configuraciones requieren una sesión de usuario activo:

- Código de acceso
- Certificado de usuario (certificado de identidad bajo el alcance del usuario)
- Firewall de Windows
- Exchange
- VPN
- Licencia de Windows
- Microsoft Defender for Endpoint
- Configuración de Windows (ámbito de usuario)
- Configuraciones dependientes del servicio puente
- Aplicaciones modernas/UWP

Configuraciones dependientes del servicio Bridge

Las configuraciones que requieren el servicio Ivanti Bridge se aprovisionan solo cuando hay una sesión de usuario activa disponible. Algunos ejemplos incluyen Restricciones de escritorio de Windows, Ajustes del navegador, Menú de inicio, Kiosco, BIOS, Guiones de Windows, GPO y otras configuraciones dependientes del servicio Bridge.

Excepción: Los siguientes scripts de Bridge predeterminados no requieren una sesión de usuario activo y se envían al dispositivo independientemente de si un usuario MDM ha iniciado sesión:

- obtener-datos-del-dispositivo.ps1
- obtener-estado-bitlocker.ps1
- hardware del dispositivo.ps1

Aplicaciones modernas/UWP

Las aplicaciones modernas/UWP se aprovisionan solo cuando hay una sesión de usuario activa disponible. Esto incluye:

- Aplicaciones internas empaquetadas como .appx o .appxbundle
- Aplicaciones de Microsoft Store/UWP

Las aplicaciones MSI y EXE tradicionales no están sujetas a este requisito.

Si una sesión de usuario requerida no está disponible cuando se programa una configuración para su implementación, la configuración se aprovisiona de forma automática después de que un usuario de MDM inicie sesión en el dispositivo.

10.2. Creación de una configuración del portal de autoservicio para usuarios

Como usuario de la empresa, puede utilizar el portal de autoservicio para gestionar sus dispositivos y certificados. La pestaña Mis dispositivos muestra los dispositivos que ha registrado.

Puede realizar las siguientes tareas desde la pestaña Mis dispositivos:

- Bloquear
- Desbloquear
- Retirar
- Restablecer código de acceso de Aplicaciones seguras

Puede realizar las siguientes tareas desde la pestaña Mis certificados:

- Cargar certificado

> Puede distribuir hasta un máximo de 100 archivos de configuración a la vez.

Procedimiento

1. Inicie sesión en el portal del administrador de Ivanti Neurons for MDM
2. Haga clic en **Añadir**.
3. Busque **Crear configuración de portal de autoservicio para usuarios**.
4. Haga clic en **Siguiente**.
5. Si no desea que esta configuración quede inmediatamente habilitada, deseleccione la opción **Habilitar esta configuración**.
6. Seleccione un nivel de distribución para la configuración:
    - **Todos los dispositivos**: distribuir la configuración a todos los dispositivos disponibles. Para delegar configuraciones entre espacios, seleccione una de las siguientes opciones:
        - **No aplicar a los otros espacios**.
        - Para delegar configuraciones en los espacios, seleccione **Resumen de distribución**> **Aplicar a todos los dispositivos en los espacios de otros dispositivos**.
            - Seleccione la casilla de verificación **Permitir que el administrador del espacio edite la distribución** para permitir que los administradores del espacio delegados editen la distribución para el espacio específico.
    - **Sin dispositivos** : seleccione esta configuración para la distribución en un momento posterior.
    - **Predeterminada** : se definen conjuntos específicos de grupos de dispositivos a los que se enviará esta configuración. Para delegar configuraciones entre espacios, seleccione una de las siguientes opciones:
        - **No aplicar a los otros espacios**.
        - **Resumen de la distribución** > **Aplicar a los dispositivos de otros espacios**.
            - Seleccione la casilla de verificación **Permitir que el administrador del espacio edite la distribución** para permitir que los administradores delegados del espacio editen la distribución para el espacio específico.
7. Si su servicio tiene espacios definidos, especifique si la configuración debe aplicarse a los demás espacios y la prioridad.
8. Haga clic en **Hecho**.

Para configuraciones que ejecutan un comando para el dispositivo en lugar de instalar un perfil en el dispositivo, los detalles de configuración no mostrarán la configuración como aplicada a ningún dispositivo.

10.3. Configuración personalizada

Esta sección contiene los siguientes temas:

- Definir una configuración personalizada
- Ajustes de la configuración personalizada

Licencia: Silver

Compatible con: iOS, macOS, tvOS, Android y Windows

Descripción

Le permite importar y distribuir un archivo de configuración predefinido.

Los formatos de archivo de configuración válidos son los siguientes:

SO	Formatos de archivo de configuración válidos
iOS y tvOS	• .plist • .mobileconfig • .xml
macOS	• .plist • .mobileconfig
Android	.xml. Actualmente, esta característica solo admite los archivos de configuración .xml para dispositivos Zebra.
Windows	SyncML.

Definir una configuración personalizada

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba «personalizada» en el campo de búsqueda y, a continuación, haga clic en la configuración **Personalizada**. Aparecerá la página de detalles de la configuración personalizada.
4. Configure los ajustes en esta página. Consulte la tabla de la sección Ajustes de la configuración personalizada para obtener ayuda acerca de los valores.
5. Haga clic en **Siguiente** para configurar los ajustes de distribución.
6. (dispositivos macOS) Seleccione una opción adicional para el ajuste **¿A quién es aplicable esta configuración?** dependiendo de lo que desee que haga esta configuración:
    - En todo el dispositivo (normalmente usado).
    - Específico para el usuario (usuario actualmente registrado).

Haga clic en **Hecho**.

Ajustes de la configuración personalizada

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Elegir OS	Haga clic en el icono del SO para cargar un archivo de configuración que se corresponda con el icono seleccionado
Elegir archivo	Esta opción aparecerá después de haber seleccionado un SO. Arrastre un archivo de la configuración al cuadro Arrastrar y soltar o haga clic en el botón **Elegir archivo** para seleccionar un archivo de configuración.

Configuración personalizada de CSP (solo Windows)

Solo puede crear una configuración CSP personalizada en dispositivos Windows. Cuando seleccione el sistema operativo Windows en la sección Elegir sistema operativo, obtendrá dos opciones:

Opción 1: archivo CSP XML: seleccione esta opción y siga el mismo proceso mencionado para el ajuste **Seleccionar archivo** .

Opción 2: nodo de esquema CSP OMA-URI personalizado

Procedimiento

1. Seleccione la opción Nodo de esquema CSP OMA-URI personalizado de la lista. La sección Configuración CSP personalizada aparecerá en pantalla.
2. En **ACCIONES**, haga clic en el botón + para empezar a crear la configuración con diferentes campos OMA-URI.
3. En la pantalla aparece la ventana emergente **Agregar fila** que tiene los siguientes campos:
    - Descripción: introduzca la información general sobre el ajuste
    - OMA-URI: introduzca el OMA-URI que desea utilizar como ajuste
    - Tipo de datos: seleccione un tipo de datos que utilizará para esta configuración: DATE, FLOAT, BASE64, NODE, XML, BINARY, CHARACTER, TIME, BOOLEAN, INTEGER
    - Valor: introduzca un valor asociado al tipo de datos seleccionado
    - Tipo de acceso: Añadir, Eliminar, Ejecutar, Reemplazar, Obtener

Haga clic en **Guardar y Cerrar** para cerrar la ventana con los datos proporcionados. Haga clic en **Guardar y Añadir** otra para crear una nueva fila.

5. Haga clic en **Siguiente**.
6. Seleccione el modo de distribución y haga clic en **Hecho**.

Temas relacionados

- Insertar SyncML en dispositivos mediante la configuración personalizada
- Cómo crear una configuración

10.4. Insertar SyncML en dispositivos mediante la configuración personalizada

Puede crear sus propios archivos de configuración de idioma de marcado de sincronización (SyncML, Synchronization Markup Language) u obtenerlos de un tercero para implementar características personalizadas añadiéndolas a una configuración personalizada.

Plataformas compatibles:

- Windows

Dispositivos compatibles:

- Windows 10+
- Microsoft HoloLens 2

Procedimiento

1. Vaya a **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Haga clic en **Configuración personalizada** para visualizar la página **Crear configuración personalizada**.
4. Introduzca un nombre para la configuración.
5. Haga clic en el icono del SO Windows.
6. Arrastre y suelte el archivo SyncML en la interfaz o haga clic en **Elegir archivo** para navegar hasta el archivo que va a seleccionar para cargar el dispositivo.

> Ivanti Neurons for MDM no realiza verificaciones de validación en el código del archivo.

7. Haga clic en **Siguiente**.

Registro personalizado de SyncML

Los comandos de SyncML que se envían al dispositivo de Windows y las respuestas de SyncML de estos comandos desde el dispositivo se pueden ver en la pestaña Registros de dispositivos. Esta información de registro estará disponible después de enviar la configuración de **SyncML personalizada de Windows**. Cuando el sistema envía una configuración personalizada de SyncML, tiene el estado "Instalado" siempre en la pestaña "Configuración" del dispositivo para su configuración, independientemente de las respuestas de SyncML.

10.5. Configuración del diseño de la pantalla de inicio

La configuración del diseño de la pantalla de inicio define un diseño de aplicaciones, carpetas y clips web para la pantalla de inicio.

Esta sección contiene los siguientes temas:

- Definir una configuración del diseño de la pantalla de inicio
- Ajustes de la configuración del diseño de la pantalla de inicio

Licencia: Silver

Dispositivos elegibles:

- Solo iOS 9.3+ supervisados
- Solo tvOS supervisado

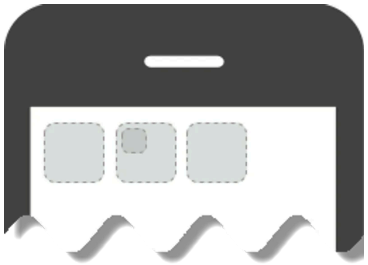
Definir una configuración del diseño de la pantalla de inicio

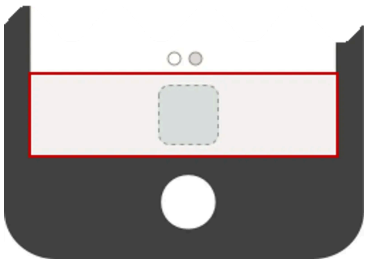
Procedimiento

1. Vaya a **Configuraciones** > haga clic en **+Añadir**.
2. Escriba "inicio" en el campo de búsqueda y, a continuación, haga clic en la configuración de **Diseño de la pantalla de inicio**. Se abre la página de detalles de Configuración del diseño de la pantalla de inicio.
3. Configure los ajustes en esta página. Consulte la tabla de la sección Home_Screen_Layout_Configuration_Settings para obtener ayuda acerca de los valores.
4. Haga clic en **Siguiente** para configurar los ajustes de distribución. Para dispositivos iPad compartidos, seleccione el canal **Dispositivo** o en el canal **Usuario**. Para obtener más información, consulte Trabajar con configuraciones.
5. Haga clic en **Hecho**.

Ajustes de la configuración del diseño de la pantalla de inicio

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Acoplar	Haga clic en el icono + para añadir una aplicación o clip web de la pantalla de inicio, que aparece resaltado aquí, y a continuación siga las instrucciones de las siguientes pantallas: Puede agregar manualmente las aplicaciones del sistema, escribiendo la ID del grupo de Apple (que empieza con "com.apple"). Por ejemplo, escriba 'com.apple.DocumentsApp' para añadir la aplicación 'Files'.
Página 1	Haga clic en el icono ⊕ para añadir una aplicación o clip web al área de página de la pantalla de inicio, que aparece resaltado aquí, y a continuación siga las instrucciones de las siguientes pantallas: Puede hacer clic en Añadir página para añadir otra página a la pantalla del teléfono.







10.6. Configuración del control de aplicaciones: controle qué aplicaciones pueden instalarse en cada dispositivo

La configuración del control de aplicaciones le permite categorizar las aplicaciones como lista de permitidos o lista de bloqueados a nivel de dispositivo. Las aplicaciones que ya estén instaladas no serán visibles y no podrán iniciarse. Las aplicaciones seguirán siendo visibles en la App Store, pero no se podrán descargar ni iniciar. Cualquier dispositivo al que se distribuya esta configuración la empleará e ignorará cualquier otro ajuste de Políticas de aplicaciones permitidas. Esta configuración sustituye a cualquier política relacionada con la aplicación que haga referencia a las mismas aplicaciones en los dispositivos de destino.

Esta configuración sustituye a cualquier política relacionada con la aplicación que haga referencia a las mismas aplicaciones en los dispositivos de destino. Para dispositivos Windows 10, las restricciones se dan a nivel del dispositivo, de modo que una configuración es la única forma de aplicar las reglas de la aplicación.

La configuración del control de aplicaciones le permite crear dos tipos de listas:

- **Lista de permitidos:** solo permite aquellas aplicaciones que se añadan de manera explícita a esta lista. No se podrá instalar ninguna otra aplicación en los dispositivos.
- **Lista de bloqueados:** No permitir la instalación de aplicaciones específicas en dispositivos.

Dispositivos compatibles

Puede utilizar la configuración del control de aplicaciones para poner en lista de bloqueados o en lista de permitidos diferentes aplicaciones en los siguientes dispositivos:

- Android Work Profile en dispositivos propiedad de la empresa
- Solo iOS 9.3+ supervisados
- tvOS 11+
- Windows

Crear la configuración del control de aplicaciones

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Introduzca **Control de Aplicaciones** en el campo resultante **Elegir configuración** y luego seleccione la configuración de **Control de aplicaciones**.
4. Introduzca un nombre y una descripción para la configuración.
5. Seleccione un SO y continúe más abajo en la sección que corresponda a su SO.

Android Work Profile en dispositivos propiedad de la empresa

Los usuarios pueden añadir hasta 50 ID de aplicaciones al grupo de la lista de permitidos o de la lista de bloqueados.

Procedimiento

1. Seleccione **Crear una lista de permitidos para aplicaciones personales** o **Crear una lista de bloqueados para aplicaciones personales** para añadir la lista de aplicaciones correspondientes para que se incluyan en la lista de permitidos o la lista de bloqueados.
2. Introduzca la ID de la aplicación (com.example.com) y haga clic en Añadir.
3. Haga clic en **Siguiente** y elija una opción de distribución.
4. Haga clic en **Hecho**.

Dispositivos iOS 9.3 supervisados

Procedimiento

1. Elija si desea crear una lista de permitidos o una lista de bloqueados.
2. Haga clic en **Añadir aplicaciones**.
3. Elija las aplicaciones que desea poner en la lista de permitidos o la lista de bloqueados haciendo clic en una o en las dos pestañas siguientes:
   - Haga clic en **Añadir por búsqueda** para buscar y elegir aplicaciones desde la App Store o App Catalog.
   - Haga clic en **Añadir manualmente** para elegir las aplicaciones introduciendo la Id. de paquete de Apple (empieza por "com.apple") solo para las aplicaciones del sistema Apple.

Haga clic en la pestaña **Lista de permitidos** o **Lista de bloqueados** para ver la lista de aplicaciones elegidas que se pondrán en la lista de permitidos o la lista de bloqueados.

5. (Opcional) Seleccione la opción **Incluir todos los clips web**.
6. Haga clic en **Siguiente** y, a continuación, elija una opción de distribución.
7. Haga clic en **Hecho**.

Dispositivos Windows

Procedimiento

1. Seleccione **Permitido** o **No Permitido** para añadir la lista de aplicaciones apropiadas a la lista de permitidos o a la lista de bloqueados.
2. En la sección **Definición de reglas**, seleccione el **tipo de aplicación** de la lista.
3. Introduzca un nombre de identificador en el **cuadro Identificador de la aplicación** para buscar una aplicación específica. También puede utilizar el enlace **Buscar aplicaciones** para abrir un nuevo diálogo y buscar identificadores de aplicaciones específicos de Windows.
4. (Opcional) Introduzca alguna descripción sobre la aplicación en el cuadro **Descripción de la aplicación**.
5. Utilice el enlace **+Añadir** para añadir más definiciones de reglas para poner las aplicaciones en la lista de permitidos o en la lista de bloqueados.
6. Haga clic en **Siguiente** y elija una opción de distribución.
7. Haga clic en **Hecho**.

10.7. Configuración de las notificaciones de la aplicación

Elija cómo reciben notificaciones los usuarios de aplicaciones seleccionadas.

Aplicable a: dispositivos iOS 9.3+ supervisados.

Crear una configuración de las notificaciones de la aplicación

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba 'notifications' en el campo de búsqueda y, a continuación, haga clic en la configuración **Notificaciones de la aplicación** : Aparecerá la página Establecimiento de la configuración de notificaciones de la aplicación.
4. Asigne un nombre a la configuración y descríbala.
5. Añada las aplicaciones buscándolas en la App Store o manualmente introduciendo la Id. de paquete.
6. Elija una aplicación a la que aplicar los ajustes de notificación.
7. Configure los ajustes de notificación. Puede elegir entre las siguientes notificaciones:
    - Permitir notificaciones
        - Mostrar en el Centro de notificaciones
        - Sonidos
        - Icono de la aplicación del distintivo
        - Mostrar en pantalla de bloqueo
        - (Dispositivos iOS 12.0+ supervisados) Mostrar las alertas críticas al usar CarPlay
        - (Dispositivos iOS 12.0+ supervisados) Permitir la activación de las alertas críticas (ignorar "No molestar")
    - Desbloquear estilo de alerta
        - Banners
        - Alerta modal
        - Ninguno
    - (Dispositivos iOS 12.0+ supervisados) Tipo de agrupación
        - Automático
        - Por aplicación
        - Desactivado
    - (iOS 14.0+) Tipo de vista previa de la notificación: seleccione un tipo de vista previa para mostrarla en las vistas previas de los mensajes de notificación del dispositivo.
        - Controlado por el usuario: muestra las vistas previas de los mensajes según los ajustes del usuario para las aplicaciones del dispositivo.
        - Siempre: muestra las vistas previas de los mensajes.
        - Cuando está desbloqueado: la pantalla de mensajes solo se muestra cuando un dispositivo esté desbloqueado.

- Nunca: evita que las aplicaciones muestren vistas previas de los mensajes en las notificaciones.

8. Haga clic en **Siguiente** para configurar los ajustes de distribución.
9. Haga clic en **Listo**.

Para obtener más información, consulte **Cómo crear una configuración**.

10.8. Exportar configuraciones

Exporte sus archivos de configuración para enviarlos al soporte técnico y que puedan utilizarlos como herramienta de ayuda para el diagnóstico. Puede exportar un único archivo de configuración como archivo de formato Yaml o exportar todas sus configuraciones a un archivo .zip.

Procedimiento

Exportar la configuración

Puede exportar archivos de distintos puntos de la página Configuración, dependiendo de qué configuraciones desee exportar.

Exportar todas las configuraciones:

1. Vaya a **Configuraciones**.
2. Marque las casillas para seleccionar las configuraciones específicas.
3. Haga clic en **Acciones** > **Exportar todas las configuraciones seleccionadas con detalles**. Si desea exportar todas las configuraciones, seleccione **Exportar todas las configuraciones con detalles**.
   Se incluye un conjunto de archivos YAML en un archivo .ZIP. El informe incluye detalles de todas las configuraciones existentes en los espacios seleccionados.

Exportar una configuración personalizada:

1. Vaya a **Configuraciones**.
2. Haga clic en **+Añadir** para seleccionar una configuración.
3. Siga los pasos para personalizar la configuración.
4. Haga clic en **Siguiente**.
5. Elija un nivel de distribución.
6. Haga clic en **Hecho**.
7. Seleccione la configuración que acaba de crear de la lista de la página **Configuración**.
8. Haga clic en el menú desplegable **Acciones** y en **Exportar.**

Se descargará un archivo con el nombre de la configuración y uno con marca de hora _aaaammdd.yaml en su dispositivo.

Exportar una configuración existente:

1. Vaya a **Configuraciones**.
2. Seleccione una configuración existente.
3. Haga clic en el menú desplegable **Acciones** y, a continuación, en **Exportar**.
   Se descargará un archivo con el nombre de la configuración y uno con marca de hora _yyyymmdd.yaml en su dispositivo.

10.9. Priorizar configuraciones

Si selecciona varios grupos de dispositivos para una configuración, es posible que se asignen varias configuraciones del mismo tipo a un determinado dispositivo.Cuando se aplican configuraciones del mismo tipo al mismo dispositivo, la prioridad definida determina qué configuración se aplica. La configuración con la prioridad más alta tendrá el número más bajo. Por ejemplo, la configuración con prioridad 1001 tiene una prioridad mayor que la configuración con prioridad 1002. El servicio asigna los números automáticamente.

> La prioridad WI-FI no se puede aplicar al dispositivo y está exenta de la prioridad.

Esta opción solo está disponible si la página contiene dos o más configuraciones del mismo tipo y si se selecciona un único espacio en la lista desplegable. Puede cambiar la prioridad de las configuraciones.

Procedimiento

1. Vaya a **Configuraciones**.
2. Sin seleccionar ninguna configuración, seleccione **Acciones > Priorizar configuraciones.**
   Si no aparece **Acciones**, quiere decir que no tiene múltiples configuraciones de un tipo que requiera prioridades.
3. Utilice las flechas para mover las configuraciones de forma que la que debe tener la mayor prioridad aparezca en la parte superior.

> Un icono de candado indica que la prioridad de la configuración no puede cambiarse sin editar el ajuste de distribución de Todos los Dispositivos en la configuración.

Haga clic en **Guardar**.

> La priorización puede hacerse hasta en 400 configuraciones.

Si no puede ver la página de Configuraciones, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes funciones:

- DispositivoAdministrador
- DispositivoSoloLectura

10.10. Administrar configuraciones

Esta sección contiene los siguientes temas:

- Configuraciones de App Connect
- Configuración de seguridad
- Configuraciones de recursos del usuario
- Configuración de acceso a la red de la empresa
- Móvil
- Otra configuración

10.10.1. Tipos de configuración

Esta sección contiene los siguientes temas:

- Buscar una configuración
- Seguridad
- Recursos del usuario
- Acceso a la red de la empresa
- Red móvil
- Más configuraciones
- Configuración de la sincronización del dispositivo

Buscar una configuración

Utilice la función buscar y filtrar en la página **Elegir configuraciones** para encontrar la configuración que quiere aplicar.

Procedimiento

1. Elegir **Configuraciones**.
2. Elija una de las configuraciones que aparecen en la lista o haga clic en el botón **+Añadir**.
3. Aparece la página **Elegir configuración**.
   Haga clic en una de las configuraciones que aparecen o:
   - Introduzca el nombre de la configuración en el cuadro de búsqueda.
   - Haga clic en el icono del filtro que está a la derecha del cuadro de búsqueda para mostrar los tipos de configuración compatibles con la plataforma.

Haga clic en el botón de la configuración para acceder a las opciones de los ajustes de la configuración.

Para obtener más información, consulte Trabajar con configuraciones.

Seguridad

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
Android Enterprise	Especifica las opciones de Android Enterprise	Android Enterprise	Licencia
Dispositivo AppConnect	Especifica los ajustes de seguridad de las aplicaciones con AppConnect activado en los dispositivos.	• Android • iOS	licencia
Atestación de Claves de Acceso de Apple	Habilitar la atestación empresarial de WebAuthn para claves de acceso específicas en dispositivos Apple.	• macOS	
Entra ID (Abonado de Azure)	Al conectar Ivanti Neurons for MDM al Entra ID, puede utilizar el estado de conformidad de los dispositivos gestionados para el acceso condicional a las aplicaciones de Microsoft 365.	• iOS • Android	• Para los nuevos clientes: UEM segura Premium • Para los clientes previos: Platinum
Certificado	Establece confianza con los servidores	• Android • iOS • macOS • watchOS • visionOS • tvOS	
Transparencia del certificado	Controla que se cumpla la transparencia del certificado, que solo puede aparecer en el perfil del dispositivo.	• iOS • macOS • tvOS • watchOS • visionOS	

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
Registro de dispositivos	Recupera los registros adicionales como los registros de red y seguridad de los dispositivos.	• Android Enterprise	
Configuración del administrador de discos	Define las políticas para gestionar los dispositivos de almacenamiento externos y de red.	• macOS 15.0+ supervisado	
Cifrado en Android	Notifica a los usuarios de que deben iniciar el cifrado.	Android	
DNS cifrado	Le permite mejorar la seguridad sin necesidad de configurar VPN.	• iOS • macOS • visionOS	licencia
Ajustes de inteligencia externa	Permite integraciones de inteligencia externa.	• iOS 26,4+ • macOS 26.4+ • visionOS 26.4+	
Defensa ante amenazas móviles	Protege los dispositivos administrados de las amenazas y vulnerabilidades móviles que afectan a dispositivos, redes y aplicaciones..	• Android • iOS	
Medidas locales de Threat Defense	Cree y distribuya una configuración del dispositivo que defina las medidas locales que se deberán tomar en dispositivos compatibles Android cuando el cliente con Threat Defense detecte una amenaza.	Android	
FileVault 2	Ofrece la posibilidad de realizar un cifrado completo del disco XTS-AES 128 en el contenido de un volumen.	macOS	licencia
Clave de recuperación de FileVault	Determina los ajustes para la redirección de las claves de recuperación de FileVault a un servidor corporativo.	macOS	licencia
Certificado de identidad	• Autentica el dispositivo para los servidores. • Autentica el dispositivo para los recursos de red.	• Android • iOS	

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
		• macOS • watch OS • vision OS	
Bloqueo de activación de iOS	Habilita la característica Bloqueo de activación de Apple en los dispositivos supervisados.	iOS	Licencia
Configuración personalizada de iOS	Distribuye un perfil de configuración iOS creado por una aplicación diferente.	iOS	
Restricciones de iOS	• Bloquea características del dispositivo. • Habilita características del dispositivo.	• iOS • watch OS • vision OS	
Ajustes de inteligencia	Permite integraciones con Apple Intelligence.	• iOS 26,4+ • macOS 26.4+ • vision OS 26.4+	
Visualización de la sala de conferencias	Activa el modo Visualización de la sala de conferencias en Apple TV.	tvOS 10.2+	
Ajustes del teclado	Permite configurar el comportamiento del teclado, las opciones de entrada y otros ajustes relacionados con la experiencia del usuario en los dispositivos.	• iOS 26,4+ • macOS 26.4+	
Bloqueo y kiosco: Android	• Bloquea características del dispositivo. • Vuelve a habilitar características del dispositivo. • Aplica la característica del kiosco.	Android	
Bloqueo y kiosco: Android	• Define qué características y aplicaciones están restringidas en los dispositivos con la versión corporativa de Android.	Android 5.0 +	

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
Enterprise	• Aplica la característica del kiosco.		
Bloqueo y kiosco: Samsung KNOX Standard	• Define qué características y aplicaciones están restringidas en los dispositivos Samsung KNOX Standard. • Aplica la característica del kiosco.	Samsung Knox	
Configuración de la solución de contraseñas de administrador local	Permite a los administradores regenerar automáticamente la contraseña del administrador local en dispositivos macOS gestionados en intervalos establecidos.	macOS	
Firewall de macOS	Administra los ajustes de cortafuegos de la aplicación a los que se puede acceder en el panel Preferencias de seguridad en dispositivos macOS. El administrador puede habilitar el modo sigiloso especificando un dispositivo que no se pueda descubrir por el comando ping.	macOS 10.12+	licencia
Restricciones de macOS	Determina qué restricciones están activadas en los dispositivos macOS.	macOS	licencia
Restricciones de la AppStore de macOS	Define qué restricciones están activadas en la AppStore de macOS.	macOS	licencia
Restricciones de grabación en disco de macOS	Administre las restricciones de grabación de discos en macOS.	macOS	licencia
Mobile@Work para macOS	Cree reglas para las ejecuciones de Mobile@Work para macOS.	macOS	licencia
Mobile@Work para secuencias de comandos de macOS	Cree secuencias de comandos para distribuir a Mobile@Work para macOS.	macOS	licencia
Preferencia de identidad	Identifique un elemento de Preferencia de identidad en la llave del usuario que haga referencia a una carga útil de la identidad incluida en el mismo perfil.	macOS	licencia
Preferencia de certificado	Identifique un elemento de Preferencia de certificado en la llave del usuario que haga referencia a una carga útil del certificado incluida en el mismo perfil.	• macOS	licencia

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
Control multimedia permitido	Configure las opciones de montaje, desmontaje y expulsión de soportes físicos.	macOS	licencia
Ajustes del Finder de macOS	Administre los ajustes de la aplicación de Finder en macOS.	macOS	licencia
Política de extensiones del kernel de macOS	Controla las restricciones y los ajustes para cargar extensiones del kernel aprobadas por el usuario.	macOS	licencia
Active Directory (macOS)	Configure opciones avanzadas para enlazar los dispositivos macOS con un dominio de Active Directory (AD) a fin de que puedan acceder a los servicios de software que dependen de Active Directory para la autenticación y seguridad.	macOS	licencia
Creación automática de cuentas en Office 365(macOS)	Configure la información y opciones de usuario para la configuración inicial de todas las aplicaciones de Microsoft Office 365.	macOS	licencia
App Catalog de Apple	Gestiona el acceso al catálogo de aplicaciones de Apple a través de un clip web.	• iOS • macOS	
Dominios administrados	Especifica los dominios de correo electrónico y web de confianza.	• iOS 8+ • vision OS 1.1+	Licencia
Código de acceso	• Hace que sea obligatorio un código de acceso. • Especifica la longitud y el contenido del código de acceso. • Cambia los requisitos del código de acceso.	• Android • iOS • macOS • watch OS	
Preferencias de privacidad (macOS)	Configurar qué aplicaciones tienen permitido obtener acceso a los servicios, archivos y recursos del sistema.	macOS	licencia
Autenticar	Proporcione una autenticación sin contraseña para los servicios de inicio de sesión en la nube o de sobremesa.	• macOS	

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
Configuración de privacidad	Especifica si se recopilan los datos de ubicación.	• Windows • iOS • Android • Windows	
Información de Declaración de la privacidad del cliente	Mostrar la política de privacidad al usuario en el cliente de Go.	• Android • Android Enterprise • iOS	
Ajustes del cliente de Ivanti Go	Configúrelo para que recopile datos a través de MixPanel incluida la información sobre el dispositivo y el uso para solucionar problemas y mantener la máxima calidad de sus servicios.	• iOS • macOS	
Configuración de los ajustes de la extensión de Safari	Administre las extensiones del navegador Safari desde varios dominios.	• iOS 18.0+ Supervisado • macOS 15.0+ supervisado	
Ajustes de Siri	Permite configurar cómo los dispositivos acceden a los ajustes de Siri y los utilizan.	• iOS 26,4+ • macOS 26.4+ • watchOS 26.4+ • visionOS 26.4+	
Configuración de archivos de	Los administradores pueden gestionar y desplegar de manera centralizada archivos de configuración para diversos servicios del	macOS	

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
configuración de servicios	sistema.		
Actualizaciones de software	Crea y distribuye reglas para las actualizaciones del SO.	• iOS • macOS • Windows	
Configuración de los ajustes de actualización del software	Crea y actualiza la configuración de Aplicación de actualizaciones de software.	• iOS 18.0+ Supervisado • macOS 15.0+ supervisado	
Servidor de zona horaria	Permite a los dispositivos conectarse a servidores de zona horaria.	macOS	licencia
Filtro de contenido web	Controla el contenido de Safari.	• iOS 7 supervisados • vision OS 1.1+	Silver
Windows_Firewall	La configuración del Firewall de Windows tiene varias restricciones de firewall. En función de las restricciones del firewall que haya aplicado el administrador, el Estado del firewall da como resultado uno de los siguientes estados del firewall en el panel Preferencias de seguridad en dispositivos Windows: • El firewall está activado y vigilando. • Se ha desactivado el firewall. • El firewall no está supervisando todas las redes o se han desactivado algunas reglas. • Temporalmente, el firewall no está supervisando todas las redes. • No se aplica.	Windows 10+	
Protección de la información de Windows	Define los ajustes de Protección de la información de Windows (WIP) para proteger los datos corporativos.	Windows 10+	licencia

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
Las **Restricciones de Windows**	Determina qué funciones están disponibles en dispositivos Windows 10+.	Windows 10+	
Configuración del administrador de IA de Windows	Permite gestionar los ajustes y configuraciones de la IA de Windows.	Windows 10+	

Recursos del usuario

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
CalDAV	• Configura el acceso a un servidor CalDAV (como Google Calendar)	• iOS • visionOS	
CardDAV	• Configura el acceso a un servidor CardDAV (como Google Contacts)	• iOS • visionOS	
Correo electrónico	• configura el acceso para el correo electrónico POP/IMAP (como Gmail)	• iOS • visionOS	
Exchange	• configura el acceso para el correo electrónico basado en ActiveSync (como Outlook) para dispositivos móviles Android y iOS • configura el correo electrónico basado en Exchange Web Services (EWS) para dispositivos macOS • define hasta qué punto sincronizar con el dispositivo • define la seguridad para el correo electrónico	• Android • iOS • macOS • visionOS	• Exchange a través del Sentry no se admite en macOS • La marca de Sincronizar correos electrónicos de días anteriores no es aplicable a macOS
Google	• Crea configuraciones de cuenta Google que conectan dispositivos iOS 9.3.2+ a cuentas Google. • Especifica qué aplicaciones utilizar para hacer llamadas de audio a contactos dentro del sistema Google.	• iOS • visionOS	
Fuente	• instala fuentes no estándar necesarias para visualizar correctamente los documentos	• iOS	
Calendario suscrito	• configura una suscripción a un calendario de Internet	• iOS • visionOS	
Clip web	• muestra un acceso directo (icono) a una página web	• iOS • macOS	
Caché de contenido	• brinda un servicio de caché de contenido para habilitar copias locales del software de la App Store y • habilita clientes conectados para que las descargas de software y aplicaciones sean más	• macOS	

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
	rápidas.		

Acceso a la red de la empresa

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
AirPlay	• configura el acceso a dispositivos alternativos para la visualización de contenido multimedia	• iOS • macOS	Silver
AirPrint	• configura la impresión inalámbrica	• iOS • macOS	Silver
VPN siempre activada	• configura el acceso a un servidor VPN sin interacción por parte del usuario	• Android 7.0 + • iOS 8+	• Gold para la versión corporativa de Android • Silver para iOS
Permisos predeterminados del tiempo de ejecución de las aplicaciones	• establece la configuración de los permisos del tiempo de ejecución para las aplicaciones instaladas en dispositivos con la versión corporativa de Android.	• Aplicaciones creadas para Android API 23+ y con Android 6.0+ en dispositivos con la versión corporativa de Android.	
Educación	• configura la carga útil de Apple Education y la aplicación Classroom para Líderes y Miembros	• supervised iOS 9.3+	licencia
Proxy global	• configura los dispositivos para que redireccionen el tráfico HTTP a un servidor proxy	• iOS 7 supervisados • tvOS supervisado	Silver
LDAP	• configura el acceso a un directorio corporativo	• iOS • visionOS	
Túnel	• define una conexión VPN por aplicación entre un cliente y Sentry mediante Tunnel	• iOS 7+ • macOS 10.13+ • Windows 10+ • Android	
Bridge	• permite que el departamento informático modernice las operaciones de Windows en UEM sin sacrificar las funcionalidades críticas	• Windows 10+ escritorio	Licencia de Bridge
Servidor macOS	• define una cuenta del servidor macOS con los tipos de cuentas configuradas y los ajustes correspondientes. Permite al	• iOS 10+	

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
	usuario activar el uso compartido de archivos en el servidor.		
VPN por aplicación	• configura conexiones entre aplicaciones específicas y un servidor VPN	• iOS • watchOS • visionOS • tvOS	Silver
Configuración del relé de red	• añade configuración para definir los ajustes de los relés de red	• iOS • macOS • visionOS	
Inicio de sesión único	• configura el inicio de sesión único para aplicaciones específicas administradas	• iOS • macOS • visionOS	
Inicio de sesión seguro multiusuario	• Establece acceso seguro multiusuario a través de un clip web	• iOS	
VPN	• configura el acceso a un servidor VPN	• Android • Windows • iOS • macOS • visionOS • tvOS	
VPN a petición	• configura el acceso a un servidor VPN basado en dominios, nombres de host, etc.	• iOS	
Wi-Fi	• configura el acceso a una red inalámbrica	• Android • Windows • iOS • macOS • watchOS • visionOS • tvOS	

Red móvil

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
APN	• configura el Nombre del punto de acceso (APN) móvil para el dispositivo	• iOS	
Móvil	• configura el acceso a redes móviles	• iOS • watchOS	
Configuración de la red móvil privada	• establece la carga útil para proporcionar información sobre los dispositivos en los despliegues de redes privadas	• iOS	
Configuración de preajustes de iOS para Telecom	• establece los valores predeterminados para restricciones de itinerancia internacional • establece los valores predeterminados para restricciones de cobertura personal	• iOS	

Más configuraciones

Tipo	Qué hace	Para estos dispositivos	Requiere esta licencia
Apple TV	• define el idioma y la configuración regional para Apple TV	• iOS 7 supervisados	Silver
Nombre predeterminado del dispositivo	• define un nombre predeterminado del dispositivo utilizando variables	• iOS 8 supervisados	Silver
Fondo de pantalla de iOS	• instala una pantalla de inicio y el fondo de pantalla de bloqueo	• iOS 7 supervisados	Silver
Fondo de escritorio de macOS	• Instala una pantalla de inicio y un fondo de pantalla de bloqueo en los dispositivos. El usuario puede cambiar los fondos de pantalla, pero no quitarlos de un dispositivo una vez que se han distribuido		No requerido
Ajustes del asistente de migración	Ayuda a los administradores y usuarios a transferir datos, aplicaciones y ajustes durante la configuración o migración de dispositivos.	• macOS 26.4+	
Modo Single-App	• restringe el dispositivo que se utiliza para la aplicación especificada	• iOS 7 supervisados • tvOS supervisado	Silver
Configuración de dominios asociados	• La configuración de dominios asociados es un diccionario que asigna las aplicaciones a sus dominios asociados. • Los dominios asociados se pueden usar con funciones como AppSSO extensible, enlaces universales y Autorrellenado de contraseñas.	• macOS 10.15+	Gold
Configuración de los ajustes del host de Compartir pantalla	• Permite a los administradores controlar de forma segura las funciones de compartir pantalla de macOS en todos los dispositivos gestionados.	• macOS 14+	

Configuración de la sincronización del dispositivo

Los ajustes de sincronización del dispositivo proporcionan puntos de datos de una lista que usted puede supervisar en los dispositivos. Las configuraciones de sincronización de dispositivos no se pueden editar. Puede ver una lista de los ajustes seleccionados.

Procedimiento

1. Vaya a **Configuraciones**.

2. Haga clic en **Configurar sincronización de dispositivos**. Se muestra la pestaña Detalles de la página **Configurar sincronización de dispositivos** con una lista de elementos marcados.

Ajustes	Tiempo entre lecturas, en minutos
Lista de certificados	
Información del dispositivo	60
Lista de aplicaciones instaladas	60
Lista de aplicaciones administradas	60
Lista de perfil	60
Lista de perfil de aprovisionamiento	60
Restricciones	60
Información de seguridad	60
iOS 9+	
Comprobar si hay actualizaciones	1440

Temas relacionados

- Variables
- Trabajar con configuraciones

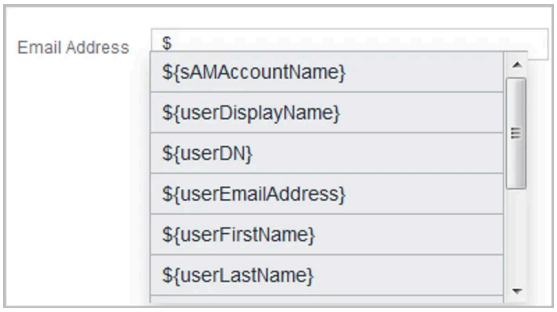
10.10.2. Variables

Puede utilizar variables en ciertos campos de la configuración para representar valores específicos para un usuario concreto. Cualquier campo que admita variables mostrará una lista de variables admitidas si escribe $ en el campo. Esta sección contiene los siguientes temas:

- Variables de la cuenta de usuario compatibles
- Variables de dispositivos compatibles

Variables de la cuenta de usuario compatibles

Variables del usuario

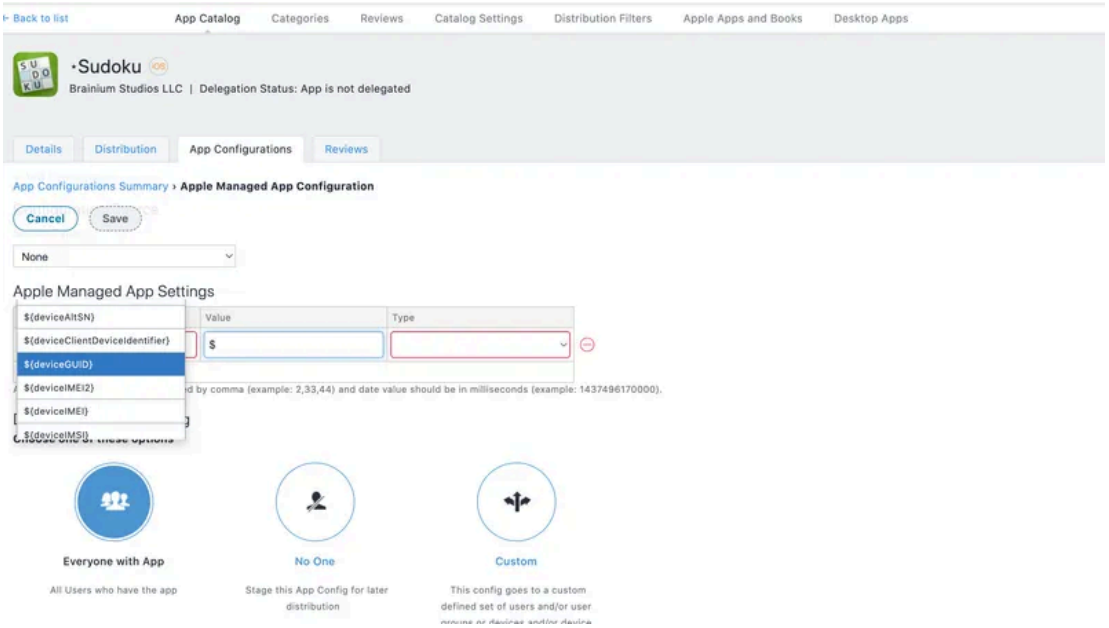


Clave de variable	Descripción del valor
$	atributo departamento (requiere Entra ID)
$	Intercambio electrónico de datos: identificador personal
$	Id. de Apple administrada del usuario
$	Atributo sAMAccountName (requiere Active Directory)
$	Atributo Nombre común (NC) extraído del nombre distintivo (requiere LDAP)
$	Nombre en pantalla
$	Nombre distintivo (requiere LDAP)
$	La parte del dominio de la dirección de correo electrónico (la parte de después de la "@")
$>	La parte local de la dirección de correo electrónico (la parte de antes de la "@")
$	Dirección de correo electrónico
$	Nombre
$	Apellido
$	Configuración regional
$	Atributo de unidad organizativa (OU) extraído del nombre distintivo (requiere LDAP)
$	Información de Kerberos Realm (requiere Active Directory)
$	El dominio que forma parte de la ID de inicio de sesión (la parte tras la "@")
$	La parte local del ID de inicio de sesión (la parte de antes de la "@")
$	ID de inicio de sesión (formato de la dirección de correo electrónico)
$	Atributo userPrincipalName (requiere Active Directory)

Variables de dispositivos compatibles

Utilice las variables del dispositivo para especificar la información acerca de un dispositivo móvil.

Variables del dispositivo


Back to list
App Catalog
Categories
Reviews
Catalog Settings
Distribution Filters
Apple Apps and Books
Desktop Apps
·Sudoku
Brainium Studios LLC | Delegation Status: App is not delegated
Details
Distribution
App Configurations
Reviews
App Configurations Summary › Apple Managed App Configuration
Cancel
Save
None
Apple Managed App Settings
${deviceAltSN}
${deviceClientDeviceIdentifier}
${deviceGUID}
${deviceIMEI2}
${deviceIMEI}
${deviceMSI}
Value
Type
$
d by comma (example: 2,33,44) and date value should be in milliseconds (example: 1437496170000).
Everyone with App
All Users who have the app
No One
Stage this App Config for later distribution
Custom
This config goes to a custom defined set of users and/or user

Clave de variable	Descripción del valor
$	Fecha de la última vez que se conectó el cliente (conexión más reciente: bien MDM o cliente)
$	Número de serie alternativo
$	Identificador que usa la aplicación del cliente
$	Identificador de dispositivo único global
$	ICCID
$	IMEI2
$	IMEI
$	IMSI
$	Fecha de la última vez que se conectó el dispositivo (conexión más reciente: bien MDM o cliente)
$	Identificador de dispositivos internos
$	Identificador usado para MDM
$	MEID
$	Modelo
$	Nombre del dispositivo
$	Número de teléfono del dispositivo
$	Identificador de dispositivo único del cluster
$	Número de serie
$	iOS UDID
$	Dirección MAC de Wi-Fi

Variables de la plantilla de correo electrónico

Clave de variable	Descripción del valor
$	Cuerpo del correo electrónico
$	Asunto del correo electrónico

Variables de la marca de hora

Clave de variable	Descripción del valor
$	Marca de hora actual (milisegundos desde epoch)

Variables de plantilla de políticas

Clave de variable	Descripción del valor
$	Nombre de política infringido
$	Siguiente acción de cumplimiento en capas (distinto a esperar y retirar) que se llevará a cabo tras enviar el mensaje
$	Número de días que el dispositivo ha estado en un estado de no compatibilidad
$	La marca de hora cuando se desencadenó por primera vez la infracción de políticas (formato UTC DD-MM-AAAA)
$	Definición de la regla (Cadena de consulta tal y como aparece ahora)

Temas relacionados:

- Atributos

10.10.3. Configuraciones de App Connect

Esta sección contiene los siguientes temas:

- Introducción a AppConnect
- Código de acceso de AppConnect

10.10.3.1. Introducción a AppConnect

AppConnect es una función que coloca las aplicaciones en contenedores para proteger los datos en dispositivos iOS y Android. Cada aplicación compatible con AppConnect se convierte en un contenedor extraíble y seguro cuyos datos están cifrados y protegidos frente accesos no autorizados. Puesto que cada usuario emplea varias aplicaciones empresariales, cada contenedor está también conectado a contenedores de otras aplicaciones protegidas. Esta conexión permite a las aplicaciones compatibles con AppConnect compartir datos, como por ejemplo documentos. Ivanti Neurons for MDM emplea políticas para administrar las aplicaciones compatibles con AppConnect.

Para obtener más información acerca de AppConnect y cómo configurar e implementar aplicaciones de AppConnect, consulte la *Guía de AppConnect para Ivanti Neurons for MDM*.

Estado de las aplicaciones seguras

En la página **Dispositivos > Dispositivos**, haga clic en un dispositivo para visualizar la página **Información general**. En esta página, los usuarios pueden comprobar el estado de las aplicaciones seguras con la siguiente información:

- **Estado de las aplicaciones seguras** - indica si AppConnect está activado o desactivado.
- **Estado del cifrado de las aplicaciones seguras** - indica si el código de acceso de AppConnect está activado o desactivado.
- **Modo del cifrado de las aplicaciones seguras** - indica el modo del cifrado (como AES 256).

Además, estos campos se pueden usar:

- Como filtros (panel izquierdo) para limitar las entradas del dispositivo que se muestran cuando los usuarios están intentando encontrar/filtrar dispositivos.
- Como reglas cuando se crea un grupo de dispositivos administrados dinámicamente.
- Como filtros de distribución, que limitan los dispositivos donde se distribuirán las aplicaciones en función de las reglas definidas.

Para cada aplicación segura, los administrados pueden revisar la Política de contenedores y los estados de configuración (Instalado, Solicitado, Enviado o Pendiente de instalación) en la pestaña **Configuraciones** de la página de detalles del dispositivo.

10.10.3.2. Código de acceso de AppConnect

Esta sección contiene los siguientes temas:

- Cambiar/restablecer un código de acceso
- Generar un PIN de un solo uso para restablecer un código de acceso de Secure Apps para dispositivos iOS

Si lo desea, puede establecer que sea obligatorio un código de acceso de AppConnect, también conocido como el código de acceso de las aplicaciones seguras. Con un inicio de sesión único con el código de acceso de AppConnect, el usuario del dispositivo puede acceder a todas las aplicaciones seguras. En el Portal de administración, se pueden configurar las reglas para el código de acceso de AppConnect. El código de acceso de AppConnect no es igual que el código de acceso que se utiliza para desbloquear el dispositivo.

Cambiar/restablecer un código de acceso

Los usuarios pueden cambiar o restablecer el código de acceso para aplicaciones seguras en la aplicación Secure Apps Manager para dispositivos Android y en la aplicación Go para iOS, siempre que se haya permitido en la configuración de AppConnect. Para dispositivos iOS:

Procedimiento

1. Abra la aplicación Go para iOS.
2. Haga clic en **Secure Apps**.
3. Haga clic en **Autenticación**.
4. Haga clic en **Cambiar código de acceso de Secure Apps** y siga las instrucciones para cambiar/restablecer el código de acceso.

Para dispositivos Android:

1. Abra la aplicación Secure Apps Manager.
2. Haga clic en **Cambiar código de acceso** en el menú de opciones.
3. Haga clic en **¿Olvidó su contraseña?** para restablecer el código de acceso.

Generar un PIN de un solo uso para restablecer un código de acceso de Secure Apps para dispositivos iOS

Los administradores pueden configurar Ivanti Neurons for MDM para permitir que los usuarios de dispositivos iOS restablezcan su código de acceso de aplicaciones seguras (AppConnect) cuando se lo olviden. Cuando se configura esta opción, los usuarios de dispositivos que se registraron con Ivanti Neurons for MDM mediante un nombre de usuario y contraseña pueden introducir dichas credenciales en Go 3.1.0 para iOS o versiones más recientes compatibles para autenticarse y, a continuación, restablecer el código de acceso de sus aplicaciones seguras. No obstante, los usuarios de dispositivos que hayan olvidado la contraseña y el PIN necesitarán un mecanismo diferente para autenticarse.

Procedimiento

1. En Ivanti Neurons for MDM, el administrador activa la opción **Código de acceso de Secure Apps** en la configuración predeterminada de iOS AppConnect (o en cualquier otra configuración de iOS AppConnect).
2. El usuario genera un PIN de un solo uso para un dispositivo iOS específico en el portal de autoservicio del usuario haciendo clic en la opción **Restablecer código de acceso de Secure Apps** y siguiendo las instrucciones. El PIN de un solo uso es válido durante 30 minutos.

3. En Go para iOS en un dispositivo, el usuario sigue las instrucciones para restablecer un código de acceso olvidado de Secure Apps.
4. Cuando se le soliciten sus credenciales de usuario, este deberá introducir su nombre de usuario y el PIN de un solo uso en lugar de su código de acceso normal.
5. A continuación, el usuario podrá restablecer su código de acceso de las aplicaciones seguras.

10.10.4. Configuración de seguridad

Esta sección contiene los siguientes temas:

- Android Enterprise
- Editar la configuración predeterminada de Android Enterprise
- Configurar Android Enterprise
- Desafío de acceso (Work Challenge) de Android
- Configuración del certificado
- Transparencia del certificado
- Configuración de comprobación de revocación de certificados
- Crear configuración en modo autónomo de una única aplicación
- Creación de una configuración de proxy de DNS
- Configuración del registro de dispositivos
- Configuración del administrador de discos
- Cifrado en Android
- DNS cifrado
- Ajustes de inteligencia externa
- Defensa contra amenazas
- FileVault 2
- Clave de recuperación de FileVault
- Configuración de opciones de FileVault
- Certificado de identidad
- Configuración del Bloqueo de activación de Apple
- Configuración personalizada iOS
- Ajustes de inteligencia
- Ajustes del teclado
- Restricciones de iOS
- Visualización de la sala de conferencias
- Bloqueo y kiosco: modo de administrador de dispositivos de Android
- Configurar el modo kiosco para Android
- Configurar el kiosco del dispositivo compartido Android
- Bloqueo y kiosco: Android Enterprise
- Bloqueo y kiosco: Samsung KNOX Standard
- Firewall de macOS
- Restricciones de macOS
- Restricciones de la AppStore de macOS
- Restricciones de grabación en disco de macOS

- Control multimedia permitido (obsoleto)
- Ajustes del Finder de macOS
- Política de extensiones del kernel de macOS
- Mobile@Work para macOS
- Configuración de las reglas de actualización de software macOS
- Preferencia de certificado
- Active Directory (macOS)
- Preferencia de identidad
- Creación automática de cuentas en Office 365(macOS)
- Autenticar
- App Catalog de Apple
- Dominios administrados
- Configuración del código de acceso
- Preferencias de privacidad (macOS)
- Ajustes del cliente de Ivanti Go
- Configuración de privacidad
- Información de Declaración de la privacidad del cliente
- Configuración de los ajustes de la extensión de Safari
- Actualizaciones de software
- Configuración de los ajustes de actualización del software
- Configuración de Preferencias de Seguridad
- Ajustes de Siri
- Servidor de zona horaria
- Filtro de contenido web
- Firewall de Windows
- Protección de la información de Windows
- Restricciones de Windows
- Restricciones de Windows Desktop
- Ajustes de escritorio para Windows 10
- Configuración predeterminada de Windows Hello para empresas
- Configuración del administrador de IA de Windows
- Play Integrity (antes SafetyNet Attestation)
- Código de acceso y pantalla de bloqueo avanzados de Android
- Microsoft Defender for Endpoint
- Autenticación basada en certificado

10.10.4.1. Android Enterprise

Licencia: Silver

Una configuración de Android Enterprise define las opciones de **Android Enterprise** que están habilitadas para los dispositivos compatibles. Puede crear configuraciones alternativas para los diferentes grupos de dispositivos o simplemente editar la configuración predeterminada. Para obtener una lista de dispositivos compatibles con Android Enterprise, consulte la página oficial de **Android** .

Ajustes de Android Enterprise

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Desactive Captura de pantalla (Android 5.0 +)	Seleccione esta opción para impedir que los dispositivos usen la función nativa de captura de pantalla.
No permitir Control de aplicaciones (Android 5.0 +)	Seleccione esta opción para impedir que los usuarios modifiquen aplicaciones en Ajustes o en Selectores.
No permitir Credenciales de configuración (Android 5.0 +)	Seleccione esta opción para impedir que los usuarios configuren las credenciales del usuario.
No permitir Copiar/Pegar perfil cruzado (Android 5.0 +)	Seleccione esta opción para impedir que los dispositivos puedan copiar y pegar en otros perfiles de trabajo de Android Enterprise.
No permitir Modificar cuentas (Android 5.0 +)	Seleccione esta opción para impedir que los usuarios añadan y eliminen cuentas.
No permitir transferencia de salida (Android 5.0 +)	Seleccione esta opción para impedir que los usuarios usen NFC para transferir datos de las aplicaciones.
No permitir Compartir ubicación (Android 5.0 +)	Seleccione esta opción para impedir que los sitios web y aplicaciones soliciten al usuario del dispositivo que comparta la ubicación del dispositivo.
Restringir métodos de entrada (Android 5.0 +)	Seleccione esta opción para restringir los métodos de entrada designando una lista de nombres de paquetes permitidos. Si no hay ningún paquete en la lista de permitidos, entonces solo se permitirán los métodos de entrada del sistema. Los métodos de entrada no solo están restringidos a las aplicaciones profesionales, sino al dispositivo entero.
Restringir los servicios de accesibilidad (Android 5.0 +)	Seleccione esta opción para restringir los métodos de entrada designando una lista de nombres de paquetes permitidos. Si no hay ningún paquete en la lista de permitidos, solo se permitirán los servicios de accesibilidad del sistema. Los métodos de entrada no solo están restringidos a las aplicaciones profesionales, sino al dispositivo entero.

Ajuste	Qué hacer
Desactivar Id. de llamada (Android 6.0 +)	Establece si la información del Id. de llamada del perfil de trabajo se mostrará en el dispositivo para las llamadas entrantes.

Temas relacionados

- Configurar Android Enterprise

10.10.4.2. Atestación de Claves de Acceso de Apple

Utilice la configuración de Atestación de clave de acceso para configurar el dispositivo de manera que permita la atestación empresarial de WebAuthn para ciertas claves de acceso.

Cuando el usuario utiliza una clave de acceso para autenticarse y registrar sus dispositivos, la configuración de Atestación de clave de acceso de Apple utiliza una Credencial gestionada por la Empresa para atestiguar la clave de acceso con un certificado corporativo. Las credenciales admitidas incluyen SCEP, ACME y credenciales de identidad.

La atestación de clave de acceso admite lo siguiente:

- Versiones mínimas de sistemas operativos soportados: macOS 14
- Métodos de inscripción compatibles: inscripción de dispositivos
- Las cuentas de Apple administradas son necesarias para controlar la sincronización de claves de acceso.
- Se puede usar junto con Access Management de ABM.

> La carga útil de Passkeys falla en Mac.

Al crear una configuración de clave de acceso, primero debe crear una configuración de certificado de identidad y vincularla a la configuración de clave de acceso. Además, proporcione los detalles siguientes en la sección Configuración de Security Passkey Attestation.

Campo	Descripción
Nombre	Nombre de la clave de acceso.
Descripción	Cualquier información acerca de la configuración.
Referencia de identidad de atestación • La clave de identidad de atestación es extraíble	Proporcione la referencia de identidad del activo que ha creado para vincularla a la Configuración de clave de acceso. Seleccione esta opción para confirmar si la clave de identidad es extraíble.
Partes dependientes	Introduzca los detalles de los dominios autenticados.

10.10.4.3. Valores predeterminados de privacidad de las aplicaciones

Utilice los **valores predeterminados de privacidad de las aplicaciones** para establecer los permisos de privacidad predeterminados de las aplicaciones en dispositivos supervisados. Los administradores pueden identificar los componentes de privacidad utilizados por una aplicación, añadir la aplicación y sus componentes a la configuración y establecer los valores de privacidad predeterminados. Cuando los usuarios inician la aplicación, esta verifica los valores de privacidad configurados y les solicita que concedan los permisos, aunque también pueden posponer esta acción o gestionar los permisos posteriormente desde los ajustes del dispositivo.

Disponible para:

- iOS 27.0+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- iPad 27.0+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- macOS 27.0+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Busque y seleccione la configuración **Valores predeterminados de privacidad de las aplicaciones**.
3. En el campo **Nombre,** introduzca un nombre que identifique esta configuración.
4. En el campo **Descripción**, introduzca una descripción que explique la finalidad de esta configuración.
5. En el panel **Ajustes de configuración,** seleccione **Añadir por búsqueda**.
6. Introduzca el nombre de la aplicación para la que desea configurar los **valores predeterminados de privacidad** y seleccione una de las siguientes opciones:

- Tienda de iOS
- Catálogo de aplicaciones
- visionOS Store
- Tienda de OS X (macOS)

> Puede seleccionar varias aplicaciones.

7. (Opcional) Seleccione **Añadir manualmente** para seleccionar una aplicación.
8. (Opcional) Introduzca el **nombre del paquete** de la aplicación.
9. (Opcional) Haga clic en **Añadir aplicación**.
10. Seleccione **Ver aplicación**.

El panel **Ver aplicación** muestra todas las aplicaciones seleccionadas.

11. Haga clic en **Añadir valores predeterminados** en cada aplicación para configurar individualmente los valores predeterminados de privacidad.

Aparecerá el panel **Añadir valores predeterminados**.

12. Selecciones los **valores predeterminados** y las **restricciones** según la siguiente tabla:

Valores predeterminados	Configurar restricciones
Cámara	Seleccione una de las siguientes opciones: • Permitir • Ninguno
Bluetooth	Seleccione una de las siguientes opciones: • Permitir • Ninguno
Accesibilidad	Seleccione una de las siguientes opciones: • Permitir • Ninguno
Dictado	Seleccione una de las siguientes opciones: • Permitir • Ninguno
Micrófono	Seleccione una de las siguientes opciones: • Permitir • Ninguno
Ubicación	Seleccione una de las siguientes opciones: • Al usar la aplicación • Ninguno • Siempre
Precisión de ubicación	Seleccione una de las siguientes opciones: • Aproximada • Precisa • Ninguno
Red local	Seleccione una de las siguientes opciones: • Permitir • Ninguno
Justificación de la organización	El aviso de **Justificación de la organización** puede mostrar el nombre de la organización y de la aplicación, la justificación proporcionada por el administrador y los detalles de cada componente, junto con el valor predeterminado de privacidad recomendado Si el usuario selecciona **Permitir**, el sistema aplica a los valores predeterminados de privacidad recomendados. Si el usuario selecciona **Ahora no**, se muestran avisos de consentimiento cuando la aplicación accede a los componentes especificados del dispositivo del usuario.

13. Haga clic en **Guardar**.
14. Haga clic en **Siguiente** para configurar los ajustes de distribución.

15. Seleccione una de las opciones de distribución para configurar los **valores predeterminados de privacidad de las aplicaciones**. Para más información sobre la configuración de las opciones de distribución, consulte **Trabajar con configuraciones**.
16. Haga clic en **Hecho**.

10.10.4.4. Editar la configuración predeterminada de Android Enterprise

Los Administradores globales pueden permitir que los administradores de espacio editen la distribución de cualquier configuración predeterminada de Android Enterprise en el espacio personalizado.

- Android Enterprise: perfil de trabajo en un dispositivo de la empresa (Android for Work)
- Android Enterprise: dispositivo administrado en el trabajo (Android for Work)
- Android Enterprise: dispositivo administrado con perfil de trabajo
- Android enterprise: AOSP

Editar la distribución para cualquiera de las configuraciones anteriores

Procedimiento

1. En la pestaña Configuraciones, seleccione la configuración que se va a editar.
2. Haga clic en el icono Editar.
3. Haga clic en **Siguiente**.
4. Seleccione cualquiera de los niveles siguientes de distribución para editar y configurar desde la página de distribución:
    - **Todos los dispositivos**: seleccione una de las opciones siguientes para distribuir la configuración en todos los dispositivos compatibles:
        1. No aplicar a otros espacios
        2. Aplicar a los dispositivos de otros espacios.
    - **Ningún dispositivo** (por defecto)
    - **Personalizado**: seleccione una de las opciones siguientes para distribuir la configuración en todos los dispositivos o usuarios compatibles:
        1. **Usuario/Grupos de usuarios**: seleccione la casilla que hay junto a los usuarios o grupos de usuarios. También puede escribir y buscar los usuarios o grupos de usuarios.
        2. **Dispositivos/Grupos de dispositivos**: seleccione la casilla que hay junto a los dispositivos o grupos de dispositivos. También puede escribir y buscar los dispositivos o grupos de dispositivos.
           En el **Resumen de distribución**, seleccione una de las opciones siguientes para activar o desactivar las configuraciones de todos los espacios:
            - No aplicar a los otros espacios.
            - Aplicar a los dispositivos de otros espacios.

            > La casilla de verificación **Permitir que el administrador del espacio edite la distribución** aparece si selecciona la opción **Aplicar a dispositivos de otros espacios**, y permite que los administradores del espacio delegados editen la distribución para el espacio específico.

> Si edita la opción de distribución, debe seleccionar la casilla de verificación "**Entiendo que cambiar la distribución de la configuración del modo Android Enterprise-Device puede hacer que los dispositivos se eliminen o se borren si se elimina la configuración de los dispositivos existentes**".

5. Haga clic en **Hecho**.

Cuando esta configuración se aplique a los espacios, los administradores del espacio podrán editar la distribución haciendo clic en el icono de distribución en el espacio personalizado.

10.10.4.5. Configurar Android Enterprise

Esta sección contiene el siguiente tema:

- Dispositivos compatibles
- Conectar Ivanti Neurons for MDM con Android Enterprise
- Obtener sus credenciales de Android Enterprise
- Añadir su token de MDM de Android Enterprise a Ivanti Neurons for MDM
- Sincronización de usuario entre Ivanti Neurons for MDM y Google
- Usuarios de Active Directory/LDAP
- Usuarios locales
- Despliegue de Android Enterprise en dispositivos compatibles
- Eliminar los dispositivos registrados
- Instalar el dispositivo
- Confirmar la instalación
- Instalar las aplicaciones Android Enterprise
- Configuración de Aplicaciones corporativas

Licencia: Silver

Android Enterprise es un programa que ofrece Google y que permite a los administradores de movilidad:

- Separar los datos profesionales y personales
- Asegurar y administrar aplicaciones corporativas
- Controlar aplicaciones del sistema (como la Cámara y Galería)
- Aprovisione centralmente y configure las aplicaciones del contenedor de Android Enterprise
- Evitar pérdida de datos (captura de pantalla)

Puede configurar Ivanti Neurons for MDM como el servidor de UEM que administra Android Enterprise. Android Enterprise requiere al menos Android 3.0. Hay dos configuraciones compatibles para Android Enterprise: Propietario del dispositivo y Perfil administrado: perteneciente a un empleado.

Dispositivos compatibles

Ivanti Neurons for MDM actualmente, es compatible con Android Enterprise solo en dispositivos que utilicen Android 5.0 y en los que el fabricante haya habilitado Android Enterprise. Android Enterprise es necesario para el modo kiosko en los dispositivos con Android 5.0.

Requisito previo

Si todavía no ha registrado su dominio con Google, primero debe inscribirse en el programa en el sitio web de Google:

https://admin.google.com.

Durante este proceso, usted:

- Reclamará un dominio (debe coincidir con el dominio para las direcciones de correo electrónico del usuario)

- Recibirá un token
- Descargará una Id. de cliente JSON

Ambos elementos son necesarios cuando se ajusta Android Enterprise en Ivanti Neurons for MDM.

Tras el proceso, recibirá un correo electrónico con instrucciones para verificar que el dominio que ha reclamado es suyo.

Si la empresa ya ha usado este nombre de dominio para registrarse en Google Apps for Work, consulte https://support.google.com/work/android/answer/6174062 para obtener información sobre cómo habilitar Android Enterprise.

Conectar Ivanti Neurons for MDM con Android Enterprise

Una vez haya iniciado sesión en Android Enterprise, ajuste Ivanti Neurons for MDM como servidor UEM.

Obtener sus credenciales de Android Enterprise

Procedimiento

1. Vaya a **Administrador > Android Enterprise**.
2. Haga clic en **Consola de Google Developers**.
3. Haga clic en el primer enlace que aparezca para ir hasta la consola de Google Developers.
4. Seleccione **Crear un proyecto** del menú desplegable.
5. Introduzca un nombre para el proyecto.
6. Acepte los términos de servicio.
7. Haga clic en **Crear**.
8. Haga clic en **API**.
9. Seleccione las **API**.
10. Escriba **emm** en el campo de búsqueda para encontrar la EMM de Google Play.
11. Haga clic en el enlace de la **API de EMM de Google Play** .
12. Haga clic en **Habilitar API**.
13. Haga clic en **Credenciales**.
14. Seleccione **Cuenta de servicio** el.
15. Haga clic en **Crear** para guardar el archivo JSON.

Añadir su token de MDM de Android Enterprise a Ivanti Neurons for MDM

Procedimiento

1. Inicie sesión en https://admin.google.com.
2. Haga clic en **Seguridad**.
3. Si no ve los Ajustes de Android Enterprise, haga clic en **Mostrar más**.
4. Seleccione **Ajustes de Android Enterprise**.
5. En **Administrar el proveedor de administración de movilidad empresarial**, copie el token de MDM.
6. Volver al portal de Ivanti Neurons for MDM.
7. Haga clic en **Listo**.

8. En el cuadro 2, pegue el token de MDM que acaba de copiar.
9. En el campo **Dominio**, ingrese el dominio que le reclamó a Google.
10. Haga clic en **Elegir archivo** y cargue el archivo JSON que descargó.
11. Haga clic en **Conectar**.
    Aparece el mensaje **Conectado a Google** cuando se logra la conexión correcta.
12. En la caja 3, haga clic en **Autorizar** para indicar que desea dar acceso a Ivanti Neurons for MDM a sus datos de usuario de Google.
13. Haga clic en **Aceptar**.
    Se muestra el mensaje **Conectado a usuarios** en el portal de Ivanti Neurons for MDM.

Sincronización de usuario entre Ivanti Neurons for MDM y Google

Antes de desplegar Android Enterprise en los usuarios de Android que se administran en Ivanti Neurons for MDMIvanti Neurons for MDM, cada usuario debe tener un registro correspondiente en el Portal de administración de Google. Los pasos necesarios para sincronizar la información del usuario entre Ivanti Neurons for MDM y el portal de administración de Google dependen de que haya ajustado una integración con los servicios del directorio de su empresa (AD/LDAP).

Usuarios de Active Directory/LDAP

Si tiene configurada una integración AD/LDAP con Ivanti Neurons for MDM, debe usar la sincronización del directorio de aplicaciones de Google para configurar una integración de AD/LDAP con el portal administrativo de Google. Consulte https://support.google.com/a/answer/106368?hl=en para obtener más información.

Usuarios locales

Si ha creado usuarios solo locales en Ivanti Neurons for MDM y no pretende integrarlo con un servicio de directorio, complete los pasos siguientes para sincronizar esos usuario con el portal administrativo de Google.

Procedimiento

1. Inicie sesión en el portal de administración de Google en https://admin.google.com.
2. Haga clic en **Usuarios**.
3. Haga clic en el icono **Añadir usuario** o **Añadir varios usuarios** situado en la esquina inferior derecha.
4. Para cada usuario de Ivanti Neurons for MDM que utilizará Android Enterprise, agregue un usuario de Google con el mismo nombre de usuario y dirección de correo electrónico que el usuario de Ivanti Neurons for MDM.
5. En el portal de Ivanti Neurons for MDM por cada usuario de Ivanti Neurons for MDM que se agregó al portal de administración de Google:
   a. Haga clic en el enlace del nombre del usuario de la pestaña Usuarios para mostrar la página de detalles del usuario.
   b. Seleccione **Sincronizar el usuario con el directorio de usuarios de Google.**
   c. Haga clic en **Sincronizar con el directorio de usuarios de Google**.
   d. Confirme que Google Status está listado como Habilitado.

Despliegue de Android Enterprise en dispositivos compatibles

Son necesarias dos configuraciones para desplegar Android Enterprise:

- Android Enterprise: la configuración de un perfil de trabajo en un dispositivo de la empresa activa Android Enterprise.

- Una configuración de Bloqueo y Kiosko define las restricciones de Android Enterprise que se van a aplicar.

Eliminar los dispositivos registrados

En escenarios de BYOD, trasladar de un perfil de Administrador de dispositivos a uno profesional de Android Enterprise en un dispositivo propiedad de la empresa no requiere que se retiren y se vuelvan a inscribir los dispositivos. El borrado o retirada del dispositivo solo son necesarios para pasar del modo Administrador del dispositivo al de Propietario del dispositivo.

Cuando se selecciona un dispositivo inscrito en modos Propietario del dispositivo / Propietario de perfil mejorado / Propiedad de la empresa activados de manera personal para la acción Retirar, aparece una ventana emergente en la pantalla que indica que "El comando Retirar no es compatible con los dispositivos que son propiedad de la empresa".

Instalar el dispositivo

Procedimiento

1. En el portal de Ivanti Neurons for MDM, vaya a **Configuraciones**.
2. Haga clic en **Android Enterprise: perfil de trabajo**.
3. Haga clic en **Editar**.
4. Haga clic en **Siguiente**.
5. Seleccione **Todos los dispositivos** o **Personalizado**.
6. Si seleccionó **Personalizado**, busque y seleccione los grupos de dispositivos que deberían recibir los ajustes de Android for Work.
7. Haga clic en **Listo**.
8. Haga clic en **Volver a la lista** (esquina superior izquierda).
9. Haga clic en **+Agregar**.
10. Haga clic en **Bloqueo y kiosko: Android Enterprise**.
11. En el campo **Nombre**, ingrese el texto que identifica la configuración.
12. En **Elegir tipo de bloqueo**, seleccione **Perfil de trabajo**.
13. Seleccione los ajustes de bloqueo que desee aplicar a los dispositivos de destino.
14. Haga clic en **Siguiente**.
15. Seleccione **Todos los dispositivos** o **Personalizado**.
16. Si seleccionó Personalizado, busque y seleccione los grupos de dispositivos que deberían recibir los ajustes de Android Enterprise.
17. Haga clic en **Listo**.

> No se pueden realizar cambios en el perfil resultante una vez que haya sido implementado. En lugar de esto, debe crear una nueva configuración de Android Enterprise y desplegarla.

Confirmar la instalación

Puede confirmar que Android Enterprise se ha desplegado de las maneras siguientes:

- En **Usuarios > Usuarios**, encuentre la entrada para un usuario determinado y, a continuación, compruebe que el **Estado de Google** esté **Habilitado**.

- En **Dispositivos > Dispositivos,** haga clic en el enlace de un dispositivo, y a continuación compruebe que el estado de **Android Enterprise** es **Habilitado**.

El **Estado de Google** del usuario debe aparecer como **Habilitado**. Si no está Habilitado, el usuario no podrá registrar los dispositivos.

> Para empresas que no estén suscritas a GSuite, el método de Cuentas de Google Play administradas permite a los usuarios inscribirse con Android Enterprise. Si Android Enterprise se configuró como Cuentas de Google Play administradas, el usuario no se mostrará como **Estado de Google: Habilitado** hasta que se haya registrado el dispositivo de Android Enterprise. Consulte Cuentas de Google Play administradas para obtener más información sobre las cuentas de Google Play administradas.

Instalar las aplicaciones Android Enterprise

Cualquier aplicación desarrollada para Android Enterprise puede incluir las opciones que puede configurar a través de Ivanti Neurons for MDM.

Procedimiento

1. En el portal de Ivanti Neurons for MDM, vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Encuentre la aplicación en la Google Play Store.
3. Haga clic en la entrada de la aplicación.
4. Acepte los permisos en nombre de los usuarios de Android Enterprise.
5. Haga clic en **Siguiente**.
6. Seleccione una opción de distribución.
7. Amplíe **Opciones avanzadas y configuración de aplicaciones**.
8. Siga las siguientes pautas para completar las opciones:
9. Haga clic en **Siguiente**.

Ajuste	Descripción
Instalar en dispositivo	Seleccione esta opción para iniciar la instalación inmediatamente después del registro. Se pedirá al usuario que confirme la instalación de la aplicación, excepto cuando el dispositivo sea un dispositivo Samsung Knox y se haya seleccionado la opción de instalación silenciosa que figura a continuación.
No mostrar la aplicación en el App Catalog del usuario final	Seleccione esta opción si no desea que el usuario vea la aplicación en el catálogo de aplicaciones del dispositivo.
Instalar de forma silenciosa en dispositivos Samsung Knox	Seleccione esta opción si no desea que se solicite al usuario que confirme la instalación en dispositivos Samsung KNOX.
Establecer la prioridad de instalación de las aplicaciones	Para las aplicaciones de Android Enterprise, puede priorizar la descarga de aplicaciones específicas antes que otras aplicaciones. Por ejemplo, se puede priorizar la descarga de las aplicaciones Tunnel y Email antes que otras aplicaciones no tan importantes. A continuación se enumeran las opciones de nivel de prioridad disponibles: • **Alto** • Media (seleccionada por defecto) • **Baja** Este ajuste se puede aplicar en aplicaciones internas, públicas, privadas y de Web. Las aplicaciones internas se instalan a través del cliente y las públicas y privadas se instalan a través de Google. La prioridad de las aplicaciones se aplica solo a las aplicaciones que se instalan a través del mismo canal.
Instalar solo cuando esté conectado a Wi-Fi	Seleccione esta opción para instalar la aplicación solo cuando el dispositivo esté conectado a la Wi-Fi.
Instalar solo cuando esté cargando	Seleccione esta opción para instalar la aplicación solo cuando la carga del dispositivo esté en curso.
Instalar solo cuando esté inactivo	Seleccione esta opción para instalar la aplicación solo cuando el dispositivo esté inactivo (no utilizado activamente por el usuario).
Lanzamiento automático al instalarlo	Seleccione esta opción para iniciar una app automáticamente después de su instalación. Esta funcionalidad solo está disponible si la aplicación está recién instalada en el dispositivo y no para una actualización de versión.

10. Seleccione una opción de promoción.
11. Haga clic en **Hecho**.

Configuración de Aplicaciones corporativas

Las aplicaciones de Android Enterprise están disponibles en la sección de Aplicaciones de empresa del catálogo de aplicaciones, incluidas las aplicaciones siguientes.

- **Divide Productivity**
- Correo electrónico+
- Túnel
- Gmail

10.10.4.6. Android Enterprise: modo no GMS para el dispositivo administrado en el trabajo (AOSP)

Ivanti Neurons for MDM admite el registro de propietarios de dispositivos en modo Work Managed Device Non-GMS (AOSP) sin necesidad de Google Mobile Services (GMS). Es una configuración del sistema y los administradores no pueden añadir la configuración. Los administradores pueden distribuirla o no distribuirla.

Procedimiento

1. Inicie sesión en Ivanti Neurons for MDM con las credenciales del usuario.
2. Configuraciones de búsqueda para Android Enterprise: Work Managed Device Non-GMS mode (AOSP).
3. Edite la configuración y distribúyala a los grupos de dispositivos adecuados. Por ejemplo: dispositivos Android.
4. Haga clic en **Hecho**.

10.10.4.7. Desafío de acceso (Work Challenge) de Android

Esta sección contiene el siguiente tema:

- Crear una configuración del Desafío de acceso (Work Challenge) de Android:
- Ajustes del establecimiento de la configuración

Licencia: Silver

La configuración del Desafío de acceso (Work Challenge) de Android define las contraseñas seguras para que los usuarios accedan a los datos y las aplicaciones del Perfil de trabajo. Requiere el perfil de trabajo de Android Enterprise.

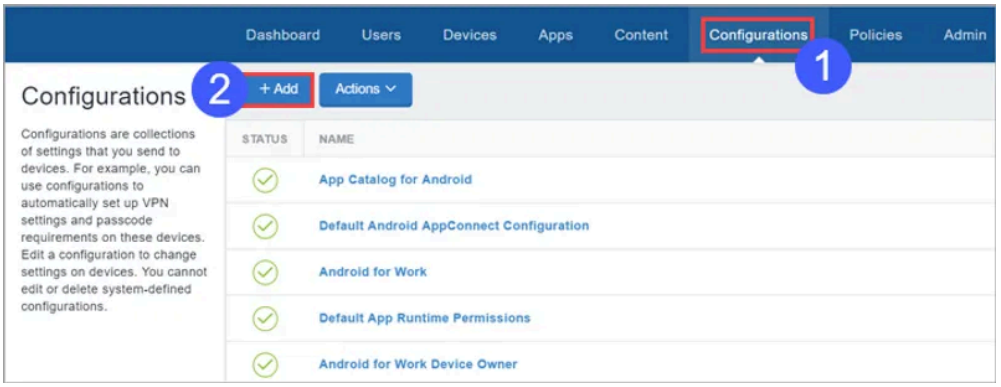
Notas sobre la implementación:

- Los administradores pueden aplicar una política de contraseña del dispositivo y otra política de contraseña del perfil de trabajo de forma independiente.
- Ivanti Neurons for MDM no enviará esta configuración a los clientes con una versión anterior a Android 7.0 porque tales dispositivos no admiten esta característica.
  Ivanti Neurons for MDM solo envía esta configuración a los dispositivos con un perfil de trabajo empresarial Android.

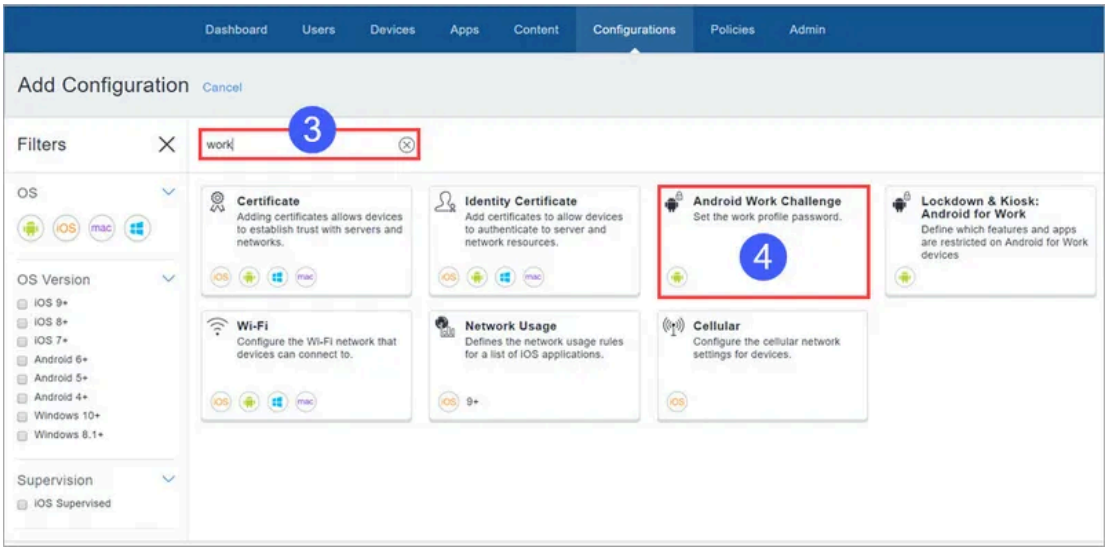
Crear una configuración del Desafío de acceso (Work Challenge) de Android:

Procedimiento

1. Haga clic en **Configuraciones**.

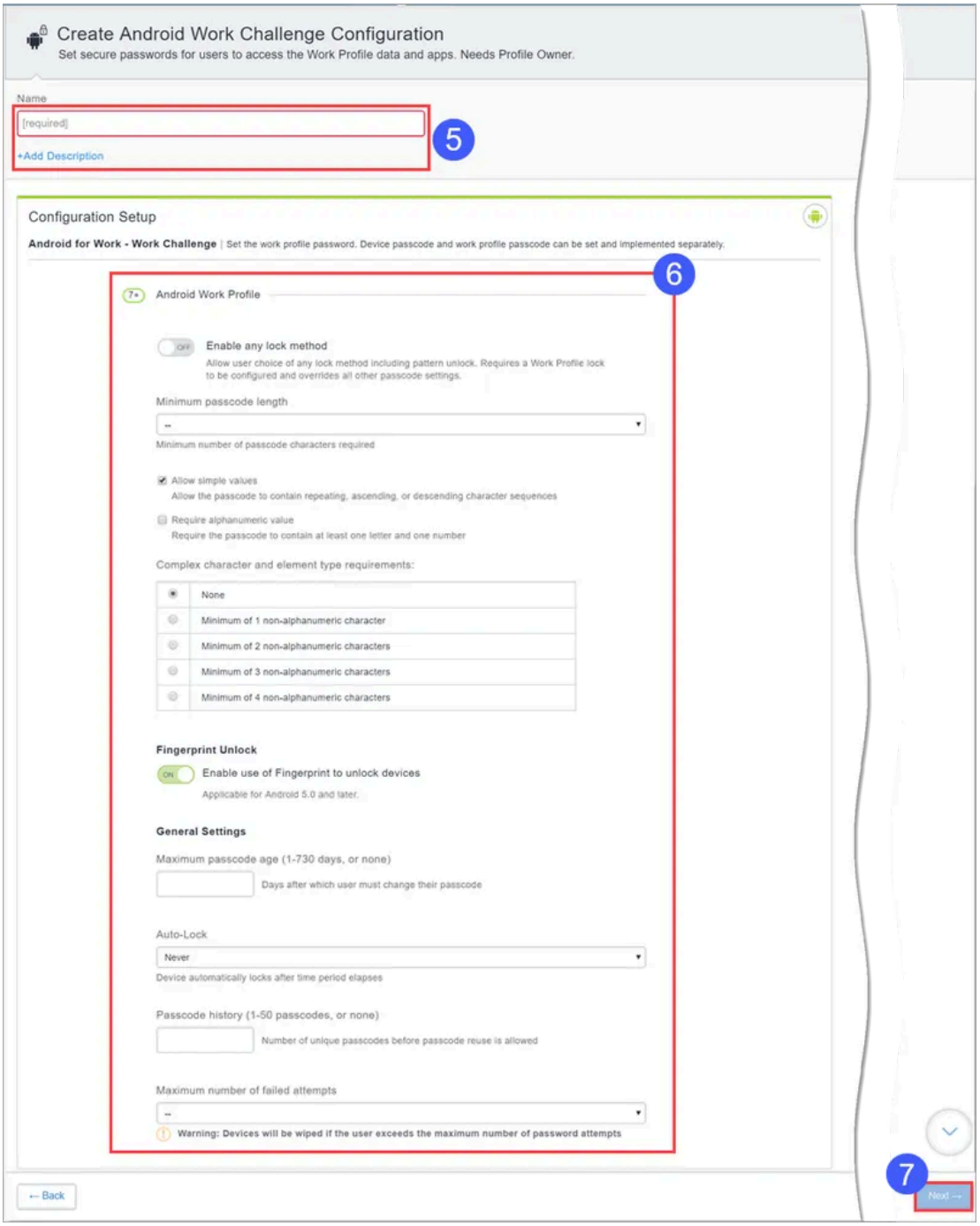


Haga clic en **+Añadir**.



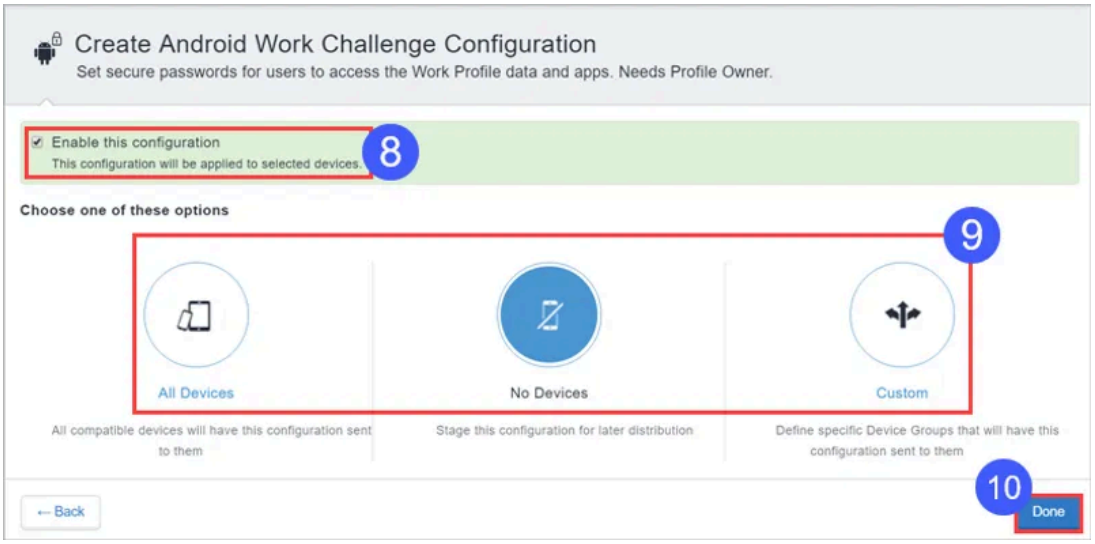
Escriba "work" ("trabajo") en el campo de búsqueda.

4. Seleccione la configuración **Desafío de acceso (Work Challenge) de Android**.



Introduzca un nombre para la configuración y, si lo desea, una descripción.

6. Utilice los campos de Ajustes de la configuración para crear la configuración. Consulte **Ajustes del establecimiento de la configuración** para ver detalles sobre los ajustes.
7. Haga clic en **Siguiente →**.



Habilite la configuración si fuera necesario.

9. Configure los ajustes de distribución para todos los dispositivos, ningún dispositivo o un conjunto personalizado
10. Haga clic en **Hecho**.

Ajustes del establecimiento de la configuración

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Activar cualquier método de bloqueo	Permitir que el usuario elija cualquier método de bloqueo, incluido el desbloqueo mediante patrón. Anula cualquier otro ajuste del código de acceso.
Longitud mínima del código de acceso	Seleccione una longitud mínima del código de acceso, de 4 a 16 caracteres.
Permitir valores simples	Habilite esta opción para permitir que el código de acceso tenga secuencias de caracteres repetidos, ascendentes o descendentes.
Requerir valor alfanumérico	Habilite esta opción para requerir que el código de acceso tenga al menos una letra y un número.
Características de caracteres complejos y tipo de elementos	Configure los requisitos de los caracteres complejos y los tipos de elemento, que varían entre: • Ninguno • Un carácter no alfanumérico como mínimo • 2 caracteres no alfanuméricos como mínimo • 3 caracteres no alfanuméricos como mínimo • 4 caracteres no alfanuméricos como mínimo
Desbloqueo de huella digital	Habilite esta opción para permitir que los usuarios desbloqueen sus dispositivos con su huella digital.
Antigüedad máxima del código de acceso	Configure una antigüedad máxima para la contraseña, desde ninguna hasta 730 días.
Autobloqueo	Seleccione un período de tiempo después del cual el dispositivo se autobloquea. Los períodos de tiempo varían de nunca a quince minutos.
Historial del código de acceso	Especifique el número de códigos de acceso exclusivos necesarios antes de que se permita volver a usar el código de acceso, que varía de ninguno a 50 códigoa de acceso.
Número máximo de intentos erróneos	Seleccione el número máximo de intentos erróneos. **ADVERTENCIA: Ivanti Neurons para MDM borra los dispositivos para los que el usuario supera el número máximo de intentos de contraseña.**

10.10.4.8. Configuración del certificado

La configuración del certificado identifica el certificado que se va a distribuir a los dispositivos. Los certificados permiten a los dispositivos establecer confianza con los servidores y los recursos de red. A partir de la versión 76 solo admitimos certificados v3.

Como administrador, ahora puede generar certificados Ivanti Neurons for MDM para el inicio de sesión con tarjeta inteligente e Id. de objetos del cliente (OID). Puede generar certificados para las siguientes opciones de autenticación:

- Autenticación de cliente - habilitada de modo predeterminado.
- IPSEC - opcional, el administrador puede habilitarlo.
- Inicio de sesión con tarjeta inteligente - opcional, el administrador puede habilitarlo.
- OID personalizados: opcional, el administrador puede habilitarlos.

Esta función es aplicable solo para las siguientes entidades de certificación:

- Entidad de Certificación local
- Entidad de certificación intermedia
- Entidad de certificación externa: configure las políticas de aplicación de la plantilla de CA en el servidor NDES para que admita IPSEC, Inicio de sesión con tarjeta inteligente y OID personalizados.
- Autoridad de certificación SCEP local

Distribución de la configuración

A partir de la versión 91 de Ivanti Neurons for MDM, los administradores globales pueden delegar en los administradores de espacio la edición de la Configuración de certificados para todos los dispositivos y para la opción de distribución personalizada. Para los certificados generados dinámicamente, puede seleccionar opcionalmente la opción Permitir que esta configuración esté disponible en todos los espacios. Esta opción hace que la configuración de los certificados estén disponibles en todos los espacios y puedan utilizarse en Exchange, Wi-Fi, VPN, VPN por aplicación y cualquier otra configuración aplicable. Esta opción se puede usar en situaciones en las que solo es necesario configurar el certificado para distribuirlo en los dispositivos (en espacios no predeterminados) como parte de configuraciones asociadas y no como configuración individual.

Procedimiento

1. Introduzca un nombre en el campo Nombre.
2. Cargar el archivo del certificado.
3. Haga clic en **Siguiente**.
4. Seleccione la opción **Habilitar esta configuración**.
5. Seleccione una de las siguientes opciones de distribución:
    - **Todos los dispositivos**. Seleccione una de las siguientes opciones:
        - **No aplicar a los otros espacios**.
        - **Aplicar a todos los dispositivos de otros espacios**.
            - Seleccione la casilla de verificación **Permitir que el administrador del espacio edite la distribución** para permitir que los administradores delegados del espacio editen la distribución para el espacio específico.
    - **Ningún dispositivo** (predeterminada)

- **Personalizar**Seleccione una de las siguientes opciones:
  - **No aplicar a los otros espacios**.
  - **Aplicar a todos los dispositivos de otros espacios**.
    - Seleccione la casilla de verificación **Permitir que el administrador del espacio edite la distribución** para permitir que los administradores delegados del espacio editen la distribución para el espacio específico.

> Independientemente de los espacios, la configuración del certificado puede configurarse en todos los espacios, distribuirse a todos los dispositivos y aplicarse a todos los dispositivos en otros espacios de dispositivos.

6. Haga clic en **Hecho**.

Ajustes del certificado

Como administrador, puede configurar una autoridad de certificación local que no sea SCEP.

Procedimiento

1. Inicie sesión en el portal del administrador de Ivanti Neurons for MDM
2. Vaya a **Admin** > **Infraestructura** > **Gestión de certificados** > **Entidad de certificación**.
3. Haga clic en **+Añadir**. Las siguiente opciones están disponibles:

- **Crear la entidad de certificación local proporcionada por Ivanti Neurons for MDM**.
- **Conecte el CA local de Ivanti Neurons for MDM con su CA existente**.
- **Conectar con una autoridad de certificados de Cloud de confianza pública**.
- **Conectar una autoridad de certificación SCEP local**.
- **Conectar una autoridad de certificación distinta a SCEP local**.

4. Complete los siguientes campos según corresponda:
5. Haga clic en **Hecho**.

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
URL	URL de la CA de OpenTrust que el administrador debe obtener de OpenTrust.
Contraseña	Introduzca la contraseña del certificado de autenticación
Certificado de autenticación	Acepta el formato de archivo .p12 proporcionado por OpenTrust/ IDnomic.
Cadena de certificados TLS CA	Acepta el formato de archivo PEM proporcionado por OpenTrust/ IDonomic.

Después de configurar la autoridad de certificación no SCEP local, debe crear el certificado de identidad. Basándose en el ID del perfil, rellene todos los campos obligatorios para completar la configuración.

> Se genera una notificación cuando falla la generación de Certificados CA SCEP debido a los siguientes dos motivos y se supera el tiempo de espera de la Fase 2:

1. No es posible alcanzar el conector

2. No es posible alcanzar el servidor de CA

10.10.4.9. Transparencia del certificado

Aplicable a: iOS 12.1.1, macOS 10.14.2, tvOS 12.1.1, watchOS 10.0+, visionOS 1.1+ y versiones más recientes compatibles.

Controla que se cumpla la transparencia del certificado, que solo puede aparecer en el perfil del dispositivo. Puede incluir múltiples certificados y desactivar dominios según sea necesario.

Creación de la configuración de la transparencia del certificado

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **certificado** en el campo de búsqueda y, a continuación, haga clic en la configuración de la **Transparencia del certificado**.
4. Introduzca un nombre y describa la configuración.
5. Especifique los **Dominios que se desactivarán**. Haga clic en **+ Añadir dominio** para añadir más de un dominio. Se puede usar un punto inicial para hacer coincidir subdominios, no obstante, una regla de coincidencia de dominios no debe coincidir con todos los dominios de un dominio de nivel superior. Por ejemplo, están permitidos «.ejemplo.com» y «.example.co.uk», mientras que «.com» y «.co.uk» no están permitidos. No se admiten los dominios de comodines.
6. Especifique el **Hash del certificado**después de seleccionar un algoritmo (SHA 256). Haga clic en **+ Añadir** para añadir más de un hash del certificado.
7. Haga clic en **Siguiente** para configurar los ajustes de distribución.
8. Haga clic en **Hecho**.

Para generar los datos especificados por la clave hash en el diccionario subjectPublicKeyInfo, utilice el siguiente comando para un certificado cifrado con PEM:

```
openssl x509 -pubkey -in example_certificate.pem -inform pem | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

Si su certificado está codificado mediante DER, use el siguiente comando:

```
openssl x509 -pubkey -in example_certificate.der -inform der | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.4.10. Configuración de comprobación de revocación de certificados

Esta configuración permite a los administradores comprobar una serie de certificados revocados de un dispositivo. Los administradores pueden especificar una autoridad de certificación (CA) que permite que la configuración habilite la comprobación de revocación para todos los certificados que están vinculados a esa CA.

Aplicable a: iOS 14.2+ y visionOS 1.1+

Procedimiento

1. Vaya a Configuraciones > +Añadir.
2. Escriba certificado en el campo de búsqueda y, a continuación, haga clic en la configuración de Configuración de comprobación de revocación de certificado.
3. Introduzca un Nombre y Descripción de la configuración.
4. Seleccione un algoritmo como SHA 256 e introduzca la Hash del certificado raíz.

> En Hash, tiene que introducir un hash SHA-256 codificado en Base64 (binario) de la clave pública del certificado. Consulte **Documentación de Apple** para los certificados de raíz confiable de los sistemas operativos Apple. Puede añadir varios certificados raíz en esta configuración.

5. Haga clic en Siguiente.
6. Seleccione la opción Habilitar esta configuración.
7. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - Personalizado.
8. Haga clic en Hecho.

10.10.4.11. Crear configuración en modo autónomo de una única aplicación

La configuración le permite asegurarse de que solo se ejecutan aplicaciones específicas en un dispositivo. Aunque el usuario intente iniciar una aplicación distinta, la configuración solo iniciará la aplicación específica.

Procedimiento

1. Vaya a **Configuraciones** > **Agregar** > **Modo autónomo de aplicación única**.
2. Siga las siguientes pautas para definir la aplicación y los ajustes relacionados.
3. Haga clic en **Siguiente**.

Ajuste	Qué hacer
Nombre,	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Establecimiento de la configuración	**Identificador de grupo**: (requerido) el identificador único del grupo. Si dos diccionarios contienen el mismo valor BundleIdentifier pero un valor TeamIdentifier distinto, se considerará un error y el perfil no se instalará.
	Identificador de Team: (requerido) el identificador del equipo del desarrollador, que se usó cuando se firmó la aplicación.

4. En la pantalla **Distribución**, seleccione los grupos que recibirán esta configuración.
5. Haga clic en **Hecho**.

10.10.4.12. Creación de una configuración de proxy de DNS

Como administrador de Ivanti Neurons for MDM, puede configurar los ajustes del proxy de DNS mediante la Configuración de proxy de DNS para usuarios de dispositivos de iPhone y de iPad. Puede usar la carga útil del proxy DNS para especificar la aplicación que proporciona la extensión de red del proxy DNS y otros valores específicos del proveedor.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Vaya a **Configuraciones**
3. Escriba **DNS** en el campo de búsqueda y haga clic en la **configuración del proxy de DNS**.
4. Introduzca un nombre y describa la configuración.
5. Introduzca los siguientes ajustes de Configuración del proxy de DNS:
    - Identificador de paquetes de aplicaciones (Requerido).
    - Identificador del grupo de proveedores
    - Configuración del proveedor (Valor de la clave).
6. Haga clic en **Siguiente**.
7. Seleccione la opción **Habilitar esta configuración**.
8. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - personalizada

Haga clic en **Hecho**.

10.10.4.13. Configuración del registro de dispositivos

La configuración de Registro de dispositivos le permite activar los registros de red y seguridad en dispositivos Android.

Creación de la configuración del registro de dispositivos

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. En el campo de búsqueda,escriba **Registro de dispositivos** y seleccione la configuración.
4. Introduzca un nombre y describa la configuración.
5. En la sección **Ajustes de configuración**, seleccione una opción o ambas:
    - Activar el registro de red
    - Registro de informes de seguridad

> Para obtener información sobre las versiones de Android compatibles con el registro de seguridad y de red, consulte las tablas en **Matriz de registro de seguridad** a continuación.

Haga clic en **Siguiente** para configurar los ajustes de distribución.

7. Haga clic en **Hecho**.

Matriz de informes de seguridad

Tipo de dispositivo	Versiones compatibles de Android
Dispositivos gestionados para el trabajo y Work Managed Device Non-GMS mode (AOSP)	7, 8, 9, 10, 11, 12, 13
Dispositivos administrados con perfil profesional	8, 9, 10
Perfil de trabajo	N/A
Perfil de trabajo en el Dispositivo propiedad de la empresa	11, 12, 13

Matriz de registros de red

Tipo de dispositivo	Versiones compatibles de Android
Dispositivos gestionados para el trabajo y Work Managed Device Non-GMS mode (AOSP)	8, 9, 10, 11, 12, 13
Dispositivos administrados con perfil profesional	8, 9, 10
Perfil de trabajo	12, 13
Perfil de trabajo en el Dispositivo propiedad de la empresa	12, 13

Después de instalar la Configuración de registro de dispositivos en el dispositivo, el usuario recibe una notificación con información sobre la Administración de dispositivos y el registro de redes. Haga clic en **Aceptar** para confirmar la notificación.

Solicitar registros de depuración

Procedimiento

1. Inicie sesión en el Ivanti Neurons for MDM.
2. Vaya a **Dispositivos** >**Detalles del ispositivo**.
3. Desde la sección **Información general**, haga clic en el botón con tres puntos verticales que aparece junto al botón de **Forzar contacto**.
4. Seleccione **Solicitar registros de Debug**.
5. Seleccione una de las dos opciones siguientes:
    - Excluir informe de errores: cuando se selecciona esta opción y se hace clic en Siguiente, aparece en la pantalla una ventana de confirmación. Haga clic en **Solicitar registros de depuración**. Los usuarios no deben dar consentimiento para esta opción y estos registros excluirán la notificación de errores para los dispositivos Android seleccionados.
    - Incluir informe de errores: cuando se selecciona esta opción y se hace clic en Siguiente, aparece en la pantalla una ventana de confirmación. Haga clic en **Solicitar registros de depuración**. Los usuarios deben dar el consentimiento para compartir un informe de errores. En el caso de dispositivos Android, se avisará a los usuarios de que deben enviar los informes del dispositivo, que deben incluir informes de errores.

10.10.4.14. Configuración del administrador de discos

Ivanti Neurons for MDM Los parámetros de configuración de la Gestión de discos definen las políticas para gestionar eficazmente los datos en dispositivos de almacenamiento externos y de red.

Aplicable a: macOS 15.0 hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Busque y seleccione la configuración de **Gestión de discos**.
3. Configure los ajustes de **Gestión de discos** según la tabla siguiente:

Ajuste	Descripción
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Gestión de discos	
Almacenamiento externo	Seleccione uno de los valores siguientes de la lista desplegable: • **Permitido**: Permite la lectura y escritura del almacenamiento. • **Solo lectura**: Permite leer el almacenamiento. • **No permitido**: No permite el acceso al almacenamiento.
Almacenamiento en red	Seleccione uno de los valores siguientes de la lista desplegable: • **Permitido**: Permite la lectura y escritura del almacenamiento. • **Solo lectura**: Permite leer el almacenamiento. • **No permitido**: No permite el acceso al almacenamiento.

4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Seleccione una de las opciones de distribución para establecer la configuración de **GEstión de discos**. Para más información sobre la configuración de las opciones de distribución, consulte **Trabajar con configuraciones**.
6. Haga clic en **Hecho**.

10.10.4.15. Cifrado en Android

La configuración de cifrado define los requisitos de cifrado del dispositivo para dispositivos Android en el modo Administrador del dispositivo. El cifrado de los dispositivos garantiza que no se pueda acceder a información corporativa confidencial mediante «jailbreak» o vulneración de la seguridad de la raíz. El cifrado almacena los datos del dispositivo de forma no legible, para que si alguien roba el dispositivo no pueda acceder a los datos.

Al habilitar el cifrado se pide al usuario del dispositivo que cifre el dispositivo y es obligatorio establecer un código de acceso para el dispositivo. El código de acceso es lo que descifrará los datos para que usted pueda leerlos. El cifrado del dispositivo se activa automáticamente en dispositivos con la versión corporativa de Android (perfil de trabajo o dispositivos administrados) o dispositivos iOS al establecer un código de acceso. El dispositivo no se puede usar mientras se está cifrando. Una vez que el cifrado está activado, para desactivarlo es necesario restablecer los valores de fábrica del dispositivo.

Ajustes de cifrado

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Activar cifrado de dispositivos	Seleccione este ajuste para activar el cifrado en todos los dispositivos Android cifrables que reciban esta configuración.

> La configuración de cifrado de Android se ha dejado en desuso para dispositivos de Samsung en el modo Administrador de dispositivos de Android 11. Este cifrado es compatible, por defecto, en los dispositivos de Android Enterprise cuando hay establecido un código de acceso del dispositivo.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.4.16. DNS cifrado

Licencia: Gold

Aplicable a:

- iOS 14.0 o versiones más recientes compatibles.
- macOS 11.0 o versiones más recientes compatibles.
- visionOS 1.1 o versiones más recientes compatibles.

La configuración del DNS cifrado que le permitirá mejorar la seguridad sin necesidad de configurar la VPN.

Esta sección contiene los siguientes temas:

- Configuración de DNS cifrado
- Ajustes de la configuración de DNS cifrado

Configuración de DNS cifrado

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **DNS** en el campo de búsqueda y, a continuación, haga clic en la configuración de **DNS cifrado**.
4. Introduzca un nombre y describa la configuración.
5. Introduzca los Ajustes de la configuración de DNS cifrado.
6. Haga clic en **Siguiente**.
7. Seleccione la opción **Habilitar esta configuración**.
8. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - personalizada
9. Haga clic en **Hecho**.

Ajustes de la configuración de DNS cifrado

Utilice los ajustes de la siguiente tabla para configurar el DNS cifrado. Para obtener más información sobre estos ajustes, consulte Documentación de Apple.

Ajuste	Descripción
Ajustes de DNS	Un diccionario que define una configuración para un servidor DNS cifrado.
Protocolo de DNS	Especifique el protocolo de transporte cifrado que se utiliza para comunicarse con el servidor DNS. Seleccione uno de los siguientes protocolos: • HTTPS • TLS
URL del servidor	La plantilla URI de un servidor DNS mediante HTTPS, tal como se define en RFC 8484. Esta URL debe utilizar el esquema https:// y el nombre de host o la dirección en la URL se van a utilizar para validar el certificado del servidor. Si no se indican Direcciones del servidor, se va a utilizar el nombre de host o la dirección en la URL para determinar las direcciones del servidor. Esta clave debe estar presente únicamente si el protocolo de DNS es HTTPS.
Direcciones del servidor	Una lista no ordenada de cadenas de direcciones IP del servidor DNS. Estas direcciones IP pueden ser una combinación de direcciones IPv4 e IPv6. Haga clic en **Añadir** para añadir una dirección de servidor o varias.
Dominios complementarios de coincidencia	Una lista de cadenas de dominio utilizadas para determinar qué consultas DNS usará el servidor DNS. Si no se proporciona este conjunto, todos los dominios utilizarán el servidor DNS. Haga clic en **Añadir** para añadir un dominio o más.
Prohibir a los usuarios desactivar los ajustes del DNS	Prohíbe a los usuarios deshabilitar los ajustes del DNS. Esta clave solo está disponible en dispositivos supervisados.
Reglas de requisitos	Un conjunto de reglas que define los ajustes de DNS. Si no hay reglas implementadas, el sistema siempre aplicará los ajustes de DNS. Haga clic en **+ Añadir reglas de requisitos** para añadir un conjunto o más de reglas de requisitos.
Red	La acción que se debe realizar si este diccionario coincide con la red actual. Seleccione una de las siguientes acciones: • **Conectar:** se aplican Ajustes de DNS cuando el diccionario coincida. • **Desconectar:** no se aplican Ajustes de DNS cuando el diccionario coincida. • **Evaluar la conexión:** se aplican Ajustes de DNS con excepciones por dominio cuando el diccionario coincida.

Evaluar la conexión	Esta opción de red tiene los siguientes ajustes:
	• **Acción de dominio**: comportamiento de los ajustes de DNS para los dominios especificados. Seleccione una de las siguientes acciones:
	  ◦ **No conectar nunca**: no utilizar los Ajustes de DNS para los dominios especificados.
	  ◦ **Conectar si es necesario**: permitir el uso de Ajustes de DNS para los dominios especificados.

Ajuste	Descripción
	• **Dominios**: los dominios para los que se aplica esta evaluación. Haga clic en **+ Añadir** para añadir un dominio o más.
Reglas	Haga clic en **+ Añadir** para añadir una regla o más para hacer coincidir los siguientes parámetros con los valores especificados correspondientes.
Coincidencia de dominio DNS	Un conjunto de nombres de dominio. Esta regla coincide si alguno de los nombres de dominio en la lista especificada coincide con algún dominio en la lista de dominios de búsqueda del dispositivo.
Coincidencia de dirección de servidor DNS	Un conjunto de direcciones IP. Esta regla coincide si alguno de los servidores DNS especificados de la red coincide con alguna entrada del conjunto.
Coincidencia SSID	Un conjunto de SSID que coinciden con la red actual. Si la red no es una red wifi o si el SSID no aparece en este conjunto, la coincidencia no se realiza. Omita esta clave y el conjunto correspondiente para coincidir con cualquier SSID.
Coincidencia del tipo de interfaz	Un tipo de interfaz. Si se especifica, esta regla coincide únicamente si el hardware de la interfaz de red primaria coincide con el tipo especificado. Seleccione uno de los siguientes tipos: • Ethernet • Wi-Fi • Móvil
Sondeo de la cadena de la URL	Una URL para realizar sondeos. Si esta URL se obtiene correctamente (con la devolución de un código de estado 200 HTTP) sin redireccionar, esta regla coincidirá.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.4.17. Ajustes de inteligencia externa

Utilice los **Ajustes de inteligencia externa** para configurar las integraciones con servicios de inteligencia externa en dispositivos supervisados. Esta configuración ayuda a los administradores a aplicar ajustes coherentes basados en políticas que controlan cómo los dispositivos se conectan a los servicios de inteligencia externa compatibles y los utilizan.

Disponible para:

- iOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- macOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- visionOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Busque **Ajustes de inteligencia externa** y seleccione la configuración correspondiente.
3. Configure los **Ajustes de inteligencia externa** según la siguiente tabla:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Permitir integraciones de inteligencia externa	Seleccione la casilla de verificación para habilitar las integraciones de inteligencia externa. Active **Enviar al dispositivo** para habilitar las integraciones de inteligencia externa en dispositivos supervisados.
Permitir el inicio de sesión de integraciones de inteligencia externa	Seleccione la casilla de verificación para habilitar el inicio de sesión en las integraciones de inteligencia externa. Active **Enviar al dispositivo** para habilitar el inicio de sesión en las integraciones de inteligencia externa en dispositivos supervisados.
ID de espacios de trabajo de inteligencia externa permitidos	Introduzca los ID de los espacios de trabajo para habilitar la inteligencia externa. Active **Enviar al dispositivo** para habilitar la inteligencia externa asociada a los ID de espacios de trabajo introducidos en dispositivos supervisados.

4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Seleccione una de las opciones de distribución para configurar los **Ajustes de inteligencia externa**. Para más información sobre la configuración de las opciones de distribución, consulte Trabajar con configuraciones.
6. Haga clic en **Hecho**.

10.10.4.18. Defensa contra amenazas

Aplicable a:

- Cliente Go para iOS versión 3.2.0 o las versiones más recientes compatibles.
- Cliente Go para Android versión 52 o las versiones más recientes compatibles.

Ivanti Neurons for MDM incluye la posibilidad de distribuir tokens de activación para activar la tecnología de Threat Defense integrada en Go para clientes Android y clientes iOS. Threat Defense protege los dispositivos administrados de las amenazas y vulnerabilidades móviles que afectan a dispositivos, redes y aplicaciones.

Cuando esta configuración esté activada en Ivanti Neurons for MDM y aplicada en los dispositivos, las bibliotecas de Threat Defense estarán activadas en los clientes de Go. El servicio de Threat Defense se puede desactivar eliminando el token de la licencia y volviendo a enviar al cliente la configuración de la licencia.

Threat Defense supervisa lo siguiente:

- En el dispositivo: los parámetros del sistema, la configuración, el firmware y las bibliotecas para identificar la actividad sospecho o maligna.
- En la red: el tráfico de red y las conexiones sospechosas hacia y desde dispositivos móviles.
- En la aplicación: aplicaciones permeables (que pueden llegar a poner los datos corporativos en riesgo) y aplicaciones malintencionadas, mediante la evaluación de los riesgos y el análisis del código.

Documentación más reciente

Para obtener las instrucciones más recientes sobre Defensa frente a amenazas, consulte la *Guía de soluciones de Ivanti Neurons for MDM Threat Defense* en el sitio Documentación del producto en **Documentación del producto Ivanti Neurons for MDM**.

10.10.4.19. FileVault 2

Licencia: Gold

FileVault 2 ofrece la posibilidad de realizar un cifrado completo del disco XTS-AES 128 en el contenido de un volumen.

Al habilitar FileVault 2, estarán disponibles los siguientes ajustes para la configuración:

Categoría	Ajustes
Ajustes del usuario de FileVault	• Activar FileVault en SetupAssist **Predeterminado**: falso • Si es cierto, y la carga útil se instala después de inscribirse con Ivanti Neurons for MDM en el Asistente de instalación, solicita al Asistente de instalación que habilite FileVault en el momento de la instalación. Además, el sistema ignora las demás claves de esta carga útil, excepto ShowRecoveryKey. **Prerrequisito**: antes de activar file vault en el asistente de configuración, asegúrese de que la opción **Esperar a la configuración del dispositivo durante la configuración de inscripción del dispositivo** está activada en el perfil de inscripción de dispositivos. • Aplazar la habilitación de FileVault hasta que el usuario designado cierre sesión ◦ Pedir siempre al usuario que active FileVault ◦ Número máximo de veces que un usuario puede omitir la activación de FileVault No solicitar la activación de FileVault en el momento en que el usuario cierra sesión
Ruta de salida	Introduzca la ruta hasta la ubicación donde se almacenarán la clave de recuperación y el plist de la información del equipo.
Clave de recuperación personal	• Crear una clave de recuperación personal • Mostrar la clave de recuperación personal al usuario una vez que se haya habilitado FileVault Esta opción solo está visible cuando la opción **Crear una clave de personal de recuperación** está habilitada. De forma predeterminada, la opción está desactivada. • Habilitar Clave de recuperación institucional: uso de la llave - si no se proporciona ninguna información sobre el certificado en esta carga útil, se usará la llave ya creada en /Library/Keychains/FileVaultMaster.keychain Seleccione una de las siguientes opciones: ◦ Cargar certificado ◦ Certificado ◦ Usar llave en el sistema del usuario
Rotar FileVault Key tras __ días	Los administradores pueden configurar la rotación periódica de las claves de FileVault de los dispositivos macOS para mitigar el riesgo de seguridad de los dispositivos implementados. Los administradores pueden establecer el intervalo de rotación en términos de días. Solo se rotan las Claves de Recuperación personal.

10.10.4.20. Clave de recuperación de FileVault

Licencia: Gold

La configuración de las claves de recuperación de FileVault determina la redirección y custodia de las claves de recuperación de FileVault a un servidor corporativo.

> La configuración de la exclusión y reinserción de la clave de recuperación de File Vault está deactivada cuando un dispositivo macOS deja de enviar la clave de recuperación al volver a insertar la configuración.

Puede personalizar las siguientes opciones:

Ajuste	Descripción
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración (opcional).
Ajustes de configuración para macOS <10.13	
Guarde la clave de recuperación del abonado de Ivanti Neurons for MDM	Seleccione esta opción para permitir que Ivanti Neurons for MDM almacene las claves en su abonado. Cuando sea necesario, la clave se puede descifrar desde la página Detalles del dispositivo.
Redirigir URL al servidor	Introduzca los siguientes ajustes: • Introduzca la **URL de redirección** a la que deben enviarse las claves de recuperación de FDE en lugar de a Apple. La URL debe comenzar con https://. • Seleccione un Certificado de la lista desplegable. Solamente es compatible el formato de certificado PKCS1.
Ajustes de configuración para macOS 10.13+	
Ubicación	(Obligatorio) Introduzca una breve descripción de la localización donde se custodiará la clave de recuperación. Este texto se insertará en el mensaje que va a ver el usuario cuando active FileVault.
Clave del dispositivo	(Opcional) Introduzca una cadena que se debe incluir en el texto de ayuda si el usuario parece haber olvidado la contraseña.

10.10.4.21. Configuración de opciones de FileVault

Esta configuración permite al administrador habilitar o deshabilitar FileVault y destruir la clave de FileVault cuando el sistema entra en modo de espera.

Aplicable a: macOS 10.7+

Procedimiento

1. Vaya a **Configuraciones** > **+Agregar.**
2. Escriba FileVault en el campo de búsqueda y, a continuación, haga clic en la configuración de Opciones de FileVault .
3. Introduzca un Nombre y Descripción de la configuración.
4. En Ajustes de configuración, seleccione las opciones requeridas:
    - Destruir la clave de FileVault cuando el sistema entra en el modo de espera
    - No permitir la desactivación del Cifrado de disco completo
    - No permitir la activación del Cifrado de disco completo
5. Haga clic en Siguiente.
6. Seleccione la opción Habilitar esta configuración.
7. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - Personalizado.
8. Haga clic en Hecho.

10.10.4.22. Certificado de identidad

Esta sección contiene los siguientes temas:

- Ajustes del certificado de identidad
- Distribución de la configuración

Una configuración del certificado de identidad define un mecanismo de identificación de certificados para dispositivos móviles. Los certificados de identidad son certificados X.509 (.p12 o .pfx). Además, los certificados de identidad pueden generarse dinámicamente utilizando la entidad de certificación como una fuente. Antes de comenzar, ya debería saber cómo desea distribuir los certificados en sus dispositivos móviles. También debe haber configurado cualquier entidad de certificación necesaria.

> A partir de la versión 91, el certificado Device Identity para dispositivos Apple se renueva automáticamente a los 30 días de su caducidad. Los dispositivos iOS reciben certificados MDM renovados de Ivanti Neurons for MDM como parte del flujo regular de comprobación de dispositivos. No obstante, los dispositivos iOS deben volver a inscribirse en Ivanti Neurons para MDM cuando están desconectados el tiempo suficiente para que caduque el certificado MDM antes de un registro que habría renovado el certificado antes de la caducidad.

- Los certificados SHA1 se dejan de utilizar mientras se crean los certificados de identidad. Puede elegir otros algoritmos. Si los certificados anteriores usaban SHA-1, puede usarse el mismo algoritmo SHA-1 mientras se actualizan los certificados. Si los certificados anteriores usaban un algoritmo posterior a SHA-1, no está permitido cambiar a SHA-1.
- Después de configurar un certificado de identidad, puede hacer clic en **Probar configuración y continuar** para emitir y verificar la validez del certificado de prueba. Puede aparecer un error al realizar esta prueba para una configuración de certificado de identidad nueva o existente generada dinámicamente si el nombre del sujeto es el mismo que el de la autoridad de certificación local. Cuando aparezca este mensaje de error, deberá modificar el nombre del sujeto del certificado de identidad, que deberá ser diferente del nombre del sujeto de la autoridad de certificación local. Para las configuraciones de certificados de identidad existentes que se modifican con el nombre del sujeto, los certificados se vuelven a emitir y las configuraciones se vuelven a insertar.
  Si ha configurado la opción para crear una configuración sin emitir certificado de prueba para la distribución de certificados **Dinámicamente generados**, haga clic en **Continuar**.
- Los certificados se reemitirán implícitamente.
- Cuando se asignan los certificados de identidad a las aplicaciones de Android, la aplicación del usuario obtiene los certificados de identidad sin solicitar a los usuarios que den su permiso (en lugar de la aplicación) para usar el certificado. Incluye todas las aplicaciones como Email+, Gmail, etc.
- Email+ se puede configurar con un certificado de identidad proporcionado por el usuario e insertarse y asignarse como configuración de la aplicación en dispositivos que tengan la versión corporativa de Android (Android Enterprise). Solo es aplicable a los modos Perfil de trabajo en el Dispositivo propiedad de la empresa y Propietario del dispositivo.

Ajustes del certificado de identidad

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Distribución de certificados	Seleccione el tipo de distribución de certificados a configurar: • **Único archivo**: Cargue un certificado existente para distribuirlo a los dispositivos. • **Generado dinámicamente**: Cree certificados según la demanda utilizando una entidad de certificación local o externa. • **Proporcionado por el usuario**: cree etiquetas para el tipo de certificados que el usuario va a cargar. Una vez creadas, el usuario podrá ver las etiquetas creadas (opciones) en el portal de autoservicio y cargar los certificados que correspondan a esas etiquetas. • **Credencial derivada:** especifique uno de los siguientes usos de la credencial derivada: ◦ Autenticación ◦ Cifrado ◦ Firma ◦ Descifrado • **Config. de SCEP**: especifique cómo solicitar un certificado desde el servidor de SCEP. Seleccione una de las siguientes configuraciones: ◦ Configurador de Apple ◦ Config. de Windows Su selección determina qué opciones se muestran en el resto del formulario.
Permitir que todas las aplicaciones accedan a la clave privada (macOS 10.10+)	**Aplicable a:** certificados de identidad de archivo único, generados de manera dinámica, proporcionados por el usuario y con configuración de SCEP Apple. (Opcional) En el caso de los certificados PKCS#12, active la opción **Permitir que todas las aplicaciones accedan a la clave privada** para permitir que todas las aplicaciones accedan a la clave privada. Por ejemplo, esta clave se puede utilizar en los casos en que se solicite al usuario una contraseña para permitir el acceso a un certificado utilizado para la VPN.
Único archivo	
Datos del certificado de identidad Contraseña **Generado dinámicamente**	Arrastre el archivo del certificado hasta el cuadro punteado o haga clic en **Elegir archivo** para seleccionarlo del sistema de archivos. Introduzca la contraseña que protege el archivo del certificado PKCS#12. Esta contraseña se utiliza para la instalación sin necesidad de solicitarla.
Origen	Seleccione la entidad de certificación local de la lista desplegable. Ya debería haber creado esta EC en **Administrador >** Administración de certificados.

Ajuste	Qué hacer
Crear una configuración sin emitir un certificado de prueba	Seleccione la casilla para crear una configuración sin emitir un certificado de prueba.
Solo para Windows - Almacén de certificados de destino	Los administradores pueden ahora seleccionar el Almacén de certificados de destino en los dispositivos Windows.
Proporcionado por el usuario	
Nombre en pantalla del certificado	Introduzca el nombre del certificado. Este nombre del certificado es exclusivo para un abonado y el usuario podrá ver el nombre del portal de autoservicio mientras carga el certificado.
Borrar la clave privada	Seleccione esta opción para borrar la clave privada del certificado después de *n* (1-30) días. También puede usar las API proporcionadas por Ivanti Neurons for MDM para estas operaciones. Consulte la Ivanti Neurons for MDM *Guía API* para obtener más información sobre las API. Si intenta usar este certificado en cualquier configuración (por ejemplo, para autenticar una aplicación o insertar una Wi-Fi o configuración de VPN) después de haber eliminado su clave privada, la tarea dará error. Asegúrese de que la tarea se realiza antes de haber eliminado la clave privada.
Borrar la clave privada después de días	Seleccione el número de días (1-30) después de los cuales se borran las claves privadas del certificado. El valor predeterminado es de 2 días.
Credencial derivada	
Uso de credenciales derivados	Seleccione cualquiera de las siguientes opciones: • **Autenticación** : para especificar que la credencial derivada se utiliza para la autenticación. • **Cifrado** : para especificar que el uso de la credencial derivada es para el cifrado. • **Firma** : para especificar que la credencial derivada se utiliza para la firma. • **Descifrado**: para especificar que el uso de la credencial derivada es para el descifrado.
Marca	Seleccione el Proveedor de credenciales derivadas que utiliza de las siguientes opciones: • **Confiar** • **Interceder** • **Pura raza** Para añadir los proveedores de credenciales derivadas personalizadas que utiliza, consulte Proveedores de credenciales derivadas.
Configuración ACME: aplicable solo a iOS/iPadOS16+ /macOS14+	
Identificador de cliente	Una cadena única que identifica un dispositivo concreto.

Ajuste	Qué hacer
URL del directorio	(Requerido) la URL del directorio del servidor de ACME. La URL debe usar el esquema https.
Uso de clave ampliado	El valor es una matriz de cadenas. Cada cadena es una OID en una anotación estándar. Por ejemplo, ["1.3.6.1.5.5.7.3.2", "1.3.6.1.5.5.7.3.4"] indica la autenticación de clientes y la protección de correo electrónico. El dispositivo solicita este campo para el certificado que emite el servidor de ACME. El servidor de ACME puede reemplazar o ignorar este campo del certificado que emite.
Tamaño de clave Tipo de clave Asunto	(Requerido) los valores válidos para KeySize dependen de los valores de KeyType y de HardwareBound. Consulte esas claves para requisitos específicos. (Requerido) el tipo de pareja de claves a generar. (Requerido) Introduzca un nombre X.500 representado en forma de matriz de OID y valores separados por comas. Normalmente, el sujeto se establece según el nombre de dominio totalmente cualificado del usuario. Por ejemplo, C=US,DC=com,DC=MobileIron,OU=InfoTech o CN=www.mobileiron.com. También puede personalizar el sujeto añadiendo una variable al OID. Por ejemplo, CN=www.mobileiron.com-${{deviceGUID}}. Para una configuración más sencilla, también puede utilizar la variable $ para rellenar el sujeto con el FQDN del usuario. No utilice el carácter de barra invertida (\) en el nombre del asunto.
Nombre alternativo del asunto Uso de clave	El Nombre Alt del asunto que el dispositivo solicita para el certificado que emite el servidor de ACME. El servidor de ACME puede reemplazar o ignorar este campo del certificado que emite. Este valor es un campo de bit. El bit 0x01 indica la firma digital. El bit 0x10 indica el acuerdo clave. El dispositivo solicita esta clave para el certificado que emite el servidor de ACME. El servidor de ACME puede reemplazar o ignorar este campo del certificado que emite.
Enlazado al Hardware Dar fe	Si el Enlace con el hardware es cierto, la clave privada estará vinculada al dispositivo y solo entonces el Tipo de clave debe ser ECSECPrimeRandom y el Tamaño de clave 256 o 384. Si es cierto, el dispositivo proporciona certificados que describen el dispositivo y la clave generada para el servidor de ACME. Cuando Certificar es cierto, Enlace con el hardware también debe ser cierto.
Configuración de SCEP: configuración de Apple	
Certificado de identidad (SCEP) Entidad de Certificación local	Seleccione esta opción para especificar un servidor SCEP. Seleccione esta opción para especificar una entidad de certificación local que ya haya creado en **Administrador >** Administración de certificados. Seleccione la entidad de certificación local de la lista desplegable que aparece al seleccionar esta opción.

Ajuste	Qué hacer
URL	Introduzca la URL para el servidor SCEP.
Identificador de EC	Introduzca el identificador proporcionado por la entidad de certificación.
Asunto	Introduzca un nombre X.500 representado en forma de matriz de OID y valores separados por comas. Normalmente, el sujeto se establece según el nombre de dominio totalmente cualificado del usuario. Por ejemplo, C=US,DC=com,DC=MobileIron,OU=InfoTech o CN=www.mobileiron.com. También puede personalizar el sujeto añadiendo una variable al OID. Por ejemplo, CN=www.mobileiron.com-$DISPOSITIVO_CLIENTE_ID$. Para una configuración más sencilla, también puede utilizar la variable $USUARIO_DN$ para rellenar el sujeto con el FQDN del usuario. No utilice el carácter de barra invertida (\) en el nombre del asunto.
Tipo de nombre alternativos de sujeto	Seleccione Nombre RFC 822, nombre DNS, Identificador uniforme de recursos o Ninguno, según los atributos de la plantilla del certificado.
Valor del nombre alternativo de sujeto	Introduzca el valor para el tipo correspondiente. Si escribe "$" como primer carácter, aparecerá una lista desplegable con posibles atributos personalizados de LDAP y Entra ID. Seleccione de la lista el atributo personalizado que desee. Si se utiliza el valor Entra ID, solo se admite 'onPremisesImmutableId'. Introduzca fn:base64tohex($)
Nombre principal de NT	Introduzca un nombre alternativo de sujeto para el entorno de Microsoft. Normalmente, esto se configuraría para incluir el UPN (nombre principal de usuario) del usuario.
Reto	(Opcional) Usado como secreto previamente compartido para inscripción automática.
Reintentos	Seleccione esta opción de la lista para establecer el número de veces que se puede intentar la autenticación después de que se devuelva el estado 'pendiente' por primera vez.
Retraso en el reintento	Seleccione esta opción de la lista para establecer el número de segundos que se esperará antes de volver a intentarlo.
Tamaño de la clave	Seleccione 1024, 2048 o 4096 bits.
Uso como firma digital	Seleccione si el certificado se puede utilizar para la firma.
Uso como cifrado clave	Seleccione si el certificado se puede utilizar para el cifrado.
Huella digital EC	Si su entidad de certificación utiliza HTTP, introduzca la cadena hexadecimal que se utilizará como huella digital del certificado de EC. Se admiten las huellas digitales MD5. Si lo prefiere, puede crear una huella digital a partir del certificado. Solo tiene que arrastrar y soltar el certificado hasta el área designada o hacer clic en **Crear a partir de certificado** para seleccionar el certificado desde su sistema de archivos.
Configuración SCEP - Config. de Windows	
EC (Entidad de Certificación)	Seleccione esta opción para especificar una entidad de certificación que ya haya creado en **Administrador >** Administración de certificados. Seleccione la entidad de certificación de la lista

Ajuste	Qué hacer
	desplegable que aparece al seleccionar esta opción.
Asunto	Introduzca un nombre X.500 representado en forma de matriz de OID y valores separados por comas. Normalmente, el sujeto se establece según el nombre de dominio totalmente cualificado del usuario. Por ejemplo, C=US,DC=com,DC=MobileIron,OU=InfoTech o CN=www.mobileiron.com. También puede personalizar el sujeto añadiendo una variable al OID. Por ejemplo, CN=www.mobileiron.com-$DISPOSITIVO_CLIENTE_ID$. Para una configuración más sencilla, también puede utilizar la variable $USUARIO_DN$ para rellenar el sujeto con el FQDN del usuario. No utilice el carácter de barra invertida (\) en el nombre del asunto.
Tipo de nombre alternativos de sujeto	Haga clic en **+ Añadir** para seleccionar Nombre RFC 822, nombre DNS, Identificador uniforme de recursos o Ninguno, según los atributos de la plantilla del certificado.
Reintentos	Seleccione esta opción de la lista para establecer el número de veces que se puede intentar la autenticación después de que se devuelva el estado 'pendiente' por primera vez.
Retraso en el reintento	Seleccione esta opción de la lista para establecer el número de segundos que se esperará antes de volver a intentarlo.
Longitud de clave	Seleccione el tamaño de la clave en 1024, 2048 o 4096 bits.
Seleccione el uso	Seleccione al menos una opción: • Usar como firma digital: seleccione esta opción si el certificado se puede usar para firmar. • Usar como cifrado de la clave: seleccione esta opción si el certificado se puede usar para el cifrado.
Validez	Seleccione la validez en días, meses o años.
Huella digital de la EC	Si su entidad de certificación utiliza HTTP, introduzca la cadena hexadecimal que se utilizará como huella digital del certificado de EC. Se admiten las huellas digitales MD5. Si lo prefiere, puede crear una huella digital a partir del certificado. Solo tiene que arrastrar y soltar el certificado hasta el área designada o hacer clic en **Crear a partir de certificado** para seleccionar el certificado desde su sistema de archivos.
Familia de algoritmos hash	Seleccione los algoritmos SHA-2 o SHA-3.

Si se aplica un certificado de identidad a un perfil para el trabajo en un dispositivo sin configurar un código de acceso para el Desafío de acceso, el dispositivo solicitará un código de acceso para el dispositivo en su lugar.

Para obtener más información, consulte **Trabajar con configuraciones**.

10.10.4.23. Configuración del Bloqueo de activación de Apple

Licencia: Silver

Esta sección contiene los siguientes temas:

- Activar el bloqueo de activación de iOS
- Activar la característica bloqueo de activación de Apple en los dispositivos supervisados
- Activar el bloqueo de activación de macOS
- Activar la característica bloqueo de activación de macOS en los dispositivos supervisados
- Usar el código de derivación del bloqueo de activación de iOS
- Quitar el código de derivación del bloqueo de activación de iOS

El Bloqueo de activación es una característica de Apple diseñada para impedir el uso de un dispositivo perdido o robado por parte de terceras personas. Después de que se activa «Buscar», se guarda en los servidores de activación de Apple una asignación entre esta cuenta de iCloud y el identificador de hardware de este dispositivo. Desde ese momento, nadie puede desactivar «Buscar», borrar el dispositivo o reactivarlo sin introducir la Id. de Apple y la contraseña existentes. Si una tercera persona ajena al usuario borra el dispositivo e intenta posteriormente reactivarlo y usarlo, se le pedirá la Id. de Apple y la contraseña en el Asistente de configuración.

Al desactivar el Bloqueo de activación no se desactivará esta característica en los dispositivos supervisados si el usuario final ha habilitado Encontrar mi dispositivo. El Asistente de configuración solicitará al usuario que realice alguna acción cuando el dispositivo sea restablecido o borrado de forma remota.

El Bloqueo de activación proporciona a los administradores más opciones para prevenir el robo de dispositivos supervisados. Sin embargo, la mayoría de los administradores corporativos tienden a dejar el Bloqueo de activación deshabilitado porque es una característica eminentemente de consumidor. La siguiente tabla resume las opciones para implementaciones corporativas:

Tipo de dispositivo	Resultado
Corporativo y con supervisión	• El Bloqueo de activación está habilitado de forma predeterminada en los dispositivos supervisados. • Los usuarios del dispositivo no pueden activar el Bloqueo de activación.
Corporativo y no supervisado	• El Bloqueo de activación estará habilitado en cuanto el usuario final inicie sesión en iCloud con su Id. de Apple y active Encontrar mi dispositivo. • Los servidores MDM, como Ivanti Neurons for MDM, no pueden controlar el Bloqueo de activación en dispositivos no supervisados. Los usuarios de dispositivos pueden bloquear la activación con sus credenciales personales, dejándole sin recursos en caso de que se vayan de la empresa.

Activar el bloqueo de activación de iOS

Aplicable a: dispositivos iOS 7+ supervisados

Esta configuración se aplicará a los dispositivos Supervisados (iOS 7 y posterior) que tengan habilitada la función **Buscar**. Si un administrador u otro usuarios intenta Borrar, Activar o desactivar la opción Buscar mi dispositivo en el dispositivo, aparecerá la

pantalla de Bloqueo de activación de Apple. Para proceder, deben introducirse las credenciales de iTunes o un código de derivación.

El código de derivación para los dispositivos supervisados se almacenará tras la activación y se puede ver en los detalles del dispositivo. El código de derivación se puede enviar de forma remota usando el comando «Quitar bloqueo de activación» para los dispositivos supervisados. No obstante, el código debe introducirse manualmente al reactivar un dispositivo o desactivar la función Encontrar mi dispositivo.

> Solo se puede crear una configuración del bloqueo de activación para todos los espacios.

Activar la característica bloqueo de activación de Apple en los dispositivos supervisados

Procedimiento

1. Habilite la función **Buscar** en su dispositivo.
2. Vaya a **Configuraciones**.
3. Seleccione la configuración del **Bloqueo de activación de Apple** en la lista de configuraciones existentes.
4. Haga clic en **Editar**.
5. En la sección iOS 7+ supervisado, haga clic en **Activar Bloqueo de activación**.
6. Haga clic en **Hecho**.
7. Registre el dispositivo.

Activar el bloqueo de activación de macOS

Aplicable a: dispositivos macOS 10.15+ supervisados

Esta configuración se aplicará a los dispositivos supervisados con macOS 10.15 y posteriores. El bloqueo de activación en macOS solo es aplicable a los Mac que tienen un chip de seguridad Apple T2. En los dispositivos supervisados, ya sean actualizados o recién instalados, y en los dispositivos registrados que estén ahora mismo actualizados, el bloqueo de activación está desactivado de forma predeterminada. La activación de «Encontrar mi...» no activa automáticamente el bloqueo de activación en estos dispositivos

Si un administrador u otro usuarios intenta Borrar, Activar o desactivar la opción «Buscar» en el dispositivo, aparecerá la pantalla de Bloqueo de activación de Apple. Para proceder, deben introducirse las credenciales de iTunes o un código de derivación. El código de derivación para los dispositivos supervisados se almacenará tras la activación y se puede ver en los detalles del dispositivo. El código de derivación se puede enviar de forma remota usando el comando «Quitar bloqueo de activación» para los dispositivos supervisados. No obstante, el código debe introducirse manualmente al reactivar un dispositivo o desactivar la función «Buscar».

> Solo se puede crear una configuración del bloqueo de activación para todos los espacios.

Activar la característica bloqueo de activación de macOS en los dispositivos supervisados

Procedimiento

1. Habilite la función «Buscar» en su dispositivo.
2. Vaya a **Configuraciones**.
3. Seleccione la configuración del **Bloqueo de activación de Apple** en la lista de configuraciones existentes.

4. Haga clic en **Editar**.
5. En la sección macOS 10.15+ supervisado, haga clic en **Activar Bloqueo de activación**.
6. Haga clic en **Hecho**.
7. Registre el dispositivo.

Usar el código de derivación del Bloqueo de activación de iOS

Cuando el dispositivo se ha borrado con el Bloqueo de activación de iOS habilitado, el código de activación se retiene en el servidor de activación de Apple y en la interfaz de administración de Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Dispositivos**.
2. Seleccione el dispositivo.
3. Haga clic en **Acciones > Borrar**. Puede que el dispositivo tarde algunos minutos en reiniciarse.
4. Cuando el dispositivo le solicite la Id. de Apple y la contraseña, deje vacío el campo de la **Id. de Apple**.
5. Introduzca el código de derivación en el campo de la **contraseña**.
6. Haga clic en **Siguiente**.
7. Continúe con la configuración.

Quitar el código de derivación del Bloqueo de activación de iOS

Cuando el bloqueo de activación de iOS está quitado de la interfaz de administración de Ivanti Neurons for MDM, el código de derivación se elimina del servidor de activación de Apple, pero sigue estando presente en los detalles del dispositivo de la interfaz de administración de Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Dispositivos**.
2. Seleccione el dispositivo.
3. Seleccione **Configuraciones**.
4. Seleccione **Bloqueo de activación de Apple**.
5. Haga clic en **Editar**.
6. En la sección iOS 7+ supervisado, desactive **Activar Bloqueo de activación**.
7. Haga clic en **Hecho**.
8. Vaya a **Dispositivos**.
9. Seleccione el dispositivo.
10. Haga clic en **Acciones > Borrar**. Puede que el dispositivo tarde algunos minutos en reiniciarse. El dispositivo ahora se puede ajustar con la nueva AppleID y contraseña del usuario.
11. Continúe con la configuración.

El estado de Quitar bloqueo de activación de iOS aparece en la interfaz de la siguiente manera:

Estado	Resultado
Pendiente	• El servidor está enviando el código de Borrar bloqueo de activación a Apple.
Enviado	• Apple confirmar la recepción del código de Quitar bloqueo de activación.
Error	• El servidor no pudo enviar el código a Apple. • Apple ha notificado un error.

10.10.4.24. Configuración personalizada iOS

La configuración personalizada de iOS le permite cargar y distribuir un perfil de configuración iOS creado por una aplicación diferente, como la utilidad de Configuración de iPhone de Apple.

Ajustes personalizados de iOS

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Datos del archivo	Arrastre y suelte el archivo de configuración o haga clic en **Elegir archivo** para seleccionarlo de su sistema de archivos.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.4.25. Ajustes de inteligencia

Utilice los Ajustes de inteligencia externa para configurar las opciones de Apple Intelligence en dispositivos supervisados. Esta declaración ayuda a los administradores a aplicar controles coherentes basados en políticas que gestionan cómo los dispositivos acceden a las funciones de Apple Intelligence y las utilizan.

Disponible para:

- iOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- macOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- visionOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Busque **Ajustes de inteligencia** y seleccione la configuración correspondiente.
3. Configure los **Ajustes de inteligencia** según la siguiente tabla:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Permitir informes de Apple Intelligence Permitir Genmoji	Seleccione la casilla para habilitar el informe de Apple Intelligence. Active **Enviar al dispositivo** para habilitar el informe de Apple Intelligence en dispositivos supervisados. Seleccione la casilla para habilitar Genmoji. Active **Enviar al dispositivo** para habilitar Genmoji en dispositivos supervisados.
Permitir Entorno de pruebas de imágenes	Seleccione la casilla para habilitar Image Playground. Active **Enviar al dispositivo** para habilitar Image Playground en dispositivos supervisados.
Permitir herramienta de selección de imágenes	Seleccione la casilla para habilitar Image Wand. Active **Enviar al dispositivo** para habilitar Image Wand en dispositivos supervisados. Este ajuste no se aplica a dispositivos macOS.
Permitir resultados de caligrafía personalizada Permitir resumen de inteligencia visual	Seleccione la casilla para habilitar resultados de caligrafía personalizada Active **Enviar al dispositivo** para habilitar resultados de caligrafía personalizada en dispositivos supervisados. Este ajuste no se aplica a dispositivos macOS y visionOS. Seleccione la casilla para habilitar el Resumen de Visual Intelligence. Active **Enviar al dispositivo** para habilitar el Resumen Visual Intelligence en dispositivos supervisados. Este ajuste no se aplica a dispositivos macOS y visionOS.
Permitir herramientas de escritura Forzar el uso exclusivo de dictado en el dispositivo	Seleccione la casilla para habilitar Herramientas de escritura. Active **Enviar al dispositivo** para habilitar las Herramientas de escritura en dispositivos supervisados. Seleccione la casilla para habilitar el uso exclusivo del dictado en el dispositivo. Active **Enviar al dispositivo** para habilitar el uso exclusivo del dictado en el dispositivo en dispositivos supervisados.
Forzar el uso exclusivo de traducción en el dispositivo **Aplicaciones** **Calendario**	Seleccione la casilla para habilitar el uso exclusivo de la traducción en el dispositivo. Active **Enviar al dispositivo** para habilitar el uso exclusivo de la traducción en dispositivos supervisados. Este ajuste no se aplica a dispositivos macOS y visionOS.
Permitir la edición del lenguaje natural	Seleccione la casilla de verificación para habilitar la edición del lenguaje natural en el calendario y los recordatorios. Alterne el **botón** Pulsar en dispositivo para habilitar la edición del lenguaje natural en el calendario y los recordatorios en los dispositivos supervisados.

Ajuste	Qué hacer
Correo	
Permitir respuestas inteligentes	Seleccione la casilla para habilitar respuestas inteligentes. Active **Enviar al dispositivo** para habilitar respuestas inteligentes en dispositivos supervisados.
Permitir resumen	Seleccione la casilla para habilitar la función Resumen. Active **Enviar al dispositivo** para habilitar la función Resumen en dispositivos supervisados.
Notas	
Permitir transcripción	Seleccione la casilla para habilitar la función Transcripción. Active **Enviar al dispositivo** para habilitar la función Transcripción en dispositivos supervisados. Este ajuste no se aplica a dispositivos visionOS.
Permitir resúmenes de transcripción	Seleccione la casilla para habilitar la función Resúmenes de transcripción. Active **Enviar al dispositivo** para habilitar la función Resúmenes de transcripción en dispositivos supervisados. Este ajuste no se aplica a dispositivos visionOS.
Safari	
Permitir resumen	Seleccione la casilla para habilitar la función Resumen. Active **Enviar al dispositivo** para habilitar la función Resumen en dispositivos supervisados.

4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Seleccione una de las opciones de distribución para configurar los **Ajustes de inteligencia**. Para más información sobre la configuración de las opciones de distribución, consulte **Trabajar con configuraciones**.
6. Haga clic en **Hecho**.

10.10.4.26. Restricciones de iOS

Las restricciones de iOS son configuraciones que ayudan al usuario principal del dispositivo a controlar lo que otros usuarios pueden hacer con los dispositivos iOS, watchOS y visionOS. Estos ajustes son definidos por Apple y administrados por Ivanti Neurons for MDM.

Durante la distribución de esta configuración a **iPads compartidos**, puede seleccionar el Canal de dispositivo o el Canal de usuario. Es muy útil para distribuir configuraciones separadas e implementar restricciones que solo se aplican al dispositivo o al canal de usuario.

Los administradores globales pueden delegar en los administradores de espacio la edición la configuración de la opción **Todos los dispositivos para la distribución personalizada**. Para configurar la restricción de iOS, puede seleccionar la opción **Permitir que esta configuración esté disponible en todos los espacios**.

> Los cambios en la distribución son aplicables sólo al espacio específico. Todos los demás espacios siguen heredando la configuración de distribución espacial predeterminada.

Ajustes de restricciones de iOS

Categoría	Ajuste	Qué hacer
	Nombre	Introduzca un nombre que identifique a esta configuración.
	Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Funcionalidad del dispositivo	**Todas las versiones de iOS**	**Activar el uso de las características del dispositivo.**
	Permitir capturas de pantalla y grabación de pantalla	Seleccione esta opción para permitir que el usuario haga capturas de pantalla utilizando la función integrada de captura de pantalla de iOS.
	Permitir la observación remota de la pantalla (iOS 9.3 y posteriores)	Seleccione esta opción para permitir al usuario que observe la pantalla remota.
	Permitir forzar la observación espontánea de la pantalla del aula administrada (solo supervisado - iOS 10.3+)	(Aplicable solo a iPads) Seleccione esta opción para permitir que aparezca en la pantalla un mensaje no solicitado cuando se configure un iPad supervisado con las clases administradas.
	Permitir sincronización automática durante la itinerancia	Seleccione esta opción para permitir la sincronización de cuentas de correo electrónico mientras que el dispositivo esté fuera de su país de origen.
	Permitir Siri	Seleccione esta opción para permitir la aplicación del asistente personal en los dispositivos compatibles.
	Permitir Siri mientras el dispositivo está bloqueado	Seleccione esta opción para permitir que la aplicación del asistente personal lleve a cabo tareas cuando el dispositivo esté bloqueado.
	Activar el filtro de obscenidades de Siri (solo modo supervisado)	Seleccione esta opción para activar el filtro de obscenidades de Siri.
	Permitir marcación de voz	Seleccione esta opción para permitir que los usuarios llamen a un número o a un contacto mediante sistemas de voz.

Categoría	Ajuste	Qué hacer
	Permitir compra en la aplicación	Seleccione esta opción para permitir que los usuarios realicen compras a través de las aplicaciones activas en su dispositivo.
	Permitir código de acceso mientras el dispositivo está bloqueado	Seleccione esta opción para permitir que se muestren las notificaciones del código de acceso mientras el dispositivo esté bloqueado.
	Permitir Control Center de la pantalla de bloqueo	Seleccione esta opción para permitir el acceso a Control Center desde la pantalla de bloqueo.
	Permitir vista Notificaciones de la pantalla de bloqueo	Seleccione esta opción para permitir que se muestren notificaciones en la pantalla de bloqueo.
	Permitir vista Hoy de la pantalla de bloqueo	Seleccione esta opción para permitir la vista Hoy desde la pantalla de bloqueo.
	Permitir Abrir entrada desde aplicaciones administradas a no administradas	**requiere una licencia Gold**. Seleccione esta opción para permitir que los documentos de las aplicaciones y cuentas administradas puedan abrirse en aplicaciones y cuentas no administradas. Al desactivar esta opción se evita el intercambio de documentos entre aplicaciones y cuentas administradas y no administradas. Por ejemplo, puede que quiera evitar que los documentos corporativos puedan abrirse con aplicaciones personales. También puede usar esta opción (desactivar) junto con la configuración de dominios administrados para garantizar que los datos descargados desde un dominio administrado solo se puedan abrir en una aplicación administrada.
	Permitir Abrir entrada desde aplicaciones no administradas a administradas	**requiere una licencia Gold**. Seleccione esta opción para permitir que los documentos de las aplicaciones y cuentas no administradas puedan abrirse en aplicaciones y cuentas administradas. Al desactivar esta opción se evita el intercambio de documentos entre aplicaciones y cuentas no administradas y administradas. Por ejemplo, puede que quiera evitar que los usuarios envíen documentos personales utilizando el correo electrónico de la empresa. También puede usar esta opción (desactivar) junto con la configuración de dominios administrados para garantizar que los datos descargados desde un dominio no administrado no se puedan abrir en una aplicación administrada.
	Requerir código de acceso en la primera sincronización de AirPlay	Seleccione esta opción para solicitar a Apple TV que muestre un código de acceso que el usuario debe introducir en el dispositivo iOS para autorizar la sincronización inicial de los dispositivos.
	Forzar contraseña en solicitudes entrantes de	Seleccione esta opción para obligar al usuario a que introduzca su contraseña para todas las solicitudes entrantes de AirPlay.

Categoría	Ajuste	Qué hacer
	AirPlay (tvOS hasta 10.1)	Predeterminado: no seleccionada
	iOS 26+ Aplicaciones exentas de restricciones por clasificación (aplicable para iOS 26.1+)	Introduzca la lista de aplicaciones que desea eximir de las restricciones de clasificación por edad, únicamente si sus ID del agrupamiento están incluidos en la intersección de todas las listas de exención de múltiples cargas útiles y aplicaciones de control parental como Tiempo de uso. Predeterminado: seleccionado
	Todas las versiones de iOS supervisadas Permitir Apple Books Permitir contenido sexual explícito en la iBooks Store (iOS y tvOS 11.3 y posterior)	 Seleccione esta opción para permitir el acceso a la aplicación Apple Books. Seleccione esta opción para permitir que los usuarios puedan descargarse material de la iBooks store catalogado como erótico.
	Permitir modificación de la cuenta Permitir modificación de datos móviles de la aplicación	Seleccione esta opción para permitir que los usuarios con dispositivos iOS 7 supervisados puedan añadir cuentas de correo electrónico y puedan hacer cambios en las cuentas de correo electrónico que habían sido configuradas previamente. Seleccione esta opción para permitir que los usuarios puedan cambiar los ajustes de los datos móviles para las aplicaciones.
	Permitir modificación de Find My Friends Permitir sincronización con hosts ajenos a Configurator Permitir AirDrop	Seleccione esta opción para permitir que los usuarios puedan modificar los ajustes de la aplicación Buscar a mis amigos. Seleccione esta opción para permitir la sincronización host para la sincronización de iTunes. A todos los efectos, habilitar esta opción permite que los dispositivos supervisados se sincronicen con iTunes en un dispositivo Mac que no sea el del host de supervisión. Desactivar esta opción desactiva todas las sincronizaciones host exceptuando la del host de supervisión. Si no se ha configurado ningún certificado host de supervisión, se desactivarán todas las sincronizaciones. Seleccione esta opción para permitir el uso de AirDrop en este dispositivo. AirDrop en sistema de Wi-Fi ad hoc de Apple que permite compartir archivos con usuarios que estén cerca. Al restringir esta característica, se asegura de que los documentos confidenciales no pueden filtrarse a dispositivos no autorizados o inseguros.
	Permitir Touch ID/Face ID para desbloquear dispositivo	Seleccione esta opción para permitir que Touch ID o Face ID desbloqueen los dispositivos.

Categoría	Ajuste	Qué hacer
	Permitir que Spotlight busque para devolver resultados de búsqueda en Internet	Seleccione esta opción para permitir que Spotlight busque para devolver resultados de búsqueda en Internet.
	Permitir aplicación en modo Single-App **iOS 8+**	Introduzca una lista de las Id. de paquete separados por comas para las aplicaciones que pueden entrar de forma autónoma en el modo Single-App en dispositivos iOS supervisados. Por ejemplo, puede especificar aplicaciones de examen personalizadas para estudiantes. Tan pronto como el estudiante inicia la aplicación, esta entra en modo Single-App para que pueda estar seguro de que el estudiante no está utilizando otros recursos mientras realiza el examen. Esta característica está presente en las aplicaciones desarrolladas para el uso autónomo del modo Single-App. La supervisión se establece en Apple Configurator.
	Permitir hacer copias de seguridad de los libros de Enterprise	Seleccione esta opción para permitir copias de seguridad personales de iBooks, ePub y documentos PDF que se enviaron al dispositivo usando MDM.
	Permitir sincronizar las notas de los libros y las secciones destacadas de Enterprise	Seleccione esta opción para permitir que las notas y secciones destacadas que se han añadido a los libros de Enterprise se sincronicen con iTunes.
	Forzar detección de muñeca del reloj Apple	Seleccione esta opción para ocultar las notificaciones en pantalla a menos que alguien lleve el Apple Watch.
	Supervisado por iOS 8+	
	Permitir teclado predictivo	Seleccione esta opción para permitir a los usuarios que habiliten la predicción de iOS de la palabra que se está escribiendo, y permitir así a los usuarios que pulsen una de las tres predicciones para completar la palabra.
	Permitir autocorrección del teclado	Seleccione esta opción para permitir el uso de la autocorrección en teclados Bluetooth.
	Permitir revisión ortográfica del teclado	Seleccione esta opción para permitir el uso de la revisión ortográfica en teclados Bluetooth.
	Permitir búsqueda de definiciones del teclado	Seleccione esta opción para permitir la búsqueda de definiciones en teclados Bluetooth.
	Permitir la modificación de huellas digitales de Touch ID y caras de Face ID	Seleccione esta opción para permitir que se cambien los ajustes de Touch ID o Face ID.

Categoría	Ajuste	Qué hacer
	Supervisado por iOS 9+ Permitir atajos del teclado en iPads	Seleccione esta opción para permitir el uso de accesos directos del teclado en el iPad.
	Permitir modificaciones del fondo de pantalla	Seleccione esta opción para permitir a los usuarios que cambien las imágenes del fondo de pantalla.
	Permitir sincronización con Apple Watch Permitir modificaciones del nombre del dispositivo	Seleccione esta opción para permitir la sincronización del iPhone con el Apple Watch. Seleccione esta opción para permitir que el usuario cambie el nombre del dispositivo.
	Permitir la modificación del ajuste de confianza en aplicaciones corporativas **Supervisado por iOS 9,3+**	Seleccione esta opción para permitir que el usuario cambie los ajustes de confianza de la aplicación con la versión corporativa.
	Permitir la modificación de los ajustes de notificaciones	Seleccione esta opción para permitir al usuario que cambie los ajustes de las notificaciones.
	iOS 9.3.2+ supervisado Permitir modificación de envío de diagnósticos	Seleccione esta opción para permitir al usuario que cambie los ajustes relacionados con el envío de datos diagnósticos a Apple.
	Supervisado por iOS 10+	
	Permitir modificación de Bluetooth	Seleccione esta opción para permitir al usuario modificar el ajuste Bluetooth en dispositivos supervisados. Resulta útil en algunos casos como en iPad compartidos utilizados para la aplicación Classroom para el ámbito educativo, cuando es necesario Bluetooth para ejecutar la aplicación.
	Supervisado por iOS 10,3+	
	Permitir dictado	Seleccione esta opción para permitir que el usuario le hable al iPhone o iPad en lugar de escribir.

Categoría	Ajuste	Qué hacer
	Supervisado por iOS 11+	
	Permitir AirPrint	Seleccione esta opción para permitir la función AirPrint para impresiones inalámbricas.
	Permitir almacenamiento de credenciales de AirPrint	Seleccione esta opción para permitir el almacenamiento en llaves de nombres de usuario y contraseñas para AirPrint.
	Permitir descubrimiento de iBeacon de AirPrint	Seleccione esta opción para permitir que el usuario establezca el descubrimiento iBeacon de impresoras AirPrint.
	Permitir que se añadan configuraciones de VPN	Seleccione esta opción para permitir que el usuario cree una configuración VPN.
	Forzar requisito de TLS de confianza de AirPrint	Seleccione esta opción para permitir certificados de confianza en la comunicación de impresiones TLS. Predeterminado: no seleccionada
	Permitir la desinstalación de la aplicación del sistema	Seleccione esta opción para permitir la eliminación de aplicaciones del sistema.
	Permitir la modificación de los ajustes del plan móvil	Seleccione esta opción para permitir a los usuarios que modifiquen los ajustes del plan móvil.
	Permitir la configuración de dispositivos cercanos	Seleccione esta opción para permitir a los usuarios que configuren nuevos dispositivos cercanos.
	Unirse automáticamente a las clases de Classroom sin solicitarlo	Seleccione esta opción para permitir a los usuarios que se unan automáticamente a clases de Classroom sin tener que esperar ninguna solicitud. Predeterminado: no seleccionada
	Permitir que Classroom bloquee una aplicación y el dispositivo sin solicitarlo	Seleccione esta opción para permitir que Classroom bloquee una aplicación y el dispositivo sin solicitarlo al usuario. Predeterminado: no seleccionada
	Forzar que el usuario deba autenticarse para poder autorrellenar la información de contraseñas o de	El propietario del dispositivo debe autenticarse para poder autorrellenar la información de contraseñas o de tarjetas de crédito en el navegador de Safari y en las aplicaciones. Predeterminado: falso

Categoría	Ajuste	Qué hacer
	tarjetas de crédito en el navegador de Safari y en las aplicaciones	
	iOS 11,3+ Permitir sincronización con aplicación Remote (tvOS 11.3 y posterior)	Seleccione esta opción para permitir la sincronización del dispositivo con la aplicación remota.
	Permitir solicitudes entrantes de AirPlay (tvOS 11.3 y posterior) **Supervisado por iOS 11,3+** Permitir el modo restringido de USB	Seleccione esta opción para permitir las solicitudes entrantes de AirPlay. Seleccione esta opción para permitir al usuario acceder al modo restringido de USB.
	Aplazar las actualizaciones de software durante 30 días (para iOS 11.3, tvOS 12.2 y versiones posteriores, solo con dispositivos supervisados) Requiere permiso del profesor para salir de clases no administradas por Classroom	Seleccione esta opción para introducir el número de días que desea aplazar las actualizaciones de software. El valor predeterminado es de 30 días y el máximo es de 90 días. Predeterminado: no seleccionada Seleccione esta opción para permitir al usuario recibir el permiso necesario del profesor para salir de las clases no administradas de Classroom.
	iOS 12+ supervisado Forzar fecha y hora automáticas (iOS 12.0 y tvOS 12.2 y posterior)	Seleccione esta opción para activar la función de "Establecer automáticamente" fecha y hora. El usuario no podrá desactivar esta opción. Predeterminado: falso
	Permitir la modificación de los ajustes de eSIM (iPhone XS, iPhone XS Max y iPhone XR - iOS 12.1 y versiones posteriores)	Seleccione esta opción para permitir que el usuario modifique la configuración eSim en los dispositivos compatibles. Esta acción también evita que los usuarios añadan o eliminen un plan móvil en los Ajustes de sus dispositivos. Predeterminado: Verdadero

Categoría	Ajuste	Qué hacer
	Supervisado por iOS 12.2+	
	Permitir la modificación de los ajustes del punto de acceso personal	Seleccione esta opción para permitir al usuario modificar los ajustes de Punto de acceso personal. Predeterminado: Verdadero
	iOS 13,0+	
	Permitir a «Archivos» el acceso a la unidad de red	Seleccione esta opción para permitir que el usuario se conecte a unidades de red en la aplicación Archivos. Predeterminado: Verdadero
	Permitir a «Archivos» el acceso a la unidad de USB	Seleccione esta opción para permitir al usuario conectarse a cualquier dispositivo USB conectado en la aplicación Archivos. Predeterminado: Verdadero
	Supervisado por iOS 13.0+	
	Permitir teclado de ruta continua	Seleccione esta opción para activar el teclado de ruta continua (escritura por deslizamiento o por trazado). Predeterminado: Verdadero
	Permitir hibernar dispositivo	Seleccione esta opción para activar el modo de suspensión del dispositivo. Predeterminado: Verdadero
	Permitir encontrar dispositivo	Seleccione esta opción para activar Buscar mi dispositivo en la aplicación «Buscar mi» (Find My). Predeterminado: Verdadero
	Permitir encontrar a mi amigo	Seleccione esta opción para activar Encontrar a mis amigos en la aplicación «Buscar mi» (Find My). Predeterminado: Verdadero
	Forzar el encendido de la Wi-Fi	Seleccione esta opción para activar la potencia de Wi-Fi en el estado de encendido. Predeterminado: falso
	iOS 13.4+	
	Permitir la sesión de invitados para el iPad compartido	Si es falso, las sesiones temporales no estarán disponibles en el iPad compartido. Predeterminado: Verdadero
	iOS 14.0+	
	Permitir publicidad personalizada de Apple	Si es falso, limita la publicidad personalizada de Apple. Esto evitará que Apple utilice la información del usuario para los anuncios dirigidos. Es posible que esto no reduzca el

Categoría	Ajuste	Qué hacer
		número de anuncios recibidos, pero los anuncios serán menos relevantes para el usuario. Predeterminado: Verdadero
	Supervisado por iOS 14.0+ Permitir la aplicación Clips	 Si es falso, impide que un usuario añada cualquier App Clips, y elimina cualquier App Clips existente en el dispositivo. Predeterminado: Verdadero
	Supervisado por iOS 14,2+	
	Permitir NFC **iOS 14.5+** Permitir el desbloqueo automático	Si es falso, desactiva NFC. Requiere un dispositivo supervisado. Disponible en iOS 14.2 y posterior Predeterminado: Verdadero Los administradores pueden utilizar la restricción existente allowAutoUnlock para gestionar esta función. Si es falso, no permite el desbloqueo automático. Disponible en macOS 10.12 y posterior, y en iOS 14.5 y posterior. Predeterminado: Verdadero
	Forzar el Dictado solo en el Dispositivo **Supervisado por iOS 14,5+**	Si es verdadero, desactiva las conexiones con los servidores de Siri para el dictado. Predeterminado: falso
	Permitir el arranque externo no emparejado a la recuperación	Si es verdadero, permite que un dispositivo no sincronizado inicie los dispositivos en modo recuperación. Predeterminado: falso
	Forzar el WiFi solo a las redes permitidas	Si es verdadero, limita el dispositivo para que solo se conecte a las redes Wi-Fi establecidas a través del perfil de configuración. Predeterminado: falso Si la restricción **Forzar el Wi-Fi solo a las redes permitidas** está activada y la configuración Wi-Fi no se distribuye al dispositivo, esta se perderá.
	iOS 15+ Forzar la Traducción solo en el Dispositivo Requerir área de pegado administrada	 Si es verdadero, el dispositivo no se conectará a los servidores de Siri para la traducción. Predeterminado: falso Si es verdadero, la funcionalidad de copiar y pegar respeta las restricciones allowOpenFromManagedToUnmanaged y allowOpenFromUnmanagedToManaged. Predeterminado: falso

Categoría	Ajuste	Qué hacer
	iOS 15.2+ Permitir la protección de privacidad del correo	Si es falso, se deshabilita la Protección de privacidad de correo en el dispositivo. Disponible para iOS 15.2 y versiones posteriores. Cuando la configuración de Permitir protección de privacidad del correo se instala y se habilita desde el portal administrativo de Ivanti Neurons for MDM, se habilita la alternancia de Proteger actividad del correo en el dispositivo y están visibles las opciones siguientes: • **Ocultar dirección IP**: el remitente del correo electrónico no puede vincular el correo electrónico a su actividad en línea ni determinar su ubicación. • **Bloquear todo el contenido remoto**: evita que el remitente del correo electrónico vea su actividad de correo electrónico Predeterminado: Verdadero
	iOS 15.4+	
	Permitir el salva pantallas automático de Apple TV (tvOS 15.4 y posterior)	Si es falso, se deshabilita el salvapantallas automático de Apple TV. Disponible para tvOS 15.4 y versiones posteriores. Predeterminado: Verdadero
	iOS 16.0 hasta 26.0	
	Permitir instalación de mejoras de seguridad de segundo plano Permitir la eliminación de mejoras de seguridad de segundo plano	Para deshabilitar las respuestas. El usuario no puede instalar mejoras de seguridad de segundo plano. Para evitar que el usuario pueda deshacer las respuestas. El usuario no puede eliminar las mejoras de seguridad de segundo plano.
	Supervisado por iOS 17.0+ Permitir widgets de iPhone en dispositivos Mac **iOS 17.2+ Supervisado**	Seleccionar para permitir que los widgets de iPhone aparezcan en dispositivos Mac que usan el mismo AppleID del iPhone para iCloud en ambos dispositivos.
	Permitir correo de voz en vivo	Seleccione para habilitar el correo de voz en vivo en el dispositivo.
	Forzar conservar ESIM al borrar	Seleccione conservar la eSIM cuando el sistema borre el dispositivo debido a demasiados intentos fallidos de contraseña o la opción Borrar todo el contenido y la configuración en **Configuración** > **General** > **Restablecer**. El sistema no conserva la eSIM si **Buscar mi** inicia el borrado del dispositivo.

Categoría	Ajuste	Qué hacer
	iOS 17.4+ Supervisado	
	Permitir la instalación de aplicaciones de Marketplace	Seleccionar para permitir que los usuarios descarguen aplicaciones de mercados alternativos. Esta restricción, si se establece en false, impedirá que los usuarios instalen aplicaciones nuevas de mercados alternativos y aplicaciones instaladas desde esos mercados.
	Permitir atenuación automática	Seleccione para permitir la opción de atenuación automática en iPads con pantallas OLED.
	iOS 17.5+ Supervisado	
	Permitir la instalación de aplicaciones de distribución web	Cuando se establece como falsa esta restricción **enableWebdistributionAppInstallation**, evitará que los usuarios instalen aplicaciones directamente desde nuevos sitios web alternativos. Es aplicable únicamente a dispositivos supervisados.
	iOS 18.0+ Supervisado	
	Permitir transferencias salientes de eSIM	Seleccione para permitir la transferencia de una eSIM a un dispositivo distinto al dispositivo en el que está instalada la restricción.
	Permitir Genmoji	Seleccione para permitir la creación de Genmojis.
	Permitir Entorno de pruebas de imágenes	Seleccione para permitir el uso de la generación de imágenes.
	Permitir herramienta de selección de imágenes	Seleccione esta opción para permitir el uso de la herramienta de selección de imágenes.
	Permitir duplicación de iPhone	Seleccione para permitir que el iPhone se duplique en un dispositivo macOS.
	Permitir resultados de caligrafía personalizada	Seleccione para permitir que el sistema genere texto utilizando la caligrafía del usuario.
	Permitir herramientas de escritura	Seleccione para activar las herramientas de escritura de Apple Intelligence.
	Permitir que las aplicaciones se oculten	Seleccione para permitir que las aplicaciones se oculten.
	Permitir que las aplicaciones se bloqueen	Seleccione para permitir que las aplicaciones se bloqueen.
	iOS 18.1+ Supervisado	
	Permitir grabación de llamadas	Seleccione para permitir la grabación de llamadas. Predeterminado: Verdadero

Categoría	Ajuste	Qué hacer
	Permitir resumen de correo	Seleccione para permitir la creación manual de resúmenes de mensajes de correo electrónico. Predeterminado: Verdadero
	Permitir mensajes RCS **iOS 18.2+ Supervisado**	Seleccione para permitir la mensajería RCS. Predeterminado: Verdadero En dispositivos iOS 26 y modelos de iPad con iPadOS 26, el uso de mensajería RCS se puede limitar en los dispositivos cuyo plan móvil esté asociado con el ICCID.
	Permitir integraciones de inteligencia externa	Seleccione para habilitar el uso de servicios de inteligencia externos basados en la nube con Siri.
	Permitir el inicio de sesión de integraciones de inteligencia externa	Seleccione para permitir que los proveedores de inteligencia externos entren en modo anónimo. Si un usuario ya ha iniciado sesión en un proveedor de inteligencia externo, la aplicación de esta restricción provocará que se cierre su sesión.
	Permitir modificación del navegador predeterminado	Seleccione para habilitar la modificación de preferencias del navegador predeterminado. La configuración Ivanti Neurons for MDM le permite configurar el navegador web predeterminado.
Aplicaciones	**Todas las versiones de iOS**	Activar el acceso a aplicaciones en los dispositivos.
	Permitir instalación de aplicaciones	Seleccione esta opción para permitir que el usuario instale aplicaciones desde Apple App Store. Desmarque esta opción para desactivar la App Store y quitar este icono de la pantalla de inicio.
	Permitir el uso de la cámara Permitir el uso de Safari Activar autorrellenar	Seleccione esta opción para permitir que el usuario pueda utilizar la cámara. Desmarque esta opción para desactivar la cámara y quitar su icono de la pantalla de inicio. En dispositivos iOS 26+ y superiores, si las aplicaciones se agregan a la lista de excepciones, no se aplicará la restricción "Permitir cámara". Seleccione esta opción para permitir el uso del explorador web Safari. Desmarque esta opción para desactivar el navegador web Safari, eliminar su icono de la pantalla de inicio y evitar que los usuarios puedan abrir clips web. Seleccione esta opción para activar la característica de autorrellenar para los campos que se muestren en Safari.
	Forzar advertencia contra el fraude	Seleccione esta opción para hacer que Safari avise al usuario cuando visite sitios web que hayan sido identificados como fraudulentos o maliciosos.
	Activar JavaScript	Seleccione esta opción para activar la asistencia Javascript para Safari.

Categoría	Ajuste	Qué hacer
Safari	Bloquear ventanas emergentes **Solo supervisado: Versión 26+**	Seleccione esta opción para bloquear las ventanas emergentes en Safari.
	Permitir la eliminación del historial de Safari	Seleccione para permitir a los usuarios que borren el historial de navegación.
	Permitir la navegación privada en Safari **Todas las versiones de iOS supervisadas**	Seleccione para permitir el uso de navegación privada.
	Permitir desinstalación de aplicaciones	Seleccione esta opción para permitir que los usuarios eliminen aplicaciones del dispositivo.
	Permitir usar Game Center	Seleccione esta opción para permitir el acceso a Game Center.
	Permitir añadir amigos a Game Center	Seleccione esta opción para permitir que los usuarios puedan añadir amigos a Game Center.
	Permitir juegos para varios jugadores	Seleccione esta opción para permitir que los usuarios puedan jugar a juegos que incluyan otros usuarios.
	Permitir iMessage	Seleccione esta opción para permitir el uso de iMessage. En los dispositivos iOS 26 y en las versiones iPad con iPadOS 26, el uso de iMessage se puede limitar si el dispositivo se añade a la lista de denegados.
	Aceptar cookies	Seleccione Nunca, Siempre o De sitios visitados.
	Permitir FaceTime **iOS 8+**	Seleccione esta opción para permitir que el usuario pueda ejecutar FaceTime si la cámara está habilitada. En los dispositivos iOS 26 y en las versiones iPad con iPadOS 26, el uso de Face Time se puede limitar si el dispositivo se añade a la lista de denegados.
	Permitir que las aplicaciones administradas utilicen sincronización en la nube	Seleccione esta opción para permitir que las aplicaciones administradas utilicen sincronización en la nube.
	Permitir continuación de la actividad	Seleccione esta opción para permitir la continuación de la actividad en aplicaciones compatibles con Handoff.

Categoría	Ajuste	Qué hacer
	Supervisado por iOS 8+	
	Permitir el uso de podcasts	Seleccione esta opción para permitir el uso de Podcasts.
	iOS 9+	
	Permitir confiar en nuevos autores de aplicaciones corporativas	Seleccione esta opción para permitir al usuario que acceda a las nuevas aplicaciones corporativas.
	Supervisado por iOS 9+	
	Permitir App Store	Seleccione esta opción para permitir que el usuario acceda a la App store de Apple.
	Permitir descarga automática de aplicaciones	Seleccione esta opción para permitir que la aplicación descargue archivos, datos y actualizaciones con solicitud previa al usuario.
	Permitir aplicación de noticias	Seleccione esta opción para permitir el uso de la aplicación de noticias (News).
	Supervisado por iOS 9,3+	
	Permitir iTunes Radio	Seleccione esta opción para permitir el uso de iTunes Radio.
	Permitir Apple Music	Seleccione esta opción para permitir el uso de Apple Music.
	Permitir los id. de paquetes de aplicaciones enumerados	Seleccione esta opción para permitir que sólo se muestren o se puedan iniciar los ID de los paquetes enumerados en la matriz. Incluya el valor com.apple.webapp para permitir todos los clips web.
	Id. de paquetes de aplicaciones bloqueados	Seleccione esta opción para evitar que se muestren o puedan iniciarse los ID de paquetes enumerados en la matriz. Incluya el valor com.apple.webapp para restringir todos los clips web.
	Supervisado por iOS 13.0+	
	Permitir usar la iTunes Store	Seleccione esta opción para permitir el uso de iTunes App Store. Desmarque esta opción para desactivar iTunes App Store y quitar su icono de la pantalla de inicio.

Categoría	Ajuste	Qué hacer
iCloud	Todas las versiones de iOS	Activar acceso a los servicios de iCloud.
	Permitir copia de seguridad	Seleccione esta opción para permitir que el dispositivo pueda hacer copias de seguridad de los datos mediante el servicio Apple iCloud.
	Permitir sincronización de documentos	Seleccione esta opción para permitir que los documentos puedan sincronizarse mediante el servicio Apple iCloud.
	Permitir secuencia de fotos	Seleccione esta opción para permitir que las fotos puedan sincronizarse con sus otros dispositivos iOS mediante Apple iCloud.
	Permitir secuencias de fotos compartidas (si se desactiva, se pueden perder los datos)	Seleccione esta opción para permitir la sincronización de fotos compartidas. Si no se selecciona esta opción, pueden perderse fotografías.
	Permitir sincronización de llaves	Seleccione esta opción para permitir la sincronización de su llave.
	iOS 9+	
	Permitir biblioteca de fotografías de iCloud	Seleccione esta opción para permitir el acceso a la biblioteca de fotografías de iCloud.
	Supervisado por iOS 15+	
	Permitir retransmisión privada en la nube	Si es falso, deshabilita la Retransmisión Privada de iCloud. Predeterminado: Verdadero

Categoría	Ajuste	Qué hacer
Seguridad y privacidad	**Todas las versiones de iOS**	Activar las políticas de seguridad y privacidad.
	Permitir actualizaciones del certificado por el aire	Seleccione esta opción para permitir las actualizaciones de los certificados de raíz por el aire.
	Forzar límite y seguimiento **Todas las versiones de iOS supervisadas**	Seleccione esta opción para solicitar el uso de la característica de límite y seguimiento.
	Permitir instalación del perfil de configuración	Seleccione esta opción para permitir que los usuarios puedan instalar perfiles de configuración y certificados de manera interactiva.
	Permitir contenido generado por el usuario asistente **Supervisado por iOS 8+**	Seleccione esta opción para permitir que Siri pueda solicitar contenido generado por el usuario desde la web.
	Permitir que el usuario borre todo el contenido y ajustes en Restablecer IU	Seleccione esta opción para habilitar la opción «Borrar todo el contenido y ajustes» en la IU Restablecer iOS del dispositivo.
	Permitir hora en pantalla	Seleccione esta opción para permitir hora en pantalla (Ajustes > Hora en pantalla).
	Permitir que se envíen los datos de diagnóstico a Apple	Seleccione esta opción para permitir que se envíen automáticamente sus datos de diagnóstico a Apple.
	Permitir que los usuarios acepten certificados TLS que no son de confianza	Seleccione esta opción para permitir que el usuario del dispositivo pueda aceptar certificados HTTPS que no sean de confianza. Si no se selecciona esta opción, el dispositivo rechazará automáticamente los certificados HTTPS que no sean de confianza sin pedir la aprobación del usuario del dispositivo.
	Forzar copias de seguridad cifradas	Seleccione esta opción para solicitar copias de seguridad cifradas mediante iTunes. Se selecciona automáticamente debido a los requisitos SCEP.
	Obligar al usuario a introducir la contraseña en la iTunes Store para todas las transacciones **iOS 9+**	Seleccione esta opción para obligar al usuario del dispositivo a introducir su contraseña de iTunes para cada transacción en la App Store. Si esta opción no se selecciona, el dispositivo no podrá realizar transacciones múltiples con una única autenticación.
	Tratar AirDrop como destino no administrado	Seleccione esta opción para permitir a un usuario que acceda al uso compartido de archivos de AirDrop

Categoría	Ajuste	Qué hacer
		Predeterminado: falso
	Supervisado por iOS 9+	
	Permitir modificaciones del código de acceso del dispositivo iOS 12+	Seleccione esta opción para permitir que el usuario cambie el código de acceso del dispositivo.
	Permitir que las aplicaciones administradas escriban contactos en cuentas de contactos no administradas	Seleccione esta opción para permitir que las aplicaciones administradas escriban contactos en cuentas de contactos no administradas. Predeterminado: falso
	iOS 12+ supervisado Permitir autocompletar contraseñas	Seleccione esta opción para permitir el uso de la función de Autocompletar contraseñas en iOS y de envíos de solicitudes para usar una contraseña guardada en Safari o en las aplicaciones.
	Permitir que los dispositivos cercanos compartan solicitudes de contraseña	Seleccione esta opción para permitir que el dispositivo del usuario solicite las contraseñas de dispositivos cercanos.
	Permitir uso compartido de contraseñas Permitir que las aplicaciones no administradas lean contactos de cuentas de contactos administradas	Seleccione esta opción para permitir que los usuarios compartan sus contraseñas con la función de compartirlas por Airdrop. Seleccione esta opción para permitir que las aplicaciones no administradas puedan leer las cuentas de contactos administradas. Predeterminado: falso
	iOS 18.3	
	Permitir ID de External Intelligence Workspace Permitir el resumen de la transcripción de notas Permitir resumen de inteligencia visual	Introduzca la ID de External Intelligence Workspace permitida. Seleccione para activar la creación de resúmenes de las transcripciones. Predeterminado: Verdadero Seleccione para activar la creación de resúmenes de la inteligencia visual de Apple con imágenes o contenido visual. Predeterminado: Verdadero

Categoría	Ajuste	Qué hacer
Clasificación del contenido		Controlar acceso a aplicaciones y contenido multimedia.
	Permitir reproducción de música explícita, podcasts y soportes multimedia de iTunes U (solo supervisado iOS 13+ y tvOS 11.3 y posterior)	El contenido explícito está marcado como tal por los proveedores de contenido, como los sellos discográficos, cuando este contenido se vende a través de iTunes Store.
	Región de la calificación	Seleccione una región de la lista desplegable para cambiar la región asociada a la clasificación de las selecciones para aplicaciones, programas de televisión y películas.
	Películas	Seleccione un límite de clasificación por edad para las películas que se almacenen en el dispositivo: • No permitir películas • G • PG • PG-13 • R • NC-17 • Permitir todas las películas
	Programas de televisión	Seleccione un límite de clasificación por edad para los programas de televisión que se almacenen en el dispositivo: • No permitir series de televisión • TV-Y • TV-Y7 • TV-G • TV-PG • TV-14 • TV-MA • Permitir todos los programas de televisión
	Aplicaciones	Seleccione un límite de clasificación por edad para las aplicaciones que se almacenen en el dispositivo: • No permitir aplicaciones • 4+ • 9+ • 12+ • 17+

Categoría	Ajuste	Qué hacer
		• Permitir todas las aplicaciones

Para obtener más información, consulte **Cómo crear una configuración**

10.10.4.27. Visualización de la sala de conferencias

Aplicable a: tvOS 10.2 y la versión más reciente compatible.

Esta configuración activará el modo Visualización de la sala de conferencias en Apple TV. El modo de Visualización de la sala de conferencias bloquea Apple TV en ese modo, para evitar otros tipos de uso.

A partir de tvOS 10.2, se pueden configurar los dispositivos supervisados de Apple TV en el modo Visualización de la sala de conferencias. El modo Visualización de la sala de conferencias bloquea los dispositivos de Apple TV en una pantalla de fondo negro y descarga un protector de pantalla predeterminado, a menos que se definan manualmente una imagen de fondo y un protector de pantalla en la configuración del dispositivo de Apple TV. Este modo también puede mostrar un mensaje según la configuración de Visualización de la sala de conferencias.

La configuración de Visualización de la sala de conferencias se puede implementar automáticamente y las aplicaciones se pueden instalar mientras los dispositivos están en este modo. Un dispositivo configurado en modo Visualización de la sala de conferencias que se reinicia reanudará automáticamente la pantalla bloqueada sin mostrar primero la pantalla de inicio.

> si un dispositivo de Apple TV funciona en modo Single-App o si el modo Single-App se implementa con la opción Visualización de la sala de conferencias, esta opción anulará el modo Single-App. Además, si un dispositivo de Apple TV está conectado a una red a través de Ethernet, la Visualización de la sala de conferencias no mostrará automáticamente una red Wi-Fi a la que unirse para compartir AirPlay. Esta instrucción se puede mostrar en la pantalla usando el campo de Mensaje personalizado de la configuración de Visualización de la sala de conferencias.

Creación de una configuración de Visualización de la sala de conferencias

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **conferencias** en el campo de búsqueda y, a continuación, haga clic en la configuración de las **Visualización de la sala de conferencias**.
4. Introduzca un nombre y describa la configuración.
5. Especifique el **Mensaje personalizado**. Este es el mensaje personalizado que se muestra en el modo Visualización de la sala de conferencias.
6. Haga clic en **Siguiente** para configurar los ajustes de distribución.
7. Haga clic en **Hecho**.

Para obtener más información, consulte Cómo crear una configuración.

10.10.4.28. Ajustes del teclado

Utilice los **Ajustes del teclado** para configurar el teclado en dispositivos supervisados. Esta declaración ayuda a los administradores a aplicar controles coherentes basados en políticas para gestionar el comportamiento del teclado, las opciones de entrada y los ajustes relacionados con la experiencia del usuario.

Disponible para:

- iOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- macOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Busque **Ajustes del teclado** y seleccione la configuración correspondiente.
3. Configure los **Ajustes del teclado** según la siguiente tabla:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Permitir corrección automática	Seleccione la casilla para habilitar la función Corrección automática. Active **Enviar al dispositivo** para habilitar la corrección automática en dispositivos supervisados. Este ajuste no se aplica a dispositivos macOS.
Permitir búsqueda de definición	Seleccione la casilla para habilitar la función Búsqueda de definición. Active **Enviar al dispositivo** para habilitar la función Búsqueda de definición en dispositivos supervisados.
Permitir dictado	Seleccione la casilla para habilitar la función Dictado. Active **Enviar al dispositivo** para habilitar la función Dictado en dispositivos supervisados.
Permitir sugerencias matemáticas del teclado	Seleccione la casilla para habilitar las sugerencias matemáticas del teclado. Active **Enviar al dispositivo** para habilitar las sugerencias matemáticas del teclado en dispositivos supervisados.
Permitir texto predictivo	Seleccione la casilla para habilitar la función Texto predictivo. Active **Enviar al dispositivo** para habilitar la función Texto predictivo en dispositivos supervisados. Este ajuste no se aplica a dispositivos macOS.
Permitir deslizar para escribir	Seleccione la casilla para habilitar la función Deslizar para escribir. Active **Enviar al dispositivo** para habilitar la función Deslizar para escribir en dispositivos supervisados. Este ajuste no se aplica a dispositivos macOS.
Permitir corrección ortográfica	Seleccione la casilla para habilitar la función Corrección ortográfica. Active **Enviar al dispositivo** para habilitar la función Corrección ortográfica en dispositivos supervisados. Este ajuste no se aplica a dispositivos macOS.
Permitir sustitución de texto	Seleccione la casilla para habilitar la función Sustitución de texto. Active **Enviar al dispositivo** para habilitar la función Sustitución de texto en dispositivos supervisados. Este ajuste no se aplica a dispositivos macOS.

4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Seleccione una de las opciones de distribución para configurar los **Ajustes del teclado**. Para más información sobre la configuración de las opciones de distribución, consulte Trabajar con configuraciones.
6. Haga clic en **Hecho**.

10.10.4.29. Bloqueo y kiosco: modo de administrador de dispositivos de Android

Bloqueo y kiosco: el modo Administrador del dispositivo de Android desactiva ciertas características de los dispositivos Android y crea una lista de permitidos para aplicaciones que estarán disponibles para los usuarios en el modo kiosco.

> La Configuración del modo de administración de dispositivos de Android se ha dejado de usar y ya no es compatible con dispositivos de Android 8 y versiones posteriores. Se recomienda usar Android Enterprise Lockdowns para Kiosk Lockdowns en Android 8 y versiones posteriores.

Puede restringir la opción de modificar ajustes o aplicaciones cuando un dispositivo Android está en modo kiosco.

- Añada aplicaciones y seleccione los ajustes en la página de configuración Crear bloqueo y kiosco: modo administrador del dispositivo de Android.
- La opción para cambiar los ajustes utilizando el icono Ajustes estará disponible en el modo kiosco.
- Seleccione aplicaciones sin seleccionar ninguna opción de configuración de los ajustes y el icono de ajustes no aparecerá en el modo kiosco.
- Si decide no incluir ninguna aplicación en la configuración, el icono de los ajustes sí aparecerá.

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Ajustes de bloqueo: desactive las características para todos los dispositivos Android.	
Desactivar Wi-Fi	Seleccione esta opción para desactivar el acceso a las LAN inalámbricas.
Desactivar cámara	Seleccione esta opción para desactivar el acceso a la cámara.
Desactivar Bluetooth	Seleccione esta opción para desactivar las características del Bluetooth. tenga cuidado al utilizar esta opción. Ivanti no recomienda desactivar el audio porque el acceso al Bluetooth manos libres está desactivado. Cada vez son más comunes los requisitos legales para el uso de dispositivos manos libres mientras se conduce.
Ajustes del modo kiosco: permite utilizar el dispositivo como kiosco, con el funcionamiento restringido a algunas aplicaciones específicas. Los ajustes del modo Kiosco no se aplicarán a ningún dispositivo con Android 8.0 o superior. Para dichos dispositivos, el estado del kiosco en la página de detalles del dispositivo indica UNSUPORTED_ON_DEVICE como estado del kiosco.	
Activar el modo kiosco	Seleccione esta opción para configurar el **Modo kiosco** en dispositivos Android.
Desactivar los ajustes rápidos	Seleccione esta opción para desactivar los Ajustes rápidos en el modo kiosco.
Permitir al usuario acceder a los ajustes Wi-Fi	Seleccione esta opción para permitir que un usuario cambie los ajustes de Wi-Fi y acceda a las redes inalámbricas preferidas.
Permitir al usuario acceder a los ajustes Bluetooth	Seleccione esta opción para permitir que un usuario cambie los ajustes del Bluetooth y sincronice dispositivos Bluetooth adicionales.
Permitir al usuario acceder a los ajustes de localización	Seleccione esta opción para permitir a un usuario que acceda a los ajustes de localización.

Ajuste	Qué hacer
Permitir al usuario retrasar las actualizaciones de la aplicación	Seleccione esta opción para permitir que un usuario retrase las actualizaciones de la aplicación.
PIN para salir del modo kiosco	Introduzca el código de cuatro dígitos que el usuario final debe escribir para poder salir del modo kiosco.
Crear una lista de permitidos de aplicaciones: estas aplicaciones estarán disponibles para los usuarios en el modo kiosko al añadir aplicaciones a la lista de aplicaciones permitidas. Arrastre y suelte para organizar las aplicaciones en el orden en que deben aparecer en el selector del modo Kiosko. Al añadir una aplicación a la lista de aplicaciones permitidas no se instalará la aplicación en el dispositivo. Asegúrese de distribuir cada aplicación a los usuarios y grupos de usuarios adecuados en el App Catalog.	
Aplicaciones integradas	Haga clic en +Añadir para incluir las aplicaciones nativas mencionadas en el grupo de aplicaciones permitido en el modo kiosco. si ha desactivado «Marcador» o «Cámara» en los ajustes de bloqueo anteriores, no podrán añadirse a la lista de aplicaciones permitidas.
Catálogo de aplicaciones	Haga clic en +Añadir para incluir las aplicaciones mencionadas del catálogo de aplicaciones en el grupo de aplicaciones permitido en el modo kiosco.
Otras aplicaciones	Haga clic en +Añadir para añadir el **nombre del paquete** de una aplicación que no esté disponible en la Google Play Store.
Aplicaciones permitidas en el modo kiosco	Haga clic en X para desinstalar una aplicación del grupo de aplicaciones permitido en el modo kiosco. Arrastre y suelte para cambiar el orden en que aparecen las aplicaciones de los dispositivos en modo kiosco.

> para los dispositivos Samsung con Knox Standard 4.0 o posterior, la característica multiusuario se bloquea automáticamente en el modo kiosco.

Para dispositivos que no son Samsung, el modo Kiosco no es compatible en Android 8.0 o superior. Ivanti recomienda utilizar los bloqueos de la versión corporativa de Android para el modo Kiosco en Android 8.0 o posterior.

Temas relacionados:

- **Configurar el modo kiosco para Android**
- **Cómo crear una configuración**

10.10.4.30. Configurar el modo kiosco para Android

Esta sección contiene los siguientes temas:

- Iniciar el modo kiosco de forma remota
- Salir de modo kiosco

Licencia: Silver

El modo kiosco para dispositivos Android le permite restringir el uso de un dispositivo a aplicaciones específicas. Puede utilizar el modo kiosco para configurar dispositivos para empleados que utilicen solo aplicaciones específicas para el trabajo.

Cuando prepare los dispositivos Android para el modo kiosco o el modo Propietario del dispositivo con el modo kiosco, tendrá que crear una lista de permitidos de aplicaciones que desee poner disponible para los usuarios en el Modo kiosco. Para dispositivos que empleen el modo Propietario del dispositivo, puede añadir aplicaciones a la lista de aplicaciones permitidas arratrándolas y soltándolas para ordenar las aplicaciones en el orden en que deben aparece en el selector del Modo kiosco cuando se configure la aplicación. Consulte Configuración de bloqueo y kiosco para obtener más información.

Requisitos previos

Antes de configurar el modo kiosco para Android, asegúrese de haber realizado las siguientes tareas:

- Instalado Go en los dispositivos.
- Configurado el catálogo de la aplicación con las aplicaciones que la configuración del kiosco necesitará.
- Distribuido el catálogo de aplicaciones a los dispositivos que funcionarán en el modo kiosco.

> Los dispositivos SonimXP5S no son compatibles con el modo Kiosco.

- Instalado las aplicaciones que necesitará la configuración de su kiosco.
- (Opcional) Configurar Personalización de marca del kiosko de Android.

> El modo kiosko es compatible con Android 5.1 y 6.0. Los dispositivos que no sean Samsung Knox se deben colocar en modo Propietario del dispositivo para evitar el uso de aplicaciones no deseadas.

Importante: algunos dispositivos tienen funciones que pueden provocar que el dispositivo se salga de la pantalla o se cree un escape de cualquier otro tipo del modo kiosco. La función «People Edge» del Samsung Galaxy S6 Edge es un ejemplo de esta función. Recomendamos que un administrador desactive este tipo de funciones antes de implementar el dispositivo.

Procedimiento

1. Vaya a **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Haga clic en **Bloqueo y kiosco: modo de administrador de dispositivos de Android**.
4. En la pantalla **Crear ajustes**, complete al menos la sección **Ajustes del modo kiosco**.
5. En la pantalla **Distribución**, seleccione los grupos dispositivos que recibirán esta configuración.
6. Haga clic en **Hecho**.
7. Para dispositivos que no son Samsung, continúe con los siguientes pasos:
    1. Vaya a **Dispositivos** >**Dispositivos**.

2. Seleccione los dispositivos que desea habilitar para el modo kiosco.
3. Seleccione **Acciones** > **Forzar ingreso**.
4. En los dispositivos, toque el botón **Modo Kiosco**.
5. Presione el botón **Inicio** en el dispositivo.
6. Si aparece el diálogo **Elegir selector**, pulse **Selector del kiosco Go** y seleccione **Siempre**. Este paso es necesario para garantizar que se utiliza el selector correcto para esta característica. De lo contrario, se pediría al usuario que seleccione un selector cualquiera.

Iniciar el modo kiosco a distancia

Procedimiento

1. Vaya a **Dispositivos > Dispositivos**.
2. Añada la columna Modo kiosco a la pantalla.
3. Seleccione los dispositivos que tienen habilitado el modo kiosco, pero que no estén actualmente en modo kiosco.
4. Seleccione **Acciones > Entrar en modo kiosco**.

Salir de modo kiosco

Puede salir del modo kiosco en el dispositivo si establece un código PIN en la configuración.

Procedimiento

1. Pulse el icono **Ajustes**.
2. Seleccione **Salir del modo kiosko**.
3. Pulse el campo **PIN del kiosco** cuando se le solicite.
4. Salga del PIN del kiosco.

Puede salir del modo kiosco en un dispositivo específico desde el portal:

Procedimiento

1. Vaya a **Dispositivos > Dispositivos**.
2. Muestre los detalles del dispositivo.
3. Seleccione **Acciones > Salir del modo kiosco**.

También puede utilizar los siguientes métodos para salir del modo kiosco:

- Eliminar la configuración
- Desactivar la configuración
- Quitar el grupo de dispositivos de la configuración

10.10.4.31. Configurar el kiosco del dispositivo compartido Android

Para implementaciones de Task Worker, es posible que las empresas ofrezcan dispositivos Android dedicados que están personalizados para una función de usuario específica. Dependiendo del perfil del usuario, se pueden presentar diferentes aplicaciones y configuraciones en un mismo dispositivo. Por ejemplo, a un usuario que tenga una función técnica se le puede presentar un conjunto específico de aplicaciones para que las use, mientras que otro usuario con una función de mantenimiento puede tener acceso a un conjunto distinto de aplicaciones.

El modo kiosko de dispositivos compartidos de Android actúa como un filtro de aplicaciones para distintos grupos de usuarios que comparten dispositivos. Un usuario que haya iniciado sesión en el kiosco del dispositivo compartido solo podrá ver las aplicaciones adecuadas para su función. Una de las principales ventajas del kiosco del dispositivo compartido es que usted puede permitir que diferentes grupos de usuarios accedan a distintos conjuntos de aplicaciones desde el mismo dispositivo. Cuando un usuario cierra sesión en un dispositivo Android compartido en modo kiosko, sus aplicaciones y datos de usuario, incluido el historial, se borran de la pantalla del siguiente usuario que inicie sesión en el dispositivo (si la aplicación está marcada para ser reinstalada). El kiosco del dispositivo compartido solo estará disponible para implementaciones de la versión corporativa de Android con cuentas administradas por Google Play.

El kiosco del dispositivo compartido requiere dos tipos de usuarios, un usuario provisional y un usuario del kiosco compartido y, además, al menos dos políticas que se correspondan con esos usuarios. El usuario provisional se utiliza para solicitar la aparición de la pantalla de inicio de sesión en un dispositivo compartido. Asimismo, el usuario provisional es un tipo especial de usuario administrador que permite a otros usuarios iniciar sesión en el dispositivo real del kiosco. Una vez que el usuario del kiosco del dispositivo compartido inicia sesión correctamente, la política provisional se sustituye por la política del kiosco compartido. El usuario del kiosco tiene acceso a las aplicaciones instaladas en el dispositivo conforme a la política asignada a este. Aunque se pueden crear múltiples políticas de dispositivos compartidos, solamente habrá una política de kiosco activa a la vez en el dispositivo de un kiosco. Cuando el usuario del kiosco cierra sesión en el kiosco compartido, el dispositivo se revierte al usuario provisional y, por extensión, a la política provisional.

El usuario provisional solo tienen la capacidad de acceder a la página de inicio de sesión. Por eso, deberá crear una política provisional que esté dedicada a este usuario. Por otro lado, los usuarios del kiosco del dispositivo compartido podrán acceder al conjunto de aplicaciones que usted defina en su política. (Naturalmente, también necesita instalar las aplicaciones permitidas en los dispositivos del kiosko de dispositivo compartido). La política de kiosko de dispositivo compartido le permite crear un filtro de aplicaciones permitidas a partir de todas las aplicaciones que instaló anteriormente. No se pueden cargar directamente aplicaciones en una política del kiosco compartido. A menudo recomendamos que dedique una política de kiosco compartido a un tipo de usuario de kiosco compartido, o grupo de usuarios, dependiendo de su organización. Por ejemplo, es posible que una empresa tenga empleados con turno de día y con turno de noche que tengan distintas funciones y requieran acceso a conjuntos de aplicaciones diferentes. En este caso, hay que crear una política de turnos de día y otra de turnos de noche.

Para obtener más información sobre la habilitación del kiosco de dispositivos compartidos, consulte **Bloqueo y kiosco: Android Enterprise**

10.10.4.32. Bloqueo y kiosco: Android Enterprise

La configuración Bloqueo y kiosco: el modo Administrador del dispositivo de Android Enterprise desactiva ciertas características de los dispositivos Android Enterprise y crea una lista de permitidos de aplicaciones que estarán disponibles para los usuarios en el modo kiosco.

Esta sección contiene los siguientes temas:

- Ajustes de bloqueo
- Perfil de trabajo
- Dispositivos administrados en el trabajo (Configuraciones Propietario del dispositivo y Modo kiosco)
- Dispositivo administrado con perfil de trabajo/perfil de trabajo en los ajustes de bloqueo del dispositivo propiedad de la empresa

Ajustes de bloqueo

Ajuste	Descripción
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Elegir el tipo de bloqueo	Seleccione el tipo de ajustes de bloqueo que desea configurar: • Perfil de trabajo • Dispositivos administrados en el trabajo (Configuraciones Propietario del dispositivo y Modo kiosco) • Dispositivo administrado con perfil de trabajo/perfil de trabajo en los ajustes de bloqueo del dispositivo propiedad de la empresa el perfil de trabajo de los ajustes de bloqueo del dispositivo propiedad de la empresa solo es aplicable a los dispositivos Android 11+. Solo se permite un tipo por configuración. Las opciones que se muestran dependen del tipo que haya seleccionado. si un dispositivo administrado en el trabajo (propietario del dispositivo) y un dispositivo administrado con Perfil de trabajo en el Dispositivo propiedad de la empresa se distribuyen al mismo dispositivo, el dispositivo administrado con Perfil de trabajo tiene prioridad.

Perfil de trabajo

Desactiva ciertas características en los dispositivos con Android Enterprise.

Ajuste	Qué hacer	Para dispositivos
Desactivar captura de pantalla	Seleccione esta opción para desactivar la posibilidad de usar la característica de captura de pantalla integrada del dispositivo.	• Android 5.0 +
No permitir el Control de aplicaciones	Seleccione esta opción para impedir que un usuario modifique aplicaciones en Ajustes o en selectores.	• Android 5.0 +
No permitir Credenciales de configuración	Seleccione esta opción para impedir que un usuario configure las credenciales.	• Android 5.0 +
No permitir Copiar/Pegar perfil cruzado	Seleccione esta opción para impedir copiar/pegar información entre perfiles.	• Android 5.0 +
No permitir Modificar cuentas	Seleccione esta opción para impedir que un usuario añada o elimine cuentas.	• Android 5.0 +
No permitir transferencia de salida	Seleccione esta opción para impedir a un usuario que use NFC para transferir datos de las aplicaciones.	• Android 5.1 +
No permitir Compartir localización	Seleccionar esta opción para impedir que un usuario revele a las aplicaciones la localización del dispositivo.	• Android 5.0 +
No permitir características de depuración	Seleccione esta opción para desactivar las características de depuración en los dispositivos. Esta opción está activada de forma predeterminada.	• Android 5.0 +
Asegurar Verify Apps	Seleccione para permitir las funciones de verificación de aplicaciones en los dispositivos. Esta opción está activada de forma predeterminada. cuando esta opción esté desactivada, el dispositivo volverá a su comportamiento predeterminado, el cual podrá variar según el dispositivo.	• Android 5.0 +
Desactivar fuentes desconocidas en el	Seleccione esta opción para evitar que el dispositivo instale aplicaciones de orígenes desconocidos.	• Android

Ajuste	Qué hacer	Para dispositivos
dispositivo	para que este ajuste entre en vigor en el dispositivo dependerá de que una actualización esperada de Google Play habilite esta función.	5.0 +
Restringir métodos de entrada	Seleccione esta opción para restringir los nombres de paquetes IME puestos en la lista de permitidos designando una lista de nombres de paquetes en la lista de permitidos a través del campo **Nombre del paquete**. Los dispositivos tendrán disponibles tanto los métodos de entrada de paquetes de la lista de permitidos como los métodos de entrada del sistema predeterminado. El usuario puede cambiar entre los métodos de entrada del sistema predeterminado y los métodos de entrada de los paquetes de la lista de permitidos. para Android 10+, la lista de permitidos se aplica a las aplicaciones IME solo en el lado del perfil de trabajo. Para versiones anteriores de Android, la lista de permitidos es aplicable a las aplicaciones IME de todo el dispositivo (tanto dentro como fuera del perfil de trabajo).	• Android 5.0 +
Restringir servicios de accesibilidad	Seleccione esta opción para restringir los servicios de accesibilidad para aplicaciones profesionales designando una lista de nombres de paquetes en la lista de permitidos a través del campo **Nombre del paquete**. Si no hay ningún paquete en la lista de permitidos, solo se permitirán los servicios de accesibilidad del sistema.	• Android 5.0 +
Desactivar fuentes desconocidas dentro del perfil de trabajo	Seleccione esta opción para no permitir la descarga de fuentes desconocidas dentro del perfil de trabajo.	• Android 5.0 +
Activar/desactivar aplicaciones del sistema	Seleccione esta opción para habilitar y deshabilitar que se puedan instalar aplicaciones del sistema designando dos listas de nombres de paquetes mediante los campos **Nombre del paquete de la aplicación del sistema**. Utilice esta característica para administrar el acceso a las aplicaciones del sistema que no estén publicadas en Google Play. añadir una aplicación al catálogo de aplicaciones y también a una lista de aplicaciones del sistema no es compatible.	• Android 5.0 +
Desactivar el Id. de llamada	Establece si la información del Id. de llamada del perfil de trabajo se mostrará en el dispositivo para las llamadas entrantes.	• Android 6,0 +
Desactivar Compartir contactos por Bluetooth	Seleccione esta opción para evitar que el dispositivo pueda compartir contactos con otros dispositivos por Bluetooth.	• Android 6,0 +
Desactivar Compartir contactos	Seleccione esta opción para evitar que los usuarios puedan buscar contactos del trabajo desde el marcador del teléfono personal.	• Android

Ajuste	Qué hacer	Para dispositivos
mediante búsquedas		7.0 +
No permitir autorrellenado	Seleccionar para no permitir el auto-rellenado	• Android 8,0 +
Desactivar las notificaciones en aplicaciones del trabajo en el perfil personal	Seleccione esta opción para restringir las notificaciones del perfil de trabajo.	• Android 8,0 +
No permitir impresión	Seleccione esta opción para restringir la impresión desde todas las aplicaciones.	• Android 9.0 +
Desactivar el uso compartido en el perfil	Seleccione esta opción para evitar que los usuarios compartan datos personales en un perfil de trabajo del dispositivo.	• Android 9.0 +
Permitir el acceso a los calendarios del perfil de trabajo	Seleccione cualquiera de las siguientes opciones para permitir todas las aplicaciones o seleccione un conjunto de aplicaciones en el lado personal para que accedan a la información del calendario presente en el perfil de trabajo: • **Todas las aplicaciones en el perfil personal**: permite que todas las aplicaciones accedan a la información del calendario que hay en el perfil de trabajo. • **Solo las siguientes aplicaciones del perfil personal**: en el siguiente campo de texto, introduzca los las Id. de las aplicaciones separadas por una coma. Solo estas aplicaciones seleccionadas del lado personal podrán acceder a la información del calendario presente en el perfil de trabajo. La aplicación del lado personal debería implementar las API específicas para poder acceder al calendario compartido.	• Android 10.0 +
Habilite la lista de permitidos de perfiles cruzados de las aplicaciones	Seleccione esta casilla para permitir a los usuarios compartir información de aplicaciones específicas desde el perfil de trabajo hasta el lado personal del dispositivo. En el campo **Aplicaciones en la lista de permitidos**, escriba los ID de paquete de las aplicaciones que se van a incluir en la lista de permitidos, separados por comas. De forma predeterminada, esta opción está desactivada.	• Android 11.0 +
Habilitar segmentación de red 5G	Seleccione para proporcionar una opción de segmentación de redes 5G en el perfil de trabajo de los dispositivos de empresa. De forma predeterminada, esta opción está desactivada.	• Android

Ajuste	Qué hacer	Para dispositivos
Rechazar la opción de compartir Wi-Fi configurado por el administrador	Seleccione esta opción para impedir que los usuarios compartan las configuraciones Wi-Fi establecidas por el administrador.	12.0 + • Android 13.0 +
Desactivar la asistencia de IA	Seleccione para evitar que los usuarios de las funciones de asistencia de IA. De forma predeterminada, esta opción está desactivada.	• Android 15.0 +

Dispositivos administrados en el trabajo (Configuraciones Propietario del dispositivo y Modo kiosco)

Desactiva ciertas características en los dispositivos administrados en el trabajo (modo Propietario del dispositivo) para Android 5.0+.

Ajuste	Descripción
Desactivar Wi-Fi	Seleccione esta opción para desactivar el acceso a las LAN inalámbricas.
Desactivar ajustes de Wi-Fi	Seleccione esta opción para desactivar el acceso a los ajustes inalámbricos.
Desactivar cámara	Seleccione esta opción para desactivar el acceso a la cámara.
Desactivar Bluetooth (Android 8.0+)	Seleccione esta opción para desactivar las características del Bluetooth. tenga cuidado al utilizar esta opción. Ivanti no recomienda desactivar el audio porque el acceso al Bluetooth manos libres está desactivado. Cada vez son más comunes los requisitos legales para el uso de dispositivos manos libres mientras se conduce.
No permitir ajustes de Bluetooth (Android 8.0+)	Seleccione esta opción para desactivar el acceso a los ajustes Bluetooth.
Desactivar captura de pantalla	Seleccione esta opción para desactivar la posibilidad de usar la característica de captura de pantalla integrada del dispositivo.
Desactivar el reinicio de la red	Seleccione esta opción para evitar el restablecimiento de la red. (Aplicable a dispositivos Android 7.0+ y no compatible en el modo Perfil de trabajo en el Dispositivo propiedad de la empresa).
Silenciar volumen principal	Seleccione esta opción para silenciar el volumen principal.
No permitir el Control de aplicaciones	Seleccione esta opción para impedir que un usuario modifique aplicaciones en Ajustes o en selectores.
No permitir credenciales	Seleccione esta opción para impedir que un usuario configure las credenciales.
No permitir emisiones de emergencia	Seleccione esta opción para impedir emisiones de emergencia.
No permitir redes móviles	Seleccione esta opción para desactivar el acceso a las redes móviles. Esta opción no se puede desactivar si la Wi-Fi está desactivada.
No permitir tethering	Seleccione esta opción para desactivar el tethering como alternativa para usar la conexión a Internet de un dispositivo con el fin de proporcionar acceso a Internet a otro dispositivo.
No permitir VPN	Seleccione esta opción para desactivar las conexiones VPN.
No permitir configuración predeterminada de fábrica	Seleccione esta opción para evitar que los usuarios puedan devolver el dispositivo a los valores predeterminados de fábrica.
Activar protección de restablecimiento de valores de fábrica	Seleccione esta opción para permitir que los usuarios puedan devolver el dispositivo a los valores predeterminados de fábrica. Opcionalmente, puede especificar una lista de Id. de cuentas Google autorizadas (un valor entero) que pueda aprovisionar el dispositivo después del restablecimiento de fábrica o dejar el cursor sobre el icono de ayuda para ver ayuda sobre cómo recuperar Id. de cuentas autorizadas.

Ajuste	Descripción
No permitir Modificar cuentas	Seleccione esta opción para impedir que un usuario añada o elimine cuentas.
No permitir NFC (transferencia de salida)	Seleccione esta opción para impedir a un usuario que use NFC para transferir datos de las aplicaciones.
No permitir llamadas salientes	Seleccione esta opción para impedir que un usuario haga llamadas salientes.
No permitir el reinicio en modo seguro (Android 6.0+)	Seleccione esta opción para evitar que los usuarios reinicien un dispositivo en modo seguro.
No permitir Compartir localización	Seleccionar esta opción para impedir que un usuario revele a las aplicaciones la localización del dispositivo.
No permitir características de depuración	Seleccione esta opción para desactivar las características de depuración en los dispositivos. Esta opción está activada de forma predeterminada.
Asegurar Verify Apps	Seleccione para permitir las funciones de verificación de aplicaciones en los dispositivos. Esta opción está activada de forma predeterminada. cuando esta opción esté desactivada, el dispositivo volverá a su comportamiento predeterminado, el cual podrá variar según el dispositivo.
No permitir SMS	Seleccione esta opción para impedir que un usuario envíe y reciba mensajes SMS.
No permitir Silenciar micrófono	Seleccione esta opción para impedir que un usuario silencie el micrófono del dispositivo.
No permitir hora automática	Seleccione esta opción para impedir que un usuario active los cambios automáticos de hora.
No permitir zona de hora automática	Seleccione esta opción para impedir que un usuario active el ajuste automático de la hora del dispositivo con los cambios de zona horaria.
Sincronizar hora con el servidor (Android 9.0+)	Seleccione esta opción para permitir que los dispositivos sincronicen la hora con los servidores de Ivanti Neurons for MDM la primera vez al registrarse y, a partir de entonces, una vez cada 24 horas después de cada registro. Esta opción solo estará disponible si se selecciona la opción **Desactivar el tiempo automático**.
Configurar zona horaria (Android 9.0+)	Especifique la cadena de Zona horaria en formato de ID de zona horaria de Olson (por ejemplo, Pacific/Midway).
Desactivar itinerancia de datos	Seleccione esta opción para desactivar el intercambio de datos mientras el dispositivo está en itinerancia.
No permitir suspensión de Wi-Fi	Seleccione esta opción para mantener la Wi-Fi activada mientras dispositivo esté en modo suspensión.
Restringir métodos de entrada	Seleccione esta opción para restringir los nombres de paquetes IME puestos en la lista de permitidos designando una lista de nombres de paquetes en la lista de permitidos a través del campo **Nombre del paquete**. Los dispositivos tendrán disponibles tanto los métodos de entrada de paquetes de la lista de permitidos

Ajuste	Descripción
	como los métodos de entrada del sistema predeterminado. El usuario puede cambiar entre los métodos de entrada del sistema predeterminado y los métodos de entrada de los paquetes de la lista de permitidos. Para Android 10+, la lista de permitidos se aplica a las aplicaciones IME solo en el lado del dispositivo. Para versiones anteriores de Android, la lista de permitidos es aplicable a las aplicaciones IME de todo el dispositivo.
Restringir servicios de accesibilidad	Seleccione esta opción para restringir los servicios de accesibilidad para aplicaciones profesionales designando una lista de nombres de paquetes en la lista de permitidos a través del campo **Nombre del paquete**. Si no hay ningún paquete en la lista de permitidos, solo se permitirán los servicios de accesibilidad del sistema.
Desactivar transferencia de archivos USB	Seleccione esta opción para desactivar la transferencia de archivos USB.
Desactivar elementos multimedia externos	Seleccione esta opción para desactivar los elementos multimedia externos.
Desactivar el protector de teclado (no tendrá efecto si está configurado el PIN/código de acceso)	Seleccione esta opción para desactivar el protector de teclado. Esta opción no tiene efecto si se ha establecido una contraseña, un PIN o un patrón. si se establece una contraseña, un PIN o un patrón después de desactivar la protección de teclado, esta deja de estar desactivada.
Mantener la pantalla encendida mientras esté conectada a la corriente.	Seleccione esta opción para mantener la pantalla ENCENDIDA cuando esté conectada a la alimentación. La pantalla puede atenuarse, pero no se apaga mientras el dispositivo está conectado a una fuente de alimentación. este ajuste solo tendrá efecto si no se utiliza el autobloqueo ni el tiempo de espera por inactividad en la configuración de la contraseña para establecer un tiempo de espera.
No permitir la creación de ventanas	Seleccione esta opción para evitar que las aplicaciones muestren ciertos tipos de ventanas superpuestas, como alertas e iconos de tostada.
Saltar consejos para el primer uso No permitir fuentes desconocidas en el dispositivo	Seleccione esta opción para activar la recomendación del sistema para que las aplicaciones omitan el tutorial de usuario y otras sugerencias introductorias durante la primera puesta en marcha. Seleccione esta opción para no permitir que el usuario instale aplicaciones de orígenes desconocidos.
Configurar el mensaje de la pantalla de bloqueo (Android 7.0+)	Seleccione esta opción para configurar el mensaje de la pantalla de bloqueo que se mostrará en el dispositivo. Escribir el mensaje de la pantalla de bloqueo (máximo de 256 caracteres) en el campo de texto. Al activar esta opción, se bloquea al usuario para que no pueda configurar el mensaje en Ajustes y se muestra al usuario el mensaje configurado por el administrador. Si el administrador no proporciona ningún mensaje de pantalla de bloqueo después de activar la opción «Configurar el mensaje de la pantalla de bloqueo», el usuario

Ajuste	Descripción
	tiene bloqueada la posibilidad de configurar el mensaje en Ajustes, pero no se muestra ningún mensaje al usuario.
Establecer el brillo de la pantalla	Seleccionar para establecer el brillo de la pantalla del dispositivo. • Manual: seleccione para introducir un número manualmente (0 a 255) • Adaptable: seleccione permitir que el dispositivo establezca el brillo Es recomendable activar la opción "Desactivar el brillo de la pantalla de configuración" antes de ajustar el brillo de la pantalla del dispositivo.
Establecer el tiempo de espera de la pantalla	Seleccionar para establecer la duración del tiempo de espera de la pantalla (en segundos). Es recomendable activar la opción "Desactivar el tiempo de espera de la pantalla de configuración" antes de ajustar el brillo de la pantalla del dispositivo.
Establecer la orientación de la pantalla	Seleccionar para establecer la orientación de la pantalla. Puede establecer la orientación de pantalla a 0, 90, 180 o 270 grados desde la lista desplegable. Esta opción no está seleccionada de forma predeterminada. Para la aplicación Go versión 89 y posterior, debe seleccionar esta opción y establecer el valor 0 para mantener el dispositivo en modo Horizontal en Kiosko.
Activar/desactivar aplicaciones del sistema **Android 8,0+** No permitir autorrellenado	Seleccione esta opción para habilitar y deshabilitar que se puedan instalar aplicaciones del sistema designando dos listas de nombres de paquetes mediante los campos **Nombre del paquete de la aplicación del sistema**. Utilice esta característica para administrar el acceso a las aplicaciones del sistema que no estén publicadas en Google Play. Añadir una aplicación al Catálogo de aplicaciones y también a una lista de aplicaciones del sistema no es una acción compatible. Seleccione esta opción para impedir que el usuario haga uso de los servicios de autorrellenado.
No permitir uso compartido de Bluetooth	Seleccione esta opción para impedir que el usuario compartir el Bluetooth de salida en el dispositivo.
No permitir servicio de copia de seguridad **Android 9.0 +** No permitir impresión No permitir modo avión No permitir Ambient Display	Seleccione esta opción para desactivar el servicio de copia de seguridad. Seleccione esta opción para impedir al usuario que pueda imprimir. Seleccione esta opción para desactivar el modo avión en todo el dispositivo. Seleccione esta opción para no permitir la función «Ambient display» para el usuario.

Ajuste	Descripción
No permitir config. de brillo	Seleccione esta opción para impedir al usuario que configure el brillo. Es recomendable definir los valores de "Establecer el modo de brillo de la pantalla" antes de seleccionar esta opción.
No permitir config. de fecha y hora	Seleccione esta opción para impedir al usuario que configure la fecha, hora y zona horaria.
No permitir config. de localización	Seleccione esta opción para impedir al usuario que desactive los proveedores de localización.
No permitir config. de tiempo de espera de pantalla **Android 12.0+**	Seleccione esta opción para impedir al usuario que cambie el tiempo de espera de apagado de la pantalla. Es recomendable definir los valores de "Establecer tiempo de espera de la pantalla" antes de seleccionar esta opción.
Habilitar USB solo para carga **Android 13.0+**	Seleccione para habilitar el puerto USB solo para cargar.
Establecer la seguridad de Wi-Fi mínima requerida	Utilice esta opción para establecer la seguridad WiFi mínima requerida: • No es necesaria una seguridad mínima: seleccione esta opción si no se requiere un nivel de seguridad mínimo • Seguridad basada en la red personal: seleccione esta opción para bloquear las redes Wi-Fi personales, como WEP, WPA/WPA2/WPA3, etc. • Seguridad basada en la red EAP de empresa: seleccione esta opción para bloquear la red Wi-Fi basada en el protocolo EAP • Seguridad basara en la red Enterprise 192: seleccione esta opción para bloquear las redes Wi-Fi basadas en EAP de empresa Se desconectarán todos los dispositivos existentes que no cumplan con los requisitos mínimos. Los detalles del dispositivo mostrarán el Nivel de seguridad Wi-Fi mínimo requerido (si estuviera disponible) en **General > Nivel de seguridad Wi-Fi**.
Rechazar la opción de compartir Wi-Fi configurado por el administrador	Seleccione esta opción para impedir que los usuarios compartan las configuraciones Wi-Fi establecidas por el administrador.
Android 15.0+	
Desactivar la asistencia de IA **Ajustes del modo kiosco:** el modo kiosco aplica restricciones adicionales a los dispositivos, como el acceso limitado a	Seleccione para evitar que los usuarios de las funciones de asistencia de IA. De forma predeterminada, esta opción está desactivada.

Ajuste	Descripción
aplicaciones a través de un selector personalizado.	
Activar el modo kiosco	Seleccione esta opción para configurar el **Modo kiosco** en dispositivos Android. • Cuando un usuario inicia sesión en el modo Kiosco Compartido y cierra la sesión, el nombre de usuario permanece disponible con el cliente Go para futuros inicios de sesión. En el modo Kiosco Compartido, el cliente Go conserva siete nombres de usuario utilizados recientemente. • El modo de Kiosco Compartido ahora es compatible con la autenticación IDP. Por lo tanto, si Ivanti Neurons for MDM está configurada con IDP, el modo de Kiosco Compartido se puede usar con la autenticación IDP.
Activar el modo de Bloqueo de tarea	Seleccione esta opción para activar el modo de bloqueo de tareas en los dispositivos Android. Si está habilitado, los dispositivos pueden mostrar el protector de teclado, la barra de estado y el modo de seguridad. Esta opción está desactivada de forma predeterminada. Los siguientes son los ajustes adicionales que se muestran cuando se activa el modo de bloqueo de tareas para Android 9 o versiones más recientes compatibles: **Icono de Ajustes**: permite que las aplicaciones tengan acceso a las funciones del sistema que dependen de la aplicación Ajustes del dispositivo. Permitir los Ajustes del dispositivo ayuda a evitar las violaciones del modo de bloqueo de tareas en escenarios como el emparejamiento de Bluetooth desde una aplicación. Se recomienda mantener este ajuste habilitado para aplicaciones específicas. **Información del sistema**: muestra la fecha/hora, la conectividad, la batería y el modo de vibración en la barra de estado. Esta opción está desactivada de forma predeterminada. **Teclado**(Activado por omisión): activa el teclado durante el modo de bloqueo de tareas. **Acciones globales**(Activadas por omisión): activa el menú que se muestra cuando el usuario deja presionado el botón de encendido. Si esta opción está desactivada, es posible que el usuario no pueda apagar el dispositivo. **Botón de inicio**: activa el botón de inicio. Esta opción está desactivada de forma predeterminada. Cuando se activa, se muestran las siguientes subopciones: • **Botón de resumen**(Desactivado por omisión): activa el botón de resumen y la pantalla de resumen durante el modo de bloqueo de tareas • **Notificaciones**(Desactivado por omisión): activa las notificaciones durante el modo de bloqueo de tareas. Esto incluye los iconos de notificación en la barra de estado, las notificaciones de preaviso y el tono de notificación ampliable. si la opción del Botón de inicio no está activada, el usuario no podrá utilizar la función de ventana múltiple.
Entrar en el modo kiosko automáticamente (solo en la configuración inicial)	Seleccione esta opción para permitir automáticamente el modo kiosco cuando se aplique la configuración.

Ajuste	Descripción
Mantener modo de kiosco después de actualizaciones de política	Seleccione para devolver el dispositivo al modo de quiosco de forma automática después de aplicar una actualización de la política de bloqueo. Este ajuste ayuda a mantener el funcionamiento ininterrumpido del quiosco y reduce la necesidad de intervención manual después de los cambios de política. Anteriormente, actualizar una política de bloqueo podría hacer que el dispositivo salga del modo de kiosco. Cuando se habilita, el dispositivo vuelve a entrar de forma automática en el modo de quiosco después de procesar la política actualizada.
Desactivar los ajustes rápidos para dispositivos Android 5	Seleccione esta opción para desactivar los Ajustes rápidos en el modo kiosco que se ejecutan en Android 5.
Desactivar los ajustes rápidos para Android 6+ y todos los dispositivos Samsung	Seleccione esta opción para desactivar los ajustes rápidos en el modo kiosco para los dispositivos con Android Enterprise desde la versión 6 hasta la versión lanzada más recientemente y para todos los dispositivos Samsung. al desactivar este ajuste no se bloquean los iconos de notificación ni los sonidos del dispositivo.
Permitir al usuario acceder a los ajustes Wi-Fi	Seleccione esta opción para permitir que un usuario cambie los ajustes de Wi-Fi y acceda a las redes inalámbricas preferidas.
Permitir al usuario acceder a los ajustes Bluetooth	Seleccione esta opción para permitir que un usuario cambie los ajustes del Bluetooth y sincronice dispositivos Bluetooth adicionales.
Permitir al usuario acceder a los ajustes de localización	Seleccione esta opción para permitir a un usuario que acceda a los ajustes de localización.
Permitir al usuario retrasar las actualizaciones de la aplicación	Seleccione esta opción para permitir que un usuario retrase las actualizaciones de la aplicación.
Permitir al usuario acceder a los ajustes de fecha y hora	Seleccione esta opción para permitir a un usuario que acceda a los ajustes de fecha y hora.
Permitir al usuario acceder a los ajustes de red móvil	Seleccione esta opción para permitir a un usuario que acceda a los ajustes de red móvil.
Permitir al usuario seleccionar el idioma	Seleccione esta opción para permitir que el usuario acceda a los ajustes de idioma.
Activar dispositivo compartido	En el kiosco de un dispositivo compartido, el dispositivo se comparte entre varios usuarios finales. Esta opción permite compartir un dispositivo mientras este está en modo kiosco: • **Activar inicio de sesión**: esta opción es para el usuario administrador de un kiosco. Cuando se configura un dispositivo con esta opción, se mostrará la pantalla de inicio de sesión del usuario, lo cual permite al usuario final iniciar sesión en el kiosco del dispositivo compartido. la opción Activar inicio de sesión estará visible solo si el usuario se crea como usuario de la cuenta de un dispositivo con Android Enterprise (usuario provisional). Seleccione Usar sustitución de dominio e introduzca el dominio de forma

Ajuste	Descripción
	adecuada. Esta opción comprueba el nombre de usuario para el sufijo del dominio. Si falta el sufijo del dominio, el sistema añadirá automáticamente el sufijo del dominio al nombre de usuario. • **Activar cierre de sesión**: cuando se configura un dispositivo con esta opción, el usuario final que ha iniciado sesión tendrá acceso a la lista de aplicaciones en la lista de permitidos. Este usuario puede ver la opción de cerrar sesión pero no podrá salir del kiosco. Cuando un usuario cierra sesión en el kiosco del dispositivo compartido, otro usuario puede iniciar sesión en el kiosco del dispositivo compartido y ver las aplicaciones según las ha configurado el administrador. • Las aplicaciones aparecen con un icono Reciclar, que se usa para forzar la reinstalación de una aplicación con cada inicio de sesión. Esta opción se puede usar para las aplicaciones que son datos locales del caché. el usuario puede salir del modo kiosco si el administrador le proporciona el PIN de salida del kiosco. • **Tiempo de espera**: especifique la duración del tiempo de espera en horas. Por ejemplo, cuando la duración del tiempo de espera se configura en 2 horas y el usuario final no cierra sesión en el kiosco del dispositivo compartido, la acción de cierre de sesión se realizará automáticamente en el dispositivo una vez trascurridas las 2 horas. el campo **Tiempo de espera** solo aparece cuando está seleccionada la opción **Activar cierre de sesión** y es opcional. También se puede cerrar la sesión de los usuarios finales desde el modo kiosco compartido haciendo clic en la opción **Cerrar sesión en el kiosco de la versión corporativa de Android** en la página de detalles del dispositivo.
Permitir la autenticación con FIDO (requiere que la aplicación de Google Chrome esté en el dispositivo)	Seleccione esta opción para usar la autenticación con FIDO para usuarios cuando utilice el kiosco compartido. Permitir que los usuarios usen las claves de FIDO para iniciar sesión en el dispositivo. Google Chrome es el único navegador compatible y debe estar disponible en el dispositivo para que la autenticación con FIDO esté disponible en el kiosco compartido.
Permitir al usuario configurar el brillo y autogiro	Seleccione esta opción para permitir al usuario configurar el brillo y autogiro.
Habilitar ventana múltiple	Seleccione esta opción para permitir la visualización de más de una aplicación al mismo tiempo con los dispositivos Samsung (kiosco del propietario del dispositivo). Para permitir la ventana múltiple en el modo bloqueo de tareas, también deben estar activadas las siguientes opciones del modo bloqueo de tareas: • **Botón de inicio** • **Botón de resumen**

Ajuste	Descripción
Activar la protección contra inactividad	Seleccione esta opción para activar la protección contra la inactividad en el modo Kiosko. Si se selecciona, el valor por defecto es de 30 segundos hasta los cuales la pantalla Kiosko permanecerá activa. Puede establecer cualquier valor entre 30 y 3600.
Imagen de marca del kiosko	Seleccione las opciones de imagen de marca personalizada o predeterminada de la lista desplegable.
PIN para salir del modo kiosco	Ingrese el PIN de 6 dígitos que el usuario debe introducir para salir del modo Kiosco. El PIN debe tener un mínimo de 6 dígitos y un máximo de 10 dígitos. Este PIN es aplicable a todos los dispositivos que estén en modo kiosco. Anteriormente, la longitud del PIN del kiosco era de 4 dígitos. El usuario puede continuar usando el PIN de 4 dígitos incluso después de actualizar desde una versión anterior a Ivanti Neurons for MDM 82. Sin embargo, si hay algún cambio en la configuración, la longitud del PIN debe establecerse según el nuevo requisito (es decir, un mínimo de 6 dígitos y un máximo de 10 dígitos). La aplicación Go protegerá el dispositivo contra ataques de fuerza bruta. Para obtener más información, consulte la documentación de Go for Android.
Activar el iniciador de aplicación única Kiosk Permitir el acceso del usuario a la configuración del agente de Ivanti	Seleccione utilizar el modo Kiosko para mantener una aplicación en primer plano en dispositivos GMS y no GMS. Debe seleccionar una aplicación del catálogo de aplicaciones o introducir un ID de paquete. Seleccione esta opción para acceder a los **Ajustes del agente de Ivanti** sin salir del **modo de quiosco de aplicación única**. Anteriormente, el administrador debía salir del modo de quiosco para acceder a los ajustes del agente. Una vez habilitada y distribuida la configuración a los dispositivos, los usuarios pueden abrir la página de ajustes del agente de Ivanti manteniendo pulsados a la vez los botones Subir volumen y Bajar volumen. Esta función solo está disponible en dispositivos Android inscritos en el modo Dispositivo administrado por el trabajo.
Activar la seguridad del controlador **Crear una lista de permitidos de aplicaciones:** estas aplicaciones estarán disponibles para los usuarios en el modo kiosko al añadir aplicaciones a la lista de aplicaciones permitidas. Arrastre y suelte para organizar las aplicaciones en el orden en que deben aparecer en el selector del modo kiosko. Al añadir una aplicación a la lista de	Seleccione para activar el icono de seguridad del controlador para todas las aplicaciones en la sección de aplicaciones permitidas en modo Kiosko. Haga clic en el icono de seguridad del controlador para deshabilitar la aplicación si la velocidad supera el límite.

Ajuste	Descripción
aplicaciones permitidas no se instalará la aplicación en el dispositivo. Asegúrese de distribuir cada aplicación a los usuarios y grupos de usuarios adecuados en el App Catalog.	
Aplicaciones integradas	Haga clic en +Añadir para incluir las aplicaciones nativas mencionadas en el grupo de aplicaciones permitido en el modo kiosco. En la configuración de las aplicaciones permitidas en el modo kiosco, están disponibles las siguientes opciones: • **Borrar los datos del usuario de la aplicación**: cuando se activa esta opción, se permite que todos los datos de la aplicación se borren automáticamente sin ningún tipo de aviso cuando el usuario cierra la sesión del kiosco. Seleccione Activar dispositivo compartido en la configuración del modo kiosco para que esta opción esté disponible con las aplicaciones. ◦ Los datos de la aplicación no se borran para Google Chrome y el paquete webview aunque se añadan en la lista de permitidos de aplicaciones con la opción «Borrar datos del usuario» activada. Esto se debe a que el kiosko podría bloquearse si se borran los datos de la aplicación para estos 2 paquetes. ◦ Los datos de la aplicación no se borran para las aplicaciones del sistema para las que no está disponible el iniciador de aplicaciones (tanto dentro como fuera del kiosco). • **Ocultar**: activar esta opción permite que a la aplicación puedan acceder otras aplicaciones pero no está disponible en el lanzador del kiosco. si ha desactivado «Marcador» o «Cámara» en los ajustes de bloqueo anteriores, no podrán añadirse a la lista de aplicaciones permitidas.
Catálogo de aplicaciones Otras aplicaciones	Haga clic en +Añadir para incluir las aplicaciones mencionadas del catálogo de aplicaciones en el grupo de aplicaciones permitido en el modo kiosco. Haga clic en +Añadir para añadir el **nombre del paquete** de una aplicación que no esté disponible en la Google Play Store. Para los dispositivos Samsung, los administradores deben poner en la lista de permitidos los siguientes paquetes de marcador/sistema para que funcionen en modo Kiosco con el fin de permitir la funcionalidad del marcador en modo Kiosco. • Llamar – com.samsung.android.incallui • Teléfono - com.samsung.android.dialer (debe estar en la lista de permitidos y el administrador debe seleccionar la opción de ocultar este paquete para evitar problemas con las dos opciones del marcador para el usuario) • Llamar - com.sec.phone • Configuración de la llamada - com.samsung.android.app.telephonyui • Marcación asistida - com.sec.providers.assisted dialing

Ajuste	Descripción
	• Copia de seguridad/Restaurar el registro de llamadas - com.android.calllogbackup • Almacenamiento del marcador - com.android.providers.telephony • Teléfono - com.android.server.telecom • Teléfono - com.androide.teléfono • Llamada inteligente - com.samsung.android.smartcallprovider • Llamadas WiFi - com.sec.unifiedwfc
Aplicaciones permitidas en el modo kiosco **Crear una lista de permitidos de aplicaciones:** estas aplicaciones estarán disponibles para los usuarios en el modo kiosko al añadir aplicaciones a la lista de aplicaciones permitidas. Arrastre y suelte para organizar las aplicaciones en el orden en que deben aparecer en el selector del modo kiosko. Al añadir una aplicación a la lista de aplicaciones permitidas no se instalará la aplicación en el dispositivo. Asegúrese de distribuir cada aplicación a los usuarios y grupos de usuarios adecuados en el App Catalog.	Haga clic en X para desinstalar una aplicación del grupo de aplicaciones permitido en el modo kiosco. Arrastre y suelte para cambiar el orden en que aparecen las aplicaciones de los dispositivos en modo kiosco. **Añadir carpeta**: puede utilizar esta opción para crear una carpeta en esta sección y mover una o más aplicaciones a esta carpeta. Puede crear carpetas de hasta dos niveles. Las aplicaciones copiadas en una carpeta no pueden copiarse en otra. Solo se admiten 25 aplicaciones dentro de una carpeta.
Aplicaciones integradas	Haga clic en +Añadir para incluir las aplicaciones nativas mencionadas en el grupo de aplicaciones permitido en el modo kiosco. En la configuración de las aplicaciones permitidas en el modo kiosco, están disponibles las siguientes opciones: • **Borrar los datos del usuario de la aplicación**: cuando se activa esta opción, se permite que todos los datos de la aplicación se borren automáticamente sin ningún tipo de aviso cuando el usuario cierra la sesión del kiosco. Seleccione Activar dispositivo compartido en la configuración del modo kiosco para que esta opción esté disponible con las aplicaciones. ◦ Los datos de la aplicación no se borran para Google Chrome y el paquete webview aunque se añadan en la lista de permitidos de aplicaciones con la opción «Borrar datos del usuario» activada. Esto se debe a que el

Ajuste	Descripción
	kiosko podría bloquearse si se borran los datos de la aplicación para estos 2 paquetes. ◦ Los datos de la aplicación no se borran para las aplicaciones del sistema para las que no está disponible el iniciador de aplicaciones (tanto dentro como fuera del kiosco). • **Ocultar**: activar esta opción permite que a la aplicación puedan acceder otras aplicaciones pero no está disponible en el lanzador del kiosco. si ha desactivado «Marcador» o «Cámara» en los ajustes de bloqueo anteriores, no podrán añadirse a la lista de aplicaciones permitidas.
Catálogo de aplicaciones Otras aplicaciones	Haga clic en +Añadir para incluir las aplicaciones mencionadas del catálogo de aplicaciones en el grupo de aplicaciones permitido en el modo kiosco. Haga clic en +Añadir para añadir el **nombre del paquete** de una aplicación que no esté disponible en la Google Play Store. Para los dispositivos Samsung, los administradores deben poner en la lista de permitidos los siguientes paquetes de marcador/sistema para que funcionen en modo Kiosco con el fin de permitir la funcionalidad del marcador en modo Kiosco. • Llamar – com.samsung.android.incallui • Teléfono - com.samsung.android.dialer (debe estar en la lista de permitidos y el administrador debe seleccionar la opción de ocultar este paquete para evitar problemas con las dos opciones del marcador para el usuario) • Llamar - com.sec.phone • Configuración de la llamada - com.samsung.android.app.telephonyui • Marcación asistida - com.sec.providers.assisted dialing • Copia de seguridad/Restaurar el registro de llamadas - com.android.calllogbackup • Almacenamiento del marcador - com.android.providers.telephony • Teléfono - com.android.server.telecom • Teléfono - com.androide.teléfono • Llamada inteligente - com.samsung.android.smartcallprovider • Llamadas WiFi - com.sec.unifiedwfc
Aplicaciones permitidas en el modo kiosco	Haga clic en X para desinstalar una aplicación del grupo de aplicaciones permitido en el modo kiosco. Arrastre y suelte para cambiar el orden en que aparecen las aplicaciones de los dispositivos en modo kiosco. **Añadir carpeta**: puede utilizar esta opción para crear una carpeta en esta sección y mover una o más aplicaciones a esta carpeta. Puede crear carpetas de hasta dos niveles. Las aplicaciones copiadas en una carpeta no pueden copiarse en otra. Solo se admiten 25 aplicaciones dentro de una carpeta.
Activar el iniciador de aplicación única Kiosk	Seleccione utilizar el modo Kiosko para mantener una aplicación en primer plano en dispositivos GMS y no GMS. Debe seleccionar una aplicación del catálogo de

Ajuste	Descripción
	aplicaciones o introducir un ID de paquete.
Crear una lista de permitidos de aplicaciones: estas aplicaciones estarán disponibles para los usuarios en el modo kiosko al añadir aplicaciones a la lista de aplicaciones permitidas. Arrastre y suelte para organizar las aplicaciones en el orden en que deben aparecer en el selector del modo kiosko. Al añadir una aplicación a la lista de aplicaciones permitidas no se instalará la aplicación en el dispositivo. Asegúrese de distribuir cada aplicación a los usuarios y grupos de usuarios adecuados en el App Catalog.	
Aplicaciones integradas	Haga clic en +Añadir para incluir las aplicaciones nativas mencionadas en el grupo de aplicaciones permitido en el modo kiosco. En la configuración de las aplicaciones permitidas en el modo kiosco, están disponibles las siguientes opciones: • **Borrar los datos del usuario de la aplicación**: cuando se activa esta opción, se permite que todos los datos de la aplicación se borren automáticamente sin ningún tipo de aviso cuando el usuario cierra la sesión del kiosco. Seleccione Activar dispositivo compartido en la configuración del modo kiosco para que esta opción esté disponible con las aplicaciones. ◦ Los datos de la aplicación no se borran para Google Chrome y el paquete webview aunque se añadan en la lista de permitidos de aplicaciones con la opción «Borrar datos del usuario» activada. Esto se debe a que el kiosko podría bloquearse si se borran los datos de la aplicación para estos 2 paquetes. ◦ Los datos de la aplicación no se borran para las aplicaciones del sistema para las que no está disponible el iniciador de aplicaciones (tanto dentro como fuera del kiosco). • **Ocultar**: activar esta opción permite que a la aplicación puedan acceder otras aplicaciones pero no está disponible en el lanzador del kiosco. si ha desactivado «Marcador» o «Cámara» en los ajustes de bloqueo anteriores, no podrán añadirse a la lista de aplicaciones permitidas.
Catálogo de aplicaciones	Haga clic en +Añadir para incluir las aplicaciones mencionadas del catálogo de aplicaciones en el grupo de aplicaciones permitido en el modo kiosco.
Otras aplicaciones	Haga clic en +Añadir para añadir el **nombre del paquete** de una aplicación que no esté disponible en la Google Play Store. Para los dispositivos Samsung, los administradores deben poner en la lista de

Ajuste	Descripción
	permitidos los siguientes paquetes de marcador/sistema para que funcionen en modo Kiosco con el fin de permitir la funcionalidad del marcador en modo Kiosco. • Llamar – com.samsung.android.incallui • Teléfono - com.samsung.android.dialer (debe estar en la lista de permitidos y el administrador debe seleccionar la opción de ocultar este paquete para evitar problemas con las dos opciones del marcador para el usuario) • Llamar - com.sec.phone • Configuración de la llamada - com.samsung.android.app.telephonyui • Marcación asistida - com.sec.providers.assisted dialing • Copia de seguridad/Restaurar el registro de llamadas - com.android.calllogbackup • Almacenamiento del marcador - com.android.providers.telephony • Teléfono - com.android.server.telecom • Teléfono - com.androide.teléfono • Llamada inteligente - com.samsung.android.smartcallprovider • Llamadas WiFi - com.sec.unifiedwfc
Aplicaciones permitidas en el modo kiosco Activar el iniciador de aplicación única Kiosk	Haga clic en X para desinstalar una aplicación del grupo de aplicaciones permitido en el modo kiosco. Arrastre y suelte para cambiar el orden en que aparecen las aplicaciones de los dispositivos en modo kiosco. **Añadir carpeta**: puede utilizar esta opción para crear una carpeta en esta sección y mover una o más aplicaciones a esta carpeta. Puede crear carpetas de hasta dos niveles. Las aplicaciones copiadas en una carpeta no pueden copiarse en otra. Solo se admiten 25 aplicaciones dentro de una carpeta. Seleccione utilizar el modo Kiosko para mantener una aplicación en primer plano en dispositivos GMS y no GMS. Debe seleccionar una aplicación del catálogo de aplicaciones o introducir un ID de paquete.
Crear una lista de permitidos de aplicaciones: estas aplicaciones estarán disponibles para los usuarios en el modo kiosko al añadir aplicaciones a la lista de aplicaciones permitidas. Arrastre y suelte para organizar las aplicaciones en el orden en que deben aparecer en el selector del modo kiosko. Al añadir una aplicación a la lista de aplicaciones permitidas no se instalará la aplicación en el dispositivo. Asegúrese de distribuir cada aplicación a los usuarios y grupos de usuarios adecuados en el App Catalog.	

Ajuste	Descripción
Aplicaciones integradas	Haga clic en +Añadir para incluir las aplicaciones nativas mencionadas en el grupo de aplicaciones permitido en el modo kiosco. En la configuración de las aplicaciones permitidas en el modo kiosco, están disponibles las siguientes opciones: • **Borrar los datos del usuario de la aplicación**: cuando se activa esta opción, se permite que todos los datos de la aplicación se borren automáticamente sin ningún tipo de aviso cuando el usuario cierra la sesión del kiosco. Seleccione Activar dispositivo compartido en la configuración del modo kiosco para que esta opción esté disponible con las aplicaciones. ◦ Los datos de la aplicación no se borran para Google Chrome y el paquete webview aunque se añadan en la lista de permitidos de aplicaciones con la opción «Borrar datos del usuario» activada. Esto se debe a que el kiosko podría bloquearse si se borran los datos de la aplicación para estos 2 paquetes. ◦ Los datos de la aplicación no se borran para las aplicaciones del sistema para las que no está disponible el iniciador de aplicaciones (tanto dentro como fuera del kiosco). • **Ocultar**: activar esta opción permite que a la aplicación puedan acceder otras aplicaciones pero no está disponible en el lanzador del kiosco. si ha desactivado «Marcador» o «Cámara» en los ajustes de bloqueo anteriores, no podrán añadirse a la lista de aplicaciones permitidas.
Catálogo de aplicaciones	Haga clic en +Añadir para incluir las aplicaciones mencionadas del catálogo de aplicaciones en el grupo de aplicaciones permitido en el modo kiosco.
Otras aplicaciones	Haga clic en +Añadir para añadir el nombre del paquete de una aplicación que no esté disponible en la Google Play Store. Para los dispositivos Samsung, los administradores deben poner en la lista de permitidos los siguientes paquetes de marcador/sistema para que funcionen en modo Kiosco con el fin de permitir la funcionalidad del marcador en modo Kiosco. • Llamar – com.samsung.android.incallui • Teléfono - com.samsung.android.dialer (debe estar en la lista de permitidos y el administrador debe seleccionar la opción de ocultar este paquete para evitar problemas con las dos opciones del marcador para el usuario) • Llamar - com.sec.phone • Configuración de la llamada - com.samsung.android.app.telephonyui • Marcación asistida - com.sec.providers.assisted dialing • Copia de seguridad/Restaurar el registro de llamadas - com.android.calllogbackup • Almacenamiento del marcador - com.android.providers.telephony • Teléfono - com.android.server.telecom • Teléfono - com.androide.teléfono

Ajuste	Descripción
	• Llamada inteligente - com.samsung.android.smartcallprovider • Llamadas WiFi - com.sec.unifiedwfc
Aplicaciones permitidas en el modo kiosco	Haga clic en X para desinstalar una aplicación del grupo de aplicaciones permitido en el modo kiosco. Arrastre y suelte para cambiar el orden en que aparecen las aplicaciones de los dispositivos en modo kiosco. **Añadir carpeta**: puede utilizar esta opción para crear una carpeta en esta sección y mover una o más aplicaciones a esta carpeta. Puede crear carpetas de hasta dos niveles. Las aplicaciones copiadas en una carpeta no pueden copiarse en otra. Solo se admiten 25 aplicaciones dentro de una carpeta.

para los dispositivos Samsung con Knox Standard 4.0 o posterior, la característica multiusuario se bloquea automáticamente en el modo kiosco.

Dispositivos administrados con perfil profesional

Desactive ciertas funciones en el dispositivo administrado con perfil profesional para Android 8.0+.

Ciertas funciones se pueden desactivar para el perfil de trabajo en los dispositivos propiedad de la empresa (aplicable a dispositivos Android 11+).

Ajuste	Descripción
Ajustes de bloqueo de dispositivos administrados	
Desactivar Wi-Fi	Seleccionar para desactivar el acceso a LAN inalámbricas.(No aplicable a dispositivos de Android 11+)
Desactivar ajustes de Wi-Fi	Seleccione esta opción para desactivar el acceso a los ajustes inalámbricos.
Desactivar cámara	Seleccione esta opción para desactivar el acceso a la cámara.
Desactivar Bluetooth	Seleccione esta opción para desactivar las características del Bluetooth. tenga cuidado al utilizar esta opción. Ivanti no recomienda desactivar el audio porque el acceso al Bluetooth manos libres está desactivado. Cada vez son más comunes los requisitos legales para el uso de dispositivos manos libres mientras se conduce.
No permitir ajustes de Bluetooth	Seleccione esta opción para desactivar el acceso a los ajustes Bluetooth.
Desactivar el reinicio de la red	Seleccione esta opción para evitar el restablecimiento de la red (aplicable a dispositivos con Android 7.0 y versiones posteriores).
Silenciar volumen principal	Seleccione esta opción para silenciar el volumen principal. (No se aplica a los dispositivos Android 11+)
No permitir emisiones de emergencia	Seleccione esta opción para impedir emisiones de emergencia.
No permitir redes móviles	Seleccione esta opción para desactivar el acceso a las redes móviles. Esta opción no se puede desactivar si la Wi-Fi está desactivada.
No permitir tethering	Seleccione esta opción para desactivar el tethering como alternativa para usar la conexión a Internet de un dispositivo con el fin de proporcionar acceso a Internet a otro dispositivo.
No permitir VPN	Seleccione esta opción para desactivar las conexiones VPN. (No se aplica a los dispositivos Android 11+)
Desactivar configuración predeterminada de fábrica	Seleccione esta opción para evitar que los usuarios puedan devolver el dispositivo a los valores predeterminados de fábrica. (No se aplica a los dispositivos Android 11+)
Activar protección de restablecimiento de valores de fábrica	Seleccione esta opción para permitir que los usuarios puedan devolver el dispositivo a los valores predeterminados de fábrica. Opcionalmente, puede especificar una lista de Id. de cuentas Google autorizadas (un valor entero) que pueda aprovisionar el dispositivo después del restablecimiento de fábrica o dejar el cursor sobre el icono de ayuda para ver ayuda sobre cómo recuperar Id. de cuentas autorizadas.
No permitir llamadas	Seleccione esta opción para impedir que un usuario haga llamadas salientes.

Ajuste	Descripción
salientes	
No permitir el reinicio en modo seguro (Android 6.0+)	Seleccione esta opción para evitar que los usuarios reinicien un dispositivo en modo seguro.
No permitir características de depuración	Seleccione esta opción para desactivar las características de depuración en los dispositivos. Esta opción está activada de forma predeterminada.
Asegurar Verify Apps	Seleccione para permitir las funciones de verificación de aplicaciones en los dispositivos. Esta opción está activada de forma predeterminada. cuando esta opción esté desactivada, el dispositivo volverá a su comportamiento predeterminado, el cual podrá variar según el dispositivo.
No permitir SMS	Seleccione esta opción para impedir que un usuario envíe y reciba mensajes SMS.
No permitir Silenciar micrófono	Seleccione esta opción para impedir que un usuario silencie el micrófono del dispositivo.
No permitir hora automática	Seleccione esta opción para impedir que un usuario active los cambios automáticos de hora.
No permitir zona de hora automática	Seleccione esta opción para impedir que un usuario active el ajuste automático de la hora del dispositivo con los cambios de zona horaria.
Desactivar itinerancia de datos	Seleccione esta opción para desactivar el intercambio de datos mientras el dispositivo está en itinerancia.
Sincronizar hora con el servidor (Android 9.0+)	Seleccione esta opción para permitir que los dispositivos sincronicen la hora con los servidores de Ivanti Neurons for MDM la primera vez al registrarse y, a partir de entonces, una vez cada 24 horas después de cada registro. Esta opción solo estará disponible si se selecciona la opción **Desactivar el tiempo automático**.
Configurar zona horaria (Android 9.0+)	Especifique la cadena de Zona horaria en formato de ID de zona horaria de Olson (por ejemplo, Pacific/Midway).
No permitir suspensión de Wi-Fi	Seleccione esta opción para mantener la Wi-Fi activada mientras dispositivo esté en modo suspensión. (No se aplica a los dispositivos Android 11+)
Restringir métodos de entrada	Seleccione para restringir los métodos de entrada para las aplicaciones de trabajo, designando una lista de nombres de paquetes en la lista de permitidos a través del campo **Nombre del paquete** (no se aplica a los dispositivos Android 11+) Los dispositivos tendrán disponibles tanto los métodos de entrada de paquetes de la lista de permitidos como los métodos de entrada del sistema predeterminado. El usuario puede cambiar entre los métodos de entrada del sistema predeterminado y los métodos de entrada de los paquetes de la lista de permitidos. En Android 10+, los métodos de entrada son aplicables solo para el lado del dispositivo, de lo contrario están restringidos en todo el dispositivo.

Ajuste	Descripción
Restringir servicios de accesibilidad	Seleccione esta opción para restringir los servicios de accesibilidad para aplicaciones profesionales designando una lista de nombres de paquetes en la lista de permitidos a través del campo **Nombre del paquete**. Si no hay ningún paquete en la lista de permitidos, solo se permitirán los servicios de accesibilidad del sistema. En Android 10+, los métodos de entrada están restringidos solo a las aplicaciones de trabajo, de lo contrario están restringidos en todo el dispositivo.
Desactivar transferencia de archivos USB	Seleccione esta opción para desactivar la transferencia de archivos USB.
Desactivar elementos multimedia externos	Seleccione esta opción para desactivar los elementos multimedia externos.
No permitir fuentes desconocidas en el dispositivo	Seleccione esta opción para evitar que el dispositivo instale aplicaciones de orígenes desconocidos. para que este ajuste entre en vigor en el dispositivo dependerá de que una actualización esperada de Google Play habilite esta función.
Configurar el mensaje de la pantalla de bloqueo (Android 7.0+)	Seleccione esta opción para configurar el mensaje de la pantalla de bloqueo que se mostrará en el dispositivo. Escribir el mensaje de la pantalla de bloqueo (máximo de 256 caracteres) en el campo de texto. Al activar esta opción, se bloquea al usuario para que no pueda configurar el mensaje en Ajustes y se muestra al usuario el mensaje configurado por el administrador. Si el administrador no proporciona ningún mensaje de pantalla de bloqueo después de activar la opción «Configurar el mensaje de la pantalla de bloqueo», el usuario tiene bloqueada la posibilidad de configurar el mensaje en Ajustes, pero no se muestra ningún mensaje al usuario.
Establecer el brillo de la pantalla	Seleccionar para establecer el brillo de la pantalla del dispositivo. • Manual: seleccione para introducir un número manualmente (0 a 255) • Adaptable: seleccione permitir que el dispositivo establezca el brillo Es recomendable activar la opción "Desactivar el brillo de la pantalla de configuración" antes de ajustar el brillo de la pantalla del dispositivo. Si el usuario puede realizar cambios, estos ajustes se restablecerán a los ajustes definidos por el administrador en el siguiente contacto. Este ajuste no es compatible con dispositivos Android 11 y versiones posteriores para el Perfil de trabajo en modo de dispositivo de la empresa.
Establecer el tiempo de espera de la pantalla	Seleccionar para establecer la duración del tiempo de espera de la pantalla (en segundos). Es recomendable activar la opción "Desactivar el tiempo de espera de la pantalla de configuración" antes de ajustar el brillo de la pantalla del dispositivo. Si el usuario puede realizar cambios, estos ajustes se restablecerán a los ajustes definidos por el administrador en el siguiente contacto. Este ajuste no es compatible con dispositivos Android 11 y versiones posteriores para el Perfil de trabajo en modo de dispositivo de la empresa.
Establecer la orientación de la pantalla	Seleccionar para establecer la orientación de la pantalla. Puede establecer la orientación de pantalla a 0, 90, 180 o 270 grados desde la lista desplegable.

Ajuste	Descripción
	Este ajuste no es compatible con dispositivos Android 11 y versiones posteriores para el Perfil de trabajo en modo de dispositivo de la empresa.
Desactivar el autorrellenado (Android 8.0+)	Seleccione esta opción para no permitir el autorrellenado. (No se aplica a los dispositivos Android 11+)
No permitir el uso compartido de Bluetooth (Android 8.0+)	Seleccione esta opción para impedir que el usuario compartir el Bluetooth de salida en el dispositivo.
No permitir servicio de copia de seguridad (Android 8.0+)	Seleccione esta opción para desactivar el servicio de copia de seguridad. (No se aplica a los dispositivos Android 11+)
No permitir impresión (Android 9.0+)	Seleccionar para restringir la impresión desde todas las aplicaciones.(No aplicable a dispositivos de Android 11+)
No permitir modo avión (Android 9.0+)	Seleccione esta opción para desactivar el modo avión en todo el dispositivo.
No permitir Ambient Display (Android 9.0+)	Seleccione esta opción para no permitir la función «Ambient display» para el usuario. (No se aplica a los dispositivos Android 11+)
No permitir brillo de la configuración (Android 9.0 +)	Seleccione esta opción para impedir al usuario que configure el brillo (no se puede aplicar a dispositivos de Android 11+). Es recomendable definir los valores de "Establecer el modo de brillo de la pantalla" antes de seleccionar esta opción.
No permitir config. de fecha y hora (Android 9.0+)	Seleccione esta opción para impedir al usuario que configure la fecha, hora y zona horaria.
No permitir config. de localización (Android 9.0 +)	Seleccione esta opción para impedir al usuario que desactive los proveedores de localización.
No permitir config. del tiempo de espera de la pantalla (Android 9.0+)	Seleccione esta opción para impedir al usuario que cambie el tiempo de espera de apagado de la pantalla. (No se aplica a los dispositivos Android 11+) Es recomendable establecer los valores de "Establecer tiempo de espera de la pantalla" antes de seleccionar esta opción.
No permitir diálogos de errores del sistema (Android 9.0+)	Seleccione para impedir los diálogos de error del sistema. (No aplicable para dispositivos de Android 11+)
Deshabilitar Captura de pantalla (Android 11.0+)	Seleccione esta opción para desactivar la posibilidad de usar la característica de captura de pantalla integrada del dispositivo. Al seleccionarla, la captura de pantalla se deshabilita en el área personal del dispositivo.

Ajuste	Descripción
Android 12.0+	
Habilitar USB solo para carga **Android 13.0+**	Seleccione para habilitar el puerto USB solo para cargar.
Establecer la seguridad de Wi-Fi mínima requerida	Utilice esta opción para establecer la seguridad WiFi mínima requerida: • No es necesaria una seguridad mínima: seleccione esta opción si no se requiere un nivel de seguridad mínimo • Seguridad basada en la red personal: seleccione esta opción para bloquear las redes Wi-Fi personales, como WEP, WPA/WPA2/WPA3, etc. • Seguridad basada en la red EAP de empresa: seleccione esta opción para bloquear la red Wi-Fi basada en el protocolo EAP • Seguridad basara en la red Enterprise 192: seleccione esta opción para bloquear las redes Wi-Fi basadas en EAP de empresa Se desconectarán todos los dispositivos existentes que no cumplan con los requisitos mínimos. Los detalles del dispositivo mostrarán el Nivel de seguridad Wi-Fi mínimo requerido (si estuviera disponible) en **General > Nivel de seguridad Wi-Fi**.
Rechazar la opción de compartir Wi-Fi configurado por el administrador	Seleccione esta opción para impedir que los usuarios compartan las configuraciones Wi-Fi establecidas por el administrador.
Ajustes de bloqueo de perfil profesional	
Desactivar captura de pantalla	Seleccione esta opción para desactivar la posibilidad de usar la característica de captura de pantalla integrada del dispositivo.
No permitir el Control de aplicaciones	Seleccione esta opción para impedir que un usuario modifique aplicaciones en Ajustes o en selectores.
No permitir Credenciales de configuración	Seleccione esta opción para impedir que un usuario configure las credenciales.
No permitir Copiar/Pegar perfil cruzado	Seleccione esta opción para impedir copiar/pegar información entre perfiles.
No permitir Modificar cuentas	Seleccione esta opción para impedir que un usuario añada o elimine cuentas.
No permitir NFC (transferencia de salida) (Android 5.1+)	Seleccione esta opción para impedir a un usuario que use NFC para transferir datos de las aplicaciones.

Ajuste	Descripción
No permitir Compartir localización	Seleccione esta opción para impedir que los sitios web y aplicaciones soliciten al usuario del dispositivo que comparta la ubicación del dispositivo.
No permitir características de depuración	Seleccione esta opción para desactivar las características de depuración en los dispositivos. Esta opción está activada de forma predeterminada.
Asegurar Verify Apps	Seleccione para permitir las funciones de verificación de aplicaciones en los dispositivos. Esta opción está activada de forma predeterminada. cuando esta opción esté desactivada, el dispositivo volverá a su comportamiento predeterminado, el cual podrá variar según el dispositivo.
Desactivar fuentes desconocidas dentro del perfil de trabajo	Seleccione esta opción para no permitir la descarga de fuentes desconocidas dentro del perfil de trabajo.
Activar/desactivar aplicaciones del sistema	Seleccione esta opción para habilitar y deshabilitar que se puedan instalar aplicaciones del sistema designando dos listas de nombres de paquetes mediante los campos **Nombre del paquete de la aplicación del sistema**. Utilice esta característica para administrar el acceso a las aplicaciones del sistema que no estén publicadas en Google Play. añadir una aplicación al catálogo de aplicaciones y también a una lista de aplicaciones del sistema no es compatible.
Desactivar Id. de llamada (Android 6.0 +)	Establece si la información del Id. de llamada del perfil de trabajo se mostrará en el dispositivo para las llamadas entrantes.
Desactivar Compartir contactos por Bluetooth (Android 6.0+)	Seleccione esta opción para evitar que el dispositivo pueda compartir contactos con otros dispositivos por Bluetooth.
Desactivar Compartir contactos mediante búsquedas (Android 7.0+)	Seleccione esta opción para evitar que los usuarios puedan buscar contactos del trabajo desde el marcador del teléfono personal.
Desactivar el autorrellenado (Android 8.0+)	Seleccione esta opción para no permitir el autorrellenado. (No se aplica a los dispositivos Android 11+)
Desactivar las notificaciones en aplicaciones del trabajo en el perfil personal (Android 8.0+)	Seleccione esta opción para restringir las notificaciones del perfil de trabajo.
No permitir impresión (Android 9.0+)	Seleccione esta opción para restringir la impresión desde todas las aplicaciones. (No se aplica a los dispositivos Android 11+)

Ajuste	Descripción
No permitir el uso compartido en el perfil (Android 9.0+)	Seleccione esta opción para evitar que los usuarios compartan datos personales en un perfil de trabajo del dispositivo.
Restringir métodos de entrada (Android 10.0 +)	Seleccione esta opción para restringir los nombres de paquetes IME puestos en la lista de permitidos designando una lista de nombres de paquetes en la lista de permitidos a través del campo **Nombre del paquete** (no se aplica a los dispositivos Android 11+). Los dispositivos tendrán disponibles tanto los métodos de entrada de paquetes de la lista de permitidos como los métodos de entrada del sistema predeterminado. El usuario puede cambiar entre los métodos de entrada del sistema predeterminado y los métodos de entrada de los paquetes de la lista de permitidos. Los métodos de entrada se aplicarán a las aplicaciones IME instaladas en el lado del perfil de trabajo. Incluso si las aplicaciones instaladas en el lado del dispositivo están en la lista de permitidos para este bloqueo, no estarán disponibles para las aplicaciones que se utilicen en el lado del perfil de trabajo.
Permitir el acceso a los calendarios del perfil de trabajo (Android 10.0+)	Seleccione cualquiera de las siguientes opciones para permitir todas las aplicaciones o seleccione un conjunto de aplicaciones en el lado personal para que accedan a la información del calendario presente en el perfil de trabajo: • **Todas las aplicaciones en el perfil personal**: permite que todas las aplicaciones accedan a la información del calendario que hay en el perfil de trabajo. • **Solo las siguientes aplicaciones del perfil personal**: en el siguiente campo de texto, introduzca los las Id. de las aplicaciones separadas por una coma. Solo estas aplicaciones seleccionadas del lado personal podrán acceder a la información del calendario presente en el perfil de trabajo. La aplicación del lado personal debería implementar las API específicas para poder acceder al calendario compartido.
Habilite la lista de permitidos de perfiles cruzados de las aplicaciones (Android 11.0+)	Seleccione esta casilla para permitir a los usuarios compartir información de aplicaciones específicas desde el perfil de trabajo hasta el lado personal del dispositivo. En el campo **Aplicaciones en la lista de permitidos**, escriba los ID de paquete de las aplicaciones que se van a incluir en la lista de permitidos, separados por comas. De forma predeterminada, esta opción está desactivada.
Habilitar el tiempo de espera máximo del perfil (Android 11.0+)	Seleccione para definir una ventana de tiempo máximo en la que se pueda desactivar el perfil de trabajo antes de que Ivanti Neurons for MDM suspenda las aplicaciones personales en el dispositivo. Puede fijar un plazo de entre 72 y 8760 horas. 8760 horas equivale a un año. El valor predeterminado se fijará en 72 horas si se selecciona esta opción. El usuario del dispositivo ve un mensaje que le indica que active el perfil de trabajo para activar las aplicaciones suspendidas. Disponible para dispositivos Android 11+ en el Perfil de trabajo en el Dispositivo propiedad de la empresa. Si el perfil se apaga para duraciones más largas, las aplicaciones personales se suspenden en el dispositivo.
Habilitar segmentación de red 5G (Android	Seleccione para proporcionar una opción de segmentación de redes 5G en el perfil de trabajo de los dispositivos de empresa.

Ajuste	Descripción
12.0+)	De forma predeterminada, esta opción está desactivada.
Desactivar la asistencia de IA (Android 15.0+)	Seleccione para evitar que los usuarios de las funciones de asistencia de IA. De forma predeterminada, esta opción está desactivada.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.4.33. Bloqueo y kiosco: Samsung KNOX Standard

La configuración Bloqueo y kiosco: Samsung KNOX Standard desactiva ciertas características de los dispositivos Samsung KNOX Standard y crea una lista de permitidos de aplicaciones que estarán disponibles para los usuarios en el modo kiosco.

> Configuración de Samsung KNOX Standard está en desuso y no es compatible con los dispositivos que usen Android 9 y versiones posteriores.

Ajustes de bloqueo

Ajuste

Qué hacer

Nombre

Introduzca un nombre que identifique a esta configuración.

Descripción

Introduzca una descripción que explique la finalidad de esta configuración.

Asustes de bloqueo de Samsung KNOX: desactiva ciertas características solamente en dispositivos Samsung KNOX.

Desactivar Wi-Fi

Seleccione esta opción para desactivar el acceso a las LAN inalámbricas.

Desactivar cámara

Seleccione esta opción para desactivar el acceso a la cámara.

Desactivar Bluetooth

Seleccione esta opción para desactivar las características del Bluetooth.

Permitir solamente el audio de Bluetooth

Seleccione esta opción para activar solamente las características de audio de Bluetooth.

Desactivar datos móviles

Seleccione esta opción para desactivar el intercambio de datos cuando un dispositivo está en contacto con otro.

Esta opción no se puede desactivar si la Wi-Fi está desactivada.

Desactivar GPS

Seleccione esta opción para desactivar el GPS.

Desactivar marcador del teléfono

Seleccione esta opción para desactivar la aplicación del teléfono.

Desactivar tarjeta SD

Seleccione esta opción para desactivar el acceso a la tarjeta SD.

Desactivar copia de seguridad de Google

Seleccione esta opción para desactivar las copias de seguridad de los servidores Google.

Desactivar copiar/pegar

Seleccione esta opción para desactivar el acceso a las funciones copiar/pegar.

Desactivar NFC

Seleccione esta opción para desactivar el intercambio de datos NFC (Near-field Communication, «transmisión de datos en proximidad») cuando los dispositivos estén en contacto.

Desactivar micrófono

Seleccione esta opción para desactivar el acceso al dispositivo del micrófono.

Desactivar captura de pantalla

Seleccione esta opción para desactivar la posibilidad de usar la característica de captura de pantalla integrada del dispositivo. Activar esta opción no permite hacer capturas de pantalla de Go. Estas capturas de pantalla no están permitidas.

Desactivar tethering de Bluetooth

Seleccione esta opción para desactivar el tethering de Bluetooth como alternativa para usar la conexión a Internet de un dispositivo con el fin de proporcionar acceso a Internet a otro dispositivo.

Desactivar depuración de USB

Seleccione esta opción para desactivar la característica de depuración de USB.

Desactivar tethering de USB

Seleccione esta opción para desactivar el tethering de USB como alternativa para usar la conexión a Internet de un dispositivo con el fin de proporcionar acceso a Internet a otro dispositivo.

Desactivar tethering de Wi-Fi

Seleccione esta opción para desactivar el tethering de Wi-Fi como alternativa para usar la conexión a Internet de un dispositivo con el fin de proporcionar acceso a Internet a otro dispositivo.

Desactivar explorador nativo

Seleccione esta opción para evitar que los usuarios puedan acceder al explorador Android.

Desactivar YouTube

Seleccione esta opción para evitar que los usuarios puedan acceder a YouTube.

Desactivar configuración predeterminada de fábrica

Seleccione esta opción para evitar que los usuarios puedan devolver el dispositivo a los valores predeterminados de fábrica.

Desactivar actualización de OTA

Seleccione esta opción para desactivar las actualizaciones OTA (por el aire) del firmware del dispositivo.

Advertencia: no desactive **Desactivar cambios en los ajustes** si está activado **Actualización de OTA**. Al **desactivar cambios en los ajustes** cuando está activada la **Actualización OTA** puede provocar que el dispositivo deje de funcionar porque sea necesario establecer cambios para la actualización.

Desactivar itinerancia de voz

Seleccione esta opción para desactivar el acceso a las llamadas de voz mientras el dispositivo está en itinerancia.

Desactivar reproductor multimedia USB

Seleccione esta opción para desactivar el reproductor multimedia de USB.

Desactivar Google Play

Seleccione esta opción para desactivar el acceso a Google Play.

Desactivar itinerancia de datos

Seleccione esta opción para desactivar el intercambio de datos mientras el dispositivo está en itinerancia.

Desactivar fuentes desconocidas

Seleccione esta opción para desactivar la instalación de aplicaciones desde otros sitios que no sean Google Play Store, con la excepción de la aplicación Go.

Desactivar eliminación de privilegios de administrador de dispositivos

Seleccione esta opción para prohibir a los usuarios que desactiven los privilegios de administrador de dispositivos de Go.

Desactivar cambios en los ajustes

Seleccione esta opción para desactivar el acceso a la aplicación Ajustes del dispositivo.

Advertencia: no desactive **Desactivar cambios en los ajustes** si está activado **Actualización de OTA**. Al **desactivar cambios en los ajustes** cuando está activada la **Actualización OTA** puede provocar que el dispositivo deje de funcionar porque sea necesario establecer cambios para la actualización.

Ajustes del modo kiosco: el modo kiosco aplica restricciones adicionales a los dispositivos, como el acceso limitado a aplicaciones a través de un selector personalizado.

Aplicable a Android hasta la versión 8.1. Para las versiones 9.0 de Android, utilice la configuración de modo kiosko para dispositivos administrados de Android Enterprise.

Activar el modo kiosco

Seleccione esta opción para configurar el **Modo kiosco** en dispositivos Android.

Permitir al usuario acceder a los ajustes Wi-Fi

Seleccione esta opción para permitir que un usuario cambie los ajustes de Wi-Fi y acceda a las redes inalámbricas preferidas.

Permitir al usuario acceder a los ajustes Bluetooth

Seleccione esta opción para permitir que un usuario cambie los ajustes del Bluetooth y sincronice dispositivos Bluetooth adicionales.

Permitir al usuario retrasar las actualizaciones de la aplicación

Seleccione esta opción para permitir que un usuario retrase las actualizaciones de la aplicación.

Ajustes de localización del GPS

Seleccione uno de los siguientes ajustes de localización GPS:

- Desactivar localización
- Activar localización
- Permitar al usuario seleccionarlo

PIN para salir del modo kiosco

Introduzca el código de cuatro dígitos que el usuario final debe escribir para poder salir del modo kiosco.

Crear una lista de permitidos de aplicaciones: estas aplicaciones estarán disponibles para los usuarios en el modo kiosko al añadir aplicaciones a la lista de aplicaciones permitidas. Arrastre y suelte para organizar las aplicaciones en el orden en que deben aparecer en el selector del modo Kiosko.

Al añadir una aplicación a la lista de aplicaciones permitidas no se instalará la aplicación en el dispositivo. Asegúrese de distribuir cada aplicación a los usuarios y grupos de usuarios adecuados en el App Catalog.

Aplicaciones integradas

Haga clic en +Añadir para incluir las aplicaciones nativas mencionadas en el grupo de aplicaciones permitido en el modo kiosco.

si ha desactivado «Marcador» o «Cámara» en los ajustes de bloqueo anteriores, no podrán añadirse a la lista de aplicaciones permitidas.

Catálogo de aplicaciones

Haga clic en +Añadir para incluir las aplicaciones mencionadas del catálogo de aplicaciones en el grupo de aplicaciones permitido en el modo kiosco.

Otras aplicaciones

Haga clic en +Añadir para añadir el **nombre del paquete** de una aplicación que no esté disponible en la Google Play Store.

Aplicaciones permitidas en el modo kiosco

Haga clic en X para desinstalar una aplicación del grupo de aplicaciones permitido en el modo kiosco. Arrastre y suelte para cambiar el orden en que aparecen las aplicaciones de los dispositivos en modo kiosco.

> Al utilizar el modo kiosco en Android 4.4 o versiones más recientes compatibles, los dispositivos Samsung que admitan múltiples usuarios bloquearán automáticamente la función multiusuario mientras se esté en el modo kiosco.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.4.34. Configuración de la solución de contraseñas de administrador local

La configuración de la **Solución de Contraseña de Administrador Local (LAPS)** permite a los administradores de Ivanti Neurons for MDM regenerar automáticamente la contraseña del administrador local en dispositivos macOS gestionados en intervalos establecidos. Para obtener más información sobre LAPS, consulte **Solución de contraseña del administrador local (LAPS, por sus siglas en inglés)**.

Aplicable a: dispositivos macOS regustradis y administrados mediante el Registro automatizado de dispositivos.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Busque y seleccione la configuración de **Solución de contraseña de administrador local (LAPS)**.
3. Configure los ajustes de **LAPS** según la tabla siguiente:

Ajuste	Descripción
Nombre,	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Plataforma	Seleccione macOS de la lista desplegable.
Intervalo de rotación	Seleccione una de las siguientes opciones del menú desplegable para definir la rotación automática de contraseñas: • Sin rotación (**predeterminado**) • 15 días • 30 días • 60 días • 90 días • 120 días • 180 días
Rotación tras el intervalo de visualización	Seleccione una de las siguientes opciones del menú desplegable para rotar automáticamente las contraseñas después de verlas desde la página **Detalles del dispositivo**: • 1 a 24 horas • 36 horas • 48 horas El valor predeterminado es **2 horas**.

4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Seleccione una de las opciones de distribución para ajustar la configuración de **Solución de contraseña de administrador local (LAPS)**. Para más información sobre la configuración de las opciones de distribución, consulte **Trabajar con configuraciones**.
6. Haga clic en **Hecho**.

10.10.4.35. Firewall de macOS

Licencia: Gold

El Firewall de macOS administra los ajustes de cortafuegos de la aplicación a los que se puede acceder en el panel Preferencias de seguridad en dispositivos macOS.

Aplicable a: macOS 12.3+

- **Permitir que el software integrado reciba conexiones entrantes**: si es cierto, permite al software integrado reciba conexiones entrantes.
- **Permitir que el software firmado descargado reciba conexiones entrantes**: si es cierto, permite que el software firmado descargado reciba conexiones entrantes.

Aplicable a: macOS 12.0+

- **Habilitar registro**: si es cierto, se habilita el registro
- **Especifique el tipo de registro**
  - **Acelerador**
  - **Resumen**
  - **Detalle**

Aplicable a: macOS 10.12+

Cuando hace clic en **Activar firewall**, puede seleccionar una o más de las siguientes opciones:

- **Bloquear todas las conexiones entrantes**: seleccione esta opción para evitar que todos los servicios de uso compartido reciban conexiones entrantes en dispositivos macOS, como compartir pantalla o compartir archivos. Los siguientes servicios del sistema aún pueden recibir conexiones entrantes:
  - configd, que implementa DHCP y otros servicios de configuración de red
  - mDNSResponder, que implementa Bonjour
  - racoon, que implementa IPSec
- **Habilitar modo sigiloso**: Seleccione esta opción para evitar que los dispositivos macOS respondan a solicitudes de sondeo. Los dispositivos macOS administrados aún responden a las solicitudes entrantes de aplicaciones autorizadas, mientras ignoran las solicitudes inesperadas, como ICMP (ping).
- **Aplicaciones**: La lista de aplicaciones con conexiones controladas por el firewall. Seleccione las aplicaciones específicas para las que desea recibir conexiones entrantes en dispositivos macOS.

Seleccione **Agregar** para agregar una fila a la lista de aplicaciones. Seleccione la celda debajo de **ID de paquete** para seleccionar la aplicación cuyas conexiones entrantes desea permitir explícitamente. Seleccione la casilla de verificación en la celda **Permitir conexiones** para permitir conexiones entrantes desde la aplicación seleccionada.

> la configuración debe existir en un perfil con ámbito del sistema. Si más de un perfil contiene esta configuración, se utilizará la unión de configuraciones más restrictiva.

No se admiten las opciones **"Permitir automáticamente el software descargado firmado"** y **"Permitir automáticamente el software integrado"**. Sin embargo, ambas se pondrán activadas (ON) obligatoriamente cuando esta configuración esté disponible.

El administrador puede habilitar el modo sigiloso especificando un dispositivo que no se pueda descubrir por el comando ping.

10.10.4.36. Restricciones de macOS

Licencia: Gold

Las restricciones de macOS determinan qué restricciones están activadas en los dispositivos macOS.

Puede establecer que las siguientes funciones estén activadas o desactivadas en los dispositivos macOS:

Versión de macOS	Características
macOS 10.11+	• Permitir cámara • Permitir sincronización de documentos de iCloud **Solo supervisados:** • Permitir resultados de Internet de Spotlight
macOS 10.11.2+	
	• Permitir búsqueda de definición
macOS 10.12+	• Permitir sincronización de llaves de iCloud • Permitir volver a mi Mac • Permitir encontrar mi Mac • Permitir uso compartido en Notas, Recordatorios o LinkedIn • Permitir sincronización de marcadores • Permitir servicio de correo de iCloud macOS • Permitir servicio de calendario de iCloud macOS • Permitir servicio de libreta de direcciones de iCloud macOS • Permitir servicio de recordatorios de iCloud • Permitir el desbloqueo automático **Solo supervisados:** • Permitir Apple Music
macOS 10.12.4+	
	• Permitir huella digital para desbloquear
macOS 10.13+	• Permitir el uso compartido de archivos en iTunes • Permitir almacenamiento en caché del contenido • Permitir modificaciones del fondo de pantalla **Solo supervisados:** • Permitir AirPrint • Permitir descubrimiento de iBeacon de AirPrint

Versión de macOS	Características
	• Forzar requisito de TLS de confianza de AirPrint • Permitir AirDrop • Permitir Game Center
macOS 10.13.4+	**Solo supervisados:** Retrasar actualizaciones del software durante un intervalo de días (de 30 a 90 días). Predeterminado: 30 días
macOS 10.14+	
macOS 10.14.4+	**Solo supervisados:** Permitir que los dispositivos cercanos compartan solicitudes de contraseña • Permitir capturas de pantalla • Permitir observación remota de la pantalla **Solo supervisados:** • Permitir unirse a Classroom automáticamente • Permitir que Classroom solicite permiso para salir de las clases • Permitir que Classroom bloquee una aplicación y el dispositivo sin solicitarlo • Permitir forzar la observación espontánea de la pantalla del aula administrada
macOS 11.0+	
macOS 11.3+	**Solo supervisados:** Permitir forzar el retraso de las actualizaciones de software de la aplicación Tiempo de espera de huella aplicado Predeterminado: 48 horas Prerrequisito: Touch ID debe estar configurado en el dispositivo
macOS 11.3+	**Solo supervisados:** • Retraso de instalación diferido del SO principal de actualización del software forzado

Versión de macOS	Características
	• Retraso de instalación diferido del SO secundario de actualización del software forzado • Retraso de instalación diferido del SO no principal de actualización del software forzado • Forzar actualizaciones retrasadas del software principal
macOS 12+	• allowCloudPrivateRelay: si ajusta la Retransmisión privada con ACTIVA en un dispositivo de macOS, el tráfico de red se cifrará para que la actividad de interne sea privada y segura. Esta restricción requiere un dispositivo supervisado. • Permitir biblioteca de fotografías de iCloud **Solo supervisados**: • Permitir eliminar contenido y ajustes
macOS 13.0 hasta 26.0	• Permitir la instalación de mejoras de seguridad de segundo plano: para deshabilitar las respuestas. El usuario no puede instalar mejoras de seguridad de segundo plano. • Permitir la eliminación de mejoras de seguridad en segundo plano: para bloquear al usuario de poder deshacer las respuestas. El usuario no puede eliminar las mejoras de seguridad de segundo plano. • Permitir Universal Control: ◦ Si **Cierto**, la configuración le permite usar los dispositivos de entrada del dispositivo principal para controlar el dispositivo de visualización secundario. ◦ Si es **Falso**, puede agregar un dispositivo de visualización secundario pero no puede controlarlo con los dispositivos de entrada principales. **Solo supervisados**: • Permitir la instalación del perfil de configuración de la interfaz de usuario: si es falso, la configuración no permite la instalación del perfil, la configuración o los certificados en el dispositivo macOS. • Permitir modo restringido de USB: si es Verdadero, la configuración impide que el dispositivo utilice dispositivos de entrada conectados de forma remota. Las opciones de Permitir que los accesorios se conecten están atenuados en el dispositivo.
macOS 14.0+	• Permitir la modificación de la administración remota de ARD ◦ Si es falso, impide la modificación de la configuración de Compartición de administración remota en la Configuración del sistema. ◦ Predeterminado: Verdadero • Permitir modificación de Bluetooth compartido

Versión de macOS	Características
	◦ Si es falso, impide la modificación de la configuración de Bluetooth en la Configuración del sistema. ◦ Predeterminado: Verdadero • Permitir Freeform en la nube ◦ Si es falso, desactiva los servicios de iCloud Freeform. ◦ Predeterminado: Verdadero • Permitir la modificación de archivos compartidos ◦ Si es falso, impide la modificación de la configuración de Compartición de archivos en la Configuración del sistema. ◦ Predeterminado: Verdadero • Permitir la modificación de internet compartida ◦ Si es falso, impide la modificación de la configuración de Compartición de internet en la Configuración del sistema. ◦ Predeterminado: Verdadero • Permitir la creación de usuarios locales ◦ Si es false, impide la creación de nuevos usuarios en Configuración del sistema. ◦ Predeterminado: Verdadero • Permitir la modificación de una impresora compartida ◦ Si es falso, impide la modificación de la configuración de Compartición de la impresora en la Configuración del sistema. ◦ Predeterminado: Verdadero • Permitir la modificación remota de eventos de Apple ◦ Si es falso, impide la modificación de la configuración de Compartición de eventos remotos de Apple en la Configuración del sistema. ◦ Predeterminado: Verdadero • Permitir Siri ◦ Predeterminado: Verdadero • Permitir la modificación del disco de inicio ◦ Si es falso, impide la modificación de la configuración del Disco de Inicio en la Configuración del sistema. ◦ Predeterminado: Verdadero • Permitir realizar una copia de seguridad de Time Machine ◦ Si es falso, impide la modificación de la configuración de Time Machine en la Configuración del sistema. ◦ Predeterminado: Verdadero **Solo supervisados**: • Permitir modificación de la cuenta ◦ Si es falso, impide la modificación de la cuenta. ◦ Predeterminado: Verdadero

Versión de macOS	Características

	• Permitir modificar el Nombre del dispositivo
	  ◦ Si es falso, impide cambiar el Nombre del dispositivo.
	  ◦ Predeterminado: Verdadero
	• Permitir la modificación de huellas digitales de Touch ID
	  ◦ Si es falso, impide modificar las huellas dactilares de Touch ID.
	  ◦ Predeterminado: Verdadero

macOS 15.0+	**Solo supervisados**:
	• Permitir Genmoji
	  ◦ Seleccione para permitir la creación de Genmojis.
	  ◦ Predeterminado: Verdadero
	• Permitir Entorno de pruebas de imágenes
	  ◦ Seleccione para permitir el uso de la generación de imágenes.
	  ◦ Predeterminado: Verdadero
	• Permitir duplicación de iPhone
	  ◦ Seleccione para permitir que el iPhone se duplique en un dispositivo macOS.
	  ◦ Predeterminado: Verdadero
	• Permitir herramientas de escritura
	  ◦ Seleccione para activar las herramientas de escritura de Apple Intelligence.
	  ◦ Predeterminado: Verdadero

macOS 15.1+	**Solo supervisados**:
	• Permitir resumen de correo
	  ◦ Seleccione para permitir la creación manual de resúmenes de mensajes de correo electrónico.
	  ◦ Predeterminado: Verdadero
	• Permitir la modificación de medios compartidos
	  ◦ Seleccione para permitir la modificación de la configuración para compartir medios.
	  ◦ Predeterminado: Verdadero

macOS 15.2+	**Solo supervisados**: • Permitir integraciones de inteligencia externa

Versión de macOS	Características
	◦ Seleccione para habilitar el uso de servicios de inteligencia externos basados en la nube con Siri. ◦ Predeterminado: Verdadero • Permitir el inicio de sesión de integraciones de inteligencia externa ◦ Seleccione para habilitar la modificación de preferencias del navegador predeterminado. El comando de configuración Ivanti Neurons for MDM para establecer la preferencia predeterminada del navegador seguirá funcionando cuando se aplique. ◦ Predeterminado: Verdadero
macOS 15.3	
	Seguridad y privacidad: • Permitir ID de External Intelligence Workspace ◦ Introduzca la ID de External Intelligence Workspace permitida • Permitir el resumen de la transcripción de notas ◦ Seleccione para activar la creación de resúmenes de las transcripciones. ◦ Predeterminado: Verdadero

10.10.4.37. Restricciones de la AppStore de macOS

Licencia: Gold

Las restricciones de la AppStore de macOS definen qué restricciones están activadas en la AppStore de macOS.

Puede personalizar las siguientes opciones:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Establecimiento de la configuración	
Versión de macOS	**Características**
10.9+	Restringir la instalación de aplicaciones a los usuarios administradores.
10,10+	• Restringir la instalación de aplicaciones solo para actualizaciones del software. • Desactivar la adopción de aplicaciones por parte de los usuarios. • Desactivar las notificaciones de actualizaciones del software.
10,11+	Restringir la instalación de aplicaciones para aplicaciones instaladas en MDM y actualizaciones del software.

Distribución de la configuración

Procedimiento

1. Ajuste las opciones utilizando la tabla anterior.
2. Haga clic en **Siguiente**.
3. Seleccione la opción **Habilitar esta configuración**.
4. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - personalizada

Haga clic en **Hecho**.

10.10.4.38. Restricciones de grabación en disco de macOS

Licencia: Gold

Las Restricciones de grabación en disco de macOS administran las restricciones para grabar en discos en macOS. Puede configurar los **Ajustes del Finder de macOS** para activar o desactivar las opciones de grabación en disco desde la aplicación Finder en macOS.

Puede personalizar las siguientes opciones:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Establecimiento de la configuración	
Ajuste	**Qué hacer**
Permitir grabación en disco	• ENCENDIDO • APAGADO • Requerir autenticación

Distribución de la configuración

Procedimiento

1. Ajuste las opciones utilizando la tabla anterior.
2. Haga clic en **Siguiente**.
3. Seleccione la opción **Habilitar esta configuración**.
4. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - Personalizada

Haga clic en **Hecho**.

10.10.4.39. Control multimedia permitido (obsoleto)

Licencia: Gold

La configuración del Control multimedia permitido administra el montaje, desmontaje y expulsión al cerrar sesión de diferentes soportes multimedia físicos en macOS.

Puede personalizar las siguientes opciones:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Establecimiento de la configuración	
Control del montaje para tipos de soportes multimedia	
Active el control del montaje para cada tipo de soporte multimedia y defina los ajustes de montaje. Si desactiva el control de montaje, se aplicará el ajuste predeterminado del OS. **Tipo de soporte multimedia** • CD • DVD • BD	**Ajustes de montaje** • Solo lectura con autenticación • Rechazar montaje • Expulsar soporte multimedia
• CD en blanco • DVD en blanco • BD en blanco • RAM de DVD • Imagen de disco • Disco duro interno • Disco duro externo • Disco de red	• Solo lectura • Rechazar montaje • Expulsar soporte multimedia • Autenticar
• Los discos duros externos incluyen los HDD USB, el almacenamiento en unidades USB y las tarjetas SD. • Los soportes multimedia de solo lectura como los CD, DVD y BD se montan como de solo lectura de forma predeterminada. **Control de desmontaje para tipos de soporte multimedia** Active el control de desmontaje para cada tipo de soporte multimedia y defina los ajustes de desmontaje. Si desactiva el control de desmontaje, se aplicará el ajuste predeterminado del OS. Tenga cuidado al definir el ajuste Rechazar desmontaje para los tipos de soporte multimedia.	
Tipo de soporte multimedia	**Ajustes de montaje**
• CD	• Rechazar desmontaje

Ajuste	Qué hacer
• DVD • BD • CD en blanco • DVD en blanco • BD en blanco • RAM de DVD • Imagen de disco • Disco duro interno • Disco duro externo • Disco de red	• Autenticar
Ajustes de la Expulsión al cerrar sesión	
Tipos de soportes multimedia que se expulsarán automáticamente cuando el usuario cierre sesión. **Tipo de soporte multimedia** • CD • DVD • BD • CD en blanco • DVD en blanco • BD en blanco • RAM de DVD • Imagen de disco • Disco duro externo • Disco de red	

Distribución de la configuración

Procedimiento

1. Ajuste las opciones utilizando la tabla anterior.
2. Haga clic en **Siguiente**.
3. Seleccione la opción **Habilitar esta configuración**.
4. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - personalizada

Haga clic en **Hecho**.

10.10.4.40. Ajustes del Finder de macOS

Licencia: Gold

Los Ajustes del Finder de macOS administran los ajustes de la aplicación Finder en macOS.

Puede personalizar las siguientes opciones:

Ajuste	**Qué hacer**
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Establecimiento de la configuración	
Ajuste	**Qué hacer**
Desactivar la compatibilidad de grabación en disco en el Finder	• Activar • Desactivar

Distribución de la configuración

Procedimiento

1. Ajuste las opciones utilizando la tabla anterior.
2. Haga clic en **Siguiente**.
3. Seleccione la opción **Habilitar esta configuración**.
4. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - Personalizada

Haga clic en **Hecho**.

10.10.4.41. Política de extensiones del kernel de macOS

Aplicable a: macOS 10.13.2 o versiones más recientes compatibles.

Controla las restricciones y los ajustes para cargar extensiones del kernel aprobadas por el usuario.

Crear una política de extensiones del kernel de macOS

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **'kernel'** en el campo de búsqueda y, a continuación, haga clic en la configuración **Política de extensiones del kernel de macOS**.
4. Asigne un nombre a la configuración y descríbala.
5. Seleccione la opción **Permitir anulaciones del usuario** para permitir que los usuarios aprueben extensiones de kernel adicionales que no se hayan permitido explícitamente en la siguiente configuración.
6. En la sección "Identificadores de equipo y extensiones de kernel permitidos" haga clic en **+ Añadir** para agregarlos. Una extensión de kernel es el identificador del paquete. Para cada identificador de equipo, puede añadir varios nombres de extensiones de kernel debidamente firmados en la ventana emergente.
7. Haga clic en **Añadir**.
8. Haga clic en **Siguiente** para configurar los ajustes de distribución.
9. Haga clic en **Listo**.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.4.42. Mobile@Work para macOS

Esta sección contiene los siguientes temas:

- Configuración de Mobile@Work para macOS y flujo de trabajo de la ejecución de secuencias de comandos
- Crear una configuración de Mobile@Work para macOS
- Habilitación de la incorporación de los usuarios para dispositivos macOS
- Crear una configuración de secuencia de comandos de Mobile@Work para macOS
- Realizar una desinstalación limpia de Mobile@Work para macOS
- Aplicación de scripts a través de macOS Mobile@Work

Ivanti Neurons for MDM le permite crear sus propias secuencia de comandos de shell de macOS que luego pueden cargarse y Ivanti Neurons for MDMejecutarse en dispositivos macOS administrados. Para obtener información sobre cómo crear, cargar y administrar el repositorio de secuencias de comandos, consulte Todas las secuencias de comandos.

Un usuario de dispositivos macOS puede iniciar el dispositivo que se va a retirar con Mobile@Work para macOS 1.1 o posterior. La opción de retirar está disponible al hacer clic en **Desinstalar** en la pantalla Acerca de Mobile@work. En Ivanti Neurons for MDM, puede verificar el estado del dispositivo en la página **Dispositivos** y en la página de detalles del dispositivo.

Mobile@Work para macOS 1.5 o posterior abre Apps@Work inmediatamente después del registro sin esperar a que se complete el registro de MDM.

En Mobile@Work para macOS, haga clic en un mosaico de aplicación para mostrar la página Detalles de la aplicación para esa aplicación. La página incluye la descripción de la aplicación, las capturas de pantalla, las puntuaciones y las opiniones.

Mobile@Work para macOS notifica al servidor de Ivanti Neurons for MDM si las aplicaciones internas macOS con marca registrada de Packager están o no instaladas en el informe del inventario.

Requisitos previos

En el App Catalog, el cliente Mobile@Work para macOS está disponible como aplicación corporativa. Antes de poder ejecutar secuencia de comandos de shell en dispositivos macOS, pida a los usuarios que registren sus dispositivos con Ivanti Neurons for MDM mediante Mobile@Work para macOS.

Procedimiento

1. Descargue la aplicación Mobile@Work para macOS. Está disponible como un archivo PKG en https://support.mobileiron.com/support/CDL.html. Consulte este artículo del foro de clientes de Ivanti para obtener información sobre cómo obtener la credenciales para el sitio de descarga.
2. Cargue el archivo PKG de Mobile@Work para macOS en un servidor seguro. Este nunca debe ser accesible para los usuarios de los dispositivos.
3. Comparta la URL del archivo de instalación de Mobile@Work para macOS con los usuarios del dispositivo por correo electrónico o mensaje.
4. Pídales a los usuarios que hagan lo siguiente:
    1. Descargue e instale Mobile@Work para macOS en el dispositivo.
    2. Registrar los dispositivos con Ivanti Neurons for MDM utilizando Mobile@Work para macOS.

Configuración de Mobile@Work para macOS y flujo de trabajo de la ejecución de secuencias de comandos

Procedimiento

1. Configure y distribuya una configuración de Mobile@Work para macOS.
2. Configure y distribuya una configuración de script de Mobile@Work para macOS para cargar el script Ivanti Neurons for MDM. Las secuencia de comandos están cifrados y firmados mediante certificado firmado, que es único para cada abonado. La clave para descifrar la secuencia de comandos se envía al dispositivo junto con la URL de descarga de la secuencia de comandos, que está cifrado y firmado.
3. Ivanti Neurons for MDM ejecuta las secuencias de comandos en dispositivos macOS mediante Mobile@Work para macOS. Mobile@Work para macOS sondea a Ivanti Neurons for MDM periódicamente para controlar si hay secuencias de comandos en espera de ejecución. En el caso de que haya alguna secuencia de comandosen la cola, Mobile@Work descargaría y ejecutaría las secuencias de comandos en los dispositivos macOS según los ajustes que usted haya definido en Ivanti Neurons for MDM.
4. Mobile@Work para macOS obtiene los resultados de la ejecución de la secuencia de comandos para Ivanti Neurons for MDM, y estos se muestran en los registros del dispositivo. Puede verificar los registros del dispositivo desde la página de detalles del dispositivo macOS, en la pestaña **Registros**.

Crear una configuración de Mobile@Work para macOS

Hay disponible una configuración predeterminada de Mobile@Work para macOS. Sin embargo, no se distribuye a ningún dispositivo de forma automática.

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **work** en el campo de búsqueda y, a continuación, haga clic en la configuración **Mobile@Work para macOS**.
4. Asigne un nombre a la configuración y descríbala.
5. Introduzca el **Tiempo máximo de ejecución** en segundos para especificar cuánto tiempo puede ejecutarse una secuencia de comandos. El valor predeterminado es de 60 segundos.
6. Introduzca el **Tamaño máximo de respuesta** en kilobytes (KB) para especificar el límite del tamaño de la salida de la secuencia de comandos devuelta a Ivanti Neurons for MDM. Es decir, los datos stdout o stderr devueltos al ejecutar la secuencia de comandos. El valor predeterminado es 1 KB.
7. Introduzca la **Frecuencia de conexión** en minutos para especificar con qué frecuencia debe la aplicación Mobile@Work para macOS ingresar en Ivanti Neurons for MDM. El valor predeterminado es de 15 minutos.
8. (Opcional) Puede activar la incorporación de usuarios para dispositivos macOS mediante la sección **Activación de la incorporación de usuarios para dispositivos macOS**.
9. Haga clic en **Siguiente** para configurar los ajustes de distribución.
    1. Elija un nivel de distribución:
    2. **Para todo el mundo:** la aplicación se añade a los dispositivos compatibles de todos los usuarios.
    3. **A nadie:** la aplicación se almacena para distribuirse posteriormente.
    4. **Distribución personalizada**: seleccione cualquiera de las siguientes opciones:
        - **Usuarios/Grupos de usuarios**: la aplicación solo se distribuye a los usuarios o grupos de usuarios que usted elija. Haga clic en la pestaña **Usuarios** para seleccionar los usuarios.

Haga clic en la pestaña **Grupos de usuarios** para seleccionar los grupos de usuarios.

- **Dispositivos/Grupos de dispositivos:** la aplicación solo se distribuye a los dispositivos o grupos de dispositivos que usted elija.
  Haga clic en la pestaña **Dispositivos** para seleccionar el o los dispositivos.
  Haga clic en la pestaña **Grupos de dispositivos** para seleccionar los grupos de dispositivos.

10. Haga clic en **Listo**.

Habilitación de la incorporación de los usuarios para dispositivos macOS

Puede habilitar la incorporación de usuarios a los dispositivos macOS durante el proceso automatizado de Inscripción de dispositivos, como sigue:

- Tan pronto como se completa la Inscripción de dispositivos, Mobile@Work para macOS (se requiere la versión 1.68 o posterior) se inserta en el dispositivo junto con los perfiles, configuraciones y aplicaciones.
- El cliente Mobile@Work para macOS y otras aplicaciones se insertan a los dispositivos solo si:
  - Las aplicaciones son aplicaciones PKG internas o aplicaciones públicas de Apps and Books de Apple.
  - La configuración de la instalación silenciosa de las aplicaciones está ajustada en «true» (verdadero). El ajuste está disponible en la página **Aplicaciones** > Detalles de la aplicación > **Configuración de la aplicación** > **Instalación en el dispositivo**.
  - La prioridad para las aplicaciones se establece en Alta. De manera predeterminada, la prioridad de la aplicación de cliente de Mobile@Work para macOS se establece en alta (y no se puede modificar), ya que **sin esta configuración, el proceso de incorporación de usuario podría fallar.**
  - Las aplicaciones están configuradas distribuirse a los dispositivos, grupos de usuarios o grupos de dispositivos.
- Una vez que Mobile@Work para macOS se instala y registra, el dispositivo macOS entra en el modo kiosco (es decir, el usuario no tiene control sobre el dispositivo) hasta que se configuren e instalen los perfiles, configuraciones y aplicaciones restantes. El progreso se muestra en pasos.

Para versiones de Mobile@Work para macOS 1.73 o posteriores, según sea compatible con Ivanti Neurons for MDM, se admiten las siguientes características adicionales:

- El proceso de incorporación del usuario se completa poco después de que se completa la Inscripción de dispositivos para un dispositivo. El proceso de incorporación de los usuarios no comenzará después de que expire la ventana de tiempo para activar la incorporación de los usuarios (generalmente 20 minutos después del registro del dispositivo) incluso si un administrador la activa en la configuración de Mobile@Work. Esto impide que el dispositivo acceda en modo kiosco de incorporación del usuario cuando el dispositivo está en uso regular.
- El proceso de incorporación del usuario se muestra por pasos en el cliente Mobile@Work para macOS. Las configuraciones se instalarán como parte del primer paso.
- Las aplicaciones de alta prioridad se instalarán inicialmente. Cada aplicación de alta prioridad contará como un paso. Las aplicaciones de propiedad de Packager no se cuentan como parte de los pasos.
- El resto de aplicaciones seguirán instalándose en segundo plano incluso después de que se haya completado la incorporación del usuario. Las aplicaciones se marcan como instaladas después de que la instalación se inicie en un dispositivo o después de que la aplicación se instale realmente en el dispositivo.
- Después de que se incorpore el usuario, usted puede ir a la página de detalles del dispositivo para verificar las configuraciones y aplicaciones que se han introducido en cada dispositivo. En los registros encontrará más información disponible.

Procedimiento

1. Cree una configuración de Mobile@Work para macOS con **Crear una configuración de Mobile@Work para macOS**.
2. Seleccione la opción **Habilitar incorporación de usuario.**
3. Introduzca los siguientes detalles:
    - **Valor de espera de la incorporación de los usuario**: introduzca el tiempo aproximado que tardará el dispositivo en instalar la aplicación y las configuraciones durante la configuración inicial del dispositivo. Por defecto, el proceso de incorporación del usuario en un dispositivo macOS caduca en 120 segundos, un tiempo que usted puede modificar según sea necesario.
    - **URL de la página de aterrizaje del usuario**: proporciona una URL de la página de aterrizaje que se mostrará al usuario una vez que se haya completado la incorporación.
4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Haga clic en **Listo**.

Creación de una configuración de secuencia de comandos Mobile@Work para macOS

Puede crear y distribuir múltiples configuraciones de secuencia de comandos de Mobile@Work para macOS en los dispositivos. Con esta configuración, puede seleccionar una secuencia de comandos del repositorio (**Administrador > Secuencia de comandos y archivos > Todas las secuencias de comandos**) para distribuirla a Mobile@Work para macOS.

Puede programar ejecuciones de secuencia de comandos en dispositivos con Mobile@Work para macOS 1.66 o versiones posteriores. Si programa la ejecución de una secuencia de comandos para que se ejecute en dispositivos con Mobile@Work para versiones de cliente de macOS anteriores a la 1.66, la secuencia de comandos se ejecutará solo una vez. Si el cliente Mobile@Work para macOS se actualiza de la versión 1.4 a la 1.66, todas las configuraciones del cliente macOS se redistribuirán a los dispositivos.

Requisitos previos

- Vaya a **Administrador > Secuencia de comandos y archivos > Todas las secuencias de comandos** para cargar y administrar secuencias de comandos que pueden utilizarse en esta configuración y distribuirse a los dispositivos.
- Configure y distribuya la configuración de Mobile@Work para macOS en los dispositivos. De lo contrario, la configuración de la secuencia de comandos de Mobile@Work para macOS tendrá el estado «Error».

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **work** en el campo de búsqueda y, a continuación, haga clic en la configuración de **Secuencia de comandos de Mobile@Work para macOS**.
4. Asigne un nombre a la configuración y descríbala.
5. En el campo **Seleccionar secuencia de comandos**, introduzca el nombre de la secuencia de comandos que desea buscar y selecciónelo en la lista desplegable.
6. En la sección Entrada de la secuencia de comandos, se muestran las etiquetas de entrada de la secuencia de comandos y las variables de la secuencia de comandos asociadas a la misma. Si debe anularlas, introduzca variables de secuencias de comandos alternativas (por ejemplo, {$userWorkEmailAddress}) y sus valores predeterminados alternativos (por ejemplo, john.doe@company.com).
7. En la sección Ejecución de la secuencia de comandos, seleccione una de las siguientes opciones de programación:
    - Ejecutar una vez en la implementación

- Ejecución periódica

8. Si selecciona Ejecución periódica, especifique la siguiente información detallada:
   - Zona horaria a utilizar: seleccione la hora local o la hora UTC del dispositivo. La secuencia de comandos se ejecutará a la hora seleccionada en este campo.
   - La ejecución comienza el: seleccione la fecha de inicio.
   - La ejecución finaliza el: seleccione la fecha de fin (posterior o igual a la fecha de inicio).
   - Ejecutar secuencia de comandos: seleccione Diario o Semanal e introduzca las horas (en formato de 24 horas), minutos y días, según corresponda.
9. Haga clic en **Siguiente** para configurar los ajustes de distribución.
10. Haga clic en **Listo**.

Realizar una desinstalación limpia de Mobile@Work para macOS

Si activó la opción **Eliminar aplicaciones al desinscribirse(disponible solo para aplicaciones gestionadas)** durante la instalación de Mobile@Work para macOS y si inicia la eliminación del dispositivo desde el portal del administrador de Ivanti Neurons for MDM, la aplicación Mobile@Work para macOS y la secuencia de comandos de desinstalación se eliminarán del dispositivo. Para evitar que los procesos y secuencias de comandos se ejecuten en el back-end, asegúrese de que -durante el registro del dispositivo de los nuevos usuarios o la eliminación de los usuarios existentes- se anule la selección de la opción desde el portal del administrador de Ivanti Neurons for MDM, para garantizar que el secuencia de comandos de desinstalación se ejecute y elimine los procesos y secuencias de comandos asociados del back-end.

Procedimiento

1. Inicie sesión en el portal del administrador de Ivanti Neurons for MDM
2. Vaya a **Aplicaciones** > **Mobile@Work** > **Configuraciones de aplicaciones** > **Lista de resumen de configuraciones de aplicaciones** > **Ajustes de aplicaciones Apple** >**Ajustes de configuración de gestión de aplicaciones Apple**.
3. En la página de **ajustes de configuración**, desactive la siguiente opción:
   - **Eliminar aplicaciones al cancelar la inscripción (Solo disponible para aplicaciones gestionadas)**.

Aplicación de scripts a través de macOS Mobile@Work

Los scripts a través de macOS Mobile@Work permiten a los administradores implementar y ejecutar scripts de shell de forma remota en dispositivos macOS administrados. Esto ayuda a automatizar tareas, aplicar correcciones, aplicar políticas y agilizar la configuración sin requerir la intervención del usuario, lo que garantiza una administración del dispositivo coherente y eficiente a escala.

Requisitos previos:

- Los dispositivos deben estar ejecutando macOS.
- Mobile@Work para macOS ya debe estar instalado en los dispositivos.
- Asegúrese de que la configuración de Mobile@Work for macOS se cree, distribuya y asigne correctamente. Para obtener más información, consulte Creación de Mobile@Work para la configuración de macOS.

> No puede aplicar scripts a través de macOS Mobile@Work si el dispositivo no tiene el cliente Mobile@Work instalado y configurado, o si la plataforma del dispositivo no soporte la ejecución de scripts. Asegúrese de que el cliente de macOS esté activo y de que solo seleccione dispositivos de macOS compatibles.

Procedimiento

1. Inicie sesión en el portal del administrador de Ivanti Neurons for MDM
2. Vaya a **Dispositivos** y seleccione la lista de dispositivos macOS para los que desea ejecutar el script.
3. En la página **Dispositivos**, vaya a **Acciones** > **macOS** > **Scripts a través de macOS Mobile@Work**.
   Aparece el panel **Scripts a través de macOS Mobile@Work**.
4. Para aplicar los scripts, en el campo **Seleccionar script**, introduzca y seleccione el nombre del script.
   Para más información sobre cómo crear un script, consulte **Todas las secuencia de comandos**.
5. Seleccione **Aceptar** para ejecutar el script en los dispositivos.

Temas relacionados:

- **Administración > Secuencias de comandos y archivos > Todas las secuencias de comandos**
- **Cómo crear una configuración**

10.10.4.43. Configuración de las reglas de actualización de software macOS

Los administradores pueden configurar la política de actualización de software de un dispositivo definiendo las **Reglas de actualización del software de macOS**.

Aplicable a: macOS 10.7 a 26.0.

1. Vaya a Configuraciones > +Añadir.
2. Escriba macOS en el campo de búsqueda y, a continuación, haga clic en la configuración Configuración de los ajustes de actualización de software macOS.
3. Introduzca un Nombre y Descripción de la configuración.
4. Seleccione las configuraciones necesarias de las **Reglas de actualización del software de macOS**.
5. Haga clic en Siguiente.
6. Seleccione la opción Habilitar esta configuración.
7. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - Personalizado.
8. Haga clic en Hecho.

Reglas de actualización del software de macOS

Los administradores pueden seleccionar de la lista de reglas entra las siguientes:

> Los usuarios no pueden cambiar estos ajustes cuando estas reglas se aplican en el dispositivo.

- Permitir la instalación de software previo al lanzamiento.
- Automáticamente:
    - Comprobar si hay actualizaciones
    - Descargar nuevas actualizaciones cuando estén disponibles
    - Instalar actualizaciones de macOS
    - Instalar actualizaciones de aplicaciones desde la tienda de aplicaciones
    - Instalar archivos de datos del sistema y actualizaciones de seguridad.
- Restringir la instalación de aplicaciones a los usuarios administradores.
- La opción de añadir la URL del catálogo de actualizaciones de software (no se admite en macOS 11+).

10.10.4.44. Preferencia de certificado

Disponible para:

- macOS 10.12 hasta la versión más reciente ha publicado una versión compatible con Ivanti Neurons for MDM.

Identifique un elemento de Preferencia de certificado en la llave del usuario que haga referencia a una carga útil del certificado incluida en el mismo perfil.

Esta función se utiliza para enlaza un certificado a una dirección de correo electrónico o a una URL. Después de enlazar un certificado a una dirección de correo electrónico, la aplicación Mail lo usará para esa cuenta de correo electrónico. Si el Certificado SSL para un sitio web no es de confianza, al añadir una preferencia de Certificado se garantizará que en el explorador no aparece un mensaje de advertencia cuando se intenta acceder al sitio web.

> Los administradores deben tener un Certificado. Para obtener más información sobre cómo agregar y distribuir un certificado, consulte **Configuración del certificado**.

Creación de la configuración de una preferencia de certificado

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **preferencia** en el campo de búsqueda y, a continuación, haga clic en la configuración de las **Preferencia de certificado**.
4. Asigne un nombre a la configuración y descríbala.
5. Dentro de la sección Ajuste de la configuración, en el campo **Nombre**, introduzca una Id. de correo electrónico o el nombre para el que se solicita un certificado preferido.
6. En el campo **UUID del certificado**, seleccione un certificado.
7. Haga clic en **Siguiente** para configurar los ajustes de distribución.
8. Haga clic en **Listo**.

Temas relacionados:

- **Preferencia de identidad**
- **Configuración del certificado**
- **Cómo crear una configuración**

10.10.4.45. Active Directory (macOS)

Aplicable a: macOS 10.9 o versiones más recientes compatibles.

Configure opciones avanzadas para enlazar los dispositivos macOS con un dominio de Active Directory (AD) a fin de que puedan acceder a los servicios de software que dependen de Active Directory para la autenticación y seguridad.

Esta sección contiene los siguientes temas:

- Creación de una configuración de Active Directory
- Ajustes de Active Directory

Creación de una configuración de Active Directory

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **privacidad** en el campo de búsqueda y, a continuación, haga clic en la configuración de **Active Directory**
4. Asigne un nombre a la configuración y descríbala.
5. Introduzca los ajustes tal y como se describe en la siguiente tabla de ajustes de Active Directory.
6. Haga clic en **Siguiente** para configurar los ajustes de distribución.
7. Haga clic en **Hecho**.

Ajustes de Active Directory

Ajuste	Qué hacer
Ajustes de Active Directory: Básico	
Nombre de host	(Obligatorio) Introduzca el nombre de host, que es el dominio de Active Directory al que desea unirse.
Nombre de usuario	Introduzca el nombre de usuario de la cuenta utilizada para unirse al dominio.
Contraseña	Introduzca la contraseña de la cuenta utilizada para unirse al dominio.
Unidad organizativa de AD	Introduzca la unidad organizativa (UO) donde se va a añadir el objeto de equipo que se une.
Estilo de montaje de AD	Seleccione una de las siguientes opciones para indicar el protocolo de red doméstica que desea utilizar: • AFP • SMB
Ajustes de Active Directory: Avanzado	
Activar la clave ADCreateMobileAccountAtLogin	Activa o desactiva la clave ADCreateMobileAccountAtLogin. Opción adicional: Crear una cuenta móvil al iniciar sesión.
Activar la clave ADWarnUserBeforeCreatingMA	Activa o desactiva la clave ADWarnUserBeforeCreatingMA. Opción adicional: Avisar al usuario antes de crear una cuenta móvil.
Activar la clave ADForceHomeLocal	Activa o desactiva la clave ADForceHomeLocal. Opción adicional: Forzar el directorio principal local.
Activar la clave ADUseWindowsUNCPath	Activa o desactiva la clave ADUseWindowsUNCPath. Opción adicional: Usar la ruta de acceso UNC en AD para derivar la ubicación principal.
Activar la clave ADAllowMultiDomainAuth	Activa o desactiva la clave ADAllowMultiDomainAuth. Opción adicional: Permitir la autenticación desde cualquier dominio del bosque.
Shell de usuario predeterminado	Introduzca el shell de usuario predeterminado, como /bin/bash.
Asignar UID de usuario al atributo	Seleccione esta opción para asignar el UID de usuario al atributo especificado.
Asignar GID de usuario al atributo	Seleccione esta opción para asignar el GID de usuario al atributo especificado.
Asignar GID de grupo al atributo	Seleccione esta opción para asignar el GID de grupo al atributo especificado.
Servidor de dominio preferido	Seleccione este servidor de dominio como preferido.
Convención de espacio de nombres	Seleccione una de las siguientes convenciones de nombres de la cuenta de usuario: • Dominio (predeterminado) • Bosque

Ajuste	Qué hacer
Firma de paquetes	Seleccione una de las siguientes opciones de firma de paquetes: • Permitir (predeterminado) • Desactivar • Requerir
Cifrado de paquetes	Seleccione una de las siguientes opciones de cifrado de paquetes: • Permitir (predeterminado) • Desactivar • Requerir • SSL
Permitir la administración por parte de grupos especificados de Active Directory	Seleccione esta opción para permitir la administración por parte de grupos especificados de Active Directory. Haga clic en **Añadir** para añadir uno o más grupos.
Restringir DNS dinámico	Seleccione esta opción para restringir las actualizaciones dinámicas de DNS a las interfaces especificadas (por ejemplo, en0, en1, etc.). Haga clic en **Añadir** para añadir uno o más nombres de interfaz.
Cambiar el intervalo de contraseñas	Especifique la frecuencia (en días) con la que se requiere un cambio de la contraseña de la cuenta de confianza del equipo. El valor cero está desactivado.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.4.46. Preferencia de identidad

Aplicable a: macOS 10.12 o versiones más recientes compatibles.

Identifique un elemento de Preferencia de identidad en la llave del usuario que haga referencia a una carga útil de la identidad incluida en el mismo perfil.

En dispositivos macOS, la Preferencia de identidad le permite elegir una identidad (par clave-valor) que desee usar con un sitio web. Una vez que haya insertado una Preferencia de identidad (que consiste en la URL y la identidad) en el dispositivo, aparecerá en **Acceso a la llave > Todos los elementos** (el «Tipo» será «Preferencia de identidad»). La próxima vez que intente conectarse a esa URL desde Safari, el dispositivo presentará el certificado configurado.

Ivanti Neurons for MDM crea una configuración predeterminada de preferencia de la identidad del sistema con una carga útil para la URL de AppStore y el certificado que se utilizará.

Mientras el usuario accede al App Catalog de macOS con Safari en macOS 10.12 y versiones posteriores, recibirá un mensaje pidiendo la contraseña del sistema para almacenar en el caché el certificado de identidad. Los usuarios deben seleccionar "Permitir siempre" la primera vez que les aparezca para evitar que salga el mismo mensaje posteriormente mientras acceden al App Catalog de macOS.

Safari con versiones de macOS previas a la 10.12 y otros navegadores mostrarán mensajes del certificado y la contraseña del sistema mientras se accede al App Catalog de macOS en una sesión nueva con un explorador desde dispositivos macOS.

Crear la configuración de una preferencia de identidad

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **preferencia** en el campo de búsqueda y, a continuación, haga clic en la configuración de las **Preferencia de identidad**.
4. Asigne un nombre a la configuración y descríbala.
5. En la sección Ajuste de la configuración, en el campo **Nombre**, introduzca una Id. de correo electrónico, un hombre de host de DNS o un nombre que identifique de forma exclusiva al servicio.
6. En el campo **UUID del certificado**, seleccione un certificado.
7. Haga clic en **Siguiente** para configurar los ajustes de distribución.
8. Haga clic en **Listo**.

Temas relacionados:

- Preferencia de certificado
- Cómo crear una configuración

10.10.4.47. Creación automática de cuentas en Office 365(macOS)

Aplicable a:

- dispositivos macOS compatibles.
- Se recomienda que las versiones de las aplicaciones de Microsoft Office 365 sean 16.13.x o posteriores.

Configure la información y opciones de usuario para la configuración inicial de todas las aplicaciones de Microsoft Office 365.

Esta sección contiene los siguientes temas:

- Configuración de la creación automática de cuentas en Office 365
- Ajustes de la creación automática de cuentas en Office 365

Configuración de la creación automática de cuentas en Office 365

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **office** en el campo de búsqueda y, a continuación, haga clic en configuración de la **Creación automática de cuentas en Office 365**.
4. Asigne un nombre a la configuración y descríbala.
5. Introduzca los ajustes tal y como se describen en la siguiente tabla de configuración de Creación automática de cuentas en Office 365.
6. Haga clic en **Siguiente** para configurar los ajustes de distribución.
7. Haga clic en **Hecho**.

Ajustes de la creación automática de cuentas en Office 365

Ajuste	Qué hacer
Dirección de correo electrónico de activación de Office	Introduzca la dirección de correo electrónico del usuario.
Inicio de sesión automático en Office	Seleccione esta opción para omitir las ventanas que se ejecuten por primera vez. Solo solicita al usuario al información necesaria, como la autenticación de Office 365.
Opción predeterminada de abrir/guardar en ubicación local	Seleccione esta opción para que el panel de abrir/guardar se dé obligatoriamente en «En mi Mac», en lugar de en «Ubicaciones en línea».
Mostrar novedades al inicio	Seleccione esta opción para mostrar la información de la nueva característica en el lanzamiento.
Estado de ejecución de macros de Visual Basic	Seleccione una de las siguientes opciones: • Desactivado con advertencias • Desactivado sin advertencias • Activado sin advertencias
Desactivar los archivos dylib externos de Visual Basic	Seleccione esta opción para desactivar las dependencias externas de Visual Basic.
Permitir que Visual Basic enlace el sistema	Seleccione esta opción para permitir que los macros usen una API DECLARE del sistema operativo para enlazar al sistema(). Esta API permite que los macros ejecuten procesos externos arbitrarios y pasa los datos arbitrarios por la línea de comandos.
Desactivar el enlace de Visual Basic a Popen	Seleccione esta opción para permitir que los macros usen una API DECLARE del sistema operativo para enlazar a Popen(). Esta API permite que los macros ejecuten procesos externos arbitrarios y pasa los datos arbitrarios por la línea de comandos.
Desactivar la secuencia de comandos de Mac de Visual Basic	Seleccione esta opción para permitir que los macros invoquen la API de Visual Basic de Apple Script.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.4.48. Autenticar

Aplicable a:

- macOS 10.13 y versiones más recientes compatibles.
- Windows 10 y versiones más recientes compatibles.

Utilice la configuración de Authenticate para proporcionar una autenticación sin contraseña para los servicios de inicio de sesión en la nube o de sobremesa. Cada dispositivo tendrá una sola configuración de Authenticate.

Requisitos previos

- Se requiere una licencia Zero Sign-On.
- Ivanti Neurons for MDM debe registrarse en Access (el perfil de Access debe estar configurado).
- Después de ajustar la configuración de Authenticate, no podrá anular el registro del perfil de Acceso, ya que la configuración de Authenticate hará referencia a este.
- Si el perfil de Access tiene algún cambio, redistribuya la configuración de Authenticate a los dispositivos macOS. Para los dispositivos Windows, copie y use los nuevos valores de CLI en las nuevas aplicaciones.

Crear una configuración de Authenticate

Procedure

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **auth** en el campo de búsqueda y, a continuación, haga clic en la configuración de **Authenticate**.
4. Asigne un nombre a la configuración y descríbala.
5. Seleccione un **Certificado de identidad de escritorio** de la lista desplegable.
6. Seleccione una o ambas de las siguientes opciones del sistema operativo:
    - macOS
    - Windows
7. Para macOS:
    1. En la región de Datos personalizados, pulse **+ Añadir** para añadir claves y valores de cadena para los datos personalizados que se insertarán a los dispositivos.
    2. Haga clic en **Siguiente** para configurar los ajustes de distribución.
    3. Haga clic en **Hecho**.
8. En los dispositivos Windows 10, esta configuración ayuda a generar argumentos de línea de comandos para la aplicación MSI de Authenticator para Windows de la siguiente manera:
    1. Pulse **Hecho** para completar la configuración de Authenticate.
    2. Desde la página **Configuraciones**, vea la configuración de Authenticate para copiar el texto de la línea de comandos que se muestra. Este texto es necesario cuando se distribuye la aplicación Authenticate a dispositivos Windows.

> Cuando la configuración de Authenticate se aplica a los dispositivos Windows, la configuración permanece en estado «Instalación pendiente». Puede ignorar esto, ya que la funcionalidad no se verá afectada.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.4.49. App Catalog de Apple

Aplicable a: iOS y macOS

La configuración del Apple App Catalog gestiona el acceso al Apple App Catalog a través de un clip web. A partir de la versión 83 de Ivanti Neurons for MDM, puede transicionar a la experiencia nativa de Apps@Work desde la aplicación Go. Para abonados nuevos, la configuración de webclip de Apps@work no se distribuye por defecto para dispositivos de iOS que estén instalados mediante iReg o un cliente. El administrador debe distribuir manualmente la configuración de webclip en los dispositivos que estén registrados mediante iReg o cliente.

> El resultado de la búsqueda el webclip de Apps@Work muestra solo 10 aplicaciones en los dispositivos iOS y iPad, aunque la solicitud de búsqueda tenga como parámetro filas superiores a 10.

Procedimiento

Los administradores pueden editar la distribución de esta configuración definida por el sistema del siguiente modo:

1. Vaya a **Configuraciones**.
2. Haga clic en **Apple App Catalog**.
3. Haga clic en **Editar distribución**.
4. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos: se enviará esta configuración a todos los dispositivos compatibles.
    - Ningún dispositivo: se desactiva el acceso al App Catalog de Apple o se lanzará esta configuración para una posterior distribución.
    - Predeterminada: se definen los grupos de dispositivos específicos a los que se enviará esta configuración.

Haga clic en **Guardar**.

10.10.4.50. Dominios administrados

Licencia: Silver

Una configuración de dominio administrado le permite especificar qué dominios son confiables para Mail y Safari en dispositivos iOS 8 y visionOS 1.1. Una vez que se aplica la configuración al dispositivo, los dominios que no se especifican en la configuración aparecerán resaltados (los que no son de confianza) en Mail y Safari en el dispositivo. Utilice esta configuración combinada con una **configuración de restricciones** para controlar las descargas de datos permitidas en Safari.

Ajustes de dominios administrados

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Dominios de correo electrónico administrados	Haga clic en **+Añadir** para introducir un dominio, como en miempresa.com.
Dominios web administrados	Haga clic en **+Añadir** para introducir un dominio, como en miempresa.com.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.4.51. Configuración del código de acceso

Una de las primeras cosas que se configuran en Ivanti Neurons for MDM (con el asistente de inicio) es la configuración del código de acceso. Esta configuración define los ajustes para la función de bloqueo de pantalla en los dispositivos.

Ajustes del código de acceso

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Permitir valores simples	Restringe si el PIN o la contraseña contienen caracteres o dígitos ordenados. **Para iOS, macOS, watchOS, y Android:** seleccione esta opción para permitir PIN o códigos de acceso que sean menos seguros porque contengan secuencias de caracteres repetidas, ascendentes o descendentes. Ejemplos: 1111, 1234, abcd. Si deselecciona esta opción para dispositivos Android, se ejecutarán los códigos de acceso con PIN complejos. Por ejemplo, los usuarios no podrán configurar secuencias de caracteres repetidos, ascendentes o descendentes. **Para Windows 10+**: seleccione permitir códigos de acceso menos seguros porque contengan secuencias de caracteres repetidos o secuencias numéricas ascendentes. Ejemplos: 1111, 1234.
Requerir valor alfanumérico	Requiere que el código de acceso contenga al menos una letra y un número. **Para iOS y Android:** seleccione esta opción para garantizar que los códigos de acceso incluyan letras y números. **Para Windows 10+**: seleccione esta opción para garantizar una contraseña segura basada en el estándar de Microsoft.
Longitud mínima del código de acceso	Seleccione un número de la lista para establecer la longitud mínima del código de acceso. **Para Windows 10 Desktop**: las cuentas locales requerirán un código de acceso con una longitud mínima de 6 dígitos.
Número mínimo de caracteres complejos	**Para iOS y Android**: seleccione un número de la lista para establecer un número mínimo de caracteres que no sean números o letras. **Para Windows 10+**: las cuentas locales aplicarán 3 caracteres complejos.
Antigüedad máxima del código de acceso	Introduzca un número para la cantidad de días después de los que el usuario del dispositivo debe restablecer el código de acceso. Si no desea establecer la antigüedad del código de acceso, deje este campo en blanco.
Autobloqueo	Seleccione un intervalo de la lista para definir cuánto tiempo puede permanecer inactivo el dispositivo antes de establecer automáticamente el bloqueo de pantalla.
Cualquier método de bloqueo	**Solo Android**. Permite que el usuario elija cualquier método de bloqueo, incluido el desbloqueo mediante patrón. Los ajustes del código de acceso anteriores no se aplicarán a este dispositivo.
Historial del código de acceso	Introduzca un número para establecer la cantidad de códigos de acceso exclusivos que debe introducir el usuario antes de volver a usar un código de acceso. Por ejemplo, si define este campo en 4, el usuario deberá establecer 4 códigos de acceso antes de poder volver a usar el primer código de acceso.

Ajuste	Qué hacer
Período de gracia del bloqueo del dispositivo	Seleccione un intervalo de la lista para establecer el tiempo que pasará desde que aparezca la pantalla de bloqueo y hasta que el usuario del dispositivo tenga que introducir un código de acceso para desbloquear el dispositivo.
Número máximo de intentos erróneos	Seleccione un número de la lista para establecer la cantidad de veces que el usuario del dispositivo puede introducir de forma consecutiva el código de acceso incorrecto antes de que el dispositivo se restablezca y se borre. **Advertencia:** los dispositivos se borrarán si el usuario excede la cantidad máxima de intentos de contraseña. Tenga cuidado con esta opción.
(Solo macOS) Activar la expresión regular del código de acceso (macOS 14+)	Especifique la cadena de expresión que coincide con la contraseña para determinar si coincide con la política.
(Solo macOS) Idioma	Especifique el idioma de la Descripción.
(Solo macOS) Descripción	Describir la complejidad de la contraseña Por ejemplo, números, caracteres especiales, cadena, etc.
(Solo macOS) Aplicar una regla de código de acceso en el siguiente inicio de sesión	Seleccione esta opción para que macOS solicite al usuario que cambie la contraseña la próxima vez que inicie sesión para que cumpla con la políticas sobre contraseñas. Esta opción no está seleccionada de forma predeterminada. Aplicable a macOS 10.13 y versiones posteriores.
(Solo macOS) Minutos hasta el reinicio tras un inicio de sesión fallido	Especifique los minutos para que se restablezca el inicio de sesión después de que se haya superado el número máximo de intentos de inicio de sesión fallidos. Asegúrese de que el número máximo de intentos fallidos está establecido para habilitar este campo. Disponible en macOS 10.10 y posterior.
SmartLock	**Para dispositivos Android 5.0 excepto en perfiles de trabajo con la versión corporativa de Android:** **Para Android 6.0 o posterior:** permite o no permite a un usuario elegir la función SmartLock para desbloquear un dispositivo. La función SmartLock desbloquea automáticamente un dispositivo en ciertas circunstancias como en la proximidad del usuario con el dispositivo, el dispositivo en una ubicación o cuando el dispositivo se sincroniza con un dispositivo de confianza.
Desbloqueo de huella digital	**Para dispositivos Android 5.0 excepto en perfiles de trabajo con la versión corporativa de Android:** **Para Android 6.0 o posterior:** Permite o no permite a un usuario elegir la función de huella digital para desbloquear un dispositivo.
Notificaciones de la pantalla de bloqueo (solo	**Permitir notificaciones para los dispositivos administrados en el trabajo (para el propietario del dispositivo)** Permitir o no permitir notificaciones en la pantalla de bloqueo para dispositivos administrados del

Ajuste	Qué hacer
para la versión corporativa de Android)	trabajo **Permitir notificaciones sin editar para el perfil profesional** **Para Android 6.0 o posterior:** Permitir o no permitir notificaciones sin editar en la pantalla de bloqueo para dispositivos administrados del trabajo. Después de activar este ajuste, recibirá la notificación pero el contenido aparecerá como «Contenido oculto por la política». Solo podrá ver el contenido (correo electrónico/notificación push) desde la aplicación.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.4.52. Preferencias de privacidad (macOS)

Aplicable a: macOS 10.14 o versiones más recientes compatibles.

Configurar qué aplicaciones tienen permitido obtener acceso a los servicios, archivos y recursos del sistema. Esta configuración controla la configuración de un dispositivo macOS en Preferencias del sistema > Seguridad y privacidad > Privacidad.

Creación de una configuración de preferencias de privacidad

Procedure

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **privacidad** en el campo de búsqueda y, a continuación, haga clic en la configuración de las **Preferencias de privacidad**.
4. Asigne un nombre a la configuración y descríbala.
5. Vaya a una de las aplicaciones enumeradas en la página. Consulte la documentación de Apple para ver información relacionada.
    1. Para macOS 10.14+, las aplicaciones y los ajustes disponibles para la configuración incluyen:
        - Accesibilidad: especifica las políticas para la aplicación a través del subsistema de accesibilidad.
        - Libreta de direcciones: especifica las políticas para la información de contacto administrada por Contacts.app.
        - Eventos de Apple: especifica las políticas para la aplicación que envía los AppleEvents restringidos a otro proceso.
        - Calendario: especifica las políticas para la información del calendario administrado por Calendar.app.
        - Cámara: una cámara del sistema. El acceso a la cámara no puede darse en un perfil; solo puede denegarse.
        - Micrófono: un micrófono del sistema. El acceso al micrófono no puede darse en un perfil; solo puede denegarse.
        - Fotos: las fotos gestionadas por la aplicación Fotos en ~/Pictures/.photoslibrary.
        - Publicar un evento: especifica las políticas para que la aplicación utilice las API de CoreGraphics para enviar CGEvents al flujo de eventos del sistema.
        - Recordatorios: especifica las políticas para la información de los recordatorios administrados por la aplicación Recordatorios.
        - Política del sistema (todos los archivos): permite el acceso de la aplicación a todos los archivos protegidos, incluidos los archivos de administración del sistema.
        - Política del sistema (archivos de administración): permite a la aplicación acceder a algunos archivos utilizados en la administración del sistema.
    2. Para macOS 10.15+, las aplicaciones y los ajustes disponibles para la configuración incluyen:
        - Uso de archivos: permite que la aplicación del Proveedor de archivos sepa cuándo está usando el usuario los archivos administrados por el Proveedor de archivos.
        - Escuchar eventos de todos los procesos: permite a la aplicación utilizar las API de CoreGraphics y HID para escuchar (recibir) eventos CGEvents y HID de todos los procesos. El acceso a estos eventos no puede darse en un perfil; solo puede denegarse. Desmarque la opción Permitido.
        - Acceso a la biblioteca multimedia: permite a la aplicación acceder a Apple Music, a la actividad de música y vídeo y a la biblioteca multimedia.
        - Captura de pantalla de la visualización del sistema: permite a la aplicación capturar (leer) el contenido de la visualización del sistema. El acceso a los contenidos no puede darse en un perfil; solo puede denegarse. Desmarque la

opción Permitido.

- Reconocer y enviar datos de voz a Apple: permite a la aplicación utilizar el sistema de reconocimiento de voz y enviar datos de voz a Apple.
- Acceder a los archivos de la carpeta Escritorio del usuario: permite a la aplicación acceder a los archivos de la carpeta del escritorio del usuario.
- Acceder a los archivos de la carpeta Documentos del usuario: permite a la aplicación acceder a los archivos de la carpeta Documentos del usuario.
- Acceder a los archivos de la carpeta Descargas del usuario: permite a la aplicación acceder a los archivos de la carpeta Descargas del usuario.
- Acceder a los archivos de los volúmenes de la red: permite a la aplicación acceder a los archivos de los volúmenes de la red.
- Acceder a los archivos de los volúmenes extraíbles: permite a la aplicación acceder a los archivos de los volúmenes extraíbles.

6. Para cada aplicación que quiera configurar, haga clic en **Acciones > Añadir**.
7. Introduzca los valores para las siguientes claves de identidad:
   - Identificador: nombre de los ajustes. Por ejemplo: «us.zoom.ZoomPresence».
   - Tipo de identificador: seleccione entre ID de paquete o Ruta. Por ejemplo: «Id. del paquete»
   - Requisito de código: especifique el valor de ID de paquete o ruta. Por ejemplo: «identifier "us.zoom.ZoomPresence" and anchor apple generic».
   - Código estático (Verdadero o Falso)
   - Permitido (Verdadero o Falso)
   - Comentar
8. Haga clic en **Guardar**.
9. (Opcional) En cualquier aplicación, haga clic en **Acciones > Eliminar** para eliminar cualquier ajuste de preferencias de privacidad existente.
10. Haga clic en **Siguiente** para configurar los ajustes de distribución.
11. Haga clic en **Hecho**.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.4.53. Configuración de privacidad

Una configuración de privacidad define si:

- Los datos de ubicación de se recopilan en el dispositivo y se envían al sistema de administración del dispositivo.
- los administradores tienen permiso para borrar el dispositivo
- el inventario de aplicaciones se recopila para todas las aplicaciones o solo para las que aparecen en el catálogo de aplicaciones

Ajustes de privacidad

> La acción «Borrar un dispositivo» y la recopilación de un inventario para todas las aplicaciones del dispositivo no se aplica a los dispositivos inscritos por el usuario.

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Recopilar datos sobre localización	Seleccione esta opción para habilitar la obtención de datos sobre localización. Vea la localización del dispositivo en la página **Dispositivos**. • La localización de un dispositivo está basada en la ubicación de la red solamente para iOS. • Para dispositivos Android, la localización está basada tanto en la ubicación de la red como en la ubicación del GPS (si estuviera disponible). • Para los dispositivos de Windows, la ubicación se basa en los valores de latitud y longitud obtenidos durante la comprobación de un dispositivo. Cuando se ha habilitado la obtención de localización en el dispositivo, la ubicación actual se actualiza cada 4 horas. Cuando el dispositivo se retira o la configuración de privacidad se desactiva o elimina, los datos sobre localización se eliminan del sistema de administración de dispositivos. Los usuarios de los dispositivos pueden **desactivar la obtención de datos de ubicación del dispositivo**.
Desactivar acción «Borrar dispositivo»	Seleccione esta opción para evitar que los administradores borren el dispositivo. Considere la posibilidad de seleccionar esta opción para dispositivos del usuario (propiedad del usuario).
Pedir al usuario que habilite los servicios de localización	Seleccione para permitir que los usuarios activen, como opción, la capacidad de permitir o rechazar el uso de los servicios de ubicación, incluida la ubicación de dispositivos, de Wi-Fi y de MTD, si fuera necesario. En el caso de dispositivos totalmente administrados, el administrador puede garantizar esto automáticamente si elige deshabilitar la opción.
Recopilar inventario de aplicaciones	Seleccione **Recopilar el inventario de aplicaciones** para recopilar la información de todas las aplicaciones instaladas en el dispositivo, independientemente de si la aplicación está presente en el catálogo de aplicaciones. Seleccione **Para las aplicaciones del dispositivo que están en el Catálogo de aplicaciones** para que se recopile información solamente sobre dichas aplicaciones instaladas en el dispositivo y presentes en el catálogo de aplicaciones. Seleccione **Para todas las aplicaciones del dispositivo** para recopilar información sobre todas las aplicaciones del dispositivo. Esta opción es aplicable a los dispositivos Windows 10+. Se muestran y seleccionan por defecto los siguientes inventarios del tipo de origen de la aplicación. • **Activar inventario que no sea de la App Store**: para aplicaciones internas (aplicaciones universales) insertadas a través de MDM o instaladas por el usuario final directamente en el dispositivo al desempaquetar manualmente la aplicación e instalarla de forma local. • **Activar inventario de la App Store**: para las aplicaciones instaladas manualmente desde Microsoft Store o a través del escaparate de Apps@work. • **Activar inventario del sistema**: para las aplicaciones comunicadas como preinstaladas junto con el sistema operativo Windows 10 de Microsoft. • **Habilitar inventario Win32**: para las aplicaciones basadas en el sistema 32, como aplicaciones como MSI, EXE, aplicaciones de Win32 Store, etc. que se instalan de manera

Ajuste	Qué hacer
	forzada a través de MDM o instaladas directamente en el dispositivo por el usuario final. Opcionalmente, puede seleccionar solo aquellos inventarios del tipo de origen de la aplicación para recopilar información sobre aplicaciones seleccionadas. Las aplicaciones instaladas por MDM aparecen en el Inventario de aplicaciones, incluso si no ha seleccionado Inventario de aplicaciones que no pertenecen a App Store o Win32. El inventario de .EXE también se recopila cuando la configuración de Privacidad utiliza la configuración predeterminada para recopilar Inventario de aplicaciones solo para AppCatalog. El inventario se debe recopilar de manera sistemática para todas las aplicaciones, cuando se recopilan solo las aplicaciones de AppCatalog. El inventario de aplicaciones Modern, MSI y EXE disponible en el Catálogo de aplicaciones se extraerá solo cuando se distribuya al menos una aplicación perteneciente a cada una de estas variantes.
Los ajustes de dispositivos Android Enterprise (7.0+) Configure los ajustes siguientes para establecer la política de privacidad en dispositivos de Android Enterprise.	
Nombre de la organización	Introduzca el nombre de la organización que gestiona el dispositivo.
Color de la organización	Seleccione el color de la organización que debe mostrarse en el fondo de la pantalla del usuario.
Mensaje breve	Introduzca un mensaje corto que se mostrará cuando el usuario intente usar una función bloqueada por el administrador.
Mensaje largo	Introduzca un mensaje largo que se debe mostrar cuando el usuario haga clic en el mensaje breve. Este mensaje proporciona más detalles sobre la restricción aplicada al usuario.
Mantenga ocultas las pantallas de la aplicación Go	Seleccione Cierto o Falso en la lista. • **Cierto**: mientras se comparte de manera remota, las pantallas de la aplicación Ivanti Go no serán visibles. • **Falso**: mientras se comparte de manera remota, las pantallas de la aplicación Ivanti Go estarán visibles para cualquier ayuda con la resolución de problemas y también para ver la documentación.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.4.54. Información de Declaración de la privacidad del cliente

Aplicable a: dispositivos Android, dispositivos con Android Enterprise y iOS o versiones más recientes compatibles.

Configuración para distribuir la información de la Declaración de Privacidad a los usuarios de los clientes de Go. Se trata de una configuración definida por el sistema que se puede editar para configurar solo los ajustes de distribución.

La información que se muestra al usuario incluye los detalles configurados como parte de las siguientes configuraciones:

- Privacidad
  - Recopilar datos sobre localización
  - Recopilar inventario de aplicaciones
  - Android 7.0 +
    - Nombre de la organización
    - Color de la organización
    - Mensaje breve
    - Mensaje largo
- Privacidad del cliente
  - SLC: cambio de localización significativo («Significant Location Change») para activar periódicamente el dispositivo.
  - Intervalo mínimo para las activaciones basadas en la ubicación
  - Activar estado MixPanel
- Administración de dispositivos móviles - Derechos de acceso de MDM (no aplicable a los dispositivos inscritos por el usuario)
  - Bloqueo del dispositivo y eliminación de códigos de acceso
  - Borrado del dispositivo
  - Información de red (números de teléfono/SIM, direcciones MAC)

10.10.4.55. Ajustes del cliente de Ivanti Go

Configure la recopilación de datos anónimos de los usuarios finales, incluyendo información sobre el dispositivo y su uso, para ayudar a identificar problemas del producto y garantizar una alta calidad del servicio. Esta configuración también habilita las opciones de configuración del contacto de soporte.

Crear una configuración de Ajustes del cliente de Ivanti Go

Aplicable a:

- Mobile@Work para macOS 1.67 o versiones más recientes compatibles.
- Go para iOS 3.5.0 o las versiones más recientes compatibles.
- Mobile@Work para Android 12.9.0.0 o versiones más recientes compatibles.
- Vaya a Android 124 o versiones más recientes compatibles.

Procedimiento

1. Vaya a **Configuraciones** > **Agregar configuración** > **Ajustes del cliente de Ivanti Go**. Aparece la página **Crear configuración de ajustes del cliente de Ivanti Go**.
2. Introduzca un nombre para la configuración en el cuadro **Nombre**.
3. Introduzca una **Descripción** de la configuración.
4. En **Activaciones basadas en la ubicación**, seleccione la opción **Habilitar SLC**. El servicio de cambio significativo de localización ofrece una alternativa más ahorrativas para instalar actualizaciones de localización en la aplicación Go para iOS solo cuando la posición del usuario cambie considerablemente, después de 15 minutos como mínimo (intervalo predeterminado). Si este servicio está activado, al cambiar la localización la aplicación Go se activa en segundo plano y efectúa un ingreso.
5. En **Recolección de datos mediante análisis para clientes**, seleccione la opción **Habilitar análisis** si esta se encuentra deshabilitada. De forma predeterminada, esta opción está activada.
6. Haga clic en **Siguiente** para configurar los ajustes de distribución.
7. Haga clic en **Listo**.

Configure la pestaña Ajuste para soporte

Aplicable a:

- Mobile@Work para macOS 1.67 o versiones más recientes compatibles.
- Go para iOS 3.5.0 o las versiones más recientes compatibles.
- Mobile@Work para Android 12.9.0.0 o versiones más recientes compatibles.
- Vaya a Android 124 o versiones más recientes compatibles.

Procedimiento

1. Vaya a **Configuraciones** > **Agregar configuración** > **Ajustes del cliente de Ivanti Go**. Aparece la página **Crear configuración de ajustes del cliente de Ivanti Go**.
2. Introduzca un nombre para la configuración en el cuadro **Nombre**.
3. Introduzca una **Descripción** de la configuración.
4. En la opción **Plataforma**, seleccione la plataforma correspondiente.

5. En la sección **Configurar la pestaña Ajustes para soporte**, haga clic en **Activar la pestaña Soporte**.

> El campo **Habilitar pestaña de soporte** solo es aplicable a dispositivos iOS.

> Puede habilitar la **Pestaña de soporte** en Go para iOS versión 118.0.0 o superior y en Go para Android versión 124 o superior. Los dispositivos con versiones anteriores no se mostrarán ni serán compatibles con esta función.

En la sección **Configuración de Contacto de Soporte**, proporcione los siguientes detalles:

- **Nombre de pestaña**: introduzca el nombre de la pestaña que se muestra en la navegación de aplicaciones de Ivanti. El valor por defecto es "Soporte". (Longitud máxima: 10 caracteres)
- **Instrucciones para el usuario final**: introduzca las instrucciones sobre cómo usar los contactos de soporte. (Longitud máxima: 40 caracteres)
- **Agregar contactos**: haga clic en **+Agregar** para agregar los contactos. (Número máximo de contactos: 5)
  - **Nombre**: introduzca el nombre del contacto. (Longitud máxima: 20 caracteres)
  - **Número de teléfono**: introduzca un número de teléfono válido. (Con código de marcación internacional)
- **Agregar URL**: haga clic en **+Agregar** para agregar las URL. (Número máximo de URL: 5)
  - **Nombre de URL**: introduzca el nombre de la URL. (Longitud máxima: 20 caracteres)
  - **URL**: introduzca una URL válida.
- **Información adicional**: introduzca cualquier mensaje relacionado con soporte técnico adicional que desee que se muestre aquí. (Longitud máxima: 120 caracteres)
- **Dirección de correo electrónico**: introduzca el correo electrónico donde desee enviar los correos de soporte. (Longitud máxima: 40 caracteres)

  > Debe introducir una dirección de correo electrónico válida con formato alias@nombrededominio.com

- **URL del sistema de tickets de soporte** - Añada un botón "**Crear un ticket de soporte**" a la pestaña **Soporte** en las aplicaciones **Ivanti Go para iOS** e **Ivanti Go para Android** . Active el conmutador para mostrar el botón en la pestaña soporte e introduzca la URL adecuada en el campo proporcionado para redirigir a los usuarios a su sistema de soporte .

  > Esta URL se utiliza en la **Pestaña de soporte** de Ivanti Go para redirigir a los usuarios al sistema de soporte designado Por motivos de seguridad, se recomienda utilizar URL que comiencen por *https://* en lugar de *http://*.

Haga clic en **Siguiente** para configurar los ajustes de distribución.

8. Haga clic en **Listo**.

Para obtener más información, consulte **Configuraciones**.

10.10.4.56. Ajustes de Siri

Utilice los **Ajustes de Siri** para gestionar los ajustes en dispositivos supervisados. Esta configuración ayuda a los administradores a aplicar controles coherentes basados en políticas para gestionar cómo los dispositivos acceden a las funciones de Siri y las utilizan.

Disponible para:

- iOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- macOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- watchOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- visionOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- Dispositivos tvOS 27 o versiones posteriores supervisados hasta la versión más reciente publicada y compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Busque **Ajustes de Siri** y seleccione la configuración correspondiente.
3. Configure los **Ajustes de Siri** según la siguiente tabla:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Activado	Seleccione la casilla para habilitar Siri. Active **Enviar al dispositivo** para habilitar Siri en dispositivos supervisados.
Habilitar Siri AI	Seleccione la casilla de verificación para habilitar las funciones **específicas de** Siri AI. Alterne el **botón** Pulsar en dispositivo para habilitar las funciones **específicas de** Siri AI en dispositivos supervisados.
Permitir contenido generado por usuarios	Seleccione la casilla para habilitar el contenido generado por los usuarios. Active **Enviar al dispositivo** para habilitar el contenido generado por usuarios en dispositivos supervisados. Este ajuste no se aplica a dispositivos macOS y visionOS.
Permitir mientras está bloqueado	Seleccione la casilla para habilitar para habilitar el uso Mientras está bloqueado. Active **Enviar al dispositivo** para permitir el uso de esta función mientras el dispositivo está bloqueado. Este ajuste no se aplica a dispositivos macOS y visionOS.
Forzar el filtro de lenguaje ofensivo	Seleccione la casilla para habilitar Forzar el filtro de lenguaje ofensivo. Active **Enviar al dispositivo** para activar el filtro de contenido ofensivo en dispositivos supervisados. Este ajuste no se aplica a dispositivos visionOS.
Forzar la reducción de contenido sensible	Seleccione la casilla de verificación para forzar a Siri a reducir el contenido sensible. Alterne el **botón** Pulsar en dispositivo para forzar a Siri a reducir el contenido sensible en dispositivos supervisados.

4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Seleccione una de las opciones de distribución para configurar los **Ajustes de Siri**. Para más información sobre la configuración de las opciones de distribución, consulte **Trabajar con configuraciones**.
6. Haga clic en **Hecho**.

10.10.4.57. Configuración de archivos de configuración de servicios

La configuración de **Archivos de configuración de servicios** permite a los administradores gestionar y desplegar centralizadamente archivos de configuración para diversos servicios del sistema en los dispositivos inscritos. Además, los administradores pueden garantizar que la configuración de los servicios se mantenga coherente y resistente a modificaciones no autorizadas al entregar los archivos a directorios seguros y específicos de cada servicio, dentro de un entorno protegido contra alteraciones.

Aplicable a: dispositivos macOS

Antes de empezar:

- Puede cargar varias configuraciones en formato de archivo *ZIP*. Para obtener más información sobre cómo agregar un archivo, consulte **Archivos**.
- Todos los archivos del archivo expandido se establecen como permisos de archivo *-r–r–r– unix*. Cualquier enlace dentro del archivo tendrá restricciones y solo podrá hacer referencia a archivos ubicados en la carpeta específica del servicio.
- Los archivos del archivo ZIP deben replicar la estructura de carpetas y los archivos de configuración que el servicio espera encontrar a partir de la raíz del sistema de archivos. El servicio utiliza únicamente los archivos proporcionados en la declaración e ignora los ubicados en sus directorios predeterminados.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Buscar y seleccionar la configuración de **Archivos de configuración del servicio**.
3. Configure los ajustes de los **Archivos de configuración del servicio** como se indica en la siguiente tabla:

Ajuste	Descripción
Nombre,	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Seleccionar archivo	Introduzca el nombre del archivo.
Elija el tipo de servicio	Seleccione uno de los **Tipos de servicios** en la lista desplegable: • SSHD • SUDO • PAM • CUPS • HTTP_D • BASH • ZSH

4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Seleccione una de las opciones de distribución para ajustar la configuración de **Archivos de configuración de servicios**. Para más información sobre la configuración de las opciones de distribución, consulte **Trabajar con configuraciones**.

6. Haga clic en **Hecho**.

10.10.4.58. Actualizaciones de software

Aplicable a:

- Dispositivos supervisados iOS 10.3 a 26.0 y tvOS 12.0 a 26.0
- Dispositivos macOS
- Dispositivos Windows 10

Cree y distribuya reglas para las actualizaciones del SO.

Esta sección contiene los siguientes temas:

- Configurar actualizaciones de software para dispositivos iOS/tvOS
- Configuración de las actualizaciones de software para los dispositivos No-DEP y DEP macOS
- Configurar actualizaciones de software para dispositivos Windows
- Aplicación de actualizaciones de software mediante gestión declarativa de dispositivos

Configurar actualizaciones de software para dispositivos iOS/tvOS

Procedimiento

Para permitir que a los dispositivos iOS/tvOS se les envíen actualizaciones del SO si están en modo supervisado:

1. Vaya a **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Haga clic en **Actualizaciones del software**.
4. Haga clic en **iOS/tvOS** para ver la sección Ajustes de la configuración.
5. Seleccione la opción **Permitir que las actualizaciones del SO se instalen automáticamente en dispositivos supervisados**.
6. Seleccione una de las siguientes opciones:
    - Actualizar a la última versión
    - Actualizar a una versión específica: por ejemplo, introduzca el número de versión de iOS como 11.3.0.
7. Seleccione una de las siguientes acciones de instalación:
    - Predeterminada
    - Solo descarga
    - Instalar lo antes posible
8. Seleccione las siguientes opciones de hora a la que deben producirse las actualizaciones:
    - Hora de inicio
    - Hora de fin
    - Zona horaria
9. Haga clic en **Siguiente**.
10. Seleccione la opción **Habilitar esta configuración**.
11. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos

- Ningún dispositivo (predeterminada)
- Personalizada

12. Haga clic en **Hecho**.

- Al instalar una versión específica de una actualización del SO para dispositivos iOS, debe seleccionar una versión que esté disponible para el dispositivo. Si selecciona una versión no válida o que no esté disponible, se ignorarán las actualizaciones de software del dispositivo.
- Si el dispositivo tiene un código de acceso, después de que MDM envíe la actualización al dispositivo, este pone en cola la actualización y se pide al usuario que introduzca su código de acceso para iniciar la instalación.
- Habilite `enforcedSoftwareUpdateDelay` en **Restricciones de iOS** para asegurarse de que el análisis manual de los dispositivos en busca de actualizaciones de software no eliminará las versiones específicas que ha descargado esta configuración.

Configuración de las actualizaciones de software para los dispositivos No-DEP y DEP macOS

El perfil de Inscripción de dispositivos forma parte de Apple Business Manager, que permite que los clientes puedan comprar dispositivos en grandes cantidades e inscribirlos automáticamente en MDM durante la activación. Para obtener información, consulte **Inscripción de dispositivos**.

El procedimiento siguiente le ayuda a enviar actualizaciones de SO a dispositivos de macOS con DEP y sin DEP.

Procedimiento

1. Vaya a **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Haga clic en **Actualizaciones del software**.
4. Haga clic en **macOS** para ver la sección Ajustes de la configuración.
5. Seleccione la opción **Habilitar actualizaciones de software de macOS**.
6. Seleccione el tipo de actualizaciones para el dispositivo. Para cada una de estas actualizaciones, también puede seleccionar actualizaciones que no requieran reiniciarse.
   - Actualizaciones del OS
   - Actualizaciones críticas
   - Actualizaciones de los datos de configuración
   - Actualización del firmware
   - Actualizaciones no críticas

   > El administrador puede gestionar (instalar/ programar) las actualizaciones no críticas de MacOS activando la opción **Habilitar actualizaciones no críticas**. Esta opción está desactivada por defecto para los abonados existentes y la debe activar el administrador explícitamente después de la actualización, si es necesario.

   > En **Actualización de OS**, los Administradores pueden actualizar el dispositivo a una versión específica de macOS.

   > Todas las actualizaciones de macOS pueden configurarse con acciones como las siguientes:

        - Predeterminada
        - Solo notificar
        - Instalar más tarde
        - Instalar el reinicio forzado
        - Solo descarga
        - Instalar lo antes posible
    -

Valores posibles: bajo, alto

Predeterminado: bajo

Prioridad

    - Aplazamientos de usuarios máximos
      Posibles valores: entero
      Es compatible solo cuando se selecciona la opción Instalar más adelante.

7. Seleccione las siguientes opciones de hora a la que deben producirse las actualizaciones:
    - Hora de inicio
    - Hora de fin
    - Zona horaria
8. Haga clic en **Siguiente**.
9. Seleccione la opción **Habilitar esta configuración**.
10. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - Personalizada
11. Haga clic en **Hecho**.

Configurar actualizaciones de software para dispositivos Windows

Procedimiento

Para configurar su calendario de actualizaciones de la instalación de Windows:

1. Vaya a **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Haga clic en **Actualizaciones del software**.
4. Haga clic en **Windows** para ver la sección Ajustes de la configuración.
5. Introduzca las siguientes opciones dependiendo de la versión de sus dispositivos Windows.
6. Haga clic en **Siguiente**.
7. Seleccione la opción **Habilitar esta configuración**.
8. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos

- Ningún dispositivo (predeterminada)
- Personalizada

Haga clic en **Hecho**.

Actualizaciones del software para dispositivos Windows 10+

- Fuentes de la actualización - Seleccione una de las siguientes fuentes:
  - WSUS para la empresa
  - Microsoft Update y/o WSUS para la empresa

Fuente de actualización de controladores

- Mostrar fuente de actualización
- Otra fuente de actualización
- Fuente de actualización de la calidad
- URL para el servidor WSUS de la empresa
- Alternar servidor de actualización de Microsoft de Intranet
- Permitir actualizaciones de 'editores de confianza' - Limite las fuentes de las actualizaciones solamente a los editores de confianza.
- Estrategia de actualización automática - Seleccione una de las siguientes opciones del menú desplegable.
- Día programado de la instalación - Establezca la frecuencia de las actualizaciones.
- Hora programada de la instalación - Seleccione una hora a la que se instalarán las actualizaciones.
- Permitir que se descarguen automáticamente las actualizaciones mediante conexiones de uso medido - Activar o desactivar la opción.
- No permitir que las políticas de postergación de actualizaciones generen escaneos frente a Windows Update - Activar o desactivar la opción.
- Fecha límite de reinicio establecido - Seleccione el número de días para el reinicio de la fecha límite.
- Posponer fecha límite de reinicio establecido - Seleccione el número de días para posponer el reinicio de la fecha límite.
- Calendario de transiciones del reinicio establecido - Seleccione el número de días para el reinicio del calendario de transiciones.
- Actualizar/rellenar las URL de contenido vacías.
- Límite de descargas de la aplicación en operadores móviles - Seleccione una de las siguientes opciones:
  - No ignorar el límite de descargas MO para aplicaciones y sus actualizaciones
  - Ignorar el límite de descargas de MO (es decir, permitir la descarga ilimitada) para las aplicaciones y sus actualizaciones
- Límite de descargas de actualizaciones en operadores móviles - Seleccione una de las siguientes opciones:
  - No ignorar el límite de descargas MO para actualizaciones del OS
  - Ignorar el límite de descargas de MO (es decir, permitir la descarga ilimitada) para las actualizaciones del OS
- Gestionar versiones preliminares - Seleccione una de las siguientes opciones:
  - Desactivar versiones preliminares
  - Desactivar versiones preliminares una vez que se haga público el próximo lanzamiento
  - Activar versiones preliminares

- Reiniciar automáticamente el calendario de notificaciones de advertencias para las actualizaciones - Seleccione los minutos que se tardará en reiniciar automáticamente las notificaciones de advertencias.
- Reiniciar el recordatorio de advertencias - Seleccione las horas para establecer el reinicio del recordatorio de advertencias.
- Calendario de actualizaciones automáticas - Seleccione la frecuencia de las actualizaciones automáticas.
- Reiniciar automáticamente las notificaciones para las actualizaciones - Active el reinicio automático de las notificaciones para las actualizaciones.
- Versión del producto: introduzca la versión del producto que aparece en la página de versiones de Actualización de Windows (URL: aka.ms/WindowsTargetVersioninfo). Por ejemplo, "Windows 11" o "11" o "Windows 10".
- Versión de destino: introduzca la versión de destino en la página de versión de actualización de Windows.
- Inicio de horas activas: si activa esta opción, el PC no se reiniciará automáticamente tras las actualizaciones durante las horas activas. El PC intentará reiniciarse fuera de las horas activas.
- Fin de horas activas: si activa esta opción, el PC no se reiniciará automáticamente tras las actualizaciones durante las horas activas. Un PC intentará reiniciarse fuera de las horas activas.
- Rango máximo de horas activas: active esta opción para indicar el número máximo de horas desde la hora de inicio en que los usuarios pueden establecer sus horas activas.
- Sin notificaciones de actualización durante las horas activas: las opciones de notificación de actualización son las siguientes.
  - Notificaciones predeterminadas de actualización de Windows
  - Desactivar todas las notificaciones, menos las advertencias de reinicio
  - Desactivar todas las notificaciones, incluidas las advertencias de reinicio
- Desactivar actualizaciones de controladores: active esta opción para excluir los controladores con actualizaciones de calidad de Windows. Si desactiva o no configura esta opción, Windows Update incluirá actualizaciones con una clasificación de controladores.
- Plazo de actualizaciones de calidad: el número de días antes de que las actualizaciones de calidad se instalen automáticamente en los dispositivos es independiente de las horas activas.
- Periodo de gracia límite para actualizaciones de calidad: el número mínimo de días desde la instalación de la actualización hasta el reinicio automático para actualizaciones de calidad.
- Periodo de gracia límite para actualizaciones de funciones: número de días que transcurren hasta que las actualizaciones de funciones se implementan automáticamente en los dispositivos, independientemente de las horas activas.
- Periodo de gracia límite para actualizaciones de funciones: número mínimo de días que transcurren hasta que las actualizaciones de funciones se implementan automáticamente en los dispositivos, independientemente de las horas activas.
- No reiniciar automáticamente hasta el final del periodo de gracia: cuando se activa, los dispositivos no se reiniciarán automáticamente fuera de las horas activas hasta que el plazo y el periodo de gracia hayan pasado, incluso si una actualización está lista para reiniciarse. Cuando está desactivado, se puede intentar llevar a cabo un reinicio automático fuera de las horas activas si la actualización está disponible para el reinicio antes de la fecha límite.

Actualizaciones de software para dispositivos pre Windows 10.0.14393

Los siguientes ajustes no funcionarán si la opción Restricción de telemetría está desactivada en el dispositivo:

- Pausar cambios de versión/actualizaciones - Active esta opción para retrasar los cambios a una fecha posterior
- Aplazar actualizaciones durante - Elija esta opción para retrasar las actualizaciones hasta cuatro semanas
- Aplazar cambios de versión - Active esta opción para aplazar los cambios de versión

- Aplazar cambios de versión durante - Elija esta opción para retrasar hasta 8 meses

Actualizaciones de software para dispositivos Windows 10.0.14393+

- Sucursal desde la que se instalan las actualizaciones: permite al administrador de TI establecer la sucursal desde la que un dispositivo recibe las actualizaciones. La rama para instalar actualizaciones desde el campo contiene las opciones siguientes:
  - Windows Insider - Rápido
  - Windows Insider - Lento
  - Publicar versión de Windows Insider
  - Cana semestral (Dirigido)
  - Cana semestral
  - Vista previa de las actualizaciones de calidad
  - Canal Canary

Actualizaciones de características (actualizaciones): solo compatibles con Windows Professional, Windows Enterprise y Windows Education.

  - Pausar actualizaciones
  - Aplazar durante - Elija esta opción para retrasar hasta 180 días.

Actualizaciones de calidad (actualizaciones): solo compatibles con Windows Professional, Windows Enterprise y Windows Education.

  - Pausar actualizaciones
  - Aplazar durante - Elija esta opción para retrasar hasta 30 días.

Actualizaciones de software para dispositivos Windows 10.0.17083+

- Destacar actualizaciones:
  - Período de desinstalación de actualizaciones destacadas - Seleccione el número de días que se tardará en desinstalar una actualización destacada.

Actualizaciones de software para dispositivos Windows 10.0.17763+

- Desactivar el acceso a «Pausar actualizaciones» por los usuarios
- Desactivar el acceso a UXWU por los usuarios (escaneo, descarga e instalación de Windows Update)
- Actualizar nivel de notificación - Seleccione una de las siguientes opciones:
  - Usar las notificaciones predeterminadas de Windows Update
  - Desactivar todas las notificaciones, menos las advertencias de reinicio
  - Desactivar todas las notificaciones, incluidas las advertencias de reinicio
- Destacar actualizaciones:
  - Fecha límite anterior al reinicio automático para la instalación de actualizaciones - Seleccione el número de días para la fecha límite anterior al reinicio automático para la instalación de actualizaciones.
  - Fecha límite de reinicio establecido - Seleccione el número de días para la fecha límite del reinicio establecido.
  - Posponer fecha límite de reinicio establecido - Seleccione el número de días para posponer el reinicio de la fecha límite.

- Calendario de transiciones del reinicio establecido - Seleccione el número de días para el reinicio del calendario de transiciones.

Aplicación de actualizaciones de software mediante DDM

El administrador puede imponer la instalación de Actualizaciones de software en dispositivos iOS, macOS y iPadOS mediante DDM.

Compatible con:

- iOS 17+
- iPadOS 17+
- macOS 14+

Procedimiento

1. Cree una configuración **Aplicación de Cumplimiento de Actualizaciones de Software** desde la sección Configuraciones.
2. Realice una comprobación forzada para asegurarse de que la configuración de actualización de software forzada está instalada en el dispositivo.

Cuando abra el dispositivo, debería ver una notificación sobre las actualizaciones de software necesarias con detalles como el número de versión, la fecha límite, etc.

> Si no desea imponer la actualización del software, debe establecer la opción de distribución de la configuración en **Ninguno**.

Distribución de predicados para una configuración de aplicación de actualizaciones de software

1. Cree una configuración de forzar actualizaciones de Software.
2. Configure el interruptor de palanca “Activación con predicados” en ON y use el botón para incluir los predicados (según sea necesario).



Para editar o eliminar un predicado, vaya a **Administrador** > **Apple** > **Predicados**. En esta página encontrará la lista de predicados disponibles. Haga clic en **Editar** para realizar cualquier cambio en el predicado existente y guardarlo. Del mismo modo, para eliminar un predicado existente, selecciónelo y haga clic en **Eliminar**.

> No puede eliminar un predicado si está asociado a alguna configuración.

10.10.4.59. Configuración de los ajustes de actualización del software

Ivanti Neurons for MDM permite la creación de configuraciones de aplicación de actualizaciones de software y define el comportamiento de las actualizaciones para el usuario final en cuanto a cadencia y aplazamientos.

Disponible para:

- iOS 18.0 supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- macOS 15.0 supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Buscar y seleccionar la configuración de **Ajustes de actualización de Safari**.
3. Configure los ajustes de **Ajustes de actualización de Safari** según la tabla siguiente:

Ajuste	Descripción
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
iOS 18+ supervisado y **macOS15+** Inscripción Beta Inscripción al programa (opcional)	Seleccione una de las siguientes opciones: • **Permitido**: el usuario puede inscribirse en cualquier programa beta aplicable asociado con su cuenta registrada en Apple. • **Siempre encendido**: se utilizan los programas beta especificados por la organización, y el usuario no puede inscribirse en un programa beta utilizando su cuenta registrada en Apple. **Programa de ofertas**: Con el Programa de ofertas, puede hacer cumplir un programa requerido. Al aplicarlo, puede establecer las versiones requeridas para dispositivos iOS y macOS. **Requerir programa**: el dispositivo se inscribe automáticamente en este programa beta. • **Siempre apagado**: el dispositivo no puede inscribirse en ningún programa beta. Si ya está inscrito, el sistema elimina el dispositivo de cualquier programa beta.
iOS 18 supervisado y **macOS15 supervisado** Notificaciones	Seleccione las casillas **Notificaciones** y **Mostrar todas las notificaciones de aplicación de actualizaciones de software** para mostrar todas las notificaciones de aplicación de actualizaciones de software en el dispositivo del usuario. Si selecciona solo la casilla **Notificaciones,** el dispositivo mostrará una única notificación de aplicación una hora antes de la hora límite establecida para la aplicación. Si no selecciona ninguna de las casillas, el dispositivo mostrará las notificaciones generadas para presentar todas las notificaciones relacionadas con la aplicación de actualizaciones de software en el dispositivo del usuario.
Acciones automáticas Descargar	Seleccione una de las siguientes opciones: • **Permitido**: el usuario puede activar o desactivar las descargas automáticas. • **Siempre activo**: las descargas automáticas están siempre "Activas" para el usuario. • **Siempre inactivo**: las descargas automáticas están siempre "Inactivas" para el usuario.
Instalar actualizaciones de SO	Seleccione una de las siguientes opciones: • **Permitido**: el usuario puede activar o desactivar para instalar automáticamente las actualizaciones del SO. • **Siempre activado**: la instalación automática de actualizaciones del sistema operativo siempre está "activada" para el usuario.

Ajuste	Descripción
	• **Siempre desactivado**: la instalación automática de actualizaciones del sistema operativo siempre está "desactivada" para el usuario.
Mejoras de seguridad en segundo plano Mejoras de seguridad en segundo plano	Seleccione la casilla **Mejoras de seguridad en segundo plano** para controlar la instalación y la reversión de las actualizaciones. Seleccione las siguientes opciones: • **Activar**: si se selecciona, ofrece al usuario la instalación de **Mejoras de seguridad en segundo plano**. • **Habilitar reversión**: si se selecciona, ofrece al usuario la reversión de **Mejoras de seguridad en segundo plano**.
iOS 18+ supervisado Cadencia recomendada	Seleccione una de las opciones siguientes para mostrar las actualizaciones de software al usuario cuando haya más de una actualización disponible: • **Todas**: muestra todas las versiones de actualización del software. • **Más antigua**: muestra solo la versión de actualización de software más antigua (con el número más bajo). • **Más nueva**: muestra solo la versión de actualización de software más nueva (con el número más alto).
Aplazamientos Periodo combinado en días	Puede optar por posponer las actualizaciones de software para todos los dispositivos supervisados. No puede posponer las **Mejoras de seguridad en segundo plano**. Establezca los días para posponer una actualización del sistema principal o secundaria en el dispositivo. Una vez configurada, la actualización de software principal o secundario aparecerá transcurrido un número determinado de días desde su publicación. Puede establecer cualquier valor entre 1 y 90 días.
macOS 15+ supervisado Permitir actualizaciones estándar del SO del usuario	Seleccione la casilla de verificación **Permitir actualizaciones estándar del SO del usuario** para permitir que un usuario realice actualizaciones del SO. Seleccione la casilla de verificación **Permitir al usuario estándar realizar actualizaciones de software principales y secundarias** para permitir que un usuario estándar realice actualizaciones de software principales y secundarias. Solo los administradores pueden realizar actualizaciones de software principales y secundarias si no selecciona la casilla de verificación.
Aplazamientos	
Periodo de actualización	Establezca los días para posponer una actualización principal del software del sistema operativo en el dispositivo. Una vez configurada, la actualización de software principal aparecerá transcurrido un

Ajuste	Descripción
principal en días	número determinado de días desde su publicación. Puede establecer cualquier valor entre 1 y 90 días.
Periodo de actualización secundario en días	Establezca los días para posponer una actualización secundaria del software del sistema operativo en el dispositivo. Una vez configurada, la actualización de software principal aparecerá transcurrido un número determinado de días desde su publicación. Puede establecer cualquier valor entre 1 y 90 días.
Periodo de actualización del sistema en días	Establezca los días para posponer una actualización del sistema SO en el dispositivo. Una vez configurada, la actualización de software principal aparecerá transcurrido un número determinado de días desde su publicación. Puede establecer cualquier valor entre 1 y 90 días.
Acciones automáticas Instalar actualizaciones de seguridad	Seleccione una de las siguientes opciones: • **Permitido**: el usuario puede activar o desactivar la instalación de actualizaciones de seguridad. • **Siempre activado**: la instalación de actualizaciones de seguridad siempre está "activada" para el usuario. • **Siempre desactivado**: la instalación de actualizaciones de seguridad siempre está "desactivada" para el usuario.

4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Seleccione una de las opciones de distribución para establecer la configuración **Ajustes de actualización de software**. Para más información sobre la configuración de las opciones de distribución, consulte Trabajar con configuraciones.
6. Haga clic en **Hecho**.

10.10.4.60. Configuración de Preferencias de Seguridad

Los administradores pueden gestionar y controlar los cambios de los usuarios en la Configuración del firewall, los Mensajes de bloqueo y los Cambios de contraseña en el dispositivo con la Configuración de las preferencias de seguridad.

Aplicable a: macOS 10.10+

Procedure

1. Vaya a Configuraciones > +Añadir.
2. Escriba seguridad en el campo de búsqueda y, a continuación, haga clic en la configuración de las Preferencias de seguridad.
3. Introduzca un Nombre y Descripción de la configuración.
4. Seleccione las configuraciones requeridas:
    - Desactivar los cambios en la configuración del cortafuegos
    - Desactivar los cambios en el mensaje de bloqueo
    - Desactivar los cambios en la contraseña
5. Haga clic en Siguiente.
6. Seleccione la opción Habilitar esta configuración.
7. Seleccione una de las siguientes opciones de canal para aplicar la configuración:
    - Canal de dispositivos (el más común)
    - Canal del usuario (usuario actualmente registrado)
8. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - Personalizado.
9. Haga clic en Hecho.

10.10.4.61. Servidor de zona horaria

Aplicable a: macOS 10.12.4 y la versión más reciente compatible.

Crear la configuración del servidor de zona horaria para permitir que los dispositivos se conecten a los servidores con horas personalizadas.

Crear una configuración de servidor de zona horaria

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **hora** en el campo de búsqueda y, a continuación, haga clic en la configuración de **Servidor de zona horaria**.
4. Introduzca un nombre y describa la configuración.
5. Especifique el **Servidor NTP**.
6. Especifique la cadena de **Zona horaria** en formato de ID de zona horaria de Olson (por ejemplo, Pacific/Midway). Para obtener el formato de zona horaria de Olson, ejecute el comando `"/usr/sbin/systemsetup -listtimezones` " en el dispositivo macOS del administrador.
7. Haga clic en **Siguiente** para configurar los ajustes de distribución.
8. Haga clic en **Hecho**.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.4.62. Filtro de contenido web

Licencia: Silver

La configuración de un filtro de contenido web limita el acceso web de dispositivos iOS 7+, macOS 10.15+ y visionOS 1.1+.

Ajustes del filtro de contenido web

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Sitios web permitidos	**Contenido limitado a adultos:** Seleccione esta opción si desea bloquear el acceso a sitios web basado en filtros automáticos iOS. Estos filtros intentan, con un alto grado de precisión, bloquear sitios web con contenido inadecuado. **Solo sitios web específicos:** Seleccione esta opción si desea enumerar manualmente los sitios web accesibles. **Complemento (solo iOS 8 supervisado y macOS 10.15+):** seleccione esta opción para utilizar un complemento de terceros.
URL permitidas	Esta opción solamente está disponible si ha seleccionado Contenido limitado a adultos. Introduzca las URL permitidas. Cada URL debe comenzar con alguna de estas dos opciones: • http:// • https:// Si desea permitir tanto http:// como https:// para el mismo sitio, incluya dos URL separadas. Estarán accesibles todas las URL en las que los caracteres iniciales coincidan con la URL permitida. Por ejemplo: http://www.SitioDeMiEmpresa.com permite acceder a las siguientes páginas: • http://www.SitioDeMiEmpresa.com • http://www.SitioDeMiEmpresa.com/empleo Se puede acceder a estas URL incluso si los filtros automáticos de iOS las bloquean.
Use Rechazar las URL de la lista	Esta opción solamente está disponible si ha seleccionado Contenido limitado a adultos. Introduzca las URL de la lista de bloqueados. Cada URL debe comenzar con alguna de estas dos opciones: • http:// • https:// Si desea bloquear http:// como https:// para el mismo sitio, incluya dos URL separadas. Estarán bloqueadas todas las URL en las que los caracteres iniciales coincidan con la URL de la lista de bloqueados. Por ejemplo: http://www.SitioDeMiEmpresa.com bloquea el acceso a las siguientes páginas: • http://www.SitioDeMiEmpresa.com • http://www.SitioDeMiEmpresa.com/empleo Estas URL estarán bloqueadas incluso si los filtros automáticos de iOS las permiten.
Marcadores incluidos en la lista de permitidos	Esta opción solamente está disponible si ha seleccionado Solo sitios web específicos. También puede introducir la carpeta en la que debe añadirse el marcador en Safari. Ejemplo: /Ventas/Productos/ Si no existiera, el marcador se añadirá al directorio predeterminado de marcadores.
Nombre del filtro	Esta opción solamente está disponible si ha seleccionado Complemento. Introduzca el texto que se va a mostrar para identificar este filtro.

Ajuste	Qué hacer
Identificador	Esta opción solamente está disponible si ha seleccionado Complemento. Introduzca el Id. del paquete del complemento que proporciona el servicio de filtros.
Dirección del servicio	Esta opción solamente está disponible si ha seleccionado Complemento. Opcional: Introduzca cualquier dirección del servido necesaria para usar el complemento. Consulte la documentación del complemento para determinar si este valor es necesario.
Organización	Esta opción solamente está disponible si ha seleccionado Complemento. Opcional: Introduzca cualquier cadena de la organización necesaria para el complemento. Consulte la documentación del complemento para determinar si este valor es necesario.
Nombre de usuario	Esta opción solamente está disponible si ha seleccionado Complemento. Opcional: Introduzca cualquier nombre de usuario necesario para el servicio del complemento. Consulte la documentación del complemento para determinar si este valor es necesario.
Contraseña	Esta opción solamente está disponible si ha seleccionado Complemento. Opcional: Introduzca cualquier contraseña necesaria para el servicio del complemento. Consulte la documentación del complemento para determinar si este valor es necesario.
Certificado	Esta opción solamente está disponible si ha seleccionado Complemento. Opcional: Introduzca cualquier certificado necesario para que el servicio del complemento autentique al usuario. Consulte la documentación del complemento para determinar si este valor es necesario.
Tráfico Webkit del filtro	Esta opción solamente está disponible si ha seleccionado Complemento. Seleccione esta opción para incluir el tráfico Webkit en el filtro.
Tráfico del Socket del filtro	Esta opción solamente está disponible si ha seleccionado Complemento. Seleccione esta opción para incluir el tráfico del socket en el filtro.
Datos personalizados	Esta opción solamente está disponible si ha seleccionado Complemento. Opcional: Introduzca cualquier par clave/valor necesarios para el servicio del complemento. Consulte la documentación del complemento para determinar si este valor es necesario.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.4.63. Firewall de Windows

La configuración del Firewall de Windows permite configurar los ajustes del perfil del cortafuegos de Windows, así como el conjunto deseado de reglas personalizadas que se aplicarán en el dispositivo. Esta configuración se puede utilizar para administrar dispositivos que no sean del dominio y para reducir el riesgo de amenazas a la seguridad en la red en todos los sistemas que se están conectando a la red corporativa.

Configuración del Firewall de Windows

Procedimiento

1. Vaya a **Configuración > +Agregar**.
2. Seleccione la configuración de **Cortafuegos**.
3. Haga clic en el icono de **Windows**.
4. Introduzca un nombre para la configuración.
5. Introduzca una descripción para la configuración del cortafuegos.
6. En la sección Establecimiento de la configuración, especifique los demás ajustes según se describe en la siguiente tabla.

Ajuste	Qué hacer
Perfiles	
Activar	Deslice el control deslizante hacia Activado (ON) para activar el perfil.
Tipo	Muestra el tipo de perfil. Ejemplo: Dominio.
Acción de entrada predeterminada	Seleccione una opción para la acción predeterminada que debe realizarse cuando haya tráfico de entrada. **Permitir**: para permitir el tráfico. **Bloquear**: para bloquear el tráfico.
Acción de salida predeterminada	Seleccione la acción predeterminada que debe realizarse cuando haya tráfico de salida. **Permitir**: para permitir el tráfico. **Bloquear**: para bloquear el tráfico.

7. Para agregar Reglas, haga clic en **+Agregar** y configure los ajustes siguientes:

Ajuste	Qué hacer
Reglas	
ENCENDIDO	Deslice el control deslizante para activar el perfil.
Nombre de la regla	Introduzca un nombre que identifique esta regla.
Descripción	Introduzca una descripción que explique el objetivo de esta regla.
Dirección	Seleccione la dirección del tráfico hacia la cual debe aplicarse la regla: • **Entrada**: para el tráfico de entrada • **Salida**: para el tráfico de salida • **Ambas**: en ambas direcciones
Acción	Seleccione la acción que se realizará: • **Permitir**: para permitir el tráfico. • **Bloquear**: para bloquear el tráfico.
Perfil	Seleccione el(los) perfil(es) a los que debe aplicarse la regla: • **Todos** • **Dominio** • **Privado** • **Pública**
Aplicación	Escriba el nombre de familia del paquete (PFN, en inglés) o la ruta completa hacia el ejecutable de la aplicación.
Protocolo	Seleccione cualquiera de los siguientes protocolos a los que debe aplicarse la regla: • **TCP** • **UDP** • **ICMP**
Rangos de direcciones locales	Escriba los rangos de direcciones IPv4/IPv6 locales o máscaras de subred.
Rangos de puertos locales	Escriba una lista separada por comas de los puertos locales o los rangos de puertos. Ejemplos: 20,50,100-120.
Rangos de direcciones remotas	Escriba los rangos de direcciones IPv4/IPv6 remotas o máscaras de subred.
Rangos de puertos remotos	Escriba una lista separada por comas de los puertos locales o los rangos de puertos. Ejemplos: 20,50,100-120.
Tipos de interfaz	Seleccione cualquiera de las siguientes opciones de tipo de interfaz: • **Todos** • **Acceso remoto** • **Inalámbrico**

Ajuste	Qué hacer
	• **LAN** • **Banda ancha móvil** La opción predeterminada **Todos** se aplica si no se selecciona ninguna opción de tipo de interfaz.

8. Haga clic en **Siguiente**.
9. Seleccione una de las siguientes opciones de distribución:
   - Todos los dispositivos
   - Ningún dispositivo (predeterminada)
   - personalizada
10. Haga clic en **Hecho**.

10.10.4.64. Protección de la información de Windows

Licencia: Gold

Disponible para: Windows 10+

La Protección de la información de Windows (WIP) define los ajustes WIP para proteger los datos corporativos. Esta configuración se puede aplicar a los dispositivos inscritos bajo la administración. También se pueden visualizar los detalles WIP de un dispositivo configurado en la página de información general de dicho dispositivo.

Configurar la Protección de la información de Windows para Windows

Procedimiento

1. Vaya a **Configuración > +Agregar**.
2. Seleccione la configuración de **Windows Information Protection**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. En la sección Establecimiento de la configuración, especifique los demás ajustes según se describe en la siguiente tabla.
6. Haga clic en **Siguiente**.
7. Seleccione una distribución para esta configuración.

Categoría	Ajuste	Qué hacer
Información sobre la empresa	Nombre Descripción **Todas las versiones (Windows 10+)**	Introduzca un nombre que identifique a esta configuración. Introduzca una descripción que explique la finalidad de esta configuración.
	Nombre de dominio protegidos	Especifique la lista de identidades para las que se configuran las políticas de protección de datos. Los correos electrónicos y otros datos asociados a estas identidades se considerarán empresariales y estarán protegidos. • Esta es una lista de dominios separados por | en la que el primer dominio de la lista se considera la identidad principal para fines de IU de Windows. • Por ejemplo: "domain1.com|domain2.co.uk"
	Nombres de dominio de red	Especifique la lista de dominios que constituyen los límites de la empresa. Los datos de uno de estos dominios que se envíen a un dispositivo se considerarán datos de empresa y estarán protegidos. • Estas ubicaciones serán consideradas destinos seguros donde compartir los datos corporativos. • Sería una lista de los dominios separados por comas. • Por ejemplo: "mail.dominio3.com, dominio4.com"
	Recursos en la nube	Contiene una lista de dominios de recursos corporativos hospedados en la nube que deben protegerse. Las conexiones a estos recursos se consideran datos corporativos. Especifique uno o más nombres de dominio con direcciones proxy opcionales entre paréntesis. • Por ejemplo: «nombrededominio1.com, nombrededominio2 (10.0.0.1)». • Si se sincroniza un proxy con un recurso en la nube, el tráfico a dicho recurso en la nube se enrutará a través de la red corporativa por el servidor especificado del proxy (en el puerto 80). • Todas las direcciones proxy especificadas en este campo también deben introducirse en el siguiente campo Servidores de proxy internos.

Categoría	Ajuste	Qué hacer
	Rango de IP	Establece los rangos de IP corporativos que definen los equipos de la red corporativa. Los datos que provienen de dichos equipos serán considerados parte de la empresa y, por lo tanto, se protegerán. Estas ubicaciones serán consideradas destinos seguros donde compartir los datos corporativos. Será una lista de rangos IPv4 y IPv6 separados por comas. • Será una lista de rangos IPv4 y IPv6 separados por comas. • Seleccione la opción **Los rangos de IP son autoritativos** cuando el cliente deba aceptar la lista configurada y no intentar encontrar otras subredes por ensayo y error.
	Recursos neutros	Especifica la lista de nombres de dominios que se pueden utilizar para recursos profesionales y personales.
	Servidores proxy	Especifica la lista de servidores proxy separados por comas. Cualquier servidor de esta lista se considerará no corporativo. • Por ejemplo: "157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59". • Seleccione la opción cuando el cliente deba aceptar la lista configurada de proxies y no intentar detectar otros proxies profesionales.
	Servidores proxy internos	Especifica la lista de servidores proxy internos separados por comas. • Por ejemplo: "157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59". • El administrador ha configurado estos proxies para que se conecten a recursos específicos de Internet. Se consideran ubicaciones de la red corporativa. Los proxies solo se emplean a la hora de configurar la política «EnterpriseCloudResources» con el fin de forzar el tráfico a los recursos en la nube correspondientes a través de dichos proxies.
Protección de datos	**Todas las versiones (Windows 10+)**	
	Nivel de cumplimiento	Elija uno de los siguientes niveles de cumplimiento: • Desactivado: sin protección (los datos previamente cifrados serán descifrados). • Silencioso: se cifran los datos y se auditan las actividades en el dispositivo una vez que se han protegido los datos. Al usuario no se le solicita información sobre datos o información sobre aplicaciones negativos.

Categoría	Ajuste	Qué hacer
		• Anular: similar al modo Silencioso. Además, si se está utilizando incorrectamente alguna aplicación o dato, se solicita al usuario que continúe o cancelar la operación que está realizando en ese momento. • Bloquear: similar al modo Silencioso. Además, si se está utilizando incorrectamente alguna aplicación o dato, se bloquea la operación que está realizando actualmente el usuario y se le advierte con el motivo por el cual se ha bloqueado la operación. Excepto en el modo Desactivado, cualquier dato o aplicación que no tenga autorización para usar datos o recursos corporativos se registrará en el dispositivo. Estos datos se podrán eliminar del dispositivo utilizando otro proveedor de servicios de configuración (CSP, en inglés).
	Certificado de recuperación de datos	Especifique un certificado de recuperación que pueda utilizarse para la recuperación de datos de archivos cifrados. • Este será el mismo que el certificado del agente de recuperación de datos (DRA) para el sistema de cifrado de archivos (EFS). Sin embargo, este certificado se entrega a través de MDM en lugar de a través de la Política de grupos. También se pueden seleccionar una o más de las siguientes opciones: • Permitir descifrado del usuario • Revocar al anular la inscripción • Mostrar iconos EDP • Requerir protección cuando esté bloqueado (solo Windows 10 Mobile)
RMS	**Todas las versiones (Windows 10+)**	
	Permitie RMS de Azure	Especifique si desea permitir el cifrado de Azure Rights Management (Azure RMS) para la WIP.
	Id. de la plantilla de RMS	Especifique la TemplateID GUID a usar para el cifrado RMS. La plantilla de RMS permite a los administradores configurar los detalles sobre quién tiene acceso a los archivos protegidos por RMS y durante cuánto tiempo tiene acceso.
Control de aplicaciones	**Todas las versiones (Windows 10+)**	

Categoría	Ajuste	Qué hacer
	Especifique una colección de aplicaciones creadas en la página **Aplicaciones > Catálogo de aplicaciones** con un valor de WIP. Especifique las definiciones de reglas para las aplicaciones utilizando el siguiente conjunto de parámetros.	
	Tipo de aplicación	Seleccione uno de los siguientes tipos de aplicaciones: • Editor/PFN igual a: se aplica a dispositivos Windows 10+ que admiten PFN. • EXE/Win32 es igual a: se aplica solo a Windows Desktop.
	Identificador de la aplicación	Seleccione la aplicación de entre las opciones mostradas para añadirla al Identificador de aplicaciones. También puede hacer clic en **Buscar aplicaciones.**
	Descripción de la aplicación	Introduzca una descripción para la aplicación.

10.10.4.65. Restricciones de Windows

Las restricciones de Windows determinan qué funciones están disponibles en dispositivos Windows 10+.

Ajustes de las restricciones de Windows

Categoría	Ajuste	Qué hacer
	Nombre	Introduzca un nombre que identifique a esta configuración.
Funciones de los dispositivos	Descripción **Todas las versiones (Windows 10+)**	Introduzca una descripción que explique la finalidad de esta configuración.
	Desactivar la descarga Wi-Fi	Seleccione esta opción para impedir que el dispositivo acceda a redes compatibles que trasladan datos destinados a redes inalámbricas autorizadas.
	Desactivar uso compartido por Internet Desactivar localización Desactivar itinerancia de datos móviles	Seleccione esta opción para evitar que el dispositivo acceda a Internet a través de otro dispositivo inalámbrico. Seleccione esta opción para desactivar los servicios de localización. Seleccione esta opción para desactivar la itinerancia de datos cuando el dispositivo esté en modo móvil.
	Desactivar Bluetooth	Seleccione esta opción para evitar que el dispositivo pueda establecer conexiones Bluetooth.
	Desactivar VPN cuando se está en itinerancia o en una red móvil Desactivar la configuración manual de Wi-Fi Desactivar Wi-Fi	Seleccione esta opción para evitar que el dispositivo pueda establecer conexiones VPN cuando no esté conectado a una Wi-Fi. Seleccione esta opción para impedir que el usuario configure manualmente los ajustes Wi-Fi del dispositivo. Seleccione para permitir o denegar la conexión WiFi.
Telemetría - Permitir que el dispositivo envíe datos de diagnóstico y telemetría de uso.	**Solo Windows 10** Nivel de telemetría	Seleccione uno de los siguientes niveles de telemetría de informe de datos: • **Seguridad**: envía información acerca de la Experiencia del usuario conectado, Ajustes de componentes de telemetría, la Herramienta de eliminación de software maligno y Windows Defender. • **Básico**: envía información básica del dispositivo que incluye datos relacionados con la calidad, compatibilidad de aplicaciones, datos de uso de la aplicación y datos del nivel de seguridad.

Categoría	Ajuste	Qué hacer
		• **Mejorado**: envía más información que incluye el uso y rendimiento de Windows, Windows Server, System Center y aplicaciones. También incluye datos avanzados sobre fiabilidad y datos de los niveles básicos y de seguridad. • **Total (predeterminado)**: envía todos los datos para identificar y ayudar a solucionar los problemas, además de los datos de los niveles Seguridad, Básico y Mejorado.
Prevención de pérdidas de datos (DLP)	**Todas las versiones (Windows 10+)**	
	Desactivar cámara Desactivar acceso a la tarjeta de almacenamiento (SD) Desactivar la captura de pantalla (solo escritorio)	Seleccione esta opción para evitar que el usuario final pueda usar la aplicación de la cámara. Seleccione esta opción para evitar que el dispositivo pueda acceder a la tarjeta de almacenamiento. Seleccione esta opción para impedir las capturas de pantalla mediante aplicaciones de captura de pantalla del dispositivo.
	Desactivar el almacenamiento masivo USB (solo HoloLens)	Seleccione esta opción para evitar que HoloLens pueda acceder a la tarjeta de almacenamiento masivo.
Uso de datos	**Windows 10+** Coste de las conexiones 3G	Seleccione una de las siguientes opciones: • **Sin restricciones**: la conexión es ilimitada y no está restringida por cargos según el uso ni límites de capacidad. • **Fijo**: la conexión está restringida por los cargos según el uso y los límites de capacidad una vez superado cierto límite de datos. • **Variable**: la conexión se cobra por bytes.
Defender	Coste de las conexiones 4G **Windows 10+** Desactivar la funcionalidad «Realtime Monitoring» (monitorización en tiempo real) de Defender	Seleccione esta opción para desactivar la funcionalidad Realtime Monitoring de Windows Defender
DeviceGuard	**Windows 10+**	
	Desactivar seguridad basada en la virtualización (VBS, virtualization based security)	Seleccione esta opción para impedir que la seguridad basada en la virtualización admita los servicios de seguridad.

Categoría	Ajuste	Qué hacer
	Protección de credenciales con seguridad basada en la virtualización	Seleccione una de las siguientes opciones: • **Desactivada**: desactive la protección de credenciales con seguridad basada en la virtualización. • **Activada con bloqueo de la UEFI**: active la protección de credenciales con seguridad basada en la virtualización con bloqueo de la Interfaz de firmware ampliable unificada (UEFI, Unified Extensible Firmware Interface). • **Activada sin bloqueo**: active la protección de credenciales con seguridad basada en la virtualización sin bloqueo de la UEFI.
	Nivel de seguridad de la plataforma (requiere características de seguridad de la plataforma)	Seleccione una de las siguientes opciones: • **VBS con arranque seguro**: seleccione esta opción para activar la seguridad basada en la virtualización con arranque seguro. • **VBS con arranque seguro y acceso directo a la memoria**: seleccione esta opción para activar la seguridad basada en la virtualización con arranque seguro y acceso directo a la memoria (DMA, direct memory access).
Privacidad	**Windows 10+**	
	Desactivar la id. de publicidad	Seleccione esta opción para desactivar la Id. de publicidad
Windows y aplicación	Desactivar para publicar la fuente de actividades por aplicaciones/OS **Todas las versiones (Windows 10+)**	Seleccione esta opción para impedir que las aplicaciones o el OS publiquen en la actividad.
	Desactivar las cuentas de Microsoft para servicios ajenos al correo electrónico	Seleccione esta opción para evitar que el usuario final pueda usar las cuentas de Microsoft para autenticarse en servicios ajenos al correo electrónico.
	Desactivar las cuentas ajenas a Microsoft	Seleccione esta opción para evitar que el usuario final pueda configurar el correo electrónico usando cuentas ajenas a Microsoft.
	Desactivar el asistente personal de Cortana	Seleccione esta opción para evitar que el usuario final pueda acceder al asistente personal de Microsoft.
	Desactivar la búsqueda basada en la ubicación	Seleccione esta opción para evitar que las búsquedas puedan aprovechar la localización del dispositivo.
	Desactivar el desbloqueo del desarrollador	Seleccione esta opción para evitar que el usuario final pueda habilitar la carga en paralelo de aplicaciones. El modo

Categoría	Ajuste	Qué hacer
		predeterminado cuando un dispositivo está inscrito en MDM es «SideLoad activado».
	11+ Solo ediciones compatibles	
	Configuración del icono del chat de equipos en la barra de tareas	Seleccione una de las siguientes opciones: • **Mostrar:** El icono del chat aparece por defecto en la barra de tareas. Los usuarios pueden mostrarlo u ocultarlo en Configuración. • **Ocultar:** El icono del chat está oculto por defecto. Los usuarios pueden mostrarlo u ocultarlo en Configuración. • **Desactivado:** El icono del chat no se muestra y los usuarios no pueden mostrarlo u ocultarlo en Configuración. • **No configurado:** El icono del chat se comporta según los valores predeterminados de la edición de Windows. Los cambios no surten efecto hasta que se reinicie el dispositivo Windows.
	Solo versiones compatibles con Windows 10+	
	Desactivar la actualización automática de las aplicaciones de Microsoft Store Desactivar el lanzamiento de todas las aplicaciones de Microsoft Store que venían preinstaladas o se han descargado	Seleccione esta opción para impedir la actualización automática de aplicaciones de la Microsoft Store. Seleccione esta opción para impedir que el usuario final inicie todas las aplicaciones preinstaladas o descargadas de la Microsoft Store. Solo admite las ediciones de Windows Enterprise y Education.
	Permitir que las aplicaciones se ejecuten en un segundo plano	Seleccione una de las siguientes opciones: • **Usuario con el control**: permite al usuario controlar la ejecución de aplicaciones en segundo plano. • **Forzar permitir**: permite la ejecución de aplicaciones en segundo plano. • **Forzar rechazar**: impide la ejecución de aplicaciones en segundo plano.
Otras restricciones	**Todas las versiones (Windows 10+)** Desactive la capacidad de anular la inscripción a UEM y elimine la cuenta del lugar de trabajo.	Seleccione esta opción para evitar que el usuario final pueda anular la inscripción de UEM y eliminar la imagen de cuenta de la empresa.
	Impedir que el usuario configure el periodo de gracia de bloqueo del	Seleccione esta opción para evitar que el usuario establezca el

Categoría	Ajuste	Qué hacer
	dispositivo (solo HoloLens).	período de gracia de bloqueo del dispositivo.
	Solo versiones compatibles con Windows 10+	
	Impedir que el usuario pueda restablecer de fábrica el dispositivo mediante el panel de control y la combinación de teclas de hardware.	Seleccione esta opción para evitar que el usuario final establezca el período de gracia de bloqueo del dispositivo.
	Requerir que los usuarios se conecten a la red durante la configuración del dispositivo (requiere un perfil de Autopilot)	Seleccione esta opción para permitir que TenantLockdown bloquee todos los dispositivos Windows que estén inscritos utilizando la función Autopilot.
	Solo versiones compatibles con Windows 11 y posteriores ¿Deshabilitar al usuario para que no realice cambios en la eSIM?a través de la interfaz de usuario.	Seleccione esta opción para impedir que el usuario realice cambios en la eSIM.perfiles.

10.10.4.66. Restricciones de Windows Desktop

Disponible para: Windows 10 Desktops

Esta sección contiene los siguientes temas:

- Configuración de las restricciones para Windows Desktop
- Creación de una lista de permitidos para dispositivos de almacenamiento extraíbles

Los administradores puede controlar la información del sistema operativo en dispositivos administrados Windows 10 Desktop restringiendo el acceso del usuario a las siguientes áreas de un dispositivo:

- Panel de control
- Administrador de tareas
- Explorador de archivos
- Editor del registro

Las funciones anteriormente mencionadas permiten al usuario realizar una gran cantidad de cambios en su dispositivo. Mediante esta característica, los administradores pueden restringir el acceso a estos controles del nivel de sistema y, por ende, segurizar el acceso.

Esta característica requiere Bridge. Vaya a **Ivanti Bridge** para obtener más información.

Configuración de las restricciones para Windows Desktop

Procedimiento

1. Vaya a **Configuración > +Añadir**.
2. Seleccione la configuración **Restricciones de escritorio de Windows**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. En la sección Establecimiento de la configuración, especifique los demás ajustes según se describe en la siguiente tabla.

Ajuste	Qué hacer
Administrador de tareas	Seleccione la casilla **Denegar acceso** para el ajuste al que se debe negar el acceso.
Panel de control	
Editor del registro	
Explorador de archivos **Almacenamiento extraíble**	Seleccione la casilla **Restringir capacidades** para restringir las funciones del Explorador de archivos. Ejemplo: desinstalación de la opción «Conectar a unidad de red». Haga clic en el enlace proporcionado para ver la lista de funciones que están restringidas.
Acceder al modo para almacenamiento extraíble	• **Restringir acceso de lectura**: esta opción impide cualquier acceso y es la configuración más restrictiva. • **Restringir acceso de escritura**: esta opción permite un acceso limitado, pero impide la eliminación no autorizada de datos o la posibilidad de añadir virus, etc. al dispositivo.

6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones de distribución:

- Todos los dispositivos
- Ningún dispositivo (predeterminada)
- personalizada

8. Haga clic en **Hecho**.

> Para que la configuración entre totalmente en vigor, el dispositivo debe reiniciarse después de haber aplicado dicha configuración.

Creación de una lista de permitidos para dispositivos de almacenamiento extraíbles

Si desea crear una lista de permitidos de dispositivos de almacenamiento permitidos, complete primero los siguientes pasos.

- Conecte a un PC los dispositivos de almacenamiento USB que desea permitir.
- Abra el Administrador de dispositivos y haga clic en el controlador USB.
- Observe los ajustes de cada controlador para ver la información sobre el dispositivo.
- Almacene la información del dispositivo que usará para crear su lista de permitidos.

Para crear una lista de permitidos para dispositivos de almacenamiento extraíbles:

Procedimiento

1. En la página de configuración de **Restricciones de escritorio de Windows**, haga clic en **+Añadir**, en la sección **lista de permitidos de Almacenamiento extraíble**.
2. En la ventana **Agregar ID de hardware**, introduzca la ID de hardware para uno o más dispositivos que desee eliminar de la lista Permitir y bloquear como dispositivos de almacenamiento.

3. Haga clic en **Añadir las Id. de hardware**. La lista de las Id. de hardware que están en la lista de permitidos aparecerán en la sección **lista de permitidos de Almacenamiento extraíble autorizado**.

Para editar o eliminar la identificación de un equipo de la lista, seleccione la opción Editar o Eliminar en la columna **Acciones**.

Para que la configuración entre totalmente en vigor, el dispositivo debe reiniciarse después de haber aplicado dicha configuración.

10.10.4.67. Ajustes de escritorio para Windows 10

Los ajustes de escritorio para la configuración de Windows 10 le permiten personalizar los ajustes de escritorio e insertarlos en dispositivos Windows 10. Con esta configuración, puede definir los siguientes ajustes de escritorio:

- Imagen de fondo de escritorio
- Imagen de pantalla de bloqueo
- Cargar un salvapantallas personalizado
- Accesos directos al escritorio

> Esta característica requiere Bridge. Vaya a **Ivanti Bridge** para obtener más información.

Procedimiento

1. En **Configuración**, haga clic en **+Agregar**.
2. Seleccione configuración de **Ajustes de escritorio para Windows 10**. Aparecerá la página de **Ajustes de escritorio para Windows 10**.
3. En el campo **Nombre**, escriba un nombre adecuado para los ajustes.
4. (Opcional) Haga clic en el enlace **+Añadir descripción** para añadir una descripción de la configuración.
5. En la sección **Ajuste de la configuración**, configure los siguientes ajustes:

Ajuste	Descripción
Entrega de archivos	Seleccione una de las siguientes opciones de envío de archivos para los Ajustes del equipo de escritorio: • **Cargar archivo**: cargue los ajustes a Ivanti Neurons for MDM. • **Anular URL**: proporcionar las URL con los archivos de los ajustes para descargar.
Ajustes del fondo de pantalla de escritorio	Haga clic en **Elegir un archivo** para localizar y cargar una imagen de fondo de escritorio: los formatos compatibles son BMP, JPG, JPEG, PNG.
Ajustes del fondo de pantalla de la pantalla de bloqueo (El ajuste Lock screen Wallpaper **NO** es compatible con dispositivos Windows 10 Pro)	Haga clic en **Elegir archivo** para encontrar y cargar una imagen de fondo de pantalla. Los formatos de archivo admitidos son BMP, JPG, JPEG y PNG.
Ajustes del salvapantallas	Haga clic en **Elegir archivo** para encontrar y cargar una imagen de protector de pantalla. Cargue solo archivos .SCR compatibles. Seleccione **Protección con contraseña para el salvapantallas** si desea establecer una contraseña para desbloquear el modo de salvapantallas. Seleccione un periodo de **Tiempo de espera del salvapantallas** (en minutos).
Accesos directos al escritorio	Haga clic en **Añadir acceso directo** para configurar accesos directos que añadir a los escritorios del dispositivo. Aparecerá la ventana **Añadir acceso directo**. Rellene la tabla usando las siguientes opciones: • **Localización**: escriba la ubicación donde deberá aparecer el acceso directo en el dispositivo Windows. • **Ruta de destino**: escriba la ruta local, la ruta UNC o la letra de la unidad a la que llevará el atajo. La ruta de destino también puede ser una URL. • **Argumentos**: escriba cualquier argumento que se usará cuando se abra el archivo de destino. • **Directorio de trabajo**: escriba la ruta de la carpeta que contiene los archivos necesarios por el destino. • **Archivo del icono**: cargue archivos válidos .ico de Windows. Después de configurar las opciones, haga clic en **Añadir acceso directo**.

6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones de distribución:
   - Todos los dispositivos
   - Ningún dispositivo (predeterminada)
   - personalizada
8. Haga clic en **Hecho**.

10.10.4.68. Configuración predeterminada de Windows Hello para empresas

Esta configuración permite a los administradores configurar Windows Hello en los dispositivos. La configuración de Windows Hello requiere configurar un PIN para iniciar sesión en el dispositivo.

Aplicable a: Windows 10

ProcedureProcedimiento

1. Vaya a Configuraciones > +Añadir.
2. Escriba windows en el campo de búsqueda y, a continuación, haga clic en la configuración de Windows Hello para empresas.
3. Introduzca un Nombre y Descripción de la configuración.
4. Cambie el interruptor de Activar/Desactivar Windows Hello para empresas para Dispositivos con Windows 10 en On.

> El indicador está en On de manera predeterminada. Al desactivar Windows Hello para empresas no se eliminarán los PIN de los dispositivos.

5. Establezca la Complejidad del PIN.
6. Seleccione las configuraciones requeridas:
    - Requiere un módulo de plataforma de confianza (TPM) para Windows Hello para empresas
    - Utilizar los certificados de Windows Hello para empresas como certificados de tarjeta inteligente
    - Uso de gestos biométricos, como la cara y la huella dactilar, como alternativa al gesto del PIN para Windows Hello para empresas
    - Requiere la mejora de la antisuplantación para el reconocimiento de rasgos faciales en la autenticación facial de Windows Hello
    - Bloqueo dinámico
    - Permite a los usuarios iniciar sesión con una clave de seguridad FIDO2.
7. Haga clic en Siguiente.
8. Seleccione la opción Habilitar esta configuración.
9. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - Personalizado.
10. Haga clic en Hecho.

10.10.4.69. Configuración del administrador de IA de Windows

Ivanti Neurons for MDM permite a los administradores gestionar los ajustes y configuraciones de IS de Windows. La administración de IA de Windows potencia la creatividad y la productividad mediante un potente asistente de IA. Utilice la **configuración de** Windows AI Management para administrar las funciones de Windows AI en los dispositivos Windows inscritos. Esta configuración permite a los administradores controlar las capacidades de Microsoft Copilot, Windows Recall y Microsoft Paint AI a través de las políticas de Windows AI Configuration Service Provider (CSP).

Los administradores pueden deshabilitar las capacidades de IA seleccionadas, eliminar el acceso a las funciones de Copilot, controlar el comportamiento de recuperación de Windows y administrar las funciones de generación de imágenes impulsadas por IA en Microsoft Paint.

Aplicable para: Windows 10+

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Buscar y seleccionar la configuración de **Administración de IA de Windows**.
3. Introduzca un **Nombre** y **Descripción** de la configuración.
4. En la **sección** Configuración, seleccione una de las siguientes opciones: ### Ajustes de Copilot

Ajuste	Descripción
Deshabilitar copiloto de Windows	Evita que los usuarios accedan a Windows Copilot.
Desactivar clave de hardware de Copilot	Desactiva la clave de hardware Copilot dedicada en los dispositivos compatibles.
Eliminar la aplicación Microsoft Copilot	Elimina la aplicación Microsoft Copilot del dispositivo.

Recuperar configuración

Ajuste	Descripción
Desactivar análisis de datos de IA	Desactiva el análisis de datos basado en IA utilizado por Windows Recall.
Establecer el almacenamiento máximo para recuperar instantáneas (GB)	Especifica la cantidad máxima de almacenamiento que Windows Recall puede utilizar para almacenar instantáneas.

Pintar ajustes de IA

Ajuste	Descripción
Deshabilitar creador de imágenes	Desactiva la función Image Creator en Microsoft Paint.
Deshabilitar cocreador	Desactiva la función Cocreator en Microsoft Paint.
Deshabilitar llenado generativo	Desactiva la función Relleno generativo en Microsoft Paint.

Microsoft ha obsoleto la **política** TurnOffWindowsCopilot utilizada por esta configuración. Como resultado, esta configuración ya no afecta a la aplicación Copilot que reside en los dispositivos.

Si no selecciona la casilla de verificación **Desactivar Copilot de Windows**, la configuración anulará la selección de configuración anterior en el dispositivo para habilitar Administración de IA de Windows.

5. Haga clic en **Siguiente** para configurar los ajustes de distribución.
6. Seleccione una de las opciones de distribución para establecer la configuración de **Administración de IA de Windows**. Para más información sobre la configuración de las opciones de distribución, consulte **Trabajar con configuraciones**.
7. Haga clic en **Hecho**.

10.10.4.70. Play Integrity (antes SafetyNet Attestation)

Play Integrity (antes SafetyNet) ayuda a evaluar la seguridad y compatibilidad de los dispositivos Android que utilizan las API Play Integrity de Google. Cuando está configurado, le permite analizar los dispositivos después de un intervalo de tiempo regular para determinar si el dispositivo se ha manipulado o no.

> Play Integrity ahora es compatible con todas las versiones de Android.

Procedimiento

1. En la pestaña **Configuración**, haga clic en **+Añadir**.
2. Seleccione configuración de **Play Integrity**. Aparece la página **Configuración de Play Integrity**.
3. En el campo **Nombre**, introduzca un nombre adecuado para la configuración de Play Integrity.
4. Haga clic en el enlace +**Añadir descripción** para añadir una descripción de la configuración. Este campo es opcional.
5. En la sección **Ajuste de configuración**, introduzca un intervalo de tiempo mínimo (en horas) que se deberá aplicar para evaluar la seguridad y la compatibilidad de los dispositivos. El valor debe estar entre 1 y 24.
6. Haga clic en **Siguiente** y seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - personalizada

Haga clic en **Hecho**.

> Cuando los nonces Play Integrity y SafetyNet se envíen al dispositivo, el nonce Play Integrity tendrá prioridad sobre el nonce SafetyNet.

10.10.4.71. Código de acceso y pantalla de bloqueo avanzados de Android

Couldn't convert your doc.

10.10.4.72. Microsoft Defender for Endpoint

La configuración de Microsoft Defender for Endpoint (MDE), antes conocida como Windows Advanced Threat Protection, permite a los clientes incorporar y eliminar dispositivos al servicio MDE.

Procedimiento

1. Vaya a **Configuración > +Añadir**.
2. Seleccione la configuración de **Microsoft Defender for Endpoint**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. En la sección Establecimiento de la configuración, especifique los demás ajustes según se describe en la siguiente tabla.

Ajuste	Descripción
Blob de incorporación o de retirada	Pegue el blob de onboarding o offboarding del sitio del Centro de seguridad de Microsoft Defender for Endpoint.

6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones de distribución:

- Todos los dispositivos
- Ningún dispositivo (predeterminada)
- personalizada

8. Haga clic en **Hecho**.

10.10.4.73. Autenticación basada en certificado

Ivanti Neurons for MDMes compatible con la autenticación basada en certificados que permite a los administradores iniciar sesión mediante certificados digitales y un nombre de host (vanity) especificado por el abonado. Cuando se habilita y se configura, los administradores pueden iniciar sesión utilizando los certificados digitales en lugar de la autenticación básica (nombre de usuario y contraseña).

> Esta opción está desactivada de forma predeterminada. Los administradores deben contactar con la Asistencia técnica para activar esta función en su(s) abonado(s). Esta función solo está disponible en los entornos de clústeres NA3 y solo si está habilitada por la Asistencia técnica. Asegúrese de que su nombre de usuario y contraseña de superadministrador se hayan comprobado y estén preparados, ya que una vez que se habilite la autenticación basada en certificados, estas credenciales serán las únicas que puede utilizar para iniciar sesión hasta que haya configurado correctamente su dominio personalizado.

Procedimiento

1. En la pestaña de **Administración**, seleccione **Configuración de host de personalización**.
2. En la página de Configuración del host mnemónico, configure las siguientes opciones:
3. Haga clic en **Guardar**.
   Pueden pasar unos minutos hasta que el host mnemónico esté accesible.

Ajuste	Qué hacer
Crear dominio personalizado	Escriba el nombre del dominio mnemónico. Este es el nombre de dominio que puede alinearse más estrechamente con su identidad corporativa y al que puede acceder mediante certificados digitales.
Cargar los certificados de EC de emisión de confianza	Haga clic en **Seleccionar archivo** para seleccionar y cargar el certificado de EC que emite los certificados a sus administradores. Para activar la comprobación de la revocación del certificado, seleccione **Habilitar la configuración de validación del estado del certificado para este certificado** (opcional). Esta opción está activada de forma predeterminada. Deseleccione esta opción para desactivar la revocación del certificado. Haga clic en **Añadir más** para añadir más certificados. Asegúrese de que el formato del archivo sea .p7b, .pem, .der, .crt o .cer.
Asignación de atributos del certificado	La asignación de atributos de certificado configura la asignación de los elementos de identidad del certificado a los atributos de la cuenta del administrador. En el campo **A partir del certificado**, seleccione cualquiera de los siguientes elementos del certificado: • **Nombre principal de NT** • **Nombre RFC 822** En el campo **Para la variable**, seleccione cualquiera de los siguientes atributos de la cuenta del administrador: • **UPN del usuario** • **$UserEmailAddress** • **$EDIPI**

10.10.5. Configuraciones de recursos del usuario

Esta sección contiene los siguientes temas:

- Configuración de CalDAV
- Configuración de CardDAV
- Configuración de Google
- Configuración de correo electrónico
- Configuración de Exchange
- Configuración de fuente
- Configuración del calendario suscrito
- Crear una configuración de Web Clip
- Instalación de Office 365
- Ajustes de GPO de Windows
- Configuración de cifrado de BitLocker

10.10.5.1. Configuración de CalDAV

La configuración CalDAV define el acceso a un calendario web utilizando el estándar de Internet CalDAV.

Ajustes de CalDAV

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Nombre de host y puerto	Introduzca el nombre de host y puerto del servidor del calendario.
URL principal	Introduzca la URL para acceder a los servicios del calendario.
Usuario	Introduzca el nombre de usuario que usará para acceder.
Contraseña	Introduzca la contraseña que usará para acceder.
Usar SSL	Seleccione esta opción para usar solamente la capa de sockets seguros para las comunicaciones entre el dispositivo y el servidor.
VPN por aplicación	**Requisito previo**: configure Tunnel o cualquier configuración de VPN por aplicación, antes de configurar la VPN por aplicación en la configuración CalDAV. En el menú desplegable, seleccione la configuración VPN pre-configurada por aplicación. **Disponible para**: iOS 14+

Para obtener más información, consulte **Cómo crear una configuración**

10.10.5.2. Configuración de CardDAV

La configuración CardDAV define el acceso a una libreta de direcciones web utilizando el estándar de Internet CalDAV.

Ajustes de CardDAV

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Nombre de host y puerto	Introduzca el nombre de host y puerto del servidor de la libreta de direcciones.
URL principal	Introduzca la URL para acceder a los servicios de la libreta de direcciones.
Nombre de usuario	Introduzca el nombre de usuario que usará para acceder.
Contraseña	Introduzca la contraseña que usará para acceder.
Usar SSL VPN por aplicación	Seleccione esta opción para usar solamente la capa de sockets seguros para las comunicaciones entre el dispositivo y el servidor. **Requisito previo**: configure Tunnel o cualquier configuración de VPN por aplicación, antes de configurar la VPN por aplicación en la configuración CardDAV. En el menú desplegable, seleccione la configuración VPN pre-configurada por aplicación. **Disponible para**: iOS 14+
iOS 10+	
Reglas del servicio de comunicación	Elija una aplicación predeterminada para hacer llamadas de audio a contactos dentro del sistema CardDAV.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.5.3. Configuración de Google

La configuración de la cuenta de Google conecta dispositivos iOS 9.3.2 y visionOS 1.1 o Android 6.0+, o versiones más recientes compatibles, a cuentas de Google. Es necesario tener la versión corporativa de Android para las cuentas de Google. La configuración puede establecer varias direcciones de correo electrónico de Google y cualquier otro servicio de Google que el usuario habilite después de la autenticación.

Procedimiento

1. Vaya a **Configuración > +Añadir**.
2. Seleccione la configuración **Cuenta de Google**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. En la sección Establecimiento de la configuración, especifique los demás ajustes según se describe en la siguiente tabla:

Ajuste	Qué hacer
iOS 9.3.2+ , Android 6.0+	
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción de la cuenta	Introduzca el nombre en pantalla de la cuenta.
Nombre de la cuenta	Introduzca el nombre completo del usuario de la cuenta.
Dirección de correo electrónico	Introduzca la dirección de correo electrónico de Google de la cuenta.
VPN por aplicación	**Requisito previo**: configure Tunnel o cualquier configuración de VPN por aplicación, antes de configurar la VPN por aplicación en la configuración de la cuenta de Google. En el menú desplegable, seleccione la configuración VPN pre-configurada por aplicación. **Disponible para**: iOS 14+
iOS 10+	
Reglas del servicio de comunicación	Seleccione una aplicación predeterminada para realizar llamadas de audio a los contactos del sistema de Google seleccionando cualquiera de las siguientes opciones: • **Desde el App Catalog y las aplicaciones del sistema**: busque la aplicación escribiendo las primeras letras de su nombre. • **Introduzca la Id. del paquete (solo para aplicaciones de sistema de Apple)**: escriba la Id. del paquete de la aplicación del sistema. La Id. del paquete debe comenzar con «com.apple».

6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones de distribución:

- Todos los dispositivos
- Ningún dispositivo (predeterminada)

- personalizada

8. Haga clic en **Hecho**.

Cuando la configuración de una cuenta de Google se aplica al dispositivo, el cliente Go solicita al usuario que iniciar sesión en sesión en Google.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.5.4. Configuración de correo electrónico

Mediante la configuración de correo electrónico se configura el correo electrónico POP o IMAP en los dispositivos.

Ajustes del correo electrónico

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Descripción de la cuenta	Introduzca el texto que desea utilizar para identificar esta cuenta de correo electrónico.
Tipo de cuenta	Seleccione IMAP o POP. Si selecciona IMAP, también puede introducir el prefijo de la ruta. El proveedor de servicios de Internet (ISP) puede darle información sobre qué tipos de cuentas hay disponibles. Suele ser necesario un prefijo cuando todas las carpetas IMAP están dentro de la bandeja de entrada. Los ISP que requieren prefijos suelen proporcionar información sobre el prefijo específico que se debe configurar.
Nombre en pantalla del usuario	Introduzca el texto que desea utilizar para identificar al usuario de la cuenta de correo electrónico. Tenga en cuenta que el usuario también puede establecer este valor en el dispositivo.
Dirección de correo electrónico	Introduzca una variable para especificar la dirección de correo electrónico para la cuenta.
Permitir Mover	Seleccione esta opción si no desea impedir que el correo electrónico se mueva de esta cuenta.
Activar S/MIME	Seleccione para activar la compatibilidad con el cifrado S/MIME. A continuación, puede seleccionar la opción de firmar y cifrar certificados. Es obligatorio el almacenamiento en caché. Asegúrese de tener habilitado el almacenamiento en caché en la Entidad de Certificación que se está utilizando en la configuración del certificado de identidad. **iOS 10.3+:** Seleccione una de las siguientes opciones para los campos **Firma S/MIME** y **Cifrado S/MIME**: • Desactivado • Activado • Selección del usuario **iOS 12.0+:** • Permitir que el usuario pueda anular los ajustes de firma S/MIME • Permitir que el usuario seleccione la identidad de firma S/MIME • Permitir que el usuario pueda anular los ajustes de cifrado S/MIME • Permitir que el usuario seleccione la identidad de cifrado S/MIME **Habilite la firma y cifrado de S/MIME por mensaje** si fuera necesario.

Ajuste	Qué hacer
Permitir Mail Drop	Seleccione esta opción para permitir Mail Drop en esta cuenta. Mail Drop permite al usuario enviar correos electrónicos con grandes archivos adjuntos almacenando el adjunto en iCloud y poniendo un enlace a este dentro del mensaje de correo electrónico. Para tener más información sobre Mail Drop, vaya a: https://support.apple.com/
VPN por aplicación	Apple admite la posibilidad de asociar varios perfiles de VPN por aplicación en los dominios de Mail. Las configuraciones de correo electrónico IMAP y POP3 son ahora compatibles con la VPN por aplicación. **Requisito previo**: configure Tunnel o la configuración de VPN por aplicación antes de configurar la VPN por aplicación en la configuración del correo electrónico. En el menú desplegable, seleccione **Configuración de VPN por aplicaciónApp**.

Correo de entrada

Ajuste	Qué hacer
Servidor de correo y puerto	El proveedor de servicios de Internet (ISP) puede darle esta dirección.
Nombre de usuario	Introduzca el nombre de usuario para acceder al servidor de correo entrante. A menudo puede ser igual a la dirección de correo electrónico. Su ISP podrá proporcionarle el formato.
Tipo de autenticación	Seleccione el tipo de autenticación definido por el ISP.
Contraseña	Introduzca la contraseña para acceder al servidor de correo entrante.
Usar SSL	Seleccione esta opción para usar solamente la capa de sockets seguros para las comunicaciones entre el dispositivo y el servidor.

Correo de salida

Ajuste	Qué hacer
Servidor de correo y puerto	El proveedor de servicios de Internet (ISP) puede darle esta dirección.
Nombre de usuario	Introduzca el nombre de usuario para acceder al servidor de correo saliente. A menudo puede ser igual a la dirección de correo electrónico. Su ISP podrá proporcionarle el formato.
Tipo de autenticación	Seleccione el tipo de autenticación definido por el ISP.
Contraseña	Introduzca la contraseña para acceder al servidor de correo saliente.
La contraseña de salida es igual a la de entrada	Seleccione esta opción si la autenticación SMTP usa la misma contraseña que la POP/IMAP.
Usar Solo en correo	Seleccione si desea que esta configuración la utilice solamente el cliente de correo electrónico. Otras aplicaciones que envían correo electrónico, como las aplicaciones que envían contenido mediante el cliente de correo electrónico nativo, no pueden utilizar esta configuración.
Usar SSL	Seleccione esta opción para usar solamente la capa de sockets seguros para las comunicaciones entre el dispositivo y el servidor.

10.10.5.5. Configuración de Exchange

Una configuración de Exchange configura el correo electrónico basado en ActiveSync en dispositivos Android, iOS y visionOS y el correo electrónico basado en Exchange Web Services (EWS) para dispositivos macOS.

> Samsung ya no utiliza la configuración de Exchange en Android 9. Para dispositivos de Samsung en versiones de Android 9 y posteriores, la configuración de Exchange no es compatible en modo Administración de dispositivos.

Ajustes de Exchange

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Host de Exchange Permitir Mover	Si está usando **Sentry** para controlar el acceso al correo electrónico, introduzca el nombre de host del servidor Sentry. De lo contrario, introduzca la dirección del servidor ActiveSync.* **Para iOS y Android:** seleccione esta opción si no desea impedir que el correo electrónico se mueva de esta cuenta. **Para Windows 10:** No aplicable.
Activar S/MIME	Seleccione para activar la compatibilidad con el cifrado S/MIME. A continuación, puede seleccionar la opción de firmar y cifrar certificados. Es obligatorio el almacenamiento en caché. Asegúrese de tener habilitado el almacenamiento en caché en la Entidad de Certificación que se está utilizando en la configuración del certificado de identidad. **iOS 10.3+:** Seleccione una de las siguientes opciones para los campos **Firma S/MIME** y **Cifrado S/MIME**: • Desactivado • Activado • Selección del usuario **iOS 12.0+:** • Permitir que el usuario pueda anular los ajustes de firma S/MIME • Permitir que el usuario seleccione la identidad de firma S/MIME • Permitir que el usuario pueda anular los ajustes de cifrado S/MIME • Permitir que el usuario seleccione la identidad de cifrado S/MIME **Habilite la firma y cifrado de S/MIME por mensaje** si fuera necesario.
Sincronizar direcciones de correo electrónico recientes Usar Solo en correo	Seleccione sincronizar las direcciones de correo electrónico con las que ha contactado recientemente entre el dispositivo y el servidor. Seleccione si desea que esta configuración la utilice solamente el cliente de correo electrónico. Otras aplicaciones que envían correo electrónico, como las aplicaciones que envían contenido mediante el cliente de correo electrónico nativo, no pueden utilizar esta configuración.
Usar SSL	Seleccione esta opción para usar solamente la capa de sockets seguros para las comunicaciones entre el dispositivo y el servidor.
Activar OAuth para la carga útil de Exchange	iOS 12.0+ y macOS 10.14+: Seleccione esta opción para habilitar la autenticación mediante OAuth. Si esta opción está activada, estarán disponibles los siguientes ajustes adicionales para las aplicaciones de correo electrónico que admiten la autenticación mediante OAuth: • URL de inicio de sesión de OAuth • URL de la solicitud del Token de OAuth

Ajuste	Qué hacer
Dominio Usuario Contraseña de la cuenta Dirección de correo electrónico	Introduzca el dominio para esta cuenta de correo electrónico, a menos que desee que se le pida al usuario. Introduzca una variable que represente la dirección de correo electrónico para esta cuenta.* Introduzca la contraseña para esta cuenta, a menos que desee que se le pida al usuario. Introduzca una variable que represente la dirección de correo electrónico para esta cuenta.*
Días anteriores de correo para sincronizar	Seleccione el número de días de correo electrónico que desea sincronizar entre el dispositivo y el servidor.
VPN por aplicación **Android y Windows**	**Requisito previo**: configure Tunnel o la configuración de VPN por aplicación antes de configurar VPN por aplicación en la configuración de la sincronización activa de Exchange. En el menú desplegable, seleccione la configuración VPN pre-configurada por aplicación. **Disponible para**: iOS 14+
Sincronizar calendario	**Para Android y Windows 10:** seleccione esta opción para sincronizar los elementos del calendario entre el dispositivo y el servidor. **Para dispositivos Samsung:** este ajuste no se utiliza (está ACTIVADO de forma predeterminada). **Para la aplicación Email+ de Android:** este ajuste sí se utiliza.
Sincronizar contactos	**Para Android y Windows 10:** seleccione esta opción para sincronizar los contactos entre el dispositivo y el servidor. **Para dispositivos Samsung:** este ajuste no se utiliza (está ACTIVADO de forma predeterminada). **Para la aplicación Email+ de Android:** este ajuste sí se utiliza.
Sincronizar correo electrónico	**Para Android y Windows 10:** seleccione esta opción para sincronizar el correo electrónico entre el dispositivo y el servidor. **Para dispositivos Samsung:** este ajuste no se utiliza (está ACTIVADO de forma predeterminada). **Para la aplicación Email+ de Android:** este ajuste no se utiliza (está ACTIVADO de forma predeterminada).
Sincronizar tareas **iOS 13,0+** • Sincronizar calendario • Sincronizar contactos	**Para Android y Windows 10:** seleccione esta opción para sincronizar tareas entre el dispositivo y el servidor. **Para dispositivos Samsung:** este ajuste no se utiliza (está ACTIVADO de forma predeterminada). **Para la aplicación Email+ de Android:** no corresponde. Especifique la sincronización individual de elementos de Outlook Exchange como Calendario, Contactos, Correo, Notas y Recordatorios. Para cada elemento, seleccione o deseleccione las opciones **Activar** y **Permitir anulación de usuarios**.

Ajuste	Qué hacer
• Sincronizar el correo • Notas de sincronización • Recordatorios de sincronización	La sincronización debe estar activada para al menos uno de estos elementos. Si desactiva la sincronización para una de las opciones pero permite al usuario anularla, este aún podrá activarla.
Certificado de identidad	Seleccione un certificado de identidad de la lista si desea que el dispositivo se autentique ante el servidor utilizando un certificado. Los certificados solo aparecen en esta lista si ya están configurados mediante una configuración de certificados de identidad.
Android	
Usar solo autenticación basada en certificado	Use el certificado de identidad seleccionado como el único medio de autenticación del servidor Exchange.
Aceptar todos los certificados SSL	Seleccione para permitir a los usuarios del dispositivo establecer que los dispositivos Android acepten todos los certificados SSL. Este ajuste se aplica a Email+ de Android y a Samsung SAFE Email. • tenga precaución al habilitar este ajuste, ya que los usuarios del dispositivo podrían exponer el dispositivo sin darse cuenta a posibles ataques. • Es necesario habilitar esta opción si el certificado Sentry es un certificado autofirmado o con un certificado desconocido.
Prioridad de la aplicación Exchange	Seleccione el cliente de correo electrónico que se configurará de forma predeterminada en los dispositivos Android: Android Email+ y Samsung Email. La aplicación Email+ se añade en el App Catalog para todos los abonados que hayan habilitado la prioridad de la aplicación Exchange.
iOS 10+	
Reglas del servicio de comunicación	Elija una aplicación predeterminada para hacer llamadas de audio a contactos dentro del sistema CardDAV.
Windows 10+ solo	
Configurar Outlook	Seleccione esta opción para configurar Microsoft Outlook en un dispositivo. Esta opción solo es compatible si está activado Bridge.

*Escriba $ para ver una lista de **variables** compatibles, si las hubiera, para este campo.

10.10.5.6. Configuración de fuente

La configuración de la fuente le permite proporcionar archivos adicionales de fuente TrueType u OpenType para los dispositivos iOS 7. La siguiente lista enumera los ajustes de fuente:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Cargar fuentes	Arrastre el archivo de la fuente hasta el cuadro punteado o haga clic en **Elegir archivo** para seleccionarlo del sistema de archivos. Los archivos de fuente deben ser archivos .otf o .ttf.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.5.7. Configuración del calendario suscrito

Mediante la configuración del calendario suscrito se define el acceso a un calendario web público.

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
URL	Introduzca la URL para acceder al calendario.*
Usuario	Introduzca el nombre de usuario que usará para acceder.
Contraseña	Introduzca la contraseña que usará para acceder.
Usar SSL	Seleccione esta opción para usar solamente la capa de sockets seguros para las comunicaciones entre el dispositivo y el servidor.

> Escriba $ para ver una lista de **variables** compatibles, si las hubiera, para este campo.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.5.8. Crear una configuración de Web Clip

Un clip web es un acceso directo a un sitio web o página web desde un dispositivo iOS. Utilice la configuración del clip web para crear clips web estándar en los dispositivos. Puede agregar un icono de clip web a su dispositivo iOS que iniciará un sitio web específico. Web Clips le ayuda a encontrar rápidamente y utilizar marcadores en las pantallas de inicio de sus dispositivos. También puede controlar algunos parámetros de la experiencia visual de Mobile Safari en el sitio.

> La opción de delegación con distribución personalizada está disponible para esta configuración. Para obtener más información, consulte el tema *Distribuir la configuración* en **Trabajar con configuraciones**.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Haga clic en **Configuraciones**.
3. Haga clic en +**Añadir**.
4. Busque y seleccione la configuración de Web Clip.
5. Configure los ajustes en esta página. Consulte la tabla del tema **Ajustes de la configuración de Web Clip** para obtener ayuda acerca de los valores.
6. Haga clic en **Siguiente** para configurar los ajustes de distribución.
7. Seleccione **Personalizado** y a continuación **Dispositivos/ Grupos de dispositivos**.
8. Haga clic en **Hecho**.

Ajustes de configuración del clip web

La siguiente lista de tablas enumera los ajustes de configuración de Web clip:

Ajuste	Qué hacer
Nombre,	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Etiqueta	Introduzca el texto que desee mostrar bajo el acceso directo en la pantalla del dispositivo.*
URL	Introduzca la URL a la que accederá el webclip.*
Extraíble	Marque la casilla para permitir que el usuario del dispositivo elimine el clip web.
Icono	Arrastre el archivo del logotipo hasta el cuadro punteado o haga clic en **Elegir archivo** para seleccionarlo desde su sistema de archivos.
Icono precompuesto	Seleccione esta opción para eliminar los efectos especiales añadidos por versiones más recientes de Safari.
Pantalla completa	Seleccione esta opción para mostrar el clip web en modo pantalla completa en lugar de hacerlo como contenido en un explorador.
Ignorar el ámbito del manifiesto	Seleccione permitir la navegación hasta un sitio web externo sin mostrar el navegador de Safari. Esta opción no tiene efecto cuando no está seleccionada la opción Pantalla completa.
Identificador del grupo de aplicaciones de destino	El identificador del grupo de aplicaciones que especifica la aplicación que abre la URL. **Ejemplo**: com.google.chrome.ios

Escriba $ para ver una lista de **variables** compatibles, si las hubiera, para este campo.

Temas relacionados:

- **Inicio de sesión seguro multiusuario para iOS**
- **Cómo crear una configuración**

10.10.5.9. Instalación de Office 365

Licencia: Silver

Disponible para: Windows 10+

Configurar la instalación de Office 365

La instalación de Office 365 es un ajuste de configuración que puede aplicarse a los dispositivos seleccionados para instalar o desinstalar Office 365. Puede definir los ajustes de configuración en formato .xml usando la herramienta de implementación de Microsoft Office y cargando el archivo. Después de haber cargado el (los) archivo(s), puede insertar las opciones de configuración en los dispositivos seleccionados.

Procedimiento

1. En la pestaña **Configuración**, haga clic en **+Añadir**.
2. Seleccione **Instalación de Office 365**. Se mostrará la página de **Instalación de Office 365**.
3. En el campo **Nombre**, introduzca un nombre adecuado para la configuración.
4. Haga clic en el enlace +**Añadir descripción** para añadir una descripción de la configuración. Este campo es opcional.
5. En la sección **Ajuste de la configuración**, actualice los siguientes campos:

Nombre del campo	Descripción
Archivo de configuración para instalar Office 365	Haga clic en el botón **Elegir archivo** para buscar y seleccionar el archivo de configuración en formato .xml que incluya los ajustes definidos para la instalación de Office 365. Ejemplo: <Configuration> <Add OfficeClientEdition="64" Channel="Current"> <Product ID="O365ProPlusRetail"> <Language ID="en-us"/> </Product> </Add> </Configuration> Asegúrese de que el archivo de configuración está en formato .xml y de que se muestra la marca verde de verificación después de añadir el archivo con los ajustes de la configuración.
Archivo de configuración para desinstalar Office 365	Haga clic en el botón **Elegir archivo** para buscar y seleccionar el archivo de configuración en formato .xml que incluya los ajustes definidos para la desinstalación de Office 365. Ejemplo: <Configuration> <Remove All="TRUE"/><Display Level="None" AcceptEULA="TRUE" /> </Configuration> Asegúrese de que el archivo de configuración está en formato .xml y de que se muestra la marca verde de verificación después de añadir el archivo con los ajustes de la configuración.

6. Haga clic en **Siguiente**.
7. Seleccione cualquiera de las siguientes opciones para distribuir los ajustes al (a los) dispositivo(s).

Opción	Descripción
Habilitar esta configuración	Seleccionar la casilla permite esta configuración en los dispositivos seleccionados. Desmarcar la casilla elimina la configuración, si ya se ha aplicado en los dispositivos.
Todos los dispositivos	Distribuye los ajustes a todos los dispositivos.
Ningún dispositivo	Retiene los ajustes que se van a distribuir al (a los) dispositivo(s).
Personalizado	Distribuye los ajustes para un grupo definido de dispositivos. Seleccione la casilla junto al tipo de dispositivo al que desea distribuir los ajustes. Como alternativa, puede buscar los grupos de dispositivos escribiendo el nombre del grupo de dispositivos en el campo de búsqueda **Buscar grupos de dispositivos**. Si desea crear un nuevo grupo de dispositivos, haga clic en el enlace **Crear un nuevo grupo de dispositivos**, situado en la parte inferior de la página. Consulte **Grupos de dispositivos** para obtener más información. A medida que seleccione la categoría del dispositivo, podrá observar los detalles (**NOMBRE**, **N.º DE TELÉFONO** y **TIPO DE DISPOSITIVO**) de la lista de usuarios del dispositivo para la categoría del dispositivo seleccionada bajo la sección **Resumen de distribución**.

8. Haga clic en **Hecho** para insertar los ajustes en los dispositivos seleccionados.

10.10.5.10. Ajustes de GPO de Windows

Licencia: Bridge

Aplicable a: Windows Desktop

Configurar ajustes de los GPO de Windows

Los Objetos de directiva de grupos (GPO) son un conjunto de ajustes que definen los permisos que se pueden configurar en el (los) dispositivo(s). Es un requisito previo tener una configuración de Bridge para administrar los ajustes de los GPO. Consulte Ivanti Bridge para obtener más información.

Contacte con el administrador del sitio si los metadatos de los GPO no se han cargado a la base de datos. La configuración de los GPO se implementa en los dispositivos mediante las secuencia de comandos PowerShell a través de Bridge. Si utiliza los ajustes de los GPO podrá configurar e insertar ajustes específicos en el (los) dispositivo(s).

Procedimiento

1. En la pestaña **Configuración**, haga clic en **+Añadir**.
2. Seleccione la configuración **Ajustes de los GPO de Windows**. Se mostrará la página **Ajustes de los GPO de Windows**.
3. En el campo **Nombre**, introduzca un nombre adecuado para los ajustes de los GPO de Windows.
4. Haga clic en el enlace +**Añadir descripción** para añadir una descripción de la configuración. Este campo es opcional.
5. En la sección **Configuración**, haga clic en **+Agregar**. Se mostrará la ventana **Añadir Objetos de directiva de grupo (GPO) de Windows**.
6. Busque y seleccione un GPO haciendo clic en el componente pertinente del árbol de jerarquía de los GPO del panel izquierdo. El árbol de jerarquía de los GPO representa la ruta de los ajustes de políticas. Como alternativa, puede buscar unos ajustes de los GPO específicos escribiendo el nombre de los ajustes de los GPO en el campo de búsqueda.
   Después de seleccionar los ajustes de los GPO, puede ver los detalles de los ajustes seleccionados en el panel derecho.
7. En el campo **Estado del ajuste**, están disponibles las siguientes opciones de ajustes:

Opción	Descripción
No configurado	Elimina los ajustes de GPO existentes.
Activado	Activa los ajustes de GPO.
Desactivado	Desactiva los ajustes de GPO.

8. En el campo **Valor del ajuste**, escriba un nombre adecuado para asignar al GPO.
   Para agregar un valor de ajustes adicional, haga clic en el icono **+**. Es posible que algunos ajustes del GPO no requieran ningún valor adicional del ajuste. Puede que algunos requieran que se especifiquen datos adicionales en Valor del ajuste en forma de valor de texto. En estos ajustes, seleccione cualquier valor de los valores disponibles en la lista desplegable.

> Este campo solo se puede editar cuando la opción **Habilitado** está seleccionada en el **Estado de ajuste**.

9. Haga clic en **Guardar y cerrar** para guardar el GPO y cerrar la ventana. Si desea añadir otro GPO, haga clic en **Guardar y añadir otro** para guardar y mantener abierta la ventana de los GPO.
   El ajuste de GPO añadido se muestra en la sección **Ajustes de la configuración**.

> Puede editar o eliminar un ajuste de GPO haciendo clic en los iconos relevantes de la columna **Acciones**.

OpciónDescripciónHabilitar esta configuración Seleccionar la casilla permite esta configuración en los dispositivos seleccionados. Desmarcar la casilla elimina la configuración, si ya se ha aplicado en los dispositivos.**Todos los dispositivos**Distribuye los ajustes a todos los dispositivos.**Ningún dispositivo**Retiene los ajustes que se van a distribuir al (a los) dispositivo(s).**Personalizado**Distribuye los ajustes para un grupo definido de dispositivos. Seleccione la casilla junto al tipo de dispositivo al que desea distribuir los ajustes. Como alternativa, puede buscar los grupos de dispositivos escribiendo el nombre del grupo de dispositivos en el campo de búsqueda **Buscar grupos de dispositivos**. Si desea crear un nuevo grupo de dispositivos, haga clic en el enlace **Crear un nuevo grupo de dispositivos**, situado en la parte inferior de la página. Consulte Grupos de dispositivos para obtener más información.

A medida que seleccione la categoría del dispositivo, podrá observar los detalles (**nombre**, **n.º de teléfono** y **tipo de dispositivo**) de la lista de usuarios del dispositivo para la categoría del dispositivo seleccionada bajo la sección **Resumen de distribución**.

10. Haga clic en **Hecho** para insertar la configuración de los GPO a los dispositivos seleccionados.

10.10.5.11. Configuración de cifrado de BitLocker

Licencia: Bridge

Aplicable a: Windows Desktop

Esta sección contiene los siguientes temas:

- Configurar el cifrado de BitLocker
- Ver los ajustes de BitLocker

Configurar el cifrado de BitLocker

La funcionalidad Cifrado de BitLocker aplica el cifrado en unidades de disco duro y extraíbles de los dispositivos para proteger los datos. Es un requisito previo tener una configuración de Bridge para administrar el cifrado de BitLocker. Vaya a **Bridge** para obtener más detalles. La configuración del cifrado de BitLocker le ayuda a configurar los ajustes del cifrado en los dispositivos.

Procedimiento

1. En la pestaña **Configuración**, haga clic en **+Añadir**.
2. Seleccione la configuración **Cifrado de BitLocker**. Aparecerá la página **Cifrado de BitLocker**.
3. En el campo **Nombre**, introduzca un nombre adecuado para el cifrado de BitLocker.
4. Haga clic en el enlace **+Añadir descripción** para añadir una descripción de la configuración. Este campo es opcional.
5. En la sección Ajuste de la configuración, configure los siguientes ajustes:

Ajuste	Descripción
Método y tipo de cifrado	Seleccione el tipo de algoritmo de cifrado según el tamaño de la clave para el cifrado. Están disponibles las siguientes opciones: • **AES-CBL 128 bit** • **AES-CBL 256 bit**
Cifrar todas las unidades de hardware	Haga clic en el botón de cambio para activar el ajuste **ON** o **OFF** para cifrar todas las unidades de hardware. Si alguna unidad de hardware ya está cifrada en un dispositivo, no se aplicará la edición de esta configuración porque el proceso de cifrado no es reversible mediante la edición.
Seleccionar unidad(es)	Seleccione la(s) unidad(es) que deben cifrarse. P. ej.: **C:** Haga clic en **+ Añadir** para añadir más unidades. Este campo no se mostrará si ha activado el ajuste **Cifrar todas las unidades de hardware** .
Cifrado basado en el hardware para tipos de unidad	El Módulo de plataforma segura (TPM, Trusted Platform Module) es un chip de la placa base del ordenador que contribuye a un cifrado a prueba de manipulaciones. Si está usando cifrado de BitLocker o cifrado del dispositivo en un ordenador con TPM, parte de la clave quedará almacenada en el TPM. Puede elegir las siguientes opciones de ajustes de cifrado según el hardware de la lista desplegable: • **TPM obligatorio al inicio** • **PIN de inicio obligatorio con TPM** • **No usar TPM** La opción del TPM solo es aplicable a unidades de OS y para la versión 1.2 del TPM y superior. si aplica un ajuste de cifrado basado en el hardware a un dispositivo, ya no podrá volver a editar este ajuste en el dispositivo. Si el dispositivo ya está establecido con una configuración de BitLocker, no podrá insertar una segunda configuración de BitLocker con una opción de TPM diferente.
Seleccione las opciones de la casilla de configuración siguientes (opcional): • **Rechazar acceso de escritura a unidades fijas no protegidas por BitLocker** • **Rechazar acceso de escritura a unidades extraíbles no protegidas por BitLocker**	
Meduda del dispositivo precifrado	Seleccione cualquiera de las siguientes opciones para definir qué se hará con una unidad que no esté totalmente descifrada o que ya tiene un protector de claves.

Ajuste	Descripción
	• Detener cifrado: Detiene el cifrado si alguno de los controladores seleccionados ya está cifrado. • Descifre la unidad seleccionada que no tenga el almacén de contraseñas de recuperación en Ivanti Neurons for MDM: seleccione esta opción para aplicar solo a las unidades que no tengan una contraseña de recuperación en Ivanti Neurons for MDM.
Opciones de recuperación	Se hace uso de la opción de recuperación si un usuario olvida la contraseña. La puede recuperar desde la página de detalles del dispositivo. Puede personalizar las siguientes opciones de recuperación: • **Desactivar recuperación** • **Usar contraseña y almacenarla en AD** • **Usar contraseña y almacenarla en AD y en MobileIron Cloud**
Intervalo de reinicio	Una vez que la configuración se haya insertado en el dispositivo, pedirá que se reinicie. El cifrado comenzará después del reinicio. Para configurar el intervalo de reinicio, seleccione de la lista desplegable la duración del tiempo que debe tardar el dispositivo en reiniciarse. El intervalo de reinicio es de 1 minuto como mínimo y 120 minutos (2 horas) como máximo.
Mensaje de reinicio	Escriba el mensaje de reinicio que aparecerá en el dispositivo. si corresponde, la contraseña o el PIN de inicio también le aparecerá al usuario. El usuario puede crear una nota o escribirlos cuando se le solicite después del reinicio.

6. Haga clic en **Siguiente**.
7. Seleccione cualquiera de las siguientes opciones para distribuir los ajustes al (a los) dispositivo(s).

Ajuste	Descripción
Habilitar esta configuración	Seleccionar la casilla permite esta configuración en los dispositivos seleccionados. Desmarcar la casilla elimina la configuración, si ya se ha aplicado en los dispositivos.
Todos los dispositivos	Distribuye los ajustes a todos los dispositivos.
Ningún dispositivo	Retiene los ajustes que se van a distribuir al (a los) dispositivo(s).
Personalizado	Distribuye los ajustes para un grupo definido de dispositivos. Seleccione la casilla junto al tipo de dispositivo al que desea distribuir los ajustes. Como alternativa, puede buscar los grupos de dispositivos escribiendo el nombre del grupo de dispositivos en el campo de búsqueda **Buscar grupos de dispositivos**. Si desea crear un nuevo grupo de dispositivos, haga clic en el enlace **Crear un nuevo grupo de dispositivos**, situado en la parte inferior de la página. Consulte Grupos de dispositivos para obtener más información. A medida que seleccione la categoría del dispositivo, podrá observar los detalles (**NOMBRE**, **N.º DE TELÉFONO** y **TIPO DE DISPOSITIVO**) de la lista de usuarios del dispositivo para la categoría del dispositivo seleccionada bajo la sección **Resumen de distribución**.

8. Haga clic en **Hecho** para insertar los ajustes en los dispositivos seleccionados.

Ver los ajustes de BitLocker

Puede ver los ajustes de BitLocker establecidos para un dispositivo en la página Detalles del dispositivo (**Dispositivos > dispositivos > [Nombre del dispositivo]**) en la sección **Ajustes de BitLocker**. Los detalles están ocultos de forma predeterminada.

Puede ver los detalles siguientes haciendo clic en el icono (ojo) de vista que hay junto a cada campo:

Ajuste	Descripción
Contraseña de recuperación	Cuando esta opción está seleccionada, Windows genera la contraseña de recuperación y la devuelve a Ivanti Neurons for MDM después de insertar la configuración de BitLocker. Si el dispositivo pasa por el modo recuperación, se solicitará al usuario que escriba esta contraseña. Se debe usar la misma contraseña de recuperación si hay más de una unidad cifrada. la contraseña de recuperación solamente se publicará si está seleccionada la opción de recuperación **Usar contraseña y almacenarla en AD y en MobileIron Cloud**.
PIN	Muestra el PIN de seis dígitos para el inicio. El PIN solo aparece si ha seleccionado la opción **PIN de inicio obligatorio con TPM** en la configuración de BitLocker.
Contraseña de inicio	La contraseña de inicio establecida para el dispositivo. La contraseña de inicio solo aparece si ha seleccionado la opción **No usar TPM** en la configuración de BitLocker.
Versión de TPM	Muestra la versión de TPM configurado.

es posible que en algunos campos aparezca **N/A** en función de los ajustes configurados en la configuración de BitLocker.

- El estado del cifrado aparecerá en Estado del cifrado del dispositivo en la página Detalles del dispositivo.
- Se usará la misma contraseña o PIN de inicio para todas las unidades de un dispositivo en las que se vaya a aplicar BitLocker.
- Si está creando una configuración para cifrar la segunda unidad de un dispositivo que ya tiene una unidad cifrada y una contraseña de recuperación guardada, se sobreescribirá la contraseña más antigua. Por lo tanto, se recomienda que la opción Contraseña de recuperación solamente se utilice para una unidad del dispositivo.

10.10.6. Configuración de acceso a la red de la empresa

Esta sección contiene los siguientes temas:

- Configuración de AirPlay
- Configuración de AirPrint
- Configuración de VPN siempre activa
- Permisos predeterminados del tiempo de ejecución de las aplicaciones
- Educación
- Configuración de proxy global
- Configuración de LDAP
- Configuración del servidor de macOS
- Configuración del relé de red
- Tunnel
- Configurar AppTunnel
- Configuración de VPN por aplicación
- Configuración de inicio de sesión único
- Inicio de sesión seguro multiusuario para iOS
- Configuración de ajustes de la APN de Android
- Configuración de VPN
- VPN a petición
- Configuración de Wi-Fi

10.10.6.1. Configuración de AirPlay

Licencia: Silver

Mediante la configuración de AirPlay se configura el acceso a dispositivos alternativos para la visualización de contenido multimedia. La siguiente lista enumera los ajustes de Airplay:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Lista de permitidos	Introduzca la Id. del dispositivo de cada destino permitido de AirPlay. Si no incluye ninguna Id. en la lista, los destinos de AirPlay no estarán restringidos. **Disponible para**: iOS 7.0+ and macOS 10.10+ (Supervisado).
Ajustes del dispositivo	Introduzca el ID del dispositivo (macOS) o el nombre del dispositivo (iOS) y la contraseña de cada destino de AirPlay conocido.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.6.2. Configuración de AirPrint

Licencia: Silver

Mediante la configuración de AirPrint se configura la impresión inalámbrica. La siguiente lista enumera los ajustes de AirPrint:

Ajustes	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Ajustes de AirPrint	**Dirección IP:** Introduzca la dirección IP de la impresora AirPrint. **Ruta del recurso:** Introduzca la ruta del recurso asociada con la impresora AirPrint, que se corresponde con el parámetro rp del registro _ipps.tcp de Bonjour. Ejemplos: • printers/Canon_MG5300_series • printers/Xerox_Phaser_7600 • ipp/print • Epson_IPP_Printer. La ruta del recurso distingue entre mayúsculas y minúsculas. **Puerto:** introduzca el puerto de escucha del destino de AirPrint. Si no se especifica, AirPrint usará el puerto predeterminado. Para ver detalles sobre los puertos estándar de Apple, visite **https://support.apple.com/en-us/HT202944** **Forzar TLS**: le permite activar la conexión para segurizarla mediante Transport Layer Security(TLS). De forma predeterminada, esta opción está desactivada.

Después de la instalación de la configuración de **AirPrint** en el macOS, los detalles de la impresora se insertan a través de la configuración de **AirPrint** al dispositivo. Los usuarios pueden ver los detalles de la impresora autorrellenados haciendo clic en Preferencia del sistema > Impresoras y escáneres > +. En la pantalla **Añadir**, el usuario debe seleccionar **Predeterminado** y luego seleccionar el perfil de impresión concreto. Esto añade la impresora requerida a la página web **Impresoras y escáneres**.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.6.3. Configuración de VPN siempre activa

Licencia:

- **Gold para la Android Enterprise**
- **Silver para iOS**

La configuración de VPN siempre activa garantiza que los usuarios se conecten automáticamente a VPN (cuando esté disponible) sin necesidad de llevar a cabo ninguna acción. Esta función requiere Android 7.0 + o iOS 8 +, además de un proveedor de VPN que admita el protocolo IKEv2.

Ajustes de VPN siempre activa para Android

La configuración de VPN siempre activa se envía a los dispositivos de Android Enterprise con Android 7.0 +. En un dispositivo administrado con un Perfil de trabajo (Android 8.0+), la configuración de VPN se aplica al Perfil de trabajo.

> Cuando se despliega un dispositivo en modo **COSU** con **AMA** como tipo de Inscripción de dispositivos, y si se envía al dispositivo una aplicación con la configuración **Siempre activo**, también se enviará la configuración **Siempre activo**.

Para habilitar esta configuración, seleccione una aplicación del Catálogo de aplicaciones o introduzca un nombre de paquete.

Ajustes de VPN siempre activa para iOS

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Use la misma configuración en túnel para Móvil y Wi-Fi	Seleccione esta opción para definir un par de identificadores del servidor para las conexiones VPN, independientemente de si la conexión se ha establecido por móvil o como red Wi-Fi.
Servidor	Introduzca el nombre de host o dirección IP del servidor VPN.
Identificador local	El identificador del cliente IKEv2 en alguno de los siguientes formatos: • FQDN • UsuarioFQDN • Dirección • ASN1DN
Identificador remoto	Identificador remoto en uno de los siguientes formatos: • FQDN • UsuarioFQDN • Dirección • ASN1DN
Activar EAP	Seleccione esta opción para habilitar la autenticación ampliada.
Autenticación del equipo	Solo disponible si «Habilitar EAP» no está seleccionado. Seleccione una de las siguientes opciones: • Certificado • Secreto compartido
Autenticación EAP	Solo disponible si «Habilitar EAP» está seleccionado. Seleccione una de las siguientes opciones: • Certificado • Nombre de usuario/contraseña
Secreto compartido	Solo disponible si se ha seleccionado Secreto compartido para la Autenticación del equipo. Introduzca el secreto compartido para la conexión.
Credencial	Solo disponible si se ha seleccionado Certificado para la Autenticación del equipo. Seleccione el certificado que desea utilizar. Este certificado se enviará para autenticación del cliente IKE. Si se usa la autenticación ampliada, este certificado se puede usar también para EAP-TLS.
Cuenta	Solo disponible si se ha seleccionado «Nombre de usuario/contraseña» para la Autenticación EAP. Introduzca la Id. de cuenta para el servidor VPN.
Contraseña	Solo disponible si se ha seleccionado «Nombre de usuario/contraseña» para la Autenticación EAP. Introduzca la contraseña para el servidor VPN.

Ajuste	Qué hacer
Intervalo de detección de pares no funcionales	Seleccione una de las siguientes opciones: • Ninguno (desactivar) • Bajo (se envía un keepalive 1 vez por hora) • Medio (se envía un keepalive cada 30 minutos) • Alto (se envía un keepalive cada 10 minutos)
Algoritmo de cifrado	Seleccione una de las siguientes opciones: • DES • 3DES • AES-128 • AES-256 • AES-128-GCM • AES-256-GCM • ChaCha20-Poly1305
Algoritmo de integridad	Seleccione una de las siguientes opciones: • SHA1-96 • SHA1-160 • SHA2-256 • SHA2-384 • SHA2-512
Grupo Diffie Hellman	Seleccione el grupo de intercambio de claves D-H.
Vigencia en minutos	Introduzca la vigencia SA (intervalo de reintroducción de clave) en minutos. Los valores válidos van del 10 al 1440.
Correo de voz	Seleccione Permitir tráfico a través de túnel para que el correo de voz esté exento de VPN siempre activa. Seleccione «Disminuir tráfico» para que no sea una excepción.
Airprint	Seleccione Permitir tráfico a través de túnel para que el tráfico de Airprint esté exento de VPN siempre activa. Seleccione «Disminuir tráfico» para que no sea una excepción.
Servicios móviles	Seleccione Permitir tráfico a través de túnel para que el tráfico de los servicios móviles esté exento de VPN siempre activa. Seleccione «Disminuir tráfico» para que no sea una excepción.
Permitir el tráfico de la hoja web cautiva fuera del túnel de la VPN	Seleccione esta opción para permitir el tráfico de la hoja web cautiva fuera del túnel de la VPN.
Permitir el tráfico de todas las aplicaciones de la red cautiva fuera del túnel de la VPN	Seleccione esta opción para permitir el trádico de todas las aplicaciones de la red cautiva fuera del túnel de la VPN para realizar la gestión de redes cautivas.

Ajuste	Qué hacer
Identificadores del paquete de aplicaciones de red cautiva	Enumere los Id. del paquete para aplicaciones de red cautiva cuyo tráfico se permitirá fuera del túnel de VPN para realizar la gestión de redes cautivas. Las aplicaciones de redes cautivas pueden requerir permisos adicionales para operar en un entorno cautivo.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.6.4. Permisos predeterminados del tiempo de ejecución de las aplicaciones

Aplicable a: las aplicaciones creadas para Android API 23+ y con Android 6.0+ en dispositivos con Android Enterprise.

Los administradores pueden establecer la configuración de los permisos del tiempo de ejecución para las aplicaciones instaladas en dispositivos con Android Enterprise. Las aplicaciones creadas para API 23 (o posterior) y con Android 6.0 o posterior pueden solicitar a los usuarios permisos en el tiempo de ejecución. La configuración de los Permisos predeterminados del tiempo de ejecución de las aplicaciones establece el valor predeterminado para los permisos del tiempo de ejecución de estas aplicaciones. Ivanti Neurons for MDM crea esta configuración por defecto. Puede editar la configuración predeterminada del sistema o crear una nueva configuración de acuerdo con sus requisitos.

Los permisos específicos para cada aplicación prevalecen sobre la configuración general de permisos para aplicaciones. Las aplicaciones internas están sujetas a los permisos globales. No está permitido definir los permisos por aplicación para aplicaciones internas.

Definir los permisos globales de tiempo de ejecución

Los administradores pueden editar los permisos predeterminados del tiempo de ejecución de aplicaciones y la distribución de esta configuración del siguiente modo:

ProcedureProcedimiento

1. Vaya a **Configuraciones**.
2. Lleve a cabo una de las siguientes acciones:
    - Para editar la configuración predeterminada del sistema, haga clic en **Permisos predeterminados del tiempo de ejecución de las aplicaciones**y, a continuación, en **Editar**.
    - Para añadir una nueva configuración, haga clic en **Añadir > Permisos predeterminados del tiempo de ejecución de las aplicaciones**.

Introduzca un nombre para la configuración.

4. Introduzca una descripción.
5. En la sección Ajustes de la configuración, establezca uno de los siguientes permisos predeterminados del tiempo de ejecución:
    - Solicitud al usuario (opción predeterminada)
    - Concesión automática
    - Denegación automática (usar con precaución)

Haga clic en **Siguiente**.

7. Seleccione la opción **Habilitar esta configuración**.

> Si deselecciona esta opción, la configuración no se aplicará a ningún dispositivo. Si se aplicó previamente a algún dispositivo, se eliminará.

8. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos

- Ningún dispositivo (predeterminada)
- Personalizada

Haga clic en **Hecho**.

Definir permisos de tiempo de ejecución específicos para cada aplicación

Los administradores pueden definir los permisos de tiempo de ejecución predeterminados para cada aplicación individual del siguiente modo:

Procedimiento

1. Vaya a **Aplicaciones**.
2. Haga clic en el nombre de la aplicación.
3. Haga clic en **Configuraciones de aplicaciones > Android Enterprise**.
4. Haga clic en **Añadir** o en el nombre de la configuración para editar una configuración existente.
5. Defina las opciones de configuración como el nombre, la descripción y las restricciones.
6. En la sección Permisos de tiempo de ejecución, haga clic en **Administrar permisos**.
7. Seleccione los permisos de la ventana que aparece y haga clic en **Seleccionar**.
   Solo se incluyen para seleccionar los permisos peligrosos aplicables a la aplicación específica. La lista completa de los permisos peligrosos (como leer sus contactos, encontrar cuentas en el dispositivo, escribir registros de llamadas, etc.) están enumerados en https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups.
   - Los permisos se aplican solamente cuando la aplicación los solicita.
   - Los permisos no se aplican si los usuarios los han aceptado o denegado previamente.

En la sección Permisos de tiempo de ejecución, seleccione uno de los siguientes permisos predeterminados del tiempo de ejecución:

- Predeterminado/global (opción predeterminada)
- Concesión automática
- Denegación automática (usar con precaución)

En la sección Distribuir la configuración de esta aplicación, seleccione una de las siguientes opciones de distribución:

- A todas las personas con la aplicación
- A nadie
- Personalizada

Haga clic en **Guardar**.

10.10.6.5. Educación

Licencia: Gold

Aplicable a: iOS 9.3+ supervisado

Configura la carga útil de Apple Education y la aplicación Classroom para Líderes y Miembros. La siguiente lista enumera los ajustes de Education:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Tipo de configuración	Seleccione uno de los siguientes tipos: • Líder • Miembro
Activar esta configuración	• Seleccione esta opción para aplicar esta configuración a los dispositivos seleccionados. • Deseleccione esta opción para eliminar esta configuración de todos los dispositivos donde se aplicó previamente.
Distribuir	Seleccione una de las siguientes opciones de distribución: • Todos los dispositivos • No hay dispositivos • Personalizada

Para obtener más información, consulte **Cómo crear una configuración**

10.10.6.6. Configuración de proxy global

Licencia: Silver

Mediante la configuración de proxy global se ajustan los dispositivos para que redireccionen el tráfico HTTP a un servidor proxy. La siguiente lista enumera los ajustes de proxy global:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Tipo	Seleccione **Manual** o **Automática**. Si selecciona **Manual**, necesitará el nombre de host y el puerto del servidor proxy y, opcionalmente, el nombre de usuario y la contraseña para el servidor proxy. Si selecciona **Automático**, puede introducir una URL de configuración automática de proxy (PAC).
Nombre de host y puerto	Si ha seleccionado **Manual**, introduzca el nombre de host y número de puerto para el servidor proxy.
Usuario	(Opcional) Nombre de usuario para acceder al servidor proxy.*
Contraseña	(Opcional) Contraseña para acceder al servidor proxy.
URL de la PAC	(Opcional) Si ha seleccionado **Automática**, puede introducir la URL del archivo PAC que define la configuración del proxy. Si deja en blanco este ajuste, el dispositivo utiliza el protocolo de autodescrubrimiento del proxy web (WPAD) para descubrir proxies.
Permitir la conexión directa si no se puede acceder a la PAC	(iOS 7 y posterior) Seleccione para permitir una conexión directa si el dispositivo no puede acceder al archivo PAC por cualquier motivo.
Permitir la omisión del proxy para acceder a redes cautivas	(iOS 7 y posterior) Seleccione para permitir la omisión del proxy para visualizar la página de inicio de sesión para una red cautiva.

Escriba $ para ver una lista de **variables** compatibles, si las hubiera, para este campo.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.6.7. Configuración de proxy global (Android)

> Solo se aplica a dispositivos Android en los modos Propietario del dispositivo y AOSP.

Mediante la configuración de proxy global se ajustan los dispositivos para que redireccionen el tráfico HTTP a un servidor proxy.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Haga clic en **Configuraciones**.
3. Haga clic en +**Añadir**.
4. Escriba **Global** en el campo de búsqueda y, a continuación, haga clic en Proxy **global**:
   Aparece la página Detalles de configuración Proxy global.
5. En el campo **Nombre**, introduzca un nombre para la configuración.
6. Opcionalmente, puede agregar alguna descripción sobre la configuración.
7. En la lista de la **plataforma**, seleccione **Android**. Aparece la sección **Establecimiento de la configuración**.
8. En Tipo, seleccione **Manual** o **Automático**.
   - **Manual**
     - Introduzca el nombre del **host** (¿Nombre de dominio/IP?dirección)?y **detalles del** puerto.
     - En **Añadir exclusiones**, puede añadir varios nombres de host (nombres de dominio o comodines) para incluirlos en la lista de exclusiones.
   - **Automático**
     - ¿Ingresar el PAC?URL.
9. Haga clic en **Siguiente** para configurar los ajustes de distribución y, a continuación, haga clic en **Hecho**.

10.10.6.8. Configuración de LDAP

Mediante la configuración LDAP se configura el acceso a un directorio corporativo. La siguiente lista enumera los ajustes de LDAP:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Nombre de host	Introduzca el nombre del host para el servidor de LDAP.*
Usuario	Introduzca el nombre de usuario para acceder a la cuenta LDAP.*
Contraseña	Introduzca la contraseña acceder a la cuenta LDAP.
Usar SSL	Seleccione esta opción si desea usar SSL para la conexión con el servidor LDAP.
Buscar ajustes	Introduzca al menos una entrada para la cuenta. Cada entrada representa un nodo del árbol LDAP desde donde empezar a buscar. Haga clic en el botón + para añadir una nueva entrada y, a continuación, edítela. Cada entrada está formada por los siguientes valores: Descripción: explica la finalidad del ajuste de búsqueda. Ámbito: seleccione Base**, Subárbol** o **Un nivel** para indicar el ámbito de la búsqueda. **Base** indica el nivel del nodo, **Subárbol** indica el nodo y todos sus elementos secundarios, **Un nivel** indica el nodo y un nivel de elementos secundarios. Base de búsqueda: la ruta conceptual hasta la nota especificada (por ejemplo: ou=people, o=mycorp).
VPN por aplicación	**Requisito previo**: configure Tunnel o cualquier configuración de VPN por aplicación, antes de configurar la VPN por aplicación en la configuración LDAP. En el menú desplegable, seleccione la configuración VPN pre-configurada por aplicación. **Disponible para**: iOS 14+
iOS 10+ Reglas del servicio de comunicación	Elija una aplicación predeterminada para hacer llamadas de audio a contactos dentro del sistema LDAP.

Escriba $ para ver una lista de **variables** compatibles, si las hubiera, para este campo.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.6.9. Configuración del servidor de macOS

La configuración del servidor de macOS define una cuenta del servidor macOS con los tipos de cuentas configuradas y los ajustes. Esta configuración permite al usuario activar el uso compartido de archivos en el servidor.

Aplicable a: iOS 10+

Configuración el servidor de macOS

Procedimiento

1. Vaya a **Configuraciones > +Añadir**.
2. Seleccione la configuración del **Servidor de macOS** para visualizar la página **Crear configuración del servidor de macOS**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. Introduzca el **Nombre de host** para especificar la dirección de servidor.
6. Introduzca el **Nombre de usuario** para especificar el nombre del inicio de sesión del usuario.
7. (Opcional) Introduzca una **Contraseña** para el usuario.
8. (Opcional) Introduzca una **Descripción** para el usuario.
9. (Opcional) En Cuentas configuradas, introduzca el número de **Puerto** que se utilizará cuando se contacte con el servidor para la cuenta del diccionario de documentos. Si no se especifica ningún número de puerto, se utilizará el número de puerto predeterminado.
10. Haga clic en **Siguiente**.
11. Seleccione una distribución para esta configuración.

10.10.6.10. Tunnel

Ivanti Tunnel permite la función VPN en dispositivos iOS, Android y Windows. Ivanti Tunnel interactúa con la plataforma Unified Endpoint Management (UEM), Standalone Sentry y Access para proteger el acceso a los recursos empresariales desde fuera de la red de la empresa. El recurso empresarial puede estar en las instalaciones o en la nube. Las plataformas UEM son: Ivanti EPMM e Ivanti Neurons for MDM.

> La configuración por aplicación está obsoleta para los dispositivos Android Enterprise. Es necesario utilizar la configuración gestionada para Ivanti Tunnel del Catálogo de aplicaciones.

Acerca de la configuración del Ivanti Tunnel

Las configuraciones para Ivanti Tunnel se crean en una plataforma de Unified Endpoint Management (UEM). Ivanti Tunnel recibe la configuración del cliente UEM. El cliente para Ivanti EPMM es Mobile@Work, y el cliente para Ivanti Neurons por MDM es Go.

Documentación más reciente

Para las últimas instrucciones de Tunnel, visite la documentación del producto:

- Tunnel para Android, consulte la **Guía de Ivanti Tunnel for Android**
- Tunnel para iOS, consulte la **Guía de Ivanti Tunnel for iOS**
- Tunnel para macOS, consulte la **Guía de Ivanti Tunnel for macOS**
- Túnel de Windows, ver la **Guía de Windows para Ivanti Tunnel**

> El túnel Ivanti para Windows está en desuso y ahora no es compatible con Ivanti Neurons for MDM.

10.10.6.11. Configurar AppTunnel

AppTunnel protege los datos de las aplicaciones al proporcionar seguridad en las sesiones «aplicación por aplicación» entre el contenedor de cada aplicación y la red corporativa.

Esta sección contiene los siguientes temas:

- **Configurar el Sentry para que use AppTunnel con certificados**
- **Carga de certificados Sentry**
- **Configurar que las aplicaciones usen AppTunnel**
- **Acerca del nombre de servicio de AppTunnel**

Configurar el Sentry para que use AppTunnel con certificados

> Cuando instala por primera vez Standalone Sentry, también se instala un certificado autofirmado. Ivanti recomienda encarecidamente que sustituya el certificado predeterminado por un certificado de terceros de confianza pública.

Requisitos previos

- AppTunnel depende de la versión más reciente compatible con el Sentry. Complete la instalación del Sentry antes de iniciar las tareas de configuración de AppTunnel.
- Si desea usar una identidad SCEP:
  - Añada una **Entidad de Certificación** local o externa. Es necesaria una instalación de Conector.
  - Añada una configuración del certificado de identidad de la aplicación. Esta es la distribución dinámica que usará cuando configure AppTunnel.

Puede configurar ActiveSync o AppTunnel mediante certificados X.509 para que la autenticación utilice los servidores Sentry asignados a un perfil.

Procedimiento

1. Vaya a **Administrador > Sentry**.
2. Haga clic en **+ Añadir perfil de Sentry**.
3. Haga clic en **ActiveSync y/o AppTunnel con certificados**.
4. Haga clic en **Siguiente**.
5. Use las directrices que aparecen en la siguiente tabla para completar la página de **Ajustes globales**.

Tabla: Ajustes globales para Administración > Sentry	
Ajuste	**Qué hacer**
Nombre,	Introduzca un nombre que identifique a este perfil.
Descripción	Introduzca una descripción que explique la finalidad de este perfil.
Nombre de host y puerto externos	Introduzca el nombre de host y el puerto del Sentry.
Modo de autenticación del dispositivo	
Utilizar un único certificado para la autenticación en dos fases	Seleccione esta opción para usar un único certificado para la autenticación. Si todavía no tiene un **certificado cargado**, puede hacerlo en el área que se muestra debajo de la opción seleccionada.
Seleccionar certificado	Para cargar un certificado de grupo necesario para la autenticación del dispositivo: 1. Haga clic en **Añadir**. Aparecerá la ventana **Añadir certificado**. 2. Escriba el nombre del certificado en el campo **Nombre del certificado**. 3. Escriba la contraseña que protege el archivo PKCS12. 4. Haga clic en **Elegir archivo** para cargar el certificado de grupo. Asegúrese de que el formato del archivo sea en .p7b, .p12, .pfx, .pem, .der, .crt o .cer.
Activar la lista de revocación de certificados (CRL)	Seleccione esta opción para validar los certificados presentados por el dispositivo junto a la lista de revocación de certificados (CRL) publicada por la EC.
Comportamiento predeterminado de los dispositivos no administrados	
Permitir que los dispositivos no administrados reciban correos electrónicos y datos	Seleccione esta opción si no quiere bloquear el acceso a los datos para los dispositivos que no estén administrados con Ivanti Neurons for MDM.

6. Haga clic en **Siguiente**.
7. En la página de **Configuración del servidor sentry**, configure los campos siguientes:
8. Haga clic en **Siguiente**.

Tabla: Configuración del servidor de Sentry para Administrador > Sentry	
Ajuste	Qué hacer
Protocolo de escucha	Seleccione cualquiera de las siguientes opciones del protocolo: • **Solo HTTPS** • **Solo HTTP** • **HTTPS y HTTP**
Puerto HTTPS	Introduzca el número de puerto Https. Este campo no se mostrará si el protocolo de escucha está seleccionado como Solo HTTP.
Puerto HTTP	Introduzca el número de puerto HTTP. Este campo no se mostrará si el protocolo de escucha está seleccionado como Solo HTTPS.
Certificado/clave del servidor TLS del Sentry	
Utilizar el certificado autofirmado de Sentry	Seleccione esta opción para usar el certificado autofirmado creado por el servicio Ivanti Neurons for MDM y se le enviará a Sentry como parte de este perfil. Este certificado se utiliza para la comunicación entre Sentry y los dispositivos móviles.
Añadir	Para cargar su propio certificado necesario para la autenticación del dispositivo: 1. Haga clic en **Añadir**. Aparecerá la ventana **Añadir certificado**. Podrá ver esta opción solo cuando anule la selección de la opción **Utilizar el certificado autofirmado de Sentry**. 2. Escriba el nombre del certificado en el campo **Nombre del certificado**. 3. Escriba la contraseña que protege el archivo PKCS12. 4. Haga clic en **Elegir archivo** para cargar el certificado. Asegúrese de que el archivo esté en formato .p12. 5. Haga clic en **Añadir**. Todos los certificados del servidor TLS cargados (incluidos los cargados desde la página principal de Sentry y desde otros perfiles) se muestran en la sección Certificado/certificado/clave del servidor TLS del Sentry. Para seleccionar el certificado TLS necesario para la autenticación, haga clic en el botón de radio que hay junto al certificado.
Agregar un segundo certificado	Seleccione para activar el segundo certificado. Una vez que el certificado principal caduque, Sentry cambiará automáticamente al certificado de respaldo sin intervención del administrador. Tunnel ya almacena ambos certificados y puede coincidir con cualquiera de ellos, asegurando una conectividad ininterrumpida.
Protocolos	Seleccione los protocolos de entrada y salida necesarios.

Tabla: Configuración del servidor de Sentry para Administrador > Sentry	
Conjuntos de cifrado	Los cifrados se utilizan en la comunicación cifrada SSL con el Sentry. Normalmente se prefieren cifrados fuertes. Puede que los dispositivos más antiguos necesiten cifrados débiles. El cifrado fuerte se selecciona de manera predeterminada. Seleccione los cifrados adicionales que desee utilizar. Se debe seleccionar, al menos, un cifrado.

9. Añada al menos uno de los servicios que se muestran.
10. Haga clic en **Guardar**.

Una vez que haya registrado el Sentry, este se mostrará en la página de Sentry en la sección de Servidores Sentry no configurados. Para asignarle un perfil al Sentry, haga clic en **Asignar** en la columna **Acciones**.

Carga de certificados Sentry

Ivanti Neurons for MDM carga los certificados del servidor TLS y los certificados de grupo cuando se crea un perfil de Sentry. También puede cargar estos certificados desde la página **Sentry**, en la sección **Certificados Sentry**.

Ivanti Neurons valida los certificados de Sentry durante la carga, y devuelve los siguientes tipos de información según las condiciones que se han encontrado en los certificados:

Condición	Tipo de información
El certificado de hoja no contiene una cadena a ninguna autoridad de certificación o no hay una autoridad de certificación en el archivo cargado.	Error
No hay disponible ninguna autoridad de certificación de raíz.	Advertencia
La autoridad de certificación de raíz no ha aprobado la autoridad de certificación intermedia para el certificado de hoja.	Advertencia

Ivanti Neurons for MDM también valida con las reglas de **este artículo**.

Procedimiento

1. En la sección **Certificados de servidor TLS**, haga clic en **Añadir**. Aparecerá la ventana **Añadir certificado**.
2. Escriba el nombre del certificado en el campo **Nombre del certificado**.
3. Escriba la contraseña que protege el archivo PKCS12.
4. Haga clic en **Seleccionar archivo** para cargar el certificado de grupo. Asegúrese de que el formato del archivo sea .p7b, .p12, .pfx, .pem, .der, .crt o .cer.
5. Haga clic en **Añadir**. El certificado cargado aparecerá en la tabla.
6. Para eliminar el certificado del servidor TLS, haga clic en el icono Eliminar en la columna **Acciones**.

> Si el certificado del servidor TLS se usa en algún perfil de Sentry, no podrá eliminar el certificado. Si se realiza la acción a eliminar, se mostrará un mensaje de error.

Certificados de Añadir grupo

Procedimiento

1. En la sección **Certificados de grupo**, haga clic en **Añadir**. Aparecerá la ventana **Añadir certificado**.
2. Escriba el nombre del certificado en el campo **Nombre del certificado**.
3. Escriba la contraseña que protege el archivo PKCS12.
4. Haga clic en **Seleccionar archivo** para cargar el certificado de grupo. Asegúrese de que el formato del archivo sea .p7b, .p12, .pfx, .pem, .der, .crt o .cer.
5. Haga clic en **Añadir**.

Para eliminar el certificado de grupo cargado, haga clic en el icono Eliminar en la columna **Acciones**.

Editar el certificado raíz de Sentry

Como administrador tiene la opción de editar la distribución de la configuración del Certificado Raíz Sentry. También puede proporcionar permiso de edición al administrador del espacio personalizado delegando la configuración a otros espacios.

1. Vaya a **Configuraciones**.
2. Busque el **certificado raíz de Sentry**.
3. Haga clic en el icono editar.
4. Seleccione las casilla de verificación que correspondan con los Dispositivos o Grupos de dispositivos a los que desee distribuir los certificados. También puede desmarcar las casillas de verificación que correspondan a los Dispositivos o Grupos de dispositivos.
5. Seleccione una de las opciones siguientes de la sección Resumen de distribución según corresponda:
   - **No aplicar a otros espacios**
   - **Aplicar a los dispositivos de otros espacios**
6. (Opcional) Haga clic en la casilla **Permitir que el administrador del espacio edite la distribución**.
7. Haga clic en **Guardar**.
8. Aparece un mensaje de advertencia. Haga clic en **Sí** para confirmar.

Configurar que las aplicaciones usen AppTunnel

Para las últimas instrucciones de Sentry, visite **Documentación del producto** y haga clic en Sentry. Seleccione el documento apropiado para su versión de Sentry.

Acerca del nombre de servicio de AppTunnel

El servicio de AppTunnel define el servicio «back-end» al que se conecta una aplicación AppConnect.

Para obtener las instrucciones más recientes, visite **Documentación del producto** y seleccione los documentos que correspondan a sus versiones de **Sentry** y **AppConnect**.

10.10.6.12. Configuración de VPN por aplicación

Licencia: Silver

Aplicable a: dispositivos iOS, watchOS, visionOS y tvOS

La configuración de VPN por aplicación define los ajustes para el acceso a redes privadas virtuales para aplicaciones específicas:

- Ajustes de VPN por aplicación
- IPsec (Cisco)
- AnyConnect de Cisco
- SSL de Juniper
- VPN de NetMotion
- SSL de F5
- Conéctese a SonicWALL Mobile
- Aruba VIA
- SSL personalizada
- GlobalProtect de Palo Alto Networks

> La configuración de VPN por aplicación depende de la configuración de la aplicación. La configuración de VPN por aplicación se crea durante la programación de la Configuración de la Aplicación. Cuando la configuración de VPN por aplicación se elimina o no se distribuye, la configuración de la aplicación funciona mal al desconectar la aplicación de la red.

Distribución de la configuración

A partir de la versión 91 de Ivanti Neurons for MDM, los administradores globales pueden delegar en los administradores de espacio la edición de la Configuración de certificados para todos los dispositivos y para la opción de distribución personalizada. Para la configuración de VPN por aplicación, puede seleccionar opcionalmente la opción Permitir que esta configuración esté disponible en todos los espacios.

> Los cambios en la distribución son aplicables sólo al espacio específico. Todos los demás espacios siguen heredando la configuración de distribución espacial predeterminada.

Especifique los ajustes de configuración de los campos utilizando la información de las tablas siguientes, corresponda, y a continuación distribuya la configuración.

Para obtener más información, consulte el tema *Distribuir la configuración* en Trabajar con configuraciones.

Ajustes de VPN por aplicación

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Tipo de conexión Activar VPN a petición	Seleccione el tipo de VPN que quiere configurar. Los siguientes ajustes dependerán de esta selección. Seleccione esta opción si desea usar esta configuración para dominios y nombres de host que establecen una VPN a petición.
Activar las reglas de iOS (aplicable si se ha seleccionado VPN a petición)	En iOS y macOS, se pueden configurar: • Reglas de red que permitan o no permitan conexiones con (y permitan o ignoren) las redes consideradas verdaderas. • Reglas de conexión que permiten cuando sea necesario, o no permiten nunca, conexiones a las redes consideradas verdaderas. Para las reglas de redes, se pueden especificar los siguientes tipos de parámetros: • Coincidencia de dominio DNS • Coincidencia de dirección de servidor DNS • Coincidencia SSID • Sondeo de la cadena de la URL • Coincidencia del tipo de interfaz Para las reglas de conexión, se pueden especificar los siguientes tipos de parámetros: • Coincidencia de dominio DNS • Coincidencia de dirección de servidor DNS • Coincidencia SSID • Sondeo de la cadena de la URL • Coincidencia del tipo de interfaz • Dominios • Servidor DNS • Sondeos de URL
Aplicación de coincidencia a petición habilitada	Seleccione esta opción para habilitar la VPN por aplicación a petición.
Habilitar segmentación de red 5G	Seleccione **DNN** (Nombre de red de datos proporcionado por el proveedor de red) para hacer un túnel, apuntando a la VPN de segmento celular específica. Seleccione **Categoría de aplicación** (proporcionada por el proveedor de red), para identificar el tipo de segmento celular que desee tunelizar.
Dominios	

Ajuste	Qué hacer
Dominios de Safari (iOS) **iOS 14.0+ y macOS 11.0+** Dominios asociados	Un conjunto cuyas entradas deben especificar un dominio que active la conexión VPN en Safari. Cada entrada está en el formato www.apple.com. Especifique un dominio asociado o más. Las conexiones a servidores dentro de uno estos dominios están asociadas con el VPN por aplicación.
Dominios excluidos	Especifique un dominio o más excluidos. Las conexiones a los servidores dentro de uno de estos dominios están excluidas del VPN por aplicación.
iOS 13+ y macOS 10.15+	
Dominios de correo Dominios de contactos Dominios del calendario	Haga clic en **+ Añadir** para introducir uno o más dominios que activarán esta conexión VPN en Mail. Cada entrada está en el formato www.apple.com. Haga clic en **+ Añadir** para introducir uno o más dominios que activarán esta conexión VPN en Contactos. Cada entrada está en el formato www.apple.com. Haga clic en **+ Añadir** para introducir uno o más dominios que activarán esta conexión VPN en Calendario. Cada entrada está en el formato www.apple.com.
iOS 9 y posterior	
Tipo de proveedor (iOS 9+)	Seleccione uno de los siguientes proveedores de Tunnel: • proxy de la aplicación - redirecciona el tráfico en la capa de la aplicación. Consulte la **documentación de Apple** para obtener una descripción general del proveedor de proxy de la aplicación. • túnel del paquete - redirecciona el tráfico en la capa IP. Consulte la **documentación de Apple** para obtener una descripción general sobre el proveedor de Tunnel del paquete.

IPsec (Cisco)

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del equipo	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Incluir el PIN de usuario	Seleccione esta opción para solicitar un PIN al usuario.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. **Si selecciona Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* **Si selecciona Automática,** estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

AnyConnect de Cisco

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Grupo	Introduzca el grupo que desea utilizar para autenticar la conexión.
Autenticación del usuario	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual**, estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática**, estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

SSL de Juniper

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Dominio	Introduzca el dominio de autenticación que desea utilizar para autenticar la conexión.
Función	Introduzca la función de autenticación que desea utilizar para autenticar la conexión.
Autenticación del usuario	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual**, estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática**, estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

VPN de NetMotion

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del usuario	El **certificado** es el método de autenticación del usuario que se debe utilizar. Está disponible el siguiente campo: **Credencial**: Seleccione el certificado de identidad que desea utilizar. Los certificados proporcionados por el usuario solo son compatibles con dispositivos iOS.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy. Seleccione las siguientes opciones: • Activar VPN a petición: añadir dominios o nombres de host que establecen una VPN a petición • Activar las reglas de iOS. • Aplicación de coincidencia a petición habilitada.
Dominios de Safari	Haga clic en **+ Añadir** para añadir dominios de Safari.
Tipo de proveedor (iOS 9,0+)	**packet-tunnel** se selecciona como el tipo de proveedor de Tunnel de forma predeterminada. Consulte la **documentación de Apple** para obtener una descripción general sobre el proveedor de Tunnel del paquete.

SSL de F5

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del usuario	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual**, estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática**, estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

Conéctese a SonicWALL Mobile

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Grupo o dominio de inicio de sesión	Introduzca el grupo de inicio de sesión o el dominio que desea utilizar para autenticar la conexión.
Autenticación del usuario	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual**, estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática**, estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

Aruba VIA

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del usuario	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual**, estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática**, estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

SSL personalizada

Ajuste	Qué hacer
Identificador	Introduzca el identificador de este VPN SSL en formato DNS invertido (por ejemplo: com.miempresa.miservidor).
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Datos personalizados	Introduzca los pares clave-valor que definen los datos personalizados para esta VPN.
Autenticación del usuario	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual**, estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática**, estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.
(iOS 9.0+) Incluir Tio de proveedor en el diccionario VPN principal y secundario	Elija incluir el tipo de proveedor al generar un plist (archivo de configuración predefinido).
Proporcione un identificador del paquete	Introduzca el identificador de paquete para el proveedor de VPN. Puede mantener varias Configuraciones de aplicaciones para la misma aplicación con distintos Identificadores de grupo de proveedores.

GlobalProtect de Palo Alto Networks

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Datos personalizados	Introduzca los pares clave-valor que definen los datos personalizados para esta VPN.
Autenticación del usuario	El certificado es el método de autenticación del usuario. Seleccione un certificado de identidad para usar en el campo **Credencial**.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual**, estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática**, estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

Escriba $ para ver una lista de **variables** compatibles, si las hubiera, para este campo.

Temas relacionados:

Cómo crear una configuración

10.10.6.13. Configuración de inicio de sesión único

Ivanti Neurons for MDM habilita el Extensible Single Sign-On (SSO) con las configuraciones Extensible SSO y Extensible SSO Kerberos. La implementación requiere una extensión de la aplicación, como Microsoft Authenticator, del proveedor de identidad. Con una implementación de SSO extensible, los usuarios solo tienen que autenticarse una vez cuando acceden a los recursos de la empresa. No se pide a los usuarios que se autentiquen para los siguientes inicios de sesión. Para obtener información de configuración del proveedor de identidad deseado, consulte **Configurar el proveedor de identidades**.

Esta sección contiene los siguientes temas:

- **Ajustes de la cuenta de inicio de sesión única**
- **Ajustes de la cuenta de Extensible de inicio de sesión única**
- **Ajustes de cuenta Kerberos de Extensible de inicio de sesión única**

Ajustes de la cuenta de inicio de sesión única

Aplicable a:

- iOS 7.0 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- visionOS 1.1 hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Utilice los siguientes ajustes para configurar el SSO corporativo con Kerberos para cualquier aplicación administrada y el navegador Apple Safari en dispositivos iOS.

> Esta configuración requiere el Tunnel y Sentry. Para obtener más información, consulte en "Configurar Single Sign on con Kerberos" en la *Guía de Tunnel para iOS*.

Ajuste	Descripción
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Nombre de usuario	Introduzca el nombre principal de Kerberos.
Nombre de dominio de Kerberos	Introduzca el nombre de dominio de Kerberos
Certificado	**Para iOS 8 con licencia Gold:** seleccione el certificado que va a usar para renovar la credencial de Kerberos.
Coincidencias de prefijos de la URL	Lista de prefijos de URL que deben coincidir para poder usar esta cuenta para la autenticación Kerberos en HTTP.
Aplicaciones de la lista de permitidos para SSO	Añada aplicaciones del Catálogo de Aplicaciones para ponerlas en la lista de permitidos para el SSO. Por ejemplo, escriba «Safari» para añadir Apple Safari. Si no se ha puesto ninguna aplicación en la lista de permitidos para el SSO utilizando una configuración de este tipo, todas las aplicaciones que admitan el SSO en iOS que puedan hacer uso del SSO, incluidas las aplicaciones de iOS integradas.

Ajustes de la cuenta de Extensible de inicio de sesión única

Aplicable a:

- iOS 13.0 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- macOS 10.15 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- visionOS 1.1 hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Utilice los siguientes ajustes para configurar el perfil de extensión SSO con el tipo de extensión genérica para habilitar el SSO para aplicaciones y sitios web nativos con diferentes métodos de autenticación.

> El Extensible SSO no funciona cuando la configuración se inserta en el canal del usuario para los dispositivos macOS 10.15.x.

Ajuste	Descripción
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Elija el tipo de SSO	Seleccione uno de los siguientes tipos de SSO: • **Credenciales** ◦ Introduzca uno o más nombres de **Host** o nombres de dominio que puedan ser autenticados a través de la extensión de la aplicación. Los nombres de host o de dominio se emparejan sin diferencias entre mayúsculas/minúsculas, y todos los nombres de host/dominio de todas las cargas útiles de Extensible SSO instaladas deben ser únicos. Los hosts que empiezan con "." son sufijos comodines y coincidirán con todos los subdominios, de lo contrario el host debe ser una coincidencia exacta. ◦ Introduzca el nombre del **Dominio**. Este valor se debe escribir con la debida mayúscula. • **Redirección** ◦ Introduzca uno o más prefijos de **URL** de los proveedores de identidad donde la extensión de la aplicación realice SSO. Las URL deben comenzar por http:// o https://, el esquema y el nombre del host se emparejan sin diferenciar entre mayúsculas y minúsculas, los parámetros de consulta y los fragmentos de URL no están permitidos, y las URL de todas las cargas útiles de Extensible SSO instaladas deben ser únicas.
Identificador de la extensión	Introduzca el identificador del paquete de la extensión de la aplicación que realice el SSO para las URL especificadas.
Identificador del equipo	El identificador del equipo de la extensión de la aplicación. Esta clave es obligatoria en macOS y se ignora en los demás lugares.
Datos personalizados	Introduzca uno o más datos personalizados como pares clave-valor.
Método de autenticación (Aplicable solo a macOS 13+)	• Contraseña • Clave del usuario de Secure Enclave
Token de registro	Introduzca el token. Este campo se activa cuando se selecciona uno de los Métodos de autenticación.
Comportamiento de	Seleccione una de las siguientes opciones: • **Cancelar**: el sistema cancela las solicitudes de autenticación cuando la pantalla está bloqueada.

Ajuste	Descripción
la pantalla bloqueada (aplicable para iOS 15.0+ y macOS 12.0+)	• **No manejar**: la solicitud de autenticación continúa sin SSO cuando la pantalla está bloqueada.
Identificadores de paquete denegados (aplicable para iOS 15.0+ y macOS 12.0+)	Agregue varios identificadores de paquetes de aplicaciones que no utilizan el SSO que proporciona esta extensión. Por ejemplo, *com.empresa.nombredeaplicación.www*.

Aplicable a: macOS 14.0 hasta la versión publicada más reciente compatible con Ivanti Neurons for MDMIvanti Neurons for MDM.

Ajuste	Descripción
Nombre en pantalla de la cuenta	Introduzca un nombre para la cuenta que se mostrará en las notificaciones y solicitudes de autenticación.
Grupos adicionales	Introduzca el nombre de los grupos que no tendrán acceso de administrador.
Grupos de administradores	Introduzca el nombre del grupo que tendrá acceso de administrador.
Método de autenticación	Seleccione uno de los métodos de autenticación de la lista desplegable: • Contraseña • Clave del usuario de Secure Enclave • Tarjeta inteligente
Grupos de autorización	Introduzca el derecho de autorización para un nombre de grupo.
Activar autorización	Seleccione la casilla para activar los avisos de autorización para grupos de administradores, grupos de autorización o grupos adicionales.
Activar Crear usuario al iniciar sesión	Seleccione la casilla para permitir la creación de nuevos usuarios durante el inicio de sesión mediante una contraseña o tarjeta inteligente como método de autenticación.
Frecuencia de inicio de sesión	La duración, en segundos, hasta que el sistema requiera un inicio de sesión completo en lugar de una actualización. El valor predeterminado es 64,800 (18 horas). El valor mínimo es 3600 (1 hora).
Nuevo modo de autorización de usuario	Seleccione uno de los modos de autorización para un usuario nuevo de la lista desplegable: • Estándar: la cuenta es para un usuario estándar. • Administrador: el sistema añade la cuenta al grupo del administrador local. • Grupos: el sistema agrupa automáticamente al nuevo usuario en el grupo de administradores, grupo de autorizaciones o grupo adicional.
Asignación de token a usuario	Introduzca el nombre de cuenta y el nombre completo de los nuevos usuarios para asignarlos a la autorización.
Modo de autorización de usuario	Seleccione uno de los modos de autorización para un usuario de la lista desplegable: • Estándar: la cuenta es para un usuario estándar. • Administrador: el sistema añade la cuenta al grupo del administrador local. • Grupos: el sistema agrupa automáticamente al nuevo usuario en el grupo de administradores, grupo de autorizaciones o grupo adicional.
Utilizar claves de dispositivo compartidos	Marque la casilla para activar el mismo inicio de sesión y claves de cifrado para todos los usuarios.

Aplicable a: macOS 15.4 hasta la versión publicada más reciente compatible con Ivanti Neurons for MDM.

Ajuste	Descripción
Permitir la certificación del identificador del dispositivo	Marque la casilla de verificación para incluir el UDID y el número de serie del dispositivo en las certificaciones SSO de la plataforma, esto permite el seguimiento de en segundo plano de los dispositivos registrados.

Aplicable a: macOS 14.0 hasta la versión publicada más reciente compatible con Ivanti Neurons for MDMIvanti Neurons for MDM.

Para ver la configuración de la cuenta de inicio de sesión único extensible, seleccione la opción desplegable como **Contraseña** en el campo **Método de autenticación**.

Ajuste	Descripción
Política de FileVault	Habilite la política para ver la siguiente configuración: • Intentar autenticación • Requerir autenticación Seleccione la casilla de verificación **Requerir autenticación** para activar opciones de configuración adicionales. • Permitir periodo de gracia sin conexión • Permitir periodo de gracia de la autenticación
Política de acceso	Habilite la política para ver la siguiente configuración: • Intentar autenticación • Requerir autenticación Seleccione la casilla de verificación **Requerir autenticación** para activar opciones de configuración adicionales. • Permitir periodo de gracia sin conexión • Permitir periodo de gracia de la autenticación
Política de desbloqueo	Habilite la política para ver la siguiente configuración: • Intentar autenticación • Requerir autenticación Seleccione la casilla de verificación **Requerir autenticación** para activar opciones de configuración adicionales. • Permitir periodo de gracia sin conexión • Permitir periodo de gracia de la autenticación • Permitir TouchID o reloj para desbloquear
Periodo de gracia de la autenticación	Introduzca la cantidad de tiempo tras seleccionar una de las políticas para utilizar cuentas locales no registradas. Si selecciona la casilla de verificación **Permitir periodo de gracia de autenticación** en una de las políticas, se convierte en un campo obligatorio.
Periodo de gracia sin conexión	Introduzca la cantidad de tiempo tras seleccionar una de las políticas para usar una contraseña de cuenta local sin conexión después de un inicio de sesión exitoso en la Plataforma SSO. Si selecciona la casilla de verificación **Permitir periodo de gracia sin conexión** en una de las políticas, se convierte en un campo obligatorio.
Cuentas SSO sin plataforma	Seleccione **+ Añadir** para introducir la lista de nombres de usuario que no están sujetos a las políticas de FileVault, Inicio de sesión o Desbloqueo.

Ajustes de cuenta Kerberos de Extensible de inicio de sesión única

Aplicable a:

- iOS 13.0 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- macOS 10.15 hasta la versión más reciente compatible con Ivanti Neurons for MDM.

- visionOS 1.1 hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Utilice los siguientes ajustes para configurar una extensión de aplicación que realice SSO con la extensión Kerberos.

> El Extensible SSO Kerberos no funciona cuando la configuración se inserta en el canal del usuario para los dispositivos macOS 10.15.x.

Ajuste	Descripción
Ajustes básicos	
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Nombre de usuario Dominio Certificado Prefijos de URL **Ajustes avanzados**	Introduzca el nombre principal de Kerberos. Introduzca el nombre de dominio de Kerberos Seleccione el certificado que se utilizará para renovar la credencial de Kerberos. Lista de prefijos de URL que deben coincidir para poder usar esta cuenta para la autenticación Kerberos en HTTP.
Permitir el acceso automático	Si es falso, no se permite guardar las contraseñas en la llave. De forma predeterminada, esta opción está activada.
Retrasar la configuración del usuario Requiere la presencia del usuario	Si es verdadero, no se pide al usuario que configure la extensión Kerberos hasta que el administrador la habilite con la herramienta app-SSO o hasta que se reciba un desafío Kerberos. Esta opción se puede aplicar a macOS 11 hasta la versión más reciente compatible con Ivanti Neurons for MDM. Si es verdadero, requiere que el usuario proporcione Touch ID, Face ID o su código de acceso para acceder a la entrada del llavero.
Monitizar el caché de credenciales Nombre del caché	Si es falso, se pide la credencial en el próximo desafío de Kerberos o cambio de estado de red. Si la credencial ha caducado o falta, se creará una nueva. Esta opción se puede aplicar a macOS 11 hasta la versión más reciente compatible con Ivanti Neurons for MDM. De forma predeterminada, esta opción está activada. Introduzca el nombre del Servicio de Seguridad Genérico (GSS) de la caché de Kerberos a utilizar. Esta opción ahora está obsoleta.
Mapeo de dominios Dominio por defecto Usar la detección automática del sitio	Introduzca el nombre del dominio como la clave. El valor es un conjunto de sufijos del DNS que se mapean en el dominio. Haga clic en **+Añadir** para añadir uno o más pares clave-valor. Esta propiedad especifica el dominio por defecto si hay más de una configuración de extensión Kerberos. Si es falso, la extensión Kerberos no usa automáticamente LDAP y DNS para determinar el nombre del sitio AD. De forma predeterminada, esta opción está activada.
Código del sitio	Introduzca el nombre del sitio de Active Directory que debe utilizar la extensión Kerberos.

Ajuste	Descripción
Tiempo de replicación	Introduzca el tiempo, en segundos, necesario para replicar los cambios en el dominio de Active Directory. La extensión Kerberos usará esto cuando compruebe la antigüedad de la contraseña después de un cambio. Esta opción se puede aplicar a macOS 11 hasta la versión más reciente compatible con Ivanti Neurons for MDM. Esta opción ahora está obsoleta.
ACL del Id. del paquete de credenciales Incluir las aplicaciones administradas en ACL del Id. del paquete	Haga clic en **+ Añadir** para añadir una lista de identificaciones de paquetes permitidos para acceder al Ticket Granting Ticket (TGT) para la autenticación. Si es verdadero, la extensión Kerberos permitirá que solo las aplicaciones administradas accedan y utilicen la credencial. Esto es además del ACL del Id. del paquete de credenciales, si se especifica. Esta opción se puede aplicar a iOS 14 o versiones más recientes compatibles de Ivanti Neurons for MDM.
Incluir las aplicaciones Kerberos en ACL del Id. del paquete	Si es cierto, la extensión de Kerberos permite que las funciones estándar de Kerberos, incluida Ticket Viewe y klist, accedan al uso de la credencial. Disponible en macOS 12 y posterior.
Etiqueta de nombre de usuario personalizada Texto de ayuda	Introduzca la etiqueta del nombre de usuario personalizado que se usó en la extensión de Kerberos en lugar de "Username." Por ejemplo, "Id de empresa." Esta opción se puede aplicar a macOS 11 mediante la versión más reciente compatible con Ivanti Neurons for MDM. Introduzca el texto que se mostrará al usuario en la parte inferior de la ventana de inicio de sesión de Kerberos. Se puede utilizar para mostrar información de ayuda o un texto sobre la exención de responsabilidad. Esta opción se puede aplicar a iOS 14 y macOS 11 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
Modo de uso de la credencial	Esta configuración afecta a cómo otros procesos utilizarán la credencial de la extensión Kerberos. Utilice una de las siguientes opciones: • Siempre (predeterminado): la credencial de la extensión siempre se usará si el nombre principal de servicio (SPN) coincide con la matriz de hosts de la extensión Kerberos. La credencial no se usará si la aplicación de llamada no está en credentialBundleIDACL. • Cuando no se especifique: la credencial solo se utilizará cuando el identificador de la llamada no haya especificado otra credencial y el SPN coincida con la matriz de hosts de la extensión Kerberos. La credencial no se usará si la aplicación de llamada no está en credentialBundleIDACL. • Kerberos por defecto: se utilizan los procesos Kerberos por defecto para la selección de credenciales que normalmente utilizan la credencial Kerberos por defecto. Esto es lo mismo que desactivar esta función. (Opcional) Seleccione **Requiere TLS para LDAP**.
Centro de distribución de claves preferido	Añadir centros de distribución de claves preferido. Hacer clic en **+Añadir** para agregar un KDC preferido.

Ajuste	Descripción
	Permitir la reserva para la autenticación SSO de la plataforma: si es Cierto y si es Cierto Usar el TGT SSO de la plataforma, el usuario puede iniciar sesión manualmente. Disponible en macOS 13 y posterior **LLevar a cabo solo Kerberos**: si Cierto, la extensión de Kerberos maneja solo las solicitudes de Kerberos. Disponible en macOS 13 y posterior. **Use el TGT de SSO de la plataforma**: si Cierto, esta configuración usa un TGT del SSO de la plataforma en lugar de uno nuevo. Disponible en macOS 13 y posterior.
Configurar Cambiar al modo Contraseña	Si es Cierto, permite al usuario cambiar la interfaz de usuario al modo Contraseña. Disponible en macOS 15 y posterior.
Configurar Cambiar al modo Smart Card	Si es Cierto, permite al usuario cambiar la interfaz de usuario al modo SmartCard. Disponible en macOS 15 y posterior.
Configurar Iniciar en modo Smart Card	Si es Cierto, la interfaz de usuario se inicia en modo SmartCard. Disponible en macOS 15 y posterior.
Filtro de selección automática del emisor de identidad	Filtra la lista de Smart Cards disponibles. Disponible en macOS 15 y posterior.
Ajustes de la contraseña	
Permitir el cambio de contraseña	Si es falso, desactiva los cambios de contraseña. Esta opción se puede aplicar a macOS 10.15 hasta la versión más reciente compatible con Ivanti Neurons for MDM. De forma predeterminada, esta opción está activada.
Cambiar la URL de la contraseña	Introduzca la URL que se lanzará en el navegador web predeterminado del usuario cuando inicie un cambio de contraseña. Esta opción se puede aplicar a macOS 10.15 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
Permitir la complejidad de la contraseña	Si es cierto, las contraseñas deben cumplir con la definición de Active Directory de "complex." Esta opción se puede aplicar a macOS 10.15 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
Longitud mínima de la contraseña	Introduzca la longitud mínima (en caracteres) de las contraseñas del dominio. Esta opción se puede aplicar a macOS 10.15 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
Notificación de caducidad de la contraseña	Introduzca el número de días antes de que venza la contraseña, momento en que se enviará al usuario una notificación de caducidad de la misma. Esta opción se puede aplicar a macOS 10.15 hasta la versión más reciente compatible con Ivanti Neurons for MDM. El valor predeterminado es de 15 días.

Ajuste	Descripción
Anulación de caducidad de la contraseña	Introduzca el número de días que las contraseñas se pueden usar en este dominio. Para la mayoría de los dominios, esto se puede calcular automáticamente. Esta opción se puede aplicar a macOS 10.15 hasta la versión más reciente compatible con Ivanti Neurons for MDM. (Esta opción ahora está obsoleta)
Texto obligatorio de la contraseña	Introduzca la versión de texto de los requisitos de contraseña del dominio. Solo para usarse si no se especifica pwReqComplexity o pwReqLength. Esta opción se puede aplicar a macOS 10.15 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
Recuento del historial de la contraseña	Introduzca el número de contraseñas previas que no se pueden reutilizar en este dominio. Esta opción se puede aplicar a macOS 10.15 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
Antigüedad mínima de la contraseña	Introduzca la antigüedad mínima (en días) de las contraseñas antes de que se puedan cambiar en este dominio. Esta opción se puede aplicar a macOS 10.15 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
Permitir la sincronización de la contraseña local	Si es falso, desactiva la sincronización de la contraseña. Esto no funcionará si el usuario está conectado con una cuenta de móvil. Esta opción se puede aplicar a macOS 10.15 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
Requisito de contraseña Datos RTF	Versión formateada en archivo RTF de los requisitos de contraseña del dominio. Disponible en macOS 15 y posterior. Solo para uso si no se especifican pwReqComplexity o pwReqLength.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.6.14. Configuración del relé de red

Ivanti Neurons for MDM habilita la configuración de retransmisión de red para la carga útil que se utiliza para configurar los ajustes de retransmisión de un dispositivo o una aplicación sin necesidad de VPN o túneles para acceder a recursos privados.

Aplicable a

- iOS 17.0 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- macOS 14 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- visionOS 1.1 hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Busque y seleccione la configuración de **Relé de red**.
3. Configure los ajustes de **Relé de red** según la tabla siguiente:

Ajuste	Descripción
Nombre,	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
URL de relé HTTP/3	Especifique un valor de URL para utilizar como valor de campo HTTP para esta configuración. Incluya la URL de retransmisión HTTP/2 o la URL de retransmisión HTTP/3, o puede incluir ambas.
URL de relé HTTP/3	Especifique un valor de URL para utilizar como valor de campo HTTP para esta configuración. Incluya la URL de retransmisión HTTP/2 o la URL de retransmisión HTTP/3, o puede incluir ambas.
Campos adicionales del encabezado HTTP	Especifique el valor del campo de cabecera HTTP para el nombre del campo de cabecera correspondiente.
Certificado	Seleccione uno de los certificados de identidad que ha creado en la lista desplegable.
Clave pública bruta	Especifique las claves públicas sin procesar para autenticar el servidor durante una conexión de red.
+ Agregar	Seleccione **+ Agregar** para añadir la configuración de múltiples relés de red.
Coincidencias de dominios	Especifique la lista de dominios para determinar qué conexión enrutar a través de los servidores en Relés.
Excluir dominios	Especifique la lista de dominios para determinar qué conexión evitar a través de los servidores en Relés.
Coincidencia de FQDN (compatible con dispositivos iOS 18.4+ y macOS 15.4+)	Especifique la lista de nombres de dominio totalmente calificados (FQDNS), también conocidos como nombres de host, que deberían enrutarse a través de los servidores contenidos en los relés. Cualquier conexión que coincida con este FQDN o nombre de host exacto usará los relés. Si no se enumeran FQDNS ni 'Matchdomains', el tráfico a todos los dominios, excepto los que coinciden con un dominio excluido o FQDN excluido, se enrutará a los servidores de retransmisión.
Excluir FQDN (compatible con dispositivos iOS 18.4+ y macOS 15.4+)	Especifique la lista de nombres de dominio totalmente calificados (FQDNS), también conocidos como nombres de host, que **NO** deberían enrutarse a través de los servidores contenidos en los relés. Cualquier conexión que coincida exactamente con FQDN no usará el servidor de retransmisión. Cuando también se especifican 'Matchdomains', cualquier FQDN enumerado aquí en 'ExcudedFQDNS' debería ser un subdominio de al menos un MatchDomain. De lo contrario, no tendrá ningún efecto.

4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Seleccione una de las opciones de distribución para establecer la configuración de **Relé de red**. Para más información sobre la configuración de las opciones de distribución, consulte Trabajar con configuraciones.
6. Haga clic en **Hecho**.

10.10.6.15. Inicio de sesión seguro multiusuario para iOS

El clip web multiusuario permite a los usuarios entrar y salir de los dispositivos iOS registrados en Ivanti Neurons for MDM. Cuando un usuario inicia sesión por primera vez, los perfiles, aplicaciones y configuraciones que están asociadas con ese usuario se insertarán en el dispositivo. Cuando haya terminado su trabajo, puede abrir el clip web y seleccionar la función «cerrar sesión», que asigna el dispositivo al usuario Nadie y elimina los perfiles, aplicaciones y configuraciones asociadas al usuario que inició sesión originalmente, siempre que las configuraciones y aplicaciones no se distribuyan al usuario Nadie. Después de cerrar sesión, el clip web se reinicia para que el siguiente usuario pueda iniciar sesión y recibir sus configuraciones, aplicaciones y políticas personalizadas. No es necesaria la supervisión del dispositivo para utilizar la función de inicio de sesión seguro multiusuario. Consulte el artículo de la base de conocimientos de la Asistencia técnica de **Ivanti Neurons for MDM: inicio de sesión seguro multiusuario para iOS**, para ver más detalles sobre la función de inicio de sesión multiusuario.

Aplicable a: dispositivos iOS (no aplicable a los dispositivos con Inscripción de usuarios)

Esta sección contiene los siguientes temas:

- **Credenciales admitidas**
- **Comprender el concepto de usuario «Nadie»**
- **Iniciar sesión en un dispositivo**
- **Cerrar sesión en un dispositivo**

Credenciales admitidas

Se deben usar el nombre de usuario y la contraseña para acceder al clip web seguro multiusuario. El registro basado en PIN no es compatible con el clip web seguro multiusuario.

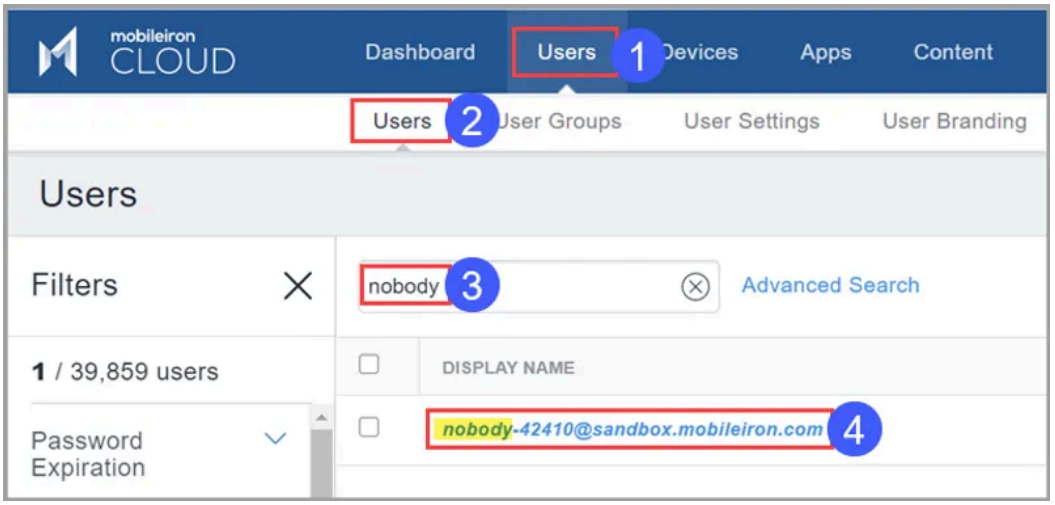
Procedimiento

1. Vaya a **Configuraciones**.
2. Haga clic en **Inicio de sesión seguro multiusuario para iOS**. Es posible que tenga que utilizar la función de búsqueda para encontrarla si hay varias páginas de configuraciones. No se accede a esta configuración seleccionando **+Añadir**.
3. Haga clic en **Editar distribución** o en el icono asociado para distribuir el clip web al Grupo de dispositivos apropiado.
   
   Si desea distribuirlo a un Grupo de usuarios, puede crear un Grupo de dispositivos dinámico que esté vinculado a un Grupo de usuarios.
4. Seleccione una de las siguientes opciones de distribución, recordando que siempre debe distribuir el clip web al usuario Nadie o al grupo de dispositivos con el que el usuario Nadie está asociado. Esto no ocurre por defecto, así que asegúrese de distribuirlo al usuario Nadie.
   - Todos los dispositivos
   - Ningún dispositivo (predeterminada)
   - Personalizada

Haga clic en **Guardar**.

Comprender el concepto *de usuario «Nadie»*

Cuando un dispositivo ha cerrado sesión a través del clip web, permanece inscrito en Ivanti Neurons for MDM con un usuario especial llamado el «usuario Nadie». Si desea eliminar aplicaciones y configuraciones del dispositivo cuando un usuario cierre la sesión, debe asegurarse de que esas aplicaciones y configuraciones no se distribuyan al usuario Nadie. Si desea que determinadas configuraciones, como la de Wi-Fi, permanezcan en el dispositivo cuando un usuario cierre la sesión del clip web de inicio de sesión seguro, debe asegurarse de que esas configuraciones también se distribuyan al usuario Nadie.



Esto significa que debe prestar atención a los Grupos de usuarios y Grupos de dispositivos a los que distribuye aplicaciones y configuraciones. Si está distribuyendo una aplicación a Todos y quiere que se elimine cuando un usuario cierre la sesión del dispositivo, entonces lo mejor es crear un Grupo de usuarios que no incluya al usuario Nadie. Los atributos personalizados facilitan la creación de un grupo de usuarios que sen «multiusuarios», y otro grupo de usuarios que consista solo en el usuario Nadie. Puede crear un atributo de usuario desde Administrador > Sistema > Atributos llamado «Propietario multiusuario» y luego asignar el valor de «Sí» o «Verdadero» al usuario Nadie. A continuación, puede crear grupos de usuarios y grupos de dispositivos en función del valor del atributo.

Iniciar sesión en un dispositivo

El usuario puede iniciar sesión en un dispositivo iOS y asignarse a sí mismo el dispositivo. Después de iniciar sesión, todas las aplicaciones, políticas, configuraciones y certificados pertinentes se insertarán en el dispositivo.

> Por motivos de seguridad, el usuario del IDP debe volver a autorenticarse cada vez que inicie sesión, incluso si ya ha iniciado sesión en el dispositivo.

Cerrar sesión en un dispositivo

El usuario puede cerrar sesión en su dispositivo iOS después de haberlo usado. Después de cerrar sesión, las aplicaciones, políticas, configuraciones y certificados se eliminarán del dispositivo, dejándolo en el mismo estado en el que estaba antes de que el usuario iniciara sesión. Después, el dispositivo estará disponible para que otro usuario inicie sesión.

> Cierre la sesión de todas las aplicaciones de Microsoft antes de cerrar la sesión de Multi-user Web Clip.

Para obtener más información, consulte **Personalización del inicio de sesión para múltiples usuarios**.

10.10.6.16. Configuración de ajustes de la APN de Android

Las Configuraciones de ajustes de la APN de Android le permiten establecer las configuraciones de Nombre del punto de acceso (APN) necesarias en los dispositivos de una red pública. Esta configuración es aplicable a los dispositivos administrados por Android Enterprise Work y a los dispositivos administrados con perfil de trabajo en el dispositivo propiedad de la empresa (en la versión 9.0 de Android o en las versiones más recientes compatibles).

Procedimiento

1. Vaya a **Configuración > +Añadir**.
2. Seleccione la configuración **Ajustes de la APN de Android**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. En la sección Ajuste de la configuración, configure las siguientes opciones:
6. Haga clic en **Siguiente**.

Ajuste	Descripción
Nombre de la entrada	Escriba el nombre de los ajustes del punto de acceso.
Nombre del punto de acceso	Escriba el nombre del punto de acceso.
Tipo de punto de acceso	Seleccione el tipo de punto de acceso de las siguientes opciones: • **Predeterminado** • **DUN** • **IMS** • **De emergencia** • MMS • **HIPRI** • **CBS** • **MCX** • **SUPL** • **FOTA** • **IA**
Tipo de MVNO	Seleccione el tipo de Operador de Red Virtual Móvil (MVNO, Mobile Virtual Network Operator) de las siguientes opciones: • **Ninguna** • **SPN** • **IMSI** • **GID** • **ICCID**
Bearer	Seleccione el tipo de servicio al portador utilizado para la transmisión de datos de las siguientes opciones: • **1xRTT** • **CDMA** • **EDGE** • **EHRPO** • **EVDO** • **EVDO A** • **EVDO B** • **GPRS** • **GSM** • **HSDPA** • **HASP**

Ajuste	Descripción
	• **HSPAP** • **HSUPA** • **IDEN** • **IWLAN** • **LTE** • **NR** • **TD_SCDMA** • **UMTS**
Protocolo de APN	Seleccione el protocolo APN necesario para la APN. A continuación se enumeran las opciones disponibles: • **Ninguna** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP** (Protocolo de punto a punto) • **NO ESTRUCTURADO**
Protocolo de itinerancia de APN	Seleccione el protocolo de itinerancia de la APN necesario para la APN. A continuación se enumeran las opciones disponibles: • **Ninguna** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP** (Protocolo de punto a punto) • **NO ESTRUCTURADO**
Activar/desactivar APN	Active la configuración de la APN.
Id. del operador	Introduzca el valor numérico de la Id. del operador.
Tipo de autenticación	Seleccione el tipo de protocolo de autenticación de las siguientes opciones: • **Ninguna** • **PAP** (protocolo de autenticación de contraseña) • **CHAP** (protocolo de autenticación por desafío mutuo) • **PAP o CHAP**
Nombre de usuario	Introduzca el nombre de usuario para iniciar sesión.

Ajuste	Descripción
Contraseña	Introduzca la contraseña para iniciar sesión.
Confirmar contraseña	Vuelva a introducir la contraseña para la confirmación.
Número de puerto	Introduzca el número de puerto (valor numérico entre 1 y 65535).
Dirección de proxy	Escriba la dirección de proxy.
Código de teléfono móvil del país	Introduzca el código de país para teléfono móvil.
Código de la red móvil	Introduzca el código de la red móvil
Dirección del proxy MMS	Escriba la dirección del proxy MMS.
Número de puerto de MMS	Introduzca el número de puerto MMS (valor numérico entre 1 y 65535)
Dirección del servidor MMS (mmsc)	Escriba la dirección del servidor MMS.

7. Seleccione una de las siguientes opciones de distribución:
8. Haga clic en **Hecho**.

- **Todos los dispositivos**
- Ningún dispositivo (predeterminada)
- **Personalizado**

No se puede agregar otra configuración de APN con los mismos valores para los siguientes campos si ya existe una configuración de APN con estos valores para el dispositivo:

- Código de teléfono móvil del país
- Código de la red móvil
- Nombre del punto de acceso
- Dirección de proxy
- Número de puerto
- Dirección del proxy MMS
- Número de puerto de MMS
- Dirección del servidor MMS
- Activar/desactivar APN
- Tipo de MVNO
- Protocolo de APN
- Protocolo de itinerancia de APN

La Configuración de ajustes de la APN de Android anulará los ajustes de APN si ya se han configurado en el dispositivo manualmente o por parte del operador de red.

10.10.6.17. Configuración de VPN

Aplicable a:

- Android (obsoleto para los dispositivos Android Enterprise. Es necesario utilizar la configuración gestionada para VPN específicas del Catálogo de aplicaciones).
- Windows
- iOS
- macOS
- tvOS
- visionOS

La configuración de VPN define los ajustes para el acceso a redes privadas virtuales.

> La opción de delegación con distribución personalizada está disponible para esta configuración. Para obtener más información, consulte el tema *Distribuir la configuración* en **Trabajar con configuraciones**.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Seleccione la configuración de **VPN**.
3. Introduzca un **Nombre** para la configuración.
4. Introduzca una descripción.
5. Configure los ajustes de VPN según las siguientes descripciones.
6. (Solamente iOS 9.0+) En la sección Unir Dominios, haga clic en **+ Añadir** para introducir uno o varios dominios coincidentes (ejemplo: empresa.com). Se utiliza una conexión proxy cuando el dominio es uno de estos dominios específicos.
7. Haga clic en **Siguiente**.
8. (solo macOS) En la página Distribución, seleccione una de las siguientes opciones de distribución:
    - Canal del dispositivo: la configuración es eficaz para todos los usuarios de un dispositivo; esta suele ser la opción más normal.
    - Canal del usuario: la configuración solo es eficaz para el usuario registrado actualmente en un dispositivo.
9. Seleccione las demás opciones de distribución para esta configuración.
10. Haga clic en **Hecho**.

Ajustes de VPN

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Tipo de conexión	Seleccione el tipo de VPN que quiere configurar. Los siguientes ajustes dependerán de esta selección.

Los protocolos y sus ajustes se enumeran a continuación:

- **L2TP** (No compatible con Ivanti Go)
- **PPTP** (No compatible con Ivanti Go)
- **IPsec (Cisco)** (No compatible con Ivanti Go)
- **Cisco AnyConnect** (Compatible con Ivanti Go)
- **Junper SSL** (No compatible con Ivanti Go)
- **VPN de NetMotion** (No compatible con Ivanti Go)
- Pulse Secure (Compatible con Ivanti Go)
- **F5 SSL** (No compatible con Ivanti Go)
- **SonicWALL Mobile Connect** (No compatible con Ivanti Go)
- **Aruba VIA** (No compatible con Ivanti Go)
- **SSL personalizado** (No compatible con Ivanti Go)
- **Palo Alto Networks GlobalProtect** (Compatible con Ivanti Go)
- **KEv2 (solo Windows)** (No compatible con Ivanti Go)
- **IKEv2** (No compatible con Ivanti Go)

L2TP

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del usuario	Seleccione el método de autenticación que desea utilizar: **Contraseña** o **SecureID RSA**.
Secreto compartido	Introduzca el código de acceso del secreto compartido si es necesario para iniciar la conexión.
Enviar todo el tráfico	Seleccione esta opción para utilizar esta conexión para todo el tráfico de red. Esta opción ayuda a proteger los datos que pueden verse afectados, especialmente en redes públicas.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

PPTP

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del usuario	Seleccione el método de autenticación que desea utilizar: **Contraseña** o **SecureID RSA**.
Nivel de cifrado	Seleccione el nivel de cifrado de datos para la conexión: **Ninguno, Automático** o **Máximo (128 bits)**.
Enviar todo el tráfico	Seleccione esta opción para utilizar esta conexión para todo el tráfico de red. Esta opción ayuda a proteger los datos que pueden verse afectados, especialmente en redes públicas.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

IPsec (Cisco)

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del equipo	Seleccione el método de autenticación que desea utilizar: **Secreto compartido / Nombre del grupo** o **Certificado**.
Nombre del grupo	Autenticación por Secreto compartido/Nombre de grupo. Especifique el nombre de grupo que desea utilizar. Si se utiliza la autenticación híbrida, la cadena debe terminar con €œ[hybrid]â€.
Secreto compartido	Autenticación por Secreto compartido/Nombre de grupo. Introduzca el código de acceso del secreto compartido.
Usar autenticación híbrida	Autenticación por Secreto compartido/Nombre de grupo. Seleccione para especificar la autenticación híbrida, p. ej., el servidor proporciona un certificado y el cliente proporciona una clave precompartida.
Solicitud de contraseña	Autenticación por Secreto compartido/Nombre de grupo. Especifique si se le debe solicitar una contraseña al usuario cuando se conecte.
Credencial	*Autenticación del certificado* Seleccione el certificado de identidad que desea utilizar.
Incluir el PIN de usuario	*Autenticación del certificado* Seleccione esta opción para solicitar un PIN al usuario.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

Cisco AnyConnect

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Grupo	Introduzca el grupo que desea utilizar para autenticar la conexión.
Autenticación del usuario	Seleccione el método de autenticación de usuario que desea utilizar: **Contraseña** o **Certificado**. Si selecciona **Certificado**, los siguientes campos adicionales estarán disponibles: **Credencial**: Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

SSL de Juniper

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Dominio	Introduzca el dominio de autenticación que desea utilizar para autenticar la conexión.
Función	Introduzca la función de autenticación que desea utilizar para autenticar la conexión.
Autenticación del usuario	Seleccione el método de autenticación de usuario que desea utilizar: **Contraseña** o **Certificado**. Si selecciona **Certificado**, los siguientes campos adicionales estarán disponibles: **Credencial**: Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

VPN de NetMotion

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del usuario	Seleccione el método de autenticación de usuario que desea utilizar: **Contraseña** o **Certificado**. Si selecciona **Certificado**, los siguientes campos adicionales estarán disponibles: **Credencial**: Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

F5 SSL

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del usuario	Introduzca el método de autenticación que desea utilizar: **Contraseña** o **Certificado**. Si selecciona **Certificado**, los siguientes campos adicionales estarán disponibles: **Credencial**: Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione Manual o Automática. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

SonicWALL Mobile Connect

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Grupo o dominio de inicio de sesión	Introduzca el grupo de inicio de sesión o el dominio que desea utilizar para autenticar la conexión.
Autenticación del usuario	Seleccione el método de autenticación de usuario que desea utilizar: **Contraseña** o **Certificado**. Si selecciona Certificado, estarán disponibles los siguientes campos adicionales: **Credencial**: Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

Aruba VIA

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del usuario	Seleccione el método de autenticación de usuario que desea utilizar: **Contraseña** o **Certificado**. Si selecciona **Certificado**, los siguientes campos adicionales estarán disponibles: **Credencial**: Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione Manual o Automática. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

SSL personalizada

Ajuste	Qué hacer
Identificador	Introduzca el identificador de este VPN SSL en formato DNS invertido (por ejemplo: com.miempresa.miservidor).
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Datos personalizados	Introduzca los pares clave-valor que definen los datos personalizados para esta VPN.
Autenticación del usuario	Seleccione el método de autenticación de usuario que desea utilizar: **Contraseña** o **Certificado**. Si selecciona Certificado, estarán disponibles los siguientes campos adicionales: **Credencial**: Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

Palo Alto Networks GlobalProtect

> No se aplica a los dispositivos Android.

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Datos personalizados	Introduzca los pares clave-valor que definen los datos personalizados para esta VPN.
Autenticación del usuario	Seleccione el método de autenticación de usuario que desea utilizar: **Contraseña** o **Certificado**. Si selecciona Certificado, estarán disponibles los siguientes campos adicionales: **Credencial**: Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

IKEv2 (solo Windows)

Ajuste	Qué hacer
Servidor	Introduzca el nombre de host o dirección IP del servidor VPN.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

IKEv2

Ajuste	Qué hacer
Servidor	Introduzca el nombre de host o dirección IP del servidor VPN.
Identificador local	El identificador del cliente IKEv2 en alguno de los siguientes formatos: • FQDN • UserFQDN • Dirección • ASN1DN
Identificador remoto	Identificador remoto en uno de los siguientes formatos: • FQDN • UserFQDN • Dirección • ASN1DN
Autenticación del equipo	Solo disponible si **Habilitar EAP** no está seleccionado. Seleccione una de las siguientes opciones: • Certificado • Secreto compartido
Autenticación EAP	Solo disponible si **Habilitar EAP** está seleccionado. Seleccione una de las siguientes opciones: • Certificado • Nombre de usuario/contraseña
Secreto compartido	Solo disponible si se ha seleccionado Secreto compartido para la Autenticación del equipo. Introduzca el secreto compartido para la conexión.
Credencial	Solo disponible si se ha seleccionado Certificado para la Autenticación del equipo. Seleccione el certificado que desea utilizar. Este certificado se enviará para autenticación del cliente IKE. Si se usa la autenticación ampliada, este certificado se puede usar también para EAP-TLS.
Activar EAP	Seleccione esta opción para habilitar la autenticación ampliada.
Cuenta	Solo disponible si se ha seleccionado «Nombre de usuario/contraseña» para la Autenticación EAP. Introduzca la Id. de cuenta para el servidor VPN.
Contraseña	Solo disponible si se ha seleccionado «Nombre de usuario/contraseña» para la Autenticación EAP. Introduzca la contraseña para el servidor VPN.
Intervalo de detección de pares no funcionales	Seleccione una de las siguientes opciones: • Ninguno (desactivar) • Bajo (se envía un keepalive 1 vez por hora) • Medio (se envía un keepalive cada 30 minutos) • Alto (se envía un keepalive cada 10 minutos)

Ajuste	Qué hacer
Nombre común de emisor del certificado del servidor	(Opcional) Nombre común de un emisor de certificados de servidor, hace que el servidor IKE envíe una solicitud de certificado basada en el emisor de certificados al servidor.
Nombre común del certificado del servidor	(Opcional) Nombre común de un emisor de certificados de servidor que se usa para validar el certificado que envía el servidor IKE.
Utilice los atributos de subred IP4 y IP6	(Opcional) Seleccione usar los atributos de subred IP4 y IP6
Activar el Protocolo de movilidad y hospedaje múltiple IKEv2 (MOBIKE)	(Opcional) El ajuste predeterminado es 0. MOBIKE (La posibilidad de admitir dispositivos móviles multi-hospedados cuando se conectan a enlaces tanto móviles como Wi-Fi con múltiples direcciones IP) está habilitado. Está habilitado de forma predeterminada. Establézcalo en 1 para desactivar MOBIKE.
Activar Perfect Forward Secrecy (PFS)	(Opcional) Si se establece en 1, habilita PFS para conexiones IKEv2. El ajuste predeterminado es 0.
Active la redirección IKEv2.	(Opcional) El ajuste predeterminado es 0. La conexión IKEv2 se redirige si se recibe una solicitud de redirección del servidor. Está habilitado de forma predeterminada. Establézcalo en 1 para desactivar la redirección IKEv2.
Active NAT keepalive	Activa la Traducción de direcciones de red (NAT) keepalive, que impide la eliminación de entradas NAT en ausencia de tráfico cuando hay NAT entre sistemas IKE.
Intervalo de NAT keepalive	Si NAT keepalive está activado, este es el tiempo en segundos que se enviarán paquetes keepalive para el dispositivo.
PPK	Introduzca la clave poscuántica precompartida (PPK) con servidores VPN compatibles con RFC 8784. Si esta clave está presente, el Identificador PPK debe estar presente.
Identificador PPK	Introduzca el identificador PPK.
PPK obligatorio	Seleccione una de las opciones desplegables: • **Mandato**: La conexión VPN se establecerá correctamente si el servidor admite RFC 8784 o si acepta el identificador PPK especificado en el Identificador PPK. • **No mandato**: La conexión VPN no se establecerá si el servidor no admite RFC 8784 o no acepta el identificador PPK especificado en el Identificador PPK.
Algoritmo de cifrado	Seleccione una de las siguientes opciones: • **DES** • **3DES** • **AES-128** • **AES-256** (opción predeterminada) • **AES-128 GCM** • **AES-256 GCM**

Ajuste	Qué hacer
Algoritmo de integridad	Seleccione una de las siguientes opciones: • **SHA2-256** (opción predeterminada) • **SHA2-384** • **SHA2-512**
Grupo Diffie Hellman	Seleccione una de las siguientes opciones: • **1** • **2** (opción predeterminada) • **5** • **14** • **15** • **16** • **17** • **18**
Vigencia en minutos	Introduzca la vigencia SA (intervalo de reintroducción de clave) en minutos. Los valores válidos van del 10 al 1440.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

*Escriba $ para ver una lista de **variables** compatibles, si las hubiera, para este campo.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.6.18. VPN a petición

Aplicable a: dispositivos iOS

Mediante la configuración de VPN a petición se configura el acceso a un servidor VPN que se basa en dominios, nombres de host, etc.

Ajustes de VPN a petición

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Tipo de conexión Activar VPN a petición	Seleccione el tipo de VPN que quiere configurar. Los siguientes ajustes dependerán de esta selección. Seleccione esta opción si desea usar esta configuración para dominios y nombres de host que establecen una VPN a petición.
Activar las reglas de iOS (aplicable si se ha seleccionado VPN a petición)	En iOS y macOS, se pueden configurar: • Reglas de red que permitan o no permitan conexiones con (y permitan o ignoren) las redes consideradas verdaderas. • Reglas de conexión que permiten cuando sea necesario, o no permiten nunca, conexiones a las redes consideradas verdaderas. Para las reglas de redes, se pueden especificar los siguientes tipos de parámetros: • Coincidencia de dominio DNS • Coincidencia de dirección de servidor DNS • Coincidencia SSID • Sondeo de la cadena de la URL • Coincidencia del tipo de interfaz Para las reglas de conexión, se pueden especificar los siguientes tipos de parámetros: • Coincidencia de dominio DNS • Coincidencia de dirección de servidor DNS • Coincidencia SSID • Sondeo de la cadena de la URL • Coincidencia del tipo de interfaz • Nombre del dominio • Servidor DNS • Sondeos de URL
Tipo de proveedor (iOS 9+)	Seleccione uno de los siguientes proveedores de Tunnel: • proxy de la aplicación - redirecciona el tráfico en la capa de la aplicación. Consulte la **documentación de Apple** para obtener una descripción general del proveedor de proxy de la aplicación. • túnel del paquete - redirecciona el tráfico en la capa IP. Consulte la **documentación de Apple** para obtener una descripción general sobre el proveedor de Tunnel del paquete.
EnforceRoutes	Cuando está habilitado, las rutas no defectuosas de la VPN anulan las rutas definidas localmente. • Si IncludeAllNetworks está habilitado, el sistema no tiene en cuenta la configuración de las ejecutores • Disponible en iOS 14.2 y posterior

Ajuste	Qué hacer
ExcludeLocalNetworks	Cuando está habilitado junto con IncludeAllNetworks, todas las rutas de tráfico de red locales fuera de la VPN.
IncludeAllNetworks	Cuando está habilitado, enruta todo el tráfico a través de la VPN.

Los protocolos y sus ajustes se enumeran a continuación:

- **IPsec (Cisco)**
- **Cisco AnyConnect**
- **SSL de Juniper**
- **VPN de NetMotion**
- **F5 SSL**
- **SonicWALL Mobile Connect**
- **Aruba VIA**
- **SSL personalizada**
- **Palo Alto Networks GlobalProtect**

IPsec (Cisco)

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del equipo	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Incluir el PIN de usuario	Seleccione esta opción para solicitar un PIN al usuario.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. **Si selecciona Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* **Si selecciona Automática,** estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

Cisco AnyConnect

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Grupo	Introduzca el grupo que desea utilizar para autenticar la conexión.
Autenticación del usuario	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. **Si selecciona Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* **Si selecciona Automática,** estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

SSL de Juniper

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Dominio	Introduzca el dominio de autenticación que desea utilizar para autenticar la conexión.
Función	Introduzca la función de autenticación que desea utilizar para autenticar la conexión.
Autenticación del usuario	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. **Si selecciona Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* **Si selecciona Automática,** estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

VPN de NetMotion

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del usuario	El certificado es el método de autenticación del usuario. **Credencial**: Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

F5 SSL

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del usuario	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. **Si selecciona Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* **Si selecciona Automática,** estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

SonicWALL Mobile Connect

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Grupo o dominio de inicio de sesión	Introduzca el grupo de inicio de sesión o el dominio que desea utilizar para autenticar la conexión.
Autenticación del usuario	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. **Si selecciona Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* **Si selecciona Automática,** estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

Aruba VIA

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Autenticación del usuario	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. **Si selecciona Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* **Si selecciona Automática,** estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

SSL personalizada

Ajuste	Qué hacer
Identificador	Introduzca el identificador de este VPN SSL en formato DNS invertido (por ejemplo: com.miempresa.miservidor).
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Datos personalizados	Introduzca los pares clave-valor que definen los datos personalizados para esta VPN.
Autenticación del usuario	Solo se puede utilizar la autenticación mediante certificado.
Credencial	Seleccione el certificado de identidad que desea utilizar.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. **Si selecciona Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* **Si selecciona Automática,** estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

Palo Alto Networks GlobalProtect

Ajuste	Qué hacer
Servidor	Introduzca la dirección IP o el nombre de host para el servidor VPN.
Cuenta	Introduzca la cuenta de usuario que desea utilizar para autenticar la conexión.
Datos personalizados	Introduzca los pares clave-valor que definen los datos personalizados para esta VPN.
Autenticación del usuario	El certificado es el método de autenticación del usuario. Seleccione un certificado de identidad para usar en el campo **Credencial**.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. **Si selecciona Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* **Si selecciona Automática,** estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.

> Escriba $ para ver una lista de **variables** compatibles, si las hubiera, para este campo.

Para obtener más información, consulte **Cómo crear una configuración**

10.10.6.19. Configuración de Wi-Fi

Aplicable a:

- Android
- Windows
- iOS
- macOS
- watchOS
- visionOS
- tvOS

Esta sección contiene los siguientes temas:

Ajustes de Wi-Fi

- **Ajustes WEP, WPA/WPA2/WPA3 u otro (Personal)**
- **Ajustes WEP Enterprise, WPA/WPA2/WPA3 Enterprise u otro (Empresa)**
- **iOS, macOS y visionOS**

Ajustes de Wi-Fi

Mediante la configuración Wi-Fi se configura el acceso a una red inalámbrica.

> El usuario puede modificar algunos de los ajustes Wi-Fi en el dispositivo. No obstante, el servidor MDM puede recibir o no información sobre los cambios, lo cual dependerá del SO del dispositivo. Por lo tanto, no se volverán a insertar automáticamente las configuraciones en el dispositivo para anular la configuración del dispositivo con la configuración del servidor.

> La opción de delegación con distribución personalizada está disponible para esta configuración. Para obtener más información, consulte el tema *Distribuir la configuración* en **Trabajar con configuraciones**.

> Algunas versiones específicas de dispositivos Android pueden requerir que los administradores introduzcan el dominio e información adicional para conectarse a un TLS, TTLS, PEAP, etc. (WPA2) redes. Es recomendable que se asegure de que los cambios en la configuración Wi-Fi se realizan en los dispositivos seleccionados antes de realizar estos cambios en un conjunto mayor de dispositivos.

> Los dispositivos Android 14.x registrados en cualquier versión Ivanti Neurons for MDM anterior a la 94 tendrán el estado de configuración "Pendiente de instalar". Cuando se actualiza Ivanti Neurons for MDM a 94 sin editar la configuración Wi-Fi, el estado de la configuración permanece como "Pendiente de instalación". Debe activar el campo Dominio para EAP_PEAP y actualizar el Dominio y los Certificados en la configuración para actualizar el estado a "Instalado".

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Seleccione la configuración **Wi-Fi**.

3. Introduzca un **Nombre** para la configuración.
4. Introduzca una descripción.
5. Configure los ajustes de Wi-Fi según las siguientes descripciones.
6. Haga clic en **Siguiente**.
7. (solo macOS) En la página Distribución, seleccione una de las siguientes opciones de distribución:
    - Canal del dispositivo: la configuración es eficaz para todos los usuarios de un dispositivo; esta suele ser la opción más normal.
    - Canal del usuario: la configuración solo es eficaz para el usuario registrado actualmente en un dispositivo.
8. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - Personalizado.
9. Haga clic en **Hecho**.

La siguiente lista enumera los Ajustes de Wi-Fi:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Identificador de red (SSID)	Introduzca el nombre de la red inalámbrica en la que se aplican estos ajustes. Este campo distingue entre mayúsculas y minúsculas.
Unirse automáticamente	Seleccione si los dispositivos deben unirse automáticamente a la red Wi-Fi correspondiente. Si esta opción no está seleccionada, los usuarios de los dispositivos deben pulsar el nombre de la red en el dispositivo para unirse a ella.
Red oculta	Seleccione esta opción si el acceso a la red no está en emisión.
Desactivar detección de red cautiva (iOS 10+)	Sus administradores pueden activar o desactivar el modo de omisión cautivo Wi-Fi. Cuando Apple detecta la presencia de un portal cautivo, abre una pantalla de inicio de sesión para solicitar el acceso. Se puede desactivar la detección de portales cautivos, lo cual requerirá al usuario lanzar manualmente un explorador web que genera un inicio de sesión en el portal de la red cautiva. Este nuevo ajuste es útil cuando un portal cautivo ISE evita que aparezca la pantalla de inicio de sesión, lo cual hace creer a los usuarios que sus dispositivos no conectados en realidad si están conectados a Internet.
Configuración del proxy	Para configurar un proxy, seleccione **Manual** o **Automática**. Si selecciona **Manual,** estarán disponibles los siguientes campos adicionales: • **Servidor y puerto**: Introduzca la dirección de la red y el número de puerto asignado al servidor proxy.* • **Autenticación**: Introduzca un nombre de usuario válido si es necesario para conectarse al proxy.* • **Contraseña**: Introduzca una contraseña válida si es necesaria para conectarse al proxy.* Para eliminar el nombre de host añadido, haga clic en el icono 'menos'. Si selecciona **Automática,** estarán disponibles los siguientes campos adicionales: • **Dirección URL del servidor proxy**: Introduzca la dirección URL completa para el proxy.
Tipo de seguridad	Seleccione el método de seguridad necesario para acceder a la red: • Cualquiera (personal) • Cualquiera (empresa) • WEP • WEP Empresa • WPA • WPA Enterprise • WPA2 • WPA2 Enterprise • WPA3

Ajuste	Qué hacer
	• WPA3 Enterprise WPA3/WPA3 Enterprise es aplicable a iOS 13+. Windows admite WPA, WPA Enterprise, WPA2 y WPA2 Enterprise.

Ajustes WEP, WPA/WPA2/WPA3 u otro (Personal)

Ajuste	Qué hacer
Contraseña	(Opcional) Introduzca la contraseña para acceder a esta red. De lo contrario, se le pedirá al usuario del dispositivo la contraseña necesaria para acceder a la red.

Ajustes WEP Enterprise, WPA/WPA2/WPA3 Enterprise u otro (Empresa)

Ajuste	Qué hacer
Protocolos	
Tipos de EAP aceptados	Seleccione los tipos de EAP que pueden utilizarse para acceder a esta red: • TLS • TTLS: en el campo Identidad interior, seleccione uno de los protocolos de autenticación como SO predeterminado, PAP, CHAP, MSCHAP, MSCHAPv2 y EAP. • PEAP • LEAP (No es compatible con dispositivos inscritos en AMAPI) • EAP-SIM • EAP-AKA • EAP-FAST (No es compatible con dispositivos inscritos en AMAPI)
EAP-FAST	Seleccione la opción EAP-FAST que define los métodos de autenticación: • **Usar PAC:** seleccione esta opción para usar la autoconfiguración del proxy (PAC). • **PAC de aprovisionamiento:** Seleccione esta opción para permitir que se aprovisione la PAC. De lo contrario, solamente podrán utilizarse las PAC ya aprovisionadas en el dispositivo. Esta opción solamente está disponible si ha seleccionado Usar PAC. • **PAC de aprovisionamiento anónimo:** Seleccione esta opción para permitir que se aprovisione una PAC sin autenticar el servidor. Esta opción solamente está disponible si ha seleccionado PAC de aprovisionamiento.
Autenticación	
Nombre de usuario	Especifique el nombre de usuario requerido para acceder a la red. Si deja esta opción en blanco, se le solicitará al usuario del dispositivo.*
Usar contraseña por conexión	Seleccione esta opción para solicitar al usuario el dispositivo una contraseña cada vez que se conecte. Cuando el dispositivo vuelva a unirse a la misma red, se solicitará al usuario del dispositivo que vuelva a autenticarse para unirse a la red. Esta opción no es compatible con los dispositivos con AMAPI.
Contraseña	(Opcional) Introduzca la contraseña para acceder a esta red. De lo contrario, se le pedirá al usuario del dispositivo la contraseña necesaria para acceder a la red.
Certificado de identidad	(Opcional) Seleccione el certificado que se utilizará para la credencial de identidad. Mediante la configuración del **Certificado de identidad** se define cada certificado de identidad disponible.
Certificado de autenticación (disponible solo para dispositivos de Windows)	Seleccione una de las siguientes tres tiendas de certificados para elegir un certificado y conectarse a una red WiFi: • Equipo o usuario: si se selecciona esta opción y el usuario no ha iniciado sesión, el certificado de Autenticación se elegirá en el almacén de equipos. Si el usuario ha iniciado sesión, se elegirá el certificado específico desde el almacén de usuario. • Equipo: si se selecciona esta opción, el certificado de Autenticación se elegirá en el almacén de equipos.

Ajuste	Qué hacer
	• Usuario: si se selecciona esta opción, el certificado de Autenticación se elegirá en el almacén de usuarios. La opción de Usuario está seleccionada de forma predeterminada.
Identidad exterior	(Opcional) para TLS, TTLS, PEAP y EAP-FAST, seleccione esta opción para permitir a los usuarios de los dispositivos que oculten su identidad. El nombre real del usuario solo aparecerá dentro del túnel cifrado. Esta opción puede mejorar la seguridad porque un atacante no puede ver claramente el nombre del usuario de autenticación.
Dominio	Compatible cuando el tipo de EAP es TLS y TTLS.
Confiar	
Certificados de confianza (no compatible para los dispositivos inscritos en AMAPI)	Seleccione las casillas de verificación para seleccionar varios certificados de la lista.
Nombres de certificado del servidor de confianza	Haga clic en **+ Añadir** para introducir los nombres de uno o más certificados de confianza del servidor. (Opcional) Seleccione **Permitir excepciones de confianza** para permitir que el usuario tome decisiones de confianza en una ventana de diálogo.

iOS, macOS y visionOS

Ajuste	Qué hacer
Todas las versiones	
Tipo de red	Seleccione esta opción si la red debe ser tratada como: • estándar • punto de acceso heredado • Passpoint
Reserva PAC del proxy permitida	(Opcional) Permite al dispositivo conectarse directamente al destino si el archivo PAC no está disponible.
Modos de configuración (opcional)	Una matriz de cadenas que contiene el tipo de modo de conexión que se va a adjuntar. • Sistema: la Wi-Fi se conecta antes de que el usuario inicie sesión en el dispositivo. • Ventana de inicio de sesión: la Wi-Fi está disponible después de que el usuario inicie sesión en el dispositivo. Actualmente, los modos de configuración solo funcionan cuando están activados los modos de Windows de Sistema y de Inicio de sesión.
Ajustes de Passpoint	Aparecerán los ajustes de esta sección si ha seleccionado Passpoint para el Tipo de red.
Nombre del dominio	Introduzca el nombre de dominio que se utilizará para la negociación de Passpoint.
Conectarse a redes de Passpoint de socios de itinerancia	(Opcional) Seleccione esta opción para permitir conexiones a los proveedores de servicios de itinerancia internacional.
Identificadores de la organización del consorcio de itinerancia	(Opcional) Introduzca los identificadores asignados por IEEE a las entidades compatibles con este perfil de Wi-Fi.
Nombres de dominios del identificador del acceso a la red	(Opcional) Introduzca los nombres de dominios del identificador del acceso a la red que se utilizarán para la negociación de Passpoint.
Par MCC y MNC	(Opcional) Introduzca los pares Código móvil del país (MCC)/Código de red móvil (MNC) que se utilizarán para la negociación de Passpoint. Cada cadena debe contener seis dígitos exactamente.
Nombre del operador mostrado	(Opcional) Introduzca el nombre del operador de red que se mostrará.

Ajuste	Qué hacer
Cola rápida de Cisco QoS	Los ajustes de esta sección son aplicables a la configuración de cola rápida de Cisco. Entre los ajustes se incluyen el uso de listas de permitidos en aplicaciones para marcado L2 y L3, y si se desea poner en listas de permitidos el tráfico de audio y vídeo o los servicios de audio/vídeo integrados como FaceTime y llamadas por Wi-Fi.
Restringir marcado de QoS	Si no se selecciona esta opción, todas las aplicaciones utilizaran el marcado L2 y L3 cuando la red sea compatible con la cola rápida de Cisco QoS. Si se selecciona esta opción, utilice los ajustes de **Elegir aplicaciones** que aparecen para añadir las aplicaciones que desea incluir en el marcado L2 y L3. Todas las aplicaciones que no sean seleccionadas no utilizarán marcado L2 y L3.
Activar marcado de QoS	Desactiva el marcado L3 y solo utiliza marcado L2 para el tráfico enviado a la red Wi-Fi. Cuando no se seleccione, el sistema tratará el Wi-Fi como si no estuviera asociado a una red de cola rápida Cisco QoS.
Poner en la lista de permitidos las llamadas de audio/vídeo	Especifica si se desea poner en una lista de permitidos el tráfico de audio y vídeo de los servicios de audio/vídeo integrados como FaceTime y llamadas por Wi-Fi.
Elegir aplicaciones	Utilice esta opción para añadir las aplicaciones que desea incluir para el marcado L2 y L3. Todas las aplicaciones que no sean seleccionadas no utilizarán marcado L2 y L3.
iOS 10+	
Cola rápida de Cisco QoS	Los ajustes de esta sección son aplicables a la configuración de cola rápida de Cisco. Entre los ajustes se incluyen el uso de listas de permitidos en aplicaciones para marcado L2 y L3, y si se desea poner en listas de permitidos el tráfico de audio y vídeo o los servicios de audio/vídeo integrados como FaceTime y llamadas por Wi-Fi.
Restringir marcado de QoS	Si no se selecciona esta opción, todas las aplicaciones utilizaran el marcado L2 y L3 cuando la red sea compatible con la cola rápida de Cisco QoS. Si se selecciona esta opción, utilice los ajustes de **Elegir aplicaciones** que aparecen para añadir las aplicaciones que desea incluir en el marcado L2 y L3. Todas las aplicaciones que no sean seleccionadas no utilizarán marcado L2 y L3.
Activar marcado de QoS	Desactiva el marcado L3 y solo utiliza marcado L2 para el tráfico enviado a la red Wi-Fi. Cuando no se seleccione, el sistema tratará el Wi-Fi como si no estuviera asociado a una red de cola rápida Cisco QoS.
Poner en la lista de permitidos las llamadas de audio/vídeo	Especifica si se desea poner en una lista de permitidos el tráfico de audio y vídeo de los servicios de audio/vídeo integrados como FaceTime y llamadas por Wi-Fi.
Elegir aplicaciones	Utilice esta opción para añadir las aplicaciones que desea incluir para el marcado L2 y L3. Todas las aplicaciones que no sean seleccionadas no utilizarán marcado L2 y L3.
Supervisado por iOS 10.3+	

Ajuste	Qué hacer
Habilitar la lista de permitidos de Wi-Fi **iOS 14.0+ y macOS 15.0+**	Determina a qué redes de Wi-Fi se puede conectar el dispositivo. Si existen múltiples configuraciones de Wi-Fi, se aplicará la más restrictiva.
Desactivar la aleatorización de la dirección MAC **Android 11+**	En iOS 14.0+ y macOS 15.0+, Apple cambió el comportamiento predeterminado de un dispositivo que informa su dirección MAC de Wi-Fi para informar una dirección aleatoria para nuevas conexiones en lugar de la dirección MAC de Wi-Fi real del dispositivo. Como resultado, esta función puede causar un comportamiento inesperado para las empresas que utilizan portales cautivos o filtrado de direcciones MAC. Los administradores pueden **Desactivar la aleatorización de la dirección MAC** para una red Wi-Fi editando la configuración Wi-Fi asociada y activando esta opción (por defecto, falso). Esto causará que la configuración Wi-Fi se vuelva a insertar en todos los dispositivos. Esta opción muestra una advertencia de privacidad en los Ajustes del dispositivo que indica que la red tiene protecciones de privacidad reducidas. El usuario del dispositivo todavía puede activarlo o desactivarlo manualmente a través de los ajustes de su dispositivo.
Aleatorización de la dirección MAC	• Desactivado: la Wi-Fi se conecta antes de que el usuario inicie sesión en el dispositivo. • Activado: la Wi-Fi está disponible después de que el usuario inicie sesión en el dispositivo. • Activado: no persistente • Activado: persistente

Escriba $ para ver una lista de **variables** compatibles, si las hubiera, para este campo.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.7. Configuración de la red móvil

Esta sección contiene los siguientes temas:

- Configuración de APN
- Móvil
- Cellular Private Network Configuration.htmConfiguración de la red móvil privada
- Configuración de preajustes de iOS para Telecom
- Configuración de eSIM

10.10.7.1. Configuración de APN

Una configuración de APN ajusta el Nombre del punto de acceso del móvil para el dispositivo. Para iOS 7, utilice mejor la **configuración móvil**.

Ajustes APN

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Nombre del punto de acceso	Introduzca en nombre para el punto de acceso correspondiente. Por lo general, el nombre lo define el operador que proporciona el servicio.
Nombre del usuario del punto de acceso	Introduzca un nombre de usuario autorizado para este punto de acceso.*
Contraseña del punto de acceso	Introduzca la contraseña que corresponde al nombre de usuario introducido.
Servidor proxy y puerto	Introduzca la dirección IP o URL y el nombre del puerto del proxy APN.
EnableXLAT464	Seleccione la casilla para habilitar el Nombre de punto de acceso (APN, por sus siglas en inglés). Esta opción proporciona servicios de IPv4 a través de una una red solo IPv6.

> Escriba $ para ver una lista de **variables** compatibles, si las hubiera, para este campo.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.7.2. Móvil

Aplicable a: iOS 7.0+ and watchOS 10.0+

Esta sección contiene los siguientes temas:

- Ajustes móviles para la APN predeterminada
- Ajustes móviles para APN de datos
- Controlar el acceso móvil durante la itinerancia
- Controlar el acceso móvil

La configuración móvil configura el perfil móvil para un dispositivo. Configure los ajustes de red móvil en dispositivos con iOS 7.0+ o watchOS 10.0+. Algunas empresas tienen contratos con sus operadores de telefonía móvil, que les otorgan acceso a un Nombre de punto de acceso (APN) exclusivo para acceder a la red remotamente o para planes de facturación especiales. Consulte con su operador de telefonía móvil para ver los parámetros de configuración.

- Los perfiles móviles solo se pueden instalar de uno en uno.
- No se puede instalar un perfil móvil si ya hay instalado un perfil APN.

Puede configurar los ajustes móviles para los siguientes tipos de APN desde el cuadro desplegable **Tipos de APN configurada**:

- APN predeterminada y de datos
- APN predeterminadas
- APN de datos

Para todas las configuraciones, introduzca un nombre que identifique la configuración y una descripción opcional.

Ajustes móviles para la APN predeterminada

Ajustes de APN predeterminadas	Qué hacer
Nombre del APN	Introduzca en nombre para el punto de acceso correspondiente. Por lo general, el nombre lo define el operador que proporciona el servicio.
Tipo de autenticación APN	(Opcional) Seleccione una de las siguientes opciones: • CHAP (protocolo de autenticación por desafío mutuo) • PAP (protocolo de autenticación de contraseña)
Nombre de usuario	(Opcional) Introduzca un nombre de usuario que se utilizará para la autenticación.
Contraseña	(Opcional) Introduzca una contraseña que se utilizará para la autenticación.

Ajustes móviles para APN de datos

Ajustes de APN de datos	Qué hacer
Nombre del APN	Introduzca en nombre para el punto de acceso correspondiente. Por lo general, el nombre lo define el operador que proporciona el servicio.
Tipo de autenticación APN	(Opcional) Seleccione una de las siguientes opciones: • CHAP (protocolo de autenticación por desafío mutuo) • PAP (protocolo de autenticación de contraseña)
Nombre de usuario	(Opcional) Introduzca un nombre de usuario que se utilizará para la autenticación.
Contraseña	(Opcional) Introduzca una contraseña que se utilizará para la autenticación.
Servidor proxy	Especifique el servidor proxy.
Puerto del servidor proxy	Especifique el puerto del servidor proxy.
10.3+	
Máscara permitida del protocolo	Seleccione IPv4, IPv6 o ambos.
Máscara permitida del protocolo en itinerancia nacional	Seleccione IPv4, IPv6 o ambos.
Máscara permitida del protocolo en itinerancia	Seleccione IPv4, IPv6 o ambos.

Controlar el acceso móvil durante la itinerancia

Se puede limitar el acceso de algunas o todas las aplicaciones administradas a los datos móviles mientras el dispositivo está en itinerancia.

Procedimiento

1. Vaya a la pestaña **Configuraciones** en el menú de navegación principal de Ivanti Neurons for MDM.
2. Haga clic en **+Añadir**.
3. Introduzca **Rojo** en el campo de búsqueda y luego haga clic en configuración de **Uso de la red**.
4. Seleccione la casilla **No permitir para todas las aplicaciones administradas** para bloquear que las aplicaciones administradas puedan acceder a los datos móviles durante la itinerancia o en todo momento.
5. Deje la casilla sin seleccionar para poder especificar las aplicaciones administradas por nombre o Id. de paquete que desea bloquear para que no reciban datos móviles.
6. Use los menús desplegables en el campo Aplicaciones para buscar una aplicación por su nombre o Id. de paquete.

Controlar el acceso móvil

Se puede limitar el acceso de algunas o todas las aplicaciones administradas a los datos móviles en cualquier momento. Las aplicaciones se podrán seguir usando de forma limitada, pero no tendrán acceso a los datos móviles.

Procedimiento

1. Vaya a la pestaña **Configuraciones** en el menú de navegación principal de Ivanti Neurons for MDM.

2. Haga clic en **+Añadir**.
3. Introduzca **Rojo** en el campo de búsqueda y luego haga clic en configuración de **Uso de la red**.
4. Seleccione la casilla **No permitir para todas las aplicaciones administradas** para bloquear que las aplicaciones administradas puedan acceder a los datos móviles en cualquier momento.
5. Opcionalmente, también puede dejar la casilla sin seleccionar para poder especificar las aplicaciones administradas que desea bloquear para que no reciban datos móviles.
6. Use los menús desplegables en el campo Aplicaciones para buscar una aplicación por su nombre o Id. de paquete.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.7.3. Configuración de la red móvil privada

Ivanti Neurons for MDM permite a la carga útil de configuración de Red privada móvil proporcionar información del dispositivo sobre los despliegues de redes privadas, incluida la ubicación geográfica, la preferencia sobre Wi-Fi y el tipo de despliegue de la red.

Aplicable a

iOS 17.0 hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Busque y seleccione la configuración de **Red de móvil privada**.
3. Configure los ajustes de **Red móvil privada** según la tabla siguiente:

Ajuste	Descripción
Nombre,	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Datos móviles preferidos	Seleccione la casilla para activar y utilizar los datos móviles a través de Wi-Fi.
NR Independiente	Seleccione la casilla si la red de datos móviles tiene NR 5G Standalone.
Nombre del conjunto de datos	Especifique el Nombre del Conjunto de datos que se identifica con esta configuración.
Número de versión	Especifique el número de versión del conjunto de datos para realizar un seguimiento de las actualizaciones del sistema.
Geovallas	Especifique la Latitud, Longitud y Radio de cada Geo ID para desplegar una red privada en una ubicación geográfica. Puede crear una lista de hasta mil geovallas para redes privadas.

4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Seleccione una de las opciones de distribución para establecer la configuración de **Red móvil privada**. Para más información sobre la configuración de las opciones de distribución, consulte **Trabajar con configuraciones**.
6. Haga clic en **Hecho**.

10.10.7.4. Configuración de preajustes de iOS para Telecom

Mediante la configuración de preajustes de iOS para Telecom se establecen los valores predeterminados para las restricciones de itinerancia internacional y de cobertura personal.

Configuración de preajustes de iOS para Telecom

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Permitir a los dispositivos usar el servicio de voz durante la itinerancia	Seleccione esta opción para habilitar la itinerancia de voz. La disponibilidad de la itinerancia de voz dependerá del operador.
Permitir a los dispositivos usar el servicio de datos durante la itinerancia	Seleccione esta opción para habilitar la itinerancia de datos. Al habilitar la itinerancia de datos, también se habilitará itinerancia de voz en el dispositivo.
Permitir a los usuarios activar la cobertura personal	Seleccione esta opción para habilitar la característica de cobertura personal. La disponibilidad de esta característica dependerá del operador.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.7.5. Configuración mejorada de segmentación de red 5G

Ivanti Neurons for MDM proporciona una configuración de segmentación de red 5G mejorada para configurar segmentaciones de red 5G para Android, lo que permite a los operadores de redes móviles asignar segmentos de red 5G dedicados, o "segmentos", para agrupar diferentes aplicaciones con necesidades similares, como baja latencia o alto ancho de banda, en un segmento específico para una mejor optimización de los recursos de la red. Esto permite que los administradores de MDM y los proveedores de red administren las porciones directamente para lograr un mejor rendimiento de la aplicación.

Características principales

1. **Red dedicada**: en lugar de que todas las aplicaciones compartan una única porción de red, la segmentación de red permite que distintas aplicaciones utilicen su propia porción de red adaptada a sus requisitos específicos.

2. **Personalización**: El administrador puede configurar cómo se asignan las aplicaciones a segmentos de red específicos según sus requisitos individuales; por ejemplo, garantizar una baja latencia para aplicaciones de comunicación en tiempo real o un alto ancho de banda para servicios de transmisión como YouTube. Una porción diseñada para juegos de alto rendimiento puede priorizar una baja latencia, mientras que una para transmisión multimedia estaría optimizada para un alto ancho de banda.

3. **Participación del socio**: esta característica a menudo requiere la colaboración con proveedores de red, que definen estas porciones de red e informan a los administradores de MDM sobre la lista de porciones y su importancia.

Creación de una configuración mejorada de segmentación de red 5G

Procedimiento

1. **Agregar configuración**

- Vaya a **Configuraciones >> +Agregar**. Se muestra la página **Agregar configuración**.
- Introduzca **Segmentación de red mejorada** en la barra de búsqueda para configurar Segmentación de red mejorada. Se muestra la página **Crear configuración de segmentación de red mejorada**.
- Haga clic en **+Agregar descripción** para introducir una descripción de la configuración.

2. **Configurar la aplicación**

- En **Configuración >> Catálogo de aplicaciones**, introduzca el nombre de la aplicación deseada.
- Haga clic en **Agregar manualmente** si la aplicación no está disponible en Play Store o App Store.
- Introduzca **ID de paquete** y seleccione el **segmento de red** adecuado en el menú desplegable.
- Seleccione la porción deseada en el menú desplegable **Seleccionar porción**.
- Haga clic en **Agregar**. La aplicación ahora aparecerá en **Configurar segmentos de red** debajo del segmento de red seleccionado.
- Para eliminar una aplicación, haga clic en **Eliminar** en la sección **Configurar porción de red**.

3. **Distribuir configuración**

- Haga clic en **Siguiente**, seleccione o desmarque la casilla de verificación "**Habilitar esta configuración**", elija una opción de distribución (Todos los dispositivos, Sin dispositivos o Personalizada),
- Haga clic en **Listo** para completar la configuración.

Configuración mejorada de segmentación de red para Lockdown y Kiosko

La creación de una configuración de segmentación de red 5G mejorada le permite configurar dispositivos para que funcionen de manera restringida, lo que garantiza que los usuarios solo tengan acceso a aplicaciones y configuraciones específicas.

En los siguientes bloqueos, hay una casilla de verificación "**Habilitar segmentación de red 5G**":

- **Perfil de trabajo**: En los dispositivos propiedad de los empleados con un perfil de trabajo configurado con Android Enterprise versión 12.0, la casilla de verificación "Habilitar segmentación de red 5G" se puede encontrar en **Ajustes de configuración > Configuración de bloqueo del perfil de trabajo**.
- **Dispositivo administrado con perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa**: En Dispositivo administrado con perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa con versiones de Android 12.0 tenemos la casilla de verificación "Habilitar segmentación de red 5G".

Esta es una configuración heredada que permite que los dispositivos utilicen la segmentación de red 5G. Su correlación con la nueva configuración de Segmentación de red 5G mejorada es la siguiente:

Si se aplica alguno de los bloqueos anteriores a un dispositivo y la opción *Habilitar segmentación de red 5G* **no** está seleccionada, la configuración *Segmentación de red 5G mejorada* fallará con un error.

Ejemplos

- **Caso 1**: Si el bloqueo del dispositivo no se distribuye y la configuración de segmentación de red mejorada se distribuye, se activará la configuración mejorada.
- **Caso 2**: Si el bloqueo del dispositivo está distribuido pero la casilla de verificación 5G no está seleccionada (falso), la configuración de red 5G mejorada generará un error.
- **Caso 3**: Si se distribuye primero la segmentación de red mejorada, seguida del bloqueo del dispositivo con la casilla de verificación habilitada, la configuración de la segmentación de red mejorada seguirá funcionando. De lo contrario, se producirá un error.

Detalles de configuración:

- Si el bloqueo del dispositivo se distribuye y se envía/distribuye la configuración de segmentación de red mejorada, los usuarios deben asegurarse de que la casilla de verificación Habilitar segmentación de red 5G esté habilitada para evitar errores.
- Si la casilla de verificación no está habilitada y se envía la configuración, se generará un error en el dispositivo.

10.10.7.6. Configuración de eSIM

La configuración de la eSIM configura la red celular en los dispositivos con el comando RefreshCellularPlans. Los administradores deben obtener la URL del operador de la eSIM antes de asignar la red celular al dispositivo.

[Compatible con: Android 15+, iOS, iPadOS y Windows 11

Procedimiento para dispositivos Android 15+

1. Vaya a **Configuraciones** > **+Agregar.**
2. Escriba eSIM en el campo de búsqueda y, a continuación, haga clic en la configuración de **eSIM**.
3. Introduzca un Nombre y Descripción de la configuración.
4. En la lista de la **plataforma**, seleccione **Android**.
5. En la sección **Configuración**, introduzca la **URL del operador**.
6. **Habilitar automáticamente**: seleccione esta opción para descargar el perfil de eSIM y habilitarlo en el dispositivo de forma automática. Si no se selecciona esta opción, se descargará el perfil de eSIM, pero no se habilitará en el dispositivo de forma automática.

> Esta opción NO está disponible para dispositivos en modo de perfil de trabajo.

7. Seleccione y distribuya la configuración mediante una de las siguientes opciones de distribución:
   - Todos los dispositivos
   - Ningún dispositivo (predeterminada)
   - personalizada
8. Haga clic en **Hecho**.

EID para dispositivos Android 13+

La opción **EID de solicitud** ahora está disponible en la página Detalles del dispositivo y lista Dispositivos. Esta opción solo es compatible con los dispositivos compatibles con eSIM en los modos perfil de trabajo, dispositivo gestionado de trabajo y perfil de trabajo en dispositivo propiedad de la empresa. Si se registra un dispositivo, el EID se seleccionará de forma automática para el dispositivo registrado y se mostrará en la página Detalles del dispositivo. Si no es así, este campo se habilitará y puede solicitar el EID haciendo clic en **Solicitar EID**. También puede exportar EID utilizando la opción **Exportar a CSV** desde la página Lista de dispositivos.

> En la página **Detalles del dispositivo**, la opción **Solicitar EID** está disponible para dispositivos Android 13+ con Ivanti Go R122 o versiones posteriores.

Mantener el plan de datos eSIM (compatible con iOS 11+ y Android 15.0+): al intentar borrar un dispositivo inscrito con una configuración eSIM, la acción **Borrar dispositivo** incluye una opción adicional para conservar el plan de datos. Si selecciona **Mantener el plan de datos eSIM (compatible con iOS 11+ y Android 15.0+)** y, a continuación, hace clic en **Borrar**, el plan de datos eSIM existente se conservará mientras se eliminan todos los demás datos del dispositivo. Puede acceder a esta opción desde la página **Detalles del dispositivo** o seleccionando el dispositivo, abriendo el menú **Acciones** y haciendo clic en **Borrar**.

Procedimiento para dispositivos iOS y iPadOS

1. Vaya a **Configuraciones** > **+Agregar.**
2. Escriba eSIM en el campo de búsqueda y, a continuación, haga clic en la configuración de eSIM.

3. Introduzca un Nombre y Descripción de la configuración.
4. Seleccione **iOS/iPadOS**.
5. Escriba la URL del Operador.
6. Haga clic en **Siguiente**.
7. Seleccione la opción Habilitar esta configuración.
8. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - personalizada
9. Haga clic en Hecho.

Procedimiento para dispositivos Windows 11

1. Vaya a **Configuraciones** > **+Agregar.**
2. Escriba eSIM en el campo de búsqueda y, a continuación, haga clic en la configuración de eSIM.
3. Introduzca un Nombre y Descripción de la configuración.
4. En la sección Elegir SO, haga clic en **Windows**.
5. En la sección Configuración, escriba la URL del operador en el cuadro de texto Nombre del servidor (en formato FQDN).
    - ¿Es un servidor de detección? Seleccione esta opción para marcar el servidor como detectable.
    - Habilitación automática: seleccione esta opción para habilitar el perfil en el dispositivo una vez descargado.
6. Haga clic en **Siguiente**.
7. Seleccione la opción Habilitar esta configuración.
8. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - personalizada
9. Haga clic en **Hecho**.

Restablecer eSIM a estado de fábrica (solo para dispositivos Windows 11)

Esta opción está disponible en la sección Detalles del dispositivo de todos los dispositivos. Al hacer clic en esta opción se eliminan todos los perfiles eSIM descargados en el dispositivo.

Notas importantes: Aplicable solo para la configuración de eSIM de Windows

>

- Cuando se registra un dispositivo, la **sección Detalles del** dispositivo muestra ahora si el dispositivo es compatible con eSIM o no con **ESIM.Capaz**de . Para los dispositivos compatibles con eSIM, los detalles del identificador eSIM respectivo también se muestran en **ESIM.Identificadores**.
- Cuando se borra y vuelve a inscribir un dispositivo Ivanti Neurons for MDM , el registro antiguo de este dispositivo (con el estado como Borrado) se debe eliminar de la página Dispositivos para evitar problemas de aprovisionamiento con la configuración de eSIM en este dispositivo vuelto a inscribir.

- Al volver a enviar la misma configuración a un dispositivo que ya ha descargado los perfiles, no se pueden descargar nuevamente los perfiles. Si el administrador desea que el dispositivo descargue los perfiles nuevamente, primero restablezca el módulo eSIM al estado de fábrica y luego se recomienda enviar/reenviar la configuración de eSIM.
- Cuando se aprovisiona correctamente una configuración de eSIM en un dispositivo, antes de retirar el dispositivo, el administrador debe realizar la acción de borrado de eSIM para garantizar que los perfiles de eSIM descargados se borren del dispositivo.
- La eliminación de la configuración de eSIM solo eliminará la configuración del dispositivo. Si se detectaron, descargaron y activaron perfiles eSIM en el dispositivo, dichos dispositivos permanecerán activos hasta que se realice un borrado de eSIM.
- Al realizar una acción de borrado de eSIM se eliminan todos los perfiles de eSIM descargados del dispositivo. No obstante, la configuración de eSIM que está en estado Instalado permanece intacta en el dispositivo. Para eliminar la configuración del dispositivo, el administrador debe no distribuir la configuración ESIM.

10.10.8. Otra configuración

Esta sección contiene los siguientes temas:

- Configuración de dominios asociados
- Configuración de la transferencia de archivos de Android
- Configuración de Apple TV
- Configuración de AirPlay
- Duplicación AirPlay
- Ajustes del navegador
- Configurar el modo Single App para iOS
- Configurar un perfil de MDM en iOS
- Configurar un perfil de MDM en macOS
- Caché de contenidos
- Crear un acceso directo de Android
- Ajustes del nombre del dispositivo
- Configuración de Ethernet (macOS)
- Configuración de la integración de servidores EMA
- Configuración del fondo de pantalla del dispositivo
- Configuración del mensaje de la pantalla de bloqueo
- Crear configuración de salva pantallas
- Configurar el salvapantallas del usuario
- Configuración de las extensiones del sistema de macOS
- MAM solo
- Configuración Google Play administrada
- Ajustes del asistente de migración
- Configuración de las notificaciones
- Ajustes de la impresora
- Configuración para eliminar el «bloatware»
- Configuración de las restricciones de teléfonos Samsung
- Configuración del modo Single-App
- Menú Inicio y Barra de tareas
- Configuración de la actualización del sistema
- Administración de actualización de Windows
- Programación de aplicaciones Windows
- Configuración del BIOS de Windows
- BitLocker de Windows
- Configuración del kiosco de Windows

- Configuración de la licencia de Windows
- Configuración de la cadencia de recomendación de actualizaciones de software

10.10.8.1. Configuración de dominios asociados

Licencia: Gold

La configuración de dominios asociados es un diccionario que asigna las aplicaciones a sus dominios asociados. Los dominios asociados se pueden usar con funciones como AppSSO extensible, enlaces universales y Autorrellenado de contraseñas.

Los ajustes de los dominios asociados son los siguientes:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Identificador de la aplicación	(Requerido) El identificador de la aplicación con el que asociar los dominios.
Dominios asociados	(Requerido) Los dominios con los que asociar la aplicación. Cada cadena de texto tiene el formato "service:domain". Los dominios deben ser nombres de host totalmente cualificados, como www.ejemplo.com.
Habilitar la descarga directa	Si es cierto, los datos de este dominio se descargarán directamente en lugar de utilizar un CDN. El valor de derechos para este dominio se debe ajustar como service:domain?mode=managed o se ignorará el valor. Disponible en macOS 11 y posterior. **Predeterminado**: falso

10.10.8.2. Configuración de la transferencia de archivos de Android

Como parte de Android 11, Google introdujo cambios significativos en el acceso al almacenamiento en un dispositivo desde las aplicaciones, lo que también afectó a la forma en que las empresas gestionan el envío de archivos a aplicaciones específicas en estos dispositivos. Teniendo en cuenta estos cambios, muchas grandes empresas se enfrentan a retos a la hora de distribuir archivos a dispositivos y aplicaciones a medida que los dispositivos se actualizan a Android 11 y versiones posteriores. Cualquier enfoque que dependa de API específicas de los proveedores de hardware limita a las empresas a la hora de tener el mismo enfoque en diferentes dispositivos de distintos fabricantes y versiones de SO.

Ivanti ha desarrollado una solución de transferencia de archivos que es agnóstica para la versión de Android y el proveedor de hardware. Esta solución se basa en la capacidad estándar de Android *Content-Provider* . *Content-Provider* permite a la aplicación Go de Ivanti generar una ubicación única en el dispositivo para cada archivo enviado a través de UEM.

La configuración de transferencia de archivos está disponible para dispositivos de Android en modo de dispositivo totalmente gestionado. Mediante esta configuración, el administrador puede proporcionar una opción para transferir archivos en el dispositivo para ser compartidos entre diferentes aplicaciones permitidas presentes en el mismo dispositivo. Otras aplicaciones pueden utilizar los archivos para lo que necesiten. Un ejemplo de uso es inicializar la configuración de la aplicación mediante JavaScript o mostrar información corporativa mediante PDF o vídeos. Cada archivo cargado en las configuraciones de transferencia de archivos de Ivanti es descargado por Ivanti Go cuando recibe la configuración correspondiente y el archivo asociado. El archivo se almacena de forma segura en Ivanti Go.

Otras aplicaciones no pueden acceder a este archivo de manera arbitraria.

Cada archivo descargado dentro del sandbox de la aplicación está referenciado por una ubicación única, también denominada *ContentURI* o *URI*. Los atributos personalizados se utilizan para mantener el valor ContentURI en el servidor para cada archivo en un dispositivo y pueden ayudar a los administradores a determinar la disponibilidad de un archivo en el dispositivo, formar grupos de dispositivos dinámicos, y son necesarios para comunicar ContentURI a la aplicación de destino utilizando la configuración de aplicaciones gestionadas, etc.

> En el caso de aplicaciones que no sean de Ivanti, los administradores deben consultar a los desarrolladores de aplicaciones de terceros sobre su compatibilidad con este enfoque, comúnmente denominado "Consumir ContentURI basado en FileProvider".

Requisitos previos:

- Añade un nuevo atributo personalizado basado en el dispositivo que se utilizará para la operación de transferencia de archivos. Para cada configuración de transferencia de archivos, debe crearse un único atributo personalizado. Cada atributo de dispositivo personalizado puede almacenar únicamente el contentURI (ubicación del archivo) del dispositivo para un archivo por config.

Procedimiento

1. Vaya a **Configuraciones** > **Agregar configuración** > **Transferencia de archivos**. Se abre la página **Crear configuración de transferencia de archivos** .
2. Introduzca un nombre para la configuración en el cuadro **Nombre**.
3. Introduzca una **Descripción** de la configuración.
4. **Establecimiento de la configuración**
   En la sección **Archivo a transferir**, seleccione los archivos a transferir mediante la opción de arrastrar y soltar o navegando a través de la opción **Elegir archivo** . Por defecto, el límite máximo de tamaño de los archivos es de 50 MB.

5. Seleccione una o más de las opciones siguientes para **Descargar en los dispositivos** (opcional):
    - **Permitir descarga en una red con contador**: seleccione esta opción para continuar descargando el archivo incluso en una red con contador.
    - **Requerir carga**: seleccione esta opción para asegurarse de que el dispositivo se está cargando durante el proceso de transferencia de archivos.
    - **Requerir dispositivo inactivo**: seleccione esta opción para mantener el dispositivo inactivo durante el proceso de transferencia de archivos.
6. Utilice una de las dos opciones siguientes para compartir un archivo con otras aplicaciones
    - **Transferencia mediante la configuración de aplicaciones administradas de Android**: utilice esta opción solo si la aplicación de destino puede consumir URI de contenido mediante la Configuración de aplicaciones administradas.
    - **Transferencia mediante intención en el dispositivo**: las intenciones son específicas de cada aplicación. Para compartir un archivo mediante esta opción, consulte la documentación de la aplicación de destino y proporcione información en la sección de intenciones que aparece a continuación. Intents permite a la aplicación Ivanti Go emitir un mensaje en el dispositivo una vez que el archivo está disponible para ser compartido con las aplicaciones.

Transferencia mediante Configuración de aplicaciones administradas de Android

Procedimiento

1. En el campo **Elegir un atributo personalizado basado en un dispositivo existente para compartir este archivo con otras aplicaciones**, introduzca un nombre de atributo existente, por ejemplo, **Custom-Filename**. Para obtener más información, consulte Asignar atributos personalizados a los dispositivos.
2. El nombre del atributo personalizado debe ser un atributo nuevo y único que se utilice exclusivamente para esta operación de transferencia de archivos. Cada atributo de dispositivo personalizado puede almacenar únicamente el contentURI (ubicación del archivo) del dispositivo para un archivo por config.
   Proporcione acceso a las siguientes aplicaciones o nombres de paquetes: puede seleccionar nombres de aplicaciones en el selector Nombres de aplicaciones y añadir Nombres de paquetes.

> Estos serán los únicos paquetes autorizados que podrán acceder al archivo.

- **Nombres de la aplicación**: puede seleccionar nombres de aplicaciones desde el selector Nombres de la aplicación.
- **Nombres de paquetes**: puede introducir los ID de grupo en esta zona, por ejemplo,Separe los nombres de varios paquetes con punto y coma (;).

```bash
com.mobileiron.filetransfer.android3.
```

Haga clic en **Guardar**. La nueva configuración de Transferencia de archivos aparece en la página Configuraciones.

Configuración de la aplicación de destino

Procedimiento

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Seleccione la aplicación de destino que recibirá el archivo.

3. Vaya a **Configuración de aplicaciones > Configuraciones gestionadas para Android**.
4. Cree una nueva configuración o utilice una configuración existente.
5. Una aplicación puede tener un ajuste como "Información de manifiesto" u otras propiedades en las que el administrador puede definir la variable de sustitución y comunicar la ubicación del archivo a la aplicación de destino. Para la aplicación Ivanti Velocity como ejemplo, en el cuadro de diálogo Configuración de aplicaciones > **Obtener configuraciones > Campo Información del manifiesto**, introduzca la variable de sustitución. Por ejemplo, $Custom-File-Name$.
   Seleccione la distribución.
6. Haga clic en **Guardar**.

Transferencia mediante intención en el dispositivo

Procedimiento

1. En el campo **Elegir un atributo de dispositivo existente para pasar la ruta del archivo en los extras de intents,** introduzca un nombre de atributo personalizado nuevo, por ejemplo, deviceIntentURI.
2. Los atributos personalizados se utilizan para mantener el valor de ubicación (URI / ContentURI) en el servidor para cada dispositivo y pueden ayudar a los administradores a determinar la disponibilidad de un archivo en el dispositivo. Para obtener más información, consulte Asignar atributos personalizados a los dispositivos.
   En el campo **Proporcionar acceso a un nombre de aplicación o paquete específico**, introduzca el **Nombre de la aplicación** o el **Nombre del pquete**, por ejemplo, Velocity.

> Estos serán los únicos paquetes autorizados que podrán acceder al archivo.

3. En la sección Intents-Standard, proporcione los detalles siguientes:
   - **Tipo de operación**: en la lista desplegable, seleccione **Iniciar actividad** / **Iniciar servicio** u otra opción similar según la aplicación. Elija el valor correcto para este campo en función de la orientación del desarrollador de la aplicación de destino o consulte la documentación de la aplicación de destino.
   - **Nombre de clase** (opcional): elija el valor correcto para este campo en función de la orientación del desarrollador de la aplicación de destino o consulte la documentación de la aplicación de destino.
   - **Acción**: ajuste la acción a:o similar, según la aplicación.

     Bash

     ```
     com.wavelink.nameofapp.action.INSTALL_CONFIG
     ```

   - **Categoría**: introduzca valores separados por punto y coma (;).
   - **Tipo de MIME** (opcional): en el servidor host del administrador, el archivo custom.mobileconfig debe ser configurado con un tipo MIME de application/x-apple-aspen-config para que el perfil MDM del dispositivo se descargue e instale en el dispositivo. Elija el valor correcto para este campo en función de la orientación del desarrollador de la aplicación de destino o consulte la documentación de la aplicación de destino.
   - **Indicadores** (opcional): seleccione el número de indicadores a utilizar. Elija el valor correcto para este campo en función de la orientación del desarrollador de la aplicación de destino.

Proporcione los valores **Intents-Extras** con KEY, TYPE y VALUE (opcional). Para parámetros más específicos, consulte la documentación de la aplicación OEM. Elija el valor correcto para este campo en función de la orientación del desarrollador de la

aplicación de destino o consulte la documentación de la aplicación de destino.

5. Haga clic en **Guardar**.
6. En la página Configuraciones, seleccione la nueva Configuración de transferencia de archivos y, a continuación, seleccione **Acciones** > **Aplicar a etiqueta**. Se abre el cuadro de diálogo **Aplicar a etiqueta** .
7. Seleccione la Etiqueta adecuada y haga clic en **Aplicar**.
   La transferencia/compartición de archivos con otras aplicaciones solo puede verificarse recopilando registros de la aplicación de destino o del dispositivo.

Verificación del estado de la descarga de archivos

Los atributos personalizados se utilizan para mantener el valor de ubicación (ContentURI) en el servidor para cada dispositivo y pueden ayudar a los administradores a determinar la disponibilidad de un archivo en el dispositivo.

Procedimiento

1. Vaya a **Dispositivos** >**Dispositivos**.
2. Seleccione un dispositivo específico en el que se haya desplegado la configuración de transferencia de archivos.
3. En la página Detalles del dispositivo, seleccione el dispositivo y, a continuación, **Acciones** > **Forzar registro del dispositivo**.
4. En la pestaña Configuraciones, compruebe que la configuración de Transferencia de archivos se muestra con el estado **Aplicada**.
5. En la pestaña Atributos personalizados, compruebe que aparece el nombre del nuevo atributo personalizado (por ejemplo, "Custom-File-Name$") con su valor correspondiente. Esto proporciona la información sobre la ubicación de almacenamiento del archivo en el dispositivo y muestra que el archivo se ha descargado localmente en el dispositivo disponible dentro del sandbox de la aplicación Ivanti Go.
   La transferencia/compartición de archivos con otras aplicaciones solo puede verificarse recopilando registros de la aplicación de destino o del dispositivo.

10.10.8.3. Configuración de Apple TV

Licencia: Silver

La configuración de la Apple TV define el idioma y la configuración regional para la Apple TV.

Los ajustes de Apple TV son los siguientes:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Idioma	Introduzca el código del idioma de dos caracteres para especificar el idioma de la IU.
Configuración regional	Introduzca la Id. de la configuración regional para especificar la combinación de país/idioma para la IU.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.8.4. Duplicación AirPlay

Licencia: Gold

Duplicación AirPlay es una característica que le ofrece la posibilidad de visualizar la pantalla de un dispositivo iOS en un monitor mediante Apple TV. Tanto la Apple TV como el dispositivo iOS deben estar conectados a la misma red de Wi-Fi. Esta función requiere los siguientes dispositivos:

- Dispositivos iOS 7 y posteriores - supervisados
- Dispositivos macOS 10.10 y posteriores - supervisados
- Versión de Apple TV - supervisada
- AirPlay

> El cambio para incluir la administración de dispositivos que no sean iOS no se puede revertir.

Esta sección contiene los siguientes temas:

- **Configurar Apple AirPlay**
- **Configurar AirPlay en el dispositivo móvil**
- **Configurar un monitor para que funcione con Apple TV**
- **Conectar su dispositivo iOS a la Apple TV**

Configurar Apple AirPlay

Para ver más información sobre los ajustes de configuración de AirPlay, consulte **Configuración de AirPlay**.

Procedimiento

1. Vaya a **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Haga clic en **AirPlay**.
4. Introduzca un Nombre y una Descripción para la configuración en los campos adecuados.
5. Para todas las versiones admitidas de iOS, introduzca un Nombre del dispositivo y una Contraseña.
6. Haga clic en **Añadir** para añadir otro dispositivo, si fuera necesario.
7. Opcionalmente, para los dispositivos iOS 7+ supervisados o macOS 10.10+ añada las ID de los dispositivos a una lista de permitidos.
8. Haga clic en **Siguiente**.
9. Elija un nivel de distribución.
10. Haga clic en **Hecho**.

Configurar AirPlay en el dispositivo móvil

Procedimiento

1. Configure **Apple Configurator**.
2. Vaya a **Dispositivos > Dispositivos**.

3. Haga clic en el nombre de un dispositivo iOS para mostrar la página de Detalles de dicho dispositivo.
4. Haga clic en el icono ⋮.
5. Seleccione **Duplicación AirPlay** para visualizar el diálogo de duplicación AirPlay.
6. Seleccione un dispositivo Apple TV del menú desplegable.
7. Introduzca un tiempo de escaneado en segundos para especificar un límite de tiempo durante el que buscar el dispositivo que ha seleccionado.
8. Introduzca la contraseña del dispositivo Apple TV.
9. Haga clic en **Enviar solicitud**.

Configurar un monitor para que funcione con Apple TV

Procedimiento

1. En un monitor conectado a Apple TV, vaya a **Ajustes > Perfil** .
2. Seleccione **Configurador de Apple para Ivanti Neurons for MDM**.
3. Haga clic en **Añadir perfil**.
4. Haga clic en el icono ⋮.
5. Seleccione **Duplicación AirPlay** para visualizar el diálogo de duplicación AirPlay.
6. Seleccione un dispositivo Apple TV del menú desplegable.
7. Introduzca un tiempo de escaneado en segundos para especificar un límite de tiempo durante el que buscar el dispositivo que ha seleccionado.
8. Introduzca la contraseña del dispositivo Apple TV.
9. Haga clic en **Enviar solicitud**.

Conectar su dispositivo iOS a la Apple TV

Procedimiento

1. Conecte el dispositivo Apple TV a un monitor.
2. Con el control remoto de Apple TV, vaya a **Ajustes > Cuentas > Compartir en casa** para activar Compartir en casa.
3. **Conecte el dispositivo iOS** a la misma red Wi-Fi que su **dispositivo Apple TV**.
4. Abra la aplicación remota en su dispositivo **iOS**.
5. Active **Compartir en casa** desde la pantalla **Ajustes remotos**.

10.10.8.5. Ajustes del navegador

Mediante la configuración de los Ajustes del navegador, puede configurar ajustes y restricciones para Google Chrome, Mozilla Firefox, , Microsoft Edge e Internet Explorer en dispositivos Windows 10.

Esta característica requiere Bridge. Vaya a **Ivanti Bridge** para obtener más información.

> Asegúrese de que los navegadores estén instalados en el dispositivo antes de aplicar la configuración del navegador.

Para configurar los ajustes del navegador:

1. Vaya a **Configuración > +Añadir**.
2. Seleccione la configuración de los **Ajustes del navegador**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. En la sección Establecimiento de la configuración, especifique los demás ajustes según se describe en la siguiente tabla.

Ajuste	Qué hacer
Navegadores	Seleccione el tipo de navegador para el que se requieren los ajustes: • **Chrome** • **Firefox** • **Microsoft Edge** • **Internet Explorer**
Ajustes del navegador	Configure las siguientes opciones: **Permitir navegadores**: • Permitir guardado de contraseñas • Permitir el modo navegación segura • Permitir que los plug-ins obsoletos sigan en el navegador **Chrome y Firefox**: • **Permitir borrado del historial del navegador** **Chrome e Internet Explorer**: • **Permitir impresión del navegador** • **URL de la página de la pestaña nueva** **Solo Chrome**: • **Mostrar accesos directos a aplicaciones en la barra de marcadores** • **Mostrar botón de inicio** • **Permitir sincronización de los datos con Google** • **Seguir ejecutando aplicaciones en segundo plano cuando Chrome esté cerrado** **Solo Firefox**: • **Permitir instalación de extensiones** **Solo Internet Explorer**: • **Permitir descarga de datos desde sitios web**
Favoritos del navegador	Haga clic en **+Añadir**. Aparecerá la ventana **Añadir favoritos del navegador**. Configure los siguientes campos: • **Mostrar nombre**: escriba el nombre en pantalla del favorito. • **URL**: escriba la URL del favorito del navegador. Haga clic en **Añadir**. Los detalles del favorito del navegador añadido se muestran en la página. En la columna **Acciones**, haga clic en el icono de Editar para editar el ajuste. Para eliminar el favorito del navegador, haga clic en el icono de Eliminar. **Nombre de la carpeta de favoritos del navegador**: escriba el nombre de la carpeta de favoritos del navegador donde quiera que se guarden los favoritos. También puede añadir los favoritos del navegador en formato CSV. Para cargar en formato CSV: 1. Haga clic en Cargar archivo CSV. Busque y elija el archivo CSV que quiera cargar. 2. Haga clic en **Cargar**. Los detalles del archivo CSV deben añadirse siguiendo este formato:

Ajuste	Qué hacer
	• La primera columna (Nombre en pantalla) debe especificar el nombre en pantalla del favorito. Ejemplo: «cesta de la compra». • Segunda columna (URL) debe especificar la URL del favorito. Ejemplo: «https://amazon.com».
Seguridad del sitio web	Configure las siguientes opciones de seguridad del sitio web: **Todos los sitios web (Chrome y Firefox)** • **Bloquear cookies** • **Bloquear Javascript** • **Bloquear plugins** • **Bloquear ventanas emergentes** Sitios web específicos (solo Chrome) **Sitios web bloqueados (Chrome y Edge)**: agregue el sitio web que desee a la Lista de sitios bloqueados. Haga clic en **+Añadir**. Aparecerá la ventana **Añadir sitio web a la lista de bloqueados**. En **URL del sitio web**, escriba la URL del sitio web que desee añadir a la lista de bloqueados. En el campo **Acceso**, seleccione **Bloquear** para añadir el sitio web a la lista de bloqueados. La opción predeterminada es **Permitir**. Haga clic en **Añadir**.
Extensiones del navegador	**Tipos de extensión permitidas (solo Chrome)**: seleccione cualquiera de las opciones siguientes: • **Extensión** • **Secuencia de comandos del usuario** • **Temas** • **Aplicación empaquetada** • **Aplicación alojada** • **Aplicación de la plataforma** **Fuentes de extensiones del explorador (solo Chrome)**: Haga clic en **+Añadir** para añadir orígenes de las extensiones del navegador. Una vez añadidos los orígenes de la extensión del navegador, puede editar o eliminar los orígenes haciendo clic en las opciones relevantes en la columna de **Acciones**. **Forzar la instalación de extensiones (solo Chrome)**: Haga clic en **+Añadir** para añadir extensiones de instalación obligatoria. Una vez añadidas las extensiones de instalación obligatoria, puede editar o eliminar los orígenes haciendo clic en las opciones relevantes en la columna de **Acciones**.

6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones de distribución:
   - Todos los dispositivos
   - Ningún dispositivo (predeterminada)
   - personalizada
8. Haga clic en **Hecho**.

10.10.8.6. Configurar el modo Single App para iOS

Licencia: Silver

El modo single-app restringe el uso de la aplicación especificada por parte de los dispositivos iOS y tvOS . Por ejemplo, es posible que quiera configurar dispositivos que solo puedan usar una aplicación personalizada desarrollada por su organización.

Procedimiento

1. Vaya a **Configuraciones > Añadir > Modo Single App**.
2. Siga las siguientes pautas para definir la aplicación y los ajustes relacionados.
3. Haga clic en **Siguiente**.

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Elegir aplicación	Seleccione el método a usar para seleccionar la aplicación: • **Desde el Catálogo de aplicaciones y las aplicaciones del sistema**: seleccione esta opción para buscar en el catálogo de aplicaciones de Ivanti Neurons for MDM y las aplicaciones del sistema (preinstalado en dispositivos Apple de forma predeterminada). • Introduzca el nombre de la aplicación y selecciónelo cuando aparezca en la lista de aplicaciones. • **Introducir la ID del paquete:** seleccionar para introducir un identificador único para la aplicación del sistema que desee seleccionar. Utilice esta opción si no puede encontrar la aplicación del sistema mediante la opción **Desde el App Catalog y aplicaciones del sistema**.
Desactivar uso táctil	Seleccione esta opción para desactivar la pantalla táctil.
Desactivar rotación del dispositivo	Seleccione esta opción para desactivar la detección de rotación del dispositivo.
Desactivar botones de volumen	Seleccione esta opción para desactivar los botones de volumen del dispositivo.
Desactivar interruptor del timbre	Seleccione esta opción para desactivar el interruptor del timbre del dispositivo.
Desactivar botón activo/inactivo	Seleccione esta opción para desactivar el botón activo/inactivo del dispositivo (arriba a la derecha en el borde del dispositivo).
Desactivar bloqueo automático	Seleccione esta opción para evitar que el dispositivo entre el modo inactivo después de un periodo de inactividad.
Activar voz en off	Seleccione esta opción para habilitar el lector de la pantalla con la voz en off (característica de accesibilidad).
Activar zoom	Seleccione esta opción para habilitar el zoom (característica de accesibilidad).
Activar invertir colores	Seleccione esta opción para habilitar el ajuste inversión de colores (característica de accesibilidad).
Activar toque auxiliar	Seleccione esta opción para habilitar AssistiveTouch (característica de accesibilidad).
Activar Reproducir	Seleccione esta opción para habilitar Reproducir selección (característica de accesibilidad).

Ajuste	Qué hacer
selección	
Activar audio mono	Seleccione esta opción para alternar entre audio estéreo y mono (característica de accesibilidad).
Ajustes de la voz en off	Seleccione esta opción para permitir a los usuarios realizar ajustes en la voz en off.
Ajustes del zoom	Seleccione esta opción para permitir a los usuarios realizar ajustes en el zoom.
Ajustes de Invertir colores	Seleccione esta opción para permitir a los usuarios invertir los colores.
Ajustes de toque auxiliar	Seleccione esta opción para permitir a los usuarios realizar ajustes en AssistiveTouch.

4. En la pantalla **Distribución**, seleccione los grupos dispositivos que recibirán esta configuración.
5. Haga clic en **Hecho**.

Si ha configurado el marcador del teléfono como la aplicación a usar, el botón Inicio funciona cuando el dispositivo entra en modo de aplicación única.

10.10.8.7. Configurar un perfil de MDM en iOS

La configuración de MDM en iOS define los límites del acceso de Ivanti Neurons for MDM. Hay dos tipos de configuraciones de MDM en iOS:

- **MDM de iOS - aprovisionado en masa:** para los dispositivos que compra la empresa y se aprovisionan como parte de una distribución en masa.
- **MDM de iOS - aprovisionado individualmente:** para los dispositivos aprovisionados uno a uno. No se aplicará a los dispositivos supervisados y con inscripción de usuarios.

Se proporciona y se permite uno para cada tipo en todos los espacios de los dispositivos.

Editar una configuración de MDM en iOS

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Vaya a **Configuraciones**.
3. Seleccione la configuración de MDM de iOS que desea editar.
4. Haga clic en el icono del lápiz (editar) para editar la configuración.
5. Siga las siguientes pautas para realizar los cambios:
6. Haga clic en **Hecho**.

Ajuste	Qué hacer
Derechos de acceso de MDM	
Permitir bloqueo del dispositivo y eliminación de contraseña	Deje esta opción sin seleccionar para evitar que se aplique una configuración de cumplimiento del código de acceso.
Permitir borrado del dispositivo	Deje esta opción sin seleccionar para evitar que se aplique una acción de borrado del dispositivo.
Permitir consulta de información de red (números de teléfono/SIM, direcciones MAC)	Deje esta opción sin seleccionar para que el dispositivo no envíe informes con información sobre redes. Si esta opción queda sin seleccionar, en la vista Lista de dispositivos y la vista Detalles de dispositivos aparecerá N/A en la información de redes que se deje de notificar. Además, la política de itinerancia no se podrá aplicar en los dispositivos afectados.
Contraseña de eliminación del perfil	
Contraseña para eliminar el perfil	Especifique una contraseña. Se indicará al usuario que debe introducir la contraseña para eliminar un perfil del dispositivo.
Añadir la aplicación requerida (iOS 15+)	
Añadir por búsqueda	Introduzca el nombre de la aplicación y busque la aplicación en la App Store y seleccione la aplicación deseada. Solo se puede añadir una aplicación a la vez. Al seleccionar una aplicación se desactivan las demás.
Añadir manualmente	Introduzca el ID de iTunes de la aplicación.

Los cambios se aplican solo a los dispositivos que se aprovisionen después de hacer el cambio.

10.10.8.8. Configurar un perfil de MDM en macOS

La configuración de MDM en macOS define los límites del acceso de Ivanti Neurons for MDM. Las configuraciones de MDM en macOS se aprovisionan individualmente para los dispositivos aprovisionados uno a uno.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Vaya a **Configuraciones**.
3. Seleccione la configuración de MDM de macOS que desea editar.
4. Haga clic en el icono del lápiz (editar) para editar la configuración.
5. Siga las siguientes pautas para realizar los cambios:
6. Haga clic en **Hecho**.

Ajuste	Qué hacer
Permitir bloqueo del dispositivo y eliminación de contraseña	Deje esta opción sin seleccionar para evitar que se aplique una configuración de cumplimiento del código de acceso.
Permitir borrado del dispositivo	Deje esta opción sin seleccionar para evitar que se aplique una acción de borrado del dispositivo.
Permitir consulta de información de red (números de teléfono/SIM, direcciones MAC)	Deje esta opción sin seleccionar para que el dispositivo no envíe informes con información sobre redes. Si esta opción queda sin seleccionar, en la vista Lista de dispositivos y la vista Detalles de dispositivos aparecerá N/A en la información de redes que se deje de notificar. Además, la política de itinerancia no se podrá aplicar en los dispositivos afectados.
Contraseña de eliminación del perfil	
Contraseña para eliminar el perfil	Especifique una contraseña. Se indicará al usuario que debe introducir la contraseña para eliminar un perfil del dispositivo.

Los cambios se aplican solo a los dispositivos que se aprovisionen después de hacer el cambio.

10.10.8.9. Caché de contenidos

Licencia: Gold

Aplicable a: macOS 10.13.4 o versiones más recientes compatibles.

Configurar el servicio de caché de contenidos para permitir las copias locales del software de App Store y habilitar a los clientes conectados para poder descargar el software y las aplicaciones con mayor rapidez.

Configuración de caché de contenidos

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **caché** en el campo de búsqueda y, a continuación, haga clic en la configuración de **Caché de contenido**.
4. Introduzca un nombre y describa la configuración.
5. Introduzca los **ajustes de la configuración de caché de contenidos**.
6. Haga clic en **Siguiente**.
7. Seleccione la opción **Habilitar esta configuración**.
8. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - personalizada
9. Haga clic en **Hecho**.

Ajustes de la configuración de caché de contenidos

Utilice los ajustes de la siguiente tabla para configurar la caché de contenidos. Para obtener más información sobre estos ajustes, consulte **Documentación de Apple**.

Ajuste	Descripción
Permitir que el sistema depure automáticamente el contenido de la memoria caché (Disponible en macOS 10.15 o en versiones más recientes compatibles.	Permitir que el sistema depure automáticamente el contenido de la memoria caché cuando necesite espacio en disco para otras aplicaciones (por ej. cuando quede poco espacio libre en el disco del equipo). De forma predeterminada, esta opción está activada.
Permitir el almacenamiento personal	Almacenar en la caché los datos de iCloud del usuario. Puede que los clientes les lleve un tiempo (horas o días) reaccionar a los cambios en este ajuste; no tiene un efecto inmediato. De forma predeterminada, esta opción está activada.
Permitir el caché compartido	Contenido de caché que no es de iCloud, como actualizaciones de software y aplicaciones. Puede que a los clientes les lleve un tiempo (horas, días) reaccionar a los cambios en este ajuste; no tiene un efecto inmediato. De forma predeterminada, esta opción está activada.
Permitir la activación automática de la memoria caché del contenido	Activar automáticamente el caché de contenidos cuando sea posible e impedir que sea desactivado.
Permitir la activación automática de la caché anclada (Disponible en macOS 10.15.4 o en versiones más recientes compatibles	Activar automáticamente el uso compartido de la conexión a Internet cuando sea posible e impedir la desactivación de este.
Desactiva el almacenamiento en caché anclado	Deshabilita el almacenamiento en caché anclado. La opción Deshabilita el almacenamiento en caché anclado anula la opción Permitir la activación automática de la caché anclada.
Límite de caché	Cantidad máxima de bytes de espacio en el disco que se utilizará para la caché de contenidos. Si el valor es 0, significa que el espacio en el disco es ilimitado. Valor predeterminado: 0
Ruta de datos	La ruta al directorio utilizada para almacenar el contenido en la caché. Si cambia manualmente este ajuste, el contenido en la caché no se trasladará automáticamente de la ubicación anterior a la nueva. Para trasladar contenidos automáticamente, utilice el panel Caché de contenidos de la preferencia del Uso compartido. El valor debe ser (o terminar con) /Library/Application Support/Apple/AssetCache/Data.
Permitir alertas de visualización (Disponible en macOS	Caché de contenidos muestra condiciones excepcionales (alertas) como notificaciones del sistema en la esquina superior de la pantalla.

Ajuste	Descripción
10.15 o en versiones más recientes compatibles.	
Mantener el dispositivo despierto (Disponible en macOS 10.15 o en versiones más recientes compatibles.	Evita que el equipo esté en suspensión mientras la Caché de contenidos esté activada (Preferencias del sistema > Uso compartido > Almacenamiento en caché de contenido activado).
Escuchar rangos	Un conjunto de diccionarios que describen un intervalo de direcciones IP de clientes a las cuales brindar servicio.
Primera dirección IP	Primera dirección IP de los clientes en los Rangos de escucha.
Última dirección IP	Última dirección IP de los clientes en los Rangos de escucha.
Tipo de dirección IP	Seleccione una de las siguientes opciones: • IPv4 (predeterminado) • IPv6
Permitir solo rangos de escucha	El caché de contenidos brinda contenido únicamente a los clientes de los Rangos de escucha.
Permitir escuchar con pares y primaria	El caché de contenidos proporciona contenido a los clientes en la unión de los Rangos de escucha, Rangos de escucha de pares y Primaria. De forma predeterminada, esta opción está activada.
Permitir solo subredes locales	El caché de contenidos ofrece contenido únicamente a los clientes en la misma red local inmediata. No se ofrece contenido a los clientes en otras redes accesibles para la caché de contenidos. Si se activa esta opción, se ignorará Escuchar rangos. De forma predeterminada, esta opción está activada.
Identidad del cliente del registro	La caché de contenidos registra la dirección IP y el número de puerto de los clientes que solicitan contenido.
Política de selección primaria	Seleccione una de las siguientes opciones de la directiva: • Primera disponible • URL ruta hash • Round-robin (predeterminado) • Aleatorio • Sticky - Disponible
Primaria	Un conjunto de las direcciones IP locales de otros tipos de caché de contenidos de los que esta caché debe descargar o a los que debe realizar cargas, en lugar de descargar de Apple o cargar en Apple directamente. Haga clic en **+ Añadir** para añadir una dirección IP o varias.

Ajuste	Descripción
Permitir solo subredes locales de pares	La caché de contenidos solo se empareja con otros tipos de caché de contenidos en la misma red local inmediata, en lugar de hacerlo con los que usan la misma dirección IP pública que el dispositivo. De forma predeterminada, esta opción está activada.
Puerto	Número de puerto de TCP en el que la caché de contenidos acepta solicitudes de descargas o cargas. Configure el puerto en 0 para elegir un puerto disponible aleatorio. Valor predeterminado: 0
Rangos públicos	Un conjunto de diccionarios que describen un rango de direcciones IP públicas que los servidores en Ivanti Neurons for MDM pueden usar para coincidir a los clientes con los almacenamiento de contenido en caché.
Primera dirección IP	Primera dirección IP de los servidores en los Rangos públicos.
Última dirección IP	Última dirección IP de los servidores en los Rangos públicos.
Tipo de dirección IP	Seleccione una de las siguientes opciones: • IPv4 (predeterminado) • IPv6

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.8.10. Crear un acceso directo de Android

Los accesos directos solo están disponibles en el modo kiosco utilizando un explorador que esté en la lista de permitidos. El explorador debe estar en la lista de permitidos en la

configuración de Bloqueo y Kiosco. Los accesos directos aparecerán en el iniciador de Kiosko de Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones**. **> +Añadir**
2. Haga clic en **Acceso directo de Android** para mostrar la página **Crear configuración de accesos directos de Android**.
3. Introduzca un nombre para la configuración en el campo **Nombre**.
4. Introduzca una breve descripción para la configuración en el campo **Descripción**.
5. Introduzca una etiqueta única para el acceso directo del campo **Etiqueta**.
6. Introduzca una URL para el destino del acceso directo del campo **URL**.
7. Alternativamente, arrastre y suelte un archivo en el campo de icono o haga clic en **Seleccionar archivo** para acceder al archivo y seleccionar un icono para el acceso directo.
8. Haga clic en **Siguiente**.

10.10.8.11. Creación de configuraciones de ajustes de accesibilidad

Esta configuración permite a las empresas restringir, realizar cambios o configurar los ajustes de accesibilidad en los dispositivos Apple.

Procedimiento

1. Vaya a **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Haga clic en **Configuración de ajustes de accesibilidad**.
4. Configure los ajustes especificados de la siguiente tabla:

Ajuste	Qué hacer
Nombre,	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Seleccione uno de los ajustes de accesibilidad	• **Ajustes de accesibilidad**: utilícelo para configurar los ajustes de accesibilidad en los dispositivos macOS. • **Restricciones en los ajustes de accesibilidad**: utilice esto para restringir los cambio que se pueden realizar a los ajustes de accesibilidad en los dispositivos iOS.
Ajustes de accesibilidad	**Establecimiento de la configuración**
Cerrar vista de punto lejano	El nivel mínimo de zoom en los ajustes de zoom
Cerrar vista de punto cercano	El nivel máximo de zoom en los ajustes de zoom
	Activar "Usar gesto de desplazamiento" en las opciones de zoom
	Activar "Suavizar imágenes" en las opciones de zoom
Valor de contraste	Especifique el valor
	Marque la casilla: Activar el "Flash de la pantalla" en las opciones de Audio
	Marque la casilla: Activar teclas del ratón en las opciones ratón y panel táctil.
Tamaño del cursor	Especifique el valor
	Marque la casilla: Ignorar panel táctil integrado
Retraso inicial del controlador del ratón	Especifique el valor
Velocidad máxima del controlador del ratón	Especifique el valor
Activar "Tecla lenta" en las opciones del teclado	Marque la casilla
Habilitar "Sonido de teclas pulsadas" para teclas lentas	Marque la casilla
Retraso de teclas lentas	Marque la casilla
Especifique el valor en milisegundos	Marque la casilla
Marque la casilla: Reproducir audio estéreo como mono	Marque la casilla
Activar las teclas especiales en las opciones del teclado	Marque la casilla

Ajuste	Qué hacer
Habilitar el pitido cuando una tecla modificadora se establece para teclas especiales	Marque la casilla
Activar la visualización en pantalla de las teclas pulsadas para las teclas especiales	Marque la casilla
Activar voz en off	Marque la casilla
Activar la inversión de colores en las adaptaciones de pantalla	Marque la casilla
Restricciones de accesibilidad	**Establecimiento de la configuración**
Activar texto en negrita	Marque la casilla
Activar el aumento del contraste	Marque la casilla
Activar movimiento reducido	Marque la casilla
Reducir la transparencia	Marque la casilla
Accesibilidad al tamaño del texto aplicación que admite el uso de texto dinámico	Seleccione la opción en la lista desplegable.
Habilitar adaptaciones táctiles	Marque la casilla
Activar voz en off	Marque la casilla
Activar zoom	Marque la casilla

5. Seleccione la opción de distribución y especifique la información necesaria según corresponda.
6. Haga clic en **Hecho**.

10.10.8.12. Crear configuración de salva pantallas

La configuración del Salva pantallas le permite agregar opciones como Contraseña, Tiempo de inactividad, ruta y nombre del módulo.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Haga clic en **Configuraciones**.
3. Haga clic en +**Añadir**.
4. Escriba pantalla en el campo de búsqueda y haga clic en **Salva pantallas**:
   Aparecerá la página de detalles de la Configuración del crear salvapantallas.
5. Configure los ajustes en esta página. Consulte la tabla de la sección **Ajustes de la configuración del salvapantallas** para obtener ayuda acerca de los valores.
6. Haga clic en **Siguiente** para configurar los ajustes de distribución y, a continuación, haga clic en **Hecho**.

Configuración de salva pantallas

Ajuste	Qué hacer
Nombre (obligatorio)	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Casilla Solicitar contraseña	Marque la casilla para pedir al usuario del dispositivo la contraseña cuando se desbloquee o se detenga el salvapantallas. (Disponible en macOS 10.13 y posterior).
Notificar del retraso de contraseña	Especifique la duración del retraso en segundos.
Tiempo de inactividad de la ventana de inicio de sesión	Especifique, en segundos, el tiempo de inactividad tras el cual debe aparecer el salvapantallas.
Ruta del módulo de salvapantallas	Especifique la ruta de acceso al módulo del salvapantallas
Nombre del módulo del salvapantallas (obligatorio)	Introduzca el nombre del salvapantallas.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.8.13. Configurar el salvapantallas del usuario

La configuración del Salvapantallas del usuario le permite agregar opciones como Contraseña, Tiempo de inactividad, ruta y nombre del módulo.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Haga clic en **Configuraciones**.
3. Haga clic en +**Añadir**.
4. Escriba "pantalla" en el campo de búsqueda y haga clic en **Salvapantallas del usuario**:
   Aparecerá la página de detalles de la Configuración del crear salvapantallas del usuario.
5. Configure los ajustes en esta página. Consulte la tabla del tema **Ajustes de la configuración del salvapantallas del usuario** para obtener ayuda acerca de los valores.
6. Haga clic en **Siguiente** para configurar los ajustes de distribución y, a continuación, haga clic en **Hecho**.

Ajustes de configuración del salvapantallas del usuario

Ajuste	Qué hacer
Nombre (obligatorio)	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Tiempo de inactividad	Especifique, en segundos, el tiempo de inactividad tras el cual debe aparecer el salvapantallas.
Ruta del módulo de salvapantallas	Especifique la ruta de acceso al módulo del salvapantallas
Nombre del módulo del salvapantallas (obligatorio)	Introduzca el nombre del salvapantallas.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.8.14. Ajustes del nombre del dispositivo

Licencia: Silver

Una configuración de nombre de dispositivo predeterminado le permite crear una nueva configuración que se envía al dispositivo en el nivel de registro o tras el registro y permite asignar un nombre al dispositivo.ç El administrador puede definir los nombres de dispositivos predeterminados solo para **dispositivos de iOS 8 supervisados**. Puede usar las siguientes variables para construir el nombre del dispositivo:

- Número de serie del dispositivo
- IMEI del dispositivo
- Modelo del dispositivo
- Ivanti Neurons for MDM Nombre de usuario (solo usuario locales)
- Unidad organizativa (OU) de LDAP
- Nombre común (CN) de LDAP

Por ejemplo, introduciría $-$ para los nombres de dispositivos que comiencen por el número de serie del dispositivo y terminen con la organización del usuario, según se define en el LDAP.

Ajustes predeterminados del nombre del dispositivo (para iOS)

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Nombre del dispositivo	Introduzca el formato del nombre del dispositivo predeterminado, incluido el dispositivo disponible y los atributos de LDAP.* Si el nombre resultante del dispositivo tiene más de 63 caracteres, se acortará para garantizar que aparece correctamente en el dispositivo.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.

> Escriba $ para ver una lista de **variables** compatibles, si las hubiera, para este campo.

Ajustes del nombre del dispositivo (Android)

El nombre del dispositivo Android se puede recuperar con Go app. Cuando el administrador genera el informe de Detalles del dispositivo, se muestra el nombre del dispositivo real en lugar del nombre del modelo o del fabricante del dispositivo. En caso de que el usuario cambie el nombre del dispositivo, el nuevo nombre se mostrará la siguiente vez que se genere el informe. El nombre de dispositivo respectivo se puede ver en **Dispositivos** > **Ajustes** > **Nombre del dispositivo**.

10.10.8.15. Configuración del fondo de pantalla del dispositivo

Licencia: Silver

La configuración del fondo de pantalla del dispositivo define una imagen de fondo de pantalla predeterminada para la pantalla de inicio y la pantalla de bloqueo de Android 7.0, en dispositivos con modo de Propietario del dispositivo o dispositivo propiedad de la empresa (COPE) habilitados, no se incluyen los dispositivos con modo EPO de Android 11.

Configuración de fondo de pantalla Android

Para definir una imagen de fondo de pantalla predeterminada para dispositivos Android:

1. Vaya a **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Haga clic en **Fondos de pantalla del dispositivo**.
4. Haga clic en el icono de Android para ver la sección Ajuste de la configuración y configure los siguientes ajustes
5. Haga clic en **Siguiente**.

Ajuste	Qué hacer
Nombre,	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Cargar fondo de pantalla de Android	
Usar la misma imagen para la pantalla de inicio y la pantalla de bloqueo	Seleccione esta opción para cargar una sola imagen para ambas pantallas.
Pantalla de inicio	Arrastre y suelte el archivo de la imagen o haga clic en **Elegir archivo** para seleccionar uno.
Pantalla de bloqueo	Arrastre y suelte el archivo de la imagen o haga clic en **Elegir archivo** para seleccionar uno.

6. Seleccione una de las siguientes opciones de distribución:

- **Todos los dispositivos**
- **Ningún dispositivo** (predeterminada)
- **Personalizado**

7. Haga clic en **Hecho**.

> La imagen cargada debe estar en formato .jpg o .png.

Configuración de fondo de pantalla iOS

Puede definir una imagen de fondo de pantalla predeterminada para dispositivos iOS.

> Este ajuste solo se puede aplicar a dispositivos supervisados.

1. Vaya a **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Haga clic en **Fondos de pantalla del dispositivo**.
4. Haga clic en el icono de iOS para ver la sección Ajuste de la configuración de iOS y configure los siguientes ajustes
5. Haga clic en **Siguiente**.

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Cargar fondo de pantalla de iPhone	
Usar la misma imagen para la pantalla de inicio y la pantalla de bloqueo	Seleccione esta opción para cargar una sola imagen para iPhone.
Pantalla de inicio	Arrastre y suelte el archivo de la imagen o haga clic en **Elegir archivo** para seleccionar uno.
Pantalla de bloqueo	Arrastre y suelte el archivo de la imagen o haga clic en **Elegir archivo** para seleccionar uno.
Cargar fondo de pantalla de iPad	
Usar la misma imagen para la pantalla de inicio y la pantalla de bloqueo	Seleccione esta opción para cargar una sola imagen para iPad.
Pantalla de inicio	Arrastre y suelte el archivo de la imagen o haga clic en **Elegir archivo** para seleccionar uno.
Pantalla de bloqueo	Arrastre y suelte el archivo de la imagen o haga clic en **Elegir archivo** para seleccionar uno.

6. Seleccione una de las siguientes opciones:

- **Todos los dispositivos**
- **Ningún dispositivo** (predeterminada)
- **Personalizado**

7. Haga clic en **Hecho**.

> Las imágenes que se carguen deben ser de 640 × 1136 píxeles y estar en formato .jpg o .png.

Ajustes de fondo de pantalla macOS

Para definir una imagen de fondo de pantalla predeterminada para dispositivos macOS:

1. Vaya a **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Haga clic en **Fondos de pantalla del dispositivo**.
4. Haga clic en el icono de macOS para ver la sección de ajustes de configuración para macOS.
5. Introduzca la ruta de acceso a la imagen del escritorio.
6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones:
    - **Todos los dispositivos**
    - **Ningún dispositivo** (predeterminada)
    - **Personalizado**
8. Haga clic en **Hecho**

> Se pueden cambiar los fondos de pantalla según la restricción. Si macOS tiene activa la restricción de la configuración **Permitir la modificación del fondo de pantalla**, puede modificar el fondo de pantalla.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.8.16. Configuración de la integración de servidores EMA

La configuración de la integración del servidor EMA permite que los dispositivos Windows 10 se vinculen con el servidor EMA de Intel configurado. Para vincular dispositivos con el servidor EMA de Intel configurado, debe proporcionar el directorio de instalación del agente EMA original y cargar el archivo.msh del agente EMA desde el nuevo servidor EMA.

Esta característica requiere Bridge. Vaya a **Bridge** para obtener más información.

Procedimiento

1. Vaya a **Configuración > +Añadir**.
2. Seleccione la configuración de la **Integración del servidor EMA**.
3. Introduzca el nombre para la configuración.
4. En la sección Ajuste de la configuración, haga clic en **Elegir archivo** para seleccionar el archivo.msh del agente de EMA.

> El archivo msh es un archivo de política de agente que se puede descargar desde el servidor EMA.

5. En el campo **Directorio de instalación del agente de EMA** original, escriba la ubicación donde está instalado el archivo original de EmaAgent.exe.
6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones de distribución:
   - Todos los dispositivos
   - Ningún dispositivo (predeterminada)
   - personalizada
8. Haga clic en **Hecho**.

10.10.8.17. Configuración de ahorro de energía

Ivanti Neurons for MDM activa la configuración de ahorro de energía para la carga útil que utiliza para configurar los ajustes de ahorro de energía en dispositivos Windows y macOS.

Disponible para:

- Windows 10 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- macOS 10.7 hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Busque y seleccione la configuración de **Ahorro de energía**.
3. En la sección Elegir sistema operativo, seleccione **Windows** o **macOS** y haga clic en **Siguiente**.
4. Haga clic en **+ Añadir descripción** para introducir una breve descripción de la configuración.
5. Para Windows, configure los siguientes ajustes de **Ahorro de energía**:
   - **Dispositivo con batería**
   - **El dispositivo está enchufado**
6. Configure los ajustes siguientes de **Ahorro de energía**:
   - **Ajustes de ahorro de energía CA del equipo de escritorio**
   - **Programar los ajustes de arranque o apagado del equipo**
   - **Ajustes de ahorro de energía CA del portátil**
   - **Ajustes de ahorro de energía de la batería del portátil**
7. Haga clic en **Siguiente** para configurar los ajustes de distribución.
8. Seleccione una de las opciones de distribución para establecer la configuración de **Ahorro de energía**. Para más información sobre la configuración de las opciones de distribución, consulte **Trabajar con configuraciones**.
9. Haga clic en **Hecho**.

Configuración de ahorro de energía de Windows

Cuando se aplica una nueva configuración de ahorro de energía a un dispositivo o cuando se modifican los ajustes de configuración de ahorro de energía existentes, los usuarios deben reiniciar sus dispositivos para que los cambios surtan efecto.

Dispositivo con batería

Utilice las configuraciones de ahorro de energía siguientes en la tabla cuando el dispositivo esté funcionando con la batería:

Ajuste	Descripción
Umbral de batería para activar el ahorro de energía	Cuando el dispositivo esté usando la batería, introduzca el nivel de carga de la batería para activar el Ahorro de energía; puede introducir valores de 0 a 100. Introduzca un valor porcentual que indique el nivel de carga de la batería. Por ejemplo, cuando se establece en 80, Energy Saver se activa cuando la batería tiene un 80 % de carga o menos carga disponible. Si no introduce un valor, Ivanti Neurons for MDM no cambia ni actualiza esta configuración. De forma predeterminada, Windows lo configurará al 70 %.
Cuando la tapa está cerrada	• **No realizar ninguna acción**: el dispositivo permanece encendido y continúa usando la batería. • **Suspender**: el dispositivo entra en modo de suspensión y utiliza una pequeña cantidad de carga de la batería. El equipo todavía está encendido y las aplicaciones y archivos abiertos se almacenan en la memoria de acceso aleatorio (RAM). • **Estado de suspensión de hibernación**: el dispositivo entra en modo de hibernación. Las aplicaciones y los archivos abiertos se almacenan en el disco duro y el dispositivo se apaga. • **Apagar**: el dispositivo se apaga. Las aplicaciones y archivos abiertos se cierran sin guardarlos.
Cuando se selecciona el botón de encendido	• **No realizar ninguna acción**: el dispositivo permanece encendido y continúa usando la batería. • **Suspender**: el dispositivo entra en modo de suspensión y utiliza una pequeña cantidad de carga de la batería. El equipo aun está encendido y las aplicaciones y archivos abiertos se almacenan en la RAM. • **Estado de suspensión de hibernación**: el dispositivo entra en modo de hibernación. Las aplicaciones y los archivos abiertos se almacenan en el disco duro y el dispositivo se apaga. • **Apagar**: el dispositivo se apaga. Las aplicaciones y archivos abiertos se cierran sin guardarlos.
Cuando se selecciona el botón Suspender	• **No realizar ninguna acción**: el dispositivo permanece encendido y continúa usando la batería. • **Suspender**: el dispositivo entra en modo de suspensión y utiliza una pequeña cantidad de carga de la batería. El equipo aun está encendido y las aplicaciones y archivos abiertos se almacenan en la RAM. • **Estado de suspensión de hibernación**: el dispositivo entra en modo de hibernación. Las aplicaciones y los archivos abiertos se almacenan en el disco duro y el dispositivo se apaga. • **Apagar**: el dispositivo se apaga. Las aplicaciones y archivos abiertos se cierran sin guardarlos.
Activar la suspensión híbrida	• **Cierto**: los dispositivos pueden entrar en modo de suspensión híbrida. Las aplicaciones y los archivos abiertos se almacenan en la RAM y en el disco duro. Utiliza una pequeña cantidad de carga de batería. • **Falso**: impide que los dispositivos entren en modo de suspensión híbrida.

El dispositivo está enchufado

Utilice las configuraciones siguientes en la tabla cuando el dispositivo esté usando energía de una fuente de alimentación externa:

Ajuste	Descripción
Umbral de batería para activar el ahorro de energía	Cuando el dispositivo esté enchufado, introduzca el nivel de carga de la batería para activar el Ahorro de energía; puede introducir valores de 0 a 100. Introduzca un valor porcentual que indique el nivel de carga de la batería. Por ejemplo, cuando se establece en 80, Energy Saver se activa cuando la batería tiene un 80 % de carga o menos carga disponible. Si no introduce un valor, Ivanti Neurons for MDM no cambia ni actualiza esta configuración. De forma predeterminada, Windows lo configurará al 70 %.
Cuando la tapa está cerrada	• **No realizar ninguna acción**: el dispositivo permanece encendido y continúa usando una fuente de alimentación externa. • **Suspender**: el dispositivo entra en modo de suspensión y utiliza una pequeña cantidad de fuente de alimentación externa. El equipo aun está encendido y las aplicaciones y archivos abiertos se almacenan en la RAM. • **Estado de suspensión de hibernación**: el dispositivo entra en modo de hibernación. Las aplicaciones y los archivos abiertos se almacenan en el disco duro y el dispositivo se apaga. • **Apagar**: el dispositivo se apaga. Las aplicaciones y archivos abiertos se cierran sin guardarlos.
Cuando se selecciona el botón de encendido	• **No realizar ninguna acción**: el dispositivo permanece encendido y continúa usando una fuente de alimentación externa. • **Suspender**: el dispositivo entra en modo de suspensión y utiliza una pequeña cantidad de fuente de alimentación externa. El equipo aun está encendido y las aplicaciones y archivos abiertos se almacenan en la RAM. • **Estado de suspensión de hibernación**: el dispositivo entra en modo de hibernación. Las aplicaciones y los archivos abiertos se almacenan en el disco duro y el dispositivo se apaga. • **Apagar**: el dispositivo se apaga. Las aplicaciones y archivos abiertos se cierran sin guardarlos.
Cuando se selecciona el botón Suspender	• **No realizar ninguna acción**: el dispositivo permanece encendido y continúa usando una fuente de alimentación externa. • **Suspender**: el dispositivo entra en modo de suspensión y utiliza una pequeña cantidad de fuente de alimentación externa. El equipo aun está encendido y las aplicaciones y archivos abiertos se almacenan en la RAM. • **Estado de suspensión de hibernación**: el dispositivo entra en modo de hibernación. Las aplicaciones y los archivos abiertos se almacenan en el disco duro y el dispositivo se apaga. • **Apagar**: el dispositivo se apaga. Las aplicaciones y archivos abiertos se cierran sin guardarlos.
Activar la suspensión híbrida	• **Cierto**: los dispositivos pueden entrar en modo de suspensión híbrida. Las aplicaciones y los archivos abiertos se almacenan en la RAM y en el disco duro. Utiliza una pequeña cantidad de fuente de alimentación externa. • **Falso**: impide que los dispositivos entren en modo de suspensión híbrida.

Configuración de macOS Energy Saver

Ajustes de ahorro de energía CA del equipo de escritorio

Utilice los ajustes siguientes para configurar los ajustes de ahorro de energía de CA del dispositivo de sobremesa macOS:

Ajuste	Descripción
Nombre,	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Arranque automático tras un fallo eléctrico	Active el arranque automático del dispositivo tras un fallo eléctrico.
Poner un disco duro en reposo después de	Active la casilla para suspender el disco duro a intervalos fijos entre 1 y 180 minutos. Un valor de 0 minutos nunca pondrá el disco duro en reposo.
Apagar la pantalla después de	Active la casilla para apagar la pantalla a intervalos fijos entre 1 y 180 minutos. Un valor de 0 minutos nunca apagará la pantalla.
Paso de potencia dinámico	Seleccione la casilla para activar el paso de potencia dinámico.
Reducir la velocidad del procesador	Seleccione la casilla para reducir la velocidad del procesador.
Poner el equipo en reposo después de	Active la casilla para suspender el equipo a intervalos fijos entre 1 y 180 minutos. Un valor de 0 minutos nunca pondrá el equipo en reposo.
Activar para acceder a la red	Seleccione la casilla para activar el equipo para el acceso a la red.
Activar por timbre de módem	Seleccione la casilla para activar el equipo para el timbre del módem.

Programar los ajustes de arranque o apagado del equipo

Utilice los siguientes ajustes para configurar los dispositivos macOS para el arranque o apagado programado de los dispositivos.

Desactivar la configuración del dispositivo

Seleccione la casilla **Apagar el dispositivo** para apagar los dispositivos a intervalos fijos.

Ajuste	Descripción
Tipo de evento	Seleccione uno de los tipos de evento opción en la lista desplegable: • Suspender • Reiniciar • Apagar
Cuando	Seleccione uno o varios días de la semana para programar un tipo de evento.
En	Seleccione la hora para programar un tipo de evento.

Inicio o activación de la configuración del dispositivo

Seleccione la casilla **Iniciar o activar el dispositivo** para activar los dispositivos a intervalos fijos.

Ajuste	Descripción
Tipo de evento	Seleccione uno de los tipos de evento opción en la lista desplegable: • Activar • Arranque / Activación
Cuando	Seleccione uno o varios días de la semana para programar un tipo de evento.
En	Seleccione la hora para programar un tipo de evento.

Ajustes de ahorro de energía CA del portátil

Utilice los ajustes siguientes para configurar los ajustes de ahorro de energía de CA del dispositivo portátil macOS:

Ajuste	Descripción
Arranque automático tras un fallo eléctrico	Active el arranque automático del dispositivo tras un fallo eléctrico.
Poner un disco duro en reposo después de	Active la casilla para suspender el disco duro a intervalos fijos entre 1 y 180 minutos. Un valor de 0 minutos nunca pondrá el disco duro en reposo.
Apagar la pantalla después de	Active la casilla para apagar la pantalla a intervalos fijos entre 1 y 180 minutos. Un valor de 0 minutos nunca apagará la pantalla.
Paso de potencia dinámico	Seleccione la casilla para activar el paso de potencia dinámico.
Reducir la velocidad del procesador	Seleccione la casilla para reducir la velocidad del procesador.
Poner el portátil en reposo después de	Active la casilla para suspender el portátil a intervalos fijos entre 1 y 180 minutos. Un valor de 0 minutos nunca pondrá el portátil en reposo.
Activar para acceder a la red	Seleccione la casilla para activar el portátil para el acceso a la red.
Activar por timbre de módem	Seleccione la casilla de verificación para despertar el ordenador portátil para el timbre del módem.

Ajustes de ahorro de energía de la batería del portátil

Utilice los ajustes siguientes para configurar los ajustes de ahorro de energía de la batería del dispositivo portátil macOS:

Ajuste	Descripción
Arranque automático tras un fallo eléctrico	Active el arranque automático del dispositivo tras un fallo eléctrico.
Poner un disco duro en reposo después de	Active la casilla para suspender el disco duro a intervalos fijos entre 1 y 180 minutos. Un valor de 0 minutos nunca pondrá el disco duro en reposo.
Apagar la pantalla después de	Active la casilla para apagar la pantalla a intervalos fijos entre 1 y 180 minutos. Un valor de 0 minutos nunca apagará la pantalla.
Paso de potencia dinámico	Seleccione la casilla para activar el paso de potencia dinámico.
Reducir la velocidad del procesador	Seleccione la casilla para reducir la velocidad del procesador.
Poner el equipo en reposo después de	Active la casilla para suspender la batería del portátil a intervalos fijos entre 1 y 180 minutos. Un valor de 0 minutos nunca pondrá la batería del portátil en reposo.
Activar para acceder a la red	Seleccione la casilla para activar la batería del portátil para el acceso a la red.
Activar por timbre de módem	Seleccione la casilla para activar la batería del portátil para el timbre del módem.

10.10.8.18. Configuración de Ethernet (macOS)

Licencia: Gold

Aplicable a: macOS 10.13+ o versiones más recientes compatibles.

El administrador puede configurar la interfaz Ethernet en variaciones. Las siguientes cargas útiles están disponibles para la configuración de Ethernet:

- Ethernet general
- Primera Ethernet activa
- Primera Ethernet
- Segunda Ethernet activa
- Segunda Ethernet
- Tercera Ethernet activa
- Tercera Ethernet

> Las diferentes cargas útiles para configurar Ethernet son: Global por defecto, Primera, Primera activa, Segunda, Segunda activa, Tercera y Tercera interfaz de Ethernet activa. Apple tiene un problema conocido con la instalación de la Primera, Primera activa, Segunda, Segunda activa, Tercera y Tercera interfaz de Ethernet activa.

Configuración de Ethernet

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Escriba **Ethernet** en el campo de búsqueda y, a continuación, seleccione configuración de **Ethernet**.
4. Introduzca un nombre y describa la configuración.
5. Elija la configuración en la lista desplegable:
6. Escriba los **ajustes de configuración de Ethernet**.
7. Haga clic en **Siguiente**.
8. Seleccione la opción **Habilitar esta configuración**.
9. Seleccione una de las siguientes opciones de canal para aplicar la configuración:
    - Canal de dispositivos (el más común)
    - Canal del usuario (usuario actualmente registrado)
10. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - personalizada
11. Haga clic en **Hecho**.

Ajustes de la configuración de Ethernet

Utilice los ajustes de la siguiente tabla para configurar la Ethernet. Para obtener más información sobre estos ajustes, consulte **Documentación de Apple**.

Ajuste	Descripción
Protocolos	
Tipos de EAP aceptados	Seleccione los tipos de EAP que pueden utilizarse para acceder a esta red: • Seguridad de la capa de transporte (TLS): la TLS es un protocolo que establece una sesión cifrada entre dos ordenadores en Internet. Verifica la identidad del servidor y evita que los hackers intercepten cualquier dato. • TTLS: en el campo **Identidad interior**, seleccione uno de los protocolos de autenticación como SO predeterminado, PAP, CHAP, MSCHAP, MSCHAPv2 y EAP. • PEAP • LEAP • EAP-SIM: en el campo **EAP SIM Number of RANDs** (Número SIM de RAND de EAP), seleccione el número de «rands» en la lista desplegable. • EAP-AKA • EAP- FAST: seleccione la opción EAP-FAST que define los métodos de autenticación: ◦ **Usar PAC:** seleccione esta opción para usar la autoconfiguración del proxy (PAC). ◦ **PAC de aprovisionamiento:** seleccione esta opción para permitir que se aprovisione la PAC. De lo contrario, solamente podrán utilizarse las PAC ya aprovisionadas en el dispositivo. Esta opción solamente está disponible si ha seleccionado Usar PAC. ◦ **PAC de aprovisionamiento anónimo:** seleccione esta opción para permitir que se aprovisione una PAC sin autenticar el servidor. Esta opción solamente está disponible si ha seleccionado PAC de aprovisionamiento.
Autenticación	**Nombre de usuario**: especifique el nombre de usuario requerido para acceder a la red. Si deja esta opción en blanco, se le solicitará al usuario del dispositivo. • Usar contraseña por conexión: seleccione esta opción para solicitar al usuario el dispositivo una contraseña cada vez que se conecte. Cuando el dispositivo vuelva a unirse a la misma red, se solicitará al usuario del dispositivo que vuelva a autenticarse para unirse a la red. Cada vez que se inicia la conexión, se solicita la contraseña. • Solicitar la contraseña una vez cuando se conecte a la red: la contraseña se solicita una sola vez cuando se envía la configuración al dispositivo. Cada conexión y desconexión a la red no solicitará ninguna contraseña. **Contraseña**: (opcional) introduzca la contraseña para acceder a esta red. De lo contrario, se le pedirá al usuario del dispositivo la contraseña necesaria para acceder a la red. **Identidad exterior**:(opcional) para TTLS, PEAP y EAP-FAST, seleccione esta opción para permitir a los usuarios de los dispositivos que oculten su identidad. El nombre real del usuario solo aparecerá dentro del túnel cifrado. Esta opción puede mejorar la seguridad porque un atacante no puede ver claramente el nombre del usuario de autenticación. **Identidad de origen de las credenciales del modo de sistema**: el modo de sistema se utiliza para la autenticación del ordenador. La autenticación mediante el modo de sistema se produce antes de que un usuario inicie sesión en el ordenador. El modo de sistema suele estar configurado para proporcionar autenticación con el certificado X.509 del ordenador (EAP-TLS) emitido por una autoridad certificadora local.
Confiar	**Certificados de confianza:** seleccione las casillas de verificación para seleccionar varios certificados de la lista. **Nombres de certificado del servidor de confianza**: agregue el nombre del certificado. • **Permitir excepciones de confianza**: permitir que el usuario tome decisiones de confianza en una ventana de diálogo.

Ajuste	Descripción
	• **Requerir certificado TLS** **Versión máxima de TLS permitida con la autenticación EAP** **Versión mínima de TLS permitida con la autenticación EAP** **Certificados de confianza TLS: certificado EC del agente de MobileIron**

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.8.19. Configuración de Google BeyondCorp

Ivanti Neurons for MDM se puede integrar con Google BeyondCorp para acceso condicional. Ivanti Neurons for MDM envía una señal de estado de legalidad del dispositivo a Google BeyondCorp. Esto garantiza que solo los dispositivos compatibles con N-MDM puedan acceder a las aplicaciones del espacio de trabajo de Google.

Aplicable a

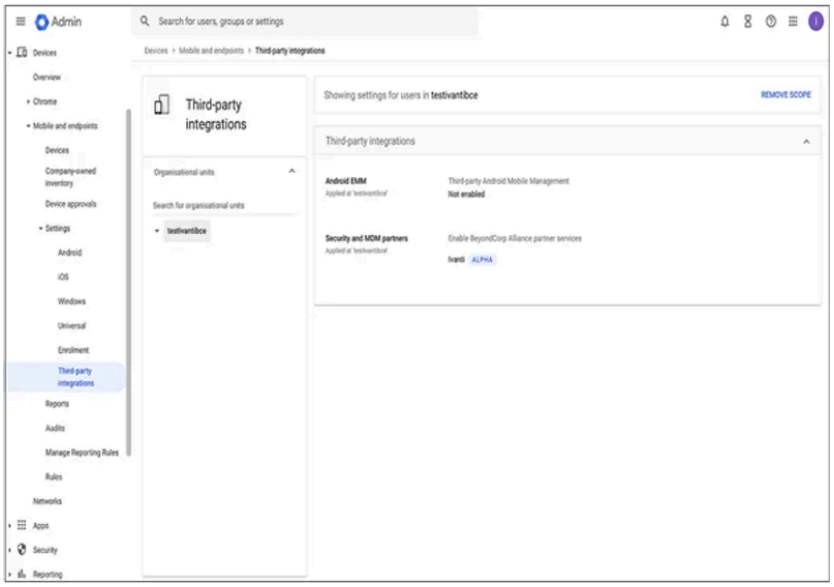
- iOS
- Android
- Windows

Requisitos previos

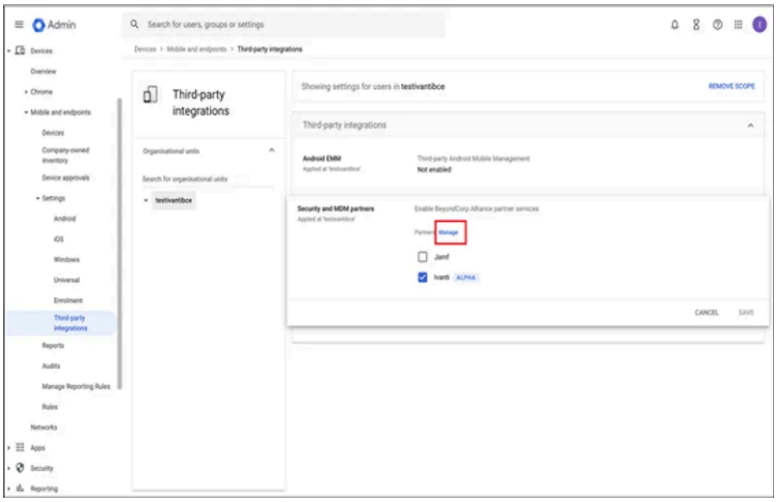
- Para Ivanti Neurons for MDM, debe tener una licencia Ivanti Professional Plus/Premium.
- Para Google, debe tener la licencia BeyondCorp Enterprise, Google Workspace Enterprise o Cloud Identity Premium.
- Para Windows, debe tener lo siguiente instalado en el dispositivo:
  - Ivanti Bridge
  - Google Chrome

Procedimiento (Google)

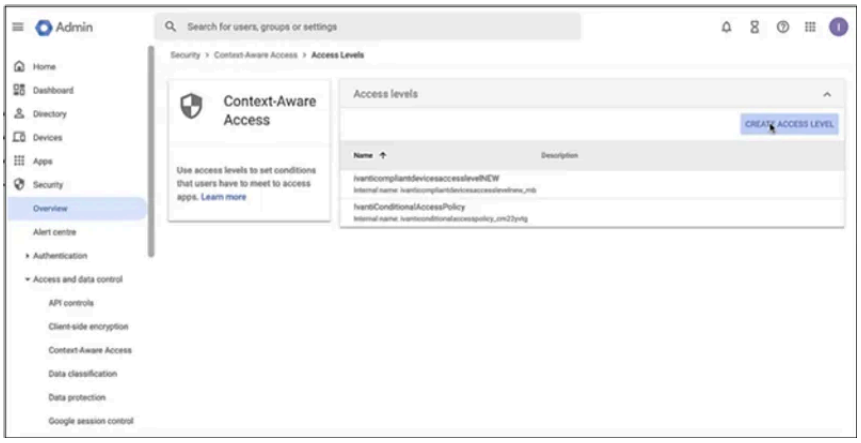
1. Inicie sesión en **Consola de administración de Google** con credenciales de administrador.
2. Vaya a **Dispositivos** > **Endpoints móviles** > **Configuración** > **Integraciones de terceros**.



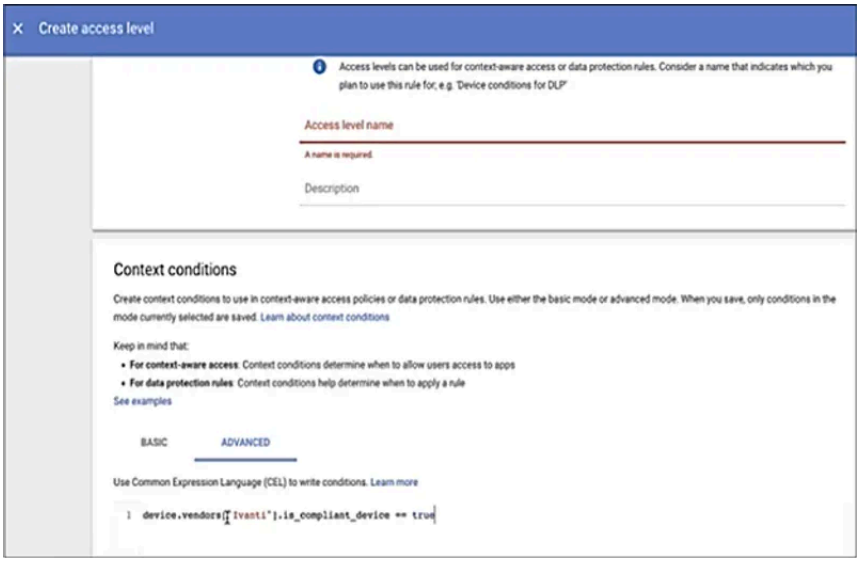
3. Haga clic en **Seguridad y socios de MDM** > **Administrar**.



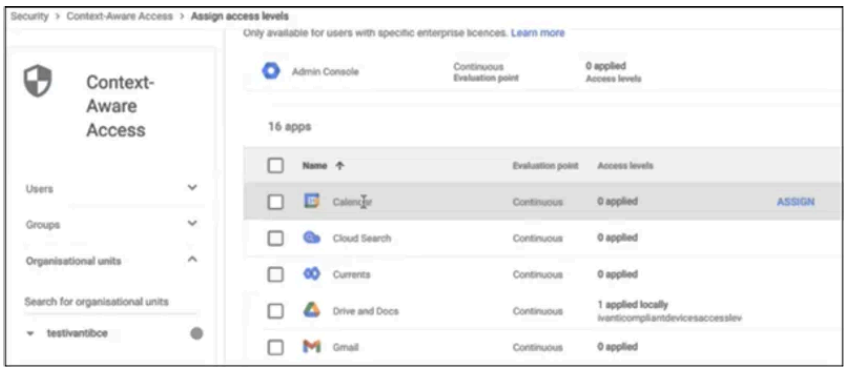
4. En la ventana **Administrar conexiones de socios** , seleccione **Ivanti**.
5. Haga clic en **Abrir conexión**.
   Serás redirigido a la página de inicio de sesión Ivanti Neurons for MDM; introduzca las credenciales de administrador del abonado. Una vez que inicie sesión en el abonado, verá que **Google BeyondCorp** está activado y vinculado a su cuenta de Google automáticamente.
6. En la Consola de administración de Google, vaya a **Seguridad** > **Acceso contextual** > **Niveles de acceso**.



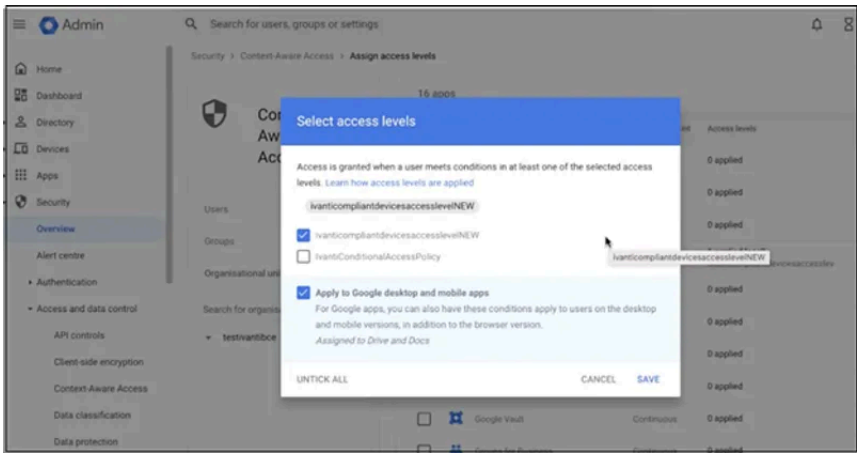
7. Haga clic en **Crear nivel de acceso**.
   En la ventana Crear nivel de acceso, en la sección Condiciones de contexto, haga clic en **AVANZADO** y proporcione la información requerida.



8. Vaya a **Seguridad** > **Acceso consciente del contexto** > **Nivel de acceso**, seleccione la aplicación para la que desea asignar la política.



9. Haga clic en **Asignar**.
10. Desde la ventana **Seleccionar niveles de acceso**, seleccione las políticas que desea asignar y haga clic en **Guardar**.



Una vez completada la configuración anterior, puede crear la configuración de legalidad del dispositivo asociado mediante **Google BeyondCorp**.

Procedimiento (Ivanti Neurons for MDM**)**:

1. Vaya a **Configuraciones** > **Agregar configuración**.
2. Seleccione la configuración de **Legalidad del dispositivo asociado**.
3. La página de configuración Crear legalidad de dispositivo asociado aparece en la pantalla.
   Introduzca un nombre para la configuración.
4. En la lista Elegir socio, seleccione **Google BeyondCorp**.
5. La sección Configuración aparece en la pantalla. Asegúrese de que la opción Informar estado de legalidad para dispositivos iOS y Android esté activada.
   Haga clic en **Siguiente**.
6. Seleccione **Habilitar esta configuración**.
7. Seleccione **Personalizado** para la opción de distribución.
8. Seleccione **Usuarios/Grupos de usuarios** en la opción **Distribución personalizada**.
9. En la sección **Seleccionar a continuación para distribuir esta configuración**, seleccione usuarios/grupos de usuarios de la lista.
10. Haga clic en **Hecho**.

El servidor de Google BeyondCorp puede identificar de forma única cada dispositivo mediante la lista de propiedades (P-List) gestionada por la aplicación.



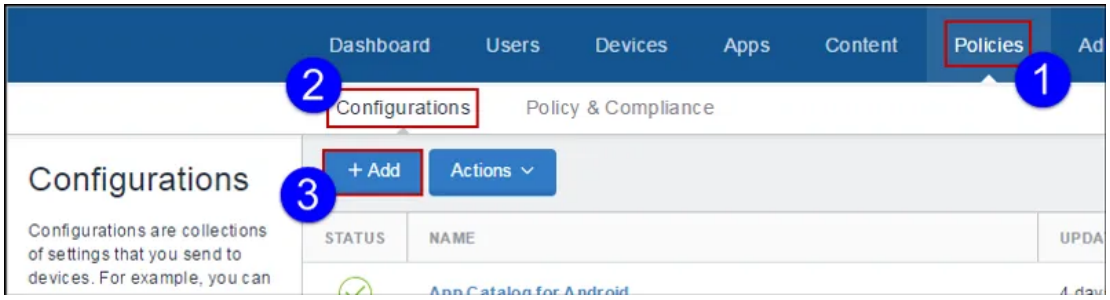
10.10.8.20. Configuración del mensaje de la pantalla de bloqueo

Muestra un mensaje y la información de la etiqueta del activo en las pantallas de inicio de sesión y de bloqueo. Esto es para dispositivos supervisados que utilizan iOS 9.3 o versiones más recientes compatibles.

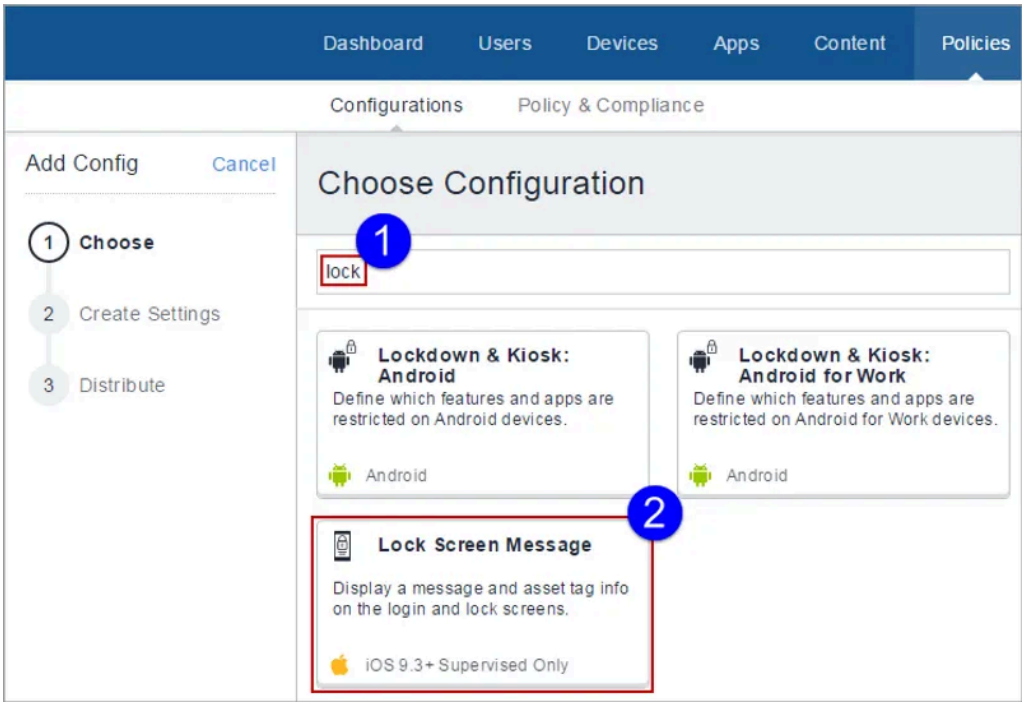
Crear una configuración del mensaje de la pantalla de bloqueo

Procedimiento

1. Seleccione **Configuraciones**.
2. Haga clic en **+Añadir**.



Escriba **'lock'** en el campo de búsqueda y, a continuación, haga clic en la configuración **Mensaje de la pantalla de bloqueo**:



Aparecerá la página de detalles Configuración del mensaje de la pantalla de bloqueo.
Configure los ajustes en esta página. Consulte la tabla de la sección **Ajustes de la configuración del mensaje de la pantalla de bloqueo** para obtener ayuda acerca de los valores.

5. Haga clic en **Siguiente** para configurar los ajustes de distribución y, a continuación, haga clic en **Hecho**.

Ajustes de la configuración del mensaje de la pantalla de bloqueo

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Bloquear nota a pie de la pantalla	Este texto aparece en la pantalla de inicio de sesión y en la pantalla de bloqueo.
Información de la etiqueta del activo	Este texto aparece en la parte inferior de la pantalla de inicio de sesión y en la pantalla de bloqueo.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.8.21. Configuración de la ventana de inicio de sesión: macOS

Procedimiento

1. Inicie sesión en Ivanti Neurons for MDM.
2. Vaya a **Configuraciones** > **Agregar configuraciones**.
3. Haga clic (o seleccione) **Ventana de inicio de sesión**.
4. En el campo **Nombre**, introduzca un nombre para la configuración de la ventana de inicio de sesión.
5. Haga clic en **+ Agregar descripción** para agregar detalles.
6. En la sección **Ajustes de configuración**, proporcione los campos siguientes:
    - **Información del host de administrador**: introduzca el nombre de host, la dirección IP o SystemVersion.
    - **Lista permitidos**: lista de GUID del usuario o GUID de grupos de usuarios a los que el sistema permite iniciar sesión. Una cadena de asteriscos ('*') especifica a todos los usuarios o grupos.
    - **Contraseña de inicio de sesión automático**: introduzca la contraseña para Inicio de sesión automático.
    - **Lista no permitido**: la lista de GUID de los usuarios o GUID de grupos de usuarios a los que el sistema no permite iniciar sesión. Esta lista tiene prioridad sobre la lista de la tecla 'AllowList'.
    - **Texto de la ventana de inicio de sesión**: introduzca el texto de la ventana de inicio de sesión.
    - Seleccione la casilla de verificación para opciones adicionales como:
        - **Desactivar el acceso a la consola**
        - **Desactivar Inicio de sesión automático de FDE (cifrado de disco de FileVault)**
        - **Desactivar las funciones de bloqueo de pantalla inmediata**
        - **Ocultar a los usuarios del administrador al mostrar una lista de usuarios**
        - **Mostrar solo usuarios de red y sistema**
        - **Ocultar cuentas móviles**
        - **Mostrar usuarios de red**
        - **Desactiva el elemento del menú de inicio de sesión**
        - **Deshabilite el apagado cuando el usuario inicia sesión**
        - **Desactive el elemento del menú de reinicio cuando el usuario inicie sesión**
        - **Desactive el elemento de reinicio**
        - **Mostrar el cuadro de diálogo Nombre y contraseña**
        - **Mostrar otros usuarios: administrado**
        - **Mostrar menú de entrada**
        - **Desactive el botón de apagado**
        - **Desactivar el botón de suspensión**
        - **Desactive el botón del menú de apagado**
7. Haga clic en **Hecho**.

10.10.8.22. Configuración de las extensiones del sistema de macOS

La configuración de la Extensión del Sistema permite la instalación de tipos de extensión como la Extensión de conductor, la Extensión de red y la Extensión de seguridad de punto final, sin acceso a nivel de núcleo.

Procedimiento

Disponible para: macOS 10.15+

1. Vaya a **Configuraciones** > **+Añadir**.
2. Escriba **extensión** en el campo de búsqueda y, a continuación, haga clic en la configuración del **Sistema de extensiones** .
3. Introduzca un **Nombre** y **Descripción** de la configuración.
4. En **Extensiones de sistema permitidas**, **+Añadir** los **Identificadores de equipo permitidos** y las **Extensiones de sistema permitidas**.
5. En **Tipos de extensiones del sistema permitidos**, **+Añadir** los **Identificadores de equipo permitidos** y los **Tipos de sistema permitidos**.
6. Marque la opción **Permitir anulaciones de usuario**.
7. Haga clic en **Siguiente**.
8. Seleccione la opción **Habilitar esta configuración**.
9. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - Personalizado.
10. Haga clic en **Hecho**.

> En macOS 12, RemovableSystemExtensions permite a la aplicación desactivar la extensión del sistema sin aprobación del administrador durante la desinstalación de la aplicación.

10.10.8.23. MAM solo

Ivanti Neurons for MDM le permite especificar dispositivos de iOS y Android como solo MAM y proporciona Mobile App Management (MAM) a esos dispositivos. La implementación de «MAM only» le permite distribuir y administrar aplicaciones sin tener que administrar el dispositivo en sí.

Solución solo MAM: alternativa de Ivanti AppStation

Como una solución alternativa a la Ivanti AppStation, Ivanti ofrece una solución moderna y flexible de administración de aplicaciones móviles (MAM) mediante el cliente Ivanti GO, disponible para plataformas iOS y Android.

La nueva solución de solo MAM presenta un App Catalog integrado junto con la función de clip web Ivanti Neurons for MDM, que en conjunto cumple los casos de uso central previamente abordados por la App Station en la garantía de una experiencia de administración de aplicaciones simplificada, segura y unificada para usuarios y administradores.

Características clave

- **App Catalog en la aplicación**: aloja y distribuye aplicaciones aprobadas y administradas directamente dentro del cliente GO.
- **Configuración y actualizaciones de la aplicación**: admite la configuración de nivel de aplicación y las actualizaciones de la versión, aplicadas a través de las políticas de MAM.
- Ivanti Neurons for MDM **Requisito**: ideal para escenarios de BYOD y contratistas donde la inscripción delvanti Neurons for MDM no es posible.

Uso de un clip web para facilitar el acceso

- **Acceso directo al All Catalog**: implementación de clips web a través de Ivanti Neurons for MDM para proporcionar un atajo al App Catalog o aplicaciones empresariales específicas basadas en la web.
- **Accesos directos a aplicaciones personalizadas**: permite a los usuarios iniciar rápidamente recursos utilizados frecuentemente desde su pantalla de inicio.

Experiencia mejorada de administrador y usuario

- **Interfaz unificada**: combina App Catalog, acceso web y mensajes de conformidad en una sola experiencia.
- **Administración simplificada**: no es necesario mantener soluciones separadas (es decir, App Station), lo que reduce la complejidad y el riesgo de la deriva de configuración.

Flexibilidad y personalización

- **Personalizar vistas del catálogo**: personalización del contenido de App Catalog basado en roles de usuario, ubicación geográfica o unidad organizativa.
- **Utiliza una infraestructura existente**: aprovecha su inversión Ivanti Neurons for MDM / MAM existente (no requiere una infraestructura separada).

Compatibilidad con usuarios de doble rol

La solución Ivanti solo MAM está diseñada para admitir escenarios de trabajo modernos, incluidos usuarios con roles duales:

- **Empleado a tiempo completo: Org A**: Accede a aplicaciones empresariales mediante un WebClip (por ejemplo, Apps@Work) desplegado a través de Ivanti Neurons for MDM.
- **Contratista: Org B**: utilice el cliente Ivanti Go en modo solo MAM para acceder a las aplicaciones administradas de forma segura, sin requerir la inscripción de dispositivos de Ivanti Neurons for MDM.

Esto permite un acceso fluido y basado en roles a las aplicaciones necesarias, sin conflictos de perfiles ni solapamientos en la gestión de dispositivos.

Guía de migración

Ivanti alienta encarecidamente a los clientes de la estación de aplicaciones a planificar y ejecutar su transición a la solución de MAM basada en el cliente GO. Para obtener asistencia migratoria paso a paso, consulte los recursos siguientes:

- Solución Ivanti solo MAM
- **Configuración de App Catalog en Go Client**
- **Crear una configuración de Web Clip**

Si tiene preguntas o necesita asistencia migratoria, comuníquese con **Soporte técnico de Ivanti** o el Administrador de operaciones correctas de su cliente.

10.10.8.24. Configuración Google Play administrada

Los administradores pueden configurar automáticamente el ajuste de actualizar que usa Google Play Store para actualizar las aplicaciones en el dispositivo de Android Enterprise.

Para configurar los ajustes de actualización automática, lleve a cabo las siguientes acciones:

1. Vaya a **Configuración > +Añadir**.
2. Selecciona la configuración **Google Play administrada**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. En la sección Ajuste de la configuración, seleccione una opción para actualizar aplicaciones de Google Play.

Ajuste	Qué hacer
Definido por el usuario	El usuario del dispositivo puede configurar la ventana de mantenimiento de aplicaciones de actualización automática para definir cuándo deben actualizarse las aplicaciones. 1. En el campo **Hora de inicio**, seleccione la hora a la que se realizará la actualización de la aplicación. 2. En el campo **Duración**, seleccione la duración (en horas) dentro de la cual debe realizarse la actualización. El intervalo mínimo y máximo es entre 1 hora y 24 horas. Las aplicaciones se pueden actualizar en cualquier momento entre la hora de inicio y la duración seleccionada. Por ejemplo, si la «Hora de inicio» está fijada a las 18:00 h. y la «Duración» en12 h, las aplicaciones se pueden actualizar en cualquier momento desde las 18:00 h. hasta las 6:00 h.
Ninguna	Google Play Store nunca actualiza automáticamente las aplicaciones del dispositivo.
Solo Wi-Fi	Google Play Store actualiza automáticamente las aplicaciones del dispositivo, pero solamente mediante conexiones Wi-Fi y no usando los datos móviles.
Siempre	Google Play Store actualiza automáticamente las aplicaciones del dispositivo mediante conexiones Wi-Fi o usando los datos móviles.

6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones de distribución:

- Todos los dispositivos
- Ningún dispositivo (predeterminada)
- personalizada

8. Haga clic en **Hecho**.

10.10.8.25. Ajustes del asistente de migración

Utilice los **Ajustes del asistente de migración** para configurar esta función en dispositivos supervisados. Esta configuración ayuda a los administradores a aplicar controles coherentes basados en políticas que gestionan cómo los usuarios transfieren datos, aplicaciones y ajustes durante la configuración o migración de dispositivos.

Disponible para:

- macOS 26.4+ supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Busque **Ajustes del asistente de migración** y seleccione la configuración correspondiente.
3. Configure los **Ajustes del asistente de migración** según la siguiente tabla:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Debe realizar la migración gestionada	Seleccione la casilla de verificación para habilitar y gestionar la migración de dispositivos. Active **Enviar al dispositivo** para habilitar la migración de dispositivos.
Cuentas excluidas	Introduzca los nombres de las cuentas que desea excluir de la migración. Active **Enviar al dispositivo** para excluir las cuentas especificadas de la migración.
Rutas que se excluirán	Introduzca los nombres de las rutas que desea excluir de la migración. Active **Enviar al dispositivo** para excluir las rutas especificadas de la migración.
Rutas necesarias	Introduzca las rutas que desea incluir en la migración Active **Enviar al dispositivo** para incluir las rutas especificadas en la migración.
Migrar los ajustes de seguridad y privacidad	Seleccione la casilla para habilitar la migración de los ajustes de seguridad y privacidad de los dispositivos. Active **Enviar al dispositivo** para permitir la migración de los ajustes de seguridad y privacidad.

4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Seleccione una de las opciones de distribución para configurar los **Ajustes del asistente de migración**. Para más información sobre la configuración de las opciones de distribución, consulte Trabajar con configuraciones.
6. Haga clic en **Hecho**.

10.10.8.26. Configuración de las notificaciones

Con la configuración de Notificaciones, los administradores pueden programar notificaciones silenciosas y visibles para dispositivos iOS. La configuración de Notificaciones también se puede clonar, exportar o eliminar.

Procedimiento

1. Vaya a **Configuración > +Añadir**.
2. Seleccione **Configuración de notificaciones**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. En la sección Configuración de configuración, seleccione una o ambas opciones de **programación de notificaciones**:
    - Programación de notificaciones silenciosas: las notificaciones silenciosas se utilizan para admitir las operaciones de administración del dispositivo de segundo plano iniciadas por Ivanti Neurons for MDM. Permiten acciones automatizadas, como comprobaciones de cumplimiento, actualizaciones de política y actualizaciones de la aplicación, sin requerir la interacción del usuario. Ivanti Neurons for MDM envía notificaciones silenciosas al dispositivo en el nivel configurado.
    - Programación de notificaciones visibles: las notificaciones visibles se utilizan cuando se requiere que el usuario conozca o actúe para mantener el cumplimiento, la seguridad o la funcionalidad del dispositivo. Las notificaciones visibles se activan solo después del intervalo especificado, incluso si se producen varias acciones o eventos durante ese periodo. Se muestra una notificación visible en el dispositivo solo si no se ha enviado una notificación silenciosa durante el intervalo de notificación visible.
6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - personalizada
8. Haga clic en **Hecho**.

> Contenido de notificación visible para dispositivos MTD: su dispositivo podría ser vulnerable a amenazas. Inicie la aplicación Ivanti Go y compruebe el estado de Threat Defense.

> Contenido de notificación visible para dispositivos no MTD: para recibir funciones de seguridad mejoradas y garantizar las medidas de protección más recientes, inicie la aplicación en su dispositivo para una experiencia de usuario más segura.

10.10.8.27. Ajustes de la impresora

Ivanti Neurons for MDM le permite crear perfiles de impresoras y añadirlos a los dispositivos. Esta característica requiere Bridge. Vaya a **Bridge** para obtener más información.

> Cuando se envían perfiles de impresoras a los dispositivos, la impresora debe estar activa o, de lo contrario, el dispositivo no la detectará.

Para establecer la configuración de los ajustes de la impresora para un dispositivo Windows:

1. Vaya a **Configuración > +Agregar**.
2. Seleccione la configuración **Ajustes de impresora**.
3. Introduzca un nombre para la configuración.
4. Seleccione la opción **Windows**.
5. En la sección **Ajuste de la configuración**, configure los siguientes ajustes:

Ajuste	Qué hacer
Nombre,	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Ajustes de impresora de Windows	
Impresora compartida	Si se selecciona la opción de **Impresora compartida**, la impresora estará compartida con otros dispositivos. Configure los siguientes campos: **Nombre**: introduzca el nombre de la configuración de la impresora. **Descripción**: introduzca una descripción de la impresora. **Servidor de impresión**: introduzca la dirección IP del servidor de impresión. **Nombre de la impresora compartida**: introduzca el nombre de la impresora.
Impresora conectada a la red	Cuando se selecciona la opción **Conectada a la red**, solo los dispositivos de la red conectada tendrán acceso a la impresora. Configure los siguientes campos: **Nombre**: introduzca el nombre de la configuración de la impresora. **Descripción**: introduzca una descripción de la impresora. **Nombre de impresión**: introduzca el nombre de la impresora conectada a la red. **Dirección host de la impresora**: introduzca la dirección IP del host de la impresora. **Número de puerto de la impresora**: seleccione el número de puerto de la impresora conectada a la red. **Nombre de la unidad de la impresora**: introduzca el nombre de la unidad de la impresora. **URL de la unidad de la impresora**: introduzca la URL de la unidad de la impresora. Para el controlador de impresora, cargue un archivo ZIP que contenga los archivos necesarios. El archivo ZIP debe incluir los archivos siguientes: • Archivo .inf (información del controlador) • Archivo .cat (catálogo/firma) • Cualquier binario adicional del controlador referenciado por el archivo INF (como .dll, .sys, etc.).

6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones de distribución:

- Todos los dispositivos
- Ningún dispositivo (predeterminada)
- personalizada

8. Haga clic en **Hecho**.

Para establecer la configuración de los ajustes de la impresora para un dispositivo macOS:

1. Vaya a **Configuración > +Añadir**.
2. Seleccione la configuración **Ajustes de impresora**.
3. Introduzca un nombre para la configuración.
4. Seleccione la opción **macOS**.
5. En la sección **Crear configuración de impresora**, configure los siguientes ajustes:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Establecimiento de la configuración	Actualice los siguientes campos para configurar la impresora para dispositivos macOS: • Permitir las impresoras locales • Nombre en pantalla de la impresora por defecto • Nombre de la fuente del pie de página • Tamaño de la fuente del pie de página • Lista de impresoras del usuario • + Añadir impresora

6. Haga clic en **Siguiente**
7. Seleccione una de las siguientes opciones de distribución:

- Todos los dispositivos
- Ningún dispositivo (predeterminada)
- personalizada

8. Haga clic en **Hecho**.

10.10.8.28. Configuración para eliminar el «bloatware»

La configuración para eliminar el «bloatware» le permite seleccionar la lista de aplicaciones instaladas en dispositivos que deben eliminarse obligatoriamente. Para esta configuración, es un requisito previo tener una configuración de Bridge. Vaya a **Bridge** para obtener más detalles.

Para ejecutar o desinstalar aplicaciones:

1. En la pestaña **Configuración**, haga clic en **+Añadir**.
2. Seleccione la configuración de **Eliminar el «bloatware»**. Aparecerá la página **Configuración para eliminar el «bloatware»**.
3. En el campo **Nombre**, introduzca un nombre adecuado para la configuración.
4. Haga clic en el enlace +**Añadir descripción** para añadir una descripción de la configuración. Este campo es opcional.
5. En la sección **Ajuste de la configuración**, seleccione las aplicaciones que deben eliminarse o desinstalarse. Como alternativa, también puede buscar una aplicación en el campo de búsqueda mediante el nombre de la aplicación que aparece en la lista de aplicaciones de escritorio.

> Antes de crear la configuración para **eliminar el bloatware**, debe recuperar las aplicaciones en **Aplicaciones > Aplicaciones de escritorio > Recuperar aplicaciones.** De lo contrario, no habrá aplicaciones disponibles para buscar o elegir cuando se cree la configuración para **eliminar el bloatware**.

Se pueden eliminar los tipos de archivo .appx, .appxbundles, .xap y .msi, pero no los .exe.

6. En las opciones avanzadas, configure las siguientes opciones:

Opción	Descripción
Ejecutar esta configuración cada	Establezca la duración del intervalo (en minutos) después de la cual debe ejecutarse la configuración.
Ejecutar al iniciar sesión	Seleccione esta casilla para ejecutar la configuración cuando se inicie sesión.
Anular el reinicio forzoso tras la desinstalación	Seleccione esta casilla para evitar un reinicio obligatorio después de desinstalar la aplicación.

10.10.8.29. Configuración de ajustes y extensión de Safari

Extensión de Safari

Ivanti Neurons for MDM permite gestionar las Extensiones de Safari en dispositivos iOS y macOS supervisados. Los administradores pueden gestionar eficazmente las extensiones de Safari para la navegación estándar y privada.

Disponible para:

- iOS 18.0 supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- macOS 15.0 supervisado hasta la versión más reciente compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Buscar y seleccionar la configuración de **Ajustes de extensión de Safari**.
3. Configure los ajustes de **Ajustes de extensión de Safari** según la tabla siguiente:

Ajuste	Descripción
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
ID de extensión	Introduzca el identificador de extensión compuesto. Por ejemplo, "*Identificador (TeamIdentifier)*". Introduzca "*" para todas las extensiones. Para generar esta cadena, utilice el signo de código *-dv <path_to_appex>*. La extensión del navegador se encuentra en la carpeta plug-ins dentro del paquete de aplicaciones. El formato esperado es "*Identificador (TeamIdentifier)*". En el caso de las extensiones que no están disponibles en macOS, el desarrollador de la aplicación debe proporcionar esta información.
Estado de la extensión	Seleccione una de las siguientes opciones: • **Permitido**: el usuario puede activar o desactivar la extensión. • **Siempre activa**: la extensión está siempre "Activa" para el usuario. • **Siempre inactiva**: la extensión está siempre "Inactiva" para el usuario.
Estado de navegación privada	Seleccione una de las siguientes opciones: • **Permitido**: el usuario puede activar o desactivar la extensión en la navegación privada. • **Siempre activa**: la extensión está siempre "Activa" para el usuario incluso durante la navegación privada. • **Siempre desactivada**: la extensión no estará disponible.
Dominios permitidos	Introduzca los valores de dominio o subdominio para dar acceso a la extensión Safari. Puede introducir múltiples valores de dominio o subdominio. La configuración del dominio permitido no se aplica en el dispositivo si introduce "*" en el campo ID de extensión.
Dominios rechazados	Introduzca los valores de dominio o subdominio para restringir el acceso a la extensión Safari. Puede introducir múltiples valores de dominio o subdominio. La configuración del dominio rechazado no se aplica en el dispositivo si introduce "*" en el campo ID de extensión.

4. Haga clic en **+Agregar** para agregar varias **Extensiones**.
5. Haga clic en **Siguiente** para configurar los ajustes de distribución.
6. Seleccione una de las opciones de distribución para configurar la configuración **Ajustes de extensión de Safari** . Para más información sobre la configuración de las opciones de distribución, consulte Trabajar con configuraciones.
7. Haga clic en **Hecho**.

Ajustes de Safari

Ivanti Neurons for MDM permite administrar los ajustes de Safari en dispositivos iOS y macOS supervisados. Los administradores pueden gestionar eficazmente las extensiones de Safari para la navegación estándar y privada.

Disponible para:

- Versiones beta de iOS 26.0+, iPadOS 26.0+, macOS 26.0+ y visionOS 26.0+ hasta la versión más recientemente lanzada, según la compatibilidad con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Buscar y seleccionar la configuración de **Ajustes y extensión de Safari**.
3. Haga clic en **Ajustes de Safari**.
4. Configure los ajustes de **Ajustes de Safari** según la tabla siguiente:

Ajuste	Descripción
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Ajustes de configuración	Seleccione una de las opciones siguientes para establecer el tipo de página de inicio: • **Inicio**: para usar la página de inicio predeterminada. Safari desactiva la página de inicio existente. • **Página de inicio**: para usar la URL de la página de inicio especificada. Safari establece esto como página de inicio. • **Extensión**: para usar la página que especifica Safari Extension para la que el identificador es ExtensionIdentifier. Safari desactiva la página de inicio existente.

5. Haga clic en **Siguiente** para configurar los ajustes de distribución.
6. Seleccione una de las opciones de distribución para configurar **Ajustes de Safari**. Para más información sobre la configuración de las opciones de distribución, consulte Trabajar con configuraciones.
7. Haga clic en **Hecho**.

Ajustes de privacidad de Safari

Los ajustes de privacidad de Safari permiten a los administradores definir los permisos predeterminados de cámara y micrófono para sitios web específicos de Safari mediante Declarative dispositivo Management (DDM). Esta función ayuda a las organizaciones a administrar los permisos de privacidad del sitio web de forma centralizada y proporciona una experiencia de navegación más consistente en dispositivos Apple administrados.

Disponible para:

- iOS 27.0+ y macOS?Más de 27.0 versiones a través de la versión más reciente compatible con Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Buscar y seleccionar la configuración de **Ajustes y extensión de Safari**.
3. Haga clic en Ajustes de privacidad **de**Safari .
4. Configure los **Ajustes de Privacidad de Safari** como se indica en la siguiente tabla:

Ajuste	Descripción
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.

Ajustes de configuración	• **Agregar url**: introduzca una url para aplicar el ajuste.
	• **+Añadir valores predeterminados**:?Especifique los valores predeterminados que desea aplicar a este ajuste.
	  ◦ Cámara: Permitir/Rechazar
	  ◦ Micrófono: Permitir/Rechazar
	  ◦ Justificación de la organización (obligatorio)

5. Haga clic en **Siguiente** para configurar los ajustes de distribución.
6. Seleccione una de las opciones de distribución para configurar **Ajustes de Safari**. Para más información sobre la configuración de las opciones de distribución, consulte **Trabajar con configuraciones**.
7. Haga clic en **Hecho**.

10.10.8.30. Configuración de las restricciones de teléfonos Samsung

Configuraciones

La configuración de Restricciones de teléfonos Samsung le permite establecer restricciones de llamada y excepciones en los dispositivos Samsung. Estas restricciones limitan los números de teléfono a los que los usuarios pueden hacer o recibir llamadas.

Aplicable a: todos los dispositivos Samsung con Knox SDK 2.0+.

Para configurar las restricciones de teléfonos Samsung:

1. En la pestaña **Configuración**, haga clic en **+Añadir**.
2. Seleccione configuración de las **Restricciones de teléfonos Samsung**. Aparecerá la página **Configuración de las restricciones de teléfonos Samsung**.
3. En el campo **Nombre**, introduzca un nombre adecuado para la configuración.
4. Haga clic en el enlace +**Añadir descripción** para añadir una descripción de la configuración. Este campo es opcional.
5. En la sección **Ajuste de la configuración**, configure las siguientes opciones:
   Opción
   Descripción
   Llamadas entrantes
   Números bloqueados
   Haga clic en el icono Añadir para añadir números y expresiones regulares de Java y definir las restricciones sobre las llamadas entrantes.
   Números en lista de permitidos
   Haga clic en el icono Añadir para añadir números y expresiones regulares de Java y definir los números permitidos dentro de un conjunto mayor de números bloqueados para las llamadas entrantes.
   Esta opción no tendrá ningún efecto si no hay ningún número bloqueado.
   Llamadas salientes
   Números bloqueados
   Haga clic en el icono Añadir para añadir números y expresiones regulares de Java y definir las restricciones sobre las llamadas salientes.
   Números en lista de permitidos
   Haga clic en el icono Añadir para añadir números y expresiones regulares de Java y definir los números permitidos dentro de un conjunto mayor de números bloqueados para las llamadas salientes.
   Esta opción no tendrá ningún efecto si no hay ningún número bloqueado.
6. Haga clic en **Hecho** para insertar los ajustes en los dispositivos seleccionados.

> Al retirar un dispositivo se eliminarán todas las restricciones de llamada de este.

Para obtener más información, consulte Cómo crear una configuración.

10.10.8.31. Configuración predeterminada del navegador: iOS y visionOS

Configuración para cambiar los ajustes de aplicaciones predeterminadas en dispositivos iOS y visionOS.

Requisitos previos

- Aplicable solo para las versiones iOS (18.2+) y VisionOS 2.2.
- Estas aplicaciones se establecen en dispositivos iOS en **Ajustes** - **Aplicaciones** - **Aplicaciones predeterminadas**.

Procedimiento

1. En la página **Dispositivos**, registre un dispositivo iOS (18.2+) o un dispositivo visionOS 2.2.
2. Vaya a **Configuraciones** > **Agregar configuración** > **Ajustes de aplicación predeterminados** para establecer el navegador predeterminado en los dispositivos iOS.
3. Haga clic en **Configuraciones** > **Crear configuración** > **Crear ajustes de configuración de aplicación predeterminadas**
4. En la sección Detalles de configuración, proporcione el **Nombre** y **Descripción**.
5. En Ajustes de configuración> Agregar aplicación > Agregar por búsqueda, busque el navegador deseado. Se muestra la lista de navegadores.
6. Seleccione el navegador deseado de la lista.
7. En la página **Crear configuración de ajustes de aplicación**, haga clic en **Personalizado** para distribuir la configuración a un dispositivo o grupos específicos de dispositivos o usuarios o grupos de usuarios.
8. En **Elegir una de estas opciones de distribución personalizada**, seleccione la opción deseada para especificar la distribución de esta configuración a Usuarios/Grupos de usuarios o Dispositivos/Grupos de dispositivos.
9. Seleccione la opción deseada en **Todos los disponibles** para distribuir esta configuración.
10. Haga clic en **Hecho**.

10.10.8.32. Configuración de los ajustes del host de Compartir pantalla

La configuración de **Ajustes del host de compartir pantalla** permite a los administradores controlar de forma segura las funciones de compartir pantalla de macOS en todos los dispositivos gestionados mediante Ivanti Neurons for MDM. Esta funcionalidad permite especificar los usuarios autorizados, los métodos de autenticación y las restricciones del servicio para garantizar un acceso remoto seguro y conforme.

Aplicable a: macOS 14.0 hasta la versión publicada más reciente compatible con Ivanti Neurons for MDMIvanti Neurons for MDM.

Antes de comenzar: para una integración fluida de la configuración de **Ajustes del host de compartir pantalla**, el usuario debe habilitar la opción "**Gestión remota**" de su dispositivo. En su dispositivo, vaya a **Ajustes** > **Gestión remota** > **Habilitar gestión remota**.

Procedimiento

1. Vaya a **Configuraciones** > **+Añadir**.
2. Buscar y seleccionar la configuración de **Ajustes del del host de compartir pantalla**.
3. Configure los ajustes de **Parámetros del host de compartir pantalla** según la tabla siguiente:

Ajuste	Descripción
Nombre,	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Puerto base	Introduzca el número de puerto UDP inicial para conectarse al host. La función de compartir pantalla requiere múltiples conexiones, por lo que el sistema incrementa este valor en 1 para cada conexión adicional. Esto no modifica el número de puerto que el sistema utiliza para establecer inicialmente la conexión con un host, que siempre es el puerto TCP 5900. **Valor mínimo del puerto base**: 1024 **Valor máximo del puerto base**: 65535
Número máximo de pantallas virtuales	Puede utilizar hasta dos pantallas virtuales.
Impedir copiar archivos desde el host	Marque la casilla de verificación para impedir que los usuarios copien archivos desde el host de compartir pantalla.
Impedir copiar archivos en el host	Marque la casilla de verificación para impedir que los usuarios copien archivos en el host de compartir pantalla.
Impedir conexiones de alto rendimiento	Marque la casilla de verificación para impedir que los usuarios establezcan conexiones de alto rendimiento con el host.

4. Haga clic en **Siguiente** para configurar los ajustes de distribución.
5. Seleccione una de las opciones de distribución para configurar **Parámetros del host de compartir pantalla**. Para más información sobre la configuración de las opciones de distribución, consulte Trabajar con configuraciones.

6. Haga clic en **Hecho**.

10.10.8.33. Configuración del modo Single-App

Configuraciones

Licencia: Silver

El modo single-app restringe el uso de la aplicación especificada por parte de los dispositivos iOS. Por ejemplo, es posible que quiera configurar dispositivos que solo puedan usar una aplicación personalizada desarrollada por su organización.

Configuración del modo Single-App

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a esta configuración.
Descripción	Introduzca una descripción que explique la finalidad de esta configuración.
Elegir aplicación	Seleccione el método a usar para seleccionar la aplicación: • **Desde el Catálogo de aplicaciones y las aplicaciones del sistema**: seleccione esta opción para buscar en el catálogo de aplicaciones de Ivanti Neurons for MDM y las aplicaciones del sistema (preinstalado en dispositivos Apple de forma predeterminada). • Introduzca el nombre de la aplicación y selecciónelo cuando aparezca en la lista de aplicaciones. • **Introducir la ID del paquete:** seleccionar para introducir un identificador único para la aplicación del sistema que desee seleccionar. Utilice esta opción si no puede encontrar la aplicación del sistema mediante la opción **Desde el App Catalog y aplicaciones del sistema**.
Desactivar uso táctil	Seleccione esta opción para desactivar la pantalla táctil.
Desactivar rotación del dispositivo	Seleccione esta opción para desactivar la detección de rotación del dispositivo.
Desactivar botones de volumen	Seleccione esta opción para desactivar los botones de volumen del dispositivo.
Desactivar interruptor del timbre	Seleccione esta opción para desactivar el interruptor del timbre del dispositivo.
Desactivar botón activo/inactivo	Seleccione esta opción para desactivar el botón activo/inactivo del dispositivo (arriba a la derecha en el borde del dispositivo).
Desactivar bloqueo automático	Seleccione esta opción para evitar que el dispositivo entre el modo inactivo después de un periodo de inactividad.
Activar voz en off	Seleccione esta opción para habilitar el lector de la pantalla con la voz en off (característica de accesibilidad).
Activar zoom	Seleccione esta opción para habilitar el zoom (característica de accesibilidad).
Activar invertir colores	Seleccione esta opción para habilitar el ajuste inversión de colores (característica de accesibilidad).
Activar toque auxiliar	Seleccione esta opción para habilitar AssistiveTouch (característica de accesibilidad).
Activar Reproducir	Seleccione esta opción para habilitar Reproducir selección (característica de accesibilidad).

Ajuste	Qué hacer
selección	
Activar audio mono	Seleccione esta opción para alternar entre audio estéreo y mono (característica de accesibilidad).
Ajustes de la voz en off	Seleccione esta opción para permitir a los usuarios realizar ajustes en la voz en off.
Ajustes del zoom	Seleccione esta opción para permitir a los usuarios realizar ajustes en el zoom.
Ajustes de Invertir colores	Seleccione esta opción para permitir a los usuarios invertir los colores.
Ajustes de toque auxiliar	Seleccione esta opción para permitir a los usuarios realizar ajustes en AssistiveTouch.

Para obtener más información, consulte **Cómo crear una configuración**.

10.10.8.34. Configuración de la cadencia de recomendación de actualizaciones de software

Los administradores tienen la opción de permitir a los usuarios ver y actualizar los dispositivos a la versión más alta (la más reciente) o a la más baja (la más antigua) o a ambas.

Aplicable a: dispositivos supervisados con iOS y iPadOS 14.5 a 26.0

Procedimiento

1. Vaya a Configuraciones > +Añadir.
2. Escriba Recomendación de actualizaciones de software en el cuadro de búsqueda y, luego, haga clic en la configuración Cadencia de recomendación de actualizaciones de software.
3. Introduzca un Nombre y Descripción de la configuración.
4. Seleccione la configuración deseada en el desplegable:
    - Presentar las dos versiones de actualización del software
    - Presentar la versión de actualización de software con el número más bajo (la más antigua)
    - Presentar solo la versión de actualización de software con el número más alto (más reciente)
5. Haga clic en Siguiente.
6. Seleccione la opción Habilitar esta configuración.
7. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - Personalizado.
8. Haga clic en Hecho.

10.10.8.35. Menú Inicio y Barra de tareas

Puede definir el diseño del menú Inicio para que sus usuarios definan las aplicaciones cuyo uso es seguro y eliminar las que no sean necesarias. Las versiones de Windows 10 y 11 son compatibles con distintas funciones, puesto que los diseños del menú de Inicio son distintos.

Para establecer el menú Inicio y la configuración de la barra de tareas:

1. Vaya a **Configuración > +Añadir**.
2. Seleccione la configuración **Menú de inicio y barra de tareas de Windows**.
3. Introduzca un nombre para la configuración.
4. Seleccione la versión de Windows específica.
5. **Dispositivos Windows 10**:
   En la sección **Ajuste de la configuración**, configure los siguientes ajustes:
   Ajuste
   Qué hacer
   Nombre,
   Introduzca un nombre que identifique a esta configuración.
   Descripción
   Introduzca una descripción que explique la finalidad de esta configuración.**Seleccionar el dispositivo estándar**
   Seleccione el dispositivo de Windows 10 que tenga las aplicaciones aprovisionadas en el menú Inicio y en la Barra de tareas.
6. Haga clic en **Recuperar diseño del menú de inicio del dispositivo** y configure las opciones siguientes.
7. **Ajuste**
   Qué hacerDiseño del menú Inicio y Barra de tareas
   Seleccione cualquiera de las siguientes opciones para ocultar la lista de aplicaciones.
   - Ninguno
   - Ocultar lista de todas las aplicaciones
   - Ocultar lista de todas las aplicaciones y desactivar «Mostrar lista de aplicaciones en menú de inicio» en la aplicación Ajustes.
   - Ocultar lista de todas las aplicaciones, eliminar el botón de todas las aplicaciones y desactivar «Mostrar lista de aplicaciones en menú de inicio» en la aplicación Ajustes

Diseño del menú InicioPersonalizar el menú Inicio
Haga clic en **Sí** para personalizar el menú Inicio y los parámetros de diseño.**Barra de tareasPersonalizar barra de tareas**Haga clic en **Sí** para personalizar la barra de tareas.**Elimine los accesos directos existentes de la barra de tareas anclados antes de agregar los personalizados**Haga clic en **Sí** para eliminar el acceso directo anclado de la Barra de tareas antes de agregar el botón personalizado de Barra de tareas.**Tipo de aplicación**Especifica el tipo de aplicación.**Aplicación**Especifica el Id.de la aplicación.**Restaurar**
Haga clic en el enlace **Restablecer** para restablecer la Barra de tareas desde la barra de tareas del dispositivo Golden.
Haga clic y arrastre el icono de la flecha a la fila y mueva la posición (arriba o abajo) a la fila específica.
Haga clic en el icono de eliminar para eliminar la fila.
Haga clic en el botón **Añadir nueva** para añadir una nueva fila.

8. **Dispositivos de Windows 11**
   En la sección **Ajuste de la configuración**, configure los siguientes ajustes:
   Ajuste

Qué hacer

Nombre,

Introduzca un nombre que identifique a esta configuración.

Descripción

Introduzca una descripción que explique la finalidad de esta configuración.**Seleccionar el dispositivo estándar**

Seleccione el dispositivo de Windows 11 que tenga configuradas las aplicaciones en la sección PINNED del menú Inicio.**Diseño del menú Inicio y Barra de tareasDiseño del menú Inicio y Barra de tareas**

Seleccione una de las opciones siguientes para ver la opción de búsqueda en la barra de tareas:

- **Ocultar**
- **Icono Buscar**
- **Icono y etiqueta de búsqueda**
- **Cuadro de búsqueda (por defecto)**

Seleccione la casilla **Ocultar vista de tareas** para ocultar la vista de tareas.**Aplicaciones más utilizadas**

Seleccione una de las opciones siguientes para configurar las aplicaciones más utilizadas en el menú Inicio:

- **No imponer la visibilidad de la lista de aplicaciones más usadas en Inicio.**
- **Forzar la visualización de la lista de aplicaciones más utilizadas en Inicio.**
- **Forzar la ocultación de la lista de aplicaciones más utilizadas en Inicio.**

La casilla **Permitir fijación en barra de tareas** está seleccionada por defecto.

Seleccione la casilla **Ocultar sección recomendada** para ocultar todas las secciones recomendadas.

Debido a un problema del proveedor, la casilla de verificación **Ocultar sección recomendada** no tendrá un impacto visible en el dispositivo incluso después de que el usuario cierre o inicie sesión. Actualmente, no se puede ocultar la sección Recomendados.**Barra de tareasTipo de aplicación**

Seleccione una de las opciones siguientes para especificar el tipo de aplicación:

- **ID del modelo de usuario de la aplicación**
- **Ruta de enlace de la aplicación de escritorio**

AplicaciónEspecifica el Id. o la ruta de la aplicación.**Restaurar**

Haga clic en el enlace **Restablecer** para restablecer la Barra de tareas desde la barra de tareas del dispositivo Golden.

Haga clic y arrastre el icono de la flecha a la fila y mueva la posición (arriba o abajo) a la fila específica.

Haga clic en el icono de eliminar para eliminar la fila.

Haga clic en el botón **Añadir nueva** para añadir una nueva fila.

9. Haga clic en **Obtener el diseño del menú Inicio desde el dispositivo**.
10. Después de obtener los ajustes del dispositivo Golden, todas las aplicaciones configuradas en la sección PINNED del menú de inicio se mostrarán para que las revise el administrador.
    Haga clic en **Siguiente** y distribuya la configuración a todos los grupos de dispositivos y usuarios aplicables.

> Debido a un problema con el proveedor, cuando la configuración no se ha distribuido, las aplicaciones ancladas permanecerán en la configuración original. No obstante, cuando se distribuye una nueva configuración, el diseño anterior se reemplazará y el se aplicará el nuevo.

10.10.8.36. Configuración de la actualización del sistema

Los administradores pueden limitar a los usuarios de dispositivos para que no administren actualizaciones del sistema en dispositivos Android 6.0 o versiones más recientes compatibles. Esta función solo se aplica a los dispositivos Android Enterprise.

Para configurarlo:

1. Vaya a **Configuración > +Añadir**.
2. Seleccione configuración de **Actualización del sistema**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. En la sección Ajuste de la configuración, configure las siguientes opciones:

Ajuste	Descripción
Automático	Aplica silenciosamente la actualización del sistema siempre que haya un nuevo firmware disponible.
Posponer	Pospone 30 días la instalación de las actualizaciones del sistema. Una vez finalizado el período de 30 días, el sistema solicita al usuario del dispositivo que instale la actualización.
Modo de ventana (Hora local)	Programa un período de tiempo para aplicar silenciosamente la actualización del sistema. Seleccione las horas de **Hora de inicio** y **Hora de fin**.

Ajuste	Descripción
Actualización manual del SO (Android 10+) No aplicable ni compatible con dispositivos Samsung y Zebra	Seleccione realizar la actualización del SO manualmente en un número limitado de dispositivos antes de implementar la actualización para todos los dispositivos. **Archivo de firmware**: seleccione la opción **Atributo personalizado** o **URL HTTPS**. Introduzca los detalles siguientes: • Ubicación del firmware: si ha seleccionado **Atributo personalizado** como opción Archivo de firmware, deberá proporcionar el atributo personalizado que se utilizó para la transferencia de archivos. El archivo de firmware puede autoalojarse o cargarse en Ivanti Neurons for MDM mediante la configuración de Transferencia de archivos. Para más detalles, consulte la página **Configuración de transferencia de archivos**. Para cargar archivos de más de 50 MB en Ivanti Neurons for MDM se requiere una licencia adicional. • Descripción (opcional) • Huella digital (obligatoria): para validar que la versión del SO deseada esté instalada en el dispositivo. La huella digital se puede encontrar en el archivo OTA descomprimiendo la carpeta OTA y abriendo el archivo /META-INF/com/android/metadata. Busque una entrada similar a la siguiente: "post-build=google/xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxxxx:user/release-keys" En la entrada anterior, **google/ xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxx:user/release-keys** es la huella digital y TQ3A.230805.001.S1 es el ID de compilación (ID de compilación es el cuarto valor desde la izquierda en los valores separados por '/' en la huella digital). • Suma de comprobación (opcional) **Ajustes de actualización** → **Solicitud de actualización de SO**: los ajustes dentro de esta sección son los mismos para Zebra Firmware Configuration. Consulte la sección *Zebra Firmware Configuration* de esta tabla. Si selecciona **HTTPS URL** como opción de Archivo de Firmware, deberá proporcionar la siguiente información: • Ubicación del firmware: introduzca la ruta desde la que se puede descargar el firmware sin necesidad de autenticación. Descripción (opcional) • Huella digital (obligatoria): para validar que la versión del SO deseada esté instalada en el dispositivo. • Suma de comprobación (opcional) Tendrá las secciones **Iniciar solicitud de descarga** y **Durante las condiciones de descarga** además de la sección "**Solicitud de actualización del SO**". Las opciones disponibles en las secciones **Iniciar solicitud de descarga** y **Durante las condiciones de descarga** son las mismas que en la sección **Zebra Firmware Configuration**. Una vez que la actualización del sistema en el dispositivo se inicia después de la descarga, reiniciar el dispositivo en medio de una actualización aborta el proceso de actualización.
Periodo de inmovilización	Congela la actualización del sistema durante un período especificado. Esta opción solo corresponde a los Android 9.0+. Haga clic en **Agregar período de inmovilización**. Seleccione la **Fecha de inicio** y la **Fecha de fin** para el período de inmovilización. El período de inmovilización no puede ser superior a 90 días y se pueden agregar varios períodos de inmovilización. El siguiente período de inmovilización solo se puede seleccionar transcurridos 60 días desde la

Ajuste	Descripción
	fecha de fin del calendario anterior. Para eliminar un período de inmovilización, haga clic en el icono Eliminar.
Configuración del firmware de Zebra	Seleccione **Configurar Zebra OTA** para actualizar el firmware operativo de los dispositivos Zebra (con Android versión 8.0 o versiones más recientes compatibles). Esto solo es aplicable a los modos de Propietario del dispositivo. Para configurar actualizaciones de OTA de Zebra, debe habilitar el servicio de OTA de Ivanti Neurons for MDM en **Administración > Administración de Firmware > OTA de Zebra** y los dispositivos Zebra deben estar en Ivanti Neurons for MDM. Debe introducir sus credenciales de Zebra en la ventana emergente. Para recrear sus credenciales, contacte directamente con Zebra. Cuando se selecciona esta opción, se muestra la lista de dispositivos Zebra registrados. Para seleccionar y aplicar el firmware al modelo de dispositivo: 1. En la columna **Acción** del dispositivo Zebra, realice cualquiera de las siguientes acciones: ◦ **Ninguna**: no se realizará ninguna acción para ese modelo de dispositivo. ◦ **Actualización completa**. En la ventana **Seleccionar firmware de destino de Zebra**, seleccione la versión de la actualización completa del firmware que se aplicará al modelo de dispositivo. Durante el proceso de **Actualización completa**, solo es necesario el puerto 443. En el campo **Buscar**, puede escribir los caracteres de una Id. de compilación para buscar actualizaciones basadas en el ID de la compilación. Las Id. de la compilación se clasifican y se muestran en orden descendente (la última en la parte superior). La opción **Actualización de parches NO** estará disponible para dispositivos Android 11+. 2. Configure cualquiera de las siguientes opciones: **Iniciar solicitud de descarga**: Go app evaluará estas condiciones. ◦ **Nivel de batería mínimo requerido**: desplace el control deslizante para establecer el nivel de batería mínimo requerido desde el rango disponible. ◦ **Requerir que el dispositivo esté cargándose**: seleccione esta opción para mantener el dispositivo en modo de carga durante el proceso. ◦ **Programa de descarga**: seleccione esta opción para crear un programa para iniciar la solicitud de descarga y la descarga de archivos. ◦ Las opciones **Requerir tiempo de inactividad del dispositivo**, **Requerir recarga** y **Permitir las descargas en la red medida** se pasan al Administrador de descargas de Android. Go app agregará la solicitud descargada al Administrador de descargas de Android en la ventana indicada con los parámetros indicados arriba. **Aplicar horario de descarga**: seleccione los **Días de la semana** y la **Hora de inicio** y **Hora de fin** para programar la descarga. Se pueden seleccionar varios días para programar la descarga. Por ejemplo, si se selecciona el sábado y domingo con hora de inicio y de fin entre las 12:00 a. m. y las 11:00 p. m., la descarga se realiza en los dispositivos Zebra solo durante este período de tiempo para el día o los días seleccionados. En el Go app, la descarga se inicia según la programación, cuando se aplica la configuración en el dispositivo. No existe un límite de tiempo de finalización de la descarga, y puede completarse en un momento posterior a la hora de finalización programada. ◦ Aplicar horario de descarga: seleccione los **Días de la semana** y la **Hora de inicio** y **Hora de fin** para programar la instalación de la actualización del firmware.

Ajuste	Descripción
	La instalación se aplazará si el nivel de la batería del dispositivo es inferior a 32. Si no se configura ningún programa de actualización, la instalación comenzará inmediatamente después de que se complete la descarga del firmware. 3. Configure cualquiera de las siguientes opciones: **Condiciones durante la descarga**: estas condiciones se evaluarán con el Gestor de descargas. Puede hacer la selección según los criterios. ◦ **Requiere que el dispositivo esté inactivo** (seleccionado por defecto): permite actualizaciones de firmware en el dispositivo cuando el dispositivo está inactivo. ◦ **Requiere carga** (seleccionado por defecto): permite actualizaciones del firmware en el dispositivo cuando está en modo de carga. ◦ **Permitir descargar a través de redes de uso medido**: seleccione esta opción para permitir la descarga en modo Wi-Fi. Esta opción no está seleccionada de forma predeterminada. ◦ Las opciones **Requerir tiempo de inactividad del dispositivo**, **Requerir recarga** y **Permitir las descargas en la red medida** se pasan al Administrador de descargas de Android. Go app agregará la solicitud descargada al Administrador de descargas de Android en la ventana indicada con los parámetros indicados arriba. **Permitir descargar para continuar fuera del "programa de descarga" especificado**: seleccione esta opción para permitir la descarga fuera del programa de descarga especificado. **Solicitud de actualización del SO** ◦ **Nivel mínimo de batería requerido**: seleccione esta opción para establecer el nivel mínimo de batería que debe estar disponible para solicitar la actualización del SO. ◦ **Requerir que el dispositivo esté cargándose**: seleccione esta opción para mantener el dispositivo en modo de carga durante el proceso. ◦ **Crear horario para iniciar la actualización del SO en el dispositivo**: seleccione esta opción para establecer un horario en el que se iniciará la actualización del SO en el dispositivo. En el Go app, la descarga se inicia según la programación, cuando se aplica la configuración en el dispositivo. No existe un límite de tiempo de finalización de la descarga, y puede completarse en un momento posterior a la hora de finalización programada. Haga clic en **Aplicar**.
Configuración de Samsung E-FOTA	Seleccione **Configurar Samsung e-FOTA** para actualizar el firmware operativo de los dispositivos Samsung (en la versión 2.7.1 de Knox y superior). Esto solo es aplicable a los modos de Dispositivo administrado con Perfil de trabajo en el Dispositivo propiedad de la empresa. Si no hay registrados dispositivos compatibles con Samsung E-FOTA, se muestra un mensaje con esta información en la página. Para configurar las actualizaciones de la licencia de Samsung E-FOTA, debe activar la licencia de Samsung E-FOTA en **Administración > Administración de Firmware > Samsung E-FOTA**. Al seleccionar esta opción, se mostrará la lista de dispositivos Samsung registrados. Para seleccionar y aplicar el firmware al modelo de dispositivo: 1. En la columna **Acción** del dispositivo Samsung, realice cualquiera de las siguientes acciones: ◦ **Última**: se aplica la última versión del firmware. Esta opción está seleccionada de forma predeterminada.

Ajuste	Descripción
	◦ **Forzar**: en la ventana Seleccionar firmware de destino de Samsung, seleccione la versión de firmware concreta que se aplicará de forma forzada (sin intervención del usuario) al modelo de dispositivo. Cuando se realiza esta acción, la descarga del firmware comienza en quince minutos. ◦ **Destino**: en la ventana Seleccionar firmware de destino de Zebra, seleccione la versión de la actualización completa del firmware que se aplicará al modelo de dispositivo. Al realizar las acciones «Forzar» o «Destino», si no hay un firmware enumerado para el dispositivo, aparecerá un mensaje con esta información en la página. 2. **Habilitar depuración del firmware** (Opcional): cuando la opción **Activar depuración del firmware** está activada y se aplica la configuración, el dispositivo se actualiza a un firmware ficticio. El firmware ficticio del firmware del dispositivo Samsung permite al administrador probar el comportamiento de la configuración de la actualización del sistema en los dispositivos, sin modificar nada en el dispositivo. Para actualizar a la mejora real de firmware, en lugar del firmware ficticio, el administrador debe asegurarse de que la opción **Habilitar FW de depuración** esté deshabilitada antes de aplicar la configuración. 3. Haga clic en **Aplicar**.

6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones de distribución:

- Todos los dispositivos
- Ningún dispositivo (predeterminada)
- personalizada

8. Haga clic en **Hecho**.

Configuración de Samsung E-FOTA (Retirado)

La configuración de Samsung E-FOTA ha quedado en desuso desde julio de 2022. Por lo tanto, esta configuración no estará disponible para nuevos dispositivos. Los dispositivos con la configuración existente solo pueden desactivar esta configuración.

10.10.8.37. Administración de actualización de Windows 10

Como administrador, puede ver y aprobar las actualizaciones notificadas por los dispositivos Windows 10 que desee actualizar mediante Windows 10 Update Management. Mediante esta característica, puede evitar que las actualizaciones innecesarias o no probadas se instalen en los dispositivos.

La función Administración de actualizaciones requiere que los dispositivos se configuren con la configuración **Actualizaciones de software** con la opción **Solicitar aprobación de actualización** habilitada. Solo aplicando esta configuración a los dispositivos, estos notificarán las actualizaciones para la instalación y esperarán la aprobación.

Administrar actualizaciones

1. Vaya a **Administrador >Windows > Actualizaciones de Windows.** En la página se mostrarán los siguientes detalles de las actualizaciones.
   Fecha de creación: la fecha en la que se creó la actualización.**Título**: describe el tipo de actualización junto con el número de artículo de la base de conocimientos.

> Al hacer clic en la actualización, aparecerá su descripción.

Clasificación: clasifica el tipo de actualización en una de las siguientes categorías:

- Actualizaciones críticas
- Actualizaciones de definiciones
- Actualizaciones de controladores
- Actualizaciones de seguridad
- Actualizaciones
- Actualización
- Actualizar lanzamientos

Distribución: la distribución realizada para la actualización. Por ejemplo, indicará **Todos** cuando la actualización se haya distribuido a todos los dispositivos.

> Si la actualización se ha distribuido a un cierto número de grupos específico, indicará el recuento de la distribución. Por ejemplo, indicará 3 si la distribución se ha realizado solo en 3 grupos.

2. Además, puede ver si se ha distribuido o no una actualización en los dispositivos requeridos. Las columnas siguientes tienen números que indican el número de dispositivos presentes en distintas categorías de las actualizaciones:
   - Dispositivos elegibles
   - Dispositivos instalados
   - Dispositivos fallidos
   - Reinice los dispositivos pendientes

Cuando hace clic sobre cualquiera de estos números, se le dirigirá a la vista filtrada de la página Dispositivos para conocer el estado de las actualizaciones y llevar a cabo las acciones necesarias.

Revise las actualizaciones y seleccione la que desea distribuir a los dispositivos haciendo clic en la casilla de verificación de dicha actualización.

3. En **Acciones**, clic en **Establecer distribución**.
4. En la ventana **Distribuir actualización de Windows**, seleccione cualquiera de las siguientes opciones de distribución:
   Todos los dispositivos: distribuye las actualizaciones a todos los dispositivos.
   Ningún dispositivo: retiene las actualizaciones y no las distribuye a ningún dispositivo.**Personalizada**: distribuye las actualizaciones para los grupos de dispositivos especificados.
5. Haga clic en **Guardar**.

Buscar y filtrar actualizaciones

Puede buscar y filtrar actualizaciones en función de los siguientes criterios:

- Id. del artículo de la base de conocimientos
- Distribución configurada

Filtrar en función de la Id. del artículo de la base de conocimientos:

1. En la página **Gestión de actualizaciones de Windows 10**, escriba el ID de la base de conocimientos en el campo de búsqueda rápida (solo el número en el campo Buscar).
   Ejemplo: para KB4056892, escriba 4056892. Aparecerá en la página la actualización que coincida con los criterios de búsqueda.

> Puede seguir buscando información adicional sobre la actualización haciendo clic en el enlace **Asistencia técnica** y **Más información**. Los enlaces de la **Asistencia técnica** dirigen a la página web de Microsoft que proporciona información sobre asistencia de productos para la actualización y **Más información** dirige a la página web de Microsoft que muestra más información sobre la actualización, como el artículo de la base de conocimientos.

Filtrar en función de la distribución configurada:

En la página **Gestión de actualizaciones de Windows 10**, seleccione cualquiera de las siguientes opciones de filtrado en función de la distribución configurada:

- **Todas**: se muestran todas las actualizaciones.
- **Configuradas**: se muestra la lista de actualizaciones que se han distribuido a los dispositivos.
- **No configuradas**: se muestra la lista de actualizaciones para las que no se ha especificado ninguna distribución.

> Los filtros Configuradas y No configuradas se basan en la distribución realizada y la distribución también puede ser **Ninguna**.

Ver actualizaciones para un dispositivo

Para ver la información detallada sobre actualizaciones específicas para un dispositivo:

1. Vaya a **Dispositivos > Dispositivos**.
2. Haga clic en el nombre del dispositivo para visualizar la página de detalles.
3. Vaya a la pestaña **Actualizaciones**. Se mostrarán las actualizaciones para el dispositivo que estén pendientes (actualización aprobada por el administrador pero no notificada como instalada en el dispositivo), que hayan fallado y que se hayan instalado.

También puede ver notificaciones sobre nuevas actualizaciones de Windows disponibles en la página «Notificaciones», en «Panel». La notificación incluye la fecha de creación de la misma, el número de notificaciones disponibles y el fin de dicha notificación. La notificación de la actualización de Windows también está visible la esquina superior derecha del Portal de administración.

10.10.8.38. Programación de aplicaciones Windows

Las aplicaciones de escritorio de Windows pueden ser grandes, lo cual añade una carga adicional y ampliada a las redes y servidores durante horas de uso fundamentales para la empresa. La característica de programación de aplicaciones de Windows le permite programar un momento para instalar aplicaciones, sobre todo las grandes, en los dispositivos durante las horas que usted elija.

Para configurar la programación de aplicaciones:

1. Vaya a **Aplicaciones > Catálogo de aplicaciones**.
2. Haga clic en **Agregar** y seleccione una aplicación de Windows y continúe a los pasos siguientes en el asistente de **Agregar aplicación**.
3. En el paso 5(Configure), haga clic en **Instalar los ajustes de configuración de la aplicación** para ver la página **Ajustes de configuración**.
4. Marque la casilla **Programar instalación**.

> La casilla **Programar instalación** solo aparece cuando está activada la instalación silenciosa.

5. Seleccione una **Hora de inicio** y una **Hora de fin** para programar la hora a la que se instalará las aplicaciones.
6. Seleccione una **Fecha de inicio** y una **Fecha final** para programar la fecha en la que se instalarán las aplicaciones.

> También puede seleccionar una de estas dos acciones, que se debe llevar a cabo cuando no se aprovecha la fecha programada: **Instalar durante la siguiente conexión** o **No instalar**.

7. Seleccione una opción de distribución de configuración de aplicaciones:**Todos los que tengan la aplicación**, **Nadie** o **Personalizado**.
8. Haga clic en **Hecho**.

> Las aplicaciones que es necesario programar no deben añadirse a Apps@Work.
> La programación de aplicaciones no es aplicable para las aplicaciones de la Store porque no está admitida la instalación silenciosa de aplicaciones de la Store.

10.10.8.39. Configuración del BIOS de Windows

Los administradores pueden configurar los ajustes del BIOS de Windows en dispositivos Lenovo. Para establecer esta configuración, hay que inscribir al menos un dispositivo Lenovo compatible con los ajustes del BIOS.

Para configurarlo:

1. Vaya a **Configuración > +Añadir**.
2. Seleccione la configuración **BIOS de Windows**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. En la sección «Elegir modelo de dispositivo», seleccione el modelo de dispositivo de la lista desplegable.
6. En la sección Ajuste de la configuración, configure las siguientes opciones:

> La lista de ajustes varía según los que estén disponibles para el modelo específico de dispositivo que se haya inscrito. Para obtener más información, consulte el sitio web correspondiente del dispositivo.

Ajuste	Qué hacer
Control de AMT	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
CA de administración térmica adaptable	Seleccione cualquiera de las siguientes opciones: • **Equilibrado** • **Rendimiento máximo**
Batería de administración térmica adaptable	Seleccione cualquiera de las siguientes opciones: • **Equilibrado** • **Rendimiento máximo**
USB siempre activado	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
BIOSPasswordAtBootDeviceList	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Contraseña de BIOS al reiniciar	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Contraseña de BIOS con arranque desatendido	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Actualización de BIOS por los usuarios finales	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Acceso Bluetooth	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Opción F12 de la lista de dispositivos de arranque	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**

Ajuste	Qué hacer
Dispositivo de visualización de arranque	Seleccione cualquiera de las siguientes opciones: • **DisplayPort** • **Pantalla de Dock** • **HDMI** • **LCD**
Modo de arranque	Seleccione cualquiera de las siguientes opciones: • **Diagnóstico** • **Rápido**
Bloqueo de la orden de arranque	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
BootTimeExtension	Seleccione cualquiera de las siguientes opciones: • **1** • **10** • **2** • **3** • **5** • **Desactivar**
Manipulación detectada de BottomCover	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Administración de energía de la CPU	Seleccione cualquiera de las siguientes opciones: • **Automático** • **Desactivar**
Activación del módulo Computrace	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Prevención de ejecución de datos	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Acceso a la red LAN de Ethernet	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
ROM de opción de la LAN de Ethernet	Seleccione cualquiera de las siguientes opciones: • **Desactivar**

Ajuste	Qué hacer
	• **Activar**
Autenticación de la contraseña con huella digital	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Autenticación preescritorio con huella digital	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Acceso al lector de huella digital	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Prioridad del lector de huella digital	Seleccione cualquiera de las siguientes opciones: • **Externo** • **Solo interno**
Modo de seguridad de huella digital	Seleccione cualquiera de las siguientes opciones: • **Alto** • **Normal**
Cambio de tecla Fn Ctrl	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
FnKeyAsPrimary	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
FnSticky	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Pila de red IPv4	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Pila de red IPv6	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Acceso a la cámara integrada	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**

Ajuste	Qué hacer
InternalStorageTamper	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Pitido del teclado	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Ajuste de BIOS de bloqueo	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Acceso a la ranura para tarjeta de memoria	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Acceso al micrófono	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Longitud mínima de la contraseña	Seleccione cualquiera de las siguientes opciones: • 4 • 5 • 6 • 7 • 8 • 9 • 10 • 11 • 12 • **Desactivar**
NFFControl	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Acceso NFC	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Activado al conectar CA	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**

Ajuste	Qué hacer
PasswordBeep	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Error de recuento excedido en la contraseña	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Presencia física para borrado de TPM	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Presencia física para aprovisionamiento de TPM	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Tecnología Rapid Start	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Arranque seguro	Seleccione **Activar**
Prevención de recuperación segura	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Chip de seguridad	Seleccione cualquiera de las siguientes opciones: • **Activo** • **Desactivar** • **Activar** • **Inactivo**
Acceso a la ranura para Smart Card	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
SpeedStep	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Teclas de opciones de inicio	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Función TXT	Seleccione cualquiera de las siguientes opciones:

Ajuste	Qué hacer
	• **Desactivar** • **Activar**
Memoria Total Graphics	Seleccione cualquiera de las siguientes opciones: • **256 MB** • **512 MB**
TouchPad	Seleccione cualquiera de las siguientes opciones: • **Automático** • **Desactivar**
TrackPoint	Seleccione cualquiera de las siguientes opciones: • **Automático** • **Desactivar**
Modo USB30	Seleccione cualquiera de las siguientes opciones: • **Automático** • **Desactivar** • **Activar**
Compatibilidad con BIOS de USB	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Acceso al puerto USB	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Prioridad del arranque UEFI PXE	Seleccione cualquiera de las siguientes opciones: • **Primero IPv4** • **Primero IPv6**
Función VTd	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Tecnología Virtualization	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**

Ajuste	Qué hacer
Wake on LAN	Seleccione cualquiera de las siguientes opciones: • **Solo CA** • **CA y batería** • **Desactivar** • **Activar**
Acceso a la red LAN inalámbrica	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**
Acceso a la red WAN inalámbrica	Seleccione cualquiera de las siguientes opciones: • **Desactivar** • **Activar**

7. Haga clic en **Siguiente**.
8. Seleccione una de las siguientes opciones de distribución:
   - Todos los dispositivos
   - Ningún dispositivo (predeterminada)
   - personalizada
9. Haga clic en **Hecho**.

10.10.8.40. BitLocker de Windows

Como administrador, puede actualizar en masa la clave de recuperación para un conjunto de dispositivos cifrados de Windows 10 cargando un archivo de Excel con el GUID del dispositivo y la contraseña de recuperación.

Para subir el archivo de Excel para la actualización en masa de la clave de recuperación:

1. Vaya a **Administrador > Windows BitLocker**.
2. Haga clic en **Descargar archivo CSV de muestra** para descargar el archivo CSV de muestra y ver un ejemplo de archivo .csv.
3. Cree y añada los registros del archivo .csv para las claves de recuperación de BitLocker.
4. Haga clic en **Cargar contraseñas de recuperación**
5. Haga clic en **Elegir archivo** para cargar el archivo .csv que ha creado.
6. Haga clic en **Cargar**. Al cargar un nuevo archivo con claves previamente subidas se sobrescribirán las entradas antiguas.

> Se pueden enviar un máximo de 1000 registros en cada carga. Después de realizar correctamente la carga, puede ver las claves individuales en los detalles del dispositivo específico.

10.10.8.41. Configuración del kiosco de Windows

Con la configuración del kiosco de Windows, se puede configurar un kiosco de una sola o varias aplicaciones en dispositivos Windows 10. Al aplicar esta configuración, sus usuarios del kiosco no podrán acceder a ninguna característica fuera de las aplicaciones del kiosco. Esta configuración requiere que Windows Bridge esté activado.

A continuación se especifican los 3 modos en los que se puede aplicar esta configuración.

- Una sola aplicación
- Varias aplicaciones (obtener la lista de aplicaciones del dispositivo Windows)
- Varias aplicaciones (seleccionar un diseño existente en la configuración del menú de inicio)

> Las aplicaciones que se utilicen para una configuración del kiosco de Windows deben estar ya presentes en el dispositivo antes de entrar en un modo kiosco de Windows configurado.

Para ajustar la configuración del kiosco de Windows:

1. Vaya a **Configuración > +Añadir**.
2. Seleccione la configuración **Kiosco de Windows**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. En la sección Establecimiento de la configuración, especifique los demás ajustes según se describe en la siguiente tabla.

Ajuste	Qué hacer
Seleccione el modo kiosco: seleccione cualquiera de las siguientes tres opciones.	
Una sola aplicación	Seleccione esta opción para configurar el modo kiosco de una sola aplicación para un dispositivo. 1. En la sección **Seleccione el dispositivo Windows (opcional)**, elija un dispositivo Windows 10. Haga clic en **Recuperar aplicaciones desde dispositivos** para recuperar la lista de aplicaciones desde un dispositivo. El dispositivo que seleccione debe estar bajo su supervisión y requiere un ingreso para poder recuperar correctamente los datos de la aplicación. Para saltar estos pasos, seleccione la casilla de verificación **Saltar este paso. Puede cambiar de opinión más tarde si lo desea**. 2. Haga clic en **Añadir desde la lista de aplicaciones recuperadas** para añadir aplicaciones desde la lista recuperada. 3. Seleccione una sola aplicación haciendo clic en el botón de radio que hay en la columna **Nombre** de la aplicación. Haga clic en **Añadir nueva** para añadir una nueva aplicación a la lista. Para borrar una aplicación de la lista, haga clic en el icono Eliminar.
Varias aplicaciones (obtener la lista de aplicaciones del dispositivo Windows)	Seleccione esta opción para configurar el modo kiosco de varias aplicaciones para un dispositivo. 1. En la sección **Seleccione el dispositivo Windows (opcional)**, elija un dispositivo Windows 10. Haga clic en **Recuperar aplicaciones desde el dispositivo** para recuperar la lista de aplicaciones desde un dispositivo. El dispositivo que seleccione debe estar bajo su supervisión y requiere un ingreso para recuperar correctamente datos de las aplicaciones. Para saltar estos pasos, seleccione la casilla de verificación **Saltar este paso. Puede cambiar de opinión más tarde si lo desea**. 2. En la opción **Diseño de las aplicaciones del kiosco y del menú de inicio**, haga clic en **Añadir desde la lista de aplicaciones recuperadas**. Aparecerá la ventana **Seleccionar aplicación del kiosco**. Seleccione la(s) aplicación(es) desde la lista de aplicaciones recuperadas y haga clic en **Usar aplicación seleccionada**. 3. En la sección Aplicaciones permitidas adicionales, haga clic en **Añadir desde la lista de aplicaciones recuperadas**. Aparecerá la ventana **Seleccionar aplicación del kiosco**. Seleccione la(s) aplicación(es) desde la lista de aplicaciones recuperadas y haga clic en **Usar aplicación seleccionada**. Las aplicaciones adicionales permitidas son aquellas aplicaciones que se consideran dependencias de las aplicaciones seleccionadas en **Diseño de las aplicaciones del kiosco y del menú de inicio.** Sin esas «aplicaciones permitidas», el SO no permite ejecutar esta aplicación ni siquiera aunque aparezca el icono de la aplicación en el menú de inicio. 4. Haga clic en **Añadir nueva** para agregar una nueva aplicación a la lista. Para borrar una aplicación de la lista, haga clic en el icono Eliminar. Puede arrastrar y mover una aplicación de la lista a cualquier posición dentro de esta. 5. En los **Otros ajustes de varias aplicaciones**, seleccione las opciones necesarias: ◦ **Ocultar el botón de encendido** ◦ **Ocultar la casilla de usuario**

Ajuste	Qué hacer
	◦ **Ocultar la barra de tareas** En Microsoft Windows 11, la opción de modo quiosco para varias aplicaciones "**Ocultar barra de tareas**" no es compatible.
Varias aplicaciones (seleccionar un diseño existente en la configuración del menú de inicio)	Si ha creado una configuración de diseño del menú de inicio, se puede importar esa configuración y usarla para configurar el modo de varias aplicaciones seleccionando esta opción. 1. En la sección **Seleccione diseño**, elija un diseño que se haya configurado anteriormente como Configuración del menú de inicio. En la lista desplegable que aparece a continuación se indican las configuraciones previamente creadas con parámetros de diseño aplicables. 2. En los Otros ajustes de varias aplicaciones, seleccione las opciones necesarias: ◦ **Ocultar el botón de encendido** ◦ **Ocultar la casilla de usuario** ◦ **Ocultar la barra de tareas** En Microsoft Windows 11, la opción de modo quiosco para varias aplicaciones "**Ocultar barra de tareas**" no es compatible.

6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones de distribución:

- Todos los dispositivos
- Ningún dispositivo (predeterminada)
- personalizada

8. Haga clic en **Hecho**.

> Para que la configuración tenga un efecto completo, el dispositivo debe reiniciarse después de aplicar o actualizar una configuración del kiosco de Windows. Según las aplicaciones para la configuración de kioscos multiaplicación, es necesario reiniciar un dispositivo por segunda vez. Algunos iconos pueden no aparecer en el primer inicio de sesión, pero los iconos que faltan se mostrarán en el siguiente inicio de sesión después del segundo reinicio.

El dispositivo debe reiniciarse después de aplicar, eliminar o actualizar una configuración de kiosco. Esto se puede hacer con el comando Reiniciar/apagar dispositivo en el menú de acciones del dispositivo. Sin reiniciar:

- El dispositivo no entra automáticamente en el modo kiosco después de aplicar una configuración de kiosco.
- El dispositivo no sale automáticamente del modo kiosco después de eliminar una configuración de kiosco aplicada.
- El dispositivo no cambia la configuración del kiosco en ejecución.

Si un dispositivo con una configuración de kiosco aplicada recibe una configuración actualizada, el sistema operativo Windows del dispositivo eliminará a un usuario existente del kiosco y recreará un nuevo usuario de kiosco con una nueva configuración de kiosco. La sesión del usuario actual debe finalizar explícitamente con el reinicio del dispositivo.

Es preferible configurar con archivos '.lnk' para una configuración de kiosco de varias aplicaciones y '.exe' para una configuración de kiosco de una sola aplicación («single-app»). Una configuración importada del menú de inicio desde un dispositivo utiliza el formato '.lnk'. Los elementos del menú de inicio creados manualmente para las aplicaciones '.exe' podrían en algún momento no mostrarse en el menú de inicio de la configuración del kiosco de varias aplicaciones, en función de la aplicación '.exe'.

Por ejemplo, se puede agregar el Reproductor de Windows Media al menú de inicio utilizando uno de los siguientes archivos '.lnk':

- %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Media Player.lnk
- %ALLUSERSPROFILE%\Microsoft\\Windows\Start Menu\Programs\Windows Media Player.lnk

Si esta aplicación se añade directamente con cualquiera de los siguientes archivos '.exe', no se mostrará el icono correspondiente, incluso la primera ruta '.exe' se utiliza internamente en los archivos '.lnk' anteriores:

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
- C:\Program Files\Windows Media Player\wmplayer.exe

Para la configuración de kiosco de una sola aplicación, puede añadir argumentos al archivo exe. E.g. '%ProgramFiles%\Internet Explorer\iexplore.exe -k www.bing.com'. Sin embargo, el icono de la aplicación exe con argumentos no se muestra en el menú de inicio en el caso de una configuración de varias aplicaciones. Si necesita una aplicación exe con argumentos en la configuración del kiosco de varia aplicaciones, utilice el archivo '.lnk' que puede tener argumentos internamente. '.lnk' no funciona en el caso de una configuración de kiosco de una sola aplicación.

Dependencias en el modo kiosco de varias aplicaciones

Las aplicaciones Win32/64 podrían requerir que se añadan dependencias a la sección de aplicaciones adicionales permitidas en el modo kiosco de varias aplicaciones. Las aplicaciones adicionales permitidas no son necesarias para el modo kiosco de una sola aplicación.

Ejemplo 1 : para la aplicación Reproductor de Windows Media, se requieren las siguientes dependencias en el modo kiosco de varias aplicaciones:

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\setup_wm.exe

La primera dependencia son los binarios de la aplicación llamados desde el archivo ".lnk" correspondiente. El segundo es un asistente de una sola vez llamado desde la primera dependencia.

Sin las aplicaciones permitidas, el sistema operativo no permite ejecutar esta aplicación incluso cuando el icono de la aplicación se muestra en el menú de inicio.

Ejemplo 2: para Internet Explorer, su icono se muestra en el menú de inicio si está configurado con cualquier elemento de la siguiente lista:

- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Accessories\Internet Explorer.lnk
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Internet Explorer.lnk
- C:\Program Files\internet explorer\iexplore.exe
- %ProgramFiles%\Internet Explorer\iexplore.exe

Internet Explorer requiere las siguientes dependencias:

- C:\Program Files (x86)\Internet Explorer\iexplore.exe
- C:\Program Files (x86)\Internet Explorer\ExtExport.exe
- C:\Program Files (x86)\Internet Explorer\ieinstal.exe
- C:\Program Files (x86)\Internet Explorer\ielowutil.exe

La primera dependencia son los binarios de la aplicación requeridos para el elemento '.lnk' solamente; las otras dependencias son para el asistente de una sola vez. Sin la primera dependencia, el sistema operativo bloquea la aplicación con el elemento emergente. Sin otras dependencias, la aplicación se cierra justo después del inicio sin ninguna notificación adicional del sistema operativo.

10.10.8.42. Configuración de la licencia de Windows

La configuración de la licencia de Windows actualiza el sistema operativo del dispositivo, como por ejemplo de Windows 10 Pro a Windows 10 Enterprise. Además, esta configuración ofrece la posibilidad de activar o modificar la clave de producto de los dispositivos de escritorio Windows 10.

Para actualizar una licencia de Windows:

1. Vaya a **Configuración > +Añadir**.
2. Seleccione la configuración de **Licencia de Windows**.
3. Introduzca un nombre para la configuración.
4. En la sección **Establecimiento de la configuración**, escriba la **Clave de producto** de Windows.
5. Haga clic en **Siguiente**.
6. Seleccione una de las siguientes opciones de distribución:
    - Todos los dispositivos
    - Ningún dispositivo (predeterminada)
    - personalizada
7. Haga clic en **Hecho**.

11. Políticas

Las Directivas definen los requisitos para los dispositivos, así como lo que pasará si un dispositivo no cumple con los requisitos. Cada política cuenta con una regla y una medida de cumplimiento (lo que sucede si se infringe la regla). Utilice la página **Políticas** para seleccionar, configurar y distribuir políticas.

> Con el proceso automatizado de registro de dispositivos, tenga en cuenta los cambios siguientes:

- Solo se evaluarán los dispositivos que se hayan registrado durante los últimos 90 días.
- Solo se enviará el comando de registro forzado a los dispositivos que se hayan registrado hace más de 90 días pero menos de un año.
- No se realizará ninguna acción en los dispositivos que no se hayan registrado durante el último año.

Esta sección contiene los siguientes temas:

- **Trabajar con políticas**
- **Política personalizada**
- **Supervisar y controlar las aplicaciones permitidas**
- **Priorizar políticas**
- **Política de hardware de Windows**

11.1. Trabajar con políticas

Esta sección contiene los siguientes temas:

- Aplicar las políticas
- Medidas de cumplimiento
- Encontrar una política existente
- Añadir una política
- Editar una política
- Eliminar una política

Aplicar las políticas

Las Directivas definen los requisitos para los dispositivos, así como lo que pasará si un dispositivo no cumple con los requisitos. Cada política cuenta con una regla y una medida de cumplimiento (lo que sucede si se infringe la regla). Utilice la página **Políticas** para seleccionar, configurar y distribuir políticas.

Existen los siguientes tipos de políticas:

Tipo	Qué hace
Dispositivos afectados	Prioridad (1 = la más alta) Infracción 1 Plugin en riesgo 2 Cliente manipulado 3 Fabricante de dispositivos desconocido: desconocido 4 Carpeta sospechosa detectada: [ruta] 5 Se ha encontrado un binario sospechoso en: [ruta] 6 La carpeta /data es navegable o la carpeta /data/data es navegable 7 Se encontró /system/app/Superuser.apk 8 El administrador del paquete ha sido vulnerado 9 Se ha encontrado una aplicación sospechosa: [package] Marca los dispositivos en los que se realizó un jailbreak (iOS) o se accedió a la raíz (Android). Para ver el motivo de la infracción por el que el sistema marcó un dispositivo Android como en riesgo debido a las violaciones de la seguridad de raíz: 1. Haga clic en la pestaña **Políticas**. 2. Haga clic en el enlace **Dispositivos en riesgo**. 3. Haga clic en la pestaña **Infracciones activas**. 4. Compruebe el motivo de la infracción en la columna Infracción. Para ver el motivo de la infracción por el que el sistema marcó un dispositivo Android como en riesgo debido a las violaciones de la seguridad de raíz: 5. Haga clic en la pestaña **Políticas**. 6. Haga clic en el enlace **Dispositivos en riesgo**. 7. Haga clic en la pestaña **Infracciones activas**. 8. Compruebe el motivo de la infracción en la columna **Infracción**. Será uno de los motivos siguientes:
Protección de datos/Cifrado deshabilitado (solo macOS)	Marca los dispositivos macOS que no tienen habilitado ningún código de acceso o cifrado.
Itinerancia internacional	Marca los dispositivos que podrían incurrir en cargos por itinerancia internacional. El estado se actualiza cuando el dispositivo ingresa. En iOS, el dispositivo utiliza la marca de itinerancia según lo establece y notifica iOS. La medida de cumplimiento solo se genera en la primera infracción.
MDM/Administración de dispositivos desactivada	Si el dispositivo está desactivado para MDM, no será evaluado para ninguna otra política o procesamiento delta más de configuraciones o aplicaciones durante los ingresos.
Fuera de contacto	Marca los dispositivos que estuvieron fuera de contacto con Ivanti Neurons for MDM por el margen de tiempo determinado. Elija las acciones que quiere llevar a cabo si un dispositivo no ha ingresado durante un intervalo determinado de horas (2-3 a 23-24) o número de días.

Tipo	Qué hace
Cliente MI fuera de contacto (solo iOS)	Marca los clientes de Ivanti Neurons for MDM que estuvieron fuera de contacto con Ivanti Neurons for MDM por el margen de tiempo determinado. Elija las acciones que quiere llevar a cabo si el cliente no ha ingresado durante un intervalo determinado de horas (2-3 a 23-24) o número de días. Esto también es aplicable a los dispositivos registrados a través de iReg. Esta política marca el dispositivo como no cumplidor si no hay ningún cliente o si el cliente no ha ingresado durante un período de tiempo definido.
Aplicaciones permitidas	Marca los dispositivos que infringen las reglas sobre qué aplicaciones están permitidas o son obligatorias.
Política personalizada	Crea una política personalizada basada en condiciones y acciones relacionadas que usted especifique.

Medidas de cumplimiento

Están disponibles las siguientes opciones de cumplimiento:

Medida de cumplimiento	Qué hace
Supervisar	Etiqueta el dispositivo de la página Dispositivos de Ivanti Neurons for MDM. Esta acción está activada de forma predeterminada.
Bloquear	Indica a Access o Sentry que deben bloquear un dispositivo si éste intenta acceder a un recurso a través de Sentry o Access después de incumplir la política en los detalles del último contacto.

Enviar un mensaje al usuario	• Etiqueta el dispositivo de la página Dispositivos de Ivanti Neurons for MDM.
	• Envía un correo electrónico al propietario del dispositivo.
	• Además de las políticas existentes, ahora la opción "**Usar la plantilla de correo electrónico de la política de legalidad**" también está disponible para las políticas siguientes:
	  ◦ Protección/cifrado de datos deshabilitado
	  ◦ Itinerancia internacional
	  ◦ MDM/Administración de dispositivos desactivada
	  ◦ Fuera de contacto
	  ◦ Cliente MI fuera de contacto
	Envía una notificación push al dispositivo.

Cuarentena	• Elimina la mayoría de las configuraciones del dispositivo. ◦ Excepciones: Configuraciones del código de acceso, Configuraciones de Wi-Fi para dispositivos de solo Wi-Fi, Configuraciones de restricciones (iOS). • Elimina todas la aplicaciones instaladas por Ivanti Neurons for MDM. • Elimina todo el contenido distribuido por Ivanti Neurons for MDM, incluidos los archivos de iBook y ePub. • Bloquea el acceso a los catálogos de Ivanti Neurons for MDM. • Suspende los avisos para instalar aplicaciones adicionales. • Bloquea el acceso a las aplicaciones habilitadas para AppConnect. • Incluye compatibilidad para aplicaciones habilitadas para AppConnect. • Si está activado, suspende las aplicaciones del área personal del dispositivo en cuarentena para indicar que el usuario del dispositivo tiene que atender los problemas de cumplimiento del dispositivo para que este vuelva a ser funcional. Compatible con los dispositivos Android 11+ provistos con el Perfil de trabajo en el Dispositivo propiedad de la empresa.
Acciones de cuarentena adicionales (opcional):	**Bloquear la descarga de aplicaciones nuevas**: evita la descarga de aplicaciones nuevas en el dispositivo. **Poner las aplicaciones administradas en cuarentena**: elimina las aplicaciones administradas por Ivanti Neurons for MDM del dispositivo y permite la opción Bloquear nuevas descargas de aplicaciones para impedir que se puedan volver a instalar las aplicaciones en el dispositivo. Seleccione una de las siguientes opciones: • **Todas las aplicaciones** • **Eliminar todas las aplicaciones excepto las siguientes**: eliminar todas las aplicaciones excepto las que se añaden a la lista de aplicaciones.

Medida de cumplimiento	Qué hace
	• **Aplicaciones designadas:** añada una o más aplicaciones por medio de búsqueda o de forma manual (utilizando la Id. de conjunto o el nombre del paquete). Haga clic en la pestaña **Ver aplicaciones** para ver la lista de aplicaciones añadidas. No se encuentra disponible la acción de cuarentena de la función predeterminada Bloquear acceso a la App Store. En algunos dispositivos, la acción de cuarentena no eliminará la aplicación del dispositivo debido a ciertas limitaciones del mismo. Por defecto, esta opción está seleccionada (para las tres: Todas las aplicaciones, Quitar todas las aplicaciones excepto las siguientes y Aplicaciones designadas) y no se puede cancelar la selección. Esto impide que las aplicaciones se reinstalen en el dispositivo. **Eliminar configuraciones**: elimina las configuraciones de Ivanti Neurons for MDM del dispositivo. Seleccione una de las siguientes opciones: • **Todas las configuraciones** • **Configuraciones designadas:** seleccione una o más configuraciones de la lista o búsquelas. Haga clic en la pestaña **Configuraciones seleccionadas** para ver la lista de las configuraciones seleccionadas. **Forzar las configuraciones designadas**: distribuya las configuraciones designadas como parte del cumplimiento personalizado. Esta lista contiene configuraciones que cumplen los siguientes criterios: • Configuración activada • Configuración sin sistema • Configuración apta para cuarentena • Las configuraciones creadas en el espacio actual o delegadas desde el espacio predeterminado Para obtener una lista de las configuraciones que no sean de cuarentena, consulte la sección Configuraciones que no son de cuarentena. **Eliminar contenido**: elimina todo el contenido y los medios asociados a aplicaciones distribuidas por Ivanti Neurons for MDM del dispositivo. **Suspender aplicaciones del área personal**: suspende las aplicaciones del área personal del dispositivo en cuarentena para indicar que el usuario del dispositivo tiene que atender los problemas de cumplimiento del dispositivo para que este vuelva a ser funcional. Compatible con los dispositivos Android 11+ provistos con el Perfil de trabajo en el Dispositivo propiedad de la empresa.

Encontrar una política existente

Puede utilizar los filtros y la función de búsqueda de la página de Políticas para encontrar una o más políticas existentes.

Procedimiento

1. Vaya a **Políticas**.
2. Para filtrar una lista de configuraciones que cumplan ciertos criterios, haga clic en **Filtros**.
3. Seleccione uno o más criterios de filtros.
4. Para buscar una política existente por su nombre, introduzca el nombre de la política en el campo **Buscar**.

Añadir una política

Procedimiento

1. Vaya a **Políticas**.
2. Haga clic en +**Añadir** (arriba a la derecha).
3. Seleccionar un tipo de política.
4. Complete los ajustes.
5. Seleccione los grupos de dispositivos en los que desea recibir esta política.

> Puede distribuir hasta un máximo de 100 archivos de configuración a la vez.

6. Haga clic en **Hecho**.

Editar una política

Procedimiento

1. Vaya a **Políticas**.
2. Para la política requerida, haga clic en el icono **Editar** (lápiz) en la columna Acciones.
3. Realice los cambios.
4. Guarde los cambios.

Eliminar una política

Procedimiento

1. Vaya a **Políticas**.
2. Para la política requerida, haga clic en el icono **Eliminar** en la columna Acciones.
3. Haga clic en **Sí** para confirmar.

Si no puede ver la página de las Políticas, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración de dispositivos
- Dispositivo de solo lectura

Para obtener más información, consulte **Priorizar políticas**.

Created at Sep 28, 2026

11.2. Política personalizada

Políticas

Licencia: Platinum

Dispositivos aptos: Android, iOS, macOS, Windows.

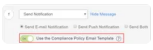
Le permite crear una política personalizada según el dispositivo y los atributos del usuario, los criterios de la sección, los valores y las medidas de cumplimiento que se especifiquen.

> Al definir una política personalizada, se puede usar incluso un ajuste de nivel de revisión de seguridad Android.

Añadir una política personalizada

1. Vaya a **Políticas**.
2. Haga clic en **+Añadir**.
3. Seleccione **Política personalizada**.
4. Proporcione un nombre para la política personalizada.
5. Haga clic en **+ Añadir descripción** para añadir detalles adicionales, si así lo desea.
6. Utilice el Creador de normas para definir las condiciones que generarán acciones cuando estas condiciones se cumplan. Consulte Entender_las_condiciones_de_configuración (Comprender los ajustes de las condiciones) para obtener pautas sobre cómo crear estas condiciones. El Administrador de Ivanti Neurons for MDM muestra el número de grupos de usuarios duplicados y el correspondiente número de GUID para identificar los grupos duplicados, cuando se selecciona el atributo Nombre del grupo de usuarios en el generador de reglas. Además, una tabla bajo esta regla muestra la lista de los grupos de usuarios duplicados y sus detalles, como el Nombre del Grupo de Usuarios, el GUID, la Fuente y el nombre distinguido (DN).
7. Seleccione una de las medidas de cumplimiento (consulte «Medidas predeterminadas» a continuación) a tomar cuando se cumplan las condiciones especificadas. Si se añade la medida «**Esperar**» en medio de otras medidas, se proporcionará a los usuarios de los dispositivos una forma de corregir su dispositivo y volverlo a poner en cumplimiento antes de que se tomen medidas adicionales. Por ejemplo, puede que prefiera enviar un mensaje de advertencia y esperar 24 horas antes de aplicar una medida de cuarentena.
8. Seleccione la opción **Enviar una notificación cuando el dispositivo vuelva a estar en estado de cumplimiento**, que está desactivada de forma predeterminada.

- **Enviar notificaciones de correo electrónico**: cuando el dispositivo vuelve a estar en estado de cumplimiento, se envía un correo electrónico a la dirección de correo electrónico del usuario del dispositivo.
    - Active la opción **Utilice la plantilla de correo electrónico de la política de cumplimiento** para insertar el mensaje que configure aquí en la plantilla de correo electrónico de notificación de la política que habrá configurado como se describe en Personalización de una plantilla de correo electrónico en Cómo personalizar las plantillas de correo electrónico. Consulte Configuración y uso de los correos electrónicos de notificación de cumplimiento de políticas para obtener información general.



    - Puede personalizar los mensajes incluyendo variables de sustitución opcional con el fin de ofrecer a los destinatarios más detalles acerca de las infracciones de políticas y otra información relevante. Haga clic en los siguientes tipos de atributos para mostrar la lista completa de variables:

    - Atributos de políticas como $, $ y $.
    - Atributos de usuario como $, $ y $.
    - Atributos de dispositivo como $, $ y $.
    - Personalice los atributos del Dispositivo/Usuario/LDAP que se crean a partir de la página **Administrador > Atributos**.
- **Enviar una notificación push:** se envía una notificación push al dispositivo cuando este vuelva a estar en estado de cumplimiento.
- **Enviar ambas:** se envía tanto una notificación push al dispositivo como un correo electrónico a la dirección de correo electrónico del usuario del dispositivo cuando el dispositivo vuelva a estar en estado de cumplimiento. Puede personalizar los mensajes incluyendo variables de sustitución opcional con el fin de ofrecer a los destinatarios más detalles según se ha descrito anteriormente en la acción Enviar correo electrónico.

9. Especifique las opciones siguientes de la tabla para notificar a los administradores y a los propietarios de dispositivos registrados si los propietarios de dispositivos infringen las reglas de la política:

Opción	Descripción
Asunto	Introduzca el texto del asunto. Por ejemplo: "¡Ha infringido una norma!".
Cuerpo	Introduzca el mensaje según sea necesario. Por ejemplo: "¡Acción requerida!".
Enviar notificación por correo electrónico solo a administradores	Seleccione esta opción para enviar una notificación por correo electrónico solo a los administradores.
CC a administradores	Este cuadro de texto no estará disponible si ha seleccionado "Enviar notificación de correo electrónico solo a administradores"?opción.
Introduzca las direcciones de correo electrónico de los administradores	Introduzca la dirección de correo electrónico de los administradores. Utilice un punto y coma (;) como separador para añadir varias direcciones de correo electrónico.
Vista previa del correo electrónico	Haga clic en el botón **Previsualizar correo electrónico** para ver la dirección de correo electrónico.

10. Haga clic en **Siguiente** para guardar los detalles de la política.

Medidas predeterminadas:

1. Haga clic en la casilla **Sí** para confirmar que entiende que, si esta política se ha desencadenado previamente en un dispositivo, añadir la política por niveles provocará el restablecimiento de la política y de las medidas de cumplimientos que se hubieran aplicado antes. La nueva política personalizada se aplicará en el próximo ingreso del dispositivo. Si seleccionó la acción Retirar, haga clic en **Sí** para confirmar que comprende que no puede deshacer la acción.

- **Supervisar**: siempre seleccionado actualmente. Es necesaria la versión 9.0.0 o posterior de Sentry para hacer uso de las medidas de cumplimiento por niveles.
- **No hacer nada**
- **Enviar notificación**
- **Enviar correo electrónico**: se envía un correo electrónico a la dirección de correo electrónico del usuario del dispositivo notificándole de que su dispositivo infringe el cumplimiento.
    - Puede utilizar la plantilla de correo electrónico de notificación de políticas como se ha descrito anteriormente.

    - Puede personalizar los mensajes incluyendo variables de sustitución opcional con el fin de ofrecer a los destinatarios más detalles acerca de las infracciones de políticas y otra información relevante. Esto proporciona a los usuarios de dispositivos no cumplidores información relevante acerca de la infracción de políticas para que puedan tomar medidas adecuadas para remediarlo. Haga clic en los siguientes tipos de atributos para mostrar la lista completa de variables:
        - Atributos de políticas como $, $ y $.
        - Atributos de usuario como $, $ y $.
        - Atributos de dispositivo como $, $ y $.
        - Personalice los atributos del Dispositivo/Usuario/LDAP que se crean a partir de la página **Administrador > Atributos**.
- **Enviar notificación push:** se envía una notificación push al dispositivo indicando que está infringiendo el cumplimiento.
- **Enviar ambas:** seleccione esta opción para enviar tanto una notificación push al dispositivo como un correo electrónico a la dirección de correo electrónico del usuario del dispositivo notificándole de que su dispositivo infringe el cumplimiento. Puede personalizar los mensajes incluyendo variables de sustitución opcional con el fin de ofrecer a los destinatarios más detalles según se ha descrito anteriormente en la acción Enviar correo electrónico.
- **Bloquear:** utiliza el Sentry para impedir que los dispositivos accedan a las aplicaciones de correo electrónico y las que son compatibles con AppConnect. Es necesaria la versión 9.0.0 o posterior de Sentry para hacer uso de la medida de bloqueo.
- **Retirar:** retira el dispositivo. **Esta acción no puede deshacerse**. Por ejemplo, puede haber una regla para retirar los dispositivos para todos los usuarios desactivados utilizando la condición Usuario activado.
- **Esperar:** retrasa la acción durante un período de tiempo específico (horas o días) con el fin de permitir que los usuarios corrijan la infracción antes de que se tomen medidas adicionales si el dispositivo sigue estando en estado de no cumplidor.
- **Cuarantena:** retira el acceso a las aplicaciones, contenido y servidores según las siguientes acciones:

Acciones de cuarentena adicionales (opcionales)	Descripción
Aplicaciones gestionadas en cuarentena	Elimina las aplicaciones administradas por Ivanti Neurons for MDM del dispositivo y permite la opción «Bloquear nuevas descargas de aplicaciones» para impedir que se puedan volver a instalar las aplicaciones en el dispositivo. Seleccione una de las siguientes opciones: • **Todas las aplicaciones** • **Aplicaciones designadas:** añada una o más aplicaciones por medio de búsqueda o de forma manual (utilizando la Id. de conjunto o el nombre del paquete). Haga clic en la pestaña **Ver aplicaciones** para ver la lista de aplicaciones añadidas. No se encuentra disponible la acción de cuarentena de la función predeterminada Bloquear acceso a la App Store. En algunos dispositivos, la acción de cuarentena no eliminará la aplicación del dispositivo debido a ciertas limitaciones del mismo.
Bloquear nuevas descargas de aplicaciones	Bloquea la descarga de cualquier aplicación nueva al dispositivo. Seleccione una de las siguientes opciones: • **Todas las aplicaciones** • **Aplicaciones designadas:** añada una o más aplicaciones por medio de búsqueda o de forma manual (utilizando la Id. de conjunto o el nombre del paquete). Haga clic en la pestaña **Ver aplicaciones** para ver la lista de aplicaciones añadidas. No se encuentra disponible la acción de cuarentena de la función predeterminada Bloquear acceso a la App Store. Por defecto, esta opción está seleccionada (tanto para Todas las Aplicaciones como para las Aplicaciones designadas) y no puede deseleccionarse. Esto impide que las aplicaciones se reinstalen en el dispositivo.
Eliminar configuraciones	Elimina las configuraciones de Ivanti Neurons for MDM del dispositivo. Seleccione una de las siguientes opciones: • **Todas las configuraciones** • **Configuraciones designadas:** seleccione una o más configuraciones de la lista o búsquelas. Haga clic en la pestaña **Configuraciones seleccionadas** para ver la lista de las configuraciones seleccionadas.
Insertar configuraciones designadas	Distribuya las configuraciones designadas como parte del cumplimiento personalizado. Esta lista contiene configuraciones que cumplen los siguientes criterios: • Configuración activada • Configuración sin sistema • Configuración apta para cuarentena • Las configuraciones creadas en el espacio actual o delegadas desde el espacio predeterminado Para obtener una lista de las configuraciones que no sean de cuarentena, consulte la sección **Configuraciones que no son de cuarentena.** Para más información, consulte la sección **Insertar una configuración designada** después de este procedimiento.

Acciones de cuarentena adicionales (opcionales)	Descripción
Eliminar contenido	Elimina todo el contenido y los medios asociados a aplicaciones distribuidas por Ivanti Neurons for MDM del dispositivo.
Suspender las aplicaciones personales	Suspende las aplicaciones del área personal del dispositivo en cuarentena para indicar que el usuario del dispositivo tiene que atender los problemas de cumplimiento del dispositivo para que este vuelva a ser funcional. Compatible con los dispositivos Android 11+ provistos con el Perfil de trabajo en el Dispositivo propiedad de la empresa.
Acciones de cuarentena predeterminadas: estas acciones siempre se llevan a cabo.	
Bloquear acceso a la App Store	Impide que el dispositivo acceda a las app stores a través de Ivanti Neurons for MDM.
Bloquear acceso a la Store de contenido	Impide que el dispositivo acceda a la content store a través de Ivanti Neurons for MDM.
Bloquear AppConnect	Impide que el dispositivo use funciones AppConnect.
Bloquear AppTunnel	Impide que las aplicaciones del dispositivo accedan a contenido y servidores a través de AppTunnel.
Bloquear ActiveSync	Impide que el dispositivo pueda acceder al correo electrónico a través del servidor ActiveSync.

2. Haga clic en **Siguiente** para configurar los dispositivos en los que se aplicarán la política y las acciones.
3. Haga clic en **Hecho**.

La siguiente tabla ilustra el comportamiento de cuarentena o varios dispositivos Android cuando el Ivanti Neurons for MDM es lo que inicia la medida de cuarentena:

Dispositivos	Comportamiento de cuarentena
Dispositivos Samsung en modo Administrador del dispositivo a través de la aplicación del cliente Go	• Desinstalar las aplicaciones administradas tanto públicas como internas • Eliminar ciertos perfiles (a excepción de Mobile Threat Defense y otros)
Dispositivos que no sean Samsung en modo Administrador del dispositivo a través de la aplicación de cliente Go MAM a través de la aplicación AppStation	• No admitir la desinstalación u ocultar las aplicaciones administradas tanto públicas como internas • Eliminar ciertos perfiles (a excepción de Mobile Threat Defense y otros)
Android Enterprise a través de la aplicación del cliente Go	• Ocultar las aplicaciones administradas tanto públicas como internas • Eliminar ciertos perfiles (a excepción de Mobile Threat Defense y otros)

Insertar una configuración designada

Distribuya las configuraciones designadas como parte del cumplimiento personalizado. Configure la Política personalizada para distribuir un conjunto de configuraciones cuando un dispositivo infrinja el cumplimiento. Restablezca el dispositivo a su estado anterior como parte de las medidas de reparación cuando el estado de un dispositivo cambie de «no cumplidor» a «cumplidor».

> Se producirá un error cuando un administrador intente delegar una política personalizada que tenga configuraciones no delegadas en la pestaña Insertar configuraciones designadas.

A continuación se enumera lo que ocurre cuando se insertan las configuraciones mediante políticas personalizadas bajo ciertas condiciones:

Condición(es)	Comportamiento
Se seleccionan dos configuraciones del mismo tipo que tienen un conjunto de prioridades	Se insertará en el dispositivo la configuración con la prioridad más alta.
Se seleccionan dos configuraciones del mismo tipo que no tengan un conjunto de prioridades	Ambas configuraciones se insertarán en el dispositivo. Esto puede dar lugar a comportamientos inesperados.
Cuando el dispositivo ya tiene una configuración del mismo tipo que admite la prioridad definida en la política personalizada	La configuración definida en la política personalizada tendrá prioridad y se insertará en el dispositivo. La que ya estaba en el dispositivo se eliminará independientemente de la prioridad (incluso aunque su prioridad sea superior a la definido en la política personalizada).
Cuando el dispositivo ya tiene una configuración del mismo tipo que no admite la prioridad definida en la política personalizada	Se enviará al dispositivo la configuración definida en la política personalizada. Ambas configuraciones estarán presentes en el dispositivo. Esto puede dar lugar a comportamientos inesperados.
Si se cambia la prioridad de una configuración después de crear la política personalizada	Cuando se ingrese en el dispositivo, se insertará la configuración con la mayor prioridad si forma parte de la política personalizada.
Cuando se cumplen ambas condiciones: • Condición A: Cuando a un dispositivo con una infracción se le ha insertado una configuración como parte de una política personalizada (y ha tenido prioridad sobre una configuración del mismo tipo ya existente en el dispositivo). • Condición B: La infracción se ha corregido y el dispositivo ya no está en cuarentena.	Se eliminará la configuración definida en la política personalizada y se insertará en el dispositivo otra del mismo tipo antes de la cuarentena a través de la aplicación de los grupos de dispositivos existentes, lo cual revertirá el dispositivo a su estado original.

En la acción Cuarentena, si selecciona Eliminar configuraciones junto con Insertar configuraciones designadas, tenga en cuenta las siguientes reglas:

- Eliminar todas las configuraciones + Insertar configuraciones designadas: en este caso, todas las configuraciones del dispositivo se eliminarán y las configuraciones seleccionadas en «Insertar configuraciones designadas» se insertarán en el dispositivo.
- Elimine las configuraciones designadas (en una política personalizada) + Envíe las configuraciones designadas (en otra política personalizada) con configuraciones comunes en la selección de ambas: puesto que las configuraciones se seleccionan en dos políticas de cumplimiento distintas, se debería tomar el enfoque más restrictivo, es decir, la configuración se eliminará del dispositivo.

Se puede delegar una política personalizada desde el **espacio** predeterminado a un espacio personalizado. Para delegar una política personalizada, las configuraciones mencionadas en la política personalizada en la pestaña «Insertar configuraciones designadas» deben delegarse a los espacios.

En la página **Dispositivos**, puede hacer clic en el nombre de un dispositivo para visitar la página de detalles del dispositivo. En la pestaña Configuraciones, la columna Método de distribución indica el método de distribución de una configuración insertada en el dispositivo. Puede ser «Grupo de dispositivos» o «Medida de cumplimiento».

En la página Configuraciones, para cada configuración, Ivanti Neurons for MDM muestra un recuento de los dispositivos que recibieron la configuración mediante el grupo de dispositivos y la medida de cumplimiento.

Comprender los ajustes de las condiciones

La siguiente tabla describe algunos campos disponibles para crear reglas:

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
Compatible con APNS	Este campo indica si el dispositivo es compatible con APNS.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS/macOS/Android
Estado nativo de antiphishing	Este campo muestra el estado nativo de antiphishing	Los operadores posibles son: • es igual a • no es igual a Posibles valores son: • No activado • N/A • Activado • Desconocido	iOS/Android
Estado de antiphishing	Este campo muestra el estado de antiphishing	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son: • No activado • N/A • Activado • Desconocido	iOS/Android
Estado de la VPN de antiphishing	Este campo muestra el estado de la VPN de antiphishing	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son: • No activado • N/A • Activado • Desconocido	iOS/Android
Información de batería	Este campo tiene los atributos siguientes: • Nivel de batería: muestra el nivel de carga actual de la batería, tal y como ha informado el SO de Android	Para obtener información sobre los valores posibles, consulte **Uso de la búsqueda avanzada**.	Android

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
	• Estado de integridad de la batería: como ha informado SO de Android • Estado de carga de la batería: como ha informado SO de Android • Porcentaje de integridad de la batería (específico de OEM): la integridad de la batería en porcentaje para los fabricantes de los dispositivos compatibles, como Zebra • Fecha de fabricación de la batería (OEM): la fecha de fabricación de la batería de los fabricantes de dispositivos compatibles, como Zebra • Ciclos de carga de la batería (OEM): número de ciclos completados en total para los fabricantes de dispositivos compatibles, como Zebra		
Estado operativo de la banda base	Este campo indica el estado de la banda base del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Aceptar o Error.	Dispositivos supervisados iOS 27.0 o posterior
Token de Bootstrap disponible	Este campo indica si se dispone de un token de arranque para un dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	macOS
Autopilot inscrito	Este campo indica si el dispositivo está registrado en Autopilot o no.	• es igual a • no es igual a Los valores posibles son Sí y No.	Windows
Último ingreso	Este campo indica la última hora de registro del cliente en bridge.	Los operadores posibles son: • es menor que	Windows

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
de Bridge		• es menor o igual a • es mayor que • es mayor o igual a • se encuentra en el intervalo • se encuentra en el rango Introduzca el valor numérico de la hora del último inicio en bridge. Seleccione una de las siguientes opciones para la duración: • horas • días Ejemplo: el último ingreso de Bridge fue hace menos de 12 horas.	
Estado operativo de la cámara	Este campo indica el estado de la cámara del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son: • Aceptar • Error • No original (si no es un componente original de Apple)	Dispositivos supervisados iOS 27.0 o posterior
Último ingreso del cliente	Este campo indica la hora del último ingreso del cliente.	Los operadores posibles son: • es menor que • es mayor que Introduzca el valor numérico de la hora del último ingreso. Seleccione una de las siguientes opciones para la duración: • horas • días Ejemplo: el último ingreso del cliente fue hace menos de 12 horas.	iOS/macOS/Android
Registrado con el cliente	Este campo indica el estado del cliente registrado.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS/macOS/Android

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
Confidencial	Este campo indica si el dispositivo está descifrado o en peligro.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son: • sometido a un «jailbreak» o descifrado • no afectado	iOS/Android
Nombre del país actual	Este campo indica el nombre del país actual que se corresponden con el Código de país móvil (MCC, en inglés) o el Código de red móvil (MNC, en inglés) al que el dispositivo notifica que está conectado actualmente.	Los operadores posibles son: • es igual a • no es igual a El posible valor es un valor de la lista desplegable que indica el nombre del país de origen.	iOS/macOS/Android
MMC actual	Este campo indica el código móvil del país actual.	Introduzca el valor del atributo que hay que verificar. Los operadores posibles son: • es igual a • no es igual a	iOS/macOS/Android
MNC actual	Este campo indica el código móvil de la red actual.	Introduzca el valor del atributo que hay que verificar. Los operadores posibles son: • es igual a • no es igual a	iOS/macOS/Android
Atributo personalizado del dispositivo	Este campo permite añadir un atributo personalizado existente de un dispositivo como condición de una norma para verificar su valor.	Introduzca el valor del atributo que hay que verificar. Los operadores posibles son: • es igual a • no es igual a • contiene • no contiene El valor puede ser una cadena de caracteres ASCII, incluidos espacios y caracteres Unicode.	iOS/macOS/Android/Windows
Atributo personalizado de LDAP	Este campo permite añadir un atributo personalizado LDAP existente como condición de una norma para verificar su valor.	Introduzca el valor del atributo que hay que verificar. Los operadores posibles son: • es igual a • no es igual a • contiene • no contiene El valor puede ser una cadena de caracteres ASCII,	iOS/macOS/Android/Windows

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
		incluidos espacios y caracteres Unicode.	
Atributo personalizado del usuario	Este campo permite añadir un atributo personalizado de un usuario existente como condición de una norma para verificar su valor.	Introduzca el valor del atributo que hay que verificar. Los operadores posibles son: • es igual a • no es igual a • contiene • no contiene El valor puede ser una cadena de caracteres ASCII, incluidos espacios y caracteres Unicode.	iOS/macOS/Android/Windows
Itinerancia de datos	Este campo permite usar la itinerancia de datos como condición de una norma para verificar su valor.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No. El valor predeterminado es «no» si el dispositivo compatible no notifica ninguna información acerca de este campo.	iOS/Android
Tipo de dispositivo	Este campo indica el modelo de dispositivo.	Los operadores posibles son: • es igual a • no es igual a • comienza con • termina con El valor posible es un valor de texto.	iOS/macOS/Android/Windows
Tipo de dispositivo (Apple)	Este campo indica el nombre bonito del modelo de dispositivo.	Los operadores posibles son: • es igual a • no es igual a • comienza con • termina con El valor posible es un valor de texto.	iOS/macOS
Estado operativo de la pantalla	Este campo indica el estado de la pantalla del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son: • Aceptar • Error	Dispositivos supervisados iOS 27.0 o posterior

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
		• No original (si no es un componente original de Apple)	
Cifrado habilitado	Este campo determina si el dispositivo tiene activados el cifrado/protección de datos.	Sí - El dispositivo tiene activados el cifrado/protección de datos. No - El dispositivo no tiene activados el cifrado/protección de datos.	iOS/Android/Windows
GUID	Este campo indica el GUID del dispositivo.	Los operadores posibles son: • es igual a • no es igual a • comienza con • termina con	iOS/macOS/Android/Windows
Estado operativo de Face ID	Este campo indica el estado de Face ID del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Aceptar o Error.	Dispositivos supervisados iOS 27.0 o posterior
Nombre del país de origen	Este campo indica el nombre del país de origen que se corresponden con el Código de país móvil (MCC, en inglés) o el Código de red móvil (MNC, en inglés) que se programa en la tarjeta SIM o eSIM del dispositivo.	Los operadores posibles son: • es igual a • no es igual a El posible valor es un valor de la lista desplegable que indica el nombre del país de origen.	iOS/Android/Windows
Hubo un error en la actualización de Windows	Este campo determina si el dispositivo está infringiendo el cumplimiento con las últimas reglas de la actualización.	Sí: el dispositivo no está cumpliendo la última actualización. No: el dispositivo está cumpliendo la última actualización.	Windows
MCC de origen	Este campo indica el código móvil delpaís de origen.	Introduzca el valor del atributo que hay que verificar. Los operadores posibles son: • es igual a • no es igual a	iOS/macOS/Android
MNC de origen	Este campo indica el código de red delpaís de origen.	Introduzca el valor del atributo que hay que verificar. Los operadores posibles son: • es igual a • no es igual a	iOS/macOS/Android

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
IMEI	Este campo indica el número IMEI de la primera ranura SIM.	Los operadores posibles son: • es igual a • no es igual a • comienza con • termina con	iOS/Android/Windows
IMEI2	Este campo indica el número IMEI de la segunda ranura SIM.	Los operadores posibles son: • es igual a • no es igual a • comienza con • termina con	Android
IMSI	Este campo indica el número IMSI de la tarjeta SIM.	Los operadores posibles son: • es igual a • no es igual a • comienza con • termina con	Android/Windows
Clave de recuperación institucional habilitada	Este campo indica si la clave de recuperación institucional está habilitada o no en el dispositivo.	Los operadores posibles son: • es igual a • no es igual a	macOS
Último ingreso	Este campo le permite establecer las condiciones relacionadas con la hora del último ingreso del dispositivo administrado a través del canal de MDM.	Los operadores posibles son: • es menor que • es mayor que • está en blanco Introduzca el valor numérico de la hora del último ingreso. Seleccione una de las siguientes opciones para la duración: • horas • días Ejemplo: el último ingreso fue hace más de 12 horas.	iOS/macOS/Android/Windows

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
Última ID de Hotfix	Este campo le permite establecer condiciones relacionadas con la última Id. de Hotfix.	Los operadores posibles son: • es igual a • no es igual a • es menor que • es menor o igual a • es mayor que • es mayor o igual a • contiene • no contiene • comienza con • no comienza con • termina con • no termina con	Windows
Hotfix instalado por última vez el	Este campo le permite establecer condiciones relacionadas con la última instalación de Hotfix.	Los operadores posibles son: • es menor que • es mayor que	Windows
Servicios de localización habilitados	Este campo indica si el dispositivo tiene activado algún servicio de localización (como Encontrar mi iPhone).	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS
Fabricante	Este campo le permite establecer condiciones relacionadas con el fabricante del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son: • Samsung • NOKIA • HTC • LGE • Apple Inc	iOS/macOS/Android/Windows

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
Estado de activación del MTD	Este campo representa el estado de activación del MTD	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son: • N/A • Error • Pendiente • Protegido	iOS/Android
Administrado por MDM	Este campo determina si el dispositivo tiene activados MDM/administrador del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS/macOS/Android
Tipo de inscripción mediante MDM	Este campo indica el tipo de inscripción del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son: • Usuario • Dispositivo • Supervisado • Ninguno	iOS 27.0+, macO27.0+, tvOS 27.0+, visionOS 27.0+ y watchOS 27.0+
Retorno al servicio mediante MDM	Este campo indica el estado del dispositivo para el retorno al servicio mediante MDM con conservación de aplicaciones.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son True o False.	iOS 27.0+ y visionOS 27.0+
Modo multiusuario	Este campo indica si el dispositivo (iPad) utiliza el modo multiusuario.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS 27,0+
Estado de la comunicación de campo cercano	Este campo indica el estado de la comunicación NFC del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Aceptar o Error.	Dispositivos supervisados iOS 27.0 o posterior

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
SO	Este campo indica el tipo de SO del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son: • macOS • Android • iOS • Windows • visionOS	iOS/macOS/visionOS/Android/Windows
Versión de compilación del SO	Este campo indica la versión de compilación del SO del dispositivo.	Los operadores posibles son: • es igual a • no es igual a • es menor que • es menor o igual a • es mayor que • es mayor o igual a • contiene • no contiene • comienza con • no comienza con • no está en blanco • está en blanco • termina con • no termina con	iOS/macOS/visionOS/Android/Windows
Versión de SO	Este campo indica la versión de SO del dispositivo.	Los operadores posibles son: • es igual a • no es igual a • es menor que • es menor o igual a • es mayor que • es mayor o igual a • se encuentra en el intervalo	iOS/macOS/visionOS/Android/Windows

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
		• se encuentra en el rango El valor posible es texto.	
SO con versión	Este campo indica el SO y la versión de SO del dispositivo	Los operadores posibles son: • es igual a • no es igual a • es menor que • es menor o igual a • es mayor que • es mayor o igual a • se encuentra en el intervalo • se encuentra en el rango El valor posible es texto.	iOS/macOS/visionOS/Android/Windows
Propiedad	Este campo indica el tipo de propiedad del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son: • propiedad del usuario • no establecido • propiedad de la empresa	iOS/macOS/Android/Windows
Clave de recuperación personal habilitada	Este campo indica si la clave de recuperación personal está habilitada o no.	Los operadores posibles son: • es igual a • no es igual a	macOS
Código de acceso en conformidad con los perfiles	Este campo indica si el dispositivo cumple los requisitos del código de acceso con los perfiles.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS/macOS/Android
Punto de acceso personal	Este campo indica si la característica de Punto de acceso personal está	Los operadores posibles son: • es igual a	iOS

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
habilitado	habilitada en el dispositivo.	• no es igual a Los valores posibles son Sí y No. El ajuste de Punto de acceso personal solo está disponible en ciertos operadores.	
N.º de teléfono	Este campo indica el número de teléfono del dispositivo.	Los operadores posibles son: • es igual a • no es igual a • contiene • comienza con • termina con	iOS/Android/Windows
Dirección IP pública	Este campo indica la dirección IP pública. Si el dispositivo utiliza una conexión VPN o un servidor proxy para conectarse a Ivanti Neurons for MDM, muestra la dirección IP de la proxy WAN.	Los operadores posibles son: • se encuentra en el intervalo • se encuentra en el rango • no está en blanco • está en blanco	Android/ChromeOS
Itinerancia	Este campo indica el estado de la itinerancia del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS/Android/Windows
Modo de bloqueo de seguridad	Este campo indica si el modo de bloqueo está habilitado o deshabilitado para un dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son True o False.	iOS 27.0+ y macOS 27.0+
Sentry bloqueado	Indica si el dispositivo está bloqueado con Sentry.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS/macOS/Android/Windows
Estado	Este campo indica el estado del registro.	Los operadores posibles son: • es igual a • no es igual a El valor posible predeterminado es «Activo». En las políticas personalizadas, restringe el estado del dispositivo a Activo eliminando todos los demás	iOS/macOS/Android

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
		valores potenciales porque la evaluación de políticas se produce cuando el dispositivo se registra en los estados Activo, Pendiente de retirada y Pendiente de borrado, y estos dispositivos tendrán sus políticas evaluadas al registrarse.	
Número de serie	Este campo indica el número de serie del dispositivo.	Los operadores posibles son: • es igual a • no es igual a • comienza con • termina con	iOS/macOS/Android/Windows
Supervisado	Este campo indica si el dispositivo está supervisado.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS/macOS
Versión de generación suplementaria	Este campo representa la versión de compilación del SO del dispositivo.	Los operadores posibles son: • es igual a • no es igual a • es menor que • es menor o igual a • es mayor que • es mayor o igual a • contiene • no contiene • comienza con • no comienza con • termina con • no termina con • no está en blanco • está en blanco	iOS/macOS
Suplemento SO/Versión Extra	Este campo representa la versión de compilación del SO del dispositivo.	Los operadores posibles son: • es igual a • no es igual a • es menor que • es menor o igual a	iOS/macOS

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
		• es mayor que • es mayor o igual a • contiene • no contiene • comienza con • no comienza con • termina con • no termina con • no está en blanco • está en blanco	
Estado operativo de Touch ID	Este campo indica el estado de Touch ID del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son: • Aceptar • Error • N/A (si es un iPhone)	Dispositivos supervisados iOS 27.0 o posterior
Usuario activado	Este campo indica si el usuario está activado.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS/macOS/Android/Windows
Grupo de usuarios	Este campo indica el grupo de usuarios.	Los operadores posibles son: • es igual a • no es igual a	iOS/macOS/Android/Windows
Estado operativo de la banda ultraancha	Este campo indica el estado de la banda ultraancha del dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Aceptar o Error.	Dispositivos supervisados iOS 27.0 o posterior
Itinerancia de voz	Este campo indica si la itinerancia de voz está habilitada en el dispositivo.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS

Campo de la IU	Descripción	Posibles valores	Plataformas compatibles
		El ajuste de itinerancia de voz solo está disponible en ciertos operadores. Al desactivar la itinerancia de voz también se desactiva la itinerancia de datos. El valor predeterminado es «no es igual a» si el dispositivo compatible no notifica ninguna información acerca de este campo.	
Acceso bloqueado	Indica si el dispositivo está bloqueado con Access.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS/macOS/Android/Windows
Cumplimiento	Indica si el dispositivo es compatible o no.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Cumple o No cumple.	iOS/macOS/Android/Windows
Medida de cumplimiento bloqueada	Indica si el dispositivo está bloqueado o no.	Los operadores posibles son: • es igual a • no es igual a Los valores posibles son Sí y No.	iOS/macOS/Android/Windows

Configuraciones no aptas para cuarentena

La siguiente tabla muestra la lista de configuraciones que no son aptas para cuarentena:

SO	Configuraciones no aptas para cuarentena
Android	• Catálogo de aplicaciones Android • Cifrado en Android • Android Enterprise • Aplicación Android Enterprise • Android Zebra • Protección antiphising • Desafío de acceso (Work Challenge) de Android • Código de acceso del dispositivo • Descarga del archivo • Bloqueo y kiosco: modo de administrador de dispositivos de Android • Bloqueo y kiosco: Samsung KNOX Standard • Solo MAM • Dispositivo administrado con perfil de trabajo/perfil de trabajo en el dispositivo propiedad de la empresa • Dispositivos administrados en el trabajo (Propietario del dispositivo) • Restricciones de teléfonos Samsung • Certificación SafetyNet • Perfil de trabajo en el Dispositivo propiedad de la empresa
iOS y macOS	• Protección antiphising (iOS) • Notificaciones de la aplicación (iOS) • Sitios de AppStation (iOS) • Clave de recuperación de FileVault (macOS) • Filevault 2 (macOS) • Proxy global (iOS y tvOS) • Diseño de la pantalla de inicio (iOS y tvOS) • Control de aplicaciones iOS • Restricciones de iOS • Actualizaciones del software iOS (iOS) • Firewall de macOS • Actualizaciones del software de macOS • «MAM Only» (iOS) • Privacidad del cliente de MI (iOS/macOS) • Uso de la red (iOS) • Creación de cuentas en Office 365 (macOS) • Modo de aplicación individual (iOS y tvOS) • Control de políticas del sistema (macOS)

SO	Configuraciones no aptas para cuarentena
	• Políticas del sistema administradas (macOS) • Opciones de reglas de políticas del sistema (macOS) • Servidor de zona horaria (macOS) • Filtro de contenido web (iOS)
Windows	• Control de aplicaciones Windows • DDF (Data Definition File) de restricciones de Windows • Firewall de Windows • Proxy de red de Windows • Restricciones de Windows • Actualización de Windows
Todos	• Active Directory • Servicios del cliente • Gestión de dispositivos móviles • Activación de Mobile Threat Defense • Medidas locales de Mobile Threat Defense • Código de acceso • Privacidad • Declaración de privacidad • ServiceConnect • Sincronización

Si no puede ver la página de la Política, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración de dispositivos
- Dispositivo de solo lectura

11.3. Supervisar y controlar las aplicaciones permitidas

Licencia: Silver

Para controlar qué aplicaciones están instaladas en los dispositivos, se crea una política de Aplicaciones permitidas. Esta política también es compatible con las aplicaciones internas macOS con marca registrada de MobileIron Packager (MIP). La política contiene la siguiente información:

- {{Aplicaciones de la lista de permitidos}}
- {{Aplicaciones de la lista de bloqueados}}
- {{aplicaciones obligatorias}}
- {{medidas de cumplimiento}}

Si una aplicación es obligatoria y además está en la lista de permitidos, prevalece la evaluación de la aplicación frente a la lista obligatoria. Por ejemplo, si una aplicación A1 está presente tanto en la lista de aplicaciones obligatorias como en la lista de bloqueados, entonces la evaluación de la política de aplicaciones para este dispositivo funcionará del siguiente modo:

- El dispositivo se considerará cumplidor si A1 está instalado en el dispositivo.
- El dispositivo se considerará no cumplidor si A1 no está instalado en el dispositivo.

Dispositivos compatibles

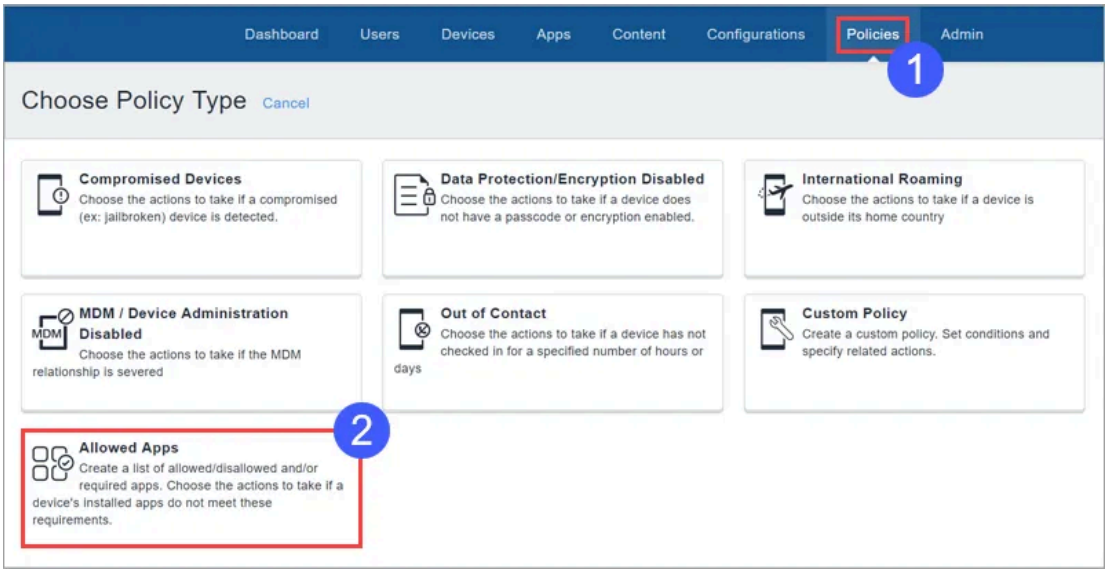
- Android 4.2 o versiones más recientes compatibles
- iOS 8.0 o versiones más recientes compatibles
- macOS 10.12 o versiones más recientes compatibles
- Windows 10 o versiones más recientes compatibles.

Requisitos previos

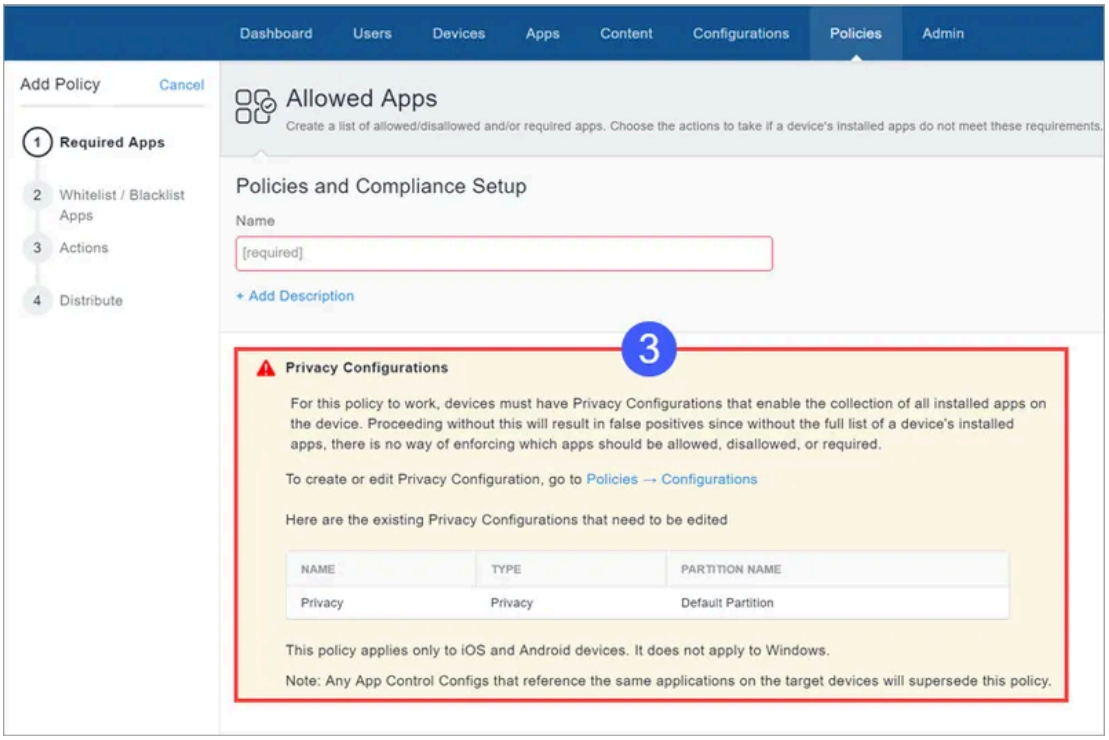
- La **configuración de privacidad** asignada a un dispositivo debe permitir la obtención de información de aplicaciones para que la política de aplicaciones permitidas funcione correctamente. Compruebe las configuraciones de privacidad asignadas a los dispositivos en los que aplicará la política de Aplicaciones permitidas.

Si no está seguro de las configuraciones que se ven afectadas:

1. Vaya a **Políticas**.



Haga clic en **Aplicaciones permitidas**.



3. En **Configuraciones de privacidad**, fíjese en las configuraciones que hay que editar.
4. Vaya a **Configuraciones**.
5. Para cada configuración de privacidad que haya anotado:
    1. Seleccione la configuración.
    2. Haga clic en **Editar**.
    3. En **Recopilar inventario de aplicaciones,** seleccione **Para todas las aplicaciones del dispositivo**.
    4. Haga clic en **Hecho**.

Crear una Política de aplicaciones permitidas

Requisitos previos

- Habilitar Android Enterprise para acceder a Google Play Store y añadir nuevas aplicaciones a la política de aplicaciones permitidas.

Procedimiento

1. Vaya a **Políticas** y haga clic en **+Añadir**.

2. Haga clic en **Aplicaciones permitidas**.

3. En el campo **Nombre**, introduzca un nombre para esta política.
4. En el campo **Descripción**, escriba texto opcional que explique la finalidad de la política.
5. Elija las aplicaciones que desea poner en la lista de permitidos o la lista de bloqueados haciendo clic en una o en las dos pestañas siguientes:

- Haga clic en Añadir por búsqueda para buscar y elegir aplicaciones desde la App Store o App Catalog.
  Asegúrese de habilitar Android Enterprise para acceder a la Google Play Store.

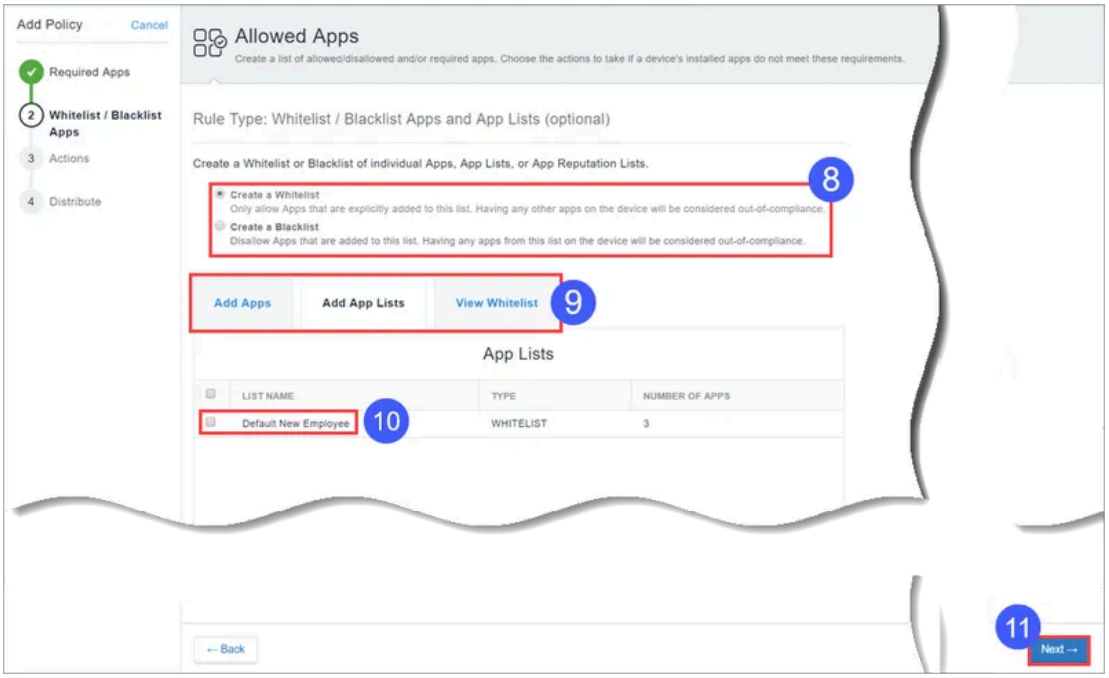
- Haga clic en **Añadir manualmente** para elegir aplicaciones introduciendo el ID del paquete para aplicaciones de sistema Android, Windows, iOS o macOS.

Seleccione la pestaña **Añadir listas de aplicaciones** y, a continuación, seleccione las listas de aplicaciones necesarias deseadas.

6. Utilice los campos resultantes para seleccionar las aplicaciones obligatorias o las listas de aplicaciones.
7. Haga clic en **Siguiente**.

> Haga clic en la pestaña **Ver lista requerida** para obtener una lista de las aplicaciones que ha seleccionado hasta ahora.

8. Seleccione si desea crear una lista de permitidos o una lista de bloqueados.



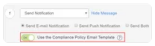
9. Utilice la sección **Aplicaciones de la lista de permitidos/lista de bloqueados y listas de aplicaciones** para seleccionar las aplicaciones y las listas de aplicaciones.

> No se puede tener una lista de permitidos como una lista de bloqueados simultáneamente para un dispositivo. Al crear una lista de permitidos, se determina que todas las demás aplicaciones estén en la lista de bloqueados.

10. Utilice los campos resultantes para seleccionar las aplicaciones obligatorias o las listas de aplicaciones.
    - Seleccione la pestaña **Añadir listas de aplicaciones** y, a continuación, seleccione las listas de aplicaciones deseadas.
11. Haga clic en **Siguiente**.

> Haga clic en la pestaña **Ver lista de permitidos o lista de bloqueados** para ver la lista de aplicaciones que ha seleccionado hasta el momento.

12. Seleccione las medidas a tomar cuando un dispositivo infrinja el cumplimiento:

Acción	Qué hacer
Supervisar	Siempre seleccionado actualmente. Es necesaria la versión 9.0.0 o posterior de Sentry para hacer uso de las medidas de cumplimiento por niveles.
No hacer nada	Seleccione esta opción para no tomar ninguna medida si el dispositivo ha infringido el cumplimiento.
Enviar notificación	
Enviar correo electrónico	Seleccione esta opción para enviar un correo electrónico a la dirección de correo electrónico del usuario del dispositivo notificándole de que su dispositivo infringe el cumplimiento. • Active la opción **Utilice la plantilla de correo electrónico de la política de cumplimiento** para insertar el mensaje que configure aquí en la plantilla de correo electrónico de notificación de la política que habrá configurado como se describe en **Personalización de una plantilla de correo electrónico** en **Cómo personalizar las plantillas de correo electrónico**. Consulte **Configuración y uso de los correos electrónicos de notificación de cumplimiento de políticas** para obtener información general.  • Puede personalizar los mensajes incluyendo variables de sustitución opcional con el fin de ofrecer a los destinatarios más detalles acerca de las infracciones de políticas y otra información relevante. Esto proporciona a los usuarios de dispositivos no cumplidores información relevante acerca de la infracción de políticas para que puedan tomar medidas adecuadas para remediarlo. Haga clic en los siguientes tipos de atributos para mostrar la lista completa de variables: ◦ Atributos de políticas como $, $, y $. ◦ Atributos de usuario como $, $ y $. ◦ Atributos de dispositivo como $, $ y $.
Enviar una notificación push	Seleccione esta opción para enviar una notificación push al dispositivo indicando que está infringiendo el cumplimiento.
Enviar ambas	Seleccione esta opción para enviar tanto una notificación push al dispositivo como un correo electrónico a la dirección de correo electrónico del usuario del dispositivo notificándole de que su dispositivo infringe el cumplimiento. Puede personalizar los mensajes incluyendo variables de sustitución opcional con el fin de ofrecer a los destinatarios más detalles según se ha descrito anteriormente en la acción Enviar correo electrónico.
Esperar	Seleccione esta opción para retrasar la acción durante un período de tiempo específico con el fin de permitir que los usuarios corrijan la infracción antes de que se tomen medidas adicionales si el dispositivo sigue estando en estado de no cumplidor.
Bloquear	Utiliza el Sentry para impedir que los dispositivos accedan a las aplicaciones de correo electrónico y las que son compatibles con AppConnect.
Cuarentena	Seleccione esta opción para retirar el acceso a las aplicaciones, contenido y servidores según las acciones de la tabla siguiente. No está permitida la acción Eliminar todas las aplicaciones.
Enviar una notificación cuando el	

Acción	Qué hacer
dispositivo vuelva a estar en estado de cumplimiento	
Enviar correo electrónico	Se envía un correo electrónico a la dirección de correo electrónico del usuario del dispositivo cuando el dispositivo vuelva a estar en estado de cumplimiento. • Puede utilizar la plantilla de correo electrónico de notificación de políticas como se ha descrito anteriormente. • Puede personalizar los mensajes incluyendo variables de sustitución opcional con el fin de ofrecer a los destinatarios más detalles acerca de las infracciones de políticas y otra información relevante. Haga clic en los siguientes tipos de atributos para mostrar la lista completa de variables: ◦ Atributos de políticas como $, $ y $. ◦ Atributos de usuario como $, $ y $. ◦ Atributos de dispositivo como $, $ y $. ◦ Personalice los atributos del Dispositivo/Usuario/LDAP que se crean a partir de la página **Administrador > Atributos**.
Enviar una notificación push	Se envía una notificación push cuando el dispositivo vuelva a estar en estado de cumplimiento.
Enviar ambas	Se envía tanto una notificación push al dispositivo como un correo electrónico a la dirección de correo electrónico del usuario del dispositivo cuando el dispositivo vuelva a estar en estado de cumplimiento. Puede personalizar los mensajes incluyendo variables de sustitución opcional con el fin de ofrecer a los destinatarios más detalles según se ha descrito anteriormente en la acción Enviar correo electrónico.

La política de Aplicaciones permitidas admite **las acciones de cumplimiento por niveles** si tiene una licencia Platinum.

Acciones de cuarentena adicionales (opcionales)	Descripción
Aplicaciones gestionadas en cuarentena	Elimina las aplicaciones administradas por Ivanti Neurons for MDM del dispositivo y permite la opción «Bloquear nuevas descargas de aplicaciones» para impedir que se puedan volver a instalar las aplicaciones en el dispositivo. Seleccione una de las siguientes opciones: • **Todas las aplicaciones** • **Aplicaciones designadas:** añada una o más aplicaciones por medio de búsqueda o de forma manual (utilizando la Id. de conjunto o el nombre del paquete). Haga clic en la pestaña **Ver aplicaciones** para ver la lista de aplicaciones añadidas. No se encuentra disponible la acción de cuarentena de la función predeterminada Bloquear acceso a la App Store. En algunos dispositivos, la acción de cuarentena no eliminará la aplicación del dispositivo debido a ciertas limitaciones del mismo.
Bloquear nuevas descargas de aplicaciones	Bloquea la descarga de cualquier aplicación nueva al dispositivo. Seleccione una de las siguientes opciones: • **Todas las aplicaciones** • **Aplicaciones designadas:** añada una o más aplicaciones por medio de búsqueda o de forma manual (utilizando la Id. de conjunto o el nombre del paquete). Haga clic en la pestaña **Ver aplicaciones** para ver la lista de aplicaciones añadidas. No se encuentra disponible la acción de cuarentena de la función predeterminada Bloquear acceso a la App Store.
Eliminar configuraciones	Elimina las configuraciones de Ivanti Neurons for MDM del dispositivo. Seleccione una de las siguientes opciones: • **Todas las configuraciones** • **Configuraciones designadas:** seleccione una o más configuraciones de la lista o búsquelas. Haga clic en la pestaña **Configuraciones seleccionadas** para ver la lista de las configuraciones seleccionadas.
Eliminar contenido	Elimina todo el contenido y los medios asociados a aplicaciones distribuidas por Ivanti Neurons for MDM del dispositivo.
Suspender las aplicaciones personales	Suspende las aplicaciones del área personal del dispositivo en cuarentena para indicar que el usuario del dispositivo tiene que atender los problemas de cumplimiento del dispositivo para que este vuelva a ser funcional. Compatible con los dispositivos Android 11+ provistos con el Perfil de trabajo en el Dispositivo propiedad de la empresa.
Acciones de cuarentena predeterminadas: estas acciones siempre se llevan a cabo.	
Bloquear acceso a la App Store	Impide que el dispositivo acceda a las app stores a través de Ivanti Neurons for MDM.

Acciones de cuarentena adicionales (opcionales)	Descripción
Bloquear acceso a la Store de contenido	Impide que el dispositivo acceda a la content store a través de Ivanti Neurons for MDM.
Bloquear AppConnect	Impide que el dispositivo use funciones AppConnect.
Bloquear AppTunnel	Impide que las aplicaciones del dispositivo accedan a contenido y servidores a través de AppTunnel.
Bloquear ActiveSync	Impide que el dispositivo pueda acceder al correo electrónico a través del servidor ActiveSync.

Haga clic en **Siguiente**.

14. Configure la distribución.
15. Haga clic en **Hecho**.

Para obtener más información sobre cómo establecer prioridades más altas o más bajas para una política de Aplicaciones permitidas, consulte **Priorizar políticas**.

11.4. Priorizar políticas

La política de Aplicaciones permitidas admite una prioridad, similar a la de las Configuraciones. Se utiliza una prioridad para determinar qué política del mismo tipo se distribuye a varios grupos de dispositivos, y el caso en que el mismo dispositivo aparece en esos grupos de múltiples de dispositivos. Por ejemplo, una prioridad de política es útil para determinar la distribución de políticas en caso de que:

- La «Aplicación obligatoria A» se debe distribuir al Grupo de dispositivos 1,
- La «Aplicación obligatoria B» se debe distribuir al Grupo de dispositivos 2, y
- El dispositivo del usuario es miembro de ambos grupos de dispositivos.

Puede priorizar las políticas del siguiente modo:

1. Vaya a **Políticas > Políticas y cumplimiento**.
2. Seleccione **Acciones > Priorizar políticas**. Si no aparece **Acciones**, quiere decir que no tiene múltiples políticas que requieran prioridades.
3. Utilice las flechas para enumerar las prioridades desde la más alta (arriba) hasta la más baja (abajo). El icono del candado significa que la prioridad de la política no se puede modificar sin editar el ajuste de distribución Todos los dispositivos dentro de la política.
4. Haga clic en **Guardar**.

11.5. Política de hardware de Windows

Couldn't convert your doc.

12. Administración

La sección de administrador le ayuda a gestionar usuarios, dispositivos y configuraciones desde el Ivanti Neurons for MDM portal. Las siguientes secciones contienen la lista de todas las tareas que puede realizar como administrador:

- Sistema
- Infraestructura
- Ajustes (Apple)
- Trabajar con dispositivos Windows
- Configuración con Microsoft Azure
- Conectar con Google Apps
- Trabajar con dispositivos de ChromeOS
- Administración del firmware
- Suspensión del abonado
- Gestionar secuencias de comandos y archivos
- Personalización de marca
- Añadir la administración de dispositivos que no sean iOS

12.1. Sistema

Esta sección contiene los siguientes temas:

- Atributos
- Ajustes de borrado del dispositivo
- Perfiles GDPR
- Correos electrónicos de notificación
- Administración de funciones
- Espacios
- Administradores de asistencia técnica
- Administrador > Notificación de uso del sistema

12.1.1. Atributos

Utilice la página Atributos para llevar a cabo las tareas siguientes:

- Administre los tipos de información que puede registrar con usuarios, dispositivos y aplicaciones.
- Visualizar los tipos de estándares de información que Ivanti Neurons for MDM monitoriza.

Los atributos de usuario personalizados incluyen información como Departamento o una ID interna. Cada atributo tiene una variable correspondiente que puede usar para crear grupos o distribuir configuraciones.

> Durante la creación de los criterios de grupos de reglas de usuario, si los atributos personalizados tienen un valor numérico, Ivanti Neurons for MDM no es compatible con las operaciones de integrales.

Creación de atributos personalizados

Puede crear atributos personalizados desde el portal administrativo de Ivanti Neurons for MDM.

Procedimiento

1. Inicie sesión en el portal administrativo.
2. Vaya a **Administrador** > **Sistema** > **Atributos**.
3. En **Atributos personalizados**, haga clic en **+Añadir**.
4. En el campo **Nombre del atributo**, introduzca el texto que vaya a representar el atributo.

> el texto que introduzca se utilizará para crear la variable correspondiente en el campo **Uso**.

Seleccione cualquier tipo de atributo de las siguientes opciones de **Tipo de atributo**.

   - **Usuario**
   - **Dispositivo**
   - **Aplicación**
   - **IDP** (para más información, consulte Aprovisionamiento de usuarios con SCIM o Conecte Ivanti Neurons for MDM con Entra ID User Source)

Si el tipo de atributo es Dispositivo, seleccione una de las siguientes opciones de **Tipo de datos**:

   - **Numérico**
   - **Texto**

7. **Conservar atributo** (opcional): esta opción solo se puede utilizar cuando el tipo de atributo es **Dispositivo**. Seleccione esta opción para conservar el atributo personalizado incluso cuando se realiza una operación de borrado/retirada en un dispositivo.
8. Haga clic en **Añadir**.
   El atributo de usuario personalizado creado se muestra en la sección **Administrador añadido** en la página Atributos.

> la combinación de atributos personalizados $ + $ + $ + ${Static String} se admite en cualquier orden.

Cambiar el nombre de un atributo personalizado

Al cambiar el nombre de un atributo personalizado, se cambiará también el nombre de todas las referencias a dicho atributo personalizado que se estén usando en las siguientes entidades:

- Política personalizada
- Grupo de usuarios
- Grupo de dispositivos
- Filtro de distribución de aplicaciones
- Espacios

> no se actualizarán las referencias al atributo personalizado en ninguna otra entidad como las configuraciones, plantillas de invitaciones por correo electrónico, correos electrónicos y mensajes push en medidas de cumplimiento de políticas, entre otros.

Procedimiento

1. En **Administrador añadido**, haga clic en **+Editar** junto al atributo del que desea cambiar el nombre.
2. En el campo **Nombre del atributo**, introduzca el nuevo nombre que vaya a representar el atributo.

> el texto que introduzca se utilizará para crear la variable correspondiente en el campo **Uso**.

Haga clic en **Guardar**.

Eliminar un atributo personalizado

Si elimina un atributo personalizado, también eliminará sus valores de todos los usuarios o dispositivos asociados. Esto no puede revertirse.

No se pueden eliminar los atributos personalizados si el atributo se está usando en cualquiera de las siguientes entidades:

- Política personalizada
- Grupo de usuarios
- Grupo de dispositivos
- Filtro de distribución de aplicaciones
- Espacios

Antes de intentar eliminar el atributo personalizado, quítelo de las entidades.

Si el atributo que está intentando eliminar no tiene referencias de ninguna de las entidades anteriores, al hacer clic en **Eliminar** junto al atributo aparecerá un mensaje emergente para confirmar la acción. Confirme la acción y haga clic en **Eliminar**.

> Los nombres de campo de los siguientes atributos personalizados se ordenan en los creadores de reglas aplicables:

- Atributo personalizado de LDAP
- Atributo personalizado del usuario
- Atributo personalizado del dispositivo
- Atributos IDP personalizados
- Atributos de aplicaciones personalizados

Ver los atributos del sistema

Los atributos del sistema son atributos predefinidos que se pueden usar en las configuraciones como variables. La lista completa se proporciona en la sección **Atributos del sistema** de la página **Administrador** > **Sistema** > **Atributos**. Los atributos del sistema incluyen los siguientes tipos de atributos:

- Atributos del usuario
- Atributos del dispositivo
- Atributos de la plantilla de correo electrónico
- Atributos del sistema
- Atributos de la marca de hora
- Atributos personalizados del usuario de Entra ID
- Atributos de políticas

Atributos del usuario

Utilice los atributos del usuario para especificar la información sobre los usuarios.

Clave	Descripción
$	atributo departamento (requiere Entra ID)
$	Intercambio electrónico de datos: identificador personal
$	Id. de Apple administrada del usuario
$	Atributo sAMAccountName (requiere Active Directory)
$	Atributo Nombre común (NC) extraído del nombre distintivo (requiere LDAP)
$	Nombre en pantalla
$	Nombre distintivo (requiere LDAP)
$	La parte del dominio de la dirección de correo electrónico (la parte de después de la "@")
$>	La parte local de la dirección de correo electrónico (la parte de antes de la "@")
$	Dirección de correo electrónico
$	Nombre
$	Apellido
$	Configuración regional
$	Atributo de unidad organizativa (OU) extraído del nombre distintivo (requiere LDAP)
$	Información de Kerberos Realm (requiere Active Directory)
$	El dominio que forma parte de la ID de inicio de sesión (la parte tras la "@")
$	La parte local del ID de inicio de sesión (la parte de antes de la "@")
$	ID de inicio de sesión (formato de la dirección de correo electrónico)
$	Atributo userPrincipalName (requiere Active Directory)

Atributos del dispositivo

Utilice los atributos del dispositivo para especificar la información acerca de un dispositivo móvil.

Clave	Descripción
$	Fecha de la última vez que se conectó el cliente (conexión más reciente: bien MDM o cliente)
$	Número de serie alternativo
$	Identificador que usa la aplicación del cliente
$	Identificador de dispositivo único global
$	ICCID
$	IMEI2
$	IMEI
$	IMSI
$	Fecha de la última vez que se conectó el dispositivo (conexión más reciente: bien MDM o cliente)
$	Identificador de dispositivos internos
$	Identificador usado para MDM
$	MEID
$	Modelo
$	Nombre del dispositivo
$	Número de teléfono del dispositivo
$	Identificador de dispositivo único del cluster
$	Número de serie
$	iOS UDID
$	Dirección MAC de Wi-Fi
	Número de teléfono 2
	ICCID 2

Cuando se crea un atributo personalizado y se hace referencia a este en la configuración de una aplicación administrada, si se actualiza el valor del atributo, el atributo que se referencia en la configuración de la aplicación administrada también se actualiza y la configuración de la aplicación administrada se volverá a enviar al dispositivo.

Cuando se actualizan los atributos Personalizado o Dispositivo y la configuración se envía a un dispositivo, la configuración de marca de Android Kiosk también debe actualizarse.

Atributos de la aplicación

Use os atributos de la aplicación para especificar la información sobre las aplicaciones y crear grupos de aplicaciones personalizadas.

Clave	Descripción
$	Fecha en que se agregó la aplicación a AppCatalog
$	Nombre de la aplicación
$	Sistema operativo de la aplicación
$	Grupo de aplicaciones o ID del paquete
$	Describe la fuente desde la que se importó la aplicación
$	Describe si una aplicación de iOS o macOS es VPP o no

Atributos de la plantilla de correo electrónico

Clave	Descripción
$	Cuerpo del correo electrónico
$	Asunto del correo electrónico

Atributos de la marca de hora

Clave de variable	Descripción
$	Marca de hora actual (milisegundos desde epoch)

Atributos de plantilla de políticas

Clave	Descripción
$	Nombre de política infringido
$	Siguiente acción de cumplimiento en capas (distinto a esperar y retirar) que se llevará a cabo tras enviar el mensaje
$	Número de días que el dispositivo ha estado en un estado de no compatibilidad
$	La marca de hora cuando se desencadenó por primera vez la infracción de políticas (formato UTC DD-MM-AAAA)
$	Definición de la regla (Cadena de consulta tal y como aparece ahora)

Temas relacionados:

- Asignar atributos personalizados a los usuarios
- Asignar atributos personalizados a los dispositivos
- Eliminar atributos personalizados de los usuarios

- Eliminar atributos personalizados de los dispositivos
- Variables

12.1.2. Ajustes de borrado del dispositivo

El borrado del dispositivo automatiza el ciclo de vida del dispositivo para los que están sin usar. Puede retirar los dispositivos que no se hayan conectado durante el número de días que especifique. Puede eliminar los dispositivos que se hayan retirado durante el número de días que especifique. La página de Audit Trails captura los ajustes Retirar dispositivo, Eliminar dispositivo y Eliminar dispositivo borrado.

La tabla siguiente proporciona información sobre los dispositivos Android que admiten la configuración de borrado de dispositivos:

Modo	Retirar en caso de incumplimiento	Eliminar retirados	Forzar la retirada del dispositivo pendiente de retirada.	Eliminar borrados	Eliminar pendientes de borrado
Perfil de trabajo de Android (propietario del perfil)	**SÍ**	**SÍ**	**SÍ**	**NO**	**NO**
Perfil Administrador del dispositivo/ Trabajo en Dispositivo propiedad de la empresa	**SÍ**	**SÍ**	**SÍ**	**SÍ**	**SÍ**
Dispositivo administrado de trabajo/Dispositivo administrado con Android con perfil de trabajo	**NO**	**NO**	**NO**	**SÍ**	**SÍ**

Requisitos previos

Para acceder a esta configuración, debe tener permisos de Rol de administración del sistema.

Retirar dispositivos

Procedimiento

1. Vaya a **Administrador** > **Sistema** > **Limpieza de dispositivos**. Se abre la página Borrado de dispositivos.
2. Seleccione **Retirar dispositivo**.
3. Utilice la tabla **Retirar dispositivos** para especificar los detalles.
4. Haga clic en **Mostrar la lista de dispositivos que no han contactado**. Muestra la lista de dispositivos que no se han comprobado en un número de días especificado.
5. Haga clic en **Retirar dispositivos ahora**, alternativamente, puede programar la retirada del dispositivo.
6. El portal administrativo de Ivanti Neurons for MDM retirará los dispositivos especificados.

7.	Haga clic en **Guardar** para guardar sus ajustes.

	8.	(Opcional) Si actualiza los valores, puede hacer clic en **Restablecer** para restablecer los ajustes a sus valores iniciales.

Retirar dispositivos

Campo	Descripción
Seleccionar plataformas	Seleccione la plataforma necesaria en la que se deben aplicar los ajustes de limpieza del dispositivo. Esta opción solo está disponible actualmente en los **ajustes** Retirar dispositivo **y** Retirar dispositivo pendiente.
Retire los dispositivos que no se han comprobado en más de (días)	Días: 30 días por defecto, 365 días es el número máximo de días permitido.
Número máximo de dispositivos para Retirar en cada sesión	Seleccione 100, 500 o 1000 (Predeterminado: 100).
Retirar automáticamente dispositivos según un calendario	Marque la casilla para retirar dispositivos según un calendario preestablecido.
Retirar la configuración programada	Seleccione una de las siguientes opciones para establecer la frecuencia de retirada: • **Diariamente:** establecer para retirar los dispositivos todos los días. • **Semanal:** especifique el día de la semana para programar la retirada. • **Mensual:** configurar para retirar los dispositivos el primer día de cada mes.

Eliminar dispositivos retirados

Procedimiento

1. Vaya a **Administrador** > **Sistema** > **Limpieza de dispositivos**. Se abre la página Borrado de dispositivos.
2. Seleccione **Eliminar dispositivos retirados**.
3. Utilice la tabla **Eliminar dispositivos retirados** para especificar los detalles.
4. Haga clic en **Mostrar lista de dispositivos retirados**. Muestra la lista de dispositivos que se han retirado durante un número de días especificado.
5. Haga clic en **Eliminar dispositivos retirados ahora**, alternativamente, puede programar la eliminación del dispositivo.
6. El portal administrativo de Ivanti Neurons for MDM eliminará los dispositivos especificados.
7. Haga clic en **Guardar** para guardar sus ajustes.
8. (Opcional) Si actualiza los valores, puede hacer clic en **Restablecer** para restablecer los ajustes a sus valores iniciales.

Eliminar dispositivos retirados

Campo	Descripción
Elimine los dispositivos que se han retirado hace más de (días)	Días: 30 días por defecto, 365 días es el número máximo de días permitido.
Número máximo de dispositivos Retirados para eliminar en cada sesión	Seleccione 100, 500 o 1000 (Predeterminado: 100)
Borrar automáticamente dispositivos retirados según un calendario	Marque la casilla para retirar dispositivos según un calendario preestablecido.
Eliminar la configuración programada	Seleccione una de las siguientes opciones para establecer la frecuencia de borrado: • **Diariamente:** establecer para eliminar los dispositivos todos los días. • **Semanal:** especifique el día de la semana para programar el borrado. • **Mensual:** configurar para borrar los dispositivos retirados el primer día de cada mes.

Eliminar dispositivos borrados

Procedimiento

1. Vaya a **Administrador** > **Sistema** > **Limpieza de dispositivos**. Se abre la página Borrado de dispositivos.
2. Seleccione **Eliminar dispositivos borrados**.
3. Utilice la tabla **Eliminar dispositivos borrados** para especificar los detalles.
4. Haga clic en **Mostrar lista de dispositivos borrados**. Muestra la lista de dispositivos que se han retirado durante un número de días especificado.
5. Haga clic en **Eliminar dispositivos borrados ahora**, alternativamente, puede programar el borrado del dispositivo.
6. El portal administrativo de Ivanti Neurons for MDM eliminará los dispositivos especificados.
7. Haga clic en **Guardar** para guardar sus ajustes.
8. (Opcional) Si actualiza los valores, puede hacer clic en **Restablecer** para restablecer los ajustes a sus valores iniciales.

Eliminar dispositivos borrados

Campo	Descripción
Elimine los dispositivos que se han borrado hace más de (días)	Días: 30 días por defecto, 365 días es el número máximo de días permitido.
Número máximo de dispositivos borrados para eliminar en cada sesión	Seleccione 100, 500 o 1000 (Predeterminado: 100)
Eliminar automáticamente dispositivos borrados según un calendario	Seleccione la casilla de verificación para eliminar los dispositivos borrados según un calendario preestablecido.
Eliminar la configuración programada borrada	Seleccione una de las siguientes opciones para establecer la frecuencia de borrado: • **Diariamente:** establecer para eliminar los dispositivos borrados todos los días. • **Semanal:** especifique el día de la semana para programar el borrado. • **Mensual:** configurar para borrar los dispositivos retirados el primer día de cada mes.

Eliminar dispositivos pendientes de borrado

Procedimiento

1. Vaya a **Administrador** > **Sistema** > **Limpieza de dispositivos**. Se abre la página Borrado de dispositivos.
2. Seleccione **Eliminar dispositivos pendientes de borrado**.
3. Utilice la tabla **Eliminar dispositivos pendientes de borrados** para especificar los detalles.
4. Haga clic en **Mostrar lista de dispositivos borrados**. Muestra la lista de dispositivos que se van ha borrar durante el número de días especificado.
5. Haga clic en **Eliminar dispositivos pendientes de borrados ahora**, alternativamente, puede programar el borrado del dispositivo.
6. El portal administrativo de Ivanti Neurons for MDM eliminará los dispositivos especificados.
7. Haga clic en **Guardar** para guardar sus ajustes.
8. (Opcional) Si actualiza los valores, puede hacer clic en **Restablecer** para restablecer los ajustes a sus valores iniciales.

Eliminar dispositivos pendientes de borrado

Campo	Descripción
Elimine los dispositivos que llevan más de (días) pendientes de borrado	Días: 30 días por defecto, 365 días es el número máximo de días permitido.
Número máximo de dispositivos pendientes de borrado para eliminar en cada sesión	Seleccione 100, 500 o 1000 (Predeterminado: 100)
Eliminar automáticamente dispositivos pendientes de borrado según un calendario	Seleccione la casilla de verificación para eliminar los dispositivos borrados según un calendario preestablecido.
Eliminar la configuración programada pendiente de borrado	Seleccione una de las siguientes opciones para establecer la frecuencia de borrado: • **Diariamente:** establecer para eliminar los dispositivos pendientes de borrados todos los días. • **Semanal:** especifique el día de la semana para programar el borrado. • **Mensual:** configurar para borrar los dispositivos pendientes de borrar el primer día de cada mes.

Retirar el dispositivo pendiente de retirada.

Procedimiento

1. Vaya a **Administrador** > **Sistema** > **Limpieza de dispositivos**. Se abre la página Borrado de dispositivos.
2. Seleccione **Retirar el Dispositivo pendiente de retirada**.
3. Utilice la tabla **Retirar dispositivos pendientes** para especificar los detalles.
4. Haga clic en **Mostrar lista de dispositivos pendientes de retirada**. Muestra la lista de dispositivos que se van a retirar durante un número de días especificado.
5. Haga clic en **Forzar la retirada de Dispositivos pendientes de retirada ahora**. También puede programar la retirada de los dispositivos pendientes.
6. El portal administrativo de Ivanti Neurons for MDM retirará los dispositivos especificados.
7. Haga clic en **Guardar** para guardar sus ajustes.
8. (Opcional) Si actualiza los valores, puede hacer clic en **Restablecer** para restablecer los ajustes a sus valores iniciales.

Retirar el dispositivo pendiente de retirada.

Campo	Descripción
Retirar los dispositivos pendientes de retirada que no se han registrado más de (días)	Días: 30 días por defecto, 365 días es el número máximo de días permitido.
Número máximo de dispositivos pendientes de retirada para Retirar en cada sesión	Seleccione 100, 500 o 1000 (Predeterminado: 100)
Retirar automáticamente los dispositivos pendientes de retirada según un calendario	Seleccione la casilla para retirar dispositivos pendientes según un calendario preestablecido.
Retire la configuración programada pendiente de retirada	Seleccione una de las siguientes opciones para establecer la frecuencia de borrado: • **Diariamente:** establecer para retirar los dispositivos pendientes todos los días. • **Semanal:** especifique el día de la semana para programar la retirada. • **Mensual:** configurar para retirar los dispositivos el primer día de cada mes.

Cuando se retira un dispositivo y si el registro se produjo hace mucho tiempo, ese último tiempo de registro solo se tendrá en cuenta para determinar la eliminación del dispositivo. Por ejemplo, si el dispositivo se verificó por última vez hace 30 días y si el dispositivo se retiró hoy (puede deberse a "Retirar dispositivos que no se han registrado más de (días)"), y si la opción "Eliminar dispositivos que se han retirado más de (días)" se establece como 30 días, el dispositivo se eliminará inmediatamente una vez que se ejecute el trabajo "Eliminar dispositivo retirado".

12.1.3. Perfiles GDPR

El portal administrativo de Ivanti Neurons for MDM ahora contiene una página de perfiles de GDPR que le permite asignar perfiles de GDPR a grupos de usuarios. Solo puede asignar el perfil de GDPR a grupos de usuarios y no a usuarios individuales.

Tenga en cuenta los puntos siguientes:

- En primer lugar debe activar los perfiles de GDPR para asignarlos a un grupo de usuarios específico.
- Si desactiva el perfil GDPR, se desactivarán todas las restricciones del perfil que ya se habían asignado al grupo de usuarios.
- Después de activar el perfil GDPR, se limitará o desactivará la función Editar para algunos campos.

Los campos que están ocultos tras la asignación del perfil GDPR

Si un usuario tiene un perfil de GDPR, Ivanti Neurons for MDM oculta los campos siguientes por defecto cuando se muestra la información del usuario:

- **Id. de Usuario**
- **Nombre de usuario**
- **Dirección de correo electrónico**
- **Número de serie**
- **ICCID**
- **IMSI**
- **MEID**
- **Dirección IP**
- **Número de teléfono**
- **IMEI**
- **Identificador eSIM**
- **Ubicación**

> Si se añade Ubicación al perfil GDPR, los campos Ubicación del dispositivo Última ubicación en, Latitud y Longitud se enmascaran en los detalles del dispositivo para los usuarios asignados con el perfil GDPR.

Activación del perfil GDPR

Puede habilitar el perfil de GDPR y seleccionar campos específicos que se deben ocultar en el portal administrativo de Ivanti Neurons for MDM y los dispositivos.

ProcedureProcedimiento

	1.	**Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.**
	2.	**Vaya a Admin > Sistema > Perfiles GDPR.**

	3.	Haga clic en **Habilitar**.
	4.	Haga clic en el icono de editar (lápiz).
	5.	Seleccione los campos que se deben ocultar.
	6.	Haga clic en **Guardar**. Los campos seleccionados se enmascararán y no mostrarán los valores de los usuarios específicos.

Asigne el perfil GDPR al Grupo de usuarios

Después de activar los perfiles GDPR, podrá asignarlos a un grupo de usuarios específico.

ProcedureProcedimiento

	1.	Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
	2.	Vaya a **Usuarios** > **Grupos de usuarios**.
	3.	Seleccione un grupo de usuario de la lista.
	4.	Haga clic en la lista desplegable **Acciones** y seleccione **Asignar perfil GDPR**. El perfil GDPR se asigna a todos los usuarios de ese grupo específico y todos los valores seleccionados se enmascararán de la vista mediante el portal administrativo y los dispositivos del usuario. Puesto que el administrador también está en el grupo Todos los usuarios, no asigne los perfiles GDPR al grupo Todos los usuarios.

12.1.4. Correos electrónicos de notificación

Licencia: Silver

Usted puede configurar la lista de direcciones de correo electrónico de los usuarios que deberían recibir notificaciones por correo electrónico en función del nivel de gravedad de la notificación.

La función Correo electrónico de notificación es opcional y puede activarla o desactivarla según le resulte necesario. Para usar esta característica, es un requisito previo tener asignada la función de administración del sistema.

1. Seleccione **Administración > Sistema > Correos electrónicos de notificación**. Aparecerá la página **Correos electrónicos de notificación**.
2. En la sección Ajustes de correos electrónicos de notificación, haga clic en **ACTIVADO** para activar la función Correos electrónicos de notificación.
3. Haga clic en **Añadir destinatario**. Aparecerá la ventana emergente **Añadir destinatario**.
4. En la ventana emergente **Añadir destinatario**, actualice los siguientes campos:
    - Id. del correo electrónico del destinatario: introduzca la id. del correo electrónico del destinatario a quien se debe enviar la notificación.
    - Tipos de notificaciones a enviar: seleccione el tipo de notificación marcando la casilla. A continuación se enumeran los diferentes tipos de notificaciones: **Notificaciones críticas, Notificaciones de advertencia, Notificaciones informativas**.
5. Haga clic en **Aceptar**. Los detalles de los ajustes aparecerán en una tabla.
6. Haga clic en **Guardar** para aplicar los cambios.

12.1.5. Administración de funciones

Las funciones son grupos de permisos empaquetados que permiten otorgar un conjunto de permisos a un usuario administrativo, a la vez que limitan su acceso para controlar áreas específicas de funcionalidad. Ivanti Neurons for MDM proporciona un conjunto de funciones del sistema que se pueden asignar (o editar) y un centro para crear funciones personalizadas. Puede buscar permisos específicos según la categoría, y la interfaz mostrará todas las opciones asociadas al rol o permiso seleccionado. Se muestra un tooltip para los permisos que se añaden como permisos dependientes.

> La página Gestión de roles y las opciones asociadas están ocultas para los abonados convergentes que tienen acceso a Ivanti Neurons for UEM y Ivanti Neurons for MDM.

Hay dos tipos de permisos disponibles y, por lo tanto, dos tipos de funciones:

- **Roles específicos para un espacio**: los permisos son específicos para un espacio y, por lo tanto, se aplican únicamente a un espacio específico. Algunos ejemplos son la administración de dispositivos y la administración de aplicaciones dentro de un espacio.
- **Roles para todos los espacios**: los permisos pueden, por su naturaleza, aplicarse a todos los roles. Algunos ejemplos son los ajustes a nivel de abonado, como los certifcados MDM y los ajustes del App Catalog.

Crear una función personalizada

Puede crear funciones personalizadas multiespacio o específicas para cada espacio. Cuando seleccione un permiso, los permisos dependientes se seleccionarán automáticamente. Por consiguiente, un usuario con una función personalizada solo puede realizar las acciones específicas disponibles (como retirar o borrar) cuando el usuario visite la página Dispositivos o la página Detalles del dispositivo.

Cuando se aplica el rol personalizado Ver PIN de registro de usuario, los usuarios pueden ver el PIN de otros usuarios que tienen el mismo nivel de acceso o con menores privilegios y los usuarios no pueden crear PIN para otros usuarios.

> La función personalizada recién creada no se puede asignar a nadie automáticamente. El superadministrador de abonados debe asignarla a los usuarios administradores requeridos que, posteriormente, podrán asignarla a otros usuarios según sea necesario.

Procedimiento

1. Vaya a **Administrador** > **Administración de roles**.
2. Haga clic en **+Añadir función personalizada**.
3. En la página **Crear rol**, introduzca el **Nombre** del nuevo rol.
4. (Opcional) agregue una descripción para el nuevo rol.
5. En **Tipo de rol**, seleccione una de las siguientes opciones:
   - **Función de espacios cruzados**
   - **Función específica para espacios**
6. En **Permisos**, seleccione los permisos granulares requeridos.
7. Consulte la siguiente tabla para conocer los permisos de Administrador y de Usuario.
   Haga clic en **Guardar**.

La tabla siguiente lista los permisos, roles y atributos que puede usar para crear un rol personalizado:

Tipo de función	Categoría de permiso	Permisos pormenorizados
Función de espacios cruzados		
Administrador		
	Administrar atributos personalizados	• Añadir atributo personalizado • Eliminar atributo personalizado • Editar atributo personalizado • Ver atributo personalizado
	Administradores de asistencia técnica	• Añadir administradores de asistencia técnica • Eliminar administradores de asistencia técnica • Desactivar administradores de asistencia técnica • Ver administradores de asistencia técnica y mostrar historial del inicio de sesión
	Autoridad de certificados	• Añadir Entidad de Certificación • Eliminar Entidad de Certificación
	Conector	• Añadir registros de Conector • Eliminar registros de Conector • Ver Conector • Actualizar Conector
	Gestión LDAP	• Añadir usuario/grupo/OU • Añadir servidor • Navegar por el servidor • Borrar servidor • Buscar en servidor

Tipo de función	Categoría de permiso	Permisos pormenorizados
		• Sincronizar servidor • Quitar usuario/grupo/OU • Ver Servicio Todos los permisos de LDAP de esta sección requieren el permiso de Ver conector. Se seleccionará automáticamente en la sección Conector cuando seleccione cualquiera de estos permisos de LDAP.
	Gestión de licencias	Ver licencias
	Gestionar la distribución de aplicaciones	**Actualizar la distribución de aplicaciones** El permiso para **Actualizar la distribución de aplicaciones** ya está disponible para roles personalizados en **Gestionar la distribución de aplicaciones**. Los usuarios con el rol Gestión del sistema reciben este permiso de forma predeterminada. La página de distribución de aplicaciones ahora incluye la casilla **Permitir que el administrador del espacio edite la distribución** , que está habilitada por defecto para las nuevas versiones de la aplicación. Los usuarios asignados a un rol personalizado con este nuevo permiso, así como aquellos con el rol Gestión de aplicaciones (sin acceso a Gestión del sistema), pueden modificar este ajuste. Para cada versión de la aplicación, la disponibilidad de la configuración Bloquear la distribución de aplicaciones se muestra en la página de distribución, y todos los intentos de exclusión se registran ahora en el registro de auditoría.
Usuarios		
	Acciones de administración del usuario	• Ver usuario • Actualizar usuario • Enviar mensaje al usuario • Añadir/asignar funciones al usuario • Crear usuario • Eliminar Usuario • Invitar usuario • Ver PIN de registro de usuario
	Asignar atributo personalizado del	• Borrar atributo • Ver atributos • Añadir/editar atributo

Tipo de función	Categoría de permiso	Permisos pormenorizados
	usuario	
	Grupos de usuarios	• Ver Grupo de usuarios • Editar grupo de usuarios • Añadir/asignar funciones al Grupo de usuarios • Crear grupo de usuarios • Eliminar grupo de usuarios
	Gestión de informes	• Crear informe • Editar informe • Ejecutar informe • Borrar registro de informe • Ver informe • Borrar informe • Descargar registro de informes
Dispositivos **Función específica para espacios**	Inscripción en masa	• Crear inscripción en masa • Actualizar inscripción en masa • Asignar usuario a la inscripción en masa • Ver inscripción en masa • Eliminar inscripción en masa
Dispositivos		
	Acciones de	• Asignar dispositivo al usuario

Tipo de función	Categoría de permiso	Permisos pormenorizados
	dispositivos	• Eliminar bloqueo de activación de dispositivos • Eliminar dispositivo • Deshabilitar Modo perdido de dispositivo • Habilitar Modo perdido de dispositivo • Ingreso forzoso del dispositivo • Bloquear dispositivo • Desbloquear dispositivo • Cierre de sesión forzado del dispositivo • Reinstalar aplicaciones del sistema de dispositivos • Reiniciar el dispositivo • Programar actualizaciones de dispositivos iOS • Renunciar a la propiedad de un dispositivo • Retirar dispositivo • Cancelar Retirar dispositivo • Apagar el dispositivo • Ver el dispositivo • Borrar dispositivo • Cancelar Borrar dispositivo • Actualizar la versión de SO del dispositivo • Asignación en masa a través de la Carga • Iniciar sesión de TeamViewer • Entrar en modo kiosko • Salir del modo Pantalla completa
	Asignar atributo del dispositivo personalizado	• Añadir/editar atributo personalizado del dispositivo • Eliminar atributo personalizado del dispositivo • Ver atributo personalizado del dispositivo Todos los permisos de Asignar atributo del dispositivo personalizado de esta sección requieren el permiso de Lectura de dispositivos. Se seleccionará automáticamente en la sección Acciones del dispositivo cuando seleccione cualquiera de estos permisos de Asignación de atributos del dispositivo personalizado.
	Configuraciones del	• Excluir perfil • Insertar perfil • Insertar perfil excluido

Tipo de función	Categoría de permiso	Permisos pormenorizados
	dispositivo	• Reinstalar tras error
	Grupos de dispositivos	• Añadir un nuevo Grupo de dispositivos • Eliminar grupo de dispositivos • Editar grupo de dispositivos • Ver grupo de dispositivos
	Inscripción en masa	• Crear inscripción en masa • Actualizar inscripción en masa • Asignar usuario a la inscripción en masa • Ver inscripción en masa • Eliminar inscripción en masa
Configuraciones	Inventario de aplicaciones	• Ver inventario de aplicaciones
Políticas	Configuraciones	• Ver/exportar configuraciones • Editar/Priorizar configuraciones • Añadir/Duplicar configuraciones • Borrar configuraciones
	Políticas	• Ver políticas • Editar/Priorizar políticas • Añadir/Duplicar políticas • Eliminar políticas

Para editar una función, vaya a la página Administración, Administración de funciones y haga clic en el icono de editar que está en **Acciones** junto al nombre de la función. Un usuario no puede cambiar una función de espacios cruzados a función específica para espacios y viceversa.

Temas relacionados:

- Para asignar una función personalizada a un usuario, consulte **Asignar funciones**.
- Consulte **Funciones de usuario** para ver una lista de funciones predeterminadas.
- **Uso de Informes personalizados**
- **Uso de Informes programados**

12.1.6. Espacios

Esta sección contiene los siguientes temas:

- Espacios
- Administrar espacios
- Ejemplos de espacios
- Delegar dispositivos
- Delegar aplicaciones

12.1.6.1. Espacios

Licencia: Silver

Los espacios se emplean para aislar un sistema de administración unificada de puntos de conexión (UEM, Unified Endpoint Management) en entidades administradas de forma independiente para poder llevar a cabo una administración delegada. Los espacios pueden crearse para reflejar una jerarquía organizativa. Ivanti Neurons for MDM admite la delegación a nivel único con una entidad administrativa central definida como espacio predeterminado y una cantidad de entidades administrativas subordinadas denominadas espacios delegados. Todos los sistemas de UEM se crean con un espacio predeterminado.

> La página Spaces y las opciones asociadas están ocultas para los abonados convergentes que tienen acceso a Ivanti Neurons for UEM y Ivanti Neurons for MDM.

Los espacios permiten la administración delegada de los siguientes componentes del sistema. Actualmente, los usuarios y los grupos de usuarios no pueden delegarse.

- Dispositivos
- Configuraciones
- Políticas
- Grupos de dispositivos
- Aplicaciones
- Un App Catalog
- Un token de Apps and Books de Apple

Cuando un administrador inicia sesión en el portal de administración de Ivanti Neurons for MDM en un abonado con al menos un único espacio delegado, al administrador se le presenta la ventana emergente de promoción para iniciar sesión en el portal de administrador. La ventana emergente de promoción no se mostrará tras la creación de un espacio delegado ni durante el inicio de sesión si ya se ha creado un espacio delegado.

Funciones para administradores globales y de espacios delegados

Al usuario administrador con las funciones necesarias para acceder al espacio predeterminado se le denomina Administrador global. El acceso al espacio predeterminado puede ser de solo lectura o de lectura y escritura. El administrador global con las funciones administrativas necesarias puede crear espacios delegados y asignar administradores delegados para administrarlos. Puede asignarse un administrador delegado para administrar uno o más espacios delegados.

Los espacios a los que puede acceder un administrador en concreto se enumeran en el selector de espacios desplegable, situado en la esquina superior izquierda de las pestañas Dispositivos y Aplicaciones. Para ver y administrar un espacio, utilice el menú desplegable para cambiar al espacio deseado.

Un administrador global puede ver y controlar todos los espacios delegados, además del espacio predeterminado. Un administrador delegado puede ver y controlar solamente los espacios que le ha asignado el administrador global. Un administrador global posee el control central de los espacios delegados, mientras que un administrador delegado tiene la autonomía para administrar los espacios que se le han delegado. Este nivel de autonomía viene determinado en función de si la delegación se ha heredado o se ha copiado desde el espacio predeterminado.

A continuación se enumeran las diferentes funciones del usuario y las tareas que pueden realizar:

Aplicación heredada en un espacio delegado

- Se heredan las puntuaciones u opiniones existentes en el momento de la delegación y son visibles para los usuarios del espacio delegado, incluido el nombre de usuario del autor.
- El administrador delegado no puede eliminar puntuaciones/opiniones de una aplicación heredada.
- El administrador delegado puede exportar puntuaciones/opiniones de una aplicación heredada.
- Los usuarios de los espacios delegados pueden añadir puntuaciones/opiniones a una aplicación heredada.
- Los usuarios de los espacios delegados pueden ver las puntuaciones/opiniones añadidas por usuarios en los espacios delegados, incluido el nombre de usuario del autor.

Aplicación en un espacio delegado (añadido, no heredado)

- Solamente un administrador global puede activar o desactivar las opiniones en **Aplicaciones > Ajustes del catálogo > Puntuaciones y opiniones**.
- Los usuarios de un espacio delegado pueden añadir puntuaciones/opiniones.
- Un administrador delegado puede eliminar opiniones añadidas por usuarios en el mismo espacio delegado.
- Los usuarios de otros espacios delegados, incluido el predeterminado, no podrán ver las puntuaciones u opiniones añadidas por usuarios de todos los espacios delegados.
- El administrador delegado puede exportar las opiniones añadidas por todos los usuarios, incluidos los nombres de usuario.

Aplicación delegada en un espacio predeterminado

- El administrador global puede eliminar las puntuaciones o revisiones añadidas por un usuario en un espacio delegado.
- El administrador global puede exportar todas las puntuaciones o revisiones, incluidas aquellas añadidas por usuarios en los espacios delegados.
- Los usuarios de un espacio predeterminado pueden ver las puntuaciones u opiniones añadidas por usuarios en los espacios delegados, incluido el nombre de usuario.

Prioridad de un espacio delegado

El espacio predeterminado de un sistema de UEM tiene siempre el nivel más bajo de prioridad. El administrador global establece la prioridad de un espacio delegado relativo a otro espacio delegado. Esta prioridad puede cambiarse en cualquier momento. Los espacios delegados se enumeran por orden en niveles de mayor a menor prioridad en la página de espacios, situada en la pestaña Administrador del Portal de administración.

Delegación mediante herencia o copia

Un concepto clave de la administración delegada es si un componente del sistema se ha heredado o copiado desde el espacio predeterminado.

12.1.6.2. Administrar espacios

Los espacios le permiten designar los grupos de dispositivos que administrarán los diferentes administradores (administración delegada). El administrador de un espacio puede definir las configuraciones y {{políticas}} que se aplican a los dispositivos de un espacio. Una vez creados los espacios, puede asignar cada uno al administrador que corresponda.

Esta página de espacios incluye:

- Funciones de búsqueda para localizar rápidamente los espacios.
- Controles de paginación para navegar por un gran número de espacios.
- Controles de priorización de espacios para gestionar el orden de los espacios delegados.
- Opciones para seleccionar y eliminar varios espacios.

> No es posible eliminar el espacio predeterminado.

- Clasificación alfabética de los espacios.
- Una lista de los espacios vistos recientemente en el selector de espacios.
- Selección persistente del espacio en las páginas Dispositivos, Configuraciones, Políticas y Contenido, lo que reduce la necesidad de volver a seleccionar un espacio al navegar entre páginas.

> El usuario solo puede ver los espacios asignados y no todos los espacios disponibles. Desde ahora, este ajuste se aplica únicamente a módulos de **Dispositivos**, **Grupos de dispositivos**, **Aplicaciones**, **Inventarios de aplicaciones**, **Contenido**, **Configuraciones**, **Políticas** y **Administración de certificados**. Los espacios seleccionados en la lista de Spaces mientras se visualiza cualquiera de estos módulos se guardan como selección predeterminada preferida del administrador para ese módulo. Estas preferencias no solo se guardan en la sesión de inicio de sesión actual, sino también en las sesiones futuras.

Los espacios que cree heredarán todas las configuraciones del espacio predeterminado. Por lo tanto, cualquier configuración que cree posteriormente en el espacio predeterminado puede aplicarse a los demás espacios. No obstante, los cambios realizados en una configuración existente no se heredan.

Los espacios que cree solamente recibirán copias de las políticas existentes en el espacio predeterminado en ese momento. Cualquier política que cree posteriormente en el espacio predeterminado solo se aplicará a este.

Cree las reglas que definirán qué dispositivos están en el espacio. Estas reglas se pueden filtrar usando los operadores correspondientes, como «comienza con», «termina con», «contiene», «no contiene», «no comienza con», «no termina con», «es menor que», «es mayor que», «está en el intervalo», «es igual a» y «no es igual a». Las reglas se pueden anidar juntas utilizando las opciones CUALQUIERA (O) o TODOS (Y). Se puede revisar la precisión de las reglas utilizando el texto que aparece al final de dichas reglas.

El portal del Administrador de Ivanti Neurons for MDM muestra el número de grupos de usuarios duplicados y el correspondiente número de GUID para identificar los grupos duplicados, cuando se selecciona el atributo Nombre del grupo de usuarios en el generador de reglas. Además, una tabla bajo esta regla muestra la lista de los grupos de usuarios duplicados y sus detalles, como el Nombre del Grupo de Usuarios, el GUID, la Fuente y el nombre distinguido (DN).

Las reglas pueden identificar los dispositivos según:

- Entra ID Inscrito
- Compatible con APNS

- Número alternativo de serie (Solo Android: aplicable a dispositivos Samsung en modo Administrador del dispositivo o Propietario del dispositivo)
- Segmentación de red 5G de Android habilitada
- Android Enterprise: modo no GMS para el dispositivo administrado en el trabajo (AOSP) activado
- Dispositivo Android dedicado
- Compatible con Android Enterprise
- Dispositivo administrado de Android con perfil profesional
- Tipo de certificación SafetyNet de Android
- Android for Work habilitado
- Nivel de revisión de la seguridad de Android (dispositivos Android)
- Dispositivos Android administrados en el trabajo (Propietario del dispositivo) habilitados
- Perfil de Android for Work habilitado
- Perfil de trabajo de Android habilitado en dispositivos que son propiedad de la empresa habilitados
- Estado nativo de antiphishing
- Estado de antiphishing
- Estado de la VPN de antiphishing
- Inscrito en la Inscripción de dispositivos automatizada
- Inscripción de dispositivos automatizada activada
- Autopilot inscrito
- Código de estado del cliente de Azure
- Hora del informe de cumplimiento del dispositivo Azure
- Estado de cumplimiento del dispositivo Azure
- Identificador del dispositivo Azure
- Sentry bloqueado
- Acceso bloqueado
- Token de Bootstrap disponible
- Tipo de aprovisionamiento masivo (configurador de Apple o ninguno)
- Operador
- Último ingreso del cliente
- Registrado con el cliente
- Cumplimiento
- Medida de cumplimiento bloqueada
- Nombre del país actual (seleccione el nombre del país de la lista desplegable)
- MMC actual
- MNC actual
- Atributo personalizado del dispositivo
- Atributo personalizado de LDAP

- Atributo personalizado del usuario
- Itinerancia de datos
- Origen del dispositivo
- Tipo de dispositivo
- Tipo de dispositivo (Apple)
- Nombre en pantalla
- Cifrado habilitado
- Nombre del país de origen (seleccione el nombre del país de origen de la lista desplegable)
- MCC de origen
- MNC de origen
- IMEI
- IMEI2 (solo en dispositivos Android con doble puerto SIM y aplicable para dispositivos Android 8.0 o superior)
- Clave de recuperación institucional habilitada
- Dirección IP
- Modo pantalla completa
- Último ingreso
- Modo perdido habilitado
- Solo MAM
- Fabricante
- Estado de activación del MTD
- Modo multiusuario
- SO
- Versión de SO
- SO con versión
- Propiedad
- Clave de recuperación personal habilitada
- N.º de teléfono
- En cuarentena
- Bloqueo de recuperación habilitado
- Itinerancia
- Estado de Secure Apps
- Número de serie
- Estado
- Supervisado
- Versión de generación suplementaria
- Suplemento SO/Versión Extra
- Desbloquear token disponible (iOS)

- Inscripción de usuarios inscritos
- Grupo de usuarios
- Nombre de usuario
- Itinerancia de voz
- Clave de recuperación personal de macOS en custodia
- Tipo de clave de recuperación de macOS

> Estas reglas están disponibles solo para la licencia **Silver** y superiores.

Crear un espacio

Procedimiento

1. Vaya a **Administración** > **Sistema** > **Espacios**.
2. Haga clic en **Crear espacio**.
3. Introduzca el nombre del espacio.
4. Configure las reglas y los ajustes correspondientes al espacio.
5. Haga clic en **Guardar**.

Priorizar espacios

Ivanti Neurons for MDM evalúa los espacios en orden de aparición.

Procedimiento

1. Haga clic en **Priorizar espacios**.
2. Seleccione el icono de flecha hacia arriba o hacia abajo situado junto a un espacio para ajustar su prioridad.
3. Haga clic en **Guardar**.

Eliminar espacios

1. Vaya a **Administración** > **Sistema** > **Espacios**.
2. Seleccione uno o varios espacios usando las casillas de verificación.
3. Haga clic en **Eliminar**. Confirme la eliminación cuando se le solicite.

Asignar un administrador a un espacio

Procedimiento

1. Vaya a **Usuarios.**
2. Busque el usuario que va a ser el administrador.
3. Haga clic en el vínculo del usuario para mostrar los detalles.
4. Seleccione **Acciones** > **Asignar roles**.
5. Seleccione **Administración de dispositivos**.
6. En **Administración de dispositivos**, seleccione el espacio para este administrador.

7. Haga clic en **Hecho**.

Cuando este administrador inicie sesión, solo serán visibles los dispositivos, configuraciones y políticas del espacio asignado.

Duplicar una configuración o política

Dentro de un espacio, se puede duplicar una configuración o política si necesita duplicarlas con algunas diferencias. También puede asociar las configuraciones o políticas duplicadas a diferentes grupos de dispositivos. Se pueden duplicar todas las políticas dentro de un espacio. También se pueden duplicar todas las configuraciones dentro de un espacio, excepto el Certificado de identidad provisto por el usuario y Threat Defense. Las siguientes configuraciones también pueden duplicarse en los distintos espacios desde el espacio predeterminado:

- Restricciones de iOS
- Clip web
- Certificado
- Código de acceso
- SCEP (iOS y Windows)
- Certificado de identidad (generado dinámicamente)

- el nombre de una configuración o tipo de política debe ser único dentro de un mismo espacio. Se pueden duplicar todas las demás propiedades de una configuración o política.
- Además, las configuraciones pueden duplicarse en todos los espacios a los que usted tiene acceso como administrador. No es necesario ser el Administrador global para poder duplicar una configuración.

Procedimiento

1. Vaya a **Configuraciones** o **Políticas**, dependiendo de lo que desee duplicar.
2. Haga clic en el enlace para que la configuración o política muestre los detalles.
3. Haga clic en el icono **Duplicar**.
4. En la ventana emergente, introduzca un **Nombre** y, opcionalmente, una **Descripción**.
5. Haga clic en **Siguiente**.
6. Modifique la configuración o la política según sus requisitos.
7. Haga clic en **Siguiente**.
8. Configure la distribución.
9. Haga clic en **Hecho**.

Para obtener más información, consulte Ejemplos de espacios.

12.1.6.3. Ejemplos de espacios

Este tema da ejemplos relacionados con cómo los administradores pueden utilizar los espacios.

Administrador por localización

ACME, Inc. tiene oficinas en Norteamérica y Europa. Por cuestiones de idioma y zona horaria, ACME quiere tener un administrador en EE. UU. que administre los dispositivos de Norteamérica y otro administrador en Alemania que administre los dispositivos de Europa.

Para configurar estos espacios, ACME llevó a cabo los siguientes cambios:

1. Se ha creado un grupo de usuarios en Ivanti Neurons for MDM para usuarios de Europa.
2. Creó un grupo de usuarios en Ivanti Neurons for MDM para usuarios en Norteamérica.
3. Creó un espacio de Europa con la siguiente regla:
4. Grupo de usuarios = Europa
   Creó un espacio de Norteamérica con la siguiente regla:
5. Grupo de usuarios = Norteamérica
   Asignó la función de Administración de dispositivos de cada espacio al administrador adecuado.

Ahora, ACME cuenta con los siguientes espacios:

- Europa
- Norteamérica
- Predeterminada

Administrador por SO por localización

ACME ha decidido que solo los expertos en Android deben administrar los dispositivos Android. Se ha añadido un experto en Android a la organización de Norteamérica y otro a la de Europa. En consecuencia, se necesitan dos nuevos espacios.

Para añadir los espacios, ACME llevó a cabo los siguientes cambios:

1. Creó un espacio de Europa-Android con las siguientes reglas:
2. Grupo de usuarios = Europa
   OS = Android
   Creó un espacio de Norteamérica-Android con las siguientes reglas:
3. Grupo de usuarios = Norteamérica
   OS = Android
   Asignó la función de Administración de dispositivos de cada espacio al administrador adecuado.

Ahora, ACME cuenta con los siguientes espacios:

- Europa-Android
- Norteamérica-Android
- Europa
- Norteamérica
- Predeterminada

Administrador para ejecutivos

Los ejecutivos de ACME han decidido que quieren recibir un servicio especial de un administrador especial. Solo los ejecutivos más importantes están en esta lista.

Para añadir este espacio, ACME llevó a cabo los siguientes cambios:

1. Creó un espacio de ejecutivos con las siguientes reglas:
2. Nombre de usuario = pruiz@acme.com
   Nombre de usuario = gmontero@acme.com
   Nombre de usuario = aperez@acme.com
   Nombre de usuario = fayuso@acme.com
   Movió el espacio a la parte superior de la lista de la página **Espacio**.
3. De lo contrario, los ejecutivos con dispositivos Android tendrían el administrador equivocado.
   Asignó la función de Administración de dispositivos del espacio al administrador especial.

Ahora, ACME cuenta con los siguientes espacios:

- Equipo directivo
- Europa-Android
- Norteamérica-Android
- Europa
- Norteamérica
- Predeterminada

Administrador para todos los demás dispositivos

Cuando ACME abra una nueva oficina en Japón, los dispositivos que se añadan se asignarán al administrador del espacio predeterminado hasta que alguien cree un espacio de Japón.

12.1.6.4. Delegar dispositivos

Los espacios se utilizan para separar sus dispositivos en partes que se controlan independientemente. La pertenencia a los espacios se determina a partir de las reglas que se creen. La delegación de dispositivos permite al administrador global hacer una partición y administrar de manera independiente los dispositivos de un sistema de UEM. Cuando se delegan los dispositivos, el acceso a estos puede asignarse a un subconjunto de administradores delegados, con lo que se distribuyen las responsabilidades de los administradores.

Los dispositivos delegados pueden agruparse en grupos de dispositivos y se les pueden aplicar diferentes configuraciones personalizadas aplicadas sin que esto afecte a los dispositivos del espacio predeterminado u otros espacios.

Crear reglas para delegar dispositivos

Las reglas que se definen para un espacio determinan qué dispositivos pertenecen a dicho espacio. Un dispositivo solo puede pertenecer a un espacio. Los dispositivos que no cumplan las reglas de los espacios que usted cree, pertenecerán automáticamente al espacio predeterminado.

1. Seleccione **Cualquiera** si desea que los dispositivos se incluyan en esta definición si cumplen cualquiera de las reglas.
2. Seleccione **Todas** si desea que los dispositivos solamente se incluyan en esta definición si cumplen todas las reglas.
3. Seleccione uno de los siguientes tipos de reglas de la lista desplegable:
    - **Atributo personalizado de LDAP:** para las reglas basadas en atributos LDAP.
    - **SO**: para las reglas basadas en el sistema operativo del dispositivo.
    - **Grupo de usuarios**: para las reglas basadas en el grupo de usuarios un dispositivo (según se define en el servicio de administración dispositivo).
    - **Nombre de usuario**: para las reglas basadas en el nombre de usuario asociado con el dispositivo.
4. Defina los criterios para el tipo de regla seleccionada:
    - **Atributo personalizado de LDAP:** introduzca el nombre del atributo LDAP personalizado que se configuró en los ajustes de LDAP.
    - **Sistema operativo**: seleccione Android, iOS, macOS o Windows.
    - **Grupo de usuarios**: seleccione uno de los grupos de usuarios mostrados en la lista desplegable. Estos son los grupos de usuarios definidos en **Usuarios > Grupos de usuarios**.
    - **Nombre de usuario**: escriba un nombre de usuario.
5. Para añadir otra regla para este espacio, haga clic en + junto a la regla anterior.
6. Haga clic en **Vista previa** para ver qué dispositivos se asignarán al espacio.
7. Haga clic en **Guardar** cuando esté satisfecho con los dispositivos del espacio.

Los dispositivos que no cumplan las reglas de un espacio serán automáticamente movidos al siguiente espacio en el que sí encajen. Si el dispositivo no cumple las reglas de un espacio existente, se moverá al espacio predeterminado. Por ejemplo, al eliminar a un usuario de un grupo de usuarios puede provocar que los dispositivos de ese usuario se muevan a un espacio diferente. Los cambios a un espacio diferente pueden resultar en cambios en las políticas y las configuraciones.

12.1.6.5. Delegar aplicaciones

La delegación de aplicaciones permite a un administrador global dividir y administrar independientemente aplicaciones en Ivanti Neurons for MDM. El administrador global puede obtener y distribuir de manera centralizada las aplicaciones públicas e internas a la vez que mantiene la separación y el control proporcionado por los espacios delegados.

Al distribuir de manera central una aplicación, el administrador global puede predefinir el comportamiento de la administración de la aplicación por medio de configuraciones de las aplicaciones, así como mediante las reglas de distribución de las aplicaciones. La aplicación puede delegarse y ponerse disponible en el App Catalog del espacio delegado.

De esta forma, la aplicación delegada se distribuye a los usuarios con dispositivos en un espacio delegado determinado. Cuando se delegan las aplicaciones, el acceso a estas puede asignarse a un subconjunto de administradores delegados, con lo que se distribuyen las responsabilidades de los administradores.

La delegación de una aplicación requiere que se definan, en primer lugar, uno o más espacios delegados. Cuando una aplicación se delega, se asignará a todos los espacios. El espacio de delegación de aplicaciones se clasifica en:

- Espacio predeterminado
- Espacios delegados

Añadir una aplicación a un espacio delegado

Las aplicaciones pueden ser añadidas a un espacio delegado por un administrador delegado o global. La aplicación aparecerá solo en el App Catalog de los espacios delegados a los que se haya añadido. Si añade una aplicación previamente delegada desde el espacio predeterminado a un espacio delegado, esto generará un error. En este caso, la herencia de la aplicación deberá desactivarse primero en el espacio predeterminado para que pueda añadirse a un espacio delegado. Para obtener más información, consulte **Añadir una configuración** en Trabajar con configuraciones.

Distribución de la aplicación en un espacio delegado

Cuando se delega una aplicación desde el espacio predeterminado, se heredan sus reglas de distribución. Esta aplicación se distribuirá a todos los dispositivos asignados al espacio delegado que cumplan las reglas de distribución de la aplicación.

Los administradores globales pueden delegar en los administradores de espacio la edición del Certificado de identidad generado dinámicamente para todos los dispositivos y para la opción de distribución personalizada.

> Los cambios en la distribución son aplicables sólo al espacio específico. Todos los demás espacios siguen heredando la configuración de distribución espacial predeterminada.

> Ajustes de aprobación de aplicaciones para aplicaciones Android: no se admite la configuración de aprobación de aplicaciones por espacio para aplicaciones de Android. Las aplicaciones aprobadas en el espacio personalizado surten efecto en todos los espacios.

> Aplicaciones de catálogo Android existentes: en los abonados en los que ya se han añadido aplicaciones públicas de Android en el espacio predeterminado, las aplicaciones deben anularse para que esa aplicación pública pueda añadirse en otro espacio no predeterminado.

Las aplicaciones de Android Enterprise solo pueden ser agregadas por el administrador a nivel de entorno, y **no** por el administrador a nivel de espacio. Google Play administrado se configura a nivel de organización, no por espacio delegado. Como resultado, las nuevas aplicaciones de Android Enterprise solo se pueden aprobar en el espacio predeterminado. Los administradores delegados pueden asignar y administrar aplicaciones ya aprobadas dentro de sus propios espacios, pero no pueden aprobar ni agregar nuevas aplicaciones de Android Enterprise desde Espacios delegados. Todas las aplicaciones nuevas deben aprobarse primero en el Espacio predeterminado y solo entonces se pueden asignar a los grupos adecuados.

Para obtener más información, consulte **Añadir una configuración** en Trabajar con configuraciones.

12.1.7. Administradores de asistencia técnica

Cree un administrador de asistencia técnica temporal para permitir que el equipo de asistencia técnica del servicio inicie sesión con sus funciones y permisos. Este usuario caduca automáticamente en siete días o bien puede finalizar el acceso en cualquier momento. Si crea un administrador de asistencia técnica, será más fácil para el equipo de asistencia técnica a solucionar problemas

Crear un administrador de asistencia técnica

Procedimiento

1. En la página **Administradores de asistencia técnica**, haga clic en **Añadir usuarios de asistencia técnica**.
2. Haga clic en **Crear usuario** para confirmarlo.

Este paso envía un correo electrónico al equipo de asistencia técnica del servicio de administración de dispositivos.

> El campo **Nombre en pantalla** se mostrará como "(disabled)" (deshabilitado) hasta que un miembro del equipo de asistencia técnica active la cuenta nueva. El nombre en pantalla resultante tendrá el siguiente formato:

asistencia-[ID_aleatoria]-[su_nombredeusuario]@[su_empresa].com

Una vez que haya creado un administrador de asistencia técnica, al seleccionar **Administrador > Administradores de asistencia técnica** irá directamente a la lista de administradores de asistencia técnica existentes. Por lo tanto, si necesita crear usuarios de asistencia técnica adicionales, vaya directamente al paso 2.

> Las cuentas de administrador de soporte recién creadas tienen acceso de solo lectura de forma predeterminada. Los roles personalizados no se asignan automáticamente, lo que reduce el riesgo de realizar cambios de configuración no deseados. Un administrador puede añadir roles y permisos posteriormente según sea necesario.

Ver el historial del usuario

En la página **Administradores de asistencia técnica**, haga clic en **Historial del usuario** para ver el historial de inicio de sesión de los administradores de asistencia técnica. La disponibilidad de los datos del historial de inicio de sesión de la página de Administradores de asistencia técnica está restringida a los datos de los últimos 90 días.

Finalizar el acceso de un administrador de asistencia técnica

Procedimiento

1. En la página **Administradores de asistencia técnica**, haga clic en el vínculo **Eliminar** que hay a la derecha de la cuenta que desea eliminar.
2. Cuando se le solicite, haga clic en **eliminar usuario** para confirmarlo.

Suspender el acceso de un administrador de asistencia técnica

En la página **Administradores de asistencia técnica**, haga clic en el vínculo **Desactivar** que hay a la derecha de la cuenta que desea suspender.

12.1.8. Administrador > Notificación de uso del sistema

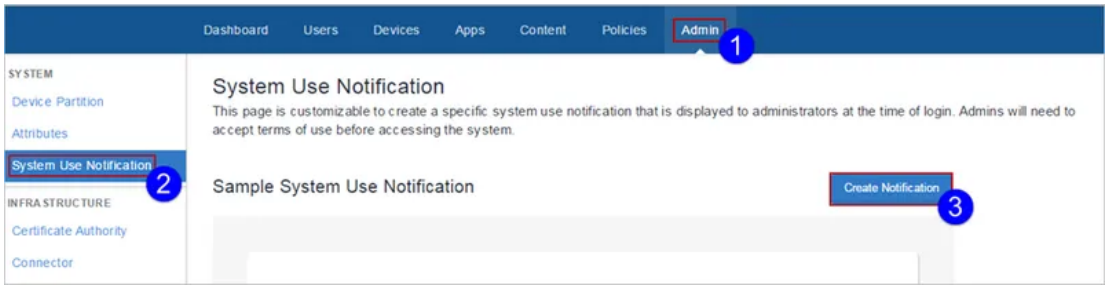
Licencia: Silver

Utilice la característica Notificación de uso del sistema para crear una notificación de uso del sistema personalizada que aparezca cuando el administrador inicie sesión y requiera que este acepte los términos de uso antes de acceder al sistema.

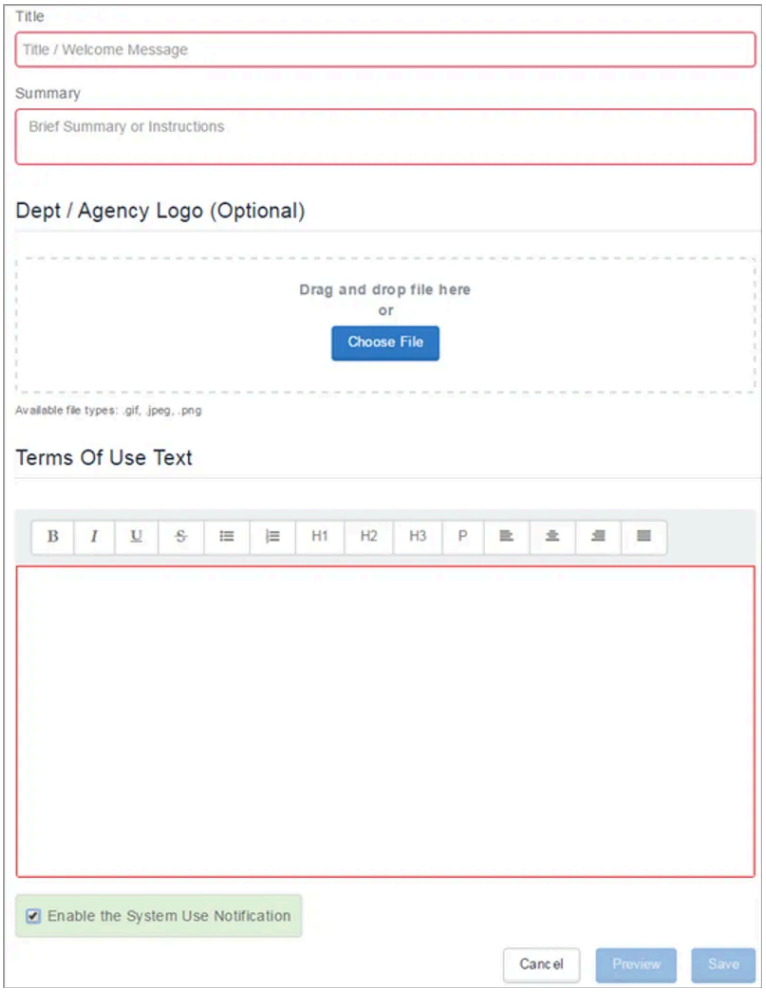
Crear una notificación de uso del sistema

Procedimiento

1. Seleccione **Administrador > Notificación de uso del sistema**.
2. Haga clic en **Crear notificación**.



Aparecerá la página Detalles de notificación de uso del sistema.



Introduzca un título en el campo **Título**.

4. Intorduzca un resumen o instrucciones en el campo **Resumen**.
5. Elija un logotipo si lo desea.
6. Introsduzca el texto de las condiciones de uso en el campo **Texto de las condiciones de uso**. Este es el texto que el administrador tendrá que aceptar al iniciar sesión.
7. Marque la casilla de verificación **Habilitar la notificación de uso del sistema** para activar la notificación.
8. Haga clic en **Vista previa** para invocar una vista previa de la notificación de uso del sistema.
9. Haga clic en **Guardar** cuando esté satisfecho con la notificación de uso del sistema.

12.2. Infraestructura

Esta sección contiene los siguientes temas:

- Acceso
- Listas de aplicaciones (plists)
- Exportar trazas de auditorías
- Gestión de certificados
- Configuración de SCEP para Entidades de Certificación externas
- Proveedores de credenciales derivadas
- Conector
- Uso del comando httpproxy para Conector
- Help@Work
- Identidad de la infrastructura
- Configuración del servidor LDAP
- Sentry
- Activación de la autenticación de Kerberos entre Ivanti Neurons for MDM y el servidor SCEP

12.2.1. Acceso

Aplicable a: dispositivos iOS y Android.

Acceda de forma segura a los datos corporativos a la vez que hace posible una experiencia del usuario fluida y productiva en cualquier dispositivo o aplicación. Además, Access instaura un límite de datos que evita que los usuarios puedan acceder a los servicios corporativos en la nube en dispositivos, aplicaciones o servicios en la nube no segurizados.

Documentación más reciente

Visite la **Documentación del producto** y haga clic en Access para obtener más información sobre Access y cómo configurarlo. Seleccione el documento apropiado para su versión de Access.

12.2.2. Listas de aplicaciones (plists)

Licencia: Silver

Puede crear listas de aplicaciones obligatorias, en la lista de permitidos y en la lista de bloqueados para usarlas con la **política de aplicaciones permitidas**, donde podrá usar estas listas para especificar medidas que se aplicarán si las aplicaciones instaladas de un dispositivo no cumplen los requisitos indicados en las listas de aplicaciones. No se pueden editar las listas de aplicaciones una vez creadas porque se puede remitir a estas listas de aplicaciones en las **políticas de aplicaciones permitidas**. Del mismo modo, no se pueden eliminar listas de aplicaciones a las que se haya remitido desde las políticas de aplicaciones permitidas.

Crear lista de aplicaciones

Procedimiento

1. Haga clic en **Administración > Infraestructura > Listas de aplicaciones**.
2. Haga clic en **Crear nueva lista**.
3. En el cuadro **Nombre de la lista de aplicaciones**, introduzca un nombre para la lista.
4. Seleccione el tipo de lista, **Lista blanca**, **Lista negra** u **Obligatorio**.
5. En la sección **Agregar aplicaciones**, seleccione el tipo de aplicación, **App Store**, **OS X store**, **Google Play** o **Catálogo de aplicaciones**.
6. Introduzca los criterios de búsqueda para limitar sus opciones.
7. Utilice las casillas para seleccionar las aplicaciones. Puede utilizar búsquedas múltiples y habilitar más de una casilla.
8. Haga clic en la pestaña **Ver aplicaciones** para ver la lista de aplicaciones que ha seleccionado hasta el momento.
   Haga clic en **Guardar**.

Ahora ya puede usar esta lista cuando configure la política de **Aplicaciones permitidas**.

Si no puede ver la página **Lista de aplicaciones**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración del sistema
- Sistema de solo lectura

12.2.3. Exportar trazas de auditorías

Exportar Audit Trails es una característica que se usa para exportar y cargar toda la información sobre Audit Trails a un servidor específico. El servidor debe ser accesible desde el puerto predeterminado. Los usuarios pueden configurar los ajustes de esta opción para que las trazas de auditorías se suban diariamente, de forma automática, a una ubicación específica.

> La exportación de Audit Trails es compatible con los servidores SFTP basados en Linux y en Windows.

Para configurar los ajustes de la exportación de trazas de auditorías:

1. Seleccione **Administrador > Infraestructura > trazas de auditorías**. Aparecerá la página **Trazas de auditorías**.
2. En la página **Trazas de auditorías**, haga clic en **ACTIVAR** para activar la exportación de trazas de auditorías.
3. En la sección **Exportar**, actualice los siguientes campos:

Característica	Descripción
Formato de exportación	Seleccione cualquiera de los siguientes formatos en los que desee exportar los datos de las trazas de auditorías: • **JSON** • **CEF** (formato de evento común) El mensaje del registro CEF contiene los siguientes valores predeterminados: ◦ Versión: número de versión del formato CEF. v25 es la versión actual compatible. ◦ Proveedor del dispositivo: Ivanti Inc ◦ Producto del dispositivo: Ivanti Neurons for MDM ◦ Versión del dispositivo: última versión de Ivanti Neurons for MDM al momento de generar el evento. ◦ Id. de clase de evento del dispositivo: Id. única de la entidad por traza ◦ Nombre: nombre de la entidad y acción por traza. Ejemplo: ajustes de la configuración de distribución de promociones, Crear. ◦ Severidad: indica la importancia del evento. Ejemplo: baja. El mensaje del registro CEF también contiene los campos de la extensión, que son una recopilación de los siguientes pares de valores de clave: ◦ CS1 y etiqueta CS1: metadatos de trazas de auditorías tales como creadoEn, TipoDeEntidad, NombreDeEntidad y TipoDeAcción ◦ CS2 y etiqueta CS2: información de los participantes. ◦ CS3 y etiqueta CS3: estado previo a la acción. ◦ CS4 y etiqueta CS4: estado posterior a la acción. En la exportación de CEF, si alguno de los campos (por ejemplo, claves CS3 o CS4) exceden los límites especificados, el valor actual se reemplaza por el texto "El valor de esta clave excede la longitud permitida para la clave de diccionario asignada".
Servidor	Introduzca el nombre del servidor al que se van a exportar las trazas de auditorías.
Usuario	Introduzca el nombre de usuario para iniciar sesión en el servidor.
Contraseña **Ruta del servidor**	Introduzca la contraseña de inicio de sesión del servidor. Introduzca la ruta del servidor. Asegúrese de que la ruta proporcionada existe en el servidor. Ejemplo: /Usuarios/Prueba/Exportación.
Algoritmo de intercambio de claves	Seleccione la lista de algoritmos de intercambio de claves para exportar las trazas de auditorías para la configuración de SFTP de salida. Los siguientes algoritmos de intercambio de claves están seleccionados por defecto: • **diffie-hellman-group-exchange-sha1** • **diffie-hellman-group14-sha1** • **curve25519-sha256** • **diffie-hellman-group-exchange-sha256** (seleccionado por defecto)

Característica	Descripción
Cifrados	Seleccione la lista de cifrados de encriptación para exportar el registro de auditorías para la configuración de SFTP de salida. Los siguientes cifrados de cifrado están seleccionados por defecto: • **aes128-ctr** • **aes192-ctr** • **aes256-ctr** (seleccionado por defecto)
HMAC	Seleccione la lista de algoritmos de HMAC para exportar las trazas de auditorías para la configuración de SFTP de salida. • **hmac-sha1 (seleccionado por defecto)** • **hmac-sha2-256** • **hmac-sha2-512**

los campos mencionados anteriormente serán de solo lectura si ya se han configurado. Para editar los campos ya configurados deberá hacer clic en el botón **Editar**. Si el administrador ya había configurado la exportación a SFTP, después de la actualización se seleccionarán todos los Algoritmos de claves.

Haga clic en **Probar conexión y continuar** para probar la conexión del servidor y guardar la configuración de las exportaciones de las trazas de auditorías.

Los archivos de las trazas de auditorías guardados están disponibles en formato JSON en un archivo .zip.

Verifique los ajustes de configuración en todos los campos antes de guardar los ajustes de exportación de las Trazas de auditoría. Si alguno de los valores de campo introducidos no es válido, aparecerá un mensaje de error.

Habilitar pistas de auditoría para la inscripción y cancelación de la inscripción del dispositivo en Spaces

Cuando se habilita, el movimiento del dispositivo entre espacios se registra en la auditoría, incluidos los eventos desencadenados por el registro del dispositivo, la eliminación del dispositivo y la actualización o eliminación del espacio. Los administradores de espacio pueden identificar los dispositivos afectados, filtrar registros por espacio y tipo de actividad y exportar registros de auditoría a CSV.

12.2.4. Gestión de certificados

Licencia: Silver

Usar la autenticación de certificados es una forma efectiva de asegurar sus dispositivos móviles. Los certificados son más seguros que las contraseñas y, además, le permiten utilizar una sola credencial para proteger las VPN, redes inalámbricas, correo electrónico, etc. Si su organización tiene acceso a una entidad de certificación externa, puede utilizar un Conector para acceder a ella. Si su organización no tiene acceso a una entidad de certificación, puede utilizar Ivanti Neurons for MDM como entidad de certificación. También puede utilizarla como entidad de certificación intermediaria para otras entidades de certificación. Los certificados generados por Ivanti Neurons for MDM se denominan certificados de autofirmados.

- Los certificados SHA1 se dejan de utilizar mientras se crean los certificados de identidad. Puede elegir otros algoritmos. Si los certificados anteriores usaban SHA-1, puede usarse el mismo algoritmo SHA-1 mientras se actualizan los certificados. Si los certificados anteriores usaban un algoritmo posterior a SHA-1, no está permitido cambiar a SHA-1.
- Durante la configuración de la entidad de certificación local o externa, seleccione la opción **Identidades del caché en** Ivanti Neurons for MDM para almacenar los certificados con el servicio de Ivanti Neurons for MDM. Borre el caché para generar los certificados, según sea necesario.
- Los certificados se reemitirán implícitamente.
- Para lograr un sistema más eficiente, los certificados de las configuraciones creadas por un administrador se generan sin conexión, usando una cola FIFO. Durante el período en que las configuraciones se están generando sin conexión, el estado de la configuración será **Generación de certificados pendiente** en la columna **Estado**, en la pestaña **Configuraciones** de la página **Detalles del dispositivo**. Tras generar los certificados, las configuraciones se cambian al estado **Instalación pendiente** y se insertan, junto con los certificados, en los dispositivos a través de ingresos forzados automáticos.
- Todos los certificados de la Entidad de certificación, incluido el certificado firmado por las Entidades de Certificación externas DigiCert PKI Platform o GlobalSign, se revocan cuando se retira o borra un dispositivo y cuando los certificados se regeneran.

Como administrador, puede generar certificados Ivanti Neurons for MDM para un inicio de sesión con tarjeta inteligente y para Id. de objetos del cliente (OID). Puede generar certificados para las siguientes opciones de autenticación:

  - Autenticación de cliente - habilitada de modo predeterminado.
  - IPSEC - opcional, el administrador puede habilitarlo.
  - Inicio de sesión con tarjeta inteligente - opcional, el administrador puede habilitarlo.
  - OID personalizados - opcional, el administrador puede habilitarlos.

> Esta función sólo es aplicable a las siguientes autoridades de certificación:

    - Entidad de Certificación local
    - Entidad de certificación intermedia
    - Entidad de certificación externa: configure las políticas de aplicación de la plantilla de CA en el servidor NDES para que admita IPSEC, Inicio de sesión con tarjeta inteligente y OID personalizados.

> En los modos Administración de dispositivos, Estación de aplicaciones u otros modos de empresa que no sean Android, la gestión de certificados no es compatible con los dispositivos Samsung que utilizan las API de Samsung. Se recomienda verificar la transición a Android Keystore basándose en la recomendación de Samsung.

Para obtener más información, consulte **Configuración del certificado**.

Conectarse a una autoridad de certificación distinta a SCEP local.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Instale y configure un Conector (**Administrador > Conector**). Para obtener más información, consulte **Conector**.
3. Vaya a **Administración** > **Infraestructura** > **Administración de certificados**.
4. Haga clic en **Agregar** en la sección **Entidad de certificación**.
5. Seleccione **Agregar una autoridad de certificación de SCEP local** y haga clic en **Continuar:**
6. Introduzca un nombre que identifique la configuración.
7. Seleccione uno de los siguientes tipos de Entidad de Certificación:
   - Microsoft
   - EJBCA
   - Servidor SCEP genérico
     La opción del servidor SCEP genérico puede usarse con la mayoría de los servidores SCEP que tengan una contraseña estática de comprobación.

Complete el formulario que aparece.

9. Haga clic en **Hecho**.

Crear una entidad de certificación externa

Elija esta opción si desea emplear una Entidad de Certificación de terceros.

Procedimiento

1. En la página **Administración de certificados**, haga clic en **Añadir** en la sección **Entidad de Certificación**.
2. En la página Añadir entidad de certificación, en Crear una Entidad de Certificación externa, haga clic en **Continuar**.
3. Seleccione la plataforma GlobalSign o DigiCert PKI como entidad de certificación externa.
4. Complete los campos restantes del formulario que aparece.
5. Haga clic en **Hecho**.

Ver un certificado de la entidad de certificación externa

Puede ver los detalles de un certificado y cargar el certificado raíz intermedio/alternativo para que esta entidad de certificación sustituya la copia almacenada existente.

Procedimiento

1. En **Entidad de Certificación** en la página **Administración de certificados**, haga clic en **Acciones** junto a la entidad de certificación externa y, a continuación, haga clic en **Ver certificado**. Aparecerá la ventana **Ver certificado**.
2. En la ventana **Ver certificado**, haga clic en **Cargar certificado**. Aparecerá la ventana **Cargar certificado: EC externa**.
3. Haga clic en **Elegir archivo** para seleccionar el certificado que se va a cargar.
4. Haga clic en **Hecho**.

Crear una Entidad de Certificación intermedia

- Si necesita un certificado, genere una CSR y envíesela a la entidad firmante. Una vez que reciba el certificado de la entidad firmante, cárguelo.
- Si ya tiene el certificado necesario, cárguelo.

Generar una CSR (solicitud de firma del certificado)

Procedimiento

1. En la sección **Entidad de Certificación** que hay en la página **Administración de certificados**, haga clic en **Añadir**.
2. En la sección Añadir entidad de certificación, en Crear una Entidad de Certificación intermedia, haga clic en **Generar CRS**.
3. Complete el formulario que aparece.
4. Haga clic en **Generar**.
5. Copie el contenido que hay entre COMENZAR SOLICITUD DE CERTIFICADO y FINALIZAR SOLICITUD DE CERTIFICADO en un archivo de texto.
6. Cargue el archivo de texto a la entidad de certificación.
7. Haga clic en **Hecho**.

Cargar el certificado firmado

Una vez que reciba el certificado firmado de la entidad de certificación, puede cargarlo.

Procedimiento

1. En la sección **Entidad de Certificación** de la página **Administración de certificados**, encuentre la entrada de la CSR que ha generado.
2. En esa sección, seleccione **Acciones > Cargar nuevo certificado firmado**.
3. Haga clic en **Elegir archivo**.
4. Seleccione el nuevo certificado firmado.
5. Haga clic en **Hecho**.

Cargar un certificado existente

Este tema describe cómo cargar un certificado firmado.

Procedimiento

1. En la sección **Entidad de Certificación** que hay en la página **Administración de certificados**, haga clic en **Añadir**.
2. En la sección Añadir entidad de certificación, en Crear una Entidad de Certificación intermedia, haga clic en **Cargar identidad existente**.
3. En el campo **Nombre**, introduzca un nombre para este certificado que sea diferente a los demás.
4. Haga clic en **Cargar**.
5. Seleccione el certificado.
6. Introduzca la contraseña para el certificado.
7. Haga clic en **Cargar**.

Ver un certificado de la entidad de certificación intermedia

Puede ver los detalles de un certificado y obtener la URL de la CRL (lista de revocación de certificados) de la entidad de certificación.

Procedimiento

1. En la sección **Entidad de Certificación**, haga clic en **Acciones** junto a la entidad de certificación y, a continuación, haga clic en **Ver certificado**. Aparecerá la ventana **Ver certificado**.
2. En la ventana **Ver certificado**, puede ver la URL en el campo **URL de CRL**.
3. Haga clic en **Copiar** para copiar esa URL en un portapapeles y pegarla en otra aplicación. Esta URL se puede usar para configurar Office 365 de modo que acepte certificados emitidos por la entidad de certificación.

Crear una Entidad de Certificación independiente

Elija esta opción si quiere crear una Entidad de certificación nueva y completamente independiente (local y autofirmada).

Procedimiento

1. En la sección **Entidad de Certificación** que hay en la página **Administración de certificados**, haga clic en **Añadir**.
2. En la página Añadir Entidad de Certificación, en Crear una Entidad de Certificación independiente, haga clic en **Continuar**.
3. Complete el formulario que aparece.
4. Haga clic en **Generar**.

Notificación de caducidad de la autoridad de certificados independiente

La información de caducidad de la autoridad de certificación independiente (local) ahora es visible como información sobre herramientas en la sección **¿CIRCUACIÓN?FECHA** ?si la fecha de caducidad del certificado es inferior a 30 días.

Si la fecha de caducidad es inferior a 365 días, además de la notificación enviada, esta información se puede ver en **Dashboards** >? **Notificaciones**. Seleccione **Caducidad** como filtro.

Configuración del periodo de validez del certificado emitido por la entidad de certificación independiente

Puede configurar el período de caducidad de la entidad de certificación (local) independiente.

Procedimiento

1. En la sección **Entidad de Certificación** en la página **Administración de certificados**, haga clic en **Acciones** junto a la entidad de certificación independiente.
2. Haga clic en **Editar**.
   Aparecerá la ventana **Editar entidad de certificación**.
3. En la sección Plantilla de certificado de cliente, en el campo **Vida útil del certificado**, introduzca el nuevo período de caducidad en días.
4. Haga clic en **Guardar**.

Puede recibir notificaciones y correos electrónicos (si está habilitado opcionalmente) cuando los certificados emitidos por una autoridad de certificación local estén a punto de caducar o ya hayan caducado.

- Notificación en los días de caducidad del certificado: las notificaciones se generan a intervalos predeterminados durante un margen de caducidad del certificado. La primera notificación se produce 365 días antes de la caducidad, seguida de notificaciones adicionales que ocurren 180 días, 60 días, 45 días y 7 días antes de la caducidad. Recibirá esta notificación hasta

que reemplace el certificado yendo a **Administrador > Administración de certificados > Acciones > Cargar nuevo certificado firmado**.

- Notificación en el certificado caducado - Usted recibe una notificación cuando el certificado caduca. Tendrá que reemplazar el certificado para reanudar el servicio normal.
- Notificación cuando se carga un nuevo certificado válido: la notificación se enviará cuando se cargue el nuevo certificado firmado.

Ver un certificado de la entidad de certificación independiente

Puede ver los detalles de un certificado y obtener la URL de la CRL (lista de revocación de certificados) de la entidad de certificación local.

Procedimiento

1. En la sección **Entidad de certificación**, en la página **Administración de certificados**, haga clic en **Acciones** junto a la entidad de certificación local y haga clic en **Ver certificado**. Aparecerá la ventana **Ver certificado**.
2. En la ventana **Ver certificado**, puede ver la URL en el campo **URL de CRL**.
3. Haga clic en **Copiar** para copiar esa URL en un portapapeles y pegarla en otra aplicación. Esta URL se puede usar para configurar Office 365 de modo que acepte certificados emitidos por la entidad de certificación local.

Visualización de la vida útil de una CRL de una entidad de certificación

Puede ver y editar la vida útil de la CRL de una entidad de certificación local o intermedia.

Procedimiento

1. En la sección **Entidad de certificación**, en la página **Administración de certificados**, haga clic en **Acciones** junto a la entidad de certificación local y haga clic en **Editar**. Aparecerá la ventana **Editar entidad de certificación**.
2. En la ventana **Editar entidad del certificado**, puede ver el valor de vida de la CRL. El valor predeterminado mínimo es de 24 horas. El valor máximo que se puede introducir es 10 950 horas.
3. Edite el valor del ciclo de vida de la CRL y haga clic en **Guardar**.

Crear una Entidad de Certificación en la nube

Elija esta opción si desea emplear una Entidad de Certificación en Cloud.

Procedimiento

1. Vaya a **Administración** > **Infraestructura** > **Administración de certificados**.
2. En la página **Gestión de certificados**, que hay en la página **Autoridad de certificación**, haga clic en **Agregar**.
3. En la página **Agregar autoridad de certificación**, que hay en **Conectar a una Autoridad de certificación de confianza pública en la nube**, haga clic en **Continuar**.
4. Introduzca un nombre en la casilla **Nombre**.
5. Seleccione la Autoridad de certificación en la nube de las siguientes opciones:
    - **Atos IDnomic CMS**
    - **Plataforma DigiCert One PKI**
    - **Plataforma DigiCert PKI**

- **Confiar**
- **GlobalSign**

6. Introduzca la URL básica y cargue los datos del certificado.
7. Haga clic en **Hecho**.

Uso de la búsqueda avanzada en los certificados

Puede utilizar la opción de Búsqueda avanzada para buscar certificados emitidos en función de reglas para identificar y ver los certificados con criterios específicos. Estas reglas se pueden crear usando los operadores correspondientes, como «comienza con», «termina con», «contiene», «no contiene», «no comienza con», «no termina con», «es menor que», «es mayor que», «está en el intervalo», «es igual a» y «no es igual a». Las opciones de reglas se pueden anidar juntas utilizando las opciones CUALQUIERA (O) o TODOS (Y). Los certificados emitidos que coincidan con las reglas se mostrarán debajo de la sección. A partir de Ivanti Neurons for MDM versión 76, los operadores de todas las plantillas de administración de certificados tienen operadores estándar. Los operadores de las siguientes plantillas están estandarizados en esta versión:

- Administrador > Administración de certificados > Certificados emitidos > Búsqueda avanzada

Búsqueda avanzada en los certificados emitidos

Procedimiento

1. En la sección de **Certificados emitidos** de la página **Gestión de certificados**, haga clic en el enlace **Búsqueda avanzada**.
2. Haga clic en **Cualquiera** si los usuarios deben coincidir con al menos una de las reglas o en **Todas** si los certificados deben coincidir con todas las reglas.
3. Cree una regla que defina los criterios de búsqueda para los siguientes atributos:
   - **EC**
   - **Nombre de la configuración**
   - **Caducidad**1
   - **Es una clave privada**
   - **SO**
   - **Número de serie**
   - **Estado**
   - **Tipo de uso**
   - **Usuario**
4. (Opcional) Haga clic en + para crear reglas adicionales, si fuera necesario.
5. (Opcional) Haga clic en **Guardar** para guardar la consulta.
6. Haga clic en **Buscar**. En la página se muestran la lista de usuarios que coinciden con los criterios de búsqueda.

Búsqueda avanzada en los certificados proporcionados por el usuario

Procedimiento

1. En la sección **Certificados proporcionados por el usuario** de la página **Administración de certificados**, haga clic en el enlace **Búsqueda avanzada**.

2. Haga clic en **Cualquiera** si los usuarios deben coincidir con al menos una de las reglas o en **Todas** si los certificados deben coincidir con todas las reglas.
3. Cree una regla que defina los criterios de búsqueda para los siguientes atributos:
    - **Nombre del certificado**
    - **Fecha de caducidad**
    - **Emitido por**
    - **Cargado el**
4. (Opcional) Haga clic en + para crear reglas adicionales, si fuera necesario.
5. (Opcional) Haga clic en **Guardar** para guardar la consulta.
6. Haga clic en **Buscar**. En la página se muestran la lista de usuarios que coinciden con los criterios de búsqueda.

Cargando las consultas de búsqueda de los certificados emitidos

Para ver la lista de consultas de búsqueda guardadas.

Procedimiento

1. En la sección de **Certificados emitidos** de la página **Gestión de certificados**, haga clic en el enlace **Búsqueda avanzada**.
2. Haga clic en el icono «Carpeta». Aparecerá la ventana **Búsqueda avanzada**. La lista de las consultas de búsqueda creadas se muestra en la sección **Cargar consulta**. En esta sección se muestran los siguientes detalles:
    - **Nombre de la consulta**: el nombre de la consulta cargada.
    - **Contenido de la consulta** muestra el contenido de las reglas que definen la consulta de búsqueda.
    - **Acciones**: seleccione la acción que se realizará en la consulta.
3. Haga clic en **Cargar consulta** en la columna **Acciones** para ver la lista de certificados emitidos que coinciden con los criterios definidos en la consulta cargada.
   Para borrar una consulta cargada, haga clic en el icono «Borrar».

> Haga clic en **Exportar a CSV** para descargar el contenido del informe de los resultados de búsqueda en un archivo CSV para consultarlo o analizarlo posteriormente.

Ver el período de vencimiento de los certificados emitidos

En la sección **Certificados emitidos**, en la columna **Caduca (en días)** se pueden ver los días que faltan para que venza el certificado si la caducidad se produce dentro de los próximos 30 días. Si el certificado ya había caducado en los últimos 30 días, en la columna **Caduca (en días)** para el certificado se mostrará el número de días que han transcurrido desde la fecha de caducidad.

Para obtener más información, consulte Configuración de SCEP para entidades de certificación externas.

Exportar a CSV

Puede exportar los certificados a un archivo CSV para consultar más adelante o para realizar análisis.

Procedimiento

1. En la página **Administración de certificados**, vaya a una de las pestañas siguientes.
    - **Autoridad de certificados**

- **Certificados emitidos**
- **Certificados proporcionados por el usuario**

2. Haga clic en **Exportar a CSV**.
3. Haga clic en **Descargar**.
4. (Opcional) Haga clic en **Eliminar** para eliminar el informe.

12.2.5. Configuración de SCEP para Entidades de Certificación externas

Esta función permite la configuración de Simple Certificate Enrollment Protocol (SCEP) para autoridades de certificación externas para dispositivos Windows 10.

> La opción de delegación con distribución personalizada está disponible para esta configuración. Para obtener más información, consulte el tema *Distribuir la configuración* en **Trabajar con configuraciones**.

Configurar una Entidad de Certificación externa

Primero debe configurar una EC externa. Puede pasar a la siguiente sección si ya tiene una EC externa.

1. Vaya a **Administración > Infraestructura > Administración de certificados**.
2. Haga clic en **+Añadir**.
3. Introduzca un nombre para la Entidad de Certificación.
4. Use el menú desplegable para seleccionar Microsoft como el **Tipo de entidad de certificación**.
5. Introduzca la **URL de SCEP**.
6. Introduzca el **Nombre de usuario** y la **Contraseña**.
7. Introduzca la **URL de comprobación**.
8. Haga clic en **Guardar**.

Configuración SCEP

Ahora puede proceder con la configuración SCEP.

1. Vaya a **Configuración > +Añadir**.
2. Seleccione el icono de Windows.
3. Seleccione **Certificado de identidad** para ir a la página **Crear configuración del certificado de identidad**.
4. Introduzca un nombre para la configuración.
5. Seleccione **Configuración de Windows** de la lista de configuraciones SCEP del menú desplegable **Distribución de certificados**.
6. Seleccione la EC externa.
7. Introduzca los detalles de distribución de certificados.
    - Introduzca el asunto. Por ejemplo: CN=$
    - Seleccione el número de intentos en el menú desplegable **Reintento**.
    - Seleccione el número de segundos a esperar antes de cada entrada en el menú desplegable **Retraso en el reintento**.
    - Seleccione un tamaño de clave del menú desplegable **Longitud de clave**.
    - Seleccione al menos una opción de uso del certificado.
    - Introduzca el tiempo en el campo **Validez** y el menú desplegable.
    - Introduzca la Huella digital de la EC.

- Vaya a la URL de SCEP challenge, copie la huella CA y péguela aquí o haga clic en **Crear desde un certificado**... para cargar el certificado desde el que se puede crear la huella de CA.
  Seleccione al menos un algoritmo hash de las opciones **Familia de algoritmos hash**.

8. Haga clic en **Siguiente**.

12.2.6. Proveedores de credenciales derivadas

En la página de Proveedores de credenciales derivadas, puede ver la lista de proveedores de credenciales derivadas que se han utilizado para la distribución de certificados. Puede especificar qué proveedores de credenciales derivadas deben establecerse como predeterminados y también añadir otros proveedores de credenciales derivadas personalizadas que utilice.

Para establecer un proveedor de credenciales derivadas como predeterminado:

1. Vaya a **Administrador > Proveedores de credenciales derivadas**. Se enumerarán los siguientes proveedores de credenciales derivadas en la página.
    - **Confiar**
    - **Interceder**
    - **Pura raza**
2. Para configurar el proveedor que desea como predeterminado, haga clic en **Configurar como predeterminado** en la columna **Acciones.** Cuando se establece, el icono de marca de verificación aparece debajo de la columna **Proveedor predeterminado** para el proveedor, lo que indica que es el proveedor de credenciales predeterminado.

Para añadir un proveedor de credenciales derivadas personalizadas:

1. Vaya a **Administrador > Proveedores de credenciales derivadas**.
2. Haga clic en **+Añadir**.
3. Escriba el nombre del proveedor de credenciales derivadas en el campo de texto de la columna **Nombre** .
4. Haga clic en **Guardar**.
   Una vez añadido, este proveedor de credenciales derivadas personalizadas estará disponible como una opción que se puede seleccionar en el campo **Marca** mientras se configura la distribución de credenciales derivadas en la configuración del Certificado de identidad.

Haga clic en **Eliminar** en la columna **Acciones** para eliminar un proveedor de credenciales derivadas.

> No podrá eliminar el proveedor de credenciales derivadas si está establecido como predeterminado.

12.2.7. Conector

Licencia: Silver

El conector de Ivanti Neurons for MDM proporciona acceso desde su servicio de Ivanti Neurons for MDM a los recursos corporativos, como un servidor LDAP o una Entidad de certificación (EC). Configure un Conector por cada recurso al que desee acceder.

Si utiliza Microsoft Active Directory o un servidor LDAP alojado en Amazon Web Services (AWS), podrá alojar el conector de Ivanti Neurons for MDM en AWS. No es necesario un Conector local.

Conector se actualiza automáticamente a la última versión del software.

Para obtener la Guía de instalación del conector de Ivanti Neurons for MDM más reciente, visite **https://help.ivanti.com/#106** y busque "Conector".

Opciones de alojamiento del Conector

Puede alojar el conector de Ivanti Neurons for MDM de forma local su centro de datos o en Amazon Web Services (AWS):

- Aloje el Conector en AWS si está usando Microsoft Active Directory alojado en AWS o Microsoft Active Directory autoadministrado en AWS. En este caso, no necesitará tener un Conector local.
- Para acceder a los recursos locales, como un servidor LDAP o una EC, establezca el Conector de forma local.

Alojar el Conector en AWS

Los clientes pueden alojar Conector en AWS para usarlo con las siguientes opciones de Microsoft Active Directory alojadas en AWS:

- Servicio del directorio de AWS para Microsoft Active Directory
- Microsoft Active Directory administrado por el cliente en el PCV de Amazon

Para ver más información sobre el Servicio de directorio de AWS para Microsoft Active Directory, consulte **https://aws.amazon.com/directoryservice**. Consulte la documentación de AWS sobre cómo alojar Microsoft Windows Server y Active Directory en un PCV de Amazon. El conector de Ivanti Neurons for MDM es compatible con Windows Server 2012, 2012 R2, 2015.

Ajuste del AMI del conector MDM de Ivanti Neurons for MDM en AWS

Para ajustar el AMI del conector de Ivanti Neurons for MDM:

1. Inicie sesión en AWS con las credenciales de administrador.
2. En la página de servicios de AWS, seleccione **EC2** en **Compute**.
3. Expanda **Imágenes** y seleccione **AMI** en el panel izquierdo.
4. Seleccione **Imágenes públicas** del menú desplegable en el panel derecho.
5. Busca el Conector de Ivanti Neurons for MDM mediante palabras clave como "mobileiron-kocab".
6. Selecciona la última versión del Conector de la lista y haga clic en **Iniciar**.
7. Siga las instrucciones para instalar el Conector en la sección, "Desplegar el conector de Ivanti Neurons for MDM en AWS" de la *Guía de instalación del conector de Ivanti Neurons for MDM* disponible en https://help.ivanti.com/mi/help/en_us/cld/*<version>*/inst/default.htm, donde *version* es la versión del Conector de Ivanti Neurons

for MDM que vaya a instalar. Por ejemplo, para la versión 74 del conector de Ivanti Neurons for MDM, la guía está disponible en https://help.ivanti.com/mi/help/en_us/cld/**74**/inst/default.htm.

Alojar el Conector de forma local

Para alojar un conector de Ivanti Neurons for MDM en las instalaciones de su centro de datos, haga clic en **Descargar conector** para descargar e instalar el conector de Ivanti Neurons for MDM. Extraiga el contenido del paquete descargado y siga las instrucciones de configuración de la Guía de instalación del conector de Ivanti Neurons for MDM que se incluye en el paquete.

Acceder a los registros del Conector

Puede acceder a los registros del Conector desde el servicio de Conector para ayudarle a solucionar problemas relacionados con el Conector. Debe tener la función de Administrador del sistema o Solo lectura del sistema.

1. Vaya a **Administrador > Conector** para ver la página del Conector.
   La interfaz del Connector muestra el estado del Conector (Activado o Desactivado), el Nombre del conector, la Conexión (Conectado o No conectada), Número de versión, Nivel de registro, Acciones (Desactivar o Eliminar el Conector).
2. Use el menú desplegable **Nivel de registro** para elegir un nivel.
   Los niveles de registro disponibles aparecen en el menú desplegable ordenados desde el nivel de registro más inferior hasta el más elevado:
   - Error
   - Advertencia
   - Información
   - Depurar
   - Rastrear

El nivel de información es el ajuste del nivel de registro predeterminado. Si elige otro nivel de registro, aparecerá un icono giratorio de sincronización que indicará que se está obteniendo información en el nivel de registro que ha seleccionado. El nivel de registro se restablecerá en el nivel de información después de una hora. El nivel de seguimiento es el ajuste del nivel de registro más elevado. Utilice este nivel para recopilar todos los mensajes en todos los demás niveles. El icono de sincronización se muestra durante toda la duración de la solicitud.

3. Si fuera necesario, mantenga el puntero sobre el icono Sincronizar para ver el icono Cancelar. Haga clic en el icono Cancelar para cancelar el cambio de nivel de registro.
4. Mantenga el puntero sobre el icono Solicitar para ver la información de la solicitud. Haga clic en el icono Solicitar para solicitar los archivos de la carpeta del registro actual en un archivo .zip.
   Los archivos del registro se añadirán a un archivo .zip cuando se haga una solicitud. Cuando se hace una solicitud, el archivo .zip de la solicitud anterior se elimina.
5. Si fuera necesario, mantenga el puntero sobre el icono Solicitar y se convertirá en el icono Cancelar. Haga clic en el icono Cancelar para detener la solicitud.
   Cuando se cancela una solicitud antes de completarse, el icono Descargar no se mostrará debido a que el archivo de registro .zip anterior se eliminó del servidor. Los archivos de registro originales del Conector siguen estando disponibles para la solicitud.
6. Haga clic en el icono Descargar cuando la solicitud se haya completado para descargar el archivo de registro .zip que contiene los archivos de registro obtenidos durante la última solicitud.
   El nombre del archivo de registro tendrá el siguiente formato: kocab.log. El nombre del archivo zip que se descarga consta del nombre del servidor, la versión de conexión y una marca de tiempo que incluye el día, el mes, el año y la hora del día en el

formato: <Connector_Hostname><Connector_Version>_<TimeStamp>.zip. El nombre del archivo de registro archivado está en el siguiente formato: kocab.aaaa-mm-dd.0.log.gz.

7. Opcionalmente, también puede usar el menú desplegable **Acciones** para Desactivar o Eliminar el Conector.

Si no puede ver la página **Conector**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración del sistema
- Sistema de solo lectura

Para obtener más información, consulte **Usar el comando httproxy para el Conector**.

12.2.8. Uso del comando httpproxy para Conector

Un nuevo comando shell klish se creó para ayudar a editar la configuración de Conector para su instalación de Ivanti Neurons for MDM. Use este comando para cambiar la información de contacto y otros parámetros para configurar el conector.

Ahora, el comando httpproxy está disponible en esta versión con estos requisitos.

- klish shell

Para configurar su conector:

1. Inicie sesión en klish shell.
2. Introduzca un ? para obtener una lista de comandos shell klish disponibles.
3. Introduzca **httpproxy** para mostrar el valor actual de estos parámetros:
    1. habilitado
    2. esquema
    3. servidor
    4. tipo de autenticación
    5. nombre de usuario
    6. contraseña
4. Introduzca **httpproxy ?** para ver un listado de los comandos disponibles para usar con httpproxy.
    1. authtype - Establecer el tipo de autenticación del proxy http en NONE, BASIC o NTLM
    2. disable - Desactivar el proxy http
    3. enable - Activar el proxy http
    4. host - Establecer el host del proxy http; debe ser un FQDN o una IP, ya sea http o https
    5. password - Establecer la contraseña de autenticación del proxy http
    6. port - Establecer el puerto del proxy http
    7. scheme - Establecer el esquema del proxy http, debe ser http o https
    8. show - Mostrar los ajustes actuales del proxy http
    9. username - Establecer el nombre de usuario de autenticación del proxy http
5. Use los comandos indicados más arriba para configurar su conector.

12.2.9. Help@Work

Licencia: Platinum

Compatible con: dispositivos Android y iOS compatibles con Ivanti Neurons for MDM

Utilice Help@Work para Android/iOS para proporcionar asistencia remota a los usuarios de los dispositivos Android y iOS. Help@Work para Android/iOS se basa en la aplicación TeamViewer QuickSupport. Necesitará una cuenta de TeamViewer para usar Help@Work para Android/iOS. Si no tiene ya una cuenta, visite teamviewer.com para obtener más detalles.

Help@Work transforma la experiencia de soporte técnico para los dispositivos iOS 11.0+ y Android permitiendo que los usuarios pidan ayuda con un solo clic y compartan su pantalla con un representante del soporte técnico. Los usuarios ya no tienen que perder tiempo explicando verbalmente el problema, mientras que el personal informático puede trabajar de forma más eficiente a la hora de solucionar problemas con un dispositivo. Esto no es compatible con los dispositivos iOS «MAM only».

> TeamViewer es compatible con los dispositivos de Propietario del dispositivo Android en modo Kiosco.

> Los comandos de inicio de TeamViewer dejan de existir si se sale de la aplicación o el dispositivo se reinicia.

> En los dispositivos Android, si la aplicación Teamviewer QuickSupport no está instalada, se le pedirá al usuario que descargue la aplicación. En los dispositivos iOS, la aplicación se tiene que insertar mediante el App Catalog o, si ya está instalada en el dispositivo, se debe convertir en aplicación administrada.

> La aplicación Teamviewer QuickSupport debe estar en primer plano para que la sesión se aplique a la aplicación. Para el modo Sin atender es necesaria la aplicación del host de TeamViewer.

> La versión de la aplicación de escritorio que instala el administrador debe ser compatible con la versión de Quicksupport instalada en el dispositivo del cliente para admitir sesiones remotas.

Configurar Help@Work para Androido iOS

A continuación le indicamos los pasos para una única configuración para personalizar y distribuir Help@Work para Androido iOS:

1. Vaya a la pestaña **Administrador**.
2. En Infraestructura, haga clic en **Help@Work**.
3. **Help@Work** requiere TeamViewer. En la sección Activar TeamViewer, active la opción **TeamViewer asistido** o **TeamViewer sin atender (solo Android)** haciendo clic en el botón **Activar ahora**.
4. Revise el acuerdo de licencia de TeamViewer y haga clic en **Aceptar** para continuar. Su licencia corporativa ya está activada. De este modo, TeamViewer identifica los clientes de Ivanti para que su acceso esté garantizado.

> La opción **Eliminar activación** está disponible al activar el TeamViewer. Cuando hace clic en **Eliminar activación** bajo la sección **Activar TeamViewer**, aparece la ventana **Confirmar la eliminación de la activación** en la pantalla. Haga clic en **Eliminar activación** para eliminar la Activación de TeamViewer, que, a su vez, eliminará la función de Help@Work en todos los dispositivos compatibles. No obstante, puede activar TeamViewer mediante una cuenta existente o una cuenta distinta en una fase posterior.

> Si quiere eliminar la cuenta de **TeamViewer** en modo Desatendido, debe cancelar el aprovisionamiento de los dispositivos asociados para los que está activado el modo Desatendido. Para desaprovisionar los dispositivos asociados, debe deshacer la distribución de la aplicación **TeamViewer** desde los dispositivos asociados y forzar una conexión. Asegúrese de que la aplicación TeamViewer se elimina de todos los dispositivos y, a continuación, elimine le unión de cuentas desde la consola del administrador.

Distribuya la aplicación TeamViewer entre los usuarios que desee utilizando el flujo de trabajo estándar de la aplicación para iniciar las sesiones remotas. Esto es específico para los modos **Atendido** y **Sin atender**. Si el administrador quiere controlar el dispositivo, el complemento universal o el complemento específico por modelo/OEM de TeamViewer se debe distribuir también en los dipositivos. Consulte Configuración de la aplicación para ver las instrucciones.

Iniciar una sesión remota utilizando Help@Work para Androido iOS

La sesión típica de Help@Work para Androido iOS empieza por un usuario final que necesita ayuda.

Para iniciar una sesión de Help@Work con el dispositivo del usuario:

1. En Ivanti Neurons for MDM, vaya a **Dispositivos**.
2. En la página de la lista de dispositivos, haga clic en el dispositivo que necesita asistencia técnica.
3. En el menú Acciones, haga clic en **Iniciar control remoto de TeamViewer** para dispositivos Android o **Visualización remota** para dispositivos iOS. Verá dos opciones:
    - Modo atendido (predeterminado): esta opción requiere tener instalada la aplicación **Compatibilidad rápida con TeamViewer** y que esté en la lista blanca del dispositivo de destino.
    - Modo desatendido (disponible solo en Android): esta opción requiere que la aplicación **TeamViewer Host** esté instalada y en la lista blanca del dispositivo de destino.

> Si desea incluir los nombres de host en la lista blanca o anular la política de seguridad de contenidos, póngase en contacto con el equipo de asistencia.

> La opción de modo Sin atender funciona también en modo Kiosco. Se debe habilitar desde la página de integración de TeamViewer. El control remoto Sin atender requiere que la aplicación del host TeamViewer esté en el dispositivo, la activación de una vez en un dispositivo y una licencia de complemento MI. Para la activación única, el aviso de permiso se mostrará cuando la aplicación de host de TeamViewer se instale y se inicie por primera vez. Si lo desea, el administrador puede usar la aplicación de TeamViewer de "Inicio automático (ajustes de Configuración de aplicaciones administradas)" después del a instalación. El número de licencias se calcula en base a la distribución de la aplicación del host de TeamViewer. Si la aplicación del host de TeamViewer se distribuye en un dispositivo, se consume una licencia de sesión de host remoto sin atender. Además de la aplicación del host de TeamViewer, es posible que necesite las otras aplicaciones complementos y se deben permitir en el modo kiosco y kiosco compartido. Es posible que sean necesarios otros complementos según el modelo y el fabricante del dispositivo.

> Los dispositivos de Google Pixel no continúan con este permiso y requieren el consentimiento de permiso para cada sesión.

Si el administrador tiene un token válido de TeamViewer, el cliente de escritorio se inicia con una sesión de asistencia al dispositivo. En caso contrario, el administrador deberá iniciar sesión con TeamViewer y conceder permisos.

Para iniciar rápidamente una sesión remota, los administradores pueden iniciar sesión en la aplicación de escritorio de antemano.

Instalar TeamViewer

Instale la aplicación de TeamViewer en su escritorio para poder acceder y proporcionar asistencia técnica a los dispositivos remotos de sus usuarios. Para instalar TeamViewer:

1. Descargue aquí el paquete de instalación para la versión completa de TeamViewer para Mac, Windows o Android: **https://www.teamviewer.com/en/download/**
2. Inicia el programa de instalación de TeamViewer.
3. Seleccione **Instalación básica**.
4. Seleccione **Uso empresarial/comercial**.
5. Haga clic en **Aceptar - finalizar**.

Solicitar una cuenta de TeamViewer

Debe tener una cuenta de TeamViewer para poder proporcionar asistencia técnica con TeamViewer. Para obtener una cuenta de TeamViewer:

1. Vaya a **https://login.teamviewer.com/**.
2. Introduzca su correo electrónico, nombre y contraseña.
3. Haga clic en **Registrarme**.
4. Utilice la cuenta de correo electrónico que introdujo en el paso 2 para recibir un mensaje de correo de activación de su cuenta en TeamViewer.
5. Complete las instrucciones que aparecen en el correo electrónico para activar su cuenta de TeamViewer.

Confirmar la Id. de la sesión de TeamViewer

TeamViewer genera una Id. de la sesión cuando se establece la conexión entre el ordenador del administrador y el dispositivo móvil del usuario.

1. Cuando se genera la ID de sesión, Ivanti Neurons for MDM la pasa a la aplicación TeamViewer QuickSupport utilizando la configuración de la aplicación administrada, que a su vez utiliza esta ID de sesión para invocar el cliente de TeamViewer en el dispositivo. En el caso de iOS, la ID de sesión caduca a los 30 minutos.
2. Se solicita al usuario que acepte el EULA de TeamViewer.

12.2.10. Identidad de la infrastructura

Esta sección contiene los siguientes temas:

12.2.10.1. Configurar el proveedor de identidades

Licencia: Silver

Configure un proveedor de identidades (IdP) para autenticar los usuarios que desean registrar dispositivos con Ivanti Neurons for MDM, acceder a este portal de administración o acceder al portal de autoservicio. Es necesario un directorio de usuarios compatible con LDAP en el entorno local. Ivanti Neurons for MDM funciona con cualquier IdP compatible con SAML 2.0. Se ha verificado que Microsoft Entra ID Authentication (Entra ID), Microsoft ADFS (Active Directory Federation Services), Okta, OneLogin, PingOne y PingFederate de Ping Identity funcionan con Ivanti Neurons for MDM.

Anteriormente, si se configuraba SAML auth/IdP, la autenticación SAML se utilizaba tanto para el registro de dispositivos como para la autenticación del portal. Ahora se ha habilitado un interruptor para elegir diferentes métodos de autenticación para el acceso al Portal de administración y el Registro de dispositivos. El interruptor solo es aplicable para el registro de dispositivos.

Durante el registro del dispositivo, el administrador puede omitir la opción del proveedor de identidad y dar al usuario la opción de autenticarse mediante un PIN, en lugar de usar la página del proveedor de identidad.

Información general

- Si está usando Microsoft AD u otro directorio de LDAP local, tendrá que configurar Conector para conectarse e importar usuarios a Ivanti Neurons for MDM. Configure Conector o **LDAP** si todavía no lo ha hecho.
- Cuando se añade un IdP, la autenticación del usuario cambia automáticamente de LDAP a IdP.
- Solo está permitido un proveedor de IdP.
- En caso de que su IdP se vuelva inaccesible, utilice la cuenta del Administrador de abonados (TA, en inglés) de Ivanti Neurons for MDM para acceder a este Portal de administración y solucionar el problema. La cuenta de TA es una cuenta local y no requiere autenticación externa. La cuenta de TA se crea cuando se aprovisiona su Ivanti Neurons for MDM y se proporciona información al contacto técnico de su organización o equivalente. Si no tiene la información de su cuenta de TA, contacte con su representante de asistencia técnica.
- Ivanti Neurons for MDM es compatible con Microsoft Entra ID (Entra ID) para autenticar usuarios durante el registro de dispositivos Windows 10.

> Establezca el tipo de autenticación para los usuarios de su LDAP utilizando las herramientas proporcionadas por su proveedor de IdP. El esquema de autenticación de su IdP tendrá prioridad sobre los ajustes de Ivanti Neurons for MDM. Los ajustes de autenticación se pueden encontrar aquí: **Usuarios > Ajustes del usuario > Ajuste del Registro de dispositivos > Tipo de autenticación del Registro de un dispositivo**.

- Las inscripciones en la inscripción de dispositivos de Apple y en dispositivos Configurator no emplean IdP para autenticar a los usuarios.
- Para configurar un proveedor de identidad para que funcione en el registro de dispositivos iOS y macOS de Apple Business Manager, debe activar los ajustes **Activar la inscripción personalizada** y los ajustes relacionados **página web alojada con Ivanti** que se encuentran en **Admin > Apple > Inscripción de dispositivos >** *editar un perfil de inscripción de dispositivos*. Consulte **Inscripción de dispositivos** para obtener más información:



Tipos de configuración de IdP

La página de identidad de Ivanti Neurons for MDM le guía por la configuración de los siguientes tipos de proveedores de IdP:

- **Configuración de Ivanti Neurons for MDM IdP**: Los proveedores de Ivanti Neurons for MDM IdP compatibles son Entra ID, OneLogin, Okta y PingOne.
- **Configuración del IdP local**: los proveedores de IdP locales son ADFS 3.0, PingFederate 8.2.1 y PingFederate 8.1.3.
- **Configuración de IdP genérico**: esta es una ruta de configuración genérica que puede utilizar si no usa Microsoft ADFS, Okta, OneLogin ni PingFederate.

Configuración de un proveedor de identidad (IdP)

Procedimiento

1. Vaya a **Administración** > **Identidad** > **Autenticación con SAML**.
2. Haga clic en un tipo de configuración de proveedor de identidad:
   - **Configuración de la IDP de Ivanti Neurons for MDM**
   - **Configuración de la IDP interna**
   - **Configuración de la IDP genérica**
3. Seleccione el correspondiente IdP. Si ha seleccionado **Configuración de la IDP genérica** en el paso 3, omita este paso y continúe desde el paso 5.
4. Siga las instrucciones en pantalla que aparecen para su IdP elegida.
5. Haga clic en **Hecho**.

> Los administradores pueden iniciar sesión única durante un máximo de 2 horas desde su autenticación inicial con el IdP.

Establecer las tareas que puede que necesite completar

Según su IdP elegida, se le guiará a través de las siguientes páginas y pasos asociados:

IdP	Procedimiento
• Entra ID • Okta • One Login • Ping One	• Generar una clave para cargar a su IdP. • Iniciar sesión en su IdP y cargar una clave generada. • Exporte un archivo de metadatos de su IdP e impórtelo a Ivanti Neurons for MDM.
• ADSF 3.0 • Ping Federate 8.2.1 • Ping Federate 8.1.3	• Descargar el archivo de metadatos desde Ivanti Neurons for MDM. • Configurar una «Relación de confianza para usuario autenticado» en ADFS o una «Conexión SP» en PingFederate e importar el archivo de metadatos de Ivanti Neurons for MDM. • Exporte el archivo de metadatos de su IdP e impórtelo a Ivanti Neurons for MDM.
• IdP genérica	1. Descargar el archivo de metadatos desde Ivanti Neurons for MDM. 2. Siga las instrucciones que proporciona su proveedor de IdP para configurar el servidor de IdP o el servicio para comunicarse con el servicio de Ivanti Neurons for MDM como "Proveedor de servicios". Esto puede incluir: 1. Cargar el archivo de metadatos del paso 1 anterior a su IdP. Este archivo de configuración contiene la información esencial que permite a Ivanti Neurons for MDM, como proveedor de servicios SAML 2.0, comunicarse con su proveedor de identidad SAML 2.0. Las URL, certificados y ajustes estándar SAML 2.0 están incluidos en el archivo de metadatos. Ivanti Neurons for MDM espera una IdP compatible con SAML 2.0 para poder importar y procesar los metadatos XML exportados desde un Proveedor de servicios. 2. Configurar su IdP para que utilice RSA-SHA1 para firmar solicitudes de autenticación SAML. La información sobre el certificado de firmas utilizado para verificar las solicitudes de autenticación está incluido en el archivo de metadatos descargado en el paso 1. 3. Configuración de la IdP para que incluya un nombre de usuario en las respuestas de SAML que se envían a Ivanti Neurons for MDM. Especifique el nombre de usuario del elemento [Name Id] de la respuesta SAML del IdP. Exporte un archivo de metadatos de su IdP e impórtelo a Ivanti Neurons for MDM. 3. (Opcional): incluir el nombre de usuario en la Solicitud de autenticación con SAML: para incluir el nombre de usuario del usuario que va a autenticarse en la solicitud de autenticación y para eliminar la información de un usuario adicional cuando se autentica una IdP. Si activa esta opción, es posible que se produzcan errores de autenticación. Si está seguro de la validación de IdP, seleccione la opción **Entiendo el impacto de este cambio**

IdP	Procedimiento
	y ajuste **Incluir nombre de usuario en la solicitud de autenticación con SAML** como **ACTIVO**. Ivanti Access es una IdP validada para este ajuste.

Habilitar a los usuarios locales omitir la autenticación de IDP

Cuando se cae la conectividad de un IdP o Ivanti Neurons for MDM y es necesario solucionar el problema desde el lado de Ivanti Neurons for MDM, algunos administradores necesitan poder iniciar sesión en Ivanti Neurons for MDM sin depender de sistemas externos, como LDAP o IdP, para la autenticación. Solo los usuarios locales con funciones de administrador del sistema pueden omitir la autenticación IdP.

Crear una lista de usuarios locales para omitir la autenticación IdP

Procedimiento

1. Haga clic en **Administrador > Identidad**.
2. En la sección «Omisión de la autenticación IdP para los usuarios locales», haga clic en **+Añadir usuarios.**
3. De la lista que muestra solo los usuarios locales con funciones de administración del sistema, seleccione algunos usuarios.
4. Haga clic en **Guardar**.

> Para eliminar a un usuario de la lista de usuarios locales que pueden omitir la autenticación IdP, haga clic en el icono eliminar que hay junto a la entrada que desee eliminar.

Si no puede ver la página de Identidades, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración del sistema
- Sistema de solo lectura

12.2.10.2. Aprovisionamiento de usuarios con SCIM

Esta sección contiene los siguientes temas:

- Aprovisionamiento de usuarios
- Generar un token desde Ivanti Neurons for MDM
- Cambie el estado del Token
- Ver el estado del token desde Pruebas de auditoría
- Configurar atributos en aprovisionamiento de SCIM

Aprovisionamiento de usuarios

El aprovisionamiento de usuarios utiliza el protocolo SCIM para sincronizar un IdP con Ivanti Neurons for MDM y permite la sincronización parcial de usuarios y grupos. El aprovisionamiento de usuarios utiliza el protocolo SCIM para crear y actualizar automáticamente objetos de usuario y grupo procedentes de un IdP a Ivanti Neurons for MDM. Al igual que la integración actual con Entra ID y Okta, el proceso de aprovisionamiento de usuarios y grupos está automatizado; si se realizan cambios en el usuario o grupo en IdP, los mismos cambios se reflejan en Ivanti Neurons for MDM.

> El nombre de usuario de un usuario aprovisionado a través de SCIM se puede cambiar en el proveedor de identidad (IdP) si el nombre de usuario es único en Ivanti Neurons for MDM.

> Ahora se pueden buscar usuarios y grupos de SCIM con sus respectivos Id externos.

Generar un token desde Ivanti Neurons for MDM

Para iniciar el aprovisionamiento de usuarios para un IdP, genere un token y la URL de destino desde Ivanti Neurons for MDM.

> Asegúrese de que guarda el token y la URL de destino.

> Se pueden generar un máximo de 2 tokens en cualquier momento.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Vaya a **Administración** > **Identidad** > **Aprovisionamiento de usuarios**.
3. Seleccione Proveedor de identidades (IdP) en la lista desplegable.
4. Para generar un nuevo token, haga clic en **Generar**. Aparece un mensaje de notificación, haga clic en **Generar**. Se abre una nueva página con detalles del token y de la URL SCIM de destino.
5. Haga clic en **Copiar** para copiar el token o la URL de SCIM.
6. Actualizar la página. La página **Aprovisionamiento de usuarios** muestra la tabla Estado del token.

Cambie el estado del Token

Puede cambiar el estado de un token existente.

Procedimiento

1. Haga clic en el menú desplegable **Seleccionar** de la página **Aprovisionamiento de usuarios de Entra ID**.
2. Haga clic en **Seleccionar** y lleve a cabo los cambios siguientes en el token:
    - **Establecer en Activo**
    - **Establecer en Inactivo**
    - **Renovar**
    - **Quitar**

Ver el estado del token desde Pruebas de auditoría

Puede ver los registros de acciones/eventos que se dieron en un token SCIM desde la sección Pruebas de auditoría. El token SCIM puede tener uno de los estados siguientes:

- Token SCIM creado: se ha creado un token SCIM.
- Token SCIM activado: se ha activado el token SCIM.
- Token SCIM desactivado: se ha desactivado el token SCIM.
- Token SCIM Renovado: se ha renovado el token SCIM.
- Token SCIM eliminado: se ha eliminado el token SCIM.

La columna DETALLES también enumera el nombre del proveedor SCIM (IDP), como Azure, Okta, etc. que facilita la comunicación con Ivanti Neurons for MDM.

Configurar atributos en aprovisionamiento de SCIM

Esta sección describe cómo crear atributos personalizados y de empresa para un IdP durante el aprovisionamiento de usuarios.

Asignación de atributos

Una vez establecida la conexión, puede asignar los atributos entre IdP y Ivanti Neurons for MDM. Ivanti Neurons for MDM es compatible con los siguientes atributos de usuario:

Atributos centrales

- id
- Nombre de usuario
- Nombre en pantalla
- activo
- Nombre
- Apellido
- correos electrónicos

> Para Entra ID IdP, se admite IdP externo.

Lista de atributos para los que se permite la operación de actualización

- Nombre de usuario
- displayName
- correos electrónicos
- Nombre
- Apellido
- activo
- urn:ietf:params:scim:schemas:extension:ivanti:2.0:User
- urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Atributo personalizado

Esquema: urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<CustomAttribute123Name>

Atributo de empresa

Actualmente solo se admite el atributo Departamento.

Esquema: urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department

12.2.10.2.1. Aprovisionamiento de usuarios para IdP de Entra ID

Esta sección contiene los siguientes temas:

- Establecer una conexión con Ivanti Neurons for MDM
- Aprovisionar a los usuarios y grupos asignados
- Aprovisionar a todos los usuarios y grupos asignados
- Verificar el aprovisionamiento de usuarios asignados
- Aprovisionamiento de usuarios para IdP de Entra ID
- Editar ajustes
- Configure los atributos personalizados y de empresa
- Notas importantes: SCIM

Establecer una conexión con Ivanti Neurons for MDM

Después de crear los usuarios y grupos en su aplicación Entra ID Enterprise, puede establecer la conexión entre Entra ID e Ivanti Neurons for MDM.

Procedimiento

1. Inicie sesión en el portal Entra ID.
2. Vaya a **Aplicación de empresa** > haga clic en **+ Crear su propia aplicación**. Se abre la ventana Crear su propia aplicación.
3. Especifique el nombre de su aplicación (**Predeterminado: No galería**) y haga clic en **Crear**. Por ejemplo, Aprovisionamiento de usuario de Ivanti Neurons for MDM.
4. Vaya a **Aprovisionamiento** > **Editar aprovisionamiento** > **Credenciales del administrador**.
5. Copie y pegue la URL del SCIM de destino del portal de administración Ivanti Neurons for MDM en el campo **URL del abonado** del portal Entra ID.
6. Copie y pegue el código de acceso de Ivanti Neurons for MDM en el campo **Secret Token** del portal Entra ID.
7. Dé uno de los siguientes pasos:
    - Seleccione **Sincronizar solo los usuarios y grupos asignados**. Para más información, consulte Aprovisionar usuarios y grupos asignados
    - Seleccione **Sincronizar todos los usuarios y grupos**. Para obtener más información, consulte Aprovisionar todos los usuarios y grupos

    > Seleccione la opción Sincronizar todos los usuario y grupos para migrar los usuario.

Haga clic en **Comprobar conexión**. Una ventana emergente con una marca verde confirma la conexión.

9. Haga clic en **Guardar**.
10. Amplíe **Asignaciones** en la página **Aprovisionar** en el portal de Entra ID.
11. Haga clic en **Aprovisionar a usuarios de Entra ID**. Se abre la página de Asignación de atributos.
12. Haga clic en **Borrar** para borrar los atributos no admitidos.

Aprovisionar a los usuarios y grupos asignados

Una vez establecida la conexión entre Entra ID y Ivanti Neurons for MDM, puede aprovisionar usuarios o grupos.

> Al aprovisionar grupos, Entra ID no añade miembros de los grupos anidados al grupo seleccionado. Entra ID añade los miembros inmediatos y los nombres de grupo sólo al grupo y no a los miembros del subgrupo durante el proceso de sincronización.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. En la aplicación, vaya a **Usuarios y grupos** > haga clic en **+ Agregar usuario/grupo**. Se abre la página de Añadir Asignación.
3. Busque el usuario o el grupo desde el campo **Búsqueda**, haga clic en **Seleccionar**, y luego en **Asignar**. Se abre la página Usuarios y grupos.
4. Seleccione la casilla del usuario o grupo correspondiente.
5. Haga clic en**Aprovisionamiento** y luego haga clic en**Iniciar aprovisionamiento**. Se muestran los detalles de la configuración correcta.

Aprovisionar a todos los usuarios y grupos asignados

Una vez establecida la conexión entre Entra ID e Ivanti Neurons for MDM, puede aprovisionar usuarios o grupos.

Procedimiento

- Haga clic en**Aprovisionamiento** y luego haga clic en**Iniciar aprovisionamiento**. La página se abre con los detalles del aprovisionamiento exitoso y el usuario será aprovisionado en Ivanti Neurons for MDM

Verificar el aprovisionamiento de usuarios asignados

Una vez que un usuario asignado haya sido aprovisionado en el portal Entra ID, verifique el aprovisionamiento en el portal administrativo Ivanti Neurons for MDM.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Vaya a la pestaña **Usuarios** debajo del menú principal. El usuario que fue aprovisionado estará presente en la lista de usuarios de esta página.

> El proceso de aprovisionamiento puede durar hasta una hora.

Verificar el aprovisionamiento de grupos

Una vez aprovisionado un grupo en el portal Entra ID, verifique el aprovisionamiento en Ivanti Neurons for MDM.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Vaya a la pestaña **Usuarios** > **Grupos de usuarios**. El grupo que se aprovisionó estará presente en la lista de los grupos de esta página.

> El proceso de aprovisionamiento puede durar hasta una hora.

Editar ajustes

Este tema le ayuda a configurar los ajustes de Entra ID.

Procedimiento

1. Vaya a **Administrador > Microsoft Azure > Aprovisionamiento de usuarios de Entra ID**.
2. Haga clic en **Generar token** y copie el token.
3. Actualizar la página. Se abre la página ajustes de Entra ID.
4. Haga clic en **Editar ajustes**.
5. Ajuste **Invitar automáticamente a los usuarios importados desde Entra ID**: administre si los usuarios importados de Entra ID a Ivanti Neurons for MDM son invitados automáticamente a registrarse por correo electrónico.
6. Establecer **ID de Apple gestionada**: esta opción está desactivada por defecto. Haga clic en el botón alternador para habilitarlo. El ID de Apple gestionado se puede establecer durante el aprovisionamiento mediante:
   - **Dirección de correo electrónico del usuario**
     - (Opcional) seleccione la opción «Incluir el subdominio "appleid"» para evitar conflictos con los ID de Apple existentes.
   - Asignación de **Atributo personalizado**

     > El atributo personalizado debe evaluarse como un dirección de correo electrónico única.
7. (Opcional) Haga clic en **Añadir atributo personalizado**: especifique los atributos de usuario personalizados que desee aplicar a la administración de dispositivos desde su servicio de directorio. Cada atributo puede estar referenciado por $ en los campos de configuración que admitan variables. El uso de esta opción requiere una implementación uniforme de los atributos personalizados en los servidores de Entra ID. Si un servidor de Entra ID incluido en la implementación no usa este atributo, es posible que las características dependientes de este atributo no funcionen como deberían. La columna **Tipo de atributo** muestra el atributo **IDP** en la tabla **Atributos personalizados** de la sección **Editar**.
8. Haga clic en **Guardar cambios** después de modificar los ajustes de Entra ID.

Configure los atributos personalizados y de empresa

Procedimiento

1. Vaya a **Administración** > **Identidad** > **Aprovisionamiento de usuarios**.
2. En **Editar ajustes**, haga clic en **+Agregar atributo personalizado**.
3. Introduzca un nombre en el campo **Nombre del atributo** (por ejemplo, custAttr1) y haga clic en **Guardar cambios**. El atributo se lista y está disponible en la página **Administrador** > **Sistema** > **Atributo**. El atributo se indica como un atributo IdP y solo puede llevar a cabo la acción Eliminar.
4. Inicie sesión en el portal **Entra ID**.
5. Vaya a **Inicio**> **Aplicación Enterprise** > Haga clic en la aplicación SCIM.
6. Haga clic en **Aprovisionar a usuarios de Entra ID** en la sección **Asignaciones**.
7. Marque la casilla **Mostrar opciones avanzadas**.
8. Haga clic en **Editar la lista de atributos de customappsso**.

9. Introduzca una nueva entrada para el atributo personalizado que creó en la interfaz de usuario de Ivanti Neurons for MDM.
10. Añada el esquema para el atributo Personalizado/Empresa (Departamento) como se indica a continuación:
    Atributo personalizado: **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<custAttr1>**consulte el paso 3.
    Atributo de empresa: **urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department**
11. Haga clic en **Guardar cambios**.
12. Haga clic en **Agregar nueva asignación** y seleccione los atributos Origen y Destino en el menú desplegable:
13. Haga clic en **Aceptar** y en **Guardar asignación**.
14. Vaya a **Inicio**> **Aplicación Enterprise** > Haga clic en la aplicación SCIM > **Usuarios y grupos**.
15. Haga clic en nombre de usuario. Se abre la página Perfil.
16. Verifique si el valor asociado con el atributo aparece en la página de Perfil.
17. (Opcional) haga clic en una aplicación de SCIM > Aprovisionamiento > Aprovisionamiento bajo demanda, busque el usuario específico y haga clic en Aprovisionamiento. Para validar las nuevas asignaciones de atributos llevadas a cabo en los pasos anteriores.
18. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
19. Ir a **Usuario** > **Usuarios**> Seleccionar el usuario.
20. Haga clic en la pestaña **Atributos** y verifique el valor del atributo. El atributo se asigna para un usuario específico.

Consideraciones sobre la migración: Fuente de usuarios de Entra ID a SCIM de aprovisionamiento de usuarios

- Al migrar de Entra ID User Source a Entra ID User Provisioning (SCIM), seleccione Sync All Users and Groups (Sincronizar todos los usuarios y grupos).
- Una vez actualizados los usuarios y grupos con una fuente de Entra ID SCIM, vuelva a la página Aprovisionamiento de Azure en Azure y establezca los usuarios y grupos específicos que gestionará el Aprovisionamiento de usuarios Entra ID mediante la opción Sincronizar solo usuarios y grupos asignados.
- Ivanti Neurons for MDMCuando se completa la sincronización, puede eliminar a los usuarios y los grupos que no están definidos en Azure desde las listas de Usuarios y grupos.
- Cuando se inicia la migración, la página Entra ID User Source es accesible en un estado de solo lectura.

Consideraciones sobre la migración: SCIM de aprovisionamiento LDAP a usuario

Requisitos previos:

1. La opción **Activar este servidor LDAP** está seleccionada de forma predeterminada. Esta opción no debe estar seleccionada antes de la migración.
2. Cree una aplicación empresarial en Entra ID, añada los usuarios/grupos de LDAP sincronizados (los mismos usuarios/grupos de LDAP presentes en Ivanti) a la aplicación SCIM. Inicie el aprovisionamiento.

Consideraciones clave para la migración de LDAP a SCIM

- LDAP no captura toda la información de usuarios/grupos sincronizados, mientras que SCIM registra eventos de usuarios/grupos en registros de auditoría.
- El usuario LDAP con atributo personalizado tiene el tipo ldap definido, mientras que para SCIM, es IdP. Así pues, cuando los usuarios con atributos personalizados se migran de LDAP a SCIM, se debe crear el atributo personalizado de IdP correspondiente en la aplicación SCIM y los usuarios se migrarán. Cuando el usuario desee actualizar el atributo personalizado

ldap más adelante, el valor del atributo ldap.custom no se actualizará en MDM después de la migración. Se actualizará el valor del atributo IdP.

- Migrar usuarios LDAP que estén asociados con uno o varios atributos personalizados, específicamente "ldap.custAttr1", que indica el registro del dispositivo LDAP y la configuración (Configuración del certificado de identidad) enviada al dispositivo con el tipo SAN correspondiente al valor del LDAP. atributo personalizado.
- Migrar un usuario de LDAP donde el Apple ID gestionado está asociado con la dirección de correo electrónico. Por lo tanto, antes de la migración de LDAP a SCIM, si el usuario desea mantener el valor del Apple ID gestionado del usuario de LDAP, el Apple ID gestionado de SCIM debe estar habilitado y se debe guardar la configuración.
- Cuando se elimina el usuario LDAP en el servidor LDAP, el usuario sigue activo pero el indicador Sin sincronización está establecido en verdadero para ese usuario LDAP sincronizado en particular. En el caso de SCIM, cuando se elimina un usuario aprovisionado, el estado del usuario se desactiva.
- Una vez que SAML esté configurado para el proveedor de identidad (IdP) para usuarios SCIM, todos los usuarios de diversas fuentes, como local y LDAP, se autenticarán a través de SAML. Solo se pueden agregar usuarios locales a una lista de excepciones para evitar el flujo de autenticación del IdP. Esta configuración se puede administrar en la página SAML en **Administrador** > **Identidad** > **SAML**.
- Una vez que se configura SAML para los usuarios de IDP (SCIM) migrados, se puede omitir el registro del dispositivo (no a través de IDP) para otros usuarios de distintas fuentes, como locales y LDAP. Esto se puede administrar en **Usuarios** > **Configuración de usuario**.
- En LDAP, se admiten usuarios, grupos y unidades organizativas, mientras que en SCIM, se admiten usuarios y grupos, pero no unidades organizativas.
- El proceso de aprovisionamiento de grupos anidados no es compatible con SCIM.

Notas importantes: SCIM

- La dirección de correo electrónico es un campo obligatorio para el aprovisionamiento y la migración de usuarios o miembros.
- SCIM proporciona aprovisionamiento unidireccional desde Microsoft Entra ID a Ivanti Neurons for MDM. Ivanti Neurons for MDM no ofrece ninguna opción de sincronización. Si elimina un grupo o usuario aprovisionado SCIM de Ivanti Neurons for MDM, asegúrese de eliminar también el usuario o grupo de Microsoft Entra ID.
- Puede utilizar un atributo (origen o destino) sólo una vez en la ventana de asignación de aplicaciones SCIM en Microsoft Entra ID. No se puede asignar dos veces la misma fuente a un atributo de destino específico.
- Los usuarios inactivos no se pueden aprovisionar o migrar a Ivanti Neurons for MDM mediante SCIM.
- Actualmente, Ivanti Neurons for MDM no es compatible la notificación de eventos SCIM.
- La duración de la migración o el aprovisionamiento depende del número de usuarios o grupos implicados.
- Microsoft Azure controla el intervalo de aprovisionamiento y es de aproximadamente 40 minutos o más.
- Durante el reaprovisionamiento, Microsoft Entra ID solo reintentará las entradas que hayan fallado. Puede descargar los registros de aprovisionamiento para verificar los usuarios que han tenido éxito o han fallado en el aprovisionamiento desde Microsoft Entra ID.
- En SCIM no se permiten grupos duplicados de diferentes fuentes.
- Cuando un usuario aprovisionado se elimina de Microsoft Entra ID, el usuario se desactiva en Ivanti Neurons for MDM.
- Cuando un grupo de usuarios aprovisionado se elimina de Microsoft Entra ID, el grupo se elimina en Ivanti Neurons for MDM y los miembros independientes que pertenecen al grupo eliminado se desactivan y se asocian a Grupo de todos los usuarios.
- Cuando un miembro aprovisionado de un grupo aprovisionado se elimina en Microsoft Entra ID, el miembro se desactiva en Ivanti Neurons for MDM; sin embargo, el miembro sigue asociado al grupo en Ivanti Neurons for MDM.

- Cuando se elimina una asignación de atributo (atributo de empresa o atributo personalizado) de una aplicación, el valor del atributo eliminado se sigue reflejando en Ivanti Neurons for MDM.
- Cuando un atributo de usuario de un usuario aprovisionado se actualiza con un valor en blanco o vacío, el valor actualizado del atributo no se refleja en Ivanti Neurons for MDM.
- Si los atributos de usuario FName y LName (name.formatted) están en blanco durante la migración o actualización de Microsoft Entra ID a SCIM, la migración o actualización falla.
- Si elimina un usuario en Entra ID, la API SCIM correspondiente no elimina el usuario permanentemente, sino que realiza un borrado suave y cambia el estado del usuario de activo a inactivo. Si desea eliminar permanentemente el usuario, inicie sesión en el portal administrativo de Ivanti Neurons for MDM y elimine manualmente el usuario inactivo/deshabilitado.
- Cuando ya existe un usuario local en Ivanti Neurons for MDM con un ID de usuario determinado, se aprovisionará un usuario similar con el mismo ID de usuario desde Entra ID a MDM, la fuente de usuario se actualizará de Local a SCIM Entra ID.
- Entra ID con suscripción "Entra ID Premium P1" tiene el privilegio de aprovisionar el grupo requerido para ser asignado y aprovisionado.

12.2.10.2.2. Aprovisionamiento de usuarios para Okta IdP

Esta sección contiene los siguientes temas:

- Establecer una conexión con Ivanti Neurons for MDM
- Aprovisionar a usuarios y grupos
- Verificar el aprovisionamiento de usuarios asignados
- Verificar el aprovisionamiento de grupos
- Editar ajustes
- Configure los atributos personalizados/de empresa en el aprovisionamiento de usuarios de SCIM

Establecer una conexión con Ivanti Neurons for MDM

Ivanti Neurons for MDMDespués de crear los usuarios y grupos en su aplicación Okta, puede establecer la conexión entre Okta y .

Procedimiento

1. Inicie sesión en **Okta**.
2. Vaya a **Aplicaciones** > **Aplicaciones** > **Navegue por App Catalog**.
3. Busque **Agregar aplicación de prueba de SCIM 2.0** (titular del token de OAuth) e instale la aplicación.
4. Haga clic en la aplicación y vaya a **Aprovisionamiento** > **Integración**.
5. Haga clic en **Editar** y proporcione la url base y pegue el token generado.
6. Haga clic en **Guardar**.
7. Vaya a **Aprovisionamiento** y haga clic en **Editar**.
8. Habilite las acciones de usuario necesarias y haga clic en **Guardar**.

Aprovisionar a usuarios y grupos

Una vez establecida la conexión entre **Okta** y Ivanti Neurons for MDM, puede aprovisionar usuarios o grupos.

Procedimiento

1. Vaya a **Asignaciones** > **Asignar** > **Asignar a personas** o **Asignar a grupo**.
2. 2. Seleccione o busque un usuario o grupo existente y haga clic en **Asignar**.
3. Repita el proceso para añadir más **Usuarios** o **Grupos**.
4. Haga clic en **Hecho**.
5. Seleccione el grupo y pulse **forzar Grupo por nombre** para guardar y sincronizar el grupo.

Verificar el aprovisionamiento de usuarios asignados

Después de aprovisionar a un usuario asignado en el portal Okta, verifique el aprovisionamiento del usuario en el portal administrativo Ivanti Neurons for MDM.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Vaya a la pestaña **Usuarios** que hay bajo el menú principal. El usuario aprovisionado estará presente en la lista de usuarios de esta página.

Verificar el aprovisionamiento de grupos

Después de que se aprovisione un grupo en el portal de Okta, verifique el aprovisionamiento en Ivanti Neurons for MDM.

Procedimiento

1. Iniciar sesión en el portal administrativo de Ivanti Neurons for MDM.
2. Vaya a la pestaña **Usuarios** y haga clic en **Grupos de usuarios**. El grupo aprovisionado estará presente en la lista de los grupos de esta página.

Editar ajustes

Este tema le ayuda a configurar los ajustes de Okta.

Procedimiento

1. Vaya a **Administración** > **Identidad** > **Okta de aprovisionamiento de usuarios**.
2. Haga clic en **Editar ajustes**.
3. Ajustar **Invitar automáticamente a los usuarios importados desde Okta**: administre si los usuarios importados de Okta a Ivanti Neurons for MDM son invitados automáticamente a registrarse por correo electrónico.
4. (Opcional) Haga clic en **Añadir atributo personalizado**: especifique los atributos de usuario personalizados que desee aplicar a la administración de dispositivos desde su servicio de directorio. Cada atributo puede estar referenciado por $ en los campos de configuración que admitan variables. El uso de esta opción requiere una implementación uniforme de los atributos personalizados en los servidores de Okta. Si un servidor Okta incluido en la implementación no usa el atributo personalizado, es posible que las características que dependen de este atributo personalizado no funcionen como deberían. La columna **Tipo de atributo** muestra el atributo **IDP** en la tabla **Atributos personalizados** de la sección **Editar**.
5. Haga clic en **Guardar cambios** después de modificar los ajustes de Okta.

Configure los atributos personalizados/de empresa en el aprovisionamiento de usuarios de SCIM

Procedimiento

1. Vaya a **Administración** > **Identidad** > **Aprovisionamiento de usuarios**.
2. Haga clic en **Editar ajustes**.
3. Introduzca el atributo personalizado (por ejemplo, custAttr1) y haga clic en **Guardar cambios**.
4. Desde el Portal de Okta, haga clic en **Directorio** > **Editor de perfiles**.
5. Haga clic en **Aplicación de prueba SCIM 2.0** aplicación **Usuraio (titular del token de OAuth)**.
6. Haga clic en **Agregar atributo**.
7. Añada los valores de atributo personalizados siguientes, por ejemplo:
    - Nombre en pantalla (el mismo valor de atributo personalizado que proporcionamos en N-MDM, consulte el paso 3).
    - Nombre Variable : custAttr1

- Nombre externo: custAttr1
- Nombre de espacio externo: **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User**
- Permiso de usuario : (Lectura / Escritura)

8. Haga clic en **Guardar atributo**.
9. Haga clic en **Editor de perfiles** > **Asignaciones**. Verá dos secciones para las asignaciones (SCIM y Okta).
10. Asigne los atributos personalizados creados en N-MDM a los atributos definidos en Okta y guarde las asignaciones.
11. Vaya a **Usuarios** y haga clic en el usuario deseado.
12. Para editar los atributos, haga clic en **Perfil** > **Editar**.
13. Vaya a **Aplicaciones** > aplicación **Aplicación de prueba de SCIM 2.0 (titular del token OAuth)**.
14. En la pestaña **Asignaciones**, haga clic en **Asignar** y seleccione **Asignar a personas**.
    La ventana **Asignar aplicación de prueba de SCIM 2.0 (Titular del token de OAuth) a Personas** aparece en la pantalla.
15. Seleccione el usuario deseado y haga clic en **Asignar**.
16. Haga clic en **Hecho**.

Para verificar el atributo personalizado y su asignación en Ivanti Neurons for MDM:

- Vaya a **Usuarios** > **Usuario** (cualquier usuario específico) > **Atributos**. Asegúrese de que el atributo personalizado asignado para Okta está visible en la sección Atributos de usuario.

12.2.11. Configuración del servidor LDAP

Licencia: Silver

Configurar un servidor LDAP y un Conector le permite importar usuarios y grupos desde su directorio corporativo. Una vez que haya instalado al menos un Conector, puede añadir uno o más servidores LDAP.

Añadir servidores LDAP significa configurar:

- la *conexión* al servidor LDAP
- los *términos de búsqueda* necesarios para ver los datos del directorio de destino
- la parte del directorio que desea *importar*
- si desea *invitar a los usuarios* automáticamente en la parte del directorio seleccionada

Una vez que haya añadido un servidor LDAP, puede regresar a esta página para **editar la información del servidor LDAP** o **cambiar los usuarios LDAP seleccionados**.

> los usuarios LDAP se deben importar después de configurar un usuario LDAP. Consulte **Importar usuarios LDAP**.
> Los nombres de usuario de LDAP, al igual que los nombres de usuario locales, deben ser exclusivos internacionalmente. Le rogamos que verifique que los usuarios no tengan ya una cuenta local con el mismo nombre de usuario o, en el caso de organizaciones con más de un abonado, que el nombre de usuario no haya sido ya asociado con otro abonado.

Añadir un servidor LDAP

Procedimiento

1. Haga clic en **+Añadir servidor**.
2. Proporcione la siguiente información:
3. Haga clic en **Probar conexión y continuar.**

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique este servidor.
Descripción	Introduzca una descripción que explique el objetivo de este servidor.
URL del directorio	Introduzca la dirección URL para el directorio. Utilice uno de los siguientes formatos: ldap://dirección IP o ldaps://dirección IP o Ejemplo: ldap://miservidor1.miempresa.com:389
Id. de Usuario	Introduzca la Id. de usuario para una cuenta que tenga las siguientes características: • que esté administrada por un servidor LDAP • que se pueda enlazar con el servidor LDAP y buscar los subárboles para el usuario, el grupo y la unidad organizativa Esta es, por lo general, una cuenta con Credenciales de administrador de directorio (DN o nombre distintivo y contraseña).
Contraseña	Introduzca la contraseña para la cuenta.
Confirmar contraseña	Vuelva a introducir la contraseña para la cuenta.
Tipo de directorio	Seleccione el tipo de directorio de la lista de directorios compatibles. • Microsoft Active Directory • Abrir LDAP • Otro (compatible con OpenLDAP)

4. Este paso valida la información que ha proporcionado hasta el momento.

- Si se comprueba que la información es válida, el servicio recupera el contexto de nomenclatura LDAP, que será utilizado para rellenar algunos de los campos de la página siguiente.
- Si la URL de LDAP no se puede conectar, puede continuar con los siguientes pasos. No obstante, pero esto podría provocar una funcionalidad limitada hasta que la conexión se haya solucionado.

Complete el resto de ajustes:

5. Haga clic en **Siguiente**.

Ajuste	Qué hacer
URL de conmutación por error del directorio	Introduzca la dirección URL para el directorio secundario. Utilice el siguiente formato: ldap://dirección IP o Ejemplo: ldap://miservidor2.miempresa.com:389
Intervalo de sincronización	Introduzca el período de tiempo que debe pasar entre cada intento de sincronización de los datos LDAP desde el servidor LDAP. El valor predeterminado es de 15 minutos. Considere aumentar el intervalo una vez que haya sincronizado correctamente todos los datos del LDAP de destino y confirmado que su configuración LDAP cumple con sus necesidades.
Habilitar Descartar sincronización	Seleccione esta opción para descartar la sincronización de datos LDAP automáticamente si el conjunto de datos cargados disminuye significativamente. Esta opción garantiza que el comportamiento anormal en la parte del sistema de LDAP no dará lugar a molestas actualizaciones innecesarias en el servicio ni a la eliminación de configuraciones desde los dispositivos registrados. Asegúrese de que esta opción no está seleccionada si tiene previstos grandes cambios en su configuración LDAP o en el servidor LDAP.
Activar este servidor LDAP	Seleccione esta opción para utilizar este servidor LDAP con su servicio. Desactive este ajuste si desea retirar este servidor LDAP o ponerlo fuera de servicio. Aunque haya configurado una conmutación para casos de error a un segundo servidor LDAP que sustituiría automáticamente este servidor, utilizar esta opción le permite planificar el futuro y evitar una breve falta de conectividad durante la conmutación por error.
Se invitará automáticamente a todos los usuarios cuando se importen.	Seleccione esta opción para enviar invitaciones automáticamente a los usuarios una vez que se hayan importado del servidor LDAP.
Actualizar certificado de EC	Haga clic en **Seleccionar archivo** para cargar el certificado TLS emitido por la EC instalada en este servidor LDAP. Puede subir varios certificados de EC.
Obtener referencias	Se aplica solo si está utilizando un dominio de múltiples bosques. Esta opción indica si quiere utilizar controladores de dominio adicionales cuando el controlador del dominio de destino no disponga de una copia del objeto solicitado. • Seleccione **Continuar** si quiere utilizar referencias. • Seleccione **Ignorar** si no quiere utilizar controladores de dominio alternativos. • **Iniciar** tiene el mismo efecto actualmente que **Ignorar**. Seleccionar **Continuar** retrasa la autenticación LDAP.
Tiempo de espera de la búsqueda de resultados	Aumente el tiempo de espera si observa problemas de rendimiento o resultados incompletos cuando realiza búsquedas en los datos sincronizados desde el servidor LDAP.
Contador de la búsqueda de	Configure el número máximo de registros que debe devolver el servidor LDAP al mismo tiempo. Las situaciones que pueden requerir cambiar este ajuste para mejorar el rendimiento incluyen:

Ajuste	Qué hacer
resultados	• El servidor LDAP está situado lejos o está detrás de un enlace de latencia alta. En este caso, los resultados de las búsquedas grandes tardarán más en ser recuperados que los de las búsquedas pequeñas, por lo que la definir un conjunto más pequeño le permite ver los subconjuntos de datos actualizados con mayor rapidez. • El LDAP es muy grande y cada búsqueda le devuelve un volumen de resultados enorme. En este caso, si el rendimiento no constituye un problema, definir conjuntos de resultados más grandes haría posible encontrar todos los datos con menos búsquedas.

Para el entorno Sandbox, el intervalo de sincronización LDAP no puede programarse con un valor inferior a 8 horas.

6. Utilice las siguientes directrices para configurar la integración con el servidor LDAP:
7. Haga clic en **Examinar**o en**Buscar**.

Ajuste	Qué hacer
Formato de miembro del grupo	Seleccione **DN** o **UID** para indicar si quiere utilizar en su búsqueda un nombre distintivo o la Id. del usuario.
Atributos de búsqueda OU	Especifique los criterios para la búsqueda en el nivel de unidad organizativa.
DN base	Introduzca el nombre distintivo para comenzar un nivel en el que quiere que su búsqueda comience o tenga la raíz. Su selección determinará los valores predeterminados para otros campos, que puede cambiar si es necesario.
GUID de objeto	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP. Este atributo identifica de forma única una unidad organizativa a través del tiempo y a través de los cambios de nombre de OU.
Nombre del atributo	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Descripción	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
DN de atributo	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Filtro de búsqueda	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Ámbito de búsqueda	Seleccione la parte de la jerarquía LDAP que desea como destino: • **Base** (solo el nivel de entrada en la base de búsqueda) • **Nivel uno** (el nivel por debajo de la base de búsqueda) • **Subárbol** (el subárbol en el árbol de información de directorio bajo el DN base de búsqueda)
Atributos de búsqueda de usuarios	Especifique los criterios para buscar usuarios en un nivel concreto del directorio.
DN base	Introduzca el nombre distintivo del nivel en el que quiere comenzar a buscar.
UID de atributo	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
GUID de objeto	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP. Este atributo identifica de forma única un usuario a través del tiempo y a través de los cambios de nombre del usuario.
DN de atributo	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Nombre	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Apellidos	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.

Ajuste	Qué hacer
Nombre en pantalla	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Dirección de correo electrónico	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Nombre principal	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Configuración regional	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Miembro de	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Filtro de búsqueda	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Ámbito de búsqueda	Seleccione la parte de la jerarquía LDAP que desea como destino: • **Base** (solo el nivel de entrada en la base de búsqueda) • **Nivel uno** (el nivel por debajo de la base de búsqueda) • **Subárbol** (el subárbol en el árbol de información de directorio bajo el DN base de búsqueda)
Id. de Apple administrada	Seleccione sincronizar la ID de Apple administrada para los usuarios de LDAP. • **Ninguna** • **Patrón**: ◦ **Dirección de correo electrónico del usuario** ◦ **userUPN** Opcionalmente, seleccione la opción **Incluir el subdominio "appleid»** para evitar conflictos con los ID de Apple existentes.
+Añadir atributo personalizado	(Opcional) Especifique hasta 7 atributos de usuario personalizados que desee aplicar a la administración de dispositivos desde su servicio de directorio. Cada atributo puede estar referenciado por $ en los campos de configuración que admitan variables. **Importante:** el uso de esta opción requiere una implementación uniforme de los atributos personalizados en los servidores LDAP. Si un servidor LDAP incluido en la implementación no usa este atributo, es posible que las características dependientes de este atributo no funcionen como deberían.
Atributos de búsqueda de grupos	
DN base	Introduzca el nombre distintivo del nivel en el que quiere comenzar a buscar.
GUID de objeto	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP. Este es el atributo que identifica de forma exclusiva a un usuario a través del tiempo y a través de los cambios de nombre del usuario.

Ajuste	Qué hacer
DN de atributo	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Nombre del atributo	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Descripción	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Miembro	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Filtro de búsqueda	Si es necesario, cambie el valor predeterminado para que coincida con su entorno LDAP.
Ámbito de búsqueda	Seleccione la parte de la jerarquía LDAP que desea como destino: • **Base** (solo el nivel de entrada en la base de búsqueda) • **Nivel uno** (el nivel por debajo de la base de búsqueda) • **Subárbol** (el subárbol en el árbol de información de directorio bajo el DN base de búsqueda)

8. Confirme que su configuración le devuelve los datos esperados.
9. Puede realizar esto examinando o buscando un elemento conocido en el directorio.

Haga clic en **Siguiente**.

Eliminar un atributo personalizado de LDAP

Puede eliminar un atributo personalizado de LDAP y quitar sus valores de los usuarios asociados.

Procedimiento

1. Vaya a **Administrador > Atributos**.
2. En la sección **Atributos personalizados**, haga clic en el enlace **Eliminar** junto al atributo de LDAP que se quiere eliminar. Se mostrará una ventana de confirmación.
3. Haga clic en **Eliminar** para confirmar la eliminación.

> El botón **Eliminar** está deshabilitado de manera predeterminada. Deberá seleccionar la casilla de la opción **Entiendo que eliminar un atributo personalizado no puede revertirse** para habilitar el botón **Eliminar**.

Editar la información del servidor LDAP

Procedimiento

1. Vaya a **Administrador > LDAP.**
2. En la entrada del servidor LDAP, seleccione el icono **Editar** de la columna **Acciones** para ver la página Conectar al servidor LDAP.
3. Realice los cambios necesarios.
4. Haga clic en **Probar conexión y continuar.**
   Si la URL de LDAP no se puede conectar, puede continuar con los siguientes pasos. No obstante, pero esto podría provocar una

funcionalidad limitada hasta que la conexión se haya solucionado.

5. Haga clic en **Examinar**o en**Buscar**.
6. Confirme que su configuración le devuelve los datos esperados.
   Puede realizar esto examinando o buscando un elemento conocido en el directorio.
7. Haga clic en **Hecho**.

Importar usuarios LDAP

Procedimiento

1. Vaya a **Usuarios.**
2. Haga clic en **+Añadir > Invitar a usuarios de LDAP.**
3. Haga clic en **Seleccionar usuarios** en la entrada del servidor LDAP.
4. En la página Añadir usuarios de LDAP, introduzca el nombre del usuario, grupo u OU en el campo de búsqueda.
5. Para añadir nuevos usuarios o grupos, haga clic en **+Añadir** junto a la entrada que desee añadir.
6. Haga clic en **Siguiente**.
7. Elija si desea o no enviar la invitación.
   - No invitar a ninguno
     Para enviar las invitaciones más tarde, vaya a **Usuarios > Usuarios** y seleccione **Acciones > Enviar invitación** para enviar las invitaciones.
   - Invitar a todos

Haga clic en **Hecho**.

Actualizar los usuarios, grupos o unidades organizativas seleccionadas

Procedimiento

1. Vaya a **Administrador > LDAP.**
2. En la entrada del servidor LDAP, seleccione el icono **Administrar usuarios** de la columna **Acciones** para ver la página Añadir usuarios de LDAP.
3. Para añadir nuevos usuarios o grupos, introduzca el nombre del usuario o grupo en el campo de búsqueda.
4. Haga clic en **+Añadir** junto a la entrada que desea añadir.
5. Para eliminar a un usuario, grupo u OU, haga clic en el icono de eliminar que hay junto a la entrada que se borrar.
6. Haga clic en **Hecho**.

Habilitar la notificación Descartar sincronización de LDAP

Habilitar la opción Descartar sincronización de LDAP ayuda a prevenir cortes de electricidad provocados por cambios a gran escala no intencionados en su entorno de LDAP.

Procedimiento

1. Vaya a **Administrador > LDAP.**
2. En la entrada del servidor LDAP, seleccione el icono **Editar** de la columna **Acciones** para ver la página Conectar al servidor LDAP.
3. Marque la casilla **Activar Descartar sincronización**.

4. Introduzca un valor para el porcentaje de datos LDAP que se han vuelto a cargar y provocar así que se descarte la sincronización.
5. Haga clic en **Probar conexión y continuar.**
   Si la URL de LDAP no se puede conectar, puede continuar con los siguientes pasos. No obstante, pero esto podría provocar una funcionalidad limitada hasta que la conexión se haya solucionado.
6. Haga clic en **Hecho**.
7. Haga clic en el icono **Sincronizar ahora** en la entrada del servidor LDAP.
   Cuando el diferencial de cambio que se sincronizará de LDAP a Ivanti Neurons for MDM cae por debajo del porcentaje de descarte establecido, se generará una notificación de ADVERTENCIA. Cuando los cambios se reviertan a un valor inferior al porcentaje establecido, la notificación aparecerá DESACTIVADA.

Activación	Gravedad	Tipo de notificación	Tipo de componente	Componente
Descartar sincronización de LDAP	Advertencia	Sincronización de datos	LDAP	Nombre del servidor LDAP
Restauración de la sincronización de LDAP	Información	Sincronización de datos	LDAP	Nombre del servidor LDAP

La notificación Descartar sincronización parcial se genera cuando uno o más registros del usuario no se sincroniza desde el LDAP. En este caso, se incluye un archivo CSV como archivo adjunto con una lista de usuarios que no se han sincronizado. Si se descartó a algún usuario porque se haya omitido un atributo, también se incluirá una lista de atributos omitidos en el archivo CSV exportado.

Sincronizar los cambios desde el servidor LDAP

En la página de LDAP, haga clic en el icono **Sincronizar ahora** en la entrada del servidor LDAP.

> Si el nombre de la pantalla es de más de 128 caracteres, la sincronización LDAP ignorará dicho usuario y procede con otros usuarios o grupos de usuarios sincronizar.

Solucionar problemas de conectividad del servidor LDAPS

Si tiene problemas al conectarse al servidor LDAPS (LDAP a través de SSL), es posible que tenga algún problema con el certificado.

Para solucionar el problema:

- Verifique que no está utilizando un certificado de firma automática en el servidor LDAPS.
- Verifique que el certificado LDAPS no haya caducado ni haya sido revocado. Compruebe también que el nombre de host coincida.

Tras verificarlo, espere la sincronización automática de LDAP o sincronícelo manualmente yendo al icono **Administrador > LDAP > Sincronizar ahora** de la entrada del servidor LDAP.

Si no puede ver la página de LDAP, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración del sistema
- Sistema de solo lectura

12.2.12. Sentry

El Sentry es un componente que actúa como puerta de enlace entre los dispositivos móviles y su sistema de correo electrónico habilitado para ActiveSync. Utilice el Sentry para controlar qué dispositivos tienen permitido acceder al correo electrónico. Hay un archivo ISO a su disposición para descargar que puede instalar en un equipo virtual. Las organizaciones deberían considerar la posibilidad de usar un equilibrador de carga para mantener múltiples (y redundantes) servidores Sentry.

Licencia: Silver

Documentación más reciente

Para las últimas instrucciones de Sentry, visite **Documentación del producto** y haga clic en Sentry.

Para ver las instrucciones más recientes de instalación del Sentry, seleccione la versión adecuada de la *Guía de instalación local de Sentry independiente*.

Para ver las instrucciones más recientes de actualización del Sentry, seleccione la versión adecuada de la *Guía de Sentry*. Consulte las siguientes secciones en la Guía de Sentry:

- Para ver las instrucciones de actualización utilizando la UI del Administrador del sistema de Sentry independiente, consulte «Actualizaciones de software del Sentry independiente».
- Para ver las instrucciones de actualización utilizando la interfaz de línea de comandos (CLI) del Sentry independiente, consulte «Actualizar utilizando CLI».

Antes de actualizar, lea las notas de la versión del Sentry independiente de la versión a la que está actualizando.

12.3. Ajustes de Apple

Esta sección contiene los siguientes temas:

- Configurador de Apple
- Inscripción de dispositivos
- Configuración del asistente de configuración
- Instalación del Certificado MDM
- Dispositivos iPad compartidos para empresas
- Director de la escuela
- Ajustes (Apple)

12.3.1. Configurador de Apple

Puede usar esta página para preparar Apple Configurator para configurar la administración de dispositivos de Ivanti Neurons for MDM en dispositivos iOS. Apple Configurator hace que sea muy fácil implementar los dispositivos iOS en grandes cantidades. Además, Configurator permite a los administradores tener los dispositivos iOS supervisados, lo que permite un mayor nivel de capacidades de configuración y administración. Para más información sobre Apple Configurator, diríjase a la Mac App Store.

Los pasos básicos son los siguientes:

1. Exporte el perfil de MDM desde el abonado de Ivanti Neurons for MDM.
2. Importe el perfil MDM al Configurator.
3. Utilice el Configurator para aplicar el perfil MDM a los dispositivos anclados.

Definir un usuario predeterminado para los dispositivos

Los dispositivos configurados a través de Apple Configurator se asignan al usuario “nadie” en Ivanti Neurons for MDM a menos que elija un usuario diferente:

1. Haga clic en el campo **Asignar dispositivos configurados a**.
2. Comience a escribir el nombre de usuario del usuario de Ivanti Neurons for MDM que desee seleccionar.
3. Seleccione el nombre de usuario cuando aparezca en la lista desplegable.
4. Haga clic en **Guardar**.

Instalar aplicaciones con Apple Configurator

Antes de usar Apple Configurator para instalar aplicaciones:

- El acceso a la app store de Apple está restringido por la configuración del dispositivo.
- La instalación de aplicaciones está permitida por la configuración del dispositivo.
- Apple Configurator debe estar instalado en el ordenador utilizado para configurar los dispositivos.

Para instalar aplicaciones con Apple Configurator:

1. En Ivanti Neurons for MDM, vaya a **Administración > Configurador de Apple**.
2. Cambie el interruptor de dispositivos de inscripción a ON (encendido).
3. Haga clic en una de las siguientes opciones:
    - **Plist predeterminada del usuario**.
    - **Plist de usuario específico**: introduzca el nombre de usuario o la identificación de correo electrónico del usuario específico.

En Apple Configurator, vaya a **Preparar > Aplicaciones**.

5. Vaya a **Preparar > Ajuste y desactivar supervisión**.
6. Seleccione la opción **No actualizar nunca el dispositivo** en Actualizar iOS.
7. Haga clic **Preparar** (en la parte inferior de Apple Configurator).
   Las aplicaciones estarán visibles en la lista de aplicaciones instaladas del dispositivo una vez que el dispositivo ingrese.

Instalar aplicaciones con el servidor UEM

Para instalar aplicaciones con el servidor UEM:

1. Cargue una aplicación desde la tienda interna de la pestaña Aplicaciones.
2. Seleccione la aplicación.
3. Haga clic en la pestaña **Configuraciones de la aplicación**.
4. Seleccione **Instalar en dispositivo**.
   Complete los ajustes de la configuración.
5. Seleccione **Acciones > Forzar ingreso**.

Qué necesita hacer el usuario final

Apple requiere que el usuario final inicie Go al menos una vez o la característica de Ubicación de Ivanti Neurons for MDM no funcionará correctamente. Esto es necesario para garantizar que el usuario final es consciente de que su localización está siendo objeto de un seguimiento.

Precaución: Si los dispositivos han sido implementados en modo Single-App mediante Configurator, este enfoque no será posible.

Si no puede ver la página **Instalar Apple Configurator**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración del sistema
- Sistema de solo lectura

12.3.2. Inscripción basada en cuentas

Esta sección es aplicable a las inscripciones de Usuarios controlados por cuentas y Dispositivos controlados por cuentas.

Dispositivos compatibles

- Dispositivos con iOS 15+ (para la inscripción de usuarios controlada por cuenta) e iOS17+ (para la inscripción de dispositivos controlada por cuenta)
- Dispositivos con macOS 14+
- Dispositivos con visionOS 1.1+

Requisitos previos:

Para la inscripción de usuarios basada en cuentas

- Una cuenta de usuario de Ivanti Neurons for MDM con ID de Apple gestionado (usuarios en Apple Business Manager o Apple School Manager).
- En la sección **Inscripción de Apple**, seleccione **Inscripción de usuarios** de la lista desplegable **Seleccionar el tipo de inscripción de Apple**.
- En **Usuarios** → **Configuración de usuario** → establezca la **Configuración del propietario del dispositivo** en **ACTIVO** > seleccione la opción **Propiedad del usuario**.

Inscripción de dispositivo generada por cuentas

- Una cuenta de usuario en Ivanti Neurons for MDM con ID de Apple gestionado (usuarios en Apple Business Manager o Apple School Manager).
- En la sección **Inscripción de Apple**, seleccione **Inscripción de dispositivos** en la lista desplegable **Seleccionar tipo de inscripción de Apple**.
- En **Usuarios** → **Configuración de usuario** → configure **Configuración del propietario del dispositivo** en **ACTIVO** > seleccione la opción **Propiedad de la empresa**.

Inscripción de usuarios basada en cuentas para dispositivos iOS 15+, macOS 14+ y visionOS 1.1+ es una opción de inscripción diseñada para empresas que implementan BYOD (Traiga su propio dispositivo). La Inscripción de Usuario generada por cuenta es una versión modificada del protocolo MDM y la Inscripción de Usuarios con Apple Business Manager con un enfoque mucho mayor sobre la privacidad del usuario, implementada con el nivel de seguridad que las empresas necesitan.

Inscripción de dispositivos basada en cuentas para dispositivos iOS 17+, macOS 14+ y visionOS 1.1+ es una opción de inscripción diseñada para que las empresas inscriban dispositivos propiedad de la empresa / corporativos. La inscripción de dispositivos basada en cuentas aprovecha el protocolo MDM e Inscripción de dispositivos con Apple Business Manager con un enfoque mucho mayor en la privacidad del usuario, implementado con un nivel de seguridad que las empresas necesitan. Los usuarios finales pueden inscribir sus dispositivos mediante la función Cuenta de trabajo en Configuración.

Configurar el servicio de localización

Si su empresa tiene un nombre de dominio de empresa, por ejemplo, acme.com, la ID de correo electrónico para su dispositivo es nombrededispositivo@acme.com.

1. El usuario introduce username@acme.com para iniciar sesión en su cuenta del trabajo o de la escuela y, a continuación, el dispositivo realiza una llamada de solicitud HTTP GET a la URL: https://acme.com/.well-known/com.apple.remotemanagement?user-identifier=user@acme.com

Para más información, consulte:
https://developer.apple.com/documentation/devicemanagement/discover_authentication_servers

2. En el dominio acme.com, configure la regla de redirección para el URI - /.well-known/com.apple.remotemanagement para redirigirlo a la siguiente URL:
https://<n-MDM cluster>/.well-known/com.apple.remotemanagement

Detección de servicio simplificado para la inscripción de dispositivos impulsados por la cuenta

> Aplicable a iOS 18.2+, macOS 15.2+ y dispositivos VisionOS 2.2+.

Para la inscripción impulsada por la cuenta, cuando un usuario introduce al correo electrónico de su empresa para iniciar sesión en su cuenta laboral o escolar, el dispositivo primero busca un recurso HTTP conocido en el dominio de la organización, que contiene un enlace a la URL de inscripción de MDM.

Procedimiento

1. Iniciar sesión en la cuenta de trabajo o la cuenta escolar.
2. Verifique los dominios en **Apple Business Manager** y **Apple School Manager**: se aplica solo a los dominios que se han verificado en Apple Business Manager o Apple School Manager. Si se verifica un dominio, el dispositivo puede contactar con Apple Business Manager /Apple School Manager para obtener una URL de inscripción alternativa de MDM.
3. Establezca una asignación predeterminada Ivanti Neurons for MDM para tipos de plataforma **Mac**, **Apple Vision Pro**, **IPhone** y **iPad**.
   Para configurar una asignación de dispositivo predeterminada, siga los pasos que se indican a continuación:
   1. En **Apple Business Manager** / **Apple School Manager**, inicie sesión con un usuario que tenga el rol de Administrador o Administrador de inscripciones de dispositivo.
   2. Seleccione su nombre en la parte inferior de la barra lateral, seleccione Preferencias y, a continuación, realice una de las siguientes acciones:
      - Seleccione Asignación de servicios de administración de dispositivo debajo de Sus servicios de administración de dispositivo y, a continuación, seleccione Editar junto a Asignación de servicios de administración de dispositivo predeterminada.
      - Seleccione un servicio existente en Servicios de administración de dispositivo y, a continuación, seleccione Cambiar en Asignación de dispositivo predeterminada.
   3. Si no tiene otros servicios de administración de dispositivo configurados, cambie todas las asignaciones automáticas de dispositivo al servicio seleccionado y, a continuación, seleccione **Guardar**.
4. En la consola Ivanti Neurons for MDM, vaya a **Administrador** > **Apple** > **Inscripción del dispositivo**. En la pantalla de **Inscripción del dispositivo**, se agregan las columnas **URL ADDE** y **ESTABLECER HORA DE URL ADDE**.

> **Primera preferencia**: el dispositivo verifica el conocido recurso HTTP en el dominio de la organización.

Opción de respaldo: si el primer método falla, el dispositivo contacta con Apple ABM/ASM para obtener el destino alternativo especificado por Ivanti Neurons for MDM.

5. En **Acciones**, seleccione **Configurar la URL ADDE**.
6. Actualizar la página.

Instrucciones del usuario del dispositivo

En este tema se tratan las acciones que el usuario del dispositivo debe realizar para registrar la inscripción de usuario controlada por cuenta o la inscripción de dispositivo controlada por cuenta.

Procedimiento

1. En el dispositivo, vaya a una de las opciones siguientes:
   - Para el dispositivo **iOS**: **Ajustes** > **General** > **VPN** y **Gestión de dispositivos**.
   - Para el dispositivo **macOS**: **Configuración del sistema** > **Privacidad y Seguridad** > **Perfiles**.
   - Para el dispositivo **visionOS**: **Ajustes** > **General** > **VPN** y **Gestión de dispositivos**.
2. Ir a **Inicie sesión en la cuenta del trabajo o la escuela**.
3. Escriba la dirección de correo electrónico de la cuenta laboral o educativa. Asegúrese de que la dirección de correo electrónico tenga el siguiente formato:
   <enterprise domain name>nombredeusuario@<nombre del dominio de empresa>, por ejemplo, nombredeusuario@acme.com.
4. La página de inicio de sesión toma automáticamente la ID de Apple administrada y lleva al usuario a través del flujo de iReg. Asegúrese de que introduce las credenciales de Ivanti Neurons for MDM.
5. Escriba las credenciales de la cuenta laboral o educativa y haga clic en **Continuar**.
6. Después de una autenticación de dos factores, queda completa la inscripción del dispositivo.

12.3.3. Inscripción de dispositivos

Inscripción de dispositivos forma parte de Apple Business Manager, que permite que los clientes puedan comprar dispositivos en grandes cantidades e inscribirlos automáticamente en MDM durante la activación. Si decide participar, puede usar Ivanti Neurons for MDM como el servidor MDM para administrar estos dispositivos. Para obtener más información, consulte https://business.apple.com/.

Conectar Ivanti Neurons for MDM con Inscripción de dispositivos

Para utilizar Ivanti Neurons for MDMcomo servidor MDM para la Inscripción de dispositivos, configure el token del servidor Apple Business Manager en Ivanti Neurons for MDM.

Para cada servidor de Apple Business Manager, las siguientes acciones están disponibles en Ivanti Neurons for MDM:

- Probar conexión
- Añadir perfil de inscripción de dispositivos
- Descargar clave pública
- Sincronización completa de la inscripción de dispositivos: Iniciar sincronización completa. Puede tardar un tiempo en completarse. Una vez que la sincronización se haya completado, podrá ver la información en la columna Última sincronización. No puede iniciar la sincronización completa si esta ya se encuentra en progreso.

> Ivanti Neurons for MDM notifica a los administradores cuando falla la sincronización de un servidor DEP, lo que facilita la identificación de problemas. Si elimina un servidor DEP, el sistema también elimina sus notificaciones relacionadas.

- Cargar nuevo token
- Eliminar

> Las acciones **Editar autenticación** y **Asignar atributos del dispositivo de la inscripción de dispositivos** ahora están disponibles para los perfiles de inscripción de dispositivos en lugar de la inscripción de dispositivos (servidor MDM).

Procedimiento

1. Vaya a **Administración** > **Apple** > **Inscripción de dispositivos.**
2. Haga clic en **Descargar clave**.
3. Guarde su clave de Ivanti Neurons for MDM.
4. Haga clic en **business.apple.com**.
5. Inicie sesión utilizando sus credenciales de Apple aptas para el Inscripción de dispositivos.
6. En el sitio de Inscripción de dispositivos de Apple:
7. En Ivanti Neurons for MDM, haga clic en **Cargar**.
8. Haga clic en **Comenzar**.
9. Seleccione el teléfono de confianza que utilizará para autenticar el servicio de Apple.
10. Introduzca el código de verificación enviado al teléfono seleccionado.
11. Haga clic en **Añadir servidor MDM**.
12. Introduzca un nombre para identificar el servidor MDM virtual que se usará con el servicio.

13. Haga clic en **Siguiente**.
14. Cargue la clave pública que había descargado anteriormente.
15. Haga clic en **Siguiente**.
16. Haga clic en **El token de su servidor** para descargar el token.
17. Haga clic en **Hecho**.
18. Haga clic en **Siguiente**.
19. Seleccione una opción de autenticación:

- **Solicitar al usuario que se registre/inicie sesión**

> No es compatible con dispositivos que funcionan con la plataforma visionOS. En su lugar, utilice **Omitir inicio de sesión de usuario** para registrar un dispositivo.

> Se solicitará a los usuarios un nombre de usuario y contraseña. Los usuarios pueden introducir una contraseña o un PIN para el campo de la contraseña. Para los dispositivos macOS 15+, hay también disponibles opciones adicionales como **Face ID**, **Touch ID** o **Clave de seguridad** para los usuarios de IDP en proveedores de identidad respaldados por Clave de acceso. Las preferencias de contraseña y PIN se pueden configurar en **Usuarios** > Configuración de usuario relacionadas con la autenticación.

- **Omitir inicio de sesión de usuario**

> Los dispositivos que se hayan asignado al usuario «nadie» (anónimo) o a un usuario definido se pueden volver a asignar posteriormente a usuarios específicos desde la página **Dispositivos**.

Seleccione una de las siguientes opciones:

  - **Definir un usuario al que asignar todos los dispositivos**
  - **Asignar todos los dispositivos a un usuario anónimo**

10. La opción seleccionada reemplaza a las selecciones de **Ajustes de usuario**.

Haga clic en **Cargar** para instalar la clave que recibió en el paso 3.

11. Complete el formulario que se muestra para definir el perfil de los dispositivos de la Inscripción de dispositivos:
12. Defina qué pasos puede omitir el usuario durante la activación del dispositivo para las siguientes opciones de configuración:

Ajuste	Qué hacer
Nombre	Introduzca un nombre que identifique a este perfil de Inscripción de dispositivos.
Descripción	Introduzca una descripción para el perfil.
Departamento	Introduzca el departamento de su empresa asociado a este perfil.
Modo supervisado iOS 17+	Permite control administrativo adicional sobre las configuraciones y restricciones. Para los dispositivos iOS 13+ y macOS 10.15+, esta opción está activada de forma predeterminada. **Versión del sistema operativo para la inscripción** • **Requerir una versión mínima del SO para la inscripción**: el administrador puede establecer una versión mínima requerida del sistema operativo para la inscripción de dispositivos. Si el dispositivo no cumple los criterios de versión mínima del sistema operativo, el sistema solicita al usuario que actualice a la versión requerida. Si el usuario se niega a actualizar, se bloquea la inscripción. **Última versión**: el administrador puede establecer la versión más reciente del sistema operativo para la inscripción de dispositivos. Si el dispositivo no cumple los criterios de la última versión del sistema operativo, el sistema solicitará al usuario que actualice a la versión requerida. Si el usuario se niega a actualizar, se bloquea la inscripción. **Versión específica**: el administrador puede establecer una versión mínima requerida del sistema operativo para la inscripción de dispositivos. Si el dispositivo no cumple los criterios de versión mínima del sistema operativo, el sistema solicita al usuario que actualice a la versión requerida. Si el usuario se niega a actualizar, se bloquea la inscripción. • **iOS mínimo**: si la versión de compilación no coincide con la versión del sistema operativo especificada en la clave "**OSVersion**", tendrá prioridad la versión del sistema operativo. • **Versión de compilación mínima**: si la versión de compilación no coincide con la versión del sistema operativo especificada en la clave "**OSVersion**", tendrá prioridad la versión del sistema operativo. Este campo es opcional, si introduce un número de compilación incorrecto. • **Mensaje**: una descripción del error adecuada para mostrar al usuario. En caso necesario, ◦ el cliente intentará por todos los medios mostrar el mensaje, pero no podrá ◦ hacerlo, debido a las condiciones locales. Como práctica se debe añadir el mensaje. • **Añadir dispositivos al programa beta** **Programas beta para iOS**: fuerza las versiones beta de software en iOS durante la inscripción automatizada de dispositivos.
macOS 14+	**Versión del sistema operativo para la inscripción** • **Requerir una versión mínima del SO para la inscripción**: el administrador puede establecer una versión mínima requerida del sistema operativo para la inscripción de dispositivos. Si el dispositivo no cumple los criterios de versión mínima del sistema operativo, el sistema solicita al usuario que actualice a la versión requerida. Si el usuario se niega a actualizar, se bloquea la inscripción. **Última versión**: el administrador puede establecer la versión más reciente del sistema operativo para la inscripción de dispositivos. Si el dispositivo no cumple los criterios de la última versión del sistema operativo, el sistema solicitará al usuario que actualice a la versión requerida. Si el usuario se niega a actualizar, se bloquea la inscripción. **Versión específica**: el administrador puede establecer una versión mínima requerida del sistema

Ajuste	Qué hacer
	operativo para la inscripción de dispositivos. Si el dispositivo no cumple los criterios de versión mínima del sistema operativo, el sistema solicita al usuario que actualice a la versión requerida. Si el usuario se niega a actualizar, se bloquea la inscripción. • **Versión mínima de macOS**: Si la versión de compilación no es consistente con la versión del sistema operativo especificada en la clave '**OSVersion**', la versión del sistema operativo tendrá prioridad. • **Versión de compilación mínima**: si la versión de compilación no coincide con la versión del sistema operativo especificada en la clave "**OSVersion**", tendrá prioridad la versión del sistema operativo. Este campo es opcional, si introduce un número de compilación incorrecto. • **Mensaje**: una descripción del error adecuada para mostrar al usuario. En caso necesario, ◦ el cliente intentará por todos los medios mostrar el mensaje, pero no podrá ◦ hacerlo, debido a las condiciones locales. Como práctica se debe añadir el mensaje. • **Añadir dispositivos al programa beta** **Programa beta para macOS**: fuerza las versiones beta de software en macOS durante la inscripción automatizada de dispositivos.
Descargar e instalar automáticamente las actualizaciones de iOS	(Solo iOS 9.0+) Si la opción Descargas automáticas está seleccionada en el dispositivo en **Ajustes > iTunes App Store**, las actualizaciones del sistema operativo se descargarán automáticamente, pero no se instalarán, incluso cuando la opción Perfil de inscripción del dispositivo esté desactivada. Este ajuste tendrá preferencia cuando haya una configuración de actualizaciones del software iOS aplicable a los dispositivos supervisados inscritos en la Inscripción de dispositivos. Cualquier cambio en este ajuste será aplicable al dispositivo supervisado inscrito en la Inscripción de dispositivos incluso sin restablecer el dispositivo.
MDM extraíble	Define si el usuario no podrá anular la inscripción de MDM después de que se registre el dispositivo. Esta configuración no se aplica a los **Shared iPads**.
MDM obligatoria	Define si el usuario no podrá omitir la instalación de MDM durante el proceso de activación. Para los dispositivos iOS 13+ y macOS 10.15+, esta opción está activada de forma predeterminada.
No utilizar el perfil desde la copia de seguridad	Cuando se habilita, el dispositivo no utiliza este perfil cuando se restaura el dispositivo desde una copia de seguridad. Aplicable solo a dispositivos iOS 26+ y visionOS 26+.
Permitir sincronización	(No aplicable para iOS 13+ y macOS 10.15+) Permite funciones de emparejamiento de host, como la sincronización con iTunes. El emparejamiento siempre está permitido para los hosts que tienen certificados de emparejamiento válidos.
Volver al servicio	Establezca **Volver al servicio** como **Verdadero** para garantizar que la aplicación se conserva cuando se ejecuta la acción **Volver al servicio** . Permite que el dispositivo realice una instantánea de las aplicaciones y ofrezca una experiencia más ágil durante el proceso de Volver al servicio. Si esta opción está desactivada, el dispositivo podrá seguir ejecutando Volver al servicio, aunque la aplicación tendrá que descargarse nuevamente durante el proceso de reinscripción. Para aprovechar la funcionalidad **Apple Migration ABM,** esta función debe estar deshabilitada.

Ajuste	Qué hacer
	El dispositivo no se puede migrar si **Volver al servicio** está establecido como**Verdadero**. Aplicable solo a dispositivos iOS 26+ y visionOS 26+.
Certificado	Haga clic en **+Añadir** para cargar certificados.
Teléfono de la asistencia técnica	Proporcione un número de teléfono al que puedan llamar los usuarios del dispositivo si necesitan asistencia.
Dirección de correo electrónico de asistencia técnica	Proporcione una dirección de correo electrónico donde puedan escribir los usuarios del dispositivo si necesitan asistencia.
Inscripción personalizada	(iOS 13.0+ y macOS 10.15+) Crear páginas web de inscripción personalizadas. Especifique su propia página web personalizada (vista web) para autenticar a los usuarios durante la Inscripción de dispositivos. Utilice esta página para mostrar información personalizada como el tipo de autenticación, la personalización de marca, el texto de consentimiento y la política de privacidad. Vea la sección «*Añadir una página web de inscripción de dispositivos personalizada*» siguiendo este procedimiento para más detalles. • Seleccione **Activar la inscripción personalizada** para habilitar esta función. • Introduzca la **URL**, como https://mycustomweburl.com. Esta URL define el valor de la URL personalizada para presentarla al usuario en una vista web.
Multiusuario	(iOS 13.4+) Shared iPads for Business Permite a las empresas compartir dispositivos entre varios empleados, sin dejar de ofrecer una experiencia personalizada. Seleccione el **Modo multiusuario** para activar Shared iPad en un dispositivo. Para obtener más información, vea **iPad compartido para empresas.** • Este ajuste no es aplicable a Apple Education. • Seleccione la configuración de **Modo supervisado** para modificar el ajuste Multiusuario.
Tamaño de la cuota	(iOS 13.4+) iPad compartido for Business. El valor está en megabytes (MB), que denota el almacenamiento asignado a un usuario en un dispositivo. Si el valor es demasiado pequeño, el dispositivo asigna un tamaño de cuota por defecto.
Usuarios residentes	(iOS 13.4+) iPad compartido for Business. El valor detalla el número de usuarios que pueden persistir o residir en el dispositivo. Si el valor es mayor que el valor del número máximo de usuarios que admite el dispositivo, el servidor MDM utiliza ese valor (número máximo de usuarios) como predeterminado. Los administradores pueden proporcionar el valor del tamaño de la cuota o de los usuarios residentes. Si se proporcionan ambos valores, el servidor de MDM utiliza el tamaño de la cuota como valor predeterminado.
Tiempo de espera de la	(iOS 14.5+) iPad compartido for Business. Muestra el tiempo de espera en segundos para una sesión de usuario. La sesión de usuario se cierra automáticamente tras el periodo de inactividad especificado. El valor mínimo es de 30 segundos. Si se

Ajuste	Qué hacer
sesión de usuario	establece este valor en 0 se elimina el tiempo de espera y se establece el tiempo de espera del dispositivo de manera predeterminada. Los valores de 1 a 29 no son válidos. Cuando se establece, el dispositivo se ajusta al tiempo de espera predeterminado.
Tiempo de espera de la sesión temporal	(iOS 14.5+) iPad compartido for Business. Muestra el tiempo de espera en segundos para una sesión temporal o de invitado. La sesión temporal se cierra automáticamente tras el periodo de inactividad especificado. El valor mínimo es 30 segundos Si se establece este valor a 0 se elimina el tiempo de espera y se establece el tiempo de espera del dispositivo de manera predeterminada. Los valores de 1 a 29 no son válidos. Cuando se establece, el dispositivo se ajusta al tiempo de espera predeterminado.
Solo sesión temporal	(iOS 14.5+) iPad compartido for Business. Si es verdadero, el usuario solo ve el panel de bienvenida de invitados y solo puede iniciar sesión como usuario invitado. Si es falso, el usuario puede iniciar sesión con un ID de Apple gestionado (el comportamiento existente). Predeterminado: falso
Dominios predeterminados de Apple ID administrados	(iOS 16.0+) iPad compartido for Business. Especifique una lista de dominios. Los usuarios pueden seleccionar el dominio de su cuenta en la lista de dominios del teclado QuickType.
Periodo de gracia de la autenticación en línea	(iOS 16.0+) iPad compartido for Business. Especifique el número de días que el usuario puede iniciar sesión sin conectarse a la red. Ajustar este valor como cero aplica la autenticación cada vez. **Predeterminado**: 0
Tiempo de bloqueo automático	(iOS 17.0+) Especifica el tiempo (en segundos) tras el cual el dispositivo pasa al modo de suspensión. El valor mínimo es 120 segundos.
Periodo de gracia de bloqueo con contraseña	Especifica el tiempo (en segundos) después del cual el usuario del dispositivo debe ingresar el código de acceso del dispositivo para desbloquearlo. El valor mínimo es 0 segundos y el valor máximo es 14400 segundos.
Zona horaria	Especifique la zona horaria a la que debe pertenecer el dispositivo. **Ejemplo**: Pacific/Midway

Opciones de configuración

- Omitir la introducción del código de acceso: al seleccionar esta opción se activará automáticamente Omitir configuración de Apple Pay y Omitir Touch ID
- Omitir servicios de localización
- Omitir restaurar a partir de copia de seguridad
- Omitir «Pasar a iOS» desde Android
- Omitir Condiciones del servicio
- Omitir el inicio de sesión en Apple ID y iCloud: al seleccionar esta opción se activará automáticamente Omitir configuración de Apple Pay
- Omitir configuración de Touch ID (solo en iPhone 5s, 6, 6+, iPad Air 2, iPad Mini 3): al seleccionar esta opción se activará automáticamente Omitir configuración de Apple Pay.
- Omitir configuración de Apple Pay (solo en iPhone 6, 6+, iPad Air 2, iPad Mini 3)
- Omitir configuración de zoom
- Omitir Siri
- Omitir inteligencia (iOS 18+ y macOS 15+)
- Saltar el envío automático de información de diagnóstico
- Omitir almacenamiento en la nube (iOS 10.3+ y macOS 10.13.4+)
- Omitir configuración del tono de la pantalla (iOS 9+ y macOS 10.14+)
- Omitir sensibilidad del botón de inicio
- Omitir la pantalla de selección de teclado
- Omitir pantallas de información iniciales: solo para fines informativos para el usuario. Ejemplos: portada, multitarea y centro de control.
- Omitir la pantalla de migración de Apple Watch
- Omitir la pantalla «Choose Your Look» («Elija su aspecto») (iOS 13.0+ y macOS 10.14+)
- Omitir la hora en pantalla (iOS 12.0+ y macOS 10.15+)
- Omitir privacidad (macOS 10.13.4+ y tvOS 11.3+)
- Omitir la activación del modo de bloqueo (iOS 17.1+ y macOS 14.0+)
- Omitir actualización de software (iOS 12.0+ y macOS 15.4+)
- Omitir el panel de Añadir plan móvil (iPhone Xs, iPhone Xs Max, Iphone XR)
- Mostrar texto personalizado en la página de inicio de sesión: seleccione esta opción para introducir un mensaje de texto personalizado en el cuadro de texto. Este mensaje se mostrará en la página de inicio de sesión del dispositivo durante la configuración de la Inscripción de dispositivos para proporcionar instrucciones adicionales a los usuarios finales para ayudarles en el proceso.
- Configuración de avance automático: seleccione esta opción para que el asistente avance automáticamente por las pantallas de configuración del dispositivo. El valor predeterminado es «falso». Compatible con tvOS y macOS 11 y posteriores. La configuración de avance automático no funciona en una conexión Wi-Fi, el dispositivo debe estar conectado a través de una Ethernet.
- Términos de tratamiento: omite el panel de Términos de tratamiento. (iOS 16+)

Opciones de configuración
• Omitir el panel Liquid Glass (iOS 27.0+ y macOS 27.0+)
iOS
• Omitir el panel de inicio (13.0+) • Omitir iMessage y FaceTime (12,0+) • Omitir lenguaje hablado (13.0+) • Omitir restauración completada (14.0+) • Omitir actualización completada (14.0+) • Saltar seguridad (16.0+) • Omitir panel de configuración del botón de acción (17.0+) • Omitir panel de filtrado de contenido web (18.2+) • Omitir panel de manejo de seguridad (18.4+) • Omitir panel de multitarea (26.0+) • Omitir panel de showcase de SO (26.0+) • Omitir el panel Apariencia de Accesibilidad (27.0+)
macOS • Omitir pantalla de iCloud Analytics • Omitir la pantalla de visualización True Tone (10.13.6+): (opcional) seleccione esta opción para omitir la ventana de visualización True Tone. • Omitir accesibilidad (11.0+) • Omitir el desbloqueo con reloj (12.0+) • Omitir la activación del modo de bloqueo (14.0+) • Omitir selección de fondo de pantalla (14.1+) • Omitir panel de privacidad de ajustes adicionales (26.0+) • Omitir actualización completada (26.0+) **tvOS** • Omitir la pantalla de sincronización de la distribución de la pantalla principal de Apple TV • Omitir la pantalla de firma del proveedor de Apple TV • Omitir la opción de tocar para configurar • Omitir la configuración del protector de pantalla aéreo **Opciones del asistente de configuración de la cuenta macOS** • Omitir creación de la cuenta del administrador • Omitir creación de la cuenta de configuración principal • Crear cuentas principales como usuarios usuales (como administrador si no se selecciona)

Opciones de configuración
Esperar la configuración del dispositivo durante la configuración de la inscripción del dispositivo
• Esperar hasta que las configuraciones y las aplicaciones de alta prioridad se transfieran a los dispositivos: seleccione esta opción para transferir las configuraciones y las aplicaciones de alta prioridad al dispositivo antes de continuar con el resto de pantallas de configuración de la inscripción de dispositivos. Esta configuración evitará que el usuario final utilice el dispositivo antes de que las configuraciones requeridas y las aplicaciones de alta prioridad se envíen al dispositivo. • Límite de tiempo - El tiempo límite predeterminado es de 3 minutos. El tiempo máximo es de 10 minutos. Para habilitar esta función, seleccione la opción **Modo supervisado** mientras edita el perfil de la Inscripción de dispositivos.

Haga clic en **Guardar**.

La siguiente tabla se rellena en la página **Administración** > **Apple** > **Inscripción de dispositivos**:

Ajuste	Qué hacer
Nombre, (Haga clic en el encabezado de la columna para ordenar de manera alfanumérica). Utilice el campo Buscar para buscar elementos de esta columna	Nombre del servidor MDM
Nombre de la cuenta de Apple (Haga clic en el encabezado de la columna para ordenar de manera alfanumérica). Utilice el campo Buscar para buscar elementos de esta columna	Id. de Apple administrada
Número de dispositivos	Número de dispositivos asignados
Perfil(es) de inscripción	Número de perfiles de inscripción asignados del dispositivo
Última sincronización (Haga clic en el encabezado de la columna para ordenar de manera alfanumérica).	Hora del último contacto
Token caduca (Haga clic en el encabezado de la columna para ordenar de manera alfanumérica).	Fecha de caducidad del token

- Cuando se añaden nuevos dispositivos a la Inscripción de dispositivos de Apple, pueden pasar hasta 15 minutos hasta que Ivanti Neurons for MDM descubra dichos dispositivos nuevos. A continuación, estos nuevos dispositivos se asignarán a un perfil de inscripción. Si no puede añadir dispositivos nuevos a la Inscripción de dispositivos, vaya a **Panel > Notificaciones** para buscar notificaciones de Apple para la Inscripción de dispositivos de Apple. Si hay alguna actualización en el EULA, se le notificará por correo electrónico qué pasos debe aceptar del nuevo EULA.
- Puede ver todos los atributos de dispositivos personalizados que existen en su abonado y asignarlos a los dispositivos durante su inscripción a través de la Inscripción de dispositivos de Apple.
- En los dispositivos compartidos de macOS, el comando ListUsers muestra una lista de todos los usuarios locales en los dispositivos y solo los detalles de la última conexión del usuario que registró el dispositivo.

Editar el perfil de Inscripción de dispositivos

Procedimiento

1. Vaya a **Administración** > **Apple** > **Inscripción de dispositivos.**
2. Busque el nombre del servidor del Apple Business Manager (que se creó en el sitio de Apple) en la columna Nombre de la cuenta de Apple.
3. Haga clic en el enlace numérico de la columna Perfil(es) de inscripción.
4. Para obtener un perfil específico, seleccione **Acciones**>**Editar perfil de inscripción de dispositivos.**
5. Actualice y guarde el perfil.

- Si se edita un perfil de Inscripción de dispositivos, el recuento de dispositivos del perfil modificado se actualizará en breve.
- Si actualiza el token del servidor en el sitio de Apple, el token existente quedará invalidado. No obstante la pantalla de la página de la Inscripción de dispositivos (incluida la fecha de caducidad del token) se mantendrán hasta que cargue el token nuevo.
- Si se crea o edita un perfil de inscripción de dispositivos, los cambios realizados en el perfil se pueden ver en la sección de rastro de la auditoría. Cuando haga clic en el enlace de Detalles, podrá ver los Atributos y los cambios realizados en los atributos en las columnas Antes y Después. Puede observar el estado de cada perfil de inscripción de dispositivos como Creado (para un nuevo perfil), Actualizado (al editar cualquier perfil existente) o Eliminado (al eliminar cualquier perfil existente). Para filtrar los perfiles de inscripción de dispositivos en Rastro de la auditoría, debe seleccionar Administrar sistema como la Categoría e Registro automatizado de dispositivos como el Tipo.

El Perfil de inscripción de dispositivos contiene la siguiente información:

Ajuste	Qué hacer
Nombre del perfil (Haga clic en el encabezado de la columna para ordenar de manera alfanumérica).	Introduzca un nombre que identifique a este perfil de Inscripción de dispositivos.
Descripción (Haga clic en el encabezado de la columna para ordenar de manera alfanumérica).	Introduzca una descripción para el perfil.
Departamento (Haga clic en el encabezado de la columna para ordenar de manera alfanumérica).	Introduzca el departamento de su empresa asociado a este perfil.
Teléfono de la asistencia técnica (Haga clic en el encabezado de la columna para ordenar de manera alfanumérica).	Proporcione un número de teléfono al que puedan llamar los usuarios del dispositivo si necesitan asistencia.
Número de dispositivos	Muestra el número de dispositivos del perfil
Acciones	Administrar perfiles

Gestión de múltiples perfiles de inscripción de dispositivos

Se pueden crear varios perfiles de inscripción de dispositivos en cada servidor de Apple Business Manager. De esta manera, diferentes conjuntos de dispositivos podrán recibir diferentes configuraciones. Los dispositivos también se pueden trasladar de un perfil de Inscripción de dispositivos a otro.

Procedimiento

1. Vaya a **Administración** > **Apple** > **Inscripción de dispositivos.**
2. Busque el nombre del servidor del Apple Business Manager en la columna Nombre de la cuenta de Apple.
3. Haga clic en el enlace numérico de la columna Perfil(es) de inscripción.

4. Para crear un nuevo perfil de Inscripción de dispositivos que se asociará al servidor seleccionado, haga clic en **Crear nuevo perfil**. Cree y guarde el perfil.
5. Para administrar cada perfil, haga clic en **Acciones** y seleccione una de las siguientes opciones:
    - **Configurar como perfil predeterminado**: configure el perfil como predeterminado en el mismo servidor virtual. Los registros de nuevos dispositivos recibirán este perfil predeterminado.
    - **Editar perfil**: actualice el perfil existente.
    - **Editar autenticación**: edita el ajuste de autenticación de la inscripción de dispositivos.
    - **Asignar atributos del dispositivo de la inscripción de dispositivos**: los administradores utilizan los atributos personalizados para que los dispositivos puedan asociar propiedades adicionales a estos objetos. Estas propiedades se pueden usar para crear grupos o distribuir configuraciones.
    - **Eliminar**: el perfil predeterminado no se puede eliminar. Cuando se elimina un perfil no predeterminado, todos los dispositivos asociados se reasignan al perfil predeterminado.
6. Para trasladar un dispositivo inscrito de un perfil a otro dentro del mismo servidor virtual (y no entre diferentes servidores de Apple Business Manager), haga clic en el enlace numérico que hay en la columna Número de dispositivos. La reasignación de perfiles es aplicable a los dispositivos que aún no se han inscrito.
    1. Para mover un solo dispositivo, haga clic en **Asignar perfil de inscripción** para el dispositivo específico, seleccione el perfil de la lista desplegable y haga clic en **Asignar**.
    2. Para mover varios dispositivos, selecciónelos y haga clic en **Acciones**> **Asignar perfil de inscripción**, seleccione el perfil de la lista desplegable y haga clic en **Asignar**.

- Si se edita un perfil de Inscripción de dispositivos, el recuento de dispositivos del perfil modificado se actualizará en breve.
- Si actualiza el token del servidor en el sitio de Apple, el token existente quedará invalidado. No obstante la pantalla de la página de la Inscripción de dispositivos (incluida la fecha de caducidad del token) se mantendrán hasta que cargue el token nuevo.

Añadir una página web de inscripción de dispositivos personalizada

Aplicable a: iOS 13.0 y macOS 10.15 y versiones más recientes compatibles

En la sección de Inscripción personalizada, puede especificar su propia página web personalizada (vista web) para autenticar a los usuarios durante la Inscripción de dispositivos. Utilice esta página para mostrar información personalizada como el tipo de autenticación, la personalización de marca, el texto de consentimiento y la política de privacidad.

Procedimiento

1. Vaya a **Administración** > **Apple** > **Inscripción de dispositivos.**
2. Encuentre el nombre del servidor que creó en el sitio de Apple.
3. Seleccione **Acciones** > **Editar perfil de Inscripción de dispositivos.**
4. En la sección Inscripción personalizada, seleccione **Activar la inscripción personalizada**.
5. Seleccione una de las siguientes opciones:
    - **Página web alojada por MobileIron**: redirigida a un proveedor de identidad (IDP) si la inscripción usa un proveedor de identidad como los Servicios de federación de Active Directory de Microsoft (ADFS) u Okta. También se puede redirigir al portal de autoservicio para un usuario de Ivanti Neurons for MDM con una autenticación no basada en la identificación.

- **URL personalizada**: introduzca una URL como https://mycustomweburl.com. Esta URL define el valor de la URL personalizada que se presentará al usuario en una vista web cargada durante la configuración inicial de un nuevo dispositivo de la Inscripción de dispositivos o de un dispositivo borrado. Utilice este campo para definir su propia interfaz de autenticación con el método de autenticación. Después de que el usuario se autentique, se descargará el perfil de inscripción de MDM.

Proceso de trabajo de la página web de inscripción de dispositivos personalizada

En esta sección se explica el comportamiento de la página web de Inscripción de dispositivos personalizada y el procedimiento para crear la página web personalizada (vista web).

Cuando la página web personalizada especificada en el campo de la **URL** se cargue inicialmente:

- La URL web de configuración tiene un esquema **https** y es una solicitud **GET**. La página web debe utilizar un certificado de confianza pública.
- Se agrega un encabezado personalizado **x-apple-aspen-deviceinfo** a la solicitud GET del dispositivo Apple en el cual se realiza la inscripción. Este contiene una codificación base64 de un sobre CMS (Cryptographic Message Syntax) que contiene un plist con atributos de dispositivo. Esta es la misma información, en el mismo formato, que la proporcionada en la solicitud POST inicial con las inscripciones de dispositivos basados en tokens.

Cuando la página web personalizada se carga posteriormente:

- El usuario del dispositivo interactúa con la página web (vista web) hasta que el servidor host del administrador proporciona un archivo **custom.mobileconfig** al cliente. El servidor Ivanti Neurons for MDM devuelve el código de bytes del perfil MDM. En el servidor host del administrador, el archivo custom.mobileconfig debe ser configurado con un tipo MIME de **application/x-apple-aspen-config** para que el perfil MDM del dispositivo se descargue e instale en el dispositivo.
- Para la autenticación con Ivanti Neurons for MDM, la página web debe contener las credenciales de nombre de usuario y contraseña de autenticación. Se recomienda crear un usuario separado en Ivanti Neurons for MDM y asignar la función de Inscripción personalizada al usuario que obtiene el perfil de MDM con la URL del servidor Ivanti Neurons for MDM (por ejemplo, https://micloudDomain.com/c/i/dep/custom.mobileconfig).
- Para el registro del dispositivo y para obtener el perfil MDM de Ivanti Neurons for MDM, el servidor web del host del administrador debe hacer una llamada POST a la URL del servidor Ivanti Neurons for MDM. También debe pasar el encabezado x-apple-aspen-deviceinfo con el valor proporcionado por el dispositivo cuando el dispositivo acceda a la URL GET para cargar la página web personalizada. Si no se proporciona la Id. de usuario de registro, el dispositivo se registrará en el usuario «nadie». Estos son los detalles adicionales:
  - Cuando un dispositivo accede a la URL web personalizada configurada en el perfil de Inscripción de dispositivos, el servidor web del host del administrador debe capturar el encabezado "x-apple-aspen-deviceinfo" presentado por el dispositivo.
  - Para obtener el perfil MDM de ese dispositivo y su usuario relacionado, el servidor web del host del administrador debe hacer una llamada POST a la URL del servidor Ivanti Neurons for MDM con el encabezado x-apple-aspen-deviceinfo. Este debe contener una autenticación básica que utilice el ID de usuario Ivanti Neurons for MDM como parámetro de la solicitud (por ejemplo, https://miCloudDomain.com/c/i/dep/custom.mobileconfig?user=name@company.com). Al usuario se le debe asignar la función de Inscripción personalizada.
  - Una vez que el servidor web del host del administrador reciba el código de bytes, debería descargar el código de bytes al dispositivo estableciendo encabezados de respuesta, Content-Disposition = attachment;filename="profile.mobileconfig" and Content-Type = application/x-apple-aspen-config.
- La vista web se cerrará y el sistema operativo intentará instalar el perfil, que debe ser un perfil de inscripción de MDM.

> Ivanti Neurons for MDM no autentica la Id. de usuario para la que se devuelve el perfil de MDM. Por lo tanto, los administradores deben realizar la autenticación necesaria para la Id. del usuario antes de solicitar el perfil de MDM.

En el caso de iOS, este proceso de trabajo es compatible con la configuración inicial de un dispositivo borrado. En el caso de macOS, este proceso de trabajo es compatible tanto en el Asistente de configuración como a través del panel de preferencias de Perfiles, si se omitió la Inscripción de dispositivos durante el Asistente de configuración.

Para obtener información del desarrollador relacionada con la creación de una página web personalizada, consulte las siguientes referencias de documentación de Apple:

- **Vistas web**
- **Autenticación mediante vistas web**
- **Código de muestra para implementar un simple navegador web para iPad que pueda ver tanto la versión de sobremesa como la móvil de un sitio web**

Edición del ajuste de autenticación en la Inscripción de dispositivos

Procedimiento

1. Vaya a **Administración** > **Apple** > **Inscripción de dispositivos.**
2. Encuentre el nombre del servidor que creó en el sitio de Apple.
3. Seleccione **Acciones**>**Editar autenticación**.

Gestión de tokens de arranque para cuentas móviles

Aplicable a: dispositivos macOS 10.15 y versiones posteriores compatibles que sean dispositivos inscritos en MDM mediante Apple School Manager o Apple Business Manager.

Ivanti Neurons for MDM admite la administración del token de Bootstrap para cuentas móviles. Los tokens de arranque permiten que las cuentas móviles se conecten a los dispositivos MacOS que utilizan FileVault. Con esta función, todas las cuentas móviles que se conectan obtienen un SecureToken automáticamente. Esta función es útil cuando varios usuarios se conectan a un equipo codificado.

Cuando una cuenta del administrador gestionada intenta acceder a un dispositivo:

- La primera vez que se inicia sesión, se solicita el token de arranque del servidor MDM.
- Si el servidor MDM proporciona el token de arranque, el dispositivo creará automáticamente un SecureToken para la cuenta.
- El dispositivo habilita el FileVault para el usuario.

El campo «Token de arranque disponible» está disponible en la página de detalles del dispositivo y como atributo de filtro al crear un nuevo grupo de dispositivos o una política personalizada.

Para la solución de problemas y la verificación, vaya a la página de detalles de un dispositivo. Utilice la página de registros para reducir los registros del dispositivo mediante filtros basados en los nombres de las acciones «Definir token de arranque» y «Obtener Token de arranque».

Configurar una cuenta del administrador macOS administrada con la Inscripción de dispositivos

Ivanti Neurons for MDM admite el registro en la Inscripción de dispositivos en dispositivos que se han restablecido a los valores de fábrica o que se están activando por primera vez. Con la Inscripción de dispositivos, se puede crear una cuenta del administrador en el dispositivo macOS. Ivanti Neurons for MDM solo es compatible con la inscripción opcional para macOSIvanti Neurons for MDM y, por lo tanto, ignora el campo **MDM obligatoria** en el perfil de Inscripción de dispositivos, ya que solamente se aplica a los dispositivos iOS.

Procedimiento

1. Vaya a **Administrador > Apple > Inscripción de dispositivos**.
2. Encuentre el nombre del servidor que creó en el sitio de Apple.
3. Seleccione **Acciones > Editar perfil de Inscripción de dispositivos**.
4. Seleccione una de las siguientes opciones de las opciones del asistente de configuración de la cuenta macOS:
    - **Omitir creación de la cuenta de administrador**: seleccione esta opción para anular la creación de una cuenta de administrador, ya sea visible u oculta. Deseleccione esta opción para permitir la creación de una cuenta de administrador en la sección **Configurar cuenta del administrador macOS administrada** (descrita más abajo).
    - **Omitir creación de la cuenta de configuración principal**: seleccione esta opción para omitir la configuración de una cuenta principal en el dispositivo macOS. Además de la cuenta del administrador, no se crea ninguna cuenta de usuario. Aparecerá una sección adicional, **Configurar cuenta del administrador macOS administrada**, (descrita a continuación) para crear la cuenta de administrador de macOS administrada. La cuenta también se puede ocultar de los Usuarios y Grupos.
    - **Crear cuentas principales como usuarios usuales (como administrador si no se selecciona)**: seleccione esta opción para crear una cuenta estándar que no sea de administrador como parte de la inscripción. El administrador podrá crear todos modos una cuenta de administrador e insertarla en el dispositivo. Aparecerá una sección adicional, **Configurar cuenta del administrador macOS administrada**, (descrita a continuación) para crear la cuenta de administrador de macOS administrada. La cuenta también se puede ocultar de los Usuarios y Grupos.

Después de seleccionar una de las opciones anteriores, introduzca los siguientes detalles de la sección **Configurar cuenta del administrador macOS administrada** si desea crear una cuenta de administrador macOS administrada:

- Nombre completo
- Nombre de la cuenta
- Contraseña
- Confirmar contraseña
- (Opcional) Ocultar cuenta del administrador administrada en Usuarios y grupos

Si no selecciona **Omitir creación de la cuenta de configuración principal**, introduzca los siguientes detalles en la sección **Configurar cuenta principal** . Esto añade soporte de canal de usuario para la cuenta de administrador administrada, estableciendo el nombre breve del usuario local administrado como el nombre breve del administrador.

- **Nombre completo**
- **Nombre breve**
- (Opcional) **Evitar la modificación por parte del usuario final**: esta configuración se anulará si el nombre completo y/o el nombre breve tienen variables de sustitución y se evalúan como vacíos. Si selecciona esta opción, confirme que entiende que esta configuración de cuenta de administrador principal es aplicable solo si una de las siguientes opciones está configurada adecuadamente:
    1. Se ha seleccionado la opción «Solicitar al usuario que se registre/inicie sesión» en la vista de configuración de Authentication.

2. La página web alojada en MobileIron es seleccionada para la personalización de la inscripción.

7. Seleccione **Omitir creación de la cuenta de configuración principal** para habilitar la compatibilidad del canal del usuario para la cuenta del administrador gestionada. Puede establecer el nombre breve del usuario local administrado como el nombre breve de un administrador.
8. Haga clic en **Guardar**.

Cambiar la contraseña local de la cuenta del administrador de macOS

El administrador puede cambiar la contraseña local de una cuenta de administrador de macOS que se haya creado mediante el Asistente de configuración durante la Inscripción de dispositivos.

Aplicable a: macOS 10.11 o versiones más recientes compatibles.

Procedimiento

1. Vaya a **Dispositivos**.
2. Haga clic en el nombre de usuario con el que está asociado el dispositivo para ver la página de detalles del dispositivo.
3. Desde el menú Acciones, haga clic en **Establecer contraseña del Administrador macOS**. Esta acción también se puede realizar en la página de la lista de dispositivos seleccionando uno o más dispositivos.
4. Introduzca la contraseña.
5. Haga clic en **Guardar**.

Exportar a CSV

Ivanti Neurons for MDM le permite exportar los dispositivos inscritos del dispositivo a un archivo CSV.

Procedimiento

1. Vaya a **Administración** > **Apple** > **Inscripción de dispositivos.**
2. Haga clic en el enlace de número de dispositivos específicos de la columna **Número de dispositivos**.
3. Haga clic en la opción **Exportar a CSV** para exportar la lista de dispositivos y detalles relacionados a un archivo CSV. Cuando el informe está listo, recibirá un mensaje que le indicará que debe descargar o eliminar el informe. Usted también recibirá un correo electrónico con un enlace para descargar el informe.
4. Haga clic en **Descargar**.
5. (Opcional) Haga clic en **Eliminar** para eliminar el informe.

12.3.4. Inscripción Beta

Ivanti Neurons for MDM puede inscribir automáticamente dispositivos de forma remota en un momento posterior si el dispositivo está supervisado y ejecuta iOS 18, iPadOS 18, macOS 15 o posterior. Si es necesario, se puede eliminar un dispositivo supervisado de los programas beta y restringir que un usuario se inscriba manualmente. Esto elimina la necesidad de que el usuario realice pasos manuales y permite un proceso optimizado durante todo el ciclo de vida de las pruebas beta.

Requisitos previos

- La inscripción del dispositivo es obligatoria para la inscripción Beta. Para obtener más información sobre la inscripción de dispositivos, consulte **Inscripción de dispositivos**.
- Para ofrecer versiones beta de AppleSeed para TI sin la necesidad de una cuenta Apple, un administrador en Apple Business Manager o Apple School Manager debe iniciar sesión en el portal de AppleSeed para TI y aceptar los términos y condiciones en nombre de su organización para el período beta actual.

Conectando Ivanti Neurons for MDM a la inscripción Beta

Para utilizar Ivanti Neurons for MDM como servidor MDM para la inscripción Beta, configure el token del servidor de Apple Business Manager o Apple School Manager en Ivanti Neurons for MDM.

Sección de inscripción beta

Nombre	Descripción
Nombre de la organización	Nombre de la organización.
Última sincronización	Fecha y hora en que se realizó la sincronización.
Estado	Estado de la sincronización.
Sincronización de tokens de inscripción beta	Haga clic en **Sincronización** para sincronizar los tokens de inscripción beta recientemente disponibles para actualizaciones beta.

12.3.5. Configuración del asistente de configuración

El Asistente de configuración le permite seleccionar las pantallas de configuración que desee omitir o incluir durante la configuración del dispositivo para dispositivos iOS y macOS.

Procedimiento

1. Iniciar sesión en la consola administrativa de Ivanti Neurons for MDM.
2. Vaya a **Configuraciones**.
3. Seleccione **Asistente de configuración**.
4. Haga clic en el icono del lápiz (editar).
5. Seleccione las casillas para omitir las pantallas de configuración específicas del dispositivo.
6. Haga clic en **Hecho**.
7. Seleccione **Canal de dispositivo**.
8. Seleccione **Todos los dispositivos**. La configuración de Asistente de configuración se envía a los dispositivos y la pestaña Configuración de la página Detalles del dispositivo muestra el estado Instalado.
9. Iniciar sesión en el dispositivo. Se omiten todas las pantallas de configuración iniciales.

12.3.6. Instalación del Certificado MDM

Debe solicitar e instalar un certificado MDM de Apple para administrar los dispositivos iOS. También tendrá que renovar este certificado una vez al año. (La cuenta de Apple que se usó para crear el certificado recibe una notificación de la web de Apple cuando se acerca la fecha de caducidad). Utilice la página Certificado de MDM para agregar o renovar este certificado.

Adquirir e instalar el certificado MDM

Procedimiento

1. Utilice la página **Certificado MDM** para descargar una solicitud de firma de certificados (CSR) desde el abonado su Ivanti Neurons for MDM.
2. Cargue el CSR en Apple para crear un certificado nuevo.
3. En el sitio de Apple, añada una nota indicando para qué es el certificado. Esta nota le resultará útil cuando sea el momento de renovarlo.
   Guarde el certificado resultante.
4. Instale el certificado de su abonado de Ivanti Neurons for MDM.

Renovar el certificado MDM

Procedimiento

1. Haga clic en **Renovar certificado**.
2. Descargue una solicitud de firma de certificado (CSR) de su abonado de Ivanti Neurons for MDM.
3. Cargue el CSR en Apple para renovar el certificado correspondiente.
4. En el sitio de Apple, asegúrese de estar renovando el certificado correcto. Al cargar un certificado diferente en Ivanti Neurons for MDM se retirarán automáticamente todos los dispositivos iOS registrados.
   Instale el certificado de su abonado de Ivanti Neurons for MDM.

Recibirá una advertencia si intenta cargar el certificado incorrecto.

Si no puede ver la página **Instalar certificado de MDM**, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:

- Administración del sistema
- Sistema de solo lectura

12.3.7. Dispositivos iPad compartidos para empresas

Los iPad compartidos para empresa están disponibles para las ID administradas de Apple que se creen en Apple Business Manager con iOS 13.4 o versiones compatibles más recientes.

- Los iPad compartidos permiten a las empresas compartir dispositivos entre varios empleados, sin dejar de ofrecer una experiencia personalizada.
- Los empleados pueden iniciar sesión con una ID de Apple administrada para empezar a cargar sus datos, incluidas sus cuentas de correo electrónico, archivos, la biblioteca de iCloud Photo, los datos de aplicaciones y más.
- Los datos se almacenan en iCloud, de manera que los empleados puedan iniciar sesión en los iPad compartidos propiedad de la empresa.

Los iPad compartidos se pueden usar en aplicaciones para sanidad, ventas e industria. Por ejemplo, doctores y enfermeras pueden compartir un iPad, ya que pueden acceder de manera segura al perfil de usuario único diseñado para ellos. En las tiendas de venta al por menor, se puede facultar a los trabajadores de primera línea para que tengan acceso a la información sobre los productos, los recursos y los conocimientos especializados para ayudar a los clientes y ofrecerles mejores experiencias de compra.

Cómo funciona

- Los dispositivos para iPad se agregan a Apple Business Manager y se inscriben mediante un perfil de inscripción automatizado con el modo compartido encendido.
- Los empleados inician sesión en el iPad compartido con una ID de Apple administrada y una contraseña que proporciona la empresa. El administrador de Apple Business Manager puede crear manualmente las cuentas para los usuarios o federar la creación de cuentas a un proveedor de identidades como Entra ID.
- Cada usuario puede tener su perfil personalizado cuando inicia sesión en el iPad compartido. Los administradores pueden distribuir aplicaciones basándose en roles de usuario, responsabilidades y departamento.
- Los usuarios pueden iniciar sesión como usuarios invitados en un iPad compartido. El inicio de sesión del usuario invitado está habilitado por defecto. Un usuario invitado no necesita iniciar sesión con una ID de Apple administrada ni una contraseña. El inicio de sesión del usuario invitado se puede deshabilitar si se selecciona la opción **Permitir la sesión de invitado para iPad compartido** como **Falso** en la configuración de **Restricciones de iOS**.
- Vaya a Ivanti Neurons for MDM **> Dispositivos**, haga clic en el nombre del iPad compartido y haga clic en la pestaña **Usuarios** para ver la lista de usuarios del dispositivo y sus detalles (como la ID de Apple administrada, los Datos disponibles en bytes, los Datos usados en bytes, Tiene datos que sincronizar con Ivanti Neurons for MDM).
- Vaya a la pestaña **Registros**, desde los filtros, seleccione la acción **Notificar lista de usuario** para ver detalles adicionales del usuario.
- El inicio de sesión del usuario invitado de un iPad compartido es distinto al de la administración del usuario invitado de Ivanti Neurons for MDM. Por defecto, la cuenta de usuario invitado está desactivada en Ivanti Neurons for MDM. Para administrar un usuario invitado en un iPad compartido, habilite la cuenta del usuario invitado.
- La grabación de pantalla está disponible desde el Centro de control en los dispositivos de iPad compartidos.
- Ivanti Neurons for MDM admite una variable de sustitución para el ID de Apple gestionado, `${managedAppleID}`. Esta variable del sistema se muestra en la sección de atributos del sistema y en la sección de atributos del dispositivo.
- Ivanti Neurons for MDM Restringe que un administrador cambie la ID de Apple administrada de los usuarios residentes que se iniciaron registrado en el dispositivo de iPad compartido en el pasado junto con los usuarios iniciados actualmente. Si intenta cambiar la ID de Apple administrada, un mensaje de error indica que la ID de Apple administrada del usuario no se puede cambiar puesto que el usuario utiliza un iPad compartido.

- En el caso de las **Aplicaciones y libros de Apple**, las aplicaciones y los libros se instalan en dispositivos de iPad compartidos basados en licencias basadas en dispositivos, independientemente de si las licencias basadas en dispositivos se seleccionan o no.

Requisitos previos

Asegúrese de que se cumplan los siguientes requisitos previos:

- Un iPad compartido requiere una ID de Apple administrada. Los administradores pueden crear las cuentas manualmente o federarlas a un proveedor de identidades como Entra ID.
- Los iPad compartidos deben tener la versión iOS 13.4 o ser compatibles con versiones más nuevas.
- Los dispositivos deben estar asociados con cuentas de Apple Business Manager.
- Los dispositivos deben contener un almacenamiento de 32 GB o más.

Tenga en cuenta los puntos siguientes:

- Ivanti Neurons for MDM evita determinadas configuraciones, como Código de acceso, para los iPad compartidos, puesto que Apple no es compatible con ellas. Estas configuraciones no se insertan en los dispositivos (Dispositivos > haga clic en el enlace del nombre de un dispositivo > pestaña Configuraciones).
- La configuración de **Código de acceso** no se aplica a los dispositivos de iPad compartidos, puesto que requieren ID de Apple administradas, que se asocian con las contraseñas, no con códigos de acceso. La acción Desbloquear del portal administrativo de Ivanti Neurons for MDM no borrará el código de acceso de un iPad compartido.
- Seleccione el canal del dispositivo o el canal de usuario durante la distribución de la **Configuración de restricciones iOS** a dispositivos de iPad compartidos. Puede distribuir configuraciones separadas e implementar restricciones que solo se aplican al dispositivo o al canal de usuario.
- Ivanti Neurons for MDM verifica las cuentas caducadas y retira los dispositivos con propietarios que son cuentas caducadas. No obstante, para un iPad compartido, el propietario del dispositivo es el último usuario que ha iniciado sesión pero puede que no sea el propietario legal. Si caduca la cuenta de un propietario, Ivanti Neurons for MDM excluye los iPad compartidos de su retirada.
- Go para el cliente de iOS no es compatible para los iPad compartidos.
- Los usuarios no pueden llevar a cabo acciones como retirar y borrar en los iPad compartidos. Solo los administradores pueden llevar a cabo acciones de retirada y borrado desde el portal administrativo de Ivanti Neurons for MDM.
- Los administradores no pueden cambiar el propietario del iPad compartido desde el portal administrativo de Ivanti Neurons for MDM.
- Cero Sign-On no es compatible con dispositivos de iPad compartidos.
- Cuando se habilita el comando ListUsers, todas la ID de usuarios administradas y su hora de conexión se muestran en la Inscripción de dispositivos (parte de Apple Business Manager) en la pestaña **Admin**.

Configurar un iPad compartido

Puede ajustar un iPad compartido y configurar los ajustes.

Procedimiento

1. Vaya a **Administración** > **Apple** > **Inscripción de dispositivos.**

2. Añada el dispositivo a Apple Business Manager inscribiéndolo mediante un perfil de inscripción de dispositivos automatizado. Para obtener información sobre este procedimiento, consulte **Inscripción de dispositivos**.
3. En los ajustes de Inscripción de dispositivos, active:
    - **Modo supervisado**.
    - **Modo multiusuario** en **iPad compartido para empresa**.
4. (Opcional) Cree una cuenta de usuario local. El dispositivo se registrará para este usuario. La autenticación, ya que este usuario solo aparece una vez durante el registro.
5. Restablecer el iPad compartido.

> El proceso de registro se inicia solo después del reinicio. El dispositivo tarda unos minutos en registrarse y configurarse como iPad compartido.

6. El propietario legal se asigna a la cuenta de usuario que registró el dispositivo. El administrador puede cambiar el propietario legal desde la página **Dispositivos**.
7. En la pantalla de inicio de sesión del dispositivo, introduzca las credenciales de ID de Apple administrada del usuario.
    - De manera similar a los dispositivos de macOS, puede enviar las configuraciones de iPad compartidos a través del dispositivo o de los canales de usuario.
    - Las variables de sustitución de usuarios no se sustituyen en las configuraciones (incluida la configuración de aplicaciones administradas) que se envían en el canal del dispositivo.
    - Si el usuario activo de un iPad compartido no es un usuario administrado, la ID de Apple administrada no pertenece a ningún usuario del portal administrativo de Ivanti Neurons for MDM, el dispositivo no se asignará a nadie. Los usuario no estarán administrados: el administrador no puede enviar configuraciones del canal del usuario desde Ivanti Neurons for MDM.
    - Por defecto, el usuario invitado predeterminado creado por Ivanti Neurons for MDM está desactivado. Cuando un usuario invitado inicia sesión, el dispositivo no se asigna a ningún usuario y el usuario no se administra. Si el usuario invitado se debe administrar, el usuario invitado predeterminado creado por Ivanti Neurons for MDM debe estar habilitado y el dispositivo se debe asignar al usuario invitado predeterminado después de que el usuario invitado inicie sesión. A continuación, se puede administrar el usuario.
    - La información del propietario del dispositivo se muestra en la página Ivanti Neurons for MDM > **Dispositivos** y en los registros de dispositivos (página de detalles del dispositivo > **Registros**).

Gestionar los propietarios legales de los iPad compartidos

Usted busca y visualiza los propietarios legales de los iPad compartidos mediante sus ID de correo electrónico desde la página del listado del dispositivo. Puede cambiar los propietarios legales de los iPad compartidos mediante la reasignación de los propietarios legales existentes a los nuevos propietarios legales. Si se reasigna el propietario legal de un iPad no compartido, Ivanti Neurons for MDM ignora la asignación.

Procedimiento

1. Vaya a **Dispositivos**.
2. Haga clic en el icono del engranaje y agregue la columna **Propietario legal** a la página de la lista de dispositivos.
3. Seleccione los iPad compartidos.
4. Haga clic en **Acciones > Asignar al propietario legal**.

Enviar un correo electrónico al propietario legal de un dispositivo de iPad compartido

Puede enviar correos electrónicos al propietario legal de un iPad compartido.

Procedimiento

1. Vaya a **Dispositivos**.
2. Haga clic en el nombre del iPad compartido.
3. Haga clic en el icono del **correo electrónico**.
4. Escriba el correo electrónico.
5. Haga clic en **Enviar**.

Uso del atributo del modo multiusuario

Puede usar el atributo Modo multiusuario de los iPad compartidos en Ivanti Neurons for MDM.

Procedimiento

1. En la página **Dispositivos**, use el atributo **Modo multiusuario**.
2. Haga clic en **Búsqueda avanzada** y cree una regla para encontrar los dispositivos que usan el atributo **Modo multiusuario**.
3. En la página **Dispositivos > Grupos de dispositivos**, cree un grupo de dispositivos dinámicos para los iPad compartidos mediante el atributo **Modo multiusuario**. Por ejemplo, se puede utilizar este grupo como filtro de distribución para distribuir las configuraciones.
4. En la página **Políticas**, cree una política personalizada para los iPad compartidos mediante el atributo **Modo multiusuario**.
5. En **Aplicaciones > Filtro de distribución**, use el atributo **Modo multiusuario** para limitar el número de aplicaciones disponibles para su instalación.

- Ivanti Neurons for MDM no es compatible con el modo multiusuario para los dispositivos Apple School Manager. No se recomienda activar el ajuste e insertar el perfil de Inscripción de dispositivos a los dispositivos de Apple School Manager.
- La configuración de Inicio de sesión segura de múltiples usuarios no se aplica a los iPad compartidos.

Eliminar usuarios de un iPad compartido

Puede eliminar una o varias cuentas de usuarios desde los iPad compartidos. En la pestaña Lista de usuarios, la etiqueta **Activo** se muestra para el usuario activo actualmente. La opción Eliminar no se puede aplicar al usuario que ha iniciado sesión en estos momentos en el iPad compartido. Los usuarios pueden eliminarse desde los **Dispositivos** o desde la pestaña **Usuarios**.

Eliminar usuarios desde la pestaña Dispositivos

Procedimiento

1. Vaya a la pestaña **Dispositivos** > **Detalles del dispositivo**.
2. Vaya a la pestaña **Usuarios**. Se muestra la lista de usuarios.
3. Haga clic en **Eliminar todos los usuarios**.
4. Haga clic en el signo menos "**-**" para eliminar usuarios específicos.

- (Opcional) En la ventana **Eliminar usuario**, seleccione la opción **Forzar la eliminación del usuario aunque esté pendiente la sincronización de los datos se hayan sincronizado con Ivanti Neurons for MDM** y haga clic en **Sí**.

  > Seleccionar **Forzar Eliminar usuario aunque esté pendiente la sincronización de datos con Ivanti Neurons for MDM** forzará la eliminación del usuario aunque los datos no se hayan sincronizado aun con el portal administrativo de Ivanti Neurons for MDM.

Eliminar usuarios desde la pestaña Usuarios

Procedimiento

1. Vaya a la pestaña **Usuarios**.
2. Seleccione un usuario o varios, vaya al menú desplegable de **Acciones**, haga clic en **Eliminar**. Aparece un mensaje de confirmación. Después de confirmar, se emite el comando de eliminar usuario en los dispositivos.
3. Vaya a **Registros del dispositivo** en los detalles del dispositivo y verifique que el comando Eliminar usuarios se envía a los usuarios seleccionados del iPad compartido.

Iniciar sesión a los usuarios desde un dispositivo de iPad compartido

El administrador puede cerrar las sesiones de los usuarios de un iPad compartido.

Procedimiento

1. En la página **Dispositivos**, seleccione un iPad compartido.
2. Seleccionar **Forzar Cierre de Sesión** del menú **Acciones**. Una solicitud emergente solicita la confirmación sobre la sesión de usuarios de registro del dispositivo de iPad compartido.
3. Haga clic en **OK** para forzar el cierre de sesión.

12.3.8. Director de la escuela

Licencia: Gold

Aplicable a: iOS 9.3+ supervisado

Apple School Manager es un servicio en la nube de Apple destinado a las instituciones educativas para brindarles servicios, incluida la compra de aplicaciones en Apps y libros de Apple, la inscripción de iPad a través de la inscripción de dispositivos de Apple y la creación de identificaciones de Apple administradas. Con la completa integración con Apple School Manager, la Ivanti Neurons for MDMsolución de UEM proporciona una forma de administrar completamente y sin interrupciones los iPads destinados a profesores y a estudiantes, con el fin de sacar provecho del ecosistema de School Manager y de las aplicaciones tales como Classroom.

> Apple Books no es compatible.

Configuración de School Manager

1. Vaya a **Administrador > School Manager**.
2. Haga clic en la opción **Configurar Education** si está desactivada.
3. Seleccione una de las siguientes opciones:
   - **Sincronice con la cuenta de Apple School Manager para importar información de la escuela**:
     1. Vaya a **Administrador > Apple > Inscripción de dispositivos** para descargar los archivos clave de su organización.
     2. Cargue los archivos a su cuenta de Apple School Manager para generar sus claves de cifrado.
     3. Descargue las claves de cifrado de Apple School Manager y cargue las claves en Ivanti Neurons for MDM (**Administración > Apple > Inscripción de dispositivos**).

        > Las cuentas existentes del programa de inscripción de dispositivos de Apple se pueden reutilizar para Apple Education. Apple le dará la opción de actualizar su cuenta de Inscripción de dispositivos para incluir funciones de Education cuando acceda a Apple School Manager. Para ver las instrucciones sobre cómo actualizar, visite https://support.apple.com/en-in/HT206960.

     Cuando se acepten las claves de cifrado, aparecerá el botón **Sincronizar ahora**.

     4. Haga clic en **Sincronizar ahora** para comenzar a sincronizar los datos con Apple School Manager.
   - **Importe datos desde archivos CSV**:
     1. Haga clic (opcional) en **Descargar archivo ZIP de plantillas CSV** para descargar un archivo zip que contiene plantillas de todos los tipos de archivo.
     2. Haga clic en **Seleccionar archivos**...
     3. Añada los siguientes seis archivos CSV:
        - Archivo de datos de los alumnos (students.csv)
        - Archivo de datos de la lista (roster.csv)
        - Archivo de datos del personal (staff.csv)
        - Archivo de datos de las clases (classes.csv)

- Archivo de datos de los cursos (courses.csv)
- Archivo de datos de las localizaciones (locations.csv)

> Debe seleccionar los seis archivos CSV juntos cada vez antes de cargarlos.

Haga clic en **Cargar**.

4. (Opcional) Si los archivos CSV tienen que modificarse, conserve todos los datos necesarios en los seis archivos que se cargaron previamente. Haga las modificaciones necesarias y vuelva a cargarlos de nuevo.

Busque los datos desde la pestaña **Clases** e **Individuos**.

> Los individuos (estudiantes y personal) también aparecen en la página **Usuarios** de Ivanti Neurons for MDM.

5. Cree dos grupos de dispositivos para dispositivos que se usarán para la educación de estudiantes y de personal, tal y como se indica a continuación:
   1. Vaya a **Administrador > Atributos personalizados**.
   2. Cree atributos personalizados para los alumnos y el personal que vayan a usarse para crear grupos de dispositivos administrados dinámicamente.
   3. Vaya a **Dispositivos > Grupos de dispositivos**.
   4. Haga clic en **Añadir+**.
   5. Vaya creando los grupos de dispositivos administrados dinámicamente para alumnos y personal utilizando los atributos personalizados creados previamente como filtros.
6. Asigne los dispositivos registrados a los alumnos y el personal desde la página **Dispositivos** utilizando la opción **Acciones > Asignar al usuario**.
7. Cree una configuración para Líderes (personal) y Miembros (alumnos) añadiendo las cargas útiles en **Configuraciones > Education**.
8. Distribuya las configuraciones para Líderes (personal) y Miembros (alumnos) a los grupos de dispositivos del personal y los alumnos.
   Esta distribución insertará las configuraciones e instalará los certificados en los dispositivos respectivos.

> En la página de **Administración > School Manager**, si no hay ningún valor para el nombre de la clase, se derivará del identificador de la fuente del sistema de clases y de los campos del identificador del curso. Estos campos son opcionales en Apple School Manager o el archivo CSV. No obstante, se recomienda introducir siempre un valor, ya que esta combinación se utiliza como identificador predeterminado cuando no hay ningún Nombre de clase.

Insertar la aplicación Classroom para los profesores

Con la aplicación Classroom, los profesores (Líderes) pueden gestionar las siguientes situaciones:

- La capacidad de gestionar Classroom para controlar los iPad y las aplicaciones de forma remota.
- La capacidad de crear un grupo de clase.
- La capacidad de un profesor para ver los alumnos miembros de ese grupo.
- La capacidad de un profesor para enviar contenido a los alumnos en ese grupo.
- Restringir qué aplicaciones y contenido pueden ver los alumnos.

Puede enviar la aplicación de Aula desde la tienda de aplicaciones de Apple.

Procedimiento

1. Vaya a la página **Aplicaciones > App Catalog**.
2. Haga clic en el botón **+Agregar**.
3. Busque y seleccione la aplicación Classroom de Apple.
4. Haga clic en **Siguiente**.
5. Introduzca la categoría y la descripción.
6. Haga clic en **Siguiente**.
7. Distribuya la aplicación en el grupo de dispositivos de los profesores que había creado previamente.
8. Configure los ajustes de la aplicación en la página Configuraciones de aplicaciones.
9. Haga clic en **Hecho**.

Desactivar School Manager

Si se desactiva School Manager, se borrarán todos los datos actuales. Tenga cuidado al hacerlo.

1. Vaya a **Administrador > School Manager**.
2. Haga clic en la opción **Configurar Education** si está activada.
3. Haga clic en **Sí**.

12.3.9. Ajustes (Apple)

Los administradores pueden configurar, activar y desactivar diferentes ajustes de los dispositivos Apple.

Registro silencioso (solo para macOS)

El registro silencioso para dispositivos macOS está bloqueado en Habilitado. Esto afecta a los registros de todos los dispositivos nuevos del abonado y es compatible con Mobile@Work 1.4 y versiones más recientes compatibles.

Ajustes generales

Desactivar conciliación de dispositivo: ahora los administradores pueden conservar las entradas del dispositivo si desean registrar el mismo dispositivo de nuevo. Esta opción no está seleccionada de forma predeterminada. Seleccione esta opción para conservar los detalles del dispositivo inactivo.

> Cuando Deshabilitar conciliación de dispositivo no está habilitado, y si se vuelve a registrar un dispositivo con el mismo usuario, se creará una nueva entrada. De lo contrario, la entrada del dispositivo se actualizará con nueva información de registro.

Ajustes del perfil

Los administradores pueden activar o desactivar el envío de correos electrónicos a los usuarios finales y notificaciones a los clientes de macOS y Go for iOS si el perfil de MDM no está instalado. La característica de notificaciones del perfil de MDM está activada de forma predeterminada.

Procedimiento

1. Vaya a **Admin. > Ajustes**.
2. Seleccione o deseleccione la opción **Enviar correo electrónico al usuario y notificación al cliente si el perfil de MDM no está instalado**.
3. Seleccione el máximo número de correo electrónicos y notificaciones entre 1 y 4.
4. Haga clic en **Guardar**.

Actualizaciones del sistema operativo para la inscripción automatizada de dispositivos (solo iOS)

Los administradores pueden activar las actualizaciones del sistema operativo iOS para la inscripción automatizada de dispositivos. Si esta opción está activada, los dispositivos de la Inscripción de dispositivos usarán la configuración de **Actualizaciones de software** en lugar del ajuste de actualización del sistema operativo programado en el perfil de Inscripción de dispositivos.

Esta opción está desactivada por defecto, en cuyo caso se utiliza el ajuste de programar la actualización del sistema operativo en el perfil de Inscripción de dispositivos. La activación de este ajuste es permanente y no se puede desactivar. Este ajuste eliminará el ajuste de la actualización del SO programada en todos los perfiles disponibles de Inscripción de dispositivos.

> Los dispositivos supervisados que no sean de la Inscripción de dispositivos utilizan la configuración de las Actualizaciones de software.

Procedimiento

1. Vaya a **Admin. > Ajustes**.
2. Seleccione o deseleccione la opción **Usar la configuración de actualización de software para la inscripción de dispositivos automatizada**.
3. Haga clic en **Sí** para confirmar.
4. Haga clic en **Guardar**.

Inicio de sesión seguro multiusuario

Los administradores pueden borrar la contraseña del dispositivo cuando el usuario cierra la sesión en el clip web «Inicio de sesión seguro multiusuario» en los dispositivos compartidos iOS seleccionando la opción «**Borrar la contraseña cuando el usuario cierre sesión**» en la sección «**Inicio de sesión seguro multiusuario**» en Administrador > Apple > Ajustes

Ajustes de prioridades para la configuración de restricciones

El administrador puede habilitar la prioridad para múltiples configuraciones de restricciones para iOS y macOS seleccionando las opciones **Configuración de restricciones para iOS** o **Configuración de restricciones para macOS** en la sección **Ajustes de prioridad para la configuración de restricciones** en la sección **Administrador > Apple > Ajustes**. Esta opción está desactivada de forma predeterminada. Para obtener más información sobre cómo funciona la prioridad, consulte Priorizar configuraciones

Procedimiento

1. Vaya a **Administrador > Apple > Ajustes**.
2. En la sección **Ajustes de prioridades para la configuración de restricciones**, seleccione la opción **Configuración de restricciones de iOS** o **Configuración de restricciones de macOS**.
3. Haga clic en **Guardar** para activar la prioridad. Aparecerá el banner «**Se han activado los ajustes de prioridades para la configuración de restricciones (iOS o macOS)**». Antes de que la prioridad esté **Aprobada**:
    - **Edite el resumen de distribución (si procede)**: cuando se activa la configuración de la prioridad, el resumen de distribución para la configuración de restricciones seleccionada se cambia de «**Aplicar a los dispositivos de otros espacios**» a «**Aplicar a todos los dispositivos de otros espacios como máxima prioridad**» por defecto.
    - **La prioridad por defecto se asigna en el orden de creación**: para la configuración del tipo de restricción seleccionada, la prioridad por defecto existente se asignará en el orden de creación.
    - **Suspensión de la gestión de la configuración**: la gestión de la configuración de restricciones seleccionada (por ejemplo, la configuración de restricciones de iOS) se suspende hasta que usted apruebe la prioridad.

> Una vez activada la prioridad, cualquier cambio en las restricciones no se procesa hasta que se apruebe. Antes de aprobarla, el administrador puede editar la distribución, el resumen de la distribución o la prioridad de las configuraciones de restricciones en la sección **Configuraciones**.

4. Seleccione la opción **Aprobar** para que la prioridad entre en vigor.
5. Haga clic en **Guardar**.

> La opción **Aprobación** no está disponible cuando se deselecciona una opción de configuración de Restricciones de iOS o macOS; los cambios se aplican de inmediato.

Cuando el ajuste de la prioridad está desactivado, no hay ninguna prioridad asociada a las configuraciones. Todas las configuraciones de restricción se transfieren al dispositivo, si procede (en la siguiente sincronización del dispositivo).

- **Resumen de distribución (si procede): cuando se desactiva el ajuste de prioridad para la configuración de restricciones, el resumen de distribución cambia de Aplicar a todos los dispositivos de otros espacios de dispositivos como máxima prioridad o Aplicar a todos los dispositivos de otros espacios de dispositivos como prioridad más baja a «Aplicar a los dispositivos de otros espacios».**
- **Ninguna prioridad asignada**: se elimina la prioridad asignada para la configuración de restricciones seleccionada

12.4. Trabajar con dispositivos Windows

Esta sección contiene los siguientes temas:

- Configuración de los perfiles de Windows Autopilot
- Audit Trails en los perfiles de Windows Autopilot
- TenantLockdown CSP
- Explorador ADMX (GPO)
- Configuración de los intervalos del inventario de aplicaciones
- Inventario de hardware

12.4.1. Configuración de los perfiles de Windows Autopilot

Windows Autopilot es una característica de Microsoft que ayuda a los administradores a configurar y pre-configurar nuevos dispositivos para que estén listos para la empresa. La función de Autopilot ayuda a un aprovisionamiento rápido, fiable y sin problemas de los dispositivos Windows Desktop o HoloLens2. Además, la función Autopilot ayuda a realizar las siguientes tareas:

- Unir automáticamente dispositivos a Entra ID (Entra ID)
- Inscribir automáticamente los dispositivos en los servicios MDM
- Crear y auto-asignar dispositivos a grupos de configuración basados en el perfil del dispositivo
- Personalizar la experiencia de inscripción
- Aplicar configuraciones y políticas
- Instalar aplicaciones esenciales

Requisitos previos

Para utilizar la página Windows Autopilot, revise los pasos para socios de Ivanti Neurons for MDM y los requisitos de licencia de Azure. Asegúrese de que se cumplen los siguientes requisitos previos para que la función Autopilot funcione como se espera:

- **Licencias de Azure para requisitos de Autopilot**: compruebe los "Requisitos de licencia de Windows Autopilot".
- **Registro de dispositivos Azure Windows Autopilot**: compruebe la "Descripción general del registro de Windows Autopilot".
- **Distribuidores que añaden dispositivos a la cuenta del cliente**: marque la opción "Usar perfiles de Windows Autopilot en dispositivos nuevos para personalizar la experiencia inicial del cliente".

Requisitos adicionales

1. Integre los abonados de Entra ID e Ivanti Neurons for MDM. Para obtener más información, consulte **Configuración con Microsoft Azure**.
2. Asegúrese de que dispone de una cuenta de administrador en Ivanti Neurons for MDM y Entra ID.
3. Para aprovechar los perfiles de despliegue automático, cree un usuario falso para el registro de dispositivos de despliegue automático sin usuario en Ivanti Neurons for MDM.
4. Cree y sincronice un usuario ficticio, fooUser@Entra IDDominioPrimario.com desde Entra ID DominioPrimario.

> No se necesitan licencias de Microsoft para crear y sincronizar un usuario ficticio.

5. La página "Nombres de dominio personalizados" en Entra ID muestra el dominio primario de su entorno Entra ID.
6. Asegúrese de que el usuario puede inscribir dispositivos y no está deshabilitado. Por ejemplo, si el dominio principal es contoso.com, el usuario resultante será fooUser@contoso.com. Si el dominio principal es contoso.onmicrosoft.com, el usuario resultante será fooUser@contoso.onmicrosoft.com.
7. Para aprovisionar al usuario con SCIM en Ivanti Neurons for MDM, edite los detalles del usuario en Entra ID y añada la dirección de correo electrónico. Generalmente, la dirección de correo electrónico será la misma que el UPN.
8. Asegúrese de que todos los usuarios, incluido fooUser, estén presentes en Azure y en Ivanti Neurons for MDM.
9. Los administradores pueden crear perfiles de Autopilot mediante Microsoft Store for Business o Ivanti Neurons for MDM. Para crear perfiles utilizando administradores de Ivanti Neurons for MDM se requieren permisos de administrador de Entra IDmin

Global e Intune.

> Los administradores necesitan Azure P1 o P2 y se necesitan licencias Ivanti Neurons for MDM Secure UEM o Secure UEM Premium. La licencia de Intune no es necesaria para los administradores.

> En Neurons for MDM, la función de creación de perfiles de autopilot aprovecha las API de Microsoft Graph para autopilot, que aún están en fase beta.

Modos de inscripción del Autopilot

Después de asociar los dispositivos con un grupo de perfiles de usuario específico, basado en el uso del dispositivo, puede configurar el modo de inscripción del Autopilot para permitir a los usuarios comenzar rápidamente con su dispositivo. Ivanti Neurons for MDM ofrece los siguientes modos de inscripción del Autopilot:

- Modo de auto-despliegue
- Impulsado por el usuario (modo preaprovisionado)
- Impulsado por el usuario

Modo Autopilot de despliegue automático: el modo Autopilot de despliegue automático de dispositivos garantiza un despliegue sin problemas de un dispositivo de empresa para un usuario evitando la configuración inicial del dispositivo y enviando todos los archivos de configuración necesarios para que el dispositivo se ponga en marcha de forma segura. Este modo asegura el hardware, conecta el dispositivo a la red de la empresa, inscribe el dispositivo al Entra ID (ID de Entra), el servicio MDM, y al portal del administrador de Ivanti Neurons for MDM usando un ID de usuario ficticio y todos los archivos de configuración necesarios son empujados al dispositivo antes de que el usuario inicie sesión. Después de que los archivos de configuración obligatorios se empujan al dispositivo, el dispositivo se reinicia y muestra la pantalla de inicio de sesión para que el usuario de la empresa comience. Puede utilizar el modo de auto-despliegue para un dispositivo que puede ser utilizado como un Kiosko o un dispositivo firmado digitalmente.

Modo de perfil de preaprovisionamiento impulsado por el usuario: Una vez que el administrador crea un perfil de preaprovisionamiento impulsado por el usuario, el administrador asigna el perfil a un grupo de usuarios, y el ID de hardware del dispositivo se carga y se asigna al grupo Entra ID. El dispositivo se asociará al perfil de pre-aprovisionamiento impulsado por el usuario. Este modo lo utiliza el administrador para configurar un dispositivo antes de entregarlo al usuario de la empresa.

Procedimiento

Siga los pasos para el despliegue preaprovisionado:

1. Conecte el nuevo dispositivo de hardware a la LAN y pulse cinco veces el botón de Windows.
2. El dispositivo muestra una pregunta. Seleccione la opción de aprovisionamiento del autopilot de Windows y haga clic en Continuar. El Entra ID detecta el modo de perfil de preaprovisionamiento dirigido por el usuario, y todos los ajustes básicos de configuración se despliegan en el dispositivo. Se muestra la pantalla de configuración del autopilot de Windows.
3. Haga clic en Continuar. El dispositivo progresa y asegura el hardware, conecta el dispositivo a la red de la empresa, inscribe el dispositivo al Entra ID (ID de Entra), el servicio MDM, y al portal del administrador de Ivanti Neurons for MDM usando un ID de usuario ficticio y todos los archivos de configuración necesarios son empujados al dispositivo y aparece un mensaje de confirmación.
4. Ahora puede entregar el dispositivo al usuario. Cuando el usuario inicia sesión en el dispositivo, el ID de usuario se registra en el portal del administrador de Ivanti Neurons for MDM con los detalles del dispositivo.

Las siguientes configuraciones se transfieren automáticamente antes de que el usuario inicie sesión en el dispositivo:

Certificado de identidad

Wi-Fi

Windows Hello para empresas

Restricciones de Windows

El resto de configuraciones se encuentran en estado Pendiente y se envían después de que el usuario inicie sesión en el dispositivo mediante una dirección de correo electrónico.

Durante el proceso de inscripción de Autpilot en los modos de autoimplantación e impulsado por el usuario (preaprovisionamiento), las aplicaciones .MSI y .EXE asignadas se instalarán en el dispositivo para completar el proceso de inscripción. Al instalar las aplicaciones .MSI y .EXE durante el proceso de inscripción en Autopilot, si las aplicaciones informan o no lo hacen durante la instalación, el proceso de Autopilot se completará y se activará el botón Volver a sellar.

Creación de perfiles de usuario de Windows Autopilot

Después de configurar la Fuente de Usuario Entra ID (Entra ID) y sincronizar los usuarios y grupos de usuarios Entra ID con el inquilino Ivanti Neurons for MDM, puede crear los perfiles de Autopilot.

Procedimiento

1. Inicie sesión en el portal del administrador de Ivanti Neurons for MDM
2. Vaya a **Administrador > Microsoft Azure > Administración de dispositivos de Windows**.

Si no está configurada la Fuente de Usuario de Entra ID, el botón **Agregar** estará desactivado. Debe configurar la Fuente de usuario mediante la opción de **Administración de dispositivos de Windows** presente en la sección de **Microsoft Azure**.

3. Haga clic en **Añadir**.
   Aparecerá en pantalla la página de **Añadir Perfil de Autopilot de Windows**.
4. Introduzca un nombre de perfil en la casilla **Nombre**.
5. Complete la **Configuración del perfil** utilizando la tabla a continuación de este procedimiento.
6. Haga clic en **Siguiente**.
   Aparecerá en pantalla una nueva página con todos los grupos de dispositivos Entra ID.
7. Seleccione uno o más Grupos de Dispositivos Entra ID a los que se debe asignar el Perfil del Autopilot.
8. También puede crear un Grupo de Dispositivos Entra ID y asignar el Perfil de Autopilot a este grupo recién creado. Consulte para obtener más información.
   Si desea asignar el Perfil de Autopilot a todos los Grupos Entra ID, seleccione la opción **Asignar a todos los Grupos Entra ID**.

No se puede asignar más de un perfil a "Todos los grupos" debido a una limitación de Microsoft.

9. Haga clic en **Hecho**.

Ajuste	Descripción
Tipo de dispositivo	Seleccione una de las dos opciones siguientes en función del dispositivo: • **PC con Windows** • **HoloLens** : Cuando se selecciona esta opción, el modo de despliegue predeterminado debe establecerse en el modo de **auto-despliegue**. En raras ocasiones, al inscribir dispositivos HoloLens 2 mediante el uso de Autopilot, la inscripción podría quedarse atascada en la pantalla "Configurar el dispositivo para el trabajo". En este caso, el usuario debe apagar y encender el dispositivo pulsando el botón de encendido. A continuación, el dispositivo muestra la pantalla de inicio de sesión, en la que el usuario debe introducir las credenciales de Entra ID para completar la inscripción.
Modo de despliegue	• **Auto-despliegue**: En este modo, el despliegue del dispositivo ocurre con poca o ninguna participación manual. • **Dirigido al usuario** :Los administradores pueden utilizar esta opción para seleccionar el modo de inscripción para configurar un nuevo dispositivo para el usuario antes de entregar el dispositivo al usuario.
Tipo de cuenta de usuario **Idioma**	• **Administrador**: Seleccione esta opción si el usuario necesita un control total una vez desplegado el dispositivo. • **Estándar**: Seleccione esta opción si el usuario necesita autorización a las opciones básicas una vez desplegado el dispositivo. De forma predeterminada, el idioma será el específico del sistema operativo. Puede cambiar a un idioma diferente de la lista.
Convertir todos los dispositivos asignados a Autopilot	Seleccione esta opción para convertir todos los dispositivos del grupo asignado al Autopilot.
Permitir el aprovisionamiento previo **Configurar automáticamente el teclado**	Seleccione esta opción para registrar los dispositivos para el Autopilot utilizando el proceso de registro normal. Esta opción no está disponible cuando se selecciona la opción de **auto-aprovisionamiento**. Seleccione **Sí** para omitir la selección del teclado en caso de que la opción **Idioma** esté configurada con un valor diferente al predeterminado.
Nombre de la plantilla del dispositivo **Términos de licencia del software de Microsoft**	Introduzca un nombre de plantilla para utilizar durante el proceso de inscripción del dispositivo. Puede mostrar u ocultar esta opción sólo en el modo de despliegue dirigido por el usuario.

Ajuste	Descripción
Ajustes de privacidad	Puede mostrar u ocultar esta opción sólo en el modo de despliegue dirigido por el usuario.
Cambiar las opciones de la cuenta	Puede mostrar u ocultar esta opción sólo en el modo de despliegue dirigido por el usuario y cuando el tipo de cuenta de usuario es de tipo estándar.

Administrador de dispositivos Windows

El administrador puede configurar la función de Autopilot en un abonado mediante la nueva opción de Administración de dispositivos de Windows. Esta opción facilita la integración con Ivanti Neurons for MDM si el usuario dispone de un entorno Entra ID.

Para acceder a esta opción, **Administrador** > **Microsoft Azure** > **Administración de dispositivos de Windows**.

Esta integración da permiso a Ivanti Neurons for MDM para que administre dispositivos, perfiles de Autopilot, comprobar el cumplimiento de dispositivos de Windows y para validar el abonado de Azure.

Temas relacionados

- TenantLockdown CSP

Creación de grupos de dispositivos de Entra ID

El administrador puede crear Grupos de Dispositivos de Entra ID, como y cuando sea necesario, desde la sección Grupos de Dispositivos de Entra ID. La validación del inquilino de Entra ID debe haber sido configurada en la sección Cumplimiento de Dispositivos para crear Grupos de Dispositivos de Entra ID.

Procedimiento

1. Vaya a **Administración** > **Microsoft Azure** > **Grupos de dispositivos de Entra ID** .
2. Aparecerá en pantalla la página **Grupos de dispositivos de Entra ID**.
   Haga clic en **ADD**.
3. La página **Ajustes del grupo** aparece en la pantalla.
   Proporcione los siguientes detalles:
   - Nombre del grupo
   - Descripción del grupo
   - Tipo de pertenencia
     - Dispositivo estático: el administrador obtendrá la lista de dispositivos estáticos en la ventana **Asignar pertenencias a grupos**. Seleccione los dispositivos necesarios y haga clic en **Guardar**.
     - Dispositivo dinámico: el administrador debe proporcionar determinados criterios en la ventana de **Consulta dinámica**.

Se creará el nuevo Grupo de Dispositivos de Entra ID y el administrador podrá añadir dispositivos al grupo recién creado.

> Después de crear un grupo dinámico, los dispositivos se listarán en la pestaña Dispositivos del grupo de dispositivos específico transcurrido un tiempo.

Edición de dispositivos Autopilot

Los usuarios pueden editar los dispositivos Autopilot desde el portal administrativo de Ivanti Neurons for MDM

Requisitos previos

Asegúrese de que se cumplan los siguientes requisitos previos:

- El usuario IT Admin debe tener permisos Azure Global Admin e Intune Admin.
- Solo se puede establecer un nombre de usuario si el usuario está configurado.
- Una vez establecido, el nombre del dispositivo no se puede anular.

Procedimiento

1. Inicie sesión en el portal administrativo de Ivanti Neurons for MDM
2. Ir a**Administración** > **Windows** > **Autopilot**. Los dispositivos Autopilot se enumeran en la pestaña Dispositivos de Autopilot.
3. Hacer clic en **Editar** (icono de lápiz). Aparece la página de edición.
4. Modifique los siguientes detalles:
    - **Usuario**
    - **Nombre fácilmente recordable por el usuario**
    - **Nombre del dispositivo**
    - **Etiqueta de grupo**

Haga clic en **Guardar**. Los detalles del dispositivo se actualizan.

Eliminación de dispositivos Autopilot

Los usuarios pueden eliminar los dispositivos Autopilot desde el portal administrativo de Ivanti Neurons for MDM.

1. Inicie sesión en el portal administrativo de Ivanti Neurons for MDM
2. Ir a**Administración** > **Windows** > **Autopilot**. Los dispositivos Autopilot se enumeran en la pestaña Dispositivos de Autopilot.
3. Haga clic en **Eliminar**. Los detalles del dispositivo se eliminan.

12.4.2. Audit Trails en los perfiles de Windows Autopilot

Audit Trails realiza un seguimiento de todas la actividades que se lleven a cabo en todas la entidades de Ivanti Neurons for MDM. Estas actividades incluyen agregar, eliminar, actualizar nuevos dispositivos, etc.

Para obtener más información, consulte **Seguimiento de auditorías**.

El administrador puede llevar a cabo las actividades siguientes mediante Seguimiento de auditoría en todos los dispositivos de Windows inscritos en el modo Autopilot:

Perfiles de Autopilot

- Crear
- Editar
- Eliminar
- Asignar el perfil a grupos

Dispositivos de Autopilot

- Cargar CSV
- Editar
- Eliminar

12.4.3. TenantLockdown CSP

El administrador puede bloquear todos los dispositivos Windows a los abonados utilizando la función TenantLockdown CSP. Para utilizar esta función, los dispositivos deben estar inscritos mediante la opción Autopilot. Esta configuración puede realizarse a nivel de dispositivo.

En los modos Autopilot Self-deployed y User-driven, el administrador puede bloquear los dispositivos directamente a los abonados. Esto es útil cuando los dispositivos son robados o se pierden. En estos casos, incluso si el dispositivo se restablece, el usuario se verá obligado a conectarse al abonado y la creación de cuentas locales no se admite en el modo Auto-desplegado. Pero si hay que impedir la creación de cuentas en el modo dirigido por el usuario, el administrador debe habilitar la opción **Ocultar** en el ajuste **Cambiar opciones de cuenta** durante la configuración del perfil del Autopilot.

El administrador puede habilitar el CSP de TenantLockdown creando una Configuración de Restricciones de Windows y seleccionando la opción **Requerir que los usuarios se conecten a la red durante la configuración del dispositivo (se requiere el perfil de Autopilot)** en **Otras Restricciones**.

Para eliminar un dispositivo del CSP de TenantLockdown, el administrador debe eliminar manualmente el dispositivo del grupo o cambiar las restricciones.

12.4.4. Explorador ADMX (GPO)

Si usa el navegador ADMX (GPO), puede visualizar los ajustes de GPO organizados en función de los objetos ADMX que existen en el abonado. Se pueden buscar y visualizar los objetos ADMX predeterminados y también añadir (cargar) archivos ADMX personalizados que proporcionen una estructura basada en XML para definir la visualización de los ajustes de GPO.

Para cargar un objeto ADMX personalizado:

1. Seleccione **Administrador > Navegador ADMX (GPO)**. Se mostrará la página **Navegador AMX (GPO)**.
2. Haga clic en **Anexo**. Aparecerá la ventana **Anexar objetos ADMX (GPO) personalizados**.
3. Haga clic en **Elegir archivo** para seleccionar el archivo ADMX que se va a cargar.

> Asegúrese de que el archivo ADMX es un archivo zip.

4. Haga clic en **Anexo**. Aparecerá un mensaje de confirmación si se ha cargado correctamente.

> Una vez descomprimido el archivo zip, asegúrese de que la carpeta raíz contiene el archivo de extensión *.admx*.

Buscar ajustes GPO

En el navegador ADMX (GPO), puede buscar y seleccionar un GPO haciendo clic en el componente pertinente del árbol de jerarquía de los GPO del panel izquierdo. El árbol de jerarquía de los GPO representa la ruta de los ajustes de políticas. Como alternativa, puede buscar un ajuste de GPO específico escribiendo el nombre del GPO o el nombre del archivo ADMX en el campo de búsqueda. Aparecerán los detalles del ajuste de GPO seleccionado en el panel derecho.

12.4.5. Configuración de los intervalos del inventario de aplicaciones

Puede establecer intervalos de recopilación de inventario de aplicaciones de Windows 10 para varios inventarios de tipos de origen de aplicaciones. Estos intervalos se usan cuando la política de privacidad se ha ajustado para que se obtengan todas las aplicaciones del dispositivo.

1. Navegue hasta **Administrador > Intervalos de inventario de la aplicación.**
2. Seleccione el intervalo (en horas) para recopilar el inventario de aplicaciones de la lista desplegable para los siguientes tipos de origen de aplicaciones.
    - **Intervalo del inventario que no sea de la App Store**
    - **Intervalo del inventario de la App Store**
    - **Intervalo del inventario del sistema**
    - **Intervalo del inventario de Win32**
      Las opciones de intervalo para recopilar el inventario de aplicaciones de Windows son entre **24** y **48** horas. El valor predeterminado es **24** horas.

12.4.6. Inventario de hardware

Usted puede activar la obtención de información sobre el hardware de dispositivos Windows 10. Los detalles del inventario de hardware se recuperan usando Bridge.

1. Navegue hasta **Administración > Inventario de hardware.**
2. Active la opción **Activar la obtención del inventario de hardware**.
3. En la opción **Intervalo del inventario**, seleccione la frecuencia de obtención del inventario de hardware. A continuación se enumeran las opciones disponibles:
    - **Una vez al día**(predeterminada)
    - **Una vez a la semana**
    - **Cada 30 días**

Una vez que se haya activado la opción de inventario de hardware, podrá visualizar los detalles de hardware del dispositivo en la pestaña **Hardware** que hay en la página de detalles del dispositivo.

12.5. Configuración con Microsoft Azure

Esta sección contiene los siguientes temas:

- Uso de Microsoft Azure
- Configuración de la gestión del endpoint unificado de Entra ID de Windows 10
- Asignación de la aplicación Entra ID UEM
- Conecte Ivanti Neurons for MDM con Entra ID User Source
- Inquilino de Azure
- Administrador > Microsoft Azure > Office 365 App Protection

12.5.1. Uso de Microsoft Azure

Ivanti Neurons for MDM se puede configurar con Microsoft Azure para una inscripción perfecta de los usuarios en sus dispositivos de escritorio de Windows y tabletas con Windows 10. Siga los siguientes pasos para configurar y conectar sus instancias.

Esta sección contiene los siguientes temas:

- Configurar una cuenta de Entra ID
- Creación de usuarios en Entra ID
- Conexión de Entra ID a UEM para dispositivos Windows 10
- Compatibilidad con varios usuario para dispositivos de Windows

Configurar una cuenta de Entra ID

Para configurar Entra ID:

1. Vaya a https://azure.microsoft.com/en-in/pricing/purchase-options/ para comprar su cuenta Azure.
2. Utilice su cuenta de Hotmail o Outlook.com existente o cree una cuenta nueva y regístrese como nuevo usuario.
3. Compre una cuenta Azure mediante alguna de las opciones de pago y siga los pasos de verificación.
4. Pida a Microsoft que incluya en la lista permitida al abonado de Ivanti Neurons for MDM.
5. Utilice la misma cuenta de Hotmail u Outlook.com que utilizó en el paso 2 para iniciar sesión en Entra ID en https://manage.windowsazure.com/https://manage.windowsazure.com/ como administrador.
6. Vaya a la pestaña **Dominio**.
   Se creará un valor predeterminado del dominio, TestMiBGLRoutlook.onmicrosoft.com, para su cuenta y cualquier usuario creado pertenecerá a este dominio. Si fuera necesario, puede volver a crear un dominio personalizado.

Creación de usuarios en Entra ID

Para crear usuarios en Entra ID:

1. Vaya a Active Directory - > **Directorio predeterminado → Usuarios**.
2. Seleccione la opción Añadir usuario → Seleccione Nuevo usuario en su organización.
3. Introduzca que el nombre de usuario. Haga clic en Siguiente **(→)**.
   Aparece la página **Perfil del usuario**.
4. Añada la información del usuario como su nombre, apellidos y nombre en pantalla.
5. Utilice el menú desplegable para asignar la función adecuada al usuario.
6. Genere la contraseña temporal.
   Se pedirá al usuario que cambie esta contraseña la primera vez que inicie sesión.

Conexión de Entra ID a UEM para dispositivos Windows 10

Para conectar Entra ID a UEM:

1. **Vaya a Administración > Microsoft Azure > Windows Enrollment And Compliance Using Entra ID.**
2. Complete los pasos de configuración de UEM descritos en la sección, Configuración de la gestión del endpoint unificado de Entra ID de Windows 10

3. Complete la configuración de **Asignación de la aplicación Entra ID UEM** en el portal de Azure.
4. En el Portal de administración Ivanti Neurons for MDM, escriba el nombre de dominio de su cuenta Entra ID y haga clic en Conectar portal Azure y, a continuación, seleccione la casilla de verificación.
5. Después de iniciar sesión correctamente, acepte el consentimiento que permite que la aplicación Validación del abonado de MobileIron AD verifique que su aplicación de UEM en Ivanti Neurons for MDM esté configurada. Aparecerá un mensaje que indica que la conexión es correcta.

Microsoft Passport for Work para dispositivos Windows 10

Microsoft Passport for Work se reemplaza con Windows Hello para empresas. Para obtener más información, consulte **Configuración predeterminada de Windows Hello para empresas**.

Inscripción en Entra ID del dispositivo Windows

Requisitos previos

Los usuarios deben registrarse en Ivanti Neurons for MDM.

Conecte su dominio para inscribir al usuario en sus dispositivos Windows 10+.

1. Haga clic en **Unirse a Entra ID**.
2. Introduzca el nombre de usuario y la contraseña.
3. Haga clic en **Iniciar sesión**.
4. Acepte el EULA.
5. Haga clic en **Crear PIN**.
    - Si ha habilitado la complejidad del PIN de Microsoft Passport for Work, se le solicitará que configure un PIN complejo de acuerdo con la política configurada.
    - Entra ID autentica al usuario y descarga un JWT (JSON Web Token) al dispositivo.
    - El dispositivo ya está inscrito.
    - Se contactará con el usuario a través del dispositivo para la verificación.
6. Introduzca y confirme el PIN.
7. Haga clic en **Aceptar**.

Compatibilidad con varios usuario para dispositivos de Windows

Ivanti Neurons for MDM admite capacidades multiusuario para los dispositivos inscritos en Entra ID de Windows 10. Esta función incluyen poder insertar algunos perfiles como de VPN, Wi-Fi, perfiles predeterminados de cliente de correo electrónico y certificados en un usuario individual y no un dispositivo. También admite la distribución de aplicaciones internas y públicas para el usuario que ha iniciado sesión. Cada vez que un nuevo usuario Entra ID se conecta a un dispositivo, Ivanti Neurons for MDM evalúa no solo el dispositivo, sino también al usuario. Si el usuario es nuevo, Ivanti Neurons for MDM actualiza el dispositivo para ese usuario. Si el usuario es un usuario existente en el dispositivo, se evaluará cualquier cambio en el dispositivo y en los ajustes del usuario que tengan que actualizarse desde la última vez que inició sesión.

Los detalles del usuario Entra ID que ha iniciado sesión en el dispositivo se notifican en el portal de administración de Ivanti Neurons for MDM. Cuando el usuario cierra sesión en el dispositivo y el segundo usuario inicia sesión en el dispositivo, los detalles del segundo usuario se actualizan en la página de detalles del dispositivo.

Usar Microsoft Store para empresas con UEM

Microsoft Store para empresas es un portal proporcionado por Microsoft como parte de Azure. Los administradores pueden acceder a este portal y comprar las aplicaciones y distribuirlas a todos los dispositivos administrados. Ivanti Neurons for MDM se puede configurar con Microsoft Store for Business para administrar aplicaciones desde el portal de administración de Ivanti Neurons for MDM mediante la configuración de los pasos siguientes.

Paso 1: Registro de la aplicación Entra ID en el Portal de Microsoft Azure

1. Abra el primer navegador e inicie sesión en el portal de Microsoft Azure (https://portal.azure.com/https://portal.azure.com/).
2. Haga clic en **Registros de aplicaciones** en el panel izquierdo.
3. Haga clic en **+Registro de nueva aplicación**.
4. Introduzca la siguiente información para registrar MobileIron como aplicación de Azure:
    - **Nombre:** escriba un nombre para la aplicación de MobileIron. (Este campo debe tener al menos 4 caracteres).
    - **Tipo de aplicación:** seleccione Aplicación web/API.
    - **URL de inicio de sesión:** introduzca la URL a la que acceden los usuarios de los dispositivos para iniciar sesión en MobileIron (obligatorio).
5. Haga clic en **Crear** para añadir la aplicación y volver a la página de inicio de Azure.
6. Vaya a Ajustes y cree una nueva clave.

Paso 2: Añadir la aplicación como herramienta de administración

1. En los ajustes de Microsoft Store para empresas, haga clic en Administrar
2. ajustes de distribución.
3. En la herramienta Añadir administración, active la aplicación creada.

Conexión de la cuenta en el Portal de administración

1. Vaya a **Administrador > Microsoft Azure > Microsoft Store para empresas**.
2. En el paso 1, **Registrar la aplicación Entra ID**, seleccione la casilla **Sí, he completado este paso**.
3. En el Paso 2, **Añadir herramienta de administración**, seleccione la casilla **Sí, completé este paso**.
4. En el Paso 3, Conexión de la cuenta, actualice los siguientes campos:
    - Dominio de Entra ID
    - Identificador de la aplicación
    - Clave de la aplicación
    - Intervalo de sincronización (horas)
5. Haga clic en **Conectar**. Verá un mensaje que confirma que la tienda de MobileIron para empresas se ha configurado correctamente.
6. Haga clic en **Sincronizar aplicación**. Cuando se sincroniza correctamente, el estado se muestra como **Aplicaciones sincronizadas correctamente**.

Cuando la Microsoft Store para aplicaciones se envía al dispositivo, los detalles de la aplicación están disponibles en la pestaña **Aplicaciones instaladas** en los detalles del dispositivo. Cada aplicación de Microsoft Store para empresas notificada desde el dispositivo, puede identificarse como **Microsoft Store para empresas** en la columna **Origen**.

12.5.2. Configuración de la gestión del endpoint unificado de Entra ID de Windows 10

Para configurar la Administración unificada de puntos de conexión de Windows 10 (UEM):

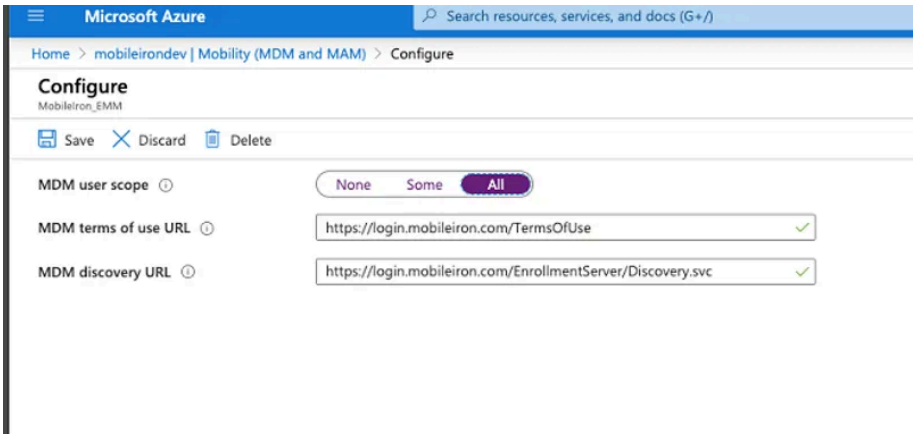
1. Inicie sesión en https://portal.azure.com/ como usuario administrador y seleccione Entra ID.
2. Seleccione «Movilidad (MDM y MAM)» en el panel de la izquierda y, luego, haga clic en **+ Añadir aplicación**.

3. Seleccione la aplicación MobileIron_UEM de la galería de aplicaciones y haga clic en **Añadir**.


12.5.3. Asignación de la aplicación Entra ID UEM

Para completar la configuración de usuarios asignados:

1. Haga clic en la aplicación de UEM en MobileIron que creó en el Paso 2 en **Configuración de la gestión del endpoint unificado de Entra ID de Windows 10**
2. En el ámbito de usuario MDM, asígnelo a sus grupos de usuarios personalizados o seleccione **Todos**.



12.5.4. Conecte Ivanti Neurons for MDM con Entra ID User Source

Para trabajar con Entra ID (Entra ID), debe configurar Ivanti Neurons for MDM con detalles sobre su cuenta de Microsoft Entra ID. Se requiere una cuenta existente y configurada de Microsoft Entra ID. Esta solución requiere un conector local o LDAP.

Esta sección contiene los siguientes temas:

- Casos de uso
- Uso de Entra ID
- Configuración de Entra ID

Casos de uso

Puede conectar Ivanti Neurons for MDM con Entra ID para uno de los siguientes casos de uso:

- Trabajar con Microsoft Office 365
- Configure Microsoft Entra ID, Microsoft ADFS u otro proveedor de identidades (IdP) SAML 2.0 para la autenticación de usuarios.
- Configure Microsoft Entra ID como su fuente de usuario
- Sincronice usuarios desde Microsoft Entra ID y comience. Todos los usuarios y grupos de su dominio de Entra ID se sincronizarán con su instancia Ivanti Neurons for MDM.
  Se muestra una notificación en la página **Notifications** si se produce un error en la sincronización de Entra ID debido a los siguientes motivos:
  - El servicio de Entra ID no está disponible
  - No están sincronizados con Entra ID todos los atributos del usuario
  - Algunos atributos del usuario no están sincronizados con Entra ID
- Actualmente no se admiten los entornos con múltiples IdP.
- Si no está utilizando Microsoft Entra ID como su fuente de usuarios, puede usar las cuentas locales u obtener los usuarios del LDAP. Para ello, es obligatorio utilizar un conector de Ivanti Neurons for MDM para acceder a los recursos locales del LDAP.
- Actualmente no se admite el uso de Microsoft Entra ID únicamente para la autenticación de usuarios ni el uso de un LDAP local para el directorio de usuarios.

Uso de Entra ID

Para utilizar Entra ID, configure su proveedor de identidad para la autenticación de usuarios en uno de los siguientes métodos:

- Para utilizar Microsoft Entra ID tanto para el origen como para la autenticación de usuarios, configure Entra ID como su IdP. Vaya a **Administrador > Identidad > Configuración de IdP de Ivanti Neurons for MDM** y seleccione **Entra ID** en el menú.
- Para utilizar Microsoft Entra ID para el origen de usuarios y ADFS para la autenticación de usuarios, configure ADFS como su IdP. Vaya a **Administración > Identidad > Configuración de IdP local** y seleccione ADFS en el menú.
- Para usar un IdP de SAML 2.0 distinto a Entra ID y utilizar ADFS para la autenticación de usuarios, vaya a **Administración > Identidad > Configuración de IdP Genérico** y siga las instrucciones de la página.

Para obtener más información, consulte Configurar el proveedor de identidades.

Configuración de Entra ID

Este tema le ayuda a configurar los ajustes de Entra ID.

Procedimiento

1. Vaya a **Administración > Microsoft Azure > Fuente de usuarios de Entra ID**.
2. Especifique los siguientes detalles:
    1. **Nombre de Entra ID**.
    2. **Intervalo de sincronización**: Modifique la frecuencia con la que Ivanti Neurons for MDM sincroniza los datos de usuario de su Entra ID.
    3. **Habilitar este Entra ID**: Utilice esta opción para habilitar o deshabilitar la instancia de Entra ID.
    4. Seleccione **Invitar automáticamente a los usuarios importados desde Entra ID**: administrar si los usuarios importados desde Entra ID hasta Ivanti Neurons for MDM son invitados automáticamente a registrarse por correo electrónico.
    5. Seleccione **ID de Apple administrada**: Elija sincronizar ID de Apple administrada para los usuarios de Entra ID.
        - **Ninguna**
        - **Patrón**:
            - **Dirección de correo electrónico del usuario**
            - **userUPN**
            - (Opcional) seleccione la opción «Incluir el subdominio "appleid"» para evitar conflictos con los ID de Apple existentes.
    6. (Opcional) Haga clic en **Añadir atributo personalizado**: especifique los atributos de usuario personalizados que desee aplicar a la administración de dispositivos desde su servicio de directorio. Cada atributo puede estar referenciado por $ en los campos de configuración que admitan variables. El uso de esta opción requiere una implementación uniforme de los atributos personalizados en los servidores de Entra ID. Si un servidor de Entra ID incluido en la implementación no usa este atributo, es posible que las características dependientes de este atributo no funcionen como deberían.

Haga clic en **Guardar** después de modificar los ajustes de Entra ID.

12.5.5. Inquilino de Azure

Esta sección contiene los siguientes temas:

- Requisitos
- Aplicar la licencia de Intune a usuarios de dispositivos
- Para añadir MobileIron como socio de cumplimiento
- Creación de una directiva de acceso condicional en Microsoft Endpoint Manager
- Conexión de Microsoft Azure con Ivanti Neurons for MDM
- Creación de una directiva de cumplimiento de los dispositivos de los socios
- Estado del dispositivo que notifica desde Ivanti Neurons for MDM a Azure
- Cancelar el aprovisionamiento del inquilino de Azure

12.5.5.1. Azure Tenant Requirements

En esta sección se describe cómo configurar Ivanti Neurons for MDM con Microsoft Azure Tenant.

Requisitos

Microsoft

Los clientes de Ivanti Neurons for MDM deben tener una suscripción válida a Microsoft Intune y asignar una licencia de Microsoft Intune a los usuarios de dispositivos.

MobileIron

- Ivanti Neurons for MDM: Ivanti Neurons for MDM versión 75 hasta la última versión compatible con MobileIron.
- Licencias adicionales: el Cumplimiento de los dispositivos de Azure es una oferta Premium y está disponible para clientes de **Secure UEM Premium** y Platinum. Una licencia Platinum es suficiente para los clientes existentes.
- Go para iOS (cliente) o Go para Android (cliente) versión 75.0 hasta la versión más reciente compatible con MobileIron.

Compatibilidad con múltiples Ivanti Neurons for MDM

Si tiene varios Ivanti Neurons for MDM conectados al mismo arrendatario de Azure, desconéctese de todos los Ivanti Neurons for MDM o desactive la política de conformidad para la integración de conformidad de Entra ID desde un Ivanti Neurons for MDM específico (único) para que no cargue los datos del dispositivo en Azure.

> Asegúrese de deshabilitar la política de cumplimiento antes de desconectar Ivanti Neurons for MDM.

Proceso del administrador de Ivanti Neurons for MDM

El proceso desde la perspectiva del administrador de Ivanti Neurons for MDM es el siguiente:

1. El administrador aplica licencias de Intune a los usuarios de dispositivos. Consulte **Aplicar la licencia de Intune a usuarios de dispositivos**.
2. El administrador inicia sesión en Azure Portal.
3. El administrador agrega MobileIron como socio de cumplimiento de Azure. Consulte **Para añadir MobileIron como socio de cumplimiento**.
4. El administrador crea la directiva de Acceso condicional para las aplicaciones. Consulte **Creación de una directiva de acceso condicional en Microsoft Endpoint Manager**.
5. El administrador establece la conexión entre MobileIron y Azure. Consulte **Conexión de Microsoft Azure con Ivanti Neurons for MDM**.
6. El administrador crea la política de cumplimiento del dispositivo en Ivanti Neurons for MDM. Consulte **Creación de una directiva de cumplimiento de los dispositivos de los socios**.
7. La directiva de Acceso condicional entra en vigor. El acceso a las aplicaciones se concede o deniega en función de que el dispositivo sea o no compatible.

> Ivanti recomienda que el administrador ejecute pruebas en cada aplicación de Microsoft.

12.5.5.2. Aplicar la licencia de Intune a usuarios de dispositivos

- No utilice esta función si:
  - está cambiando usuarios o administrando situaciones en las que es probable que los usuarios cambien
  - el dispositivo pertenece a usuarios múltiples
- Ivanti le recomienda que no ejecute Asignar al usuario y no distribuya la configuración de cumplimiento de los dispositivos a dispositivos para usuarios múltiples como, por ejemplo:
  - dispositivos con Secure Sign-In WebClip
  - iPad compartidos
  - dispositivos en el modo kiosco de Android

Ivanti Neurons for MDM requisitos de la licencia

El Cumplimiento de los dispositivos es una oferta Premium y está disponible para clientes de Secure UEM Premium y Platinum. Para los clientes existentes, la licencia Platinum es suficiente.

Asignar licencias en masa a usuarios de dispositivos

Para asignar licencias en masa a usuarios de dispositivos existentes:

Asignación basada en el grupo

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

Asignación basada en PowerShell

https://docs.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365-powershell?view=o365-worldwide

12.5.5.3. Para añadir MobileIron como socio de cumplimiento

Requisitos previos

- una licencia de Microsoft Intune instalada. Consulte **Aplicar la licencia de Intune a usuarios de dispositivos**.
- usuarios creados en Microsoft Azure.
- grupos creados en Microsoft Azure.

Procedimiento

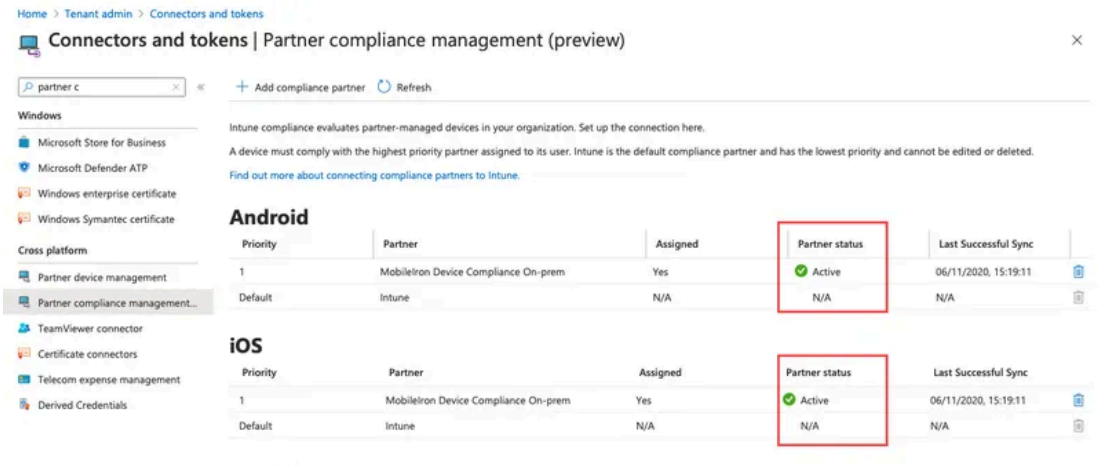
1. Inicie sesión en: **https://endpoint.microsoft.com**.
2. En el panel izquierdo de la página del centro de administración de Microsoft Endpoint Manager, haga clic en Administrador de inquilinos. Haga clic en Conectores y tokens > Administración de cumplimiento de socios.

3. A la derecha del campo Buscar, haga clic en + Añadir socio de cumplimiento.

4. En la pestaña Básico, seleccione MobileIron Device Compliance Cloud en la lista desplegable del campo Asociado de cumplimiento.

5. En el campo Plataforma, seleccione iOS o Android y, a continuación, haga clic en Siguiente.
6. Haga clic en la pestaña Asignaciones. En la lista desplegable Asignar a, seleccione el usuario/grupo de usuarios de dispositivos para el cual corresponde el estado de cumplimiento. Seleccione el usuario/grupo que posea la licencia.

7. Seleccione Siguiente.
8. Haga clic en Crear. El nuevo socio de cumplimiento aparece en la página de administración de cumplimiento del Socio.



12.5.5.4. Creación de una directiva de acceso condicional en Microsoft Endpoint Manager

Procedimiento

1. Inicie sesión en Microsoft Endpoint Manager **https://endpoint.microsoft.com**.
2. En el centro del administrador de Microsoft Endpoint Manager, acceda a Inicio > Seguridad de puntos de conexión > Acceso condicional.
3. Haga clic en Directivas y después en + Nueva directiva.

4. Introduzca el nombre de la directiva de acceso condicional.

5. En Asignaciones, haga clic para asignar la directiva a los usuarios y grupos.

6. Haga clic en Aplicaciones o acciones en la nube y, a continuación, haga clic en Seleccionar. Busque y seleccione las aplicaciones que se deben proteger.

7. Haga clic en Condiciones y, a continuación, haga clic en Plataforma de dispositivo. Seleccione las plataformas de dispositivos apropiadas.

8. En la página Nueva directiva de acceso condicional > Controles de acceso, haga clic en Conceder y realice las selecciones de acceso y bloqueo.

9. Para habilitar la nueva directiva, haga clic en Activado.

10. Haga clic en Crear.

12.5.5.5. Conexión de Microsoft Azure con Ivanti Neurons for MDM

Procedimiento

1. Inicie sesión en Ivanti Neurons for MDM y vaya a **Administración** > **Microsoft Azure**.
2. En el panel de navegación izquierdo, haga clic en **Microsoft Azure** > **Conformidad del dispositivo**.
3. En la sección Conectar cuenta, proporcione los detalles siguientes:
    - **Id. del inquilino de Azure**: búsquelo en su instancia de Microsoft Azure.
    - **URL de inscripción (opcional)**: si el dispositivo no está inscrito en MDM, los usuarios del dispositivo serán dirigidos a esta URL para la inscripción. Al realizar la configuración, utilice el formato HTTPS. Si hospeda una página en su organización para que redirija a los usuarios de dispositivos para obtener información de Inscripción, añada ese enlace aquí.
    - **URL de corrección (opcional)**: si el dispositivo no está conforme, los usuarios del dispositivo serán dirigidos a esta URL para su corrección. Al realizar la configuración, utilice el formato HTTPS. Si hospeda una página en su organización para que redirija a los usuarios de dispositivos para obtener información sobre corrección, añada ese enlace aquí.
4. Haga clic en **Conectar cuenta**. Se abre el cuadro de diálogo Validación de abonados de Azure.

> Los abonados actualmente conectados a Azure y que deseen agregar conformidad de dispositivos para dispositivos macOS deben desconectar la cuenta y luego restablecer la conexión.

5. En el cuadro de diálogo Validación de abonados de Azure, haga clic en el **enlace** del paso 1.
6. **Iniciar sesión**.
7. Revise los permisos y haga clic en **Aceptar**.

> Si se conecta y la página le pide que vuelva a conectarse, cierre la pestaña/ventana del navegador.

8. Volver a Ivanti Neurons for MDM. En la casilla de diálogo Conectar cuenta de Azure, marque la casilla de verificación **He dado mi consentimiento**. Haga clic en **Confirmar**.

- Para editar la cuenta, haga clic en **Editar la cuenta**.
- Para desconectar la cuenta, haga clic en **Desconectar la cuenta**. Para obtener más instrucciones, consulte Cancelar el aprovisionamiento del inquilino de Azure.
- Toda la actividad de adición, edición y desactivación de una cuenta se almacena en los Registros.

12.5.5.6. Creación de una directiva de cumplimiento de los dispositivos de los socios

Cree una política de cumplimientos para el dispositivos asociado en Ivanti Neurons for MDM y aplique la etiqueta que desee. La política de conformidad de socios informa del estado de conformidad del dispositivo a Azure o a BeyondCorp para el acceso condicional.

Aplicable a

- iOS
- Android
- Windows

Requisitos previos

Debe tener configurado un ID de abonado de Azure o un ID de Google BeyondCorp. Para obtener más información sobre Conformidad con el dispositivo asociado de Azure, consulte **Conexión de Microsoft Azure con Ivanti Neurons for MDM**.



Procedimiento

1. Inicie sesión en Ivanti Neurons for MDM, vaya a **Configuraciones**.
2. Haga clic en **Agregar** y busque la configuración **Cumplimiento del dispositivo socio** .
3. Introduzca los siguientes datos en la página **Crear configuración de conformidad de dispositivos socios**:

Elemento	Descripción
Nombre,	Introduzca nombre.
+ Añadir descripción	Introduzca una explicación.
Elegir socio	Seleccione **Conformidad con Microsoft Azure**. o **Google BeyondCorp Compliance: beta**.
Establecimiento de la configuración Informar del estado de conformidad a Azure para dispositivos iOS, macOS y Android.	Está activado de manera predeterminada. Si no ve este campo, debe configurar su ID de abonado de Azure. Si la opción Informar del estado de conformidad de dispositivos iOS, macOS y Android está activada y la política de conformidad se aplica al cliente, este mostrará "Acceso a Microsoft 365" en los dispositivos en Configuración. Se informa del estado de cumplimiento del dispositivo cuando: • el dispositivo no es compatible • el dispositivo es compatible • el dispositivo vuelve a ser compatible • pases de 24 horas. Si no hay cambios en el estado, se envía un informe una vez por semana/cada siete días.
Informar del estado de conformidad a Google BeyondCorp para dispositivos iOS, macOS, Android y Windows.	Está activado de manera predeterminada. Se informa del estado de cumplimiento del dispositivo cuando: • el dispositivo no es compatible • el dispositivo es compatible • el dispositivo vuelve a ser compatible • pases de 24 horas. Si no hay cambios en el estado, se envía un informe cada 24 horas.

4. Haga clic en **Siguiente**.
5. **Habilitar esta configuración** está seleccionada de manera predeterminada.
6. Seleccione un nivel de distribución para la configuración. Para obtener más información sobre la distribución de la configuración, consulte **Añadir una configuración**.
7. Haga clic en **Hecho**.

12.5.5.7. Estado del dispositivo que notifica desde Ivanti Neurons for MDM a Azure

En los siguientes casos, Ivanti Neurons for MDM informa del inventario de dispositivos y del estado de cumplimiento.

- Cambio de estado del cumplimiento en el dispositivo
- Cambio de inventario en el dispositivo
- Una vez a la semana, Ivanti Neurons for MDM informa del estado de cumplimiento y del inventario

En función de la acción seleccionada en la directiva de cumplimiento, se enviará el siguiente estado del dispositivo:

Acción **(se aplica la más restrictiva)**	**Lo que envía Ivanti Neurons for MDM**
Bloquear correo electrónico, Aplicaciones de AppConnect, Cuarentena	Dispositivo no compatible
Enviar alerta	Compatible con Azure
Retirar un dispositivo	Datos del dispositivo eliminados de la plataforma de Azure

Página de detalles del dispositivo

Para ver la información de Azure sobre el dispositivo, visite la página de detalles del dispositivo. La descripción de los campos y sus posibles valores:

Campo	Descripción
Identificador del dispositivo Azure	El Id. de dispositivo informado por Microsoft al dispositivo iOS o Android. Por ejemplo: 007c8232-9489-4074-9b35-345b16f0a72d. Ivanti Neurons for MDM recibe este Id. de dispositivo porque los usuarios de dispositivos tienen que registrarse en la aplicación Autenticador de Microsoft. Si no puede obtener el Id. de dispositivo, este campo se deja en blanco.
Estado de cumplimiento del dispositivo Azure	Detalla el estado de cumplimiento del dispositivo en Azure. Valores posibles: • En curso • Correcto • Error
Código de estado del cliente de Azure	Indica si el dispositivo está o no conectado a Azure. Valores posibles: • Correcto: se pudo obtener el Id. de dispositivo. • Internal_Error: se produjo un error irrecuperable por parte del cliente o del servidor. • Workplace_Join_Required: es necesario registrar el dispositivo. El usuario del dispositivo puede mitigar este estado. • Interaction_Required: es necesario un inicio de sesión interactivo. El usuario del dispositivo puede mitigar este estado. • Server_Declined_Scopes: no se concedió acceso a algunos ámbitos. • Server_Protection_Policies_Required: el recurso solicitado está protegido por una directiva de Acceso condicional de Intune. • User_Canceled: el usuario del dispositivo canceló la sesión de autenticación web al tocar el botón «Hecho» o «Cancelar» del navegador web. • Account_logged_out: se cerró la sesión de la cuenta.
Hora del informe de cumplimiento del dispositivo Azure	La hora en que Ivanti Neurons for MDM informó sobre el estado de cumplimiento de los dispositivos a Microsoft Intune. Un campo en blanco indica una de las siguientes situaciones: • esa característica está deshabilitada • Ivanti Neurons for MDM recibió los datos y todavía tiene que llamar a la API de Microsoft • hay un error como user_Cancelled o Error interno

12.5.5.8. Cancelar el aprovisionamiento del inquilino de Azure

Si se habilitan múltiples Ivanti Neurons for MDM para que utilicen el mismo abonado de Azure, cancele el aprovisionamiento de todos los Ivanti Neurons for MDM. Si un solo Ivanti Neurons for MDM precisa dejar de utilizar Azure, puede deshabilitar la directiva de cumplimiento de socios únicamente para ese Ivanti Neurons for MDM.

Si el administrador desconecta una Ivanti Neurons for MDM, esta deja de informar sobre el inventario del dispositivo y el estado de cumplimiento con Azure.

Requisitos previos

- asegúrese de que todos los dispositivos sean no gestionados
- asegurarse de que todos los dispositivos sean no conformes

Procedimiento

Microsoft

1. Inicie sesión en Microsoft Azure.
2. Acceda a Intune > Acceso condicional. Asegúrese de que la directiva de acceso condicional esté deshabilitada.

Ivanti Neurons for MDM

1. Inicie sesión en Ivanti Neurons for MDM y vaya a Administrador.
2. En el panel de navegación izquierdo, haga clic en Microsoft Azure > Cumplimiento de los dispositivos para iOS y Android.
3. Haga clic en Desconectar la cuenta.



4. Haga clic en Sí.

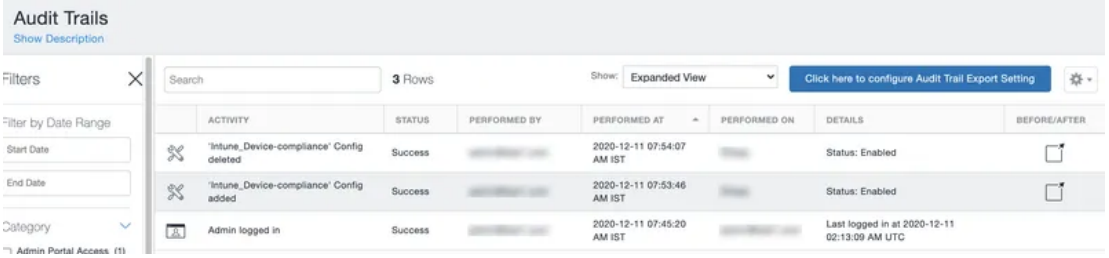
Retirar un dispositivo de Azure

Al retirar el dispositivo, Ivanti Neurons for MDM informa a Azure de que el dispositivo ya no se administra y de que no es compatible.

Azure elimina la entrada del dispositivo retirado después de 90 días.

Actividad de la cuenta de Azure almacenada en los registros

Toda la actividad se almacena en los Registros.



12.5.6. Administrador > Microsoft Azure > Office 365 App Protection

Licencia: Gold

Puede configurar políticas de protección de aplicaciones de Office 365 para ayudarle a proteger los datos de su empresa. Estas políticas aplican los controles de Prevención de pérdida de datos (DLP, en inglés) para las aplicaciones de Microsoft Office 365 que utilizan API de Microsoft Graph. Algunas de estas API de Graph permiten a los administradores garantizar la protección de las aplicaciones nativas de iOS y Android que aprovechan el SDK de Graph.

Utilice esta función para reforzar políticas como las siguientes:

- Impedir que los usuarios puedan imprimir desde aplicaciones de Office 365.
- Evitar compartir datos con el exterior desde las aplicaciones de Office 365.
- Obligar el uso del PIN para las aplicaciones de Office 365.
- Desactivar la sincronización de contactos desde las aplicaciones de Office 365.

Requisitos previos para usar la protección de aplicaciones de Office 365

Antes de hacer uso de la protección de aplicaciones de Office 365, debe tener:

- Una licencia válida de MobileIron
- La función de protección de aplicaciones de Office 365 está habilitada en Ivanti Neurons for MDM
- Una suscripción a Intune o a Microsoft EMS que incluya Intune.
    - Cada uso al que se aplica la política requiere una licencia, pero para habilitar y probar la integración se requiere solo una licencia.
- Una suscripción válida a Office Enterprise o Business con acceso a aplicaciones de Office 365 en un dispositivo móvil.
- Una o varias aplicaciones de Office 365.
- Sincronice sus usuarios de Active Directory con su Entra ID.
- Un Drive for Business instalado en los dispositivos para proteger los datos en Word, Excel y PowerPoint. Esto no es obligatorio.
- Acceso al portal Microsoft Azure (**https://portal.azure.com/**) para configurar las políticas de protección de las aplicaciones de Intune.
- Aplicación Intune Company Portal instalada en dispositivos Android.
  Los usuarios de dispositivos no están obligados a iniciar sesión, pero esta aplicación debe estar instalada en el dispositivo para proteger los datos del mismo. La protección se aplicará cuando el usuario inicie sesión en la aplicación.

Registrar MobileIron como aplicación de Azure

Este apartado describe cómo registrar y almacenar sus credenciales de abonado de Azure con el software Ivanti Neurons for MDM y administrar de forma remota las políticas de protección de aplicaciones en la nube de Microsoft Azure para aplicaciones de Office 365 de Android y iOS. Aunque no es necesario, se pueden abrir dos navegadores para realizar los pasos de los siguientes procedimientos. Con el primer navegador deberá iniciar sesión en el portal de Microsoft Azure. Con el segundo navegador deberá iniciar sesión en el portal de administración Ivanti Neurons for MDM.

Procedimiento del portal de Microsoft Azure

Microsoft puede cambiar la interfaz de usuario del portal Azure de vez en cuando. Estas instrucciones dan por hecho que usted está familiarizado con Microsoft Portal Azure y puede hacer los ajustes necesarios cuando registre MobileIron como una aplicación Azure.

1. Abra el primer navegador e inicie sesión en el portal de Microsoft Azure (https://portal.azure.com/).
2. Haga clic en **Registros de aplicaciones** en el panel izquierdo.
3. Haga clic en **+Registro de nueva aplicación**.
4. Introduzca la siguiente información para registrar MobileIron como aplicación de Azure.
    - **Nombre:** escriba un nombre para la aplicación de MobileIron. (Este campo debe tener al menos 4 caracteres).
    - **Tipo de aplicación:** seleccione Aplicación web/API.
    - **URL de inicio de sesión:** introduzca la URL a la que acceden los usuarios de los dispositivos para iniciar sesión en MobileIron (obligatorio).

Haga clic en **Crear** en la parte inferior del panel para añadir la aplicación y volver a la página de inicio de Azure.

6. Haga clic en la aplicación de MobileIron recientemente creada en la página de inicio de Azure.
7. Vuelva a la página de inicio de Azure para asignar permisos a la aplicación de MobileIron Azure.
8. Para establecer los permisos de API necesarios para la aplicación MobileIron recién creada, haga clic en el nombre de la aplicación en Registros de aplicaciones.
9. Haga clic en **Permisos de API** > **Añadir un permiso**.
10. En la sección **Microsoft Graph > Permisos delegados > Aplicaciones de administración de dispositivos**, seleccione el permiso **DeviceManagementApps.Read.All** y haga clic en **Guardar**. De forma predeterminada, se activará el permiso user.Read para la aplicación.
11. Para conceder el acceso, haga clic en **Otorgar consentimiento del administrador para MobileIron**.
12. Realice el siguiente procedimiento para el portal de administración de Ivanti Neurons for MDM.

Procedimiento para el portal administrativo de Ivanti Neurons for MDM

1. Abra el segundo navegador e inicie sesión en el portal de administración Ivanti Neurons for MDM.
2. Vaya a **Administrador > Microsoft Azure > Office 365 App Protection**.
3. Pegue la **ID de la aplicación** en el portal de administración Ivanti Neurons for MDM .
4. **Procedimiento**
    1. Vaya al portal de Azure.
    2. Seleccione la aplicación de MobileIron > **Propiedades**.
    3. Copie el **Id. de la aplicación**.
    4. Vuelva a **Administrador > Microsoft Azure > Office 365 App Protection** en el Portal de administración.
    5. Péguelo en el campo **Id. de la aplicación**.

Pegue el **Secreto de la aplicación** (secreto del cliente) en el Portal de administración Ivanti Neurons for MDM .

5. **Procedimiento**
    1. Vaya al portal de Azure.
    2. Seleccione la aplicación de MobileIron.

3. Haga clic en **Claves** e introduzca un nombre en la **Descripción de la clave** y seleccione un tiempo-período de caducidad en **Duración**.
4. Haga clic en **Guardar** y copie el valor **Clave**.
5. Vuelva a **Administrador > Microsoft Azure > Office 365 App Protection** en el Portal de administración.
6. Péguelo en el campo **Secreto de la aplicación**.

Pegue el **Id. del abonado** en el portal de administración Ivanti Neurons for MDM .

6. **Procedimiento**
    1. Vaya al portal de Azure.
    2. Haga clic en Entra ID en el panel izquierdo y luego en Propiedades.
    3. Copie el Id. de Directory.
    4. Vuelva a **Administrador > Microsoft Azure > Office 365 App Protection** en el Portal de administración.
    5. Péguelo en el campo **Id. del abonado**.

Introduzca su **Nombre de usuario** y **Contraseña** de administrador de Intune.

- La cuenta Azure debe tener derechos de administración global o derechos limitados de administración + de administración del servicio de Intune.
- Ivanti recomienda crear una cuenta local Azure con solo los derechos de administración del servicio de Intune. Las cuentas de usuario que se federan a un proveedor de identidad no son compatibles con Microsoft para la autenticación con las API de Graph.

Haga clic en **Autenticar y Guardar**.
Si la fecha introducida es incorrecta, aparecerá un mensaje de error.

Políticas para la protección de aplicaciones de Office 365

Después de configurar las credenciales de Microsoft Graph, vaya a **Aplicaciones > Protección de la aplicación Office 365** para añadir nuevas políticas de protección de aplicaciones de Office 365 para dispositivos iOS o Android para diferentes grupos de usuarios.

Las políticas se enumeran en la página **Aplicaciones > Protección de aplicaciones de Office 365**, en la pestaña **Políticas de aplicaciones**. Esta lista de políticas ofrece detalles tabulares como la marca de hora actualizada, la plataforma, aplicaciones asignadas y grupos de usuarios implementados.

Añadir una política de protección de aplicaciones de Office 365 para dispositivos iOS

Procedimiento

1. Vaya a **Aplicaciones > Protección de aplicaciones de Office 365**.
2. Haga clic en **Políticas de aplicaciones > + Añadir**.
3. Introduzca un **Nombre** y una **Descripción** opcional para la política.
4. En Elegir SO, haga clic en **iOS**.
5. En **Reubicación de los datos**, seleccione una opción de los siguientes ajustes y opciones:
    - Impedir copias de seguridad de iTunes y iCloud

- Permitir que la aplicación transfiera datos a otras aplicaciones: Todas las aplicaciones (predeterminado), Aplicaciones administradas por políticas, Ninguna
- Permitir que la aplicación reciba datos de otras aplicaciones: Todas las aplicaciones (predeterminado), Aplicaciones administradas por políticas, Ninguna
- Impedir la función «Guardar como»
- Restringir las funciones de cortar, copiar y pegar con otras aplicaciones: Cualquier aplicación (predeterminado), Bloqueado, Aplicaciones administradas por políticas, Política administrada con función «pegar en»
- Restringir el contenido web que se mostrará en el navegador administrado
- Cifrar datos de las aplicaciones: Cuando el dispositivo está bloqueado (predeterminado), Cuando el dispositivo está bloqueado y hay archivos abiertos, Después del reinicio del dispositivo, Usar ajustes del dispositivo
- Desactivar la sincronización de contactos
- Desactivar la impresión

6. En **Acceso**, seleccione una opción de los siguientes ajustes y opciones:
   - Requerir un PIN para el acceso
   - Número de intentos permitidos antes de restablecer el PIN (valor predeterminado: 5 intentos)
   - Permitir un PIN simple
   - Longitud del PIN (valor predeterminado: 4)
   - Permitir huella digital en lugar de PIN (iOS 8+)
   - Desactivar el PIN de la aplicación cuando el PIN del dispositivo está administrado
   - Requerir credenciales corporativas para acceder
   - Bloquear aplicaciones administradas para que no puedan ejecutarse en dispositivos con «jailbreaks» y descifrados.
   - Volver a comprobar los requisitos de acceso después de (minutos)
     - Tiempo de espera: debe ser un valor entre 1 y 65535 (valor predeterminado: 30)
     - Período de gracia sin conexión: debe ser un valor entre 1 y 65535 (valor predeterminado: 720)
     - Intervalo sin conexión (días) antes de borrar los datos de la aplicación: debe ser un valor entre 1 y 65535 (valor predeterminado: 90)

   Requerir un sistema operativo mínimo de iOS
   - Requerir un sistema operativo mínimo de iOS (solo advertencia)
   - Requiere una versión mínima de la aplicación
   - Requerir una versión mínima de la aplicación (solo advertencia)
   - Requiere una versión mínima de SDK de la política de protección de aplicaciones de Intune

Haga clic en **Siguiente**.

8. Seleccione y asigne las aplicaciones en las que se implementará esta política.
9. Haga clic en **Siguiente**.
10. Seleccione los grupos de usuarios en los que se aplicará esta política.
11. Haga clic en **Hecho**.

Añadir una política de protección de aplicaciones de Office 365 para dispositivos Android

Procedimiento

1. Vaya a **Aplicaciones > Protección de aplicaciones de Office 365**.
2. Haga clic en **Políticas de aplicaciones > + Añadir**.
3. Introduzca un **Nombre** y una **Descripción** opcional para la política.
4. En Elegir SO, haga clic en **Android**.
5. En **Reubicación de los datos**, seleccione una opción de los siguientes ajustes y opciones:
    - Impedir copias de seguridad de Android
    - Permitir que la aplicación transfiera datos a otras aplicaciones: Todas las aplicaciones (predeterminado), Aplicaciones administradas por políticas, Ninguna
    - Permitir que la aplicación reciba datos de otras aplicaciones: Todas las aplicaciones (predeterminado), Aplicaciones administradas por políticas, Ninguna
    - Impedir la función «Guardar como»
    - Restringir las funciones de cortar, copiar y pegar con otras aplicaciones: Cualquier aplicación (predeterminado), Bloqueado, Aplicaciones administradas por políticas, Política administrada con función «pegar en»
    - Restringir el contenido web que se mostrará en el navegador administrado
    - Cifrar datos de las aplicaciones
    - Desactivar el cifrado de aplicaciones cuando está activado el cifrado de dispositivos
    - Desactivar la sincronización de contactos
    - Desactivar la impresión
6. En **Acceso**, seleccione una opción de los siguientes ajustes y opciones:
    - Requerir un PIN para el acceso
    - Número de intentos permitidos antes de restablecer el PIN (valor predeterminado: 5 intentos)
    - Permitir un PIN simple
    - Longitud del PIN (valor predeterminado: 4)
    - Permitir huella digital en lugar de PIN (Android 6+)
    - Desactivar el PIN de la aplicación cuando el PIN del dispositivo está administrado
    - Requerir credenciales corporativas para acceder
    - Bloquear aplicaciones administradas para que no puedan ejecutarse en dispositivos con «jailbreaks» y descifrados.
    - Volver a comprobar los requisitos de acceso después de (minutos)
        - Tiempo de espera: debe ser un valor entre 1 y 65535 (valor predeterminado: 30)
        - Período de gracia sin conexión: debe ser un valor entre 1 y 65535 (valor predeterminado: 720)
        - Intervalo sin conexión (días) antes de borrar los datos de la aplicación: debe ser un valor entre 1 y 65535 (valor predeterminado: 90)
    - Bloquear captura de pantalla y asistente de Android
    - Requerir un sistema operativo mínimo de Android
    - Requerir un sistema operativo mínimo de Android (solo advertencia)
    - Requiere una versión mínima de la aplicación
    - Requerir una versión mínima de la aplicación (solo advertencia)

- Requiere una versión mínima de SDK de la política de protección de aplicaciones de Intune

7. Haga clic en **Siguiente**.
8. Seleccione las aplicaciones en las que se implementará esta política.
9. Haga clic en **Siguiente**.
10. Seleccione los grupos de usuarios en los que se aplicará esta política.
11. Haga clic en **Hecho**.

Modificar una política de protección de aplicaciones de Office 365

Procedimiento

1. Vaya a **Aplicaciones > Protección de aplicaciones de Office 365**.
2. Haga clic en **Políticas de aplicaciones**.
3. Haga clic en el nombre de la política que desee modificar.
4. En la página de detalles de la política, haga clic en **Editar**.
5. Modifique los ajustes de configuración de la política.
6. Haga clic en **Siguiente**.
7. Modifique la lista de aplicaciones en las que se aplicará esta política.
8. Haga clic en **Siguiente**.
9. Modifique los grupos de usuarios en los que se aplicará esta política.
10. Haga clic en **Hecho**.

Eliminar una política de protección de aplicaciones de Office 365

Procedimiento

1. Vaya a **Aplicaciones > Protección de aplicaciones de Office 365**.
2. Haga clic en **Políticas de aplicaciones**.
3. En la columna **Acciones**, haga clic en el icono de eliminar que hay junto al nombre de la política que desea eliminar.
4. Haga clic en **Sí** para confirmar.

Configuraciones de las aplicaciones de Office 365

Vaya a la página **Aplicaciones > Protección de aplicaciones de Office 365**, en la pestaña **Configuración de aplicaciones**, para añadir, modificar o eliminar las configuraciones de aplicaciones de Office 365 para diferentes grupos de usuarios. En las configuraciones de estas aplicaciones, los administradores pueden añadir una lista de pares clave/valor. y asignar las configuraciones a una o más aplicaciones de Office 365. La pestaña Configuración de aplicaciones enumera las configuraciones con detalles tabulares como la marca de hora actualizada, las aplicaciones asignadas y el estado de la implementación.

Añadir una configuración de las aplicaciones de Office 365

Procedimiento

1. Vaya a **Aplicaciones > Protección de aplicaciones de Office 365**.
2. Haga clic en **Configuración de aplicaciones > + Añadir**.

3. Introduzca un **Nombre** y una **Descripción** opcional para la configuración.
4. Introduzca los pares clave/valor.
5. Haga clic en **Siguiente**.
6. Seleccione las aplicaciones en las que se implementará esta configuración.
7. Haga clic en **Siguiente**.
8. Seleccione los grupos de usuarios en los que se aplicará esta configuración.
9. Haga clic en **Hecho**.

Modificar una configuración de las aplicaciones de Office 365

Procedimiento

1. Vaya a **Aplicaciones > Protección de aplicaciones de Office 365**.
2. Haga clic en **Configuración de aplicaciones**.
3. Haga clic en el nombre de la configuración que desee modificar.
4. En la página de detalles de configuración, haga clic en **Editar**.
5. Alternativamente, también puede hacer clic en las pestañas **Distribución de aplicaciones** o **Distribución de grupo de usuarios**. Haga clic en **Editar** para modificar solo esos ajustes y haga clic en **Guardar**.
6. Modifique los ajustes de configuración.
7. Haga clic en **Siguiente**.
8. Modifique la lista de aplicaciones en las que se aplicará esta configuración.
9. Haga clic en **Siguiente**.
10. Modifique los grupos de usuarios en los que se aplicará esta configuración.
11. Haga clic en **Hecho**.

Eliminar una configuración de las aplicaciones de Office 365

Procedimiento

1. Vaya a **Aplicaciones > Protección de aplicaciones de Office 365**.
2. Haga clic en **Configuración de aplicaciones**.
3. En la columna **Acciones**, haga clic en el icono de eliminar que hay junto al nombre de la configuración que desea eliminar.
4. Haga clic en **Sí** para confirmar.

Usuarios que infringen el cumplimiento de las aplicaciones de Office 365

Los administradores pueden revisar la lista de usuarios y sus dispositivos en cuanto al no cumplimiento. Utilice esta página para borrar cualquier aplicación de Office 365 en dichos dispositivos marcados.

Borrar aplicaciones de Office 365

Procedimiento

1. Vaya a **Aplicaciones > Protección de aplicaciones de Office 365**.
2. Haga clic en **Usuarios que infringen el cumplimiento**.

3. Lleve a cabo una de las siguientes acciones:
    - Seleccione a los usuarios de la lista y haga clic en **Borrar aplicaciones de Office 365**.
    - Haga clic en el nombre del usuario para visualizar la lista de dispositivos que tienen aplicaciones que infringen el cumplimiento. En la columna **Acción**, haga clic en el icono **Borrar aplicaciones de Office 365** que hay junto a un dispositivo específico.
    - Haga clic en el nombre del usuario para visualizar la lista de dispositivos que tienen aplicaciones que infringen el cumplimiento. Haga clic en el nombre de un dispositivo específico para ver las aplicaciones enumeradas con Id. del conjunto/nombres de paquetes y los motivos marcados. Haga clic en **Borrar aplicaciones de Office 365**.
4. Haga clic en **Sí** para confirmar la acción.

Alternativamente, lleve a cabo los siguientes pasos:

1. Vaya a **Usuarios.**
2. Haga clic en el nombre del usuario para visualizar la página de detalles del usuario.
3. Haga clic en **Acción > Borrar aplicaciones de Office 365**.
4. Seleccione los dispositivos de los que hay que borrar aplicaciones de Office 365.
5. Haga clic en **Aceptar** para confirmar la acción.

Cancelar solicitudes de borrado de aplicaciones de Office 365

Procedimiento

1. Vaya a **Usuarios.**
2. Haga clic en el nombre del usuario para visualizar la página de detalles del usuario.
3. Haga clic en la pestaña **Protección de Office 365**.
4. Desde el cuadro desplegable **Seleccionar tipo de informe**, seleccione el informe **Solicitudes de borrado** para visualizar la información correspondiente.
5. Seleccione los dispositivos en los que hay que cancelar solicitudes de borrado. Solo se pueden seleccionar dispositivos con estado «Borrado pendiente».
6. Haga clic en **Cancelar borrado**.
7. Haga clic en **Aceptar** para confirmar la acción.

Informes de aplicaciones para los usuarios con la Protección de aplicaciones de Office 365

Los administradores pueden seleccionar uno de los siguientes informes para revisar la lista de usuarios con Protección de aplicaciones de Office 365 e información relacionada:

- Informe de política de aplicaciones
- Informe de configuración de aplicaciones
- Borrar solicitudes

La información en los Informes de aplicaciones incluye el Id. del conjunto/nombre del paquete, Nombre del dispositivo, Tipo de dispositivo, Políticas o Configuraciones (implementadas en el dispositivo, Estado (Sincronizado, Sincronizado pero desactualizado o No sincronizado) y la hora del Último ingreso. La información de los Informes de aplicaciones se puede exportar a un archivo CSV para consultarla o analizarla posteriormente.

La información del informe de Solicitudes de borrado incluye en Nombre en pantalla, Nombre del usuario, Nombre del dispositivo, Tipo de dispositivo y Estado de borrado (Borrado pendiente o Borrado completo).

Realice los siguientes pasos para ver uno de los informes:

1. Vaya a **Usuarios.**
2. Haga clic en el nombre del usuario para visualizar la página de detalles del usuario.
3. Haga clic en la pestaña **Protección de Office 365**.
4. Desde el cuadro desplegable **Seleccionar tipo de informe**, seleccione uno de los informes para visualizar la información correspondiente.
5. (Opcional) Desde la página de informes de Solicitudes de borrado, seleccione los dispositivos en los que hay que cancelar solicitudes de borrado y haga clic en **Cancelar borrado**. Solo se pueden seleccionar dispositivos con estado «Borrado pendiente».
6. (Opcional) Haga clic en **Exportar a CSV** para descargar el contenido del informe en un archivo CSV para consultarlo o analizarlo posteriormente.

12.6. Conectar con Google Apps

Esta sección contiene los siguientes temas:

- Cuentas administradas de Google Play (cuentas con Android Enterprise)
- Registro de dispositivos Android
- API de administración de Android
- API de Google Apps
- Administrador- Android Enterprise

12.6.1. Cuentas administradas de Google Play (cuentas con Android Enterprise)

Licencia: Silver

Las cuentas administradas de Google Play son necesarias para habilitar el uso y configuración de dispositivos con Android Enterprise. Ya no es necesario que use Google Apps Directory Sync (GADS) o las cuentas de Google para registrar los dispositivos.

Importante: si ya ha configurado Android Enterprise, primero debe retirar esos dispositivos para poder usar esta función.

Configuración de Android Enterprise utilizando una cuenta administrada de Google Play

Procedimiento

1. Inicie sesión en el portal de Ivanti Neurons for MDM.
2. Vaya a **Administrador > Google > Android Enterprise**.
3. En **Cuenta de Google Play administrada**, haga clic en **Autorizar Google** para mostrar la página de **Google Play for Work** .
4. Introduzca la **dirección de correo electrónico de su cuenta de Google Play**.
5. Haga clic en **Comenzar**.
6. Acepte el acuerdo de Android Enterprise.
7. Haga clic en **Confirmar**.
8. Haga clic en **Completar registro**.
   La sección **Android Enterprise configurado** muestra la siguiente información:
   - **Estado**
   - **Correo electrónico del administrador**
   - **Tipo de empresa**
   - **ID de empresa de Google**

Cuando Android Enterprise esté configurado mediante las cuentas de Google Play, hay un límite en el número de dispositivos que se pueden inscribir por usuario. Para superar esta limitación, cuando cree un nuevo usuario, seleccione la opción **Cuenta de dispositivo con Android Enterprise** para activar que se asigne automáticamente una Cuenta de dispositivo Google a las inscripciones de dispositivos administrados en el trabajo con Android Enterprise vinculadas a esta cuenta.

Las cuentas de dispositivos están previstas para implementaciones de tipo COSU (un solo uso), como por ejemplo con el modo Kiosco. Es posible que los usuarios con cuentas de dispositivos tengan acceso limitado a Google Play.

De vez en cuando, una cuenta administrada de Google Play o su token caduca por diferentes motivos, como la caducidad del token de autenticación o la cuenta o empresa que se va a borrar. En dichas situaciones, los servicios de Google Play notificarán al cliente con una acción de retransmisión que hará que el cliente reaprovisione el dispositivo eliminando la cuenta existente y añadiendo una cuenta con un token nuevo obtenido del servidor de UEM.

En esos casos, no se puede reaprovisionar la cuenta porque la cuenta anterior no se ha podido eliminar o porque se han producido demasiados intentos de reaprovisionamiento. Al usuario se le notifica para que vuelva a empezar de nuevo retirando el cliente o restableciendo los valores de fábrica del dispositivo, según sea el caso, en función de si el dispositivo está en modo perfil de trabajo o en modo dispositivo administrado.

Migrar una cuenta existente de Managed Google Play a una cuenta de Managed Google Domain (BTE).

Esta función permite migrar cuentas y dispositivos de **Managed Google Play Account** a una cuenta de **Managed Google Domain**.

La migración comprende:

- Actualización de la cuenta
- Migración de dispositivos

Requisitos previos

- Los dispositivos deben estar inscritos en el modo Dispositivo administrado por el trabajo o Perfil de trabajo. Los dispositivos inscritos en el modo Perfil de trabajo en dispositivo propiedad de la empresa (WPCOD) deben utilizar Android 12 o una versión posterior.
- Los dispositivos deben tener asignada una dirección de correo electrónico corporativa o profesional válida..

> Si el dispositivo tiene asignada una dirección de correo electrónico no corporativa, el administrador debe asignarle una válida para que pueda optar a la migración.

Actualizar la cuenta de Android Enterprise

Actualice la cuenta de Android Enterprise de Managed Google Play a Managed Google Domain.

Procedimiento

1. Vaya a **Administración** > **Google** > **Android Enterprise**.
2. Haga clic en **Actualizar cuenta**.
3. Inicie sesión con una dirección de correo electrónico corporativa o profesional válida.
4. Complete el proceso de actualización.
5. Actualice la página.

Aplicar la configuración de migración de dispositivos

Procedimiento

1. Vaya a Configuraciones.
2. Seleccione **Android Enterprise: Migración de dispositivos de Managed Google Play a Managed Google Account** y, a continuación, > **Editar** > **Siguiente** > **Todos los dispositivos o Personalizado** > **Distribución gradual** – De forma predeterminada está seleccionada la opción **Implementación manual** > Elija el **porcentaje de dispositivos** o **todos los dispositivos en el resumen de selección**.
3. Haga clic en **Hecho**.

Migración de dispositivos

Procedimiento

1. En el dispositivo, pulse **Continuar** cuando se le solicite "Añadir su cuenta de trabajo".
2. Verifique que la **dirección de correo electrónico corporativa** sea correcta.
3. Introduzca la **contraseña**.
4. Complete la **autenticación de dos factores (2FA),**si está disponible.
5. Complete el proceso de configuración de la cuenta.

Verificar la migración

En el dispositivo

1. Abra **Google Play Store**.
2. Confirme que el tipo de cuenta haya cambiado de Cuenta de trabajo a Cuenta de dominio corporativo.

En la consola de administración

- Para consultar el estado de esta configuración, vaya a **Android Enterprise: Migración de dispositivos de Managed Google Play a Managed Google Account** navegue hasta **Dispositivos** > **Dispositivos** > **Detalles del dispositivo** > **Configuración** > **Android Enterprise: Migración de dispositivos de Managed Google Play a Managed Google Account)**. Asegúrese de que el estado de la configuración sea Instalado.

Monitorización del estado de migración

Los administradores pueden rastrear el progreso de la migración (**Migrada a Managed Google Account** mediante:

- **Detalles del dispositivo:** consulte el estado de la migración de cada dispositivo.
- **Búsqueda avanzada:** filtre los dispositivos según su estado de migración.
- **Grupos de dispositivos:** agrupe los dispositivos migrados y no migrados.

Estas opciones permiten identificar los dispositivos que requieren alguna acción adicional.

Nueva inscripción con una cuenta de Managed Google Domain (BTE)

Android Enterprise se puede configurar mediante una cuenta de **Managed Google Domain Account** con o sin autenticación de Google.

Procedimiento

1. Inicie sesión en el portal.
2. Vaya a **Administrador** > **Google** > **Android Enterprise**.
3. En **Cuenta de Managed Google Play**, haga clic en **Autorizar**.
4. Introduzca su **dirección de correo electrónico corporativa** o **profesional** y haga clic en **Siguiente**.
5. Seleccione **Crear una nueva vinculación con...** en la página **Seleccionar una opción de vinculación** .
6. Haga clic en **Confirmar**. Se mostrarán las opciones **Omitir** y **Habilitar**.

- **Omitir**: para continuar sin autenticación
- **Habilitar**: para continuar con autenticación.

En la sección Android Enterprise se muestra la siguiente información:

- **Estado**: muestra el estado de la conexión.
- **Correo electrónico del administrador**: muestra la dirección de correo electrónico corporativa o profesional utilizada.
- **Tipo de empresa**: muestra el tipo de empresa.
- **Ajustes de autenticación de Google**: muestra No o Sí según sea necesario utilizar autenticación.
- **ID de empresa de Google**: muestra un identificador único de empresa de Google.
- **Nombre de la empresa**: muestra el nombre de la empresa.

12.6.2. Registro de dispositivos Android

Durante el registro de un dispositivo Android puede configurar esta opción si requiere permisos de teléfonos de usuarios, lo cual es obligatorio para comunicar el IMEI, el número de teléfono y otros identificadores del teléfono para completar el registro. Una vez configurada, a los usuarios del dispositivo se les pedirá que otorguen su permiso para permitir que el cliente Go acceda a los identificadores del dispositivo.

> Esta configuración solo es aplicable a los registros nuevos de todos los dispositivos Android con una versión de Android superior a 6.0.

1. Seleccione **Admin > Google > Registro**.
2. Seleccione **Requerir identificadores de dispositivos Android durante el registro (Administración de dispositivos de perfil de trabajo)**.
3. Haga clic en **Guardar**.

Para obtener más información sobre el Modo perdido, consulte **Administración de dispositivos Android en modo Perdido**

12.6.3. API de administración de Android

Android Management API (AMAPI) es la API de la plataforma en la nube de Google que integra las funciones UEM de Google Android en Ivanti Neurons for MDM. En la configuración Android Enterprise, puede habilitar el marco de la API de administración de Android para gestionar los dispositivos de Android Enterprise sin necesidad de tener una aplicación de cliente instalada en los dispositivos para la administración de los mismos. Actualmente, Go app no es compatible con el envío al dispositivo para funciones distintas a MTD, etc.

Cuando tenga una cuenta de Android Enterprise configurada en sus ajustes, podrá habilitar y utilizar el marco de la API de administración de Android. Después de habilitarlo, podrá:

- Añadir un perfil de inscripción para usar el código QR para la inscripción de dispositivos.
- Crear una configuración de dispositivos dedicados (de uso único y propiedad de la empresa, o COSU) para que el dispositivo inscrito cumpla un fin específico.

Actualmente, la API de gestión de Android solo es compatible con los dispositivos que se ejecutan en la versión 9 de Android o superior y que tienen Google Play instalado y aprovisionado en modo Dedicado. El modo dedicado corporativo también se conoce como modo de uso único corporativo (COSU) y es una variante del modo de propietario del dispositivo. Esta función también admite las siguientes acciones del dispositivo:

- Bloquear
- Reiniciar
- Sincronizar con el servidor
- Borrar

Los ingresos del dispositivo se programan a intervalos regulares (cada hora). Pero, para una acción inmediata, use la acción del dispositivo «Sincronizar con el servidor» en la página de detalles del dispositivo. Los dispositivos AMAPI no envían registros obligatorios a Ivanti Neurons for MDM. Las actualizaciones del inventario se realizan cuando hay alguna actividad en el dispositivo.

Habilitar la API de administración de Android

Para habilitar el API de administración de Android, vaya a **Admin > Android Enterprise > Autorizar Google (requiere una dirección de Google válida) > Android Enterprise activado**.

El estado de la función API de administración de Android activada (**Sí** para activado y **No** para desactivado) también se muestra en la página de detalles del dispositivo.

> Las cuentas de GSuite actualmente no son compatibles con COSU.

Agregar un perfil de inscripción

Se requiere la creación de un perfil de inscripción para inscribir un dispositivo Android utilizando el escaneo de código QR o la cadena alfanumérica del token. Los perfiles de inscripción solo se pueden crear cuando la API de administración de Android está habilitada. También puede crear atributos personalizados del dispositivo para asociarlos al perfil de inscripción.

1. Seleccione **Administrador > Android Enterprise > Perfiles de inscripción**.
2. Configure los siguientes ajustes en la ventana **Perfil de Inscripción - Dispositivo dedicado de propiedad corporativa** .
3. Haga clic en **Guardar**. La ventana **Resumen del perfil** muestra los siguientes detalles del token:

Ajuste	Descripción
Nombre,	Introduzca un nombre que identifique a este perfil de inscripción.
Descripción	Introduzca una descripción que explique la finalidad de este perfil de inscripción.
Nombre de usuario	Introduzca las primeras letras de un nombre de usuario válido y seleccione uno de los que se muestran en los resultados coincidentes. Un nombre de usuario válido podría ser de un usuario local o de un usuario LDAP. Los perfiles de inscripción etiquetan los dispositivos inscritos con el código QR en el perfil para que se muestren como dispositivos pertenecientes al usuario para el que se creó el perfil de inscripción.
Validez del token **Atributos personalizados del dispositivo**	Introduzca el número de días de validez del escaneo del código QR del token de autenticación. El número introducido deben estar entre 1 y 30. El dispositivo se reiniciará si utiliza el token o el perfil de inscripción después del período de caducidad. En la columna Acciones, haga clic en **+Añadir nuevo** para añadir atributos personalizados del dispositivo que se asociarán al perfil de inscripción. 1. Seleccione el atributo personalizado de dispositivo en la lista desplegable de la columna **Nombre del atributo**. 2. En la columna **Valor**, introduzca el valor del atributo personalizado. 3. Haga clic en **Guardar**. En la tabla aparecerá el atributo personalizado de dispositivo añadido. Para eliminarlo, haga clic en la opción **Eliminar** de la columna Acciones. Los atributos personalizados solo se pueden agregar a un perfil de inscripción durante la creación del perfil. Los campos de atributos no se pueden editar después de la creación del perfil.

- Nombre
- Descripción
- Nombre de usuario
- Fecha de creación del token
- Fecha de caducidad del token
- Valor del token
- Código QR
- Atributos personalizados del dispositivo.

> Los dispositivos se reinician si la configuración adecuada para el dispositivo no se adquiere en el intervalo de tiempo de 10 minutos después del registro. En tales casos, debe volver a registrarse usando el token de inscripción/código QR.

Cuando se crea un perfil de inscripción, este aparece en la página **Perfiles de inscripción**. Puede realizar cualquiera de las siguientes acciones de la columna **Acciones**.

- Haga clic en el icono Ver para ver los detalles del perfil de inscripción en la ventana Resumen del perfil. El código QR también se muestra en esta ventana.
- Haga clic en el icono Editar para editar los detalles del perfil de inscripción.

> Solo se puede editar la validez del token. No se pueden editar otros atributos.

Haga clic en el icono Eliminar para eliminar el perfil de inscripción.

Crear la configuración COSU

Los administradores pueden configurar dispositivos dedicados que se pueden utilizar para un fin específico con Android Enterprise, utilizando los dispositivos dedicados (configuración COSU: «corporate-owned single use», de un solo uso y propiedad de la empresa). La configuración COSU se distribuye a los dispositivos administrados en el trabajo (modo propietario del dispositivo) para proporcionar una sola aplicación disponible para los usuarios en modo Kiosco. Los dispositivos que están en el Perfil de trabajo en un Dispositivo propiedad de la empresa no son compatibles.

Con esta configuración, el administrador puede configurar los dispositivos para que la aplicación quede anclada en la pantalla de modo que el usuario en modo Kiosco no pueda desanclar esta aplicación y navegar desde la aplicación a otras pantallas del dispositivo o utilizar cualquier otra aplicación del dispositivo.

> También se puede forzar la instalación de otras aplicaciones en el dispositivo AMA seleccionando la opción «Instalar en el dispositivo» en Opciones avanzadas y configuración de aplicaciones, pero no podrá interactuar con ellas mientras la aplicación Kiosco esté fijada en la pantalla a través de la configuración. Para el Kiosco multiaplicación, se recomienda utilizar la funcionalidad de Kiosco del Dispositivo Administrado por el Trabajo (modo propietario del dispositivo). Esto proporciona un mayor control sobre las aplicaciones y la configuración del dispositivo y también puede ampliarse a un modo multiusuario.

Los administradores pueden realizar cambios de configuración, como permitir la navegación por el sistema y la posibilidad de utilizar otras aplicaciones que se transfieren al dispositivo para el usuario final a través del CPD de Google, revisando las distintas opciones en función de sus necesidades.

Las configuraciones COSU están determinadas por la prioridad que se les asigna. La configuración de mayor prioridad se utiliza para insertar la configuración de la política a Google. Las configuraciones COSU se aplican a los dispositivos dentro del espacio definido. Se puede delegar a otros espacios, si se define en el espacio predeterminado.

Para configurarlo:

1. Vaya a **Configuración > +Añadir**.
2. En la configuración **Bloqueo y kiosco: Android Enterprise**, haga clic en **Dispositivos dedicados (de un solo uso y propiedad de la empresa, o COSU)**.
3. Introduzca un nombre para la configuración.
4. Introduzca una descripción.
5. Puede configurar los siguientes ajustes haciendo clic en las pestañas correspondientes:

- **Ajustes de la aplicación**
- **Bloqueos generales**
- **Personalización del kiosco**
- **Ajustes del sistema**

La siguiente tabla proporciona los detalles de los campos configurables:

Ajuste	Descripción
Ajuste de la aplicación **Nombre de la aplicación**	Seleccione la aplicación que se va a anclar en el dispositivo escribiendo el nombre de la aplicación, escriba primero la letra inicial del nombre de la aplicación hasta que vea la aplicación deseada en el menú desplegable. Si no ve la aplicación deseada en el menú desplegable, asegúrese de que la aplicación que desea implementar sea una aplicación Pública/Privada disponible en la Play Store y que se añada al App Catalog. Este campo es obligatorio. No se le permitirá crear la configuración si no selecciona una aplicación para añadir en este campo. Solo puede añadir aplicaciones públicas y privadas. No se pueden añadir aplicaciones internas y aplicaciones web (privadas).
Bloqueos generales	
Mantener la pantalla encendida	Configure los modos de la batería conectada para que el dispositivo permanezca encendido. Seleccione cualquiera de las siguientes opciones: • **CA**: la fuente de alimentación es un cargador de CA. • **Inalámbrico** • **USB**: la fuente de alimentación es un puerto USB. • **Cualquiera**: la fuente de alimentación es un cargador de CA, un puerto USB o un cargador inalámbrico.
Personalización del kiosco	
Personalizar la barra de estado	Seleccione cualquiera de las siguientes opciones para personalizar la barra de estado de los dispositivos de destino: • **Información sobre notificaciones y del sistema activada**: para mostrar información del sistema y notificaciones en la barra de estado. • **Solo información del sistema activada**: para mostrar solo la información del sistema en la barra de estado.
Personalizar la navegación del sistema	Seleccione una de las opciones siguientes para especificar el acceso a las funciones de navegación (Botones de Inicio y Visión general) en el modo Kiosko: • **Activado**: permite la navegación de los botones de Inicio y Resumen. Los usuarios pueden navegar fuera de la aplicación especificada si se selecciona esta opción. • **Deshabilitado**: deshabilita la navegación de los botones de Inicio y Resumen. • **Solo el botón de inicio**: solo permite la navegación del botón de inicio. El botón de regreso está disponible con todas estas opciones.
Habilitar las acciones globales	Seleccione esta opción para activar las acciones globales en el modo Kiosco. La funcionalidad de reinicio y apagado asociada a los botones de encendido se controla a través de esta opción.

Ajuste	Descripción
Habilitar diálogos de errores del sistema	Seleccione esta opción para habilitar los diálogos de error de las aplicaciones que se han bloqueado o que no responden en el modo Kiosco.
Ajustes del sistema	
Ajustes de actualizaciones del sistema	Configure los siguientes ajustes para administrar las actualizaciones del sistema: • **Actualización del sistema**: seleccione el tipo de actualización del sistema requerido. ◦ **Automático**: instalar una actualización automáticamente en cuanto esté disponible. ◦ **Posponer**: pospone la instalación automática hasta un máximo de 30 días. ◦ **En intervalo**: se instala automáticamente dentro de un intervalo diario de mantenimiento. Establezca las horas de inicio y fin para el período del intervalo de mantenimiento. Las actualizaciones instaladas en los dispositivos pueden variar en función del conjunto de funciones compatibles, de la versión de Android y de la versión de Google DPC instalada en el dispositivo. • **Período de congelación**: cuando un dispositivo se configura dentro del período de congelación, todas las actualizaciones entrantes del sistema se bloquean y no se instalan. Haga clic en **Añadir período de congelación** para establecer la **fecha de inicio** y la **fecha de fin** del período de congelación. Cuando un dispositivo está fuera del período de congelación, se aplica el comportamiento de actualización normal. Si la fecha final es anterior a la fecha de inicio, el período de congelación se prorroga entre el año actual y el sucesivo. El período de congelación puede fijarse en un máximo de 90 días. Dos períodos de congelación consecutivos deben estar separados por un mínimo de 60 días.

6. Haga clic en **Siguiente**.
7. Seleccione una de las siguientes opciones de distribución:

- **Todos los dispositivos**
- **Ningún dispositivo** (predeterminada)
- **Personalizado**

8. Haga clic en **Hecho**.

Administrar aplicaciones en dispositivos AMAPI

Cuando se distribuye la configuración COSU a los dispositivos, las aplicaciones se insertan y se fijan a la pantalla del dispositivo AMA. Independientemente de la configuración del COSU que se haya insertado en el dispositivo, se pueden seguir administrando las aplicaciones que se instalen en el dispositivo AMA. A continuación se enumeran los detalles de la administración de las aplicaciones en estos dispositivos:

- Solo se admiten aplicaciones públicas y privadas; no se admiten las aplicaciones internas ni los clips web.
- Las aplicaciones se insertan solo si los ajustes de la instalación tienen activadas las opciones «Instalar en dispositivo» o «Instalación silenciosa». Las aplicaciones asignadas al usuario/dispositivo sin ninguna de estas opciones activadas no estarán visibles en el dispositivo ni en la Play Store del dispositivo para ninguna acción del usuario.

- Las configuraciones de aplicaciones compatibles son: ajustes de Managed Google Play y Work Managed Device (Android for Work). Compatibilidad con la configuración administrada para las aplicaciones, incluida la compatibilidad con la configuración administrada para las aplicaciones de OEMConfig.

> La hora en que se completó la instalación y desinstalación de la configuración puede variar según las notificaciones de Google (servicio de mensajería) sobre la realización, o no, de la acción deseada.

- El Go app ahora se instalará por defecto como parte del registro de dispositivos de AMA. Durante el proceso de registro, la aplicación se fijará en la pantalla y, cuando se complete la configuración, se ejecutará en segundo plano.

> No son compatibles las políticas, excepto el requisito de registro de dispositivos basado en el fabricante, la versión del sistema operativo y el nivel de revisión de seguridad. Lista permitida del dispositivo que permite registrar con Ivanti Neurons for MDM solo los dispositivos de la lista es compatible.

Administrar comentarios de aplicaciones en dispositivos AMAPI

El soporte de comentarios de la aplicación se puede gestionar en dispositivos AMAPI (COSU). Cuando se registra un dispositivo en modo AMAPI (COSU), la configuración de la aplicación administrada se enviará directamente a Ivanti Neurons for MDM desde Google sin intervención alguna por parte de Go app. La información de Comentarios administrados de la aplicación se puede visualizar en el nivel de dispositivo desde **Detalles del dispositivo > Aplicaciones instaladas > Ver comentario**, o se puede ver en el nivel individual de cada aplicación accediendo a la aplicación específica de Android en el Catálogo de aplicaciones desde la pestaña "Comentarios de configuración de la aplicación" para el informe general de todos los dispositivos. Para obtener información sobre el mecanismo de comentarios de la aplicación, consulte **Sincronizar y obtener comentarios de aplicaciones**.

Limitaciones de AMAPI

Actualmente, AMAPI tiene la siguiente limitación:

- Solo es compatible con dispositivos dedicados (modo COSU).

Configuraciones admitidas

Las siguientes configuraciones son compatibles con AMAPI:

- Distribución de aplicaciones (una o varias aplicaciones)
- Configuración de aplicaciones gestionadas para aplicaciones enviadas al dispositivo
- Configuración de Wi-Fi
- Configuración de Android Enterprise Lockdown-Dedicated (COSU)
- Configuración de VPN siempre activa

12.6.4. API de Google Apps

Es posible que los clientes de Google que utilizan Inicio de sesión único (SSO) para autenticar el acceso de los usuarios a los servicios de Google Apps no puedan usar Exchange para conectar a los usuarios al correo electrónico, los contactos y el calendario debido a las limitaciones en el protocolo que impiden que los dispositivos activados mediante SSO se conecten a servicios de autenticación externos. Este servicio puede controlar esto creando y administrando con seguridad las contraseñas de las cuentas para la conectividad ActiveSync.

Requisitos previos

Antes de intentar configurar la función de la API de Google Apps, necesita tener:

- Acceso de administrador a una cuenta en https://console.developers.google.com/.
- Acceso de administrador a una cuenta en https://admin.google.com.

Activar la función de la API de Google Apps

Procedimiento

1. Seleccione **Administrador > Google > API de Google Apps**.
2. Haga clic en **Paso 1: Google Dev**en la parte inferior del rectángulo de la izquierda, donde dice 1.
3. Aparecerá la página "Paso 1: Google Dev".
   Siga las instrucciones que aparecen en la página "Paso 1: Google Dev" y haga clic en **Hecho**.
4. Haga clic en **Paso 2: Google Admin** en la parte inferior del rectángulo central, donde dice 2.
5. Aparecerá la página "Paso 2: Google Admin".
   Siga las instrucciones que aparecen en la página "Paso 2: Google Admin" y haga clic en **Hecho**.
6. Introduzca el nombre de usuario de Google Admin en el campo **Introduzca el nombre de usuario de Google Admin** del rectángulo de la derecha, donde dice 3.
7. En ese mismo rectángulo, haga clic en **Elegir archivo** para cargar el archivo JSON que descargó en el paso 1.
8. Haga clic en **Guardar**.
9. Si no puede ver la página del API de Google Apps, puede ser que no tenga los permisos necesarios. Necesita tener una de las siguientes **funciones**:
   - Administración del sistema
   - Solo lectura del sistema

12.6.5. Administrador- Android Enterprise

Licencia: Silver

- Las aplicaciones de productividad Ivanti, Inc que tienen habilitado Android Enterprise, como Email+, Docs@Work y Web@Work requieren una licencia Gold.
- Tunnel para Android Enterprise requiere una licencia Platinum.

Android Enterprise habilita el uso y configuración de aplicaciones de Android Enterprise. Los usuarios de Android Enterprise pueden ver e instalar aplicaciones desde el catálogo de aplicaciones y a través de Google Play.

Si es un cliente nuevo, la distribución de la aplicación se establece por dispositivo de manera predeterminada. Esta configuración no se puede cambiar. Los clientes que hayan actualizado pueden elegir entre la distribución de aplicaciones por usuario o por dispositivo. Además, para los clientes que hayan actualizado, la distribución por usuario se selecciona de manera predeterminada. Muchos usuarios tienen varios dispositivos. Si un usuario tiene varios dispositivos, cuando la distribución de aplicaciones se establece por dispositivo, puede crear un conjunto diferente de aplicaciones disponibles en cada dispositivo.

Esta sección contiene los siguientes temas:

- Configurar Android Enterprise
- Configurar el modo Perfil de trabajo de Android Enterprise

Configurar Android Enterprise

1. En el portal de Ivanti Neurons for MDM, haga clic en **Administrador > Google > Android Enterprise**.
2. Seleccione una de las siguientes opciones:
    - **Cuenta de Google Play administrada:** para las empresas que no sean suscriptoras de G Suite, este método permite a los usuario inscribirse en Android Enterprise sin enviar información personal (direcciones de correo electrónico a Google). Ivanti Neurons for MDM aprovisionará y administrará a los usuarios automáticamente con Google. Se le pedirá que autorice Android Enterprise con una cuenta de administrador de Google.
    - **Cuenta de Google administrada:** para las empresas que sean suscriptoras de G Suite, este método permite a sus usuario inscribirse en Android Enterprise con sus cuentas de Google. Cada usuario debe tener una cuenta de Google para inscribirse en Android Enterprise.

Siga las instrucciones que aparecen en pantalla para completar el proceso de configuración:

4. Para el método automático, haga lo siguiente:
    - Habilite su API de UEM y cree sus credenciales de empresa.
    - Inscríbase en Google autorizando al propietario de la integración. Esta debe ser una cuenta del departamento informático en lugar de una cuenta personal.
    - Defina su credencial arrastrando y soltando su ID de cliente JSON de la cuenta de servicio.

Para el método alternativo, haga lo siguiente:

- Consulte el ID de CLIENTE de la sección siguiente y agréguelo a Google Admin.
- Busque su token de MDM en Google Admin y la cuenta de servicio de la consola de Google Cloud.
- En Ivanti Neurons for MDM, introduzca el token de MDM, el dominio de empresa de Google y la dirección de correo electrónico de administrador de empresa para conectarse al servicio de Google.

- En Ivanti Neurons for MDM, arrastre y suelte su ID de cliente de JSON de la cuenta de servicio.
- En Ivanti Neurons for MDM, autorice a Ivanti Neurons for MDM para ver o administrar los Usuarios de Google haciendo clic en **Autorizar**.

La interfaz de usuario de Ivanti Neurons for MDM le guiará por estos pasos.

ID de CLIENTE para vincular Ivanti Neurons for MDM con la cuenta administrada de Google

Agregue la identificación del cliente como **140561810807-tiiglke17laibbrt5darupmvo4ae7cbj.apps.googleusercontent.com** en la consola de administración para vincular el abonado de Ivanti Neurons for MDM con la cuenta de Google administrada.

Configurar el modo Perfil de trabajo de Android Enterprise

1. En el portal de Ivanti Neurons for MDM, vaya a **Configuraciones**.
2. Haga clic en **+Añadir**.
3. Seleccione **Bloqueo y kiosco: configuración de Android Enterprise**.
4. Introduzca un nombre y descripción para la configuración.
5. Haga clic en el tipo de bloqueo **Perfil de trabajo**.
   Seleccione los **ajustes de bloqueo** que desee aplicar a los dispositivos de destino.
   Importante: cuando el usuario añade una cuenta Google utilizando la opción Añadir cuenta en Ajustes, el servidor de autenticación de Google comprueba si el dominio de la cuenta está registrado como dominio administrado por UEM. Verifique que la opción **Aplicar directivas de UEM en dispositivos Android** esté seleccionada. Si lo está, el cliente Go se instala o actualiza automáticamente (si no está ya instalado en el dispositivo) y se inicia. Una vez que el usuario pasa por el proceso de registro, se le pide que cree un Perfil de trabajo y la cuenta Google migra automáticamente al perfil de trabajo.

12.7. Trabajar con dispositivos de ChromeOS

Esta sección contiene los siguientes temas:

- ChromeOS e Ivanti Neurons for MDM
- Distribuir aplicaciones de Android en dispositivos de ChromeOS
- Configuración de ChromeOS Blueprint
- Acciones de dispositivos
- Preguntas más frecuentes
- Pasos recomendados para la evaluación

12.7.1. ChromeOS e Ivanti Neurons for MDM

ChromeOS es un sistema operativo basado en Linux creado y distribuido por Google. Ivanti Neurons for MDM es compatible con los dispositivos que funcionen en Android, Windows, iOS y macOS. Esta compatibilidad ahora se ha ampliado también a los dispositivos de ChromeOS. Ivanti Neurons for MDM proporciona una solución sencilla y unificada para la gestión de movilidad con la que configurar y administrar los dispositivos de ChromeOS. Ivanti proporciona una solución unificada, sencilla y muy completa para dispositivos de ChromeOS similar a los flujos de trabajo de administración que están disponibles para iOS, Android, Windows y Mac en Ivanti Neurons for MDM. El administrador puede conectarse a Ivanti Neurons for MDM con su Google Cloud (también denominado consola del administrador de Google) mediante una sencilla integración desde **Administrador > Google > Gestión de ChromeOS**.

Requisitos previos

1. Debe tener una cuenta de administrador de Google.
2. Los usuarios de LDAP y las UO se deben importar en la consola de administración de Google. Ivanti Neurons for MDM solo es compatible con UO importadas de una fuente de LDAP. Las OU locales no son compatibles.
3. El administrador debe tener sincronizadas las unidades organizativas (grupos de usuarios) en Ivanti Neurons for MDM. Esto se puede hacer mediante la configuración del servidor de LDAP y agregando las unidades organizativas.

Autorización de Google

Los dispositivos de ChromeOS disponibles en la consola del administrador de Google no se pueden registrar directamente en Ivanti Neurons for MDM. Como alternativa, estos dispositivos se registran con Google y la información de estos dispositivos se sincroniza entre Google y Ivanti Neurons for MDM. El administrador debe autorizar a Google para importar los dispositivos y llevar a cabo otras acciones, como asignar aplicaciones, configuraciones, etc.

Procedimiento

1. Vaya a **Administrador → Google > Gestión de ChromeOS**.
2. Haga clic en **Autorizar Google**.
3. Seleccione la cuenta de Administrador de Google que desee autorizar.
4. Haga clic en **Continuar** para aceptar los permisos que proporcionarán los servicios necesarios.
   La configuración **ChromeOS configurado correctamente** aparece en la pantalla. También puede encontrar la información del dominio bajo la confirmación.

Sincronizar dispositivos de ChromeOS desde Google

El administrador debe sincronizar los dispositivos de ChromeOS desde la consola del administrador de Goodle. Al usar la consola de administración de Google para acceder a los dispositivos de ChromeOS por primera vez, el administrador debe sincronizar manualmente los dispositivos mediante la opción Sincronizar ahora en la página de administración de ChromeOS.

> Después de sincronizar los dispositivos manualmente por primera vez, las sincronizaciones siguientes se producirán automáticamente cada hora.

Eliminación de la integración de la consola de administración de Google con Ivanti Neurons for MDM

Eliminar la integración revoca el token OAuth que recibimos de Google para acceder a los recursos de Google. Elimina los dispositivos de ChromeOS, el inventario asociado a configuración de Blueprint y configuración de aplicaciones, y los metadatos de inscripción. No

se eliminarán la configuración del Blueprint ni las aplicaciones cargadas.

En caso de que la inscripción del abonado no se elimine, puede abrir un billete para comprobar el problema.

Procedimiento

1. Vaya a **Administrador → Google > Gestión de ChromeOS**.
2. En la sección de registro de ChromeOS Ivanti Neurons for MDM, haga clic en **Eliminar**.
   Aparecerá una ventana emergente en la pantalla que indicará si desea proceder con la operación de Borrado, y se borrarán todos los dispositivos asociados a esta integración. Seleccione **Aceptar**.

12.7.2. Distribuir aplicaciones de Android en dispositivos de ChromeOS

El administrador puede distribuir aplicaciones de Android desde el Catálogo de aplicaciones a los dispositivos de ChromeOS.

Requisitos previos

1. Se debe configurar Android Enterprise. Para obtener información sobre cómo configurar Android Enterprise, consulte **Configurar Android Enterprise**.
2. Las aplicaciones de Android se deben presentar en el Catálogo de aplicaciones.
3. Asegúrese de que el usuario del dispositivo de ChromeOS (Chromebook) forma parte de un Grupo de usuarios (también denominado Unidad organizativa) antes de distribuir aplicaciones de Android y configuración de ChromeOS Blueprint.

Una vez identificada la aplicación de Android, debe distribuir la aplicación siguiente el mismo proceso que siguió para distribuir cualquier otra aplicación. Cuando distribuya la aplicación de Android, asegúrese de seleccionar los Grupos de usuarios a los que desee distribuir la aplicación y realice una instalación silenciosa en el dispositivo.

> Si su despliegue de aplicaciones de Android existente está establecido para que se distribuya a dispositivos/grupos de dispositivos o usuario, deberá cambiar la distribución para que se base den Grupos de usuarios. Esto puede afectar a los despliegues existentes si la aplicación ya se está usando. Se recomienda hacer esto primero en una aplicación completamente nueva.

> Ajustes de instalación permite a los administradores controlar la instalación en segundo plano final y es necesario para forzar la aplicación en dispositivos de ChromeOS. Los Grupos de usuarios se deben seleccionar aquí.

12.7.3. Agregar y distribuir aplicaciones de extensión de ChromeOS

El administrador puede agregar aplicaciones de extensión de ChromeOS desde el Catálogo de aplicaciones y distribuir estas aplicaciones a los dispositivos de ChromeOS.

Procedimiento

1. Vaya a **Aplicaciones** > **Catálogo de aplicaciones**.
2. Haga clic en **+Añadir**.
3. Seleccione **ChromeOS** en la lista. La página **Agregar información de aplicación de ChromeOS** aparece en pantalla.
4. Proporcione los siguientes datos: **Nombre de la aplicación**: nombre de la aplicación de extensión de ChromeOS; **ID de extensión**: puede obtener esta información en la tienda web de Chrome.
5. Haga clic en **Siguiente**. La página **Configuración de aplicaciones** aparece en la pantalla. Ahí podrá seleccionar una actualización inmediata que se producirá la próxima vez que se ingrese el dispositivo o bien puede elegir que la aplicación se actualice automáticamente cuando haya disponibles nuevas versiones.
6. Seleccione una de las opciones de distribución de aplicaciones y proporcione la información necesaria.

> La distribución de la aplicación ChromeOS solo es compatible con grupos de usuarios LDAP.

Cuando se haya identificado la aplicación de extensión de ChromeOS, debe distribuir la aplicación siguiente el mismo proceso que siguió para distribuir cualquier otra aplicación. Cuando distribuya la aplicación de extensión de Android, asegúrese de seleccionar los Grupos de usuarios a los que desee distribuir la aplicación y realice una instalación en segundo plano en el dispositivo.

> Ajustes de instalación permite a los administradores controlar la instalación en segundo plano final y es necesario para forzar la aplicación en dispositivos de ChromeOS. Los Grupos de usuarios se deben seleccionar aquí.

Puede editar la información de una aplicación de extensión de ChromeOS o eliminar una aplicación de extensión de ChromeOS del catálogo de aplicaciones. Debe seguir un proceso similar al que sigue para editar o eliminar cualquier otra aplicación del Catálogo de aplicaciones.

Editar una extensión de ChromeOS

1. Vaya a **Aplicaciones > Catálogo de aplicaciones > Detalles**.
2. Haga clic en **Editar**. Realice los cambios necesarios y haga clic en **Guardar**.

Para obtener información sobre cómo eliminar una aplicación, consulte **Eliminar aplicaciones del Catálogo de aplicaciones**.

12.7.4. Configuración de ChromeOS Blueprint

La configuración de ChromeOS Blueprint tiene los ajustes siguientes:

- Ajustes del dispositivo
- Ajustes de usuario y explorador
- Ajustes de Sesión de invitado administrado

Puede aplicar la configuración de ChromeOS en Grupos de usuarios específicos (también denominados Unidades organizativas). Cuando intente distribuir la configuración de ChromeOS Blueprint, solo estará disponible la sección Grupos de usuarios y todos los Grupos de usuarios de LDAP asociados con la consola de administración de Google autorizada se enumerará en la sección. Puede seleccionar uno o más grupos de la lista y aplicar la configuración.

Procedimiento

1. Vaya a **Configuraciones > Añadir**.
2. Seleccione **Google ChromeOS** en la sección SO. La pestaña **Configuración de ChromeOS Blueprint** aparece en la pantalla.
3. Haga clic en **ChromeOS Blueprint**. La página **Crear configuración de ChromeOS Blueprint** aparece en la pantalla.
4. Introduzca un nombre para la configuración en el cuadro **Nombre**.
5. En los Ajustes de configuración, puede modificar los Ajustes del dispositivo, el Usuario y los Ajustes del explorador, y los ajustes de la sesión de invitado administrada, como necesite, así como alternar el botón "Enviar al dispositivo" para aplicar los ajustes modificados.
6. Haga clic en **Siguiente**.
7. Seleccione **Personalizado** para las opciones de distribución.

> Solo los grupos de usuarios de LDAP estarán disponibles para distribuir la configuración.

> En el caso de distribuir la configuración a todos, se puede hacer solo para los Grupos de usuario de LDAP disponibles en Ivanti Neurons for MDM y en la consola del administrador de Google.

Seleccione uno o más grupos y haga clic en **Hecho**.

> Cuando la configuración distribuida no se distribuye, la configuración aplicada no se revertirá.

> Puede cargar los archivos en la configuración de ChromeOS Blueprint.

12.7.5. Acciones de dispositivos

Las acciones siguientes son compatibles con los dispositivos de ChromeOS:

- **Borrar**: la acción Borrar elimina todos los datos de un dispositivo y este se restablece a los ajustes de fábrica. Para más información, consulte **Borrar un dispositivo**.
- **Bloquear**: la acción Bloquear le impide llevar a cabo más acciones en el dispositivo. Para más información, consulte **Bloquear un dispositivo**.
- **Desbloquear**: la acción Desbloquear libera el dispositivo para más usos. Para obtener más información, consulte **Desbloquear un dispositivo**.

12.7.6. Preguntas más frecuentes

Esta sección lista algunas de las preguntas frecuentes más comunes que puede tener cuando utiliza dispositivos de ChromeOS en Ivanti Neurons for MDM.

- ¿En qué se diferencia la gestión de Chromebook con la de otros SO?
- A partir de ahora, Google solo permite la distribución de configuraciones basadas en grupo de usuarios de LDAP y el administrador debe asegurarse cuando trabaje con configuraciones o aplicaciones, que la distribución se basa en grupos de usuarios de LDAP. Los grupos de usuarios locales y los grupos de dispositivos no son compatibles con la gestión de dispositivos de ChromeOS.
  ¿Qué licencia necesito con Ivanti para administrar los dispositivos de ChromeOS?
- Los dispositivos de ChromeOS deben tener licencias como Chrome Enterprise Upgrade o Chrome Education Upgrade. Estos se puede obtener de vendedores, como parte del hardware o como licencias independientes. Consulte la documentación de Google para obtener más información. Para empezar a usar la gestión de dispositivos de Chrome, es necesaria una licencia de UEM (Gestión de puntos terminales unificados) segura con Ivanti.
  ¿Estará disponible la solución Mobile Threat Defense (MTD) o una similar? ¿Necesito una licencia distinta para MTD?
- Esto no está disponible actualmente en el producto. Consulte las limitaciones actuales. Proporcionaremos más información sobre los cambios en la funcionalidad a través de las Preguntas frecuentes y los anuncios de versiones.
  ¿Por qué la pestaña de configuraciones y aplicaciones no tiene detalles como en otros dispositivos?
- Pues que las configuraciones se distribuyen a los Grupos de usuarios y no se aplican según el usuario activo, actualmente, las configuraciones no se muestran en los detalles del dispositivo. Las aplicaciones siguen la misma lógica de distribución y tienen el mismo límite. Proporcionaremos más información sobre los cambios en estas limitaciones a través de las Preguntas frecuentes y los anuncios de versiones.
  ¿Cuántas configuraciones son compatibles actualmente con ChromeOS?
- Con ChromeOS, hemos reducido el número de iconos de configuración disponibles así como las tareas de administración asociadas con la configuración. Nos referimos a esta configuración como "ChromeOS Blueprint". ChromeOS Blueprint es compatible con unas 700 configuraciones en estos dispositivos. Consulte la documentación de Google para las opciones de configuración.
  ¿Con qué facilidad se gestiona una configuración para todos los dispositivos?
- Los administradores pueden sencillamente clonar una configuración existente y modificarla (en caso necesario) para sus grupos de usuarios respectivos. No necesita empezar de cero.
  ¿Cómo agregado la configuración VPN a los dispositivos de Chrome?
- Esto se puede hacer mediante las aplicaciones de Android, no utilizando la VPN nativa.
  ¿Las acciones de dispositivos como Retirar y Borrar funcionan en estos dispositivos?
- Chromebooks en Enterprise siempre se gestionan con una empresa y los datos de tales dispositivos se consideran totalmente empresariales. Teniendo esto en cuenta:
  - Retirar está bloqueado
  - Borrar está permitido
  - Se permite Bloquear
  - Se permite Desbloquear
  - Otras acciones: no son compatibles

¿Qué Chromebooks, en términos de hardware son compatibles con Ivanti?

- Se espera que los dispositivos compatibles con las soluciones de administración de dispositivos en la nube de Google sean compatibles con Ivanti. Ivanti actualmente no publica una lista de hardware específico compatible con la solución de Ivanti.
  ¿Qué versión de Chrome OS es compatible?
- Google Cloud solo es compatible con la versión estable más reciente de ChromeOS y la compatibilidad con Ivanti sigue el modelo compatible con Google debido a la naturaleza de las integraciones backend.
  ¿Puede listar los límites actuales, puesto que se trata del primer lanzamiento de esta función?

Con la nueva compatibilidad con Chrome OS, nos estamos esforzando por proporcionar funciones que nuestros clientes esperan con ganas. A continuación hay algunos límites que los administradores deben observar:

- Las extensiones de Chrome OS (aplicaciones del explorador) actualmente no son compatibles (como "aplicaciones") para su distribución.
- Configuración de aplicaciones administradas para aplicaciones de Android no es compatible en la actualidad.
- La API de configuración Wi-Fi se publicó recientemente y actualmente no es compatible.
- Actualmente no es compatible la distribución de certificados.
- Actualmente no hay compatibilidad para distribuir la aplicación de Android con Ivanti Go (antes conocido como MobileIron Go).
- La aplicación de Ivanti Tunnel (VPN) actualmente no es compatible.
- Spaces y la delegación de espacio actualmente no son compatibles.
- La solución de Mobile Threat Defense actualmente no es compatible.
- La solución Zero Sign-on de Ivanti es compatible en estos dispositivos, categorizada como dispositivos sin administrar.
- Las acciones de política no son totalmente compatibles.

12.7.7. Pasos recomendados para la evaluación

Los pasos siguientes se recomiendan para validar una solución:

1. Crear una UO separada (Grupo de usuarios) que tenga un usuario de prueba en la fuente del directorio (ejemplo, Active Directory). Esto evitará el impacto a las Unidades organizativas activas.
2. Sincronice los usuarios entre Ivanti, Google y la fuente de directorios (LDAP). Verifique que la "UO de prueba" está disponible en los Grupos de usuarios.
3. Integrar Ivanti Neurons for MDM con Google como se indica en los pasos anteriores.
4. Cree una configuración de ChromeOS Blueprint y distribúyala solo al grupo de usuarios "UO de prueba".
5. Arranque un Chromebook (nuevo o registrado anteriormente). Asegúrese de que está disponible en la lista de dispositivos.
6. Verifique que los ajustes de ChromeOS Blueprint están disponibles en el dispositivo.
7. Seguir pasos similares para la distribución de aplicaciones de Android.

12.8. Administración del firmware

Esta sección contiene los siguientes temas:

- Inscripción al servicio Zebra OTA
- Administración de licencias de Samsung E-FOTA (Retirado)

12.8.1. Inscripción al servicio Zebra OTA

Una vez inscrito en el servicio Zebra OTA (Over the Air), se puede activar la configuración de Zebra OTA para recibir y actualizar los detalles del firmware de los dispositivos Zebra registrados en Ivanti Neurons for MDM.

Procedimiento

1. Vaya a **Administración > Infraestructura > Zebra OTA**. Aparecerá la página **Servicio OTA Zebra**.
2. En **Enlace al servicio OTA de Zebra**, haga clic en **Comenzar**.
3. Introduzca sus credenciales de Zebra OTA para iniciar sesión y siga los pasos para solicitar una aprobación para hacer uso de los servicios de Zebra.
4. Haga clic en **Completar verificación** para obtener la confirmación de la conexión al servicio Zebra. Cuando se confirme la conexión, el estado de la inscripción correcta se muestra en la página Servicio Zebra OTA.

Para revocar la inscripción, haga clic en **Revocar** en la columna **Acciones** . La acción **Revocar** elimina todas las configuraciones OTA de Zebra de las configuraciones existentes. Para volver a inscribirse con Zebra OTA, haga clic en **Actualizar**. La acción de actualizar no tiene ningún impacto en las configuraciones existentes.

Después de la inscripción, puede habilitar la configuración del firmware de Zebra que recibe el cliente Go y se aplica a los dispositivos Zebra (que se ejecutan en la versión 8.0 de Android o versiones más recientes compatibles) en el modo Propietario de dispositivo. Cuando se aplica la configuración, se descarga el firmware y se instala en el dispositivo según lo programado en la configuración. Para obtener más información sobre cómo activar la configuración del firmware de Zebra, consulte **Configuración de actualización del sistema**.

Una vez completada la actualizaciones del firmware, puede ver el estado de actualización del firmware en el dispositivo Zebra en la columna **Actualización del sistema** de la página Dispositivos. A continuación se enumeran los posibles estados:

- **Desconocido**: no admitido por el cliente o el sistema operativo
- **Actual**: el dispositivo tiene la actualización más reciente disponible
- **Pendiente**: se aplica la configuración de actualización del sistema pero no se ha descargado ni aplicado la actualización
- **En descarga**: la actualización del sistema se está descargando para el cliente
- **Disponible**: la actualización del sistema está actualmente disponible para el dispositivo.
- **Error**: error en la descarga o instalación.

La columna **Versión de la revisión de Zebra** que hay en la página Dispositivos muestra la información de la revisión de Zebra del dispositivo.

> La **Versión de Zebra Patch** no es compatible con dispositivos de Android 11 y posteriores. Solo es compatible la **Actualización completa de Zebra**.

12.8.2. Administración de licencias de Samsung E-FOTA (Retirado)

El servicio Samsung E-FOTA se retirará en julio de 2022. Para obtener más información, consulte el anuncio de Samsung.

A partir de ahora, no podrá configurar el servicio Samsung E-FOTA. No obstante, si tiene una configuración existente de E-FOTA, puede desactivar la configuración accediendo a **Administracióni** > **Administración de Firmware** > **Samsung E-FOTA** y haciendo clic en la opción **Desactivar**.

12.9. Gestionar secuencias de comandos y archivos

Los administradores pueden gestionar secuencias de comandos que se pueden utilizar en Configuraciones e insertarse en los dispositivos.

Esta sección contiene los siguientes temas:

Todas las secuencia de comandos

Archivos

12.9.1. Todas las secuencia de comandos

Aplicable a: dispositivos macOS y Windows

En la página **Administrador > Secuencias de comandos y archivos > Todas las secuencias de comandos**, Ivanti Neurons for MDM permite a los usuarios con el rol de administración del sistema crear o cargar y administrar secuencias de comandos que se pueden utilizar en configuraciones y distribuir a dispositivos. Puede asociar atributos personalizados a las secuencia de comandos y asignar los valores resultantes a los dispositivos configurados. UtiliceAudit Trails para ver los registros de los cambios del script y la página Detalles del dispositivo para ver los resultados de ejecución.

Puede escribir una secuencia de comandos que configure cualquier configuración en los dispositivos. Por ejemplo, puede ejecutar secuencias de comandos que hagan lo siguiente:

- obligar a los usuarios de los dispositivos a cambiar sus contraseñas mensualmente;
- bloquear la pantalla después de 5 minutos de inactividad; o
- configurar una red Wi-Fi segura.

Esta sección contiene los siguientes temas:

- Añadir una secuencia de comandos
- Modificar una secuencia de comandos
- Uso de variables de script (aplicable a Windows y macOS)
- Probar una secuencia de comandos
- Verificar los resultados de ejecución de la secuencia de comandos

Añadir una secuencia de comandos

Puede crear o cargar un repositorio de scripts bash (para macOS) y scripts ps1 (para Windows). Este repositorio puede utilizarse en una configuración para seleccionar un script y distribuirlo para su ejecución en los dispositivos según el horario especificado en la configuración.

Por ejemplo, puede crear una secuencias de comandos de shell para su ejecución en dispositivos. Si fuera necesario, puede usar contenedores. La ejecución de archivos binarios desde una secuencia de comandos de shell no es compatible.

> Ivanti le recomienda encarecidamente que pruebe las secuencias de comandos de shell antes de ejecutarlos en los dispositivos para garantizar su solidez y calidad. Ejecute su secuencia de comandos a nivel local y corrija los errores que se produzcan.

Procedimiento

1. Vaya a **Administración > Secuencias de comandos > Todas las secuencias de comandos**.
2. Haga clic en **+Añadir**.
3. Introduzca un Nombre y una Descripción para el script.
4. En Tipo de plataforma, seleccione macOS o Windows.
5. Seleccione uno de los siguientes **Tipos de secuencia de comandos**:
    - **bash**
    - **zsh**

- **python**
- **swift**
- **ps1**

6. Seleccione la casilla **Ejecutar como raíz** para ejecutar la secuencia de comandos como raíz en los dispositivos. De forma predeterminada, esta opción se encuentra deshabilitada.
7. En el **Editor de secuencias de comandos**, puede escribir, arrastrar y soltar o copiar y pegar una secuencia de comandos en el cuadro de texto.
8. Alternativamente, haga clic en **Importar código de una secuencia de comandos** para arrastrar y soltar un archivo de secuencia de comandos existente o haga clic en Elegir archivo para examinar y seleccionar el archivo de secuencia de comandos que va a cargar en Ivanti Neurons for MDM. Esto reemplazará cualquier secuencia de comandos que haya en el editor de secuencias de comandos. Esta acción no podrá deshacerse. Haga clic en **Importar**. El código de la secuencia de comandos cargado se mostrará en el editor de secuencias de comandos.
9. (Opcional) En la sección **Atributos personalizados disponibles**, seleccione uno o más atributos personalizados del dispositivo que aparecen para asociarlos con la secuencia de comandos. Estos se pueden utilizar para asignar los valores de ejecución de secuencia de comandos resultantes a los atributos personalizados del dispositivo de los dispositivos configurados. Haga clic en **Código de ejemplo para atributos personalizados** para ver un código de ejemplo que usa atributos personalizados en una secuencia de comandos.
10. Haga clic en **Guardar**.

Los nombres de atributos personalizados en la secuencia de comandos deben estar en minúsculas. Si se hace referencia a los atributos personalizados en cualquier secuencia de comandos, los atributos no se podrán eliminar. Cuando modifique un atributo personalizado (por ejemplo, su nombre) y si está asociado a una secuencia de comandos, deberá realizar los cambios correspondientes en las secuencia de comandos asociadas.

Modificar una secuencia de comandos

Para editar o eliminar una secuencia de comandos:

1. Vaya a **Administración > Secuencias de comandos > Todas las secuencias de comandos**.
2. En la columna **Acciones** de la secuencia de comandos, haga clic en el icono correspondiente para la acción de editar o eliminar.
3. Siga las instrucciones que aparecen en pantalla para completar la acción.

Cuando se cambia una secuencia de comandos (contenido, nombre, descripción), todas las configuraciones asociadas a la secuencia de comandos se redistribuirán en los dispositivos.

Uso de variables de script (aplicable a Windows y macOS)

Definir y almacenar entradas de secuencia de comandos como variables de entorno y de sustitución en el repositorio de secuencias de comandos. En la configuración del script de Mobile@Work for macOS o Ivanti Bridge for Windows Scripts and Actions Configuration, dependiendo de qué script esté vinculado, las variables de script relacionadas estarán disponibles para su uso según sea necesario. En macOS, esta característica requiere **Mobile@Work para macOS** 1.71.0 hasta la versión más reciente compatible con Ivanti Neurons for MDM. Para Windows, esta función requiere **Ivanti Bridge**.

Use las variables para ejecutar una secuencia de comandos con valores diferentes cada vez que se ejecute. Por ejemplo, un administrador puede crear un script para utilizar la variable de entorno $ como variable de script y asociarla a una configuración de script de Mobile@Work para macOS o para Windows. Cuando la configuración se distribuye e instala en cada dispositivo de usuario,

Ivanti Neurons for MDM envía una dirección de correo electrónico de usuario registrado diferente para que cada dispositivo realice ciertas acciones. El portal administrativo de Ivanti Neurons for MDM es compatible con variables personalizadas.

Para añadir una variable de secuencia de comandos:

1. Vaya a **Administración > Secuencias de comandos > Todas las secuencias de comandos**.
2. En la sección Entrada de la secuencia de comandos, haga clic en **+ Añadir**.
3. En la página emergente Añadir entrada de secuencias de comandos - Variable de entorno, introduzca los siguientes detalles:
    - Etiqueta que se mostrará: este texto se mostrará como una etiqueta en la página de configuración de la secuencia de comandos de Mobile@Work para macOS. Por ejemplo, Introducir la carpeta del sistema operativo, Introducir el número de Apache, etc.
    - Nombre de la variable de entorno: por ejemplo, JAVA_HOME, OS_VERSION, etc. Ivanti Neurons for MDM sustituye los valores de las variables de secuencia de comandos mientras envía los detalles de la configuración a un dispositivo de destino a la vez que los valores se mantienen en la base de datos.
    - Valor predeterminado de la variable de entorno: por ejemplo, 1024, bin/java, $, y así sucesivamente. Las variables de entrada se utilizarían en la secuencia de comandos cargado o las editaría un administrador. Consulte también las siguientes notas.

En el área Vista previa, revise cómo se mostrará el valor de la variable de entorno como entrada de secuencia de comandos en la página de configuración.

5. Haga clic en **Guardar**.

De este modo, solo la etiqueta y el valor por defecto estarán disponibles para la configuración y no el nombre de la variable de entorno, lo cual proporciona una capa de abstracción.

- El valor alfanumérico (por ejemplo, 1024, bin/java, root@localhost) o los atributos de sistema (por ejemplo, $) son aceptables como valor de la variable de entorno.
- El valor de la variable de entorno se puede modificar o eliminar durante la implementación en la página de configuración.
- Si no se proporciona el valor de la variable de entorno, asegúrese de proporcionar un valor durante la implementación de la secuencia de comandos. De lo contrario, se trasladará el valor vacío a la secuencia de comandos.
- Después de distribuir e instalar una configuración de la secuencia de comandos en el dispositivo, la edición de las variables de entorno en la página **Administrador > Secuencias de comandos y archivos > Todas las secuencias de comandos** no afectará a las configuraciones existentes asociadas a la secuencia de comandos. Consulte también **Configuración del script de Mobile@Work para macOS**. Para Windows, consulte **Configuración de scripts y acciones de Ivanti Bridge for Windows**.

Editar una variable de la secuencia de comandos

Para modificar una variable de la secuencia de comandos, haga clic en el icono de edición (lápiz) que hay junto a la variable y guarde los cambios.

Si la configuración de una secuencia de comandos se refiere a una secuencia de comandos que tiene variables de secuencia de comandos, la edición de la etiqueta de una variable de secuencia de comandos existente también se reflejará en la configuración de la secuencia de comandos. Sin embargo:

- Un cambio en el valor por defecto de la variable de la secuencia de comandos no se reflejará en las configuraciones existentes.
- Un cambio en el valor por defecto de la variable de secuencia de comandos se reflejará en cualquier nueva configuración creada con la secuencia de comandos anterior.

Borrar una variable de la secuencia de comandos

Para eliminar una variable de la secuencia de comandos, haga clic en el icono de eliminación (menos) que hay junto a la variable y confirme.

Una variable de secuencia de comandos recién creada, o la eliminación de una variable de secuencia de comandos existente, se reflejará incluso en una configuración ya existente.

Probar una secuencia de comandos

Pruebe ejecutar una secuencia de comandos en la herramienta de depuración rápidamente antes de probarlo en un dispositivo y sin necesidad de guardar las secuencias de comandos.

Requisitos previos

- Esta característica requiere **Mobile@Work para macOS** 1.67 hasta la versión más reciente compatible con Ivanti Neurons for MDM.
- Para Windows, esta función requiere **Ivanti Bridge for Windows Scripts and Actions Configuration**.

Procedimiento

1. Vaya a **Administración > Secuencias de comandos > Todas las secuencias de comandos**.
2. En el Editor de secuencias de comandos, añada o importe una secuencias de comandos.
3. Si el abonado tiene varios espacios, seleccione uno de ellos.
4. En la sección Script de prueba, seleccione **macOS** o **Windows** como la plataforma.
5. En el campo de texto **Buscar dispositivos**, busque y seleccione el dispositivo en el que se puede probar la secuencia de comandos. El dispositivo se puede buscar por número de serie,nombre de usuario,nombre de dispositivo yversión del sistema operativo.
6. Haga clic en **Probar ahora**. De esta manera, se puede añadir, editar y eliminar una variable de entorno, y el script se puede probar con ese estado (sin siquiera guardar los cambios realizados). Para **Windows** Script, aparece una ventana emergente en la pantalla que indica que se iniciará la ejecución de Script y puede ver el estado desde la pestaña de registros de detalles del dispositivo después de algún tiempo.
7. Haga clic en **Guardar**.
8. En macOS, espere a que el script se inserte y ejecute en el dispositivo.
9. Revise los resultados de las pruebas publicadas en las secciones Entrada de secuencia de comandos (que contiene detalles de las variables de entorno), Salida de secuencia de comandos y Atributos personalizados. También se muestran los valores por defecto de las variables de entorno.

Verificar los resultados de ejecución de la secuencia de comandos

Para ver los registros de los resultados de la ejecución de la secuencia de comandos:

1. Vaya a **Dispositivos**.
2. Haga clic en el nombre del dispositivo.
3. Haga clic en la pestaña **Registros**.
4. En una línea que muestre la acción Ejecución de la secuencia de comandos, podrá verificar la siguiente información:
    - Nombre de la secuencia de comandos en la columna Detalles.
    - Estado de ejecución de la secuencia de comandos en la columna Estado.

- Fecha y hora de ejecución de la secuencia de comandos en la columna Fecha.
- Registros de ejecución de la secuencia de comandos (plist de registros de dispositivos) haciendo clic en el icono del ojo que hay debajo en la columna Acciones.

Utilice filtros para mostrar las filas de **Ejecución de la secuencia de comandos**. Los registros de estas filas incluyen la salida (plist) de la salida estándar y el error estándar de las secuencias de comandos .

6. Utilice filtros para mostrar las filas de **Procesamiento de los resultados de la ejecución de la secuencia de comandos**. Los registros de estas líneas incluyen detalles (plist) de cómo se procesaron los resultados.
   - Si una secuencia de comandos no tiene ningún atributo personalizado asociado, no habrá ningún resultado que procesar. Dichas secuencias de comandos no se mostrarán en la lista de filas filtradas.
   - Si una secuencia de comandos tuviera atributos personalizados asociados con este y si estos tuvieran el formato esperado, entonces los atributos personalizados de los resultados se asignan y el estado se ve como Correcto. Puede verificar los atributos personalizados asignados y sus valores en la pestaña **Atributos**.
   - Si una secuencia de comandos tenía atributos personalizados asociados y estaban en el formato esperado, los atributos personalizados de los resultados se asignarán y el estado se mostrará como «Error».
   - Si el formato del resultado es correcto pero no todos los atributos personalizados asociados se envían en el resultado, el estado se mostrará como «Error».
   - Si se envía una variable de secuencia de comandos con la secuencia de comandos, los registros de procesamiento de resultados de la ejecución de la secuencia de comandos incluirán detalles (plist) para la variable de secuencia de comandos.

Temas relacionados:

- **Configuración de secuencia de comandos de Mobile@Work para macOS**
- **Cómo crear una configuración**
- **Configuración de acciones y scripts de Ivanti Bridge for Windows**

12.9.2. Archivos

Aplicable a: dispositivos macOS

La Ivanti Neurons for MDM permite a los usuarios con el rol de Administración del sistema crear o cargar y gestionar archivos utilizados para configurar y distribuir a los dispositivos.

Procedimiento

1. Vaya a **Administrador** > **Secuencias de comandos y archivos** > **Archivos**.
2. En la página **Archivos**, haga clic en **+ Agregar**.
3. En la ventana **Crear archivo**, introduzca los detalles siguientes:
    1. En el campo **Nombre**, introduzca un nombre para identificar el archivo.
    2. En el campo **Descripción**, introduzca una descripción que explique la finalidad de este archivo.
    3. En el panel **Cargar archivo**, haga clic en **Elegir un archivo** para cargar el archivo .zip. Alternativamente, puede arrastrar y soltar un archivo desde su dispositivo.
4. Haga clic en **Guardar**.
   El archivo recién añadido aparece en la página **Archivos**.

Editar un archivo

1. Vaya a **Administrador** > **Secuencias de comandos y archivos** > **Archivos**.
2. Seleccione al archivo que desea editar y haga clic en **Editar**.
   Aparece la ventana **Editar archivo**.
3. (opcional) Puede editar los campos de **Nombre** y **Descripción**.
4. En el panel **Cargar archivo**, haga clic en **Elegir un archivo distinto** para cargar el archivo .zip. Alternativamente, puede arrastrar y soltar un archivo desde su dispositivo.
5. Haga clic en **Actualizar**.

Eliminar un archivo

Para eliminar **Archivos** existentes, vaya a **Administración** > **Secuencias de comandos y archivos** > **Archivos**, seleccione todos los archivos que quiera eliminar y haga clic en **+ Eliminar**.

Si los **archivos** están asociados a una configuración, Ivanti Neurons for MDM mostrará un mensaje de **advertencia**: **"No se puede eliminar el archivo porque está siendo utilizado por otras políticas".**

12.10. Personalización de marca

Esta sección contiene los siguientes temas:

- Administrador > Catálogo de aplicaciones Apple (personalización de marca)
- Personalizar el App Catalog de Android
- Administrador > Personalización de marca del kiosko de Android
- Cómo personalizar las plantillas de correo electrónico
- Portal de autoservicio
- Portal de autoservicio (personalización)
- Personalización del inicio de sesión multiusuario (clip web)
- Organización

12.10.1. Administrador > Catálogo de aplicaciones Apple (personalización de marca)

Licencia: Gold

Puede personalizar el {{app catalog}} de Apple para que su aspecto le resulte más familiar a los usuarios finales para dispositivos iPhone, iPad y Mac. Se pueden personalizar los siguientes elementos en el catálogo de aplicaciones de Apple:

- Icono de aplicación (PNG, 360px cuadrado)
- Nombre de la aplicación
- Imagen del banner de la aplicación (PNG, 360x64)
- Color del texto

> Hay dos modos de acceder al App Catalog de Apple: App Catalog independiente y App Catalog integrado. El App Catalog independiente está disponible en dispositivos iPhone, iPad y Mac. El Catálogo de aplicaciones integrado está disponible en dispositivos iOS Mac.

Personalizar el App Catalog de Apple

Los cambios realizados en esta página afectan a la pantalla de inicio, la pantalla de presentación y la pantalla de inicio de la aplicación. El procedimiento es similar tanto para el App Catalog independiente como para el App Catalog integrado.

Procedimiento

1. En la página **Personalización de marca del App Catalog de Apple**, haga clic en **Personalizar** (arriba a la derecha).
2. En la sección **Icono de la aplicación**, arrastre el archivo del logotipo hasta el cuadro punteado o haga clic en **Elegir archivo** para seleccionarlo desde su sistema de archivos. El icono de la aplicación se muestra en la pantalla de inicio de iOS
3. En la sección **Nombre de la aplicación**, edite el texto **Nombre del App Catalog** para cambiar la etiqueta que se muestra en la pantalla de presentación.
4. El nombre y el icono se aplican en el banner de la pantalla de inicio. Para cambiar una imagen de banner personalizada, deseleccione la opción **Aplicar el nombre y el icono en el banner de la pantalla de inicio**. Esto mostrará la sección **Imagen del banner de la aplicación**.
5. Para cambiar la imagen del banner de la aplicación, arrastre y suelte el nuevo archivo de la imagen del banner hasta el cuadro punteado o haga clic en **Elegir archivo** para seleccionarlo desde su sistema de archivos. La imagen del banner de la aplicación aparece en la barra superior de la pantalla de inicio de la aplicación.
6. En la sección **Color del texto**, haga clic en el cuadro de código de color hexadecimal para elegir un color o introduzca el código de color hexadecimal para asignarlo al texto y a los iconos. Esto se aplicará al texto de la pantalla de presentación, al nombre de la aplicación, al banner y al botón de acción.
7. Haga clic en **Guardar cambios**.

El nombre del catálogo de aplicaciones que introduzca se aplicará tanto a Android como a iOS y macOS.

12.10.2. Personalizar el App Catalog de Android

Licencia: Gold

Puede personalizar el {{app catalog}} de Android para que la apariencia le resulte más familiar a sus usuarios finales. Se pueden personalizar los siguientes elementos en el catálogo de aplicaciones de Android:

- Logotipo del catálogo (PNG, 360x64)
- Nombre del catálogo
- Color de la barra de acciones
- Icono de acceso directo
- Nombre del acceso directo

Personalizar el App Catalog de Android

Procedimiento

1. En la pantalla **Personalización de marca del Catálogo de aplicaciones**, haga clic en **Personalizar (arriba a la derecha)**.
2. Para cambiar el logotipo de la aplicación, arrastre el archivo del logotipo hasta el cuadro punteado o haga clic en **Elegir archivo** para seleccionarlo desde su sistema de archivos.
3. Haga clic en el campo **Color de la barra de acciones** para mostrar una paleta de colores de la que seleccionar o introduzca el número hexadecimal del color que prefiera.
4. Edite el texto de **Nombre del catálogo de aplicaciones** para cambiar la etiqueta del catálogo.
5. El nombre del catálogo de aplicaciones que introduzca se aplicará tanto a Android como a iOS y macOS.
   Para cambiar el icono del logotipo, arrastre el archivo del icono hasta el cuadro punteado o haga clic en **Elegir archivo** para seleccionarlo desde su sistema de archivos.
6. Edite el texto de **Nombre del acceso directo** para cambiar el acceso directo de la aplicación.
7. Haga clic en **Guardar cambios**.

12.10.3. Administrador > Personalización de marca del kiosko de Android

Licencia: Silver

Puede personalizar la página del kiosco de Android para que la apariencia le resulte más familiar a sus usuarios finales. Puede personalizar los siguientes elementos:

- logotipo (PNG, 840x114) o texto del banner
- color del borde del banner
- color de fondo del banner
- color de fondo de la pantalla
- imagen de fondo de la pantalla (1280x800)
- formato de fondo de la pantalla

Cómo personalizar la pantalla del kiosco de Android

Procedimiento

1. Vaya hasta **Administrador > Kiosco de Android**.
2. En la página **Personalización de marca en el modo kiosco** haga clic en **Crear imagen de marca**.
3. En el campo **Nombre**, escriba el nombre de la imagen de marca en el modo kiosco.
4. Si desea desactivar el banner, quite la marca de verificación de **Habilitar banner superior.**
5. Haga clic en el campo **Color de fondo del banner** para mostrar una paleta de colores de la que seleccionar o introduzca el número hexadecimal del color que prefiera.
6. Haga clic en el campo **Color del borde del banner** para mostrar una paleta de colores de la que seleccionar o introduzca el número hexadecimal del color que prefiera.
7. Seleccione **Imagen/logotipo** o **Texto** para establecer el contenido del banner.
8. Si ha seleccionado **Imagen/logotipo**, arrastre y suelte el archivo de la imagen o haga clic en **Elegir archivo** para seleccionar uno.
9. Si ha seleccionado **Texto**, escriba el texto que desea mostrar en el banner.
10. Haga clic en la pestaña **Fondo**.
11. Haga clic en el campo **Color de fondo** para mostrar una paleta de colores de la que seleccionar o introduzca el número hexadecimal del color que prefiera.
12. Para cambiar la imagen de fondo:
13. a. Eliminar la imagen predeterminada.
    b. Arrastre y suelte la imagen seleccionada o haga clic en E **legir archivo** para seleccionar una.
    c. Seleccione el diseño preferido.
    Haga clic en **Guardar cambios**.
    La imagen de marca en el modo kiosco creada se muestra en la página **Personalización de marca en el modo kiosco**. Para seguir editando la personalización de marca, haga clic en el icono Editar de la columna **Acciones**. Para eliminar la personalización de marca, haga clic en el icono de Eliminar. Al eliminar la personalización del kiosco personalizada, la configuración que use la personalización se revertirá a la personalización predeterminada.

12.10.4. Cómo personalizar las plantillas de correo electrónico

Puede personalizar la invitación por correo electrónico del usuario final para que la apariencia le resulte más familiar a sus usuarios finales. Haga clic en **Revertir a los ajustes predeterminados** para borrar las personalizaciones.

Puede personalizar las siguientes plantillas de correo electrónico en todos los idiomas compatibles:

- **Invitación del usuario final**- invite a un usuario a conectar sus dispositivos para obtener acceso a aplicaciones y configuraciones.
- **Notificación de restablecimiento de contraseña**- el sistema envía correos electrónicos recordatorios 7 días y 24 horas antes de la caducidad de la contraseña de las cuentas locales. Esta opción no es aplicable a las cuentas LDAP.
- **Confirmación de registro**- el correo electrónico se envía una vez que el usuario completa el registro. Puede usar esta opción para agradecer a los usuarios que se hayan registrado y para indicarles más recursos de aprendizaje.
- **Notificación de cumplimiento de políticas**- el correo electrónico se envía cuando los dispositivos no cumplen con la política.

Esta sección contiene los siguientes temas:

- Previsualizar y probar una plantilla de correo electrónico
- Personalizar los encabezados de los mensajes
- Personalización de una plantilla de correo electrónico
- Variables de correo electrónico compatibles

Previsualizar y probar una plantilla de correo electrónico

Puede previsualizar y probar las plantillas de correo electrónico. Esta prueba le permite enviar un correo electrónico basado en la plantilla a una dirección de correo electrónico que usted especifique.

Para previsualizar y probar una plantilla de correo electrónico:

1. Haga clic en **Administrador**.
2. En Plantillas de correo electrónico, haga clic en **Invitación de usuario final**, **Notificación de restablecimiento de contraseña** , **Confirmación de registro**, o**Notificación de cumplimiento de políticas**.
3. Haga clic en el enlace **Previsualizar y probar** asociado con la plantilla de correo electrónico que desea previsualizar y probar.
4. Vea la plantilla procesada en el panel de plantillas procesadas.
5. Especifique una dirección de correo electrónico de prueba a la que enviar el correo electrónico de prueba.
   Si la dirección de correo electrónico que usted especifica pertenece a un usuario actual, el correo electrónico de prueba sustituirá los valores de la mayoría de las variables de la plantilla de correo electrónico, proporcionándole una idea bastante precisa de cómo será la experiencia del usuario con el correo electrónico. No obstante, el correo electrónico de prueba no sustituirá los valores de las variables que Ivanti Neurons for MDM genera en el momento en que genera una invitación real por correo electrónico.
6. Haga clic en **Enviar correo electrónico de prueba**.

Personalizar los encabezados de los mensajes

1. Haga clic en **Administrador**.

2. Haga clic en **Plantillas de correo electrónio**.
3. Haga clic en el vínculo del icono **Editar** (situado en la columna Acciones) asociado con la plantilla de correo electrónico que desea editar.
4. Proporcione los nuevos ajustes que desee para **Nombre para mostrar del correo electrónico**, **Dirección de correo electrónico del remitente**, **Dirección de correo electrónico de respuesta** y **Configurar correo electrónico SMTP**.
5. Si personaliza las direcciones de correo electrónico del remitente y a la que responder, recomendamos que ponga en la lista de permitidos el servicio de retransmisión de correo electrónico para asegurarse de que sus mensajes de correo electrónico no los bloqueen los servicios de filtrado de SPAM. Consulte **este documento** para ver más información.
   Haga clic en **Guardar**.
6. Revise la previsualización de la plantilla de correo electrónico y haga clic en **Guardar**.

Uso de la configuración de SMTP

Se ha añadido **Ajustar la configuración de correo electrónico de SMTP** para que el administrador pueda configurar su propia integración del servidor de correo electrónico para las notificaciones salientes.

1. Vaya a **Administración > Marca > Ajustes de correo electrónico**, active la opción **Establecer la configuración de correo electrónico SMTP**.
2. Actualice los siguientes campos:
   - Servidor SMTP
   - Puerto del servidor SMTP
   - Protocolo
   - Nombre de usuario
   - Contraseña
3. Haga clic en **Probar** para enviar un correo de prueba, aparecerá una pantalla emergente **Correo electrónico de prueba**.
4. Introduzca el nombre **Destinatario** y **Cuerpo** del mensaje, haga clic en **Guardar**.

> Si las credenciales no son correctas, aparecerá un mensaje de error.

5. Haga clic en **Guardar**.

La tabla siguiente resume los campos y descripciones de la ventana Configuración de SMTP:

Campos	Descripción
Servidor SMTP	Especifique la dirección IP o el nombre de host completo del servidor SMTP que utilizará el servidor Ivanti Neurons for MDM.
Puerto del servidor SMTP	Especifique el puerto configurado para el servidor SMTP.
Protocolo	Si el servidor SMTP que está configurando es un servidor seguro, es decir, utiliza el protocolo SMTPS, seleccione el botón SMTPS. En caso contrario, deje seleccionado SMTP.
Nombre de usuario	Introduzca el nombre de usuario necesario para la autenticación SMTP.
Contraseña	Introduzca la contraseña necesaria para la autenticación SMTP.

Personalización de una plantilla de correo electrónico

1. Seleccione **Administrador > Personalización > Plantillas de correo electrónico**.
2. Seleccione la plantilla que se va a editar, **Invitación de usuario final**, **Notificación de restablecimiento de contraseña**, **Confirmación de registro** o **Notificación de cumplimiento de políticas**.
3. Haga clic en el icono del lápiz para editar que aparece junto a la plantilla de correo electrónico que desee personalizar.

4. Edite la línea de asunto, si así lo desea.
5. Edite la plantilla de correo electrónico que contiene los elementos HTML del panel del cuerpo para personalizar el contenido del mensaje.

Puede utilizar las variables que aparecen en la parte derecha del cuerpo del correo electrónico. Consulte **Variables compatibles del correo electrónico**.

6. Haga clic en **Vista previa** para previsualizar la plantilla de correo electrónico a medida va creando iteraciones según lo desee.
7. Cuando esté listo para guardar la plantilla, haga clic en **Vista previa**. Esto generará la vista previa y le ofrecerá la función de guardado.

8. Haga clic en **Guardar** si está satisfecho con la vista previa.

Contenido en la lista de permitidos y la lista de bloqueados en la invitación personalizada para el usuario

Mientras personaliza la plantilla de correo electrónico de la invitación del usuario en **Invitación del usuario final**, hay un conjunto de etiquetas de HTML en la lista de permitidos y atributos que están permitidos. También existe una lista de cadenas en la lista de bloqueados que no están permitidas en la invitación del usuario para evitar la vulnerabilidad de Cross Site Scripting (XSS).

Solo tiene permiso para usar las etiquetas y atributos de la lista de permitidos que hay en el correo electrónico de la invitación. En la siguiente tabla se enumeran las etiquetas de la lista de permitidos y sus atributos correspondientes permitidos.

Algunas etiquetas de la lista permitida (ejemplo: <big>) no deben tener ningún atributo de la lista permitida y, por tanto, se muestran en blanco.

Etiquetas incluidas en la lista de permitidos	Atributos incluidos en la lista de permitidos
<big>	[]
<img>	["id","label","editable","height","border","src","style","width", "align", "class","cellpadding","alt","title","data-max-width","data-default"]
	[]
<singleline>	["label"]
<tbody>	[]
<!DOCTYPE>	[]
<h1>	["style"]
<h2>	["style"]
<hr>	["noshade","style"]
<h3>	[]
<body>	["style", "class", "bgcolor", "paddingwidth", "paddingheight", "offset", "toppadding", "leftpadding", "lang","link","vlink","border","cellspacing","cellpadding"]
<title>	["id"]
<head>	[]
	["style","class","width","align","id"]
 	[]
<path>	["d"]
	["style"]
<html>	["xmlns","xmlns:mso","xmlns:msdt"]
	["start"]
<table>	["class","width","border","cellspacing","cellpadding","style","height","bgcolor", "align","background"]
<a>	["href","style","target","rel","class","title"]
<b>	[]
<o:p>	[]
<svg>	["xmlns","class","viewbox","width","height","role","aria-labelledby"]
	[]

Etiquetas incluidas en la lista de permitidos	Atributos incluidos en la lista de permitidos
	[]
<i>	[]
<label>	["style"]
<td>	["valign","width","height","class", "cellpadding", "cellspacing","border","bgcolor","align", "style","colspan","id"]
<p>	["style","class","align"]
<u>	[]
<meta>	["name","content","http-equiv","charset"]
<multiline>	["label"]
<style>	["type","id"]
	["style"]
<tr>	["style"]
	["style","class","lang"]
<font>	["color"]

A continuación se muestra la lista de cadenas en la lista de bloqueados que no están permitidas en la invitación de usuario personalizada.

- Script, @import, ¼script¾, script>, <script, <script>, </script>, javascript, alert(, moz-binding, expression(, +ADw-SCRIPT+AD4-,+ADw-/SCRIPT+AD4-, xml:base
- Caracteres especiales y búsqueda de javascript o secuencia de comandos
- El atributo de metacontenido que contiene "url=" no distingue entre mayúsculas y minúsculas
- El img src que no contiene .svg.
- Valor de atributo que contiene "\00"

Si se usa alguna de las cadenas de texto de la lista de bloqueados anterior en el contenido HTML de la invitación del usuario final, aparecerá un mensaje de error al hacer clic en **Vista previa**. Este mensaje de error muestra el contenido HTML que no está permitido en la invitación del usuario final. Edite y elimine el contenido HTML no permitido y, a continuación, haga clic en **Vista previa** para continuar.

> No se le permitirá guardar las plantillas editadas que contengan contenido HTML en una lista de bloqueados.

Variables de correo electrónico compatibles

Ivanti Neurons for MDM ofrece diversas variables que puede utilizar para personalizar sus plantillas de correo electrónico.

Variables de la invitación del usuario final

Variable	Descripción
$	La URL de activación del usuario: este es el hipervínculo que aparece en torno al texto $.
$	La URL de registro del clúster: NO aparece en la plantilla predeterminada, pero se hace referencia a ella indirectamente (a través de la variable $).
$	El nombre de marca del producto: éste se define como etiqueta <title> en el encabezado de la plantilla predeterminada.
$	URL del logotipo de la empresa: esta es la imagen que aparece en la plantilla predeterminada: redirecciona a una imagen en la CDN de MobileIron. Actualizar los ajustes de **Marca del usuario** cambia el valor de referencia de **$**.
${message:$	El registro del título del dispositivo del usuario.
${message:$}	Título de la invitación por correo electrónico.
${message:$}	Verificación de que el usuario está en el dispositivo.
${message:$}	El texto de introducción de la invitación por correo electrónico.
${message:$}	Instrucciones de inicio de sesión y registro.
${message:$}	Correo electrónico y aplicaciones insertadas en la información del dispositivo.
${message:$}	Información del registro si el usuario no está en su dispositivo, que incluye la URL de registro del clúster.
${message:$}	El pie de página de la invitación por correo electrónico, que incluye la etiqueta del sitio web de la empresa.
$	La etiqueta del sitio web de la empresa: NOaparece en la plantilla predeterminada pero sehace referencia a ella indirectamente (a través dela variable $).

Variables de notificación de caducidad de la contraseña

Variable	Descripción
$	La URL para restablecer la contraseña.
$	El nombre de marca del producto: éste se define como etiqueta <title> en el encabezado de la plantilla predeterminada.
$	URL del logotipo de la empresa: esta es la imagen que aparece en la plantilla predeterminada: redirecciona a una imagen en la CDN de MobileIron. Actualizar los ajustes de **Marca del usuario** cambia el valor de referencia de **$**.
${message:$}	El título de la notificación sobre la caducidad de la contraseña
${message:$}	El párrafo introductorio de la notificación sobre la caducidad de la contraseña
${message:$}	El nombre de la URL para restablecer la contraseña
${message:$}	El pie de página de la invitación por correo electrónico, que incluye la etiqueta del sitio web de la empresa.
$	La etiqueta del sitio web de la empresa: NOaparece en la plantilla predeterminada pero sehace referencia a ella indirectamente (a través dela variable $).

Variables de confirmación de registro

Variable	Descripción
$	El nombre de marca del producto: éste se define como etiqueta <title> en el encabezado de la plantilla predeterminada.
$	URL del logotipo de la empresa: esta es la imagen que aparece en la plantilla predeterminada: redirecciona a una imagen en la CDN de MobileIron. Actualizar los ajustes de **Marca del usuario** cambia el valor de referencia de **$**.
${message:$}	El título de la confirmación de registro.
${message:$}	El párrafo introductorio de la confirmación de registro.

Variables de cumplimiento de políticas

Variable	Descripción
$	Esta variable será reemplazada por el contenido que se introduce en la línea de asunto de la medida de cumplimiento del correo electrónico de envío dentro de la política.
$	Esta variable será reemplazada por el contenido que se introduce en la parte del mensaje de la medida de cumplimiento de la política de envío de correo electrónico.
$	El nombre de marca del producto: éste se define como etiqueta <title> en el encabezado de la plantilla predeterminada.
$	URL del logotipo de la empresa: esta es la imagen que aparece en la plantilla predeterminada: redirecciona a una imagen en la CDN de MobileIron. Actualizar los ajustes de **Marca del usuario** cambia el valor de referencia de **$**.
${message:$}	El pie de página de la invitación por correo electrónico, que incluye la etiqueta del sitio web de la empresa.
$	La etiqueta del sitio web de la empresa: NOaparece en la plantilla predeterminada pero sehace referencia a ella indirectamente (a través dela variable $).

Variables de atributos personalizados del usuario

El administrador puede usar **atributos personalizados del usuario** como variables de correo electrónico en la plantilla personalizada del correo electrónico en las siguientes condiciones:

- Los atributos personalizados del usuario existen en la página **Administrador > Atributos**.
- El administrador ha **asignado los atributos personalizados del usuario a los usuarios**, con valores dados para los atributos personalizados del usuario para cada usuario.

12.10.5. Portal de autoservicio

La invitación a registrarse incluye también un vínculo al Portal de autoservicio. Los usuarios finales pueden usar este portal para realizar las siguientes tareas:

- Bloquear
- Desbloquear
- Ver ubicación (si está activada en la **configuración de privacidad**)
- Borrar
- Retirar
- Cambiar la información de la cuenta (nombre, contraseña, dirección de correo electrónico)
- Forzar ingreso
- Añadir certificados de cifrado y firma

Para registrar dispositivos adicionales, los usuarios finales deben hacer clic en el vínculo del portal del registro que aparece en el Portal de autoservicio.

Si los usuarios finales pierden la URL para el Portal de autoservicio, envíelos a **https://mydevices.mobileiron.com/user/login.html**. Para los usuarios de iOS, considere la posibilidad de crear una **Configuración del clip web** para el Portal de autoservicio.

Cargar certificados de firma y cifrado

Puede permitir que los usuarios finales carguen sus certificados de firma y cifrado en el portal de autoservicio dentro de la configuración de Certificados proporcionados por el usuario. Este ajuste se puede configurar mediante la configuración de Certificados proporcionados por el usuario. Una vez configurado, los usuarios finales pueden cargar sus certificados de firma y cifrado de correos electrónicos.

1. En la pestaña **Mis certificados**, haga clic en **Añadir certificado**. Aparecerá la ventana **Añadir certificado**.
2. Actualice los siguientes campos:

Nombre del campo	Descripción
Tipo de certificado	Seleccione el tipo de certificado a cargar. Existen las siguientes opciones: • **Certificado de cifrado** • **Certificado de firma** Estas opciones son creadas desde el Portal de administración delvanti Neurons for MDM. Consulte **Configuración del certificado de identidad** para obtener más información.
Certificado a cargar	Haga clic en **Elegir archivo** para seleccionar el archivo del certificado que se va a cargar. Asegúrese de que el archivo esté en formato PKCS12.
Contraseña	Escriba la contraseña utilizada para el archivo.

3. Haga clic en **Cargar**.

Una vez cargado, podrá ver la lista de certificados en una tabla que muestra los siguientes detalles.

Nombre del campo	Descripción
Nombre del certificado	Especifica el tipo de certificados, ya sea de **cifrado** o de **firma**.
Emitido por	Los detalles de los certificados emitidos.
Cargado el	La fecha en que se cargó el certificado.
Fecha de caducidad Acciones	L fecha de caducidad del certificado. Puede llevar a cabo las siguientes acciones: • **Editar certificado**: se pueden editar los detalles del certificado. • **Borrar clave privada**: borra la clave privada del paquete del certificado(PKCS#12). • **Eliminar certificado**: se elimina el certificado del servidor de Ivanti Neurons for MDM.

Cuando el usuario carga la configuración de un certificado, el servidor vuelve a insertar la configuración que está utilizando ese certificado.

> si un usuario elimina y borra la clave privada, no se volverán a insertar las configuraciones.

Para obtener más información, consulte **Personalización del Portal de autoservicio**.

12.10.6. Portal de autoservicio (personalización)

Licencia: Silver

Puede personalizar el **Portal de autoservicio** con el logotipo de su organización. Si no añade su logotipo, el Portal de autoservicio mostrará el logotipo de servicio predeterminado.

Personalización del Portal de autoservicio

Procedimiento

1. En la pantalla Personalización del Portal de autoservicio, haga clic en **Personalizar** (arriba a la derecha).
2. Arrastre el archivo del logotipo (PNG, 182x34) hasta el cuadro punteado o haga clic en **Elegir archivo** para seleccionarlo desde su sistema de archivos.
3. Haga clic en **Guardar cambios**.

12.10.7. Personalización del inicio de sesión multiusuario (clip web)

Personalice su inicio de sesión seguro multiusuario para iOS añadiendo un nuevo título e icono del clip web.

Procedimiento

1. Vaya a **Administrador > Inicio de sesión multiusuario (clip web)**.
2. En la pantalla del Inicio de sesión multiusuario (clip web), haga clic en **Personalizar**.
3. Arrastre el archivo del logotipo hasta el cuadro punteado o haga clic en **Elegir archivo** para seleccionarlo desde su sistema de archivos.
4. Para cambiar la etiqueta, edite el texto de **Inicio de sesión seguro**.
5. Para cambiar el icono del clip web, arrastre y suelte el archivo del clip web hasta el cuadro punteado o haga clic en **Elegir archivo** para seleccionarlo desde su sistema de archivos.
6. Previsualice las actualizaciones y haga clic en **Guardar cambios**.

Para dispositivos iPhone y iPod touch, cree iconos que midan 120 x 120 píxeles o 60 x 60 píxeles (resolución estándar).

Para iPad, cree iconos que midan 152 x 152 píxeles o 76 x 76 píxeles (resolución estándar).

Para obtener más información, consulte **Inicio de sesión seguro multiusuario para iOS**.

12.10.8. Organización

Puede proporcionar un nombre de marca a la organización o personalizar el asunto de los correos electrónicos de alerta del sistema incorporando identificadores específicos del entorno (p. ej., el nombre del cliente) en cada asunto. Si no actualiza el nombre de Organización, la pantalla de Organización mostrará el valor predeterminado.

Marca de la organización

Procedimiento

1. En la pantalla Organización, introduzca el nombre deseado en el campo **Nombre**.
2. Para agregar un prefijo, haga clic en **Editar** y habilite la opción **Agregar un prefijo del nombre de empresa en todos los correos electrónicos generados por el sistema, p. ej., Caducidad de licencia**.
3. Haga clic en **Guardar** para aplicar los cambios.

12.11. Añadir la administración de dispositivos que no sean iOS

Licencia: Gold

Actualmente está utilizando una versión de Ivanti Neurons for MDM optimizada para dispositivos iOS. Esta sección describe cómo cambiarlo para permitir la administración de dispositivos que no sean iOS. Una vez que haya cambiado, también podrá administrar los siguientes dispositivos:

- Android 5.0 o versiones más recientes compatibles
- Windows 10+

El cambio para incluir la administración de dispositivos que no sean iOS no se puede revertir.

Para realizar el cambio e incluir dispositivos que no sean iOS:

1. Haga clic en **Administrador > Plataformas permitidas**.
2. Haga clic en el botón **Permitir todas las plataformas**.
3. Marque **Entiendo que esta acción no puede deshacerse** para confirmar que sabe y entiende que esta operación no se puede deshacer.
4. Haga clic en el botón **Permitir todas las plataformas**.

13. Paquetes

Esta sección contiene los siguientes temas:

- Actualización
- Paquetes Secure UEM y Secure UEM Premium
- Paquetes Legacy Bronze, Silver y Gold
  - Licencia
  - licencia
  - Platinum
- Espacio aislado para previsualizar/probar

Paquetes Secure UEM y Secure UEM Premium

Los paquetes Secure UEM y Secure UEM Premium ofrecen las funciones siguientes:

	Secure UEM	Secure UEM Premium
Device management and security		
Easy on-boarding	✓	✓
Multi-OS security and management	✓	✓
Secure email gateway	✓	✓
App distribution and configuration	✓	✓
Mobile application management (MAM)	✓	✓
Scale IT operations		
Helpdesk tools	✓	✓
Reporting	✓	✓
Secure connectivity		
Per app VPN		✓
Conditional Access		✓
Secure productivity		
Secure email and personal information management (PIM) app		✓
Secure web browsing		✓
Secure content collaboration		✓
Mobile app containerization		✓
Derived Credentials		✓
Zero Sign-On		
Passwordless user authentication (single app)		✓

Estos paquetes puede cambiar. Deberá contactar con **Ivanti Sales** para confirmar el esquema actual.

Paquetes Legacy Bronze, Silver y Gold

Esta sección describe los paquetes legados Bronze, Silver y Gold. La paquetería ha evolucionado al esquema **Secure UEM y Secure UEM Premium**.

Bronze

Las funciones básicas de Ivanti Neurons for MDM se proporcionan en el paquete Bronze. Puede ampliar el paquete Bronze de los siguientes modos:

- añadiendo más positivos
- añadiendo Silver
- añadiendo Gold

- añadiendo Platinum

Estas actualizaciones amplían su solución móvil más allá de la configuración básica del dispositivo.

Los administradores pueden contactar con la **Asistencia técnica** si están interesados en activar una o más de las **características a petición**, desactivadas de manera predeterminada, para su(s) abonado(s).

Licencia

Al actualizar a Silver se añaden las siguientes características:

- **LDAP y Conector:** compatibilidad para añadir directorios corporativos y entidades de certificación a Ivanti Neurons for MDM.
- **Sentry:** compatibilidad para controlar el acceso al correo electrónico.
- **Espacios:** compatibilidad para designar los dispositivos que administrarán los diferentes administradores (administración delegada).
- **Modo supervisado:** compatibilidad a nivel de dispositivo para la configuración específica, incluido el modo single-app.
- **Personalización del portal de autoservicio:** utilice su logotipo en el portal de autoservicio.
- **Entidades de certificación:** utilice Ivanti Neurons for MDM como una entidad de certificación.
- **Instalación/desinstalación silenciosa de aplicaciones:** implemente y desinstale automáticamente aplicaciones desde un dispositivo móvil.
- **Aplicaciones en la lista de permitidos/lista de bloqueados/obligatorias:** supervise y controle qué aplicaciones están instaladas en los dispositivos.
- **Filtro de contenido web:** aplique políticas de lista de permitidos/lista de bloqueados de sitios web a todos los exploradores web.
- **Funcionalidad específica de Apple:** habilitar/restringir AirPlay, AirDrop, distribución de fondos de pantalla de iOS y Apple TV.
- **Abrir en el administrador:** controle qué contenido de la empresa puede ser abierto por determinadas aplicaciones móviles.
- **Apps and Books de Apple:** distribuya las licencias de la aplicación móvil a los dispositivos, recupere y reasigne estas licencias cuando se retire un dispositivo.
- **Compatibilidad con la versión corporativa de Android (Android for Work)**
- **Inscripción de dispositivos:** permite que los clientes puedan comprar dispositivos en grandes cantidades e inscribirlos automáticamente en MDM durante la activación.
- **Configuración por aplicación:** implemente las aplicaciones móviles configuradas a escala, casi sin necesidad de que el usuario final haga nada.
- **VPN de terceros por aplicación:** la seguridad VPN ahora es inmediata, invisible y específica para la aplicación móvil.
- **Medidas de políticas por niveles**
- Filtros de distribución de aplicaciones
- **Audit Trails**
- **Modo kiosco de Android:** compatibilidad para configurar dispositivos Android para que funcionen en el modo kiosco.
- **Personalización de marca del kiosko de Android:** cambie el fondo de pantalla y el banner que se muestran cuando el dispositivo funciona en modo kiosco.
- **Prevención de pérdida de datos (DLP) de Office 365 a través de las API de Microsoft Graph**: garantiza los controles de DLP para las aplicaciones de Office 365 a través de las API de Graph.

licencia

La actualización a Gold añade a las características proporcionadas por Silver, así como las siguientes características:

- **Inicio de sesión único:** los usuarios se autentican una sola vez e inician sesión automáticamente en las otras aplicaciones móviles de la empresa.
- **Personalización de marca del App Catalog de iOS y Android:** se muestra el logotipo de su empresa en el catálogo de aplicaciones.
- **Límite de contenido aumentado:** 50 archivos de 25 MB cada uno
- **AppConnect para iOS:** asegure y configure aplicaciones habilitadas para AppConnect.
- **AppTunnel para iOS:** asegure el acceso de las aplicaciones a los recursos corporativos.
- **Docs@Work para iOS:** permita que los usuarios vean, almacenen y compartan documentos.
- **Inicio de sesión único basado en certificado iOS 8**
- **Administración de iOS 8 iBook/ePub**
- **Compatibilidad con macOS**
- **Marca del usuario**
- **Mobile Application Management (MAM) con AppConnect**
- **Credenciales derivadas**
- **Soporte para Windows 10 (incluye Bridge)**

Platinum

La actualización a Platinum añade las características proporcionadas por Gold, así como las siguientes características:

- **Tunnel:** configure el acceso específico de las aplicaciones a los datos corporativos.
- **Help@Work**
- **Supervisar**
- **ServiceConnect (ServiceNow, Splunk)**

Espacio aislado para previsualizar/probar

Los clientes de Ivanti Neurons for MDM pueden obtener un abonado aislado para previsualizar y probar los nuevos lanzamientos antes de que estos vean la luz si se adquiere **Premium Plus**.

13.1. Actualización

Esta sección contiene los siguientes temas:

- Actualizar una licencia
- Solicitar una actualización
- Actualizar desde una versión anterior

Actualizar una licencia

Las funciones básicas se proporcionan en el paquete Bronze. Puede ampliar el paquete Bronze de los siguientes modos:

- añadiendo más positivos
- añadiendo Silver
- añadiendo Gold
- añadiendo Platinum

Estas actualizaciones amplían su solución móvil más allá de la configuración básica del dispositivo.

Solicitar una actualización

Procedimiento

1. Seleccione **Opciones de actualización** en el menú desplegable del administrador.
2. Haga clic en **Solicitar actualización/Añadir dispositivos** (arriba a la derecha).
3. Seleccione los elementos que desea añadir e introduzca su número de teléfono.

Un representante se pondrá en contacto con usted en las próximas 24 horas con más detalles.

Actualizar desde una versión anterior

Cuando se actualiza desde una versión anterior, no se conservan los ajustes de la página **Editar perfil de Inscripción de dispositivos** . Anote sus ajustes opcionales antes de actualizar.

- Si se ha habilitado **Omitir el inicio de sesión en AppleID y en iCloud** antes de la actualización, **Omitir configuración de Apple Pay** estará habilitado después de actualizar.
- Si se ha habilitado **Omitir introducir código de acceso** antes de la actualización, **Omitor Touch ID** y **Omitir configuración de Apple Pay** estarán habilitados después de actualizar.

Procedimiento

1. Una vez que la actualización se haya completado, vuelva a la página **Editar perfil de Inscripción de dispositivos** para editar el perfil de Inscripción de dispositivos a fin de restaurar los ajustes deseados.
2. Haga clic en **Guardar**.

Después de la actualización, varios ajustes de la configuración se verán afectados.

- Las opciones de promoción están establecidas en **Off**.
  Los ajustes de instalación están establecidos en **No**.

La opción **No mostrar en el App Catalog** ya no aparece seleccionada.

La opción **Instalar de forma silenciosa en dispositivos Android Samsung KNOX** está establecida en 'Falso'.

Las marcas de administración de iOS están establecidas en:

- Copia de seguridad en iCloud.
- Eliminar dadas de baja.

Estos ajustes de marcas de administración de iOS se pueden seleccionar individualmente para cada aplicación.

Ajustes de la aplicación:

- Ahora, los ajustes de la aplicación se llaman Configuraciones.
- Todos los demás ajustes de la aplicación se mantienen como estaban antes de la actualización.

Para más información, consulte los **Paquetes**.

14. Licencias de dispositivo

Ivanti Neurons for MDM las licencias basadas en el dispositivo definen el número de usuarios que puede registrar, la cantidad de contenido que puede configurar para la distribución a los dispositivos y qué funciones están disponibles. Si alcanza el límite de dispositivos, aparece un triángulo rojo en la página del administrador. Si alcanza el límite de contenido, el servicio impedirá que pueda añadir más y mostrará un mensaje indicándole que ha llegado al límite.

14.1. Suspensión del abonado

El acceso a un abonado que se utiliza junto con una licencia de evaluación o de producción puede ser suspendido por Ivanti Neurons for MDM. Se puede suspender una licencia de evaluación cuando caduque el período de evaluación o se exceda el límite de uso. Igualmente, se puede suspender una licencia de producción cuando caduque el período de suscripción o se exceda el límite de uso. Ivanti Neurons for MDM restablecerá los derechos del abonado suspendido cuando se haya renovado la licencia o se hayan comprado licencias adicionales, en los casos que excedan el límite de uso.

Cuando se suspende la licencia de un abonado:

- Los dispositivos existentes registrados continuarán funcionando con normalidad.
- Los administradores no podrán iniciar sesión en el Portal de administración.
- No se podrán registrar nuevos dispositivos.
- El acceso a la API por parte del abonado estará bloqueado.
- Los usuarios finales podrán seguir accediendo al Portal de autoservicio.

Acciones y mensajes de error de la suspensión de abonados

Acción de suspensión	Error	Mensaje de error mostrado	Ubicación
El acceso a la API de integración del cliente final está bloqueado.	La llamada a la API no funciona.	Acceso denegado. Su licencia de evaluación ha caducado. Renueve su licencia para volver a habilitar el acceso a la API. Contacte con su administrador de sistemas para obtener más detalles.	Error de API 401.
Se bloquea el registro de nuevos dispositivos.	Aparece un mensaje de error en la pantalla de inscripción.	No se ha podido registrar su dispositivo. La licencia de su sistema ha caducado. Contacte con su administrador de sistemas para obtener más detalles. Los dispositivos previamente inscritos seguirán funcionando con normalidad.	Tras la verificación de la contraseña.
Se bloquea el inicio de sesión del administrador en el Portal de administración.	Aparece un mensaje de error en la pantalla de inicio de sesión.	No se ha podido iniciar sesión. Su licencia ha caducado. Renueve su licencia para recuperar el acceso al Portal de administración y para inscribir nuevos dispositivos. Los dispositivos previamente inscritos seguirán funcionando con normalidad. Contacte con su representante de ventas para renovar sus licencias. Tenga en cuenta que la contraseña del administrador caduca después de un año (365 días).	Tras la verificación de la contraseña.

15. Abrir un tique de asistencia

Visite el **Portal de soporte de Ivanti** para abrir un tique de soporte.

16. Atributos de terceros

Ivanti Neurons for MDM incluye componentes desarrollados por terceros. Puede ver la lista **aquí**.

17. Apps@Work

A partir de la versión 83 de Ivanti Neurons for MDM, puede transicionar a la experiencia nativa de Apps@Work desde la aplicación Go. Para abonados nuevos, la configuración de webclip de Apps@work no se distribuye por defecto para dispositivos de iOS que estén instalados mediante iReg o un cliente. El administrador debe distribuir manualmente la configuración de webclip en los dispositivos que estén registrados mediante iReg o cliente. Tenga en cuenta los puntos siguientes:

Ivanti Neurons for MDM **portal administrativo**:

- Por defecto, solo a los nuevos abonados se les distribuye en los dispositivos iOS el Catálogo de aplicaciones de la configuración de clientes nativos.
- Para abonados existentes, por defecto, no se distribuye la aplicación nativa de Apps@Work.
- El administrador debe enviar el Catálogo de aplicaciones para la configuración del cliente nativo de los dispositivos para que Apps@Work esté disponible en la experiencia de la tienda de aplicaciones nativas.

Cliente:

- La aplicación Go ahora tiene una pestaña para Apps@Work.
- El Catálogo de aplicaciones de configuración del cliente nativo tiene la Identidad del catálogo de aplicaciones del certificado del cliente nativo y del certificado de identidad de la Estación de aplicaciones. Ivanti Neurons for MDM envía los certificados con el Catálogo de aplicaciones para la configuración de clientes nativos.

Funciones de Apps@Work

La pestaña Apps@Work tiene las funciones siguientes:

- **Acceda a la pestaña de Apps@Work desde la aplicación Go**
- **Buscar**
- **Instalar una aplicación: botón Estados**
- **Aplicaciones destacadas y banner**
- **Notificación de actualizaciones de las aplicaciones**
- **Notificación de actualizaciones de las aplicaciones**

Acceda a la pestaña de Apps@Work desde la aplicación Go

- Se agrega una nueva pestaña en Go app para Apps@Work.
- Hay disponibles dos pestañas predeterminadas en Apps@Work: Todas las aplicaciones y Categorías.
- La pestaña Todas las aplicaciones es una lista de todas las aplicaciones en orden alfabético.
- La pestaña Categorías solo muestra las categorías que tienen aplicaciones en ella.
- Cada categoría muestra el número de aplicaciones que contiene.
- La fila de MyApps que hay bajo la pestaña Categorías es un elemento de la lista que contiene todas las aplicaciones instaladas. MyApps siempre será la primera categoría y el resto de categorías se listan en orden alfabético.
- Cuando no se instalan aplicaciones, la lista de MyApps muestra Ninguna.
- Cuando hace clic en una categoría, todas las aplicaciones que son específicas de la categoría se listan con la opción Instalar. El asistente le permite instalar individualmente cada aplicación o puede hacer clic en Instalar todo para instalar todas las

aplicaciones de la categoría. Se le solicitará que permita la instalación de cada aplicación.

Buscar

- Pulse el icono de búsqueda (lupa) para buscar lo siguiente:
  - Nuevas versiones: aparece una lista de nuevas aplicaciones cuando no se escribe texto en la barra de búsqueda
  - Escriba cualquier texto y el campo de búsqueda predecirá de manera dinámica y mostrará las aplicaciones que coincidan.
  - El número de resultados de búsqueda se muestra como subtítulo
  - Puede pulsar el botón Instalar para instalar una aplicación sin acceder a la página de detalles.

Instalar una aplicación: botón Estados

- Puesto que la instalación de aplicaciones requiere que el servidor procese la solicitud y aplique la aplicación en el dispositivo, el botón de instalar no se mostrará en el progreso en tiempo real.
- El botón de instalar cambia los estados de Instalar > Solicitado > Instalado.
- Aparece un mensaje de alerta, la primera vez, que indica que se ha solicitado una instalación.
- La alerta también aparece cuando pulsa el botón "Solicitado".
- El estado Instalado no es un botón.

Aplicaciones destacadas y banner

- La pestaña Destacados es visible según la configuración del administrador.
- La pestaña Destacados es la página de inicio predeterminada cuando no hay actualizaciones disponibles.
- El banner de la aplicación destacada muestra una aplicación en el banner.
- La Aplicación destacada contiene una lista de todas las aplicaciones destacadas.

Notificación de actualizaciones de las aplicaciones

- Go envía una notificacióni cuando hay disponible alguna actualización. La notificación no muestra el nombre de la aplicación.
- Si pulsa la notificación de actualización de la aplicación, se verá redirigido a la página Todas la aplicaciones de Apps@Work.
- En la aplicación Go, el icono de Apps@Work muestra una insignia de recuento del número de aplicaciones que tienen pendientes actualizaciones.
- En la pestaña Apps@Work, la subsección Actualizaciones disponibles aparece en la pestaña Todas las aplicaciones y muestra el número de aplicaciones que hay disponibles para su actualización.
- Se muestra un icono de un punto rojo por cada aplicación que requiere una actualización.

Ajustes: Mis dispositivos

- La pestaña de Mis dispositivos ahora se encuentra en Ajustes.
- Si pulsa la notificación de actualización de la aplicación, se verá redirigido a la página Todas la aplicaciones de Apps@Work.
- En la aplicación Go, el icono de Apps@Work muestra una insignia de recuento del número de aplicaciones que tienen pendientes actualizaciones.
- En la pestaña Apps@Work, la subsección Actualizaciones disponibles aparece en la pestaña Todas las aplicaciones y muestra el número de aplicaciones que hay disponibles para su actualización.

- Se muestra un icono de un punto rojo por cada aplicación que requiere una actualización.

18. Activación de la autenticación de Kerberos entre Ivanti Neurons for MDM y el servidor SCEP

Puede utilizar la autenticación de Kerberos para la comunicación entre Ivanti Neurons for MDM y SCEP. En las siguientes secciones se explica cómo activar la autenticación de Kerberos en servidores SCEP y Ivanti Neurons for MDM.

> Esta característica será funcional cuando esté disponible la versión 93 del conector Ivanti Neurons for MDM.

Pasos de configuración previa

1. Compruebe qué cuenta de servicio se está usando para el servicio SCEP en el servidor SCEP.
2. En el servidor SCEP, compruebe que la cuenta de servicio pertenece al grupo local IIS_USRS.
3. En la plantilla de certificado de servidor CA que se está aprovisionando, compruebe que la cuenta de servicio tiene permiso de inscripción.

Configuración de servidores Windows

1. Ejecute el comando siguiente en un controlador de dominio:
   setspn -s http/<SCEP-SERVER-FQDN> <domain>\<service account>
2. En **Usuarios y equipos de Active Directory**, haga clic en la pestaña **Delegación** de la cuenta de servicio:
   1. En **Confiar en este usuario solo para la delegación a servicios especificados**, seleccione **Usar solo Kerberos**.
   2. Haga clic en **Agregar** y añada el nombre del servidor SCEP.
   3. Seleccione el servicio HTTP.
   4. Haga clic en **Aceptar**.
3. Haga lo siguiente en el servidor IIS para asegurarse de que las credenciales del grupo de aplicaciones se utilizan para descifrar los tickets de Kerberos:
   1. Compruebe que el grupo de aplicaciones SCEP se está ejecutando con la cuenta de servicio que ha verificado anteriormente.
   2. Para activar useAppPoolCredentials, en la página web de Microsoft SCEP Admin (mscep_admin) o Microsoft SCEP (mscep), seleccione **Editor de configuración > System.webServer > Seguridad > Autenticación > Autenticación de Windows** y establezca el valor useAppPoolCredentials=True.
4. Desactive **Autenticación anónima** en la página web de administración de Microsoft SCEP (mscep_admin) seleccionando **Autenticación > Autenticación anónima** y haciendo clic en **Desactivar**.
5. Desactive la autenticación en modo Kernel en la configuración avanzada de la autenticación de Windows.

> Asegúrese de utilizar **Negociar** como primera opción en el servicio de autenticación.

6. Desactive la autenticación en modo Kernel en la página web de configuración avanzada de la autenticación de Windows.
7. Reinicie el servicio de IIS.

Configuración de Kerberos

En esta sección se explica cómo configurar Kerberos en el servidor Ivanti Neurons for MDM.

Configuración de ajustes de Kerberos en Ivanti Neurons for MDM

Vaya a **Administración > Infraestructura > Kerberos**e introduzca los parámetros que se indican en la tabla:

Sección de IU	Elección
Dominio Kerberos de Active Directory Servidor del Centro de Distribución de Claves (KDC) correspondiente Credenciales de usuario del servicio	IVANTI.COM kdc.ivanti.com usuario@dominio Por ejemplo: serviceuser@IVANTI.COM
Dominios para la comunicación saliente con Microsoft AD Certificate Services (los nombres de host no distinguen mayúsculas de minúsculas y deben terminar en .ivanti.com o .IVANTI.COM) Servidor SCEP o NDES: también puede utilizar nombres de host, como: ndes.ivanti.com o scep.ivanti.com.	

Activación de la autenticación de Kerberos en la configuración de inscripción de certificados SCEP de Microsoft en una entidad emisora de certificados existente

Lleve a cabo los siguientes pasos para activar la autenticación de Kerberos en una entidad emisora de certificados existente:

1. En Ivanti Neurons for MDM, seleccione **Administración > Infraestructura > Administración de certificados**.
2. Seleccione el tipo de entidad de certificación con la opción **Externa** .

> Estos tipos de autoridad de certificación externa deben indicarse como Microsoft.

3. En el menú desplegable **Acciones**, seleccione **Editar**.
4. En la ventana **Editar CA externa**, seleccione la casilla **Preferir autenticación de Kerberos** para activar la autenticación de Kerberos.

Activación de la autenticación de Kerberos en la configuración de inscripción de certificados SCEP de Microsoft para una nueva entidad de certificación

Lleve a cabo los siguientes pasos para activar la autenticación de Kerberos para una nueva entidad emisora de certificados:

1. En Ivanti Neurons for MDM, seleccione **Administración > Infraestructura > Administración de certificados**.
2. Seleccione la opción **+Agregar**.
3. En la ventana **Agregar una autoridad de certificación**, seleccione la opción **Conectarse a una autoridad de certificación SCEP de las instalaciones** .
4. Haga clic en Continuar.
5. En la ventana **Agregar una autoridad de certificación externa**, lleve a cabo los pasos siguientes:
    1. Seleccione la opción **Microsoft** en el menú desplegable **Tipo de entidad de certificación**.

2. Seleccione la casilla **Preferir autenticación de Kerberos** para activar la autenticación de Kerberos.
3. Rellene todos los campos obligatorios.
4. Haga clic en **Hecho**.

19. Guía de administración de Ivanti Neurons for MDM 127

Septiembre de 2026

Como método moderno para la seguridad de dispositivos móviles, Ivanti Neurons for MDM proporciona soluciones de Administración unificada de extremos (UEM) en una infraestructura sumamente escalable, segura y fácil de actualizar que es compatible con millones de dispositivos en el mundo.

{{Si su idioma no está disponible}}

Resumen de nuevas funciones

Ver en formato PDF

Vídeos

20. Welcome

21. Welcome CSH

22. Administración de actualización de Windows

Como administrador, puede ver y aprobar las actualizaciones notificadas por dispositivos Windows que desee actualizar mediante Gestión de actualizaciones de Windows. Mediante esta característica, puede evitar que las actualizaciones innecesarias o no probadas se instalen en los dispositivos.

La función Administración de actualizaciones requiere que los dispositivos se configuren con la configuración **Actualizaciones de software** con la opción **Solicitar aprobación de actualización** habilitada. Solo aplicando esta configuración a los dispositivos, estos notificarán las actualizaciones para la instalación y esperarán la aprobación.

Administrar actualizaciones

1. Vaya a **Administración > Actualizaciones de Windows.** En la página se mostrarán los siguientes detalles de las actualizaciones. **Fecha de creación**: la fecha en la que se creó la actualización.**Título**: describe el tipo de actualización junto con el número de artículo de la base de conocimientos.

> Al hacer clic en la actualización, aparecerá su descripción.

Clasificación: clasifica el tipo de actualización en una de las siguientes categorías:

- Actualizaciones críticas
- Actualizaciones de definiciones
- Actualizaciones de controladores
- Actualizaciones de seguridad
- Actualizaciones
- Actualización
- Actualizar lanzamientos

Distribución: la distribución realizada para la actualización. Por ejemplo, indicará **Todos** cuando la actualización se haya distribuido a todos los dispositivos.

> Si la actualización se ha distribuido a un cierto número de grupos específico, indicará el recuento de la distribución. Por ejemplo, indicará 3 si la distribución se ha realizado solo en 3 grupos.

2. Además, puede ver si se ha distribuido o no una actualización en los dispositivos requeridos. Las columnas siguientes tienen números que indican el número de dispositivos presentes en distintas categorías de las actualizaciones:
   - Dispositivos elegibles
   - Dispositivos instalados
   - Dispositivos fallidos
   - Reinice los dispositivos pendientes

Cuando hace clic sobre cualquiera de estos números, se le dirigirá a la vista filtrada de la página Dispositivos para conocer el estado de las actualizaciones y llevar a cabo las acciones necesarias.
Revise las actualizaciones y seleccione la que desea distribuir a los dispositivos haciendo clic en la casilla de verificación de dicha actualización.

3. En **Acciones**, clic en **Establecer distribución**.
4. En la ventana **Distribuir actualización de Windows**, seleccione cualquiera de las siguientes opciones de distribución:
   Todos los dispositivos: distribuye las actualizaciones a todos los dispositivos.
   Ningún dispositivo: retiene las actualizaciones y no las distribuye a ningún dispositivo.**Personalizada**: distribuye las actualizaciones para los grupos de dispositivos especificados.
5. Haga clic en **Guardar**.

Buscar y filtrar actualizaciones

Puede buscar y filtrar actualizaciones en función de los siguientes criterios:

- Id. del artículo de la base de conocimientos
- Distribución configurada

Filtrar en función de la Id. del artículo de la base de conocimientos:

1. En la página **Gestión de actualizaciones de Windows**, escriba el ID de la base de conocimientos en el campo de búsqueda rápida (solo el número en el campo Buscar).
   Ejemplo: para KB4056892, escriba 4056892. Aparecerá en la página la actualización que coincida con los criterios de búsqueda.

> Puede seguir buscando información adicional sobre la actualización haciendo clic en el enlace **Asistencia técnica** y **Más información**. Los enlaces de la **Asistencia técnica** dirigen a la página web de Microsoft que proporciona información sobre asistencia de productos para la actualización y **Más información** dirige a la página web de Microsoft que muestra más información sobre la actualización, como el artículo de la base de conocimientos.

Filtrar en función de la distribución configurada:

En la página **Gestión de actualizaciones de Windows**, seleccione cualquiera de las siguientes opciones de filtrado en función de la distribución configurada:

- **Todas**: se muestran todas las actualizaciones.
- **Configuradas**: se muestra la lista de actualizaciones que se han distribuido a los dispositivos.
- **No configuradas**: se muestra la lista de actualizaciones para las que no se ha especificado ninguna distribución.

> Los filtros Configuradas y No configuradas se basan en la distribución realizada y la distribución también puede ser **Ninguna**.

Ver actualizaciones para un dispositivo

Para ver la información detallada sobre actualizaciones específicas para un dispositivo:

1. Vaya a **Dispositivos > Dispositivos**.
2. Haga clic en el nombre del dispositivo para visualizar la página de detalles.
3. Vaya a la pestaña **Actualizaciones**. Se mostrarán las actualizaciones para el dispositivo que estén pendientes (actualización aprobada por el administrador pero no notificada como instalada en el dispositivo), que hayan fallado y que se hayan instalado.

También puede ver notificaciones sobre nuevas actualizaciones de Windows disponibles en la página «Notificaciones», en «Panel». La notificación incluye la fecha de creación de la misma, el número de notificaciones disponibles y el fin de dicha notificación. La notificación de la actualización de Windows también está visible la esquina superior derecha del Portal de administración.