ivanti

NMDM Admin Guide IT

ivanti

CONTENTS

1. **Informazioni su Ivanti Neurons for MDM** **9**
2. **Riepilogo delle nuove funzionalità** **10**
3. **Video** **14**
4. **Introduzione** **17**
   - 4.1. Configurazione dei dispositivi macOS 24
   - 4.2. Configurazione e utilizzo di messaggi e-mail di conferma della registrazione 27
   - 4.3. Configurazione e utilizzo di e-mail di notifica sulla conformità delle policy 28
   - 4.4. Funzionalità on-demand 29
   - 4.5. Preparazione per il supporto dei dispositivi Android Enterprise 32
5. **Dashboard** **33**
   - 5.1. Utilizzo di widget 34
   - 5.2. Approfondimenti app 40
   - 5.3. Utilizzo di report pianificati 45
   - 5.4. Utilizzo di report personalizzati 52
6. **Utenti** **60**
   - 6.1. Aggiunta di utenti 61
   - 6.2. Gruppi di utenti 65
   - 6.3. Impostazioni utente 70
   - 6.4. Personalizzazione degli utenti 81
   - 6.5. Registrazione utenti con Apple Business Manager 82
   - 6.6. Licenze utente 91
   - 6.7. Gestione degli utenti 92
     - 6.7.1. Aggiunta di un utente API per operazioni Cisco ISE 93
     - 6.7.2. Assegnazione di ruoli 94
     - 6.7.3. Ruoli utente 96
     - 6.7.4. Ricerca e applicazione di filtri agli utenti 99
     - 6.7.5. Assegna utenti 102
     - 6.7.6. Invio di inviti agli utenti 103
     - 6.7.7. Attivazione e disattivazione di utenti 104
     - 6.7.8. Gestione di accessi multipli dell'amministratore 106
     - 6.7.9. Modifica password 107
     - 6.7.10. Invio di messaggi 109
     - 6.7.11. Rimozione di utenti dai gruppi di utenti 111
     - 6.7.12. Eliminazione di un utente 112
     - 6.7.13. Esportazione di utenti 113
     - 6.7.14. Assegnazione di attributi personalizzati agli utenti 114
     - 6.7.15. Rimozione di attributi personalizzati dagli utenti 115
     - 6.7.16. Modifica delle impostazioni locali degli utenti 116
     - 6.7.17. Modifica di un nome utente 117
     - 6.7.18. Interruzione della raccolta di dati sulla posizione 118
     - 6.7.19. Informazioni sul timeout 119
     - 6.7.20. Disattivazione dell'analisi di utilizzo del sistema 120
     - 6.7.21. Registrazione dispositivo tramite generazione PIN 121
7. **Dispositivi** **122**
   - 7.1. Introduzione all'uso di dispositivi 123
   - 7.2. Gruppi di dispositivi 138
   - 7.3. Dispositivi non gestiti 144
   - 7.4. Inventario delle applicazioni 145
   - 7.5. Gestione dei dispositivi 148
     - 7.5.1. Distribuzione di dispositivi Apple 150
     - 7.5.2. Distribuzione di dispositivi Windows 159
     - 7.5.3. Configurazione di Apple Remote Desktop su dispositivi macOS 163
     - 7.5.4. Registrazione del dispositivo (iOS, macOS e Android) 164
     - 7.5.5. Registrazione dei dispositivi (PC Windows versione 10 e successive e sistemi Microsoft Hololens 2) 168
     - 7.5.6. Local Admin Password Solution (LAPS) 171
     - 7.5.7. Registrazione dei pacchetti di provisioning con PIN 173
     - 7.5.8. Utilizzo della registrazione in blocco per i dispositivi Android 176
       - 7.5.8.1. Ivanti Bulk Enrollment 178
     - 7.5.9. Configurazione passcode 180

7.5.10. Modifica del nome dispositivo ... 181
7.5.11. Ricerca e applicazione di filtri ai dispositivi ... 182
7.5.12. Utilizzo della modalità Proprietario del dispositivo ... 185
7.5.13. Dispositivo gestito con profilo di lavoro ... 192
7.5.14. Registrazione in blocco di dispositivi Android ... 193
7.5.15. Registrazione in blocco utilizzando il caricamento file CSV ... 195
7.5.16. Device_to_User_BulkEnrollment ... 198
7.5.17. Registrazione a Samsung Knox Mobile ... 199
7.5.18. Registrazione di dispositivi Oculus ... 200
7.5.19. Abilitazione di Bluetooth su un dispositivo ... 202
7.5.20. Pianifica aggiornamento iOS ... 203
7.5.21. Reinstallare le app del sistema iOS ... 204
7.5.22. Assegnazione di un dispositivo a un nuovo utente ... 205
7.5.23. Riassegnazione di un dispositivo Android ... 206
7.5.24. Come forzare il check-in ... 207
7.5.25. Individuazione di un dispositivo ... 208
7.5.26. Blocco di un dispositivo ... 209
7.5.27. Gestione dei dispositivi Apple in modalità smarrimento ... 210
7.5.28. Gestione dispositivi Android in Modalità smarrimento ... 212
7.5.29. Richiesta registri di debug ... 214
7.5.30. Apple_Enhanced_Logging ... 215
7.5.31. Disattivazione di un dispositivo ... 216
7.5.32. Cessione della proprietà di un dispositivo ... 217
7.5.33. Cancellazione di un dispositivo ... 218
7.5.34. Eliminazione di dispositivi ... 220
7.5.35. Sblocco di un dispositivo ... 221
7.5.36. Riavvio o arresto dei dispositivi ... 223
7.5.37. Cancellazione della password restrizioni (solo iOS) ... 225
7.5.38. Eliminazione dell'associazione Sentry per un dispositivo ... 226
7.5.39. Assegnazione di attributi personalizzati ai dispositivi ... 227
7.5.40. Rimozione di attributi personalizzati dai dispositivi ... 228
7.5.41. Sincronizzazione e recupero del feedback per un'app ... 229
7.5.42. Impostazione della password del firmware ... 231
7.5.43. Rilascio di una nuova chiave di ripristino personale ... 232
7.5.44. Impostazione o modifica di un blocco di ripristino ... 234
7.5.45. Gestione accessi Apple ... 235
7.5.46. Registrazione criteri di gruppo ... 236
8. App ... 237
8.1. Catalogo app ... 238
8.2. Gestione app Gestione dichiarativa dei dispositivi (DDM) ... 257
8.2.1. Impostazioni Gestione app DDM ... 259
8.3. Apps@Work (iOS, Android, Windows e macOS) ... 262
8.4. Caratteristiche dell'AppStore iOS Apps@Work ... 265
8.5. Funzioni avanzate di iOS Go ... 268
8.6. Visualizzazione dei dettagli delle app ... 275
8.7. Configurazione dell'app ... 278
8.8. Assegnazione di attributi personalizzati alle app ... 294
8.9. Configurazioni gestite per Android ... 296
8.10. Gestione delle app Google Play ... 301
8.11. Rimozione di app dal Catalogo app ... 303
8.12. Aggiornamento di app interne ... 304
8.13. Ricerca del nome del pacchetto per le applicazioni Android ... 305
8.14. Categorie ... 306
8.15. Filtri di distribuzione ... 307
8.16. Escludere o distribuire le app ... 310
8.17. Recensioni ... 311
8.18. Apple App e libri ... 313
8.19. Impostazioni catalogo ... 322
8.20. Distribuzione di dipendenze delle app ... 325
8.21. Distribuzione di Divide Productivity con Android Enterprise ... 328
8.22. Configurazione dell'app Provisioner ... 331
8.23. Gestione delle applicazioni Windows ... 334

8.24. Ivanti Bridge ... 337
9. Contenuti ... 342
9.1. Gestione di contenuti ... 343
9.2. Categorie ... 345
10. Configurazioni ... 346
10.1. Utilizzo delle configurazioni ... 347
10.2. Creazione di una configurazione del Portale self-service utente ... 359
10.3. Configurazione personalizzata ... 361
10.4. Invio di SyncML su dispositivi con configurazioni personalizzate ... 363
10.5. Configurazione layout schermata principale ... 364
10.6. Configurazione del controllo delle app: controllo delle app installate per dispositivo ... 366
10.7. Configurazione delle notifiche app ... 368
10.8. Esportazione di configurazioni ... 370
10.9. Assegnazione della priorità alle configurazioni ... 371
10.10. Gestione delle configurazioni ... 372
10.10.1. Tipi di configurazione ... 373
10.10.2. Variabili ... 388
10.10.3. Configurazioni App Connect ... 393
10.10.3.1. Panoramica di AppConnect ... 394
10.10.3.2. Passcode di AppConnect ... 395
10.10.4. Configurazione di sicurezza ... 396
10.10.4.1. Android Enterprise ... 398
10.10.4.2. Attestazione Apple PassKeys ... 400
10.10.4.3. Impostazioni predefinite privacy app ... 401
10.10.4.4. Modifica della configurazione predefinita di Android Enterprise ... 404
10.10.4.5. Configurazione di Android Enterprise ... 406
10.10.4.6. Android Enterprise: dispositivo di lavoro gestito in modalità non GMS (AOSP) ... 413
10.10.4.7. Richiesta di verifica di Android Work ... 414
10.10.4.8. Configurazione dei certificati ... 419
10.10.4.9. Trasparenza certificato ... 422
10.10.4.10. Configurazione della verifica della revoca dei certificati ... 423
10.10.4.11. Crea Configurazione modalità autonoma Single App ... 424
10.10.4.12. Creazione della configurazione del proxy DNS ... 425
10.10.4.13. Configurazione registrazione dispositivo ... 426
10.10.4.14. Configurazione gestione disco ... 428
10.10.4.15. Cifratura Android ... 429
10.10.4.16. DNS cifrato ... 430
10.10.4.17. Impostazioni Intelligence esterna ... 433
10.10.4.18. Difesa dalle minacce ... 434
10.10.4.19. FileVault 2 ... 435
10.10.4.20. Chiave di ripristino di FileVault ... 436
10.10.4.21. Configurazione Opzioni FileVault ... 437
10.10.4.22. Certificato di identità ... 438
10.10.4.23. Configurazione blocco attivazione Apple ... 444
10.10.4.24. Configurazione personalizzata iOS ... 448
10.10.4.25. Impostazioni Intelligence ... 449
10.10.4.26. Restrizioni iOS ... 452
10.10.4.27. Visualizzazione Sala conferenze ... 474
10.10.4.28. Impostazioni tastiera ... 475
10.10.4.29. Blocco e tutto schermo: modalità di amministrazione del dispositivo Android ... 477
10.10.4.30. Configurazione della modalità tutto schermo per Android ... 480
10.10.4.31. Configurazione di tutto schermo per dispositivi Android condivisi ... 482
10.10.4.32. Blocco e tutto schermo: Android Enterprise ... 483
10.10.4.33. Blocco e tutto schermo: Samsung Knox Standard ... 511
10.10.4.34. Configurazione soluzione password amministratore locale ... 515
10.10.4.35. Firewall macOS ... 516
10.10.4.36. Restrizioni di macOS ... 518
10.10.4.37. Restrizioni dell'App Store di macOS ... 525
10.10.4.38. Restrizioni della masterizzazione dischi in macOS ... 526
10.10.4.39. Controllo supporti multimediali consentito (deprecato) ... 527
10.10.4.40. Impostazioni Finder in macOS ... 531
10.10.4.41. Policy di estensione kernel di macOS ... 532

10.10.4.42. Mobile@Work per macOS ... 533
10.10.4.43. Configurazione delle regole di aggiornamento del software macOS ... 539
10.10.4.44. Preferenza certificato ... 540
10.10.4.45. Active Directory (macOS) ... 541
10.10.4.46. Preferenza identità ... 544
10.10.4.47. Creazione automatica dell'account Office 365 (macOS) ... 545
10.10.4.48. Autentica ... 547
10.10.4.49. Catalogo app Apple ... 549
10.10.4.50. Domini gestiti ... 550
10.10.4.51. Impostazioni passcode ... 551
10.10.4.52. Preferenze di privacy (macOS) ... 555
10.10.4.53. Configurazione della privacy ... 557
10.10.4.54. Informazioni relative all'informativa sulla privacy del client ... 560
10.10.4.55. Impostazioni client Ivanti Go ... 561
10.10.4.56. Impostazioni Siri ... 563
10.10.4.57. Configurazione servizi Configurazione file ... 565
10.10.4.58. Aggiornamenti software ... 566
10.10.4.59. Configurazione impostazioni aggiornamento software ... 573
10.10.4.60. Configurazione delle preferenze di sicurezza ... 577
10.10.4.61. Server di riferimento orario ... 578
10.10.4.62. Filtro contenuto Web ... 579
10.10.4.63. Windows Firewall ... 582
10.10.4.64. Protezione delle informazioni di Windows ... 585
10.10.4.65. Restrizioni di Windows ... 590
10.10.4.66. Restrizioni del desktop Windows ... 596
10.10.4.67. Impostazioni desktop per Windows 10 ... 599
10.10.4.68. Configurazione di Windows Hello for Business ... 601
10.10.4.69. Configurazione Gestione IA Windows ... 602
10.10.4.70. Play Integrity (in precedenza SafetyNet Attestation) ... 604
10.10.4.71. Passcode avanzato Android e schermata di blocco ... 605
10.10.4.72. Microsoft Defender for Endpoint ... 606
10.10.4.73. Autenticazione basata su certificati ... 607
10.10.5. Configurazioni delle risorse utenti ... 608
10.10.5.1. Configurazione CalDAV ... 609
10.10.5.2. CardDAV ... 610
10.10.5.3. Configurazione di Google ... 611
10.10.5.4. Configurazione delle e-mail ... 613
10.10.5.5. Configurazione di Exchange ... 617
10.10.5.6. Configurazione del tipo di carattere ... 621
10.10.5.7. Configurazione del calendario sottoscritto ... 622
10.10.5.8. Creare una configurazione clip Web ... 623
10.10.5.9. Installazione di Office 365 ... 625
10.10.5.10. Impostazioni GPO Windows ... 627
10.10.5.11. Configurazione della crittografia BitLocker ... 629
10.10.6. Configurazione dell'accesso alla rete aziendale ... 634
10.10.6.1. Configurazione di AirPlay ... 635
10.10.6.2. Configurazione di AirPrint ... 636
10.10.6.3. Configurazione VPN Always-on ... 637
10.10.6.4. Autorizzazioni di runtime delle app predefinite ... 641
10.10.6.5. Istruzione ... 643
10.10.6.6. Configurazione proxy globale ... 644
10.10.6.7. Configurazione proxy globale (Android) ... 645
10.10.6.8. Configurazione LDAP ... 646
10.10.6.9. Configurazione server macOS ... 647
10.10.6.10. Tunnel ... 648
10.10.6.11. Configurazione di AppTunnel ... 649
10.10.6.12. Configurazione VPN per-app ... 654
10.10.6.13. Configurazione Single Sign-On ... 664
10.10.6.14. Configurazione relay di rete ... 676
10.10.6.15. Accesso sicuro multiutente per iOS ... 678
10.10.6.16. Configurazione delle impostazioni di APN Android ... 680
10.10.6.17. Configurazione VPN ... 684

10.10.6.18. VPN on Demand ... 696
10.10.6.19. Configurazione Wi-Fi ... 703
10.10.7. Configurazione della rete cellulare ... 712
10.10.7.1. Configurazione APN ... 713
10.10.7.2. Cellulare ... 714
10.10.7.3. Configurazione della rete mobile privata ... 717
10.10.7.4. Configurazione delle impostazioni delle telecomunicazioni iOS ... 718
10.10.7.5. Configurazione Slicing di rete 5G migliorato ... 719
10.10.7.6. Configurazione eSIM ... 721
10.10.8. Altra configurazione ... 724
10.10.8.1. Configurazione dei domini associati ... 726
10.10.8.2. Configurazione del trasferimento di file Android ... 727
10.10.8.3. Configurazione di Apple TV ... 731
10.10.8.4. Mirroring di AirPlay ... 732
10.10.8.5. Impostazioni browser ... 734
10.10.8.6. Configurazione della modalità Single-App per iOS ... 738
10.10.8.7. Configurazione di un profilo MDM iOS ... 741
10.10.8.8. Configurare un profilo MDM di macOS ... 743
10.10.8.9. Cache dei contenuti ... 744
10.10.8.10. Creazione di un collegamento per Android ... 748
10.10.8.11. Creazione delle configurazioni delle impostazioni di accessibilità ... 749
10.10.8.12. Crea configurazione screen saver ... 752
10.10.8.13. Configura Screen Saver utente ... 753
10.10.8.14. Impostazioni nome dispositivo ... 754
10.10.8.15. Configurazione dello sfondo del dispositivo ... 755
10.10.8.16. Configurazione Integrazione server EMA ... 758
10.10.8.17. Configurazione risparmio energetico ... 759
10.10.8.18. Configurazione Ethernet (macOS) ... 765
10.10.8.19. Configurazione di Google BeyondCorp ... 769
10.10.8.20. Configurazione del messaggio schermata di blocco ... 773
10.10.8.21. Configurazione finestra di accesso - macOS ... 775
10.10.8.22. Configurazione delle estensioni di sistema macOS ... 776
10.10.8.23. Solo MAM ... 777
10.10.8.24. Configurazione Google Play gestito ... 779
10.10.8.25. Impostazioni Assistente migrazione ... 780
10.10.8.26. Configurazione delle notifiche ... 781
10.10.8.27. Impostazioni della stampante ... 782
10.10.8.28. Configurazione Rimuovi Bloatware ... 784
10.10.8.29. Configurazione impostazioni ed estensione Safari ... 785
10.10.8.30. Configurazione delle restrizioni per telefoni Samsung ... 789
10.10.8.31. Configurazione predefinita browser - iOS e visionOS ... 790
10.10.8.32. Configurazione delle impostazioni host per la Condivisione schermo ... 791
10.10.8.33. Configurazione della modalità Single-App ... 793
10.10.8.34. Configurazione della frequenza di raccomandazione di aggiornamento software ... 796
10.10.8.35. Menu Start e barra delle applicazioni ... 797
10.10.8.36. Configurazione aggiornamento di sistema ... 799
10.10.8.37. Gestione aggiornamenti di Windows 10 ... 805
10.10.8.38. Pianificazione delle app Windows ... 808
10.10.8.39. Configurazione del BIOS di Windows ... 809
10.10.8.40. Windows BitLocker ... 817
10.10.8.41. Configurazione tutto schermo Windows ... 818
10.10.8.42. Configurazione licenza Windows ... 823
11. Criteri ... 824
11.1. Utilizzo di policy ... 825
11.2. Policy personalizzata ... 831
11.3. Monitoraggio e controllo delle app consentite ... 854
11.4. Assegnazione della priorità alle policy ... 862
11.5. Policy Hardware Windows ... 863
12. Amministratore ... 864
12.1. Sistema ... 865
12.1.1. Attributi ... 866
12.1.2. Impostazioni pulizia dispositivo ... 873

12.1.3. Profili GDPR ... 879
12.1.4. E-mail di notifica ... 881
12.1.5. Gestione dei ruoli ... 882
12.1.6. Spazi ... 889
12.1.6.1. Spazi ... 890
12.1.6.2. Gestione degli spazi ... 892
12.1.6.3. Esempi di spazi ... 897
12.1.6.4. Delega di dispositivi ... 899
12.1.6.5. Delega di app ... 900
12.1.7. Amministratori di supporto ... 902
12.1.8. Admin > Notifica di utilizzo del sistema ... 903
12.2. Infrastruttura ... 905
12.2.1. Accesso ... 906
12.2.2. Elenchi di app ... 907
12.2.3. Esportazione degli Audit trail ... 908
12.2.4. Gestione certificati ... 911
12.2.5. Configurazione SCEP per autorità di certificazione esterna ... 919
12.2.6. Provider di credenziali derivate ... 921
12.2.7. Connettore ... 922
12.2.8. Utilizzo del comando httpproxy per Connettore ... 925
12.2.9. Help@Work ... 926
12.2.10. Identità dell'infrastruttura ... 929
12.2.10.1. Configurare il provider di identità ... 930
12.2.10.2. Provisioning utente con SCIM ... 934
12.2.10.2.1. Provisioning utente per Entra ID IdP ... 937
12.2.10.2.2. Provisioning utente per Okta IdP ... 943
12.2.11. Configurazione del server LDAP ... 946
12.2.12. Sentry ... 956
12.3. Impostazioni Apple ... 957
12.3.1. Apple Configurator ... 958
12.3.2. Registrazione guidata dall'account ... 960
12.3.3. Registrazione dispositivo ... 963
12.3.4. Registrazione alla beta ... 979
12.3.5. Configurazione dell'assistente di installazione ... 980
12.3.6. Installa certificato MDM ... 981
12.3.7. Dispositivi iPad condivisi per business ... 982
12.3.8. School Manager ... 987
12.3.9. Impostazioni (Apple) ... 990
12.4. Utilizzo di dispositivi Windows ... 993
12.4.1. Configurazione di profili Windows Autopilot ... 994
12.4.2. Audit trail sui profili di Windows Autopilot ... 1000
12.4.3. CSP TenantLockdown ... 1001
12.4.4. Browser ADMX (GPO) ... 1002
12.4.5. Configurazione degli intervalli dell'inventario app ... 1003
12.4.6. Inventario hardware ... 1004
12.5. Configurazione con Microsoft Azure ... 1005
12.5.1. Utilizzo di Microsoft Azure ... 1006
12.5.2. Configurazione di Entra ID Windows 10 Unified Endpoint Management ... 1009
12.5.3. Assegnazione dell'app Entra ID UEM ... 1010
12.5.4. Collegare Ivanti Neurons per MDM con origine utente Entra ID ... 1011
12.5.5. Tenant Azure ... 1013
12.5.5.1. Azure Tenant Requirements ... 1014
12.5.5.2. Applicare la licenza Intune agli utenti dei dispositivi ... 1016
12.5.5.3. Aggiunta di MobileIron come partner di conformità ... 1017
12.5.5.4. Creazione di un criterio di accesso condizionale in Microsoft Endpoint Manager ... 1018
12.5.5.5. Connessione di Microsoft Azure a Ivanti Neurons per MDM ... 1019
12.5.5.6. Creazione di una policy di conformità dispositivo partner ... 1020
12.5.5.7. Segnalazione stato dispositivi da Ivanti Neurons for MDM ad Azure ... 1022
12.5.5.8. Deprovisioning del tenant Azure ... 1024
12.5.6. Amministratore > Microsoft Azure > Sicurezza delle app Office 365 ... 1025
12.6. Connessione a Google Apps ... 1033
12.6.1. Account Google Play gestiti (account Android Enterprise) ... 1034

12.6.2. Registrazione di dispositivi Android ... 1038
12.6.3. API di gestione Android ... 1039
12.6.4. API Google App ... 1045
12.6.5. Amministratore - Android Enterprise ... 1046
12.7. Lavorare con i dispositivi ChromeOS ... 1048
12.7.1. ChromeOS e Ivanti Neurons per MDM ... 1049
12.7.2. Distribuire applicazioni Android su dispositivi ChromeOS ... 1051
12.7.3. Aggiungere e distribuire app di estensione per ChromeOS ... 1052
12.7.4. Configurazione del Progetto ChromeOS ... 1053
12.7.5. Azioni relative ai dispositivi ... 1054
12.7.6. Domande frequenti ... 1055
12.7.7. Passi consigliati per la valutazione ... 1057
12.8. Gestione firmware ... 1058
12.8.1. Registrazione al servizio OTA Zebra ... 1059
12.8.2. Gestione licenze Samsung E-FOTA (dismesso) ... 1060
12.9. Gestisci script e file ... 1061
12.9.1. Tutti gli script ... 1062
12.9.2. File ... 1067
12.10. Personalizzazione ... 1068
12.10.1. Amministratore > Catalogo app Apple (Personalizzazione) ... 1069
12.10.2. Personalizzazione dell'App Catalog Android ... 1070
12.10.3. Amministratore > Personalizzazione tutto schermo Android ... 1071
12.10.4. Personalizzazione dei modelli e-mail ... 1072
12.10.5. Portale self-service ... 1080
12.10.6. Portale self-service (personalizzazione) ... 1082
12.10.7. Personalizzazione dell'accesso multiutente (clip Web) ... 1083
12.10.8. Organizzazione ... 1084
12.11. Aggiunta della gestione di dispositivi non iOS ... 1085
13. Pacchetti ... 1086
13.1. Aggiornamento ... 1090
14. Licenze dispositivo ... 1092
14.1. Sospensione tenant ... 1093
15. Apertura di un ticket di supporto ... 1094
16. Attributi di terze parti ... 1095
17. Apps@Work ... 1096
18. Abilitare l'Autenticazione Kerberos tra Ivanti Neurons per MDM e il server SCEP ... 1098
19. Guida per l'amministratore a Ivanti Neurons for MDM 127 ... 1101
20. Welcome ... 1102
21. Welcome CSH ... 1103
22. Gestione aggiornamenti di Windows ... 1104

1. Informazioni su Ivanti Neurons for MDM

Con un approccio moderno alla sicurezza mobile, Ivanti Neurons for MDM offre soluzioni per la Unified Endpoint Management (UEM) in un'infrastruttura altamente scalabile, sicura e semplice da aggiornare, che supporta milioni di dispositivi in tutto il mondo.

- Aggiornamenti immediati: è possibile ottenere aggiornamenti software e di sicurezza automatici e l'accesso alle nuove funzionalità nel momento in cui diventano disponibili.
- Scalabilità on-demand: l'implementazione è scalabile man mano che cambiano le esigenze aziendali, senza la necessità di pianificare la capacità.
- Riduzione dei costi hardware: eliminando la necessità di mantenere l'hardware in locale, la gestione dei servizi basati su cloud non richiede spazio.
- Tempi di attività e disponibilità elevati.
- Ottimizzazione degli investimenti esistenti: le risorse IT vengono riallocate dalla manutenzione hardware ad attività più strategiche che aggiungono valore al business.

È possibile visualizzare i riepiloghi delle **Riepilogo delle nuove funzionalità** disponibili in questa versione.

2. Riepilogo delle nuove funzionalità

Nella presente sezione vengono riepilogate le nuove funzionalità e i miglioramenti disponibili in questa versione. Ove disponibili, vengono forniti anche riferimenti alla documentazione che descrive tali funzionalità nuove e migliorate.

Funzionalità e miglioramenti generali

Funzionalità Android

Funzionalità iOS, macOS, watchOS, visionOS e tvOS

Funzionalità Windows

Funzionalità e miglioramenti generali

- **Gestione avanzata ID pacchetto macOS :** migliorata la distribuzione interna delle app PKG di macOS rilevando e popolando in automatico l'ID pacchetto corretto durante il caricamento delle app e garantendo che lo stesso ID pacchetto venga inviato a dispositivi. Ciò migliora l'accuratezza dell'identificazione delle app, risolve le non corrispondenze dello stato di installazione del server-dispositivo e migliora il reporting dello stato di installazione. Gli ID bundle possono essere rivisti e modificati durante il caricamento prima di essere bloccati dopo la distribuzione.
- **Visibilità dell'ID bundle per le app installate**: la sezione App installate nella pagina Dettagli dispositivo ora include una colonna ID bundle, che può essere attivata o nascosta dalle impostazioni della pagina.
- **Riprova automaticamente per installazioni di app Android non riuscite**: le installazioni di app Android che entrano in uno stato di installazione Errore vengono ora riprovate in automatico a partire da un'ora dopo la registrazione del dispositivo. I comandi di installazione vengono reinviati ogni 30 minuti per un massimo di cinque tentativi per migliorare il successo della distribuzione delle app.
- **Audit Trail movimento dispositivo per gli spazi**: aggiunta l'opzione Abilita audit trail per la registrazione e l'annullamento della registrazione del dispositivo nell'impostazione Spazi per tenere traccia del movimento del dispositivo tra gli spazi. Per ulteriori informazioni, vedere Esportazione degli Audit trail.
- **Filtro della piattaforma OS per le impostazioni di pulizia del dispositivo**: gli amministratori possono ora filtrare le azioni di pulizia dispositivo in base alla piattaforma OS quando si rimuovono i dispositivi ritirati e con ritiro sospeso. Per impostazione predefinita, tutte le piattaforme supportate rimangono selezionate, preservando il comportamento esistente. Gli amministratori possono modificare la selezione e limitare le operazioni di pulizia a piattaforme specifiche come richiesto. Per maggiori informazioni, vedere Impostazioni pulizia dispositivo.
- **Sincronizzazione dei criteri app di protezione delle app Office 365**: in precedenza, gli amministratori potevano selezionare le app direttamente all'interno di Ivanti Neurons per MDM durante la creazione o la modifica dei criteri di protezione delle app. Microsoft ha deprecato l'API utilizzata per recuperare l'elenco delle app disponibili, facendo sì che gli elenchi delle app protette appaiano vuoti in Ivanti Neurons per MDM. La gestione dei criteri di protezione delle app di Microsoft Office 365 viene aggiornata per allinearsi alle modifiche in Microsoft Intune. Le applicazioni configurate in Intune sono ora sincronizzate automaticamente con Ivanti Neurons per MDM, garantendo una visibilità continua delle app protette. Mentre la rimozione delle app rimane supportata da Ivanti Neurons per MDM, le nuove assegnazioni delle app devono essere configurate in Microsoft Intune e verranno visualizzate automaticamente.
- **Registrazione audit movimento dispositivo per spazi**: gli amministratori possono ora monitorare il movimento del dispositivo tra gli spazi attraverso i Registri di controllo. Se attivata, la nuova impostazione di audit registra gli eventi ogni volta che un dispositivo viene rimosso da uno spazio e aggiunto a un altro, fornendo una maggiore visibilità sulle assegnazioni di spazio automatizzate e basate su regole. Per ulteriori informazioni, vedere Esportazione degli Audit trail.

- **Assegnazione automatica di attributi personalizzati utilizzando Gruppi di dispositivi**: gli amministratori possono ora assegnare attributi personalizzati a livello di gruppo di dispositivi. I dispositivi che fanno parte di un gruppo di dispositivi ereditano automaticamente i valori di attributo configurati, riducendo la configurazione manuale e contribuendo a garantire una categorizzazione coerente del dispositivo. Per maggiori informazioni, vedere **Gruppi di dispositivi**.
- **Restrizioni di registrazione dei dispositivi a livello di sistema operativo**: limitare la registrazione dei dispositivi per piattaforma, consentendo la registrazione solo ai dispositivi **Apple**, **Android** e **Windows** approvati. Per maggiori informazioni, vedere **Impostazioni utente**.

Funzionalità Android

- **Previeni gli aggiornamenti delle app mentre l'app è in uso**: gli amministratori possono ora impedire che le app Android gestite vengano aggiornate mentre sono attivamente in uso. Quando l'opzione **Non aggiornare mentre l'app è in uso** è attivata, l'aggiornamento dell'app viene posticipato fino a quando l'utente non chiude l'app o la sposta in background, contribuendo a ridurre al minimo le interruzioni durante le sessioni attive. Per ulteriori informazioni, consultare **Configurazione dell'app**.
- **Mantieni la modalità Kiosk tra le modifiche ai criteri di blocco**: aggiunta del supporto per il mantenimento della modalità Kiosk tra le modifiche ai criteri di blocco. I dispositivi tornano automaticamente in modalità Kiosk dopo un aggiornamento dei criteri di blocco, riducendo l'intervento manuale e minimizzando le interruzioni sui dispositivi dedicati. Per maggiori informazioni, vedere **Blocco e tutto schermo: Android Enterprise**.
- **Abilita notifiche non redatte**: aggiunto supporto per la configurazione della visibilità delle notifiche della schermata di blocco sui dispositivi del proprietario del dispositivo. Gli amministratori possono visualizzare, nascondere o oscurare il contenuto delle notifiche sulla schermata di blocco per proteggere le informazioni sensibili mantenendo al contempo la funzionalità di notifica. Per maggiori informazioni, vedere **Passcode avanzato Android e schermata di blocco**.
- **Supporto per il mapping da dispositivo a utente durante la registrazione in blocco dei profili**: è stato aggiunto il supporto per il mapping da dispositivo a utente nei profili di registrazione in blocco. Gli amministratori possono assegnare un utente specifico a ciascun dispositivo tramite il file CSV di registrazione in blocco o durante l'aggiunta manuale del dispositivo, consentendo l'assegnazione automatica dell'utente durante la registrazione e riducendo le attività amministrative post-registrazione. Gli amministratori possono anche aggiornare le assegnazioni degli utenti prima della registrazione del dispositivo. Per maggiori informazioni, vedere **Mapping da dispositivo a utente in Profili di registrazione in blocco**.

Funzionalità iOS, macOS, watchOS, visionOS e tvOS

- **Nuove chiavi ignora per i profili di registrazione del dispositivo**: gli amministratori possono ora utilizzare le seguenti chiavi ignora quando creano i profili di registrazione dei dispositivi:
  - **Salta riquadro Liquid Glass** (iOS 27.0+ e macOS 27.0+)
  - **Salta riquadro Aspetto accessibilità** (iOS 27.0+)
    Queste chiavi ignora aiutano a semplificare l'esperienza di registrazione consentendo agli amministratori di nascondere specifici riquadri di configurazione durante la registrazione dei dispositivi. Per ulteriori informazioni, vedere **Registrazione dispositivo**.
- **Supporto per lo stato di integrità del sistema di dispositivi DDM**: Ivanti Neurons per MDM ora supporta lo stato di integrità del sistema di dispositivi DDM nella pagina **Dettagli dispositivi**. Gli amministratori possono visualizzare questo stato nella sezione **Integrità componenti dispositivi** per monitorare l'integrità del sistema riportata dai dispositivi supervisionati. Per maggiori informazioni, vedere **Introduzione all'uso di dispositivi**.
- **Aggiunta di nuovi campi Dettagli dispositivo per dispositivi Apple**: aggiunti nuovi **Dettagli dispositivi** per offrire maggiore visibilità sugli stati di Gestione dispositivi Apple. Gli amministratori possono ora visualizzare i seguenti dettagli:

  - **Modalità multiutente** per dispositivi che funzionano su iOS 27.0+. Questo campo indica se un iPad è configurato come dispositivo condiviso.
  - **Tipo di registrazione MDM** per dispositivi che funzionano su iOS 27.0+, macOS 27.0+, tvOS 27.0+, visionOS 27.0+ e watchOS 27.0+.
  - **Ritorno in servizio MDM** con conservazione delle app per i dispositivi che funzionano su iOS 27.0+ e visionOS 27.0+.

  Questi campi aiutano gli amministratori a rivedere le informazioni di configurazione e registrazione dei dispositivi direttamente dalla pagina Dettagli dispositivo. Per maggiori informazioni, vedere **Introduzione all'uso di dispositivi**.

- **Supporto per la configurazione delle impostazioni predefinite per la privacy delle app**: gli amministratori possono ora configurare le **Impostazioni predefinite per la privacy delle app** per una o più app utilizzando Gestione dichiarativa del dispositivo Apple (DDM). Quando un'app viene lanciata per la prima volta, gli utenti ricevono un singolo prompt di consenso per consentire o differire le autorizzazioni consigliate per i componenti privacy supportati, come videocamera, microfono, posizione, Bluetooth e accesso alla rete locale. Per maggiori informazioni, vedere **Impostazioni predefinite privacy app**.

> La configurazione Impostazioni predefinite privacy app è ora supportata sui dispositivi supervisionati macOS 27.0+.

- **Aggiunto nuovo attributo Gestione app DDM**: aggiunto il campo **App DDM Apple abilitata** all'attributo Gestione app DDM nelle pagine 'Ricerca avanzata' ed elenco dispositivi. Mostra quali dispositivi hanno app distribuite tramite DDM. Gli amministratori possono attivarlo tramite Impostazioni utente. Per maggiori informazioni, vedere **Introduzione all'uso di dispositivi**.
- **Configurazione SSO estendibile macOS avanzata**: aggiornamento della configurazione SSO estensibile macOS per mappare correttamente gli attributi dei token come **nome utente preferito** e **nome**. Ciò risolve gli errori di configurazione causati da mapping da token a utente non validi e consente di distribuire correttamente i profili SSO sui dispositivi.
- **Registrazione avanzata Apple**: gli amministratori possono avviare la raccolta registri avanzata Apple sui dispositivi Apple supportati utilizzando un token fornito da AppleCare. I dettagli del dispositivo visualizzano informazioni su stato sessione, token e timestamp e le sessioni attive possono essere annullate se necessario. Per maggiori informazioni, vedere **Registrazione ottimizzata Apple**.
- **Stato modalità di blocco** (iOS 27+, macOS 27+): aggiunto il supporto per la visualizzazione e il filtraggio dei dispositivi in base allo Stato modalità di blocco utilizzando il nuovo campo **Modalità di blocco di sicurezza** nella pagina **Dettagli dispositivo**, **Ricerca avanzata** e nelle regole del gruppo di dispositivi. Questo campo indica se la Modalità di blocco è attivata (**true**) o disabilitata (**false**) su un dispositivo. Per maggiori informazioni, vedere **Introduzione all'uso di dispositivi** , **Gruppi di dispositivi** e **Policy personalizzata**.
- **Aggiornamento supporto impostazioni aggiornamento software macOS**: la configurazione **Impostazioni aggiornamento software macOS** non è più supportata sui dispositivi macOS 27 e successivi. Questa configurazione ora si applica solo alle versioni supportate fino a macOS 26.x. Per maggiori informazioni, vedere **Configurazione delle regole di aggiornamento del software macOS**.
- **Aggiornamento del supporto delle restrizioni** (iOS 27+, macOS 27+): aggiornate le restrizioni **Consenti installazione miglioramenti della sicurezza in background** e **Consenti rimozione miglioramenti della sicurezza in background** per indicare che non sono più supportati su iOS 27 e versioni successive e su macOS 27 e dispositivi successivi. Per maggiori informazioni, vedere **Restrizioni iOS** e **Restrizioni di macOS**.
- **Aggiornamenti alla configurazione delle impostazioni Siri** (iOS 27.0+, macOS 27.0+, tvOS 27.0+ e visionOS 27.0+): aggiunto il supporto per le nuove impostazioni di restrizione nella configurazione Impostazioni Siri. Per maggiori informazioni, vedere **Impostazioni Siri**.
- **Aggiornamenti alla configurazione delle impostazioni di Intelligence** (iOS 27.0+, macOS 27.0+ e visionOS 27.0+): aggiunto il supporto per le nuove impostazioni di restrizione nella configurazione Impostazioni Intelligence. Per maggiori informazioni, vedere **Impostazioni Intelligence**.

- **Impostazioni privacy Safari (** iOS 27.0+, macOS 27.0+): aggiunto il supporto per le Impostazioni sulla privacy Safari nella configurazione Estensione e impostazioni Safari, che consente agli amministratori di configurare le autorizzazioni predefinite per fotocamera e microfono per siti Web specifici utilizzando la Gestione dichiarativa dei dispositivi (DDM) Apple. Per maggiori informazioni, vedere **Configurazione impostazioni ed estensione Safari**

Funzionalità Windows

- **Configurazione gestione Windows IA**: la Gestione Windows IA ora supporta criteri CSP aggiuntivi di Windows IA per la gestione delle funzionalità Microsoft Copilot, Windows Recall e Microsoft Paint IA. Gli amministratori possono disabilitare la chiave hardware Copilot, eliminare l'app Microsoft Copilot, disabilitare l'analisi dei dati IA per il Richiamo, impostare i limiti di archiviazione snapshot Richiamo e disabilitare Image Creator, Cocreator e Riempimento generativo in Paint. È stato inoltre aggiunto il supporto sia per i criteri di ambito utente che per quelli di ambito dispositivo, consentendo un controllo più granulare delle funzionalità IA sui dispositivi Windows. Per maggiori informazioni, vedere **Configurazione Gestione IA Windows**.

Funzionalità Mobile Threat Defense

Mobile Threat Defense (MTD) protegge i dispositivi gestiti dalle vulnerabilità e dalle minacce per i dispositivi mobili che colpiscono dispositivi, reti e applicazioni. Per informazioni sulle funzionalità correlate a MTD applicabili alla versione corrente, vedere la guida alla soluzione Mobile Threat Defense per la piattaforma in uso, disponibile nella sezione MOBILE THREAT DEFENSE della pagina della **Documentazione del prodotto** Ivanti.

> Ogni versione della guida di MTD contiene tutte le funzionalità di Mobile Threat Defense che attualmente risultano completamente testate e disponibili per l'uso, sia in ambiente client che in ambiente server. A causa del gap tra le versioni client e server, le nuove versioni della guida di MTD vengono rese disponibili con la versione finale della serie quando le funzionalità sono completamente operative.

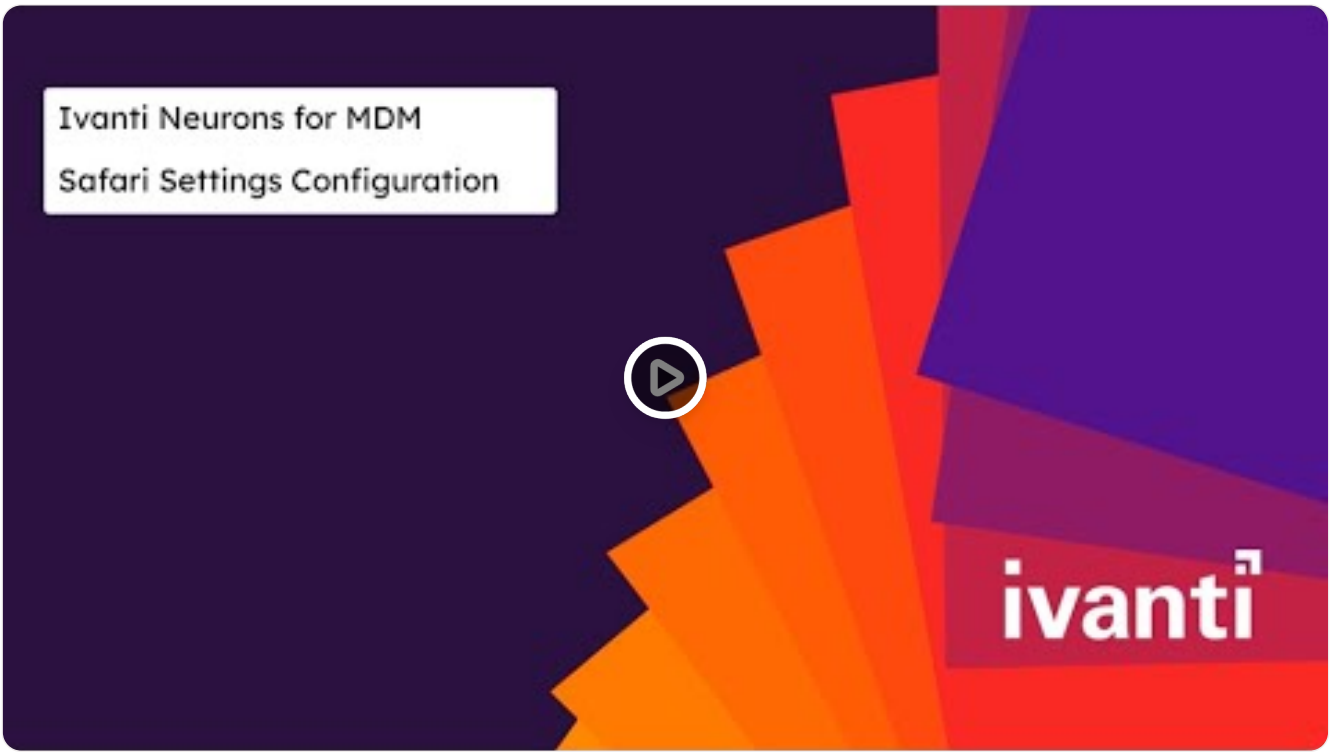
3. Video

Video in primo piano




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.



Stai cercando un video su una funzione o una funzionalità specifica in Ivanti Neurons per MDM? Faccelo sapere condividendo il tuo feedback nella sezione "**Questo articolo è stato utile?**" su qualsiasi pagina di questo documento.

4. Introduzione

Questa sezione include le panoramiche di configurazione e utilizzo delle funzioni che richiedono l'interazione nel portale di Ivanti Neurons for MDM. Argomenti della sezione:

- Panoramica della soluzione
  - Funzioni chiave
  - Diagramma dell'architettura
  - Applicazioni Ivanti Neurons per MDM
  - Ruoli
  - Introduzione
- Impostazione della lingua preferita in un browser
- Interfaccia di navigazione unificata per Ivanti Neurons for MDM e Access
- Modalità Amministratore dispositivo (DA) per la gestione di dispositivi Android - Deprecata

Panoramica della soluzione

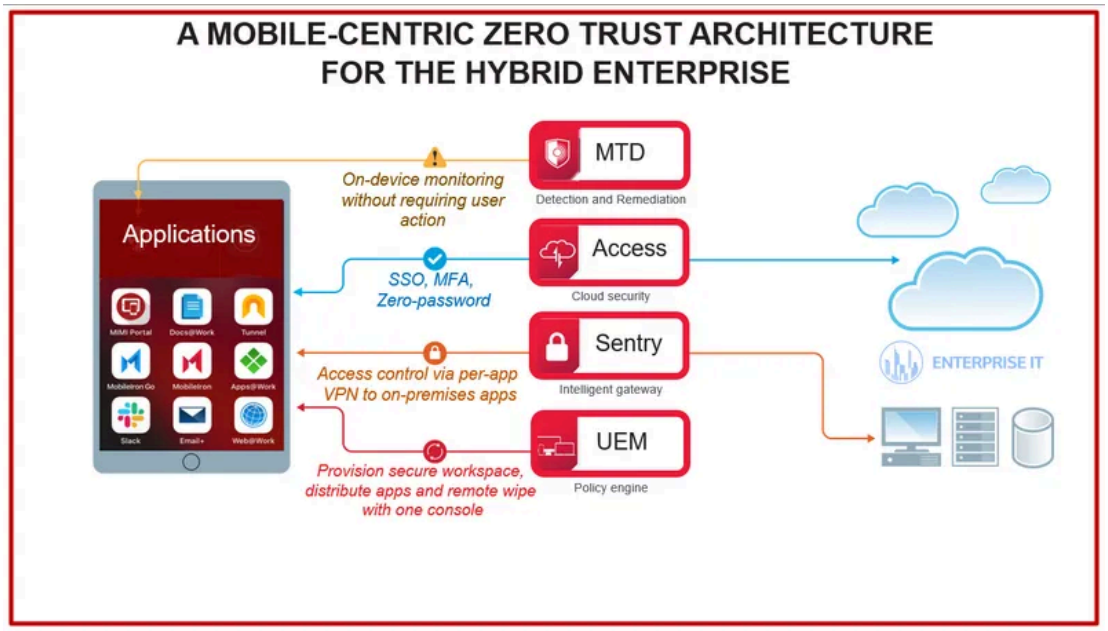
L'accesso continuo a dati aziendali su dispositivi mobili e altri endpoint fuori dalla rete aziendale richiede un'attenzione dedicata alla sicurezza. Per riuscire a gestire le esigenze di sicurezza correnti, le aziende devono considerare in che modo possono:

- Eseguire il provisioning di endpoint quali telefoni cellulari e computer portatili
- Concedere l'accesso in base a un set di dati imperativi
- Proteggere dati inattivi e di movimento
- Imporre misure in base alle esigenze

La soluzione Ivanti a questo problema moderno soddisfa tutte le esigenze. È possibile monitorare gli endpoint e attivare policy adattive per correggere le minacce, mettere in quarantena i dispositivi e mantenere la conformità. Insieme, i seguenti componenti aiutano l'organizzazione dell'utente a realizzare il quadro zero trust mobile-centrico:

- Ivanti Neurons per MDM - Consente di creare un'area di lavoro sicura in qualsiasi dispositivo con app, configurazioni e policy per l'utente in base al ruolo di quest'ultimo. Gli utenti ottengono un accesso semplice e sicuro alle risorse di cui necessitano per essere produttivi
- **Sentry**: un gateway intelligente in linea che consente di accedere in modo sicuro alle risorse locali
- **Access**: consente di verificare l'utente, il dispositivo, l'app, il tipo di rete e la presenza di minacce. La verifica adattiva di controllo dell'accesso è la base del modello zero trust. Access offre l'accesso Single Sign-On e sicurezza nel cloud
- **Mobile Threat Defense**: la combinazione di Ivanti Neurons per MDM e Mobile Threat Defense (MTD) consente di proteggere i dati nel dispositivo e nella rete con crittografia all'avanguardia e monitoraggio delle minacce per rilevare attacchi a livello di dispositivo, rete e app

La seguente illustrazione mostra la panoramica della soluzione:



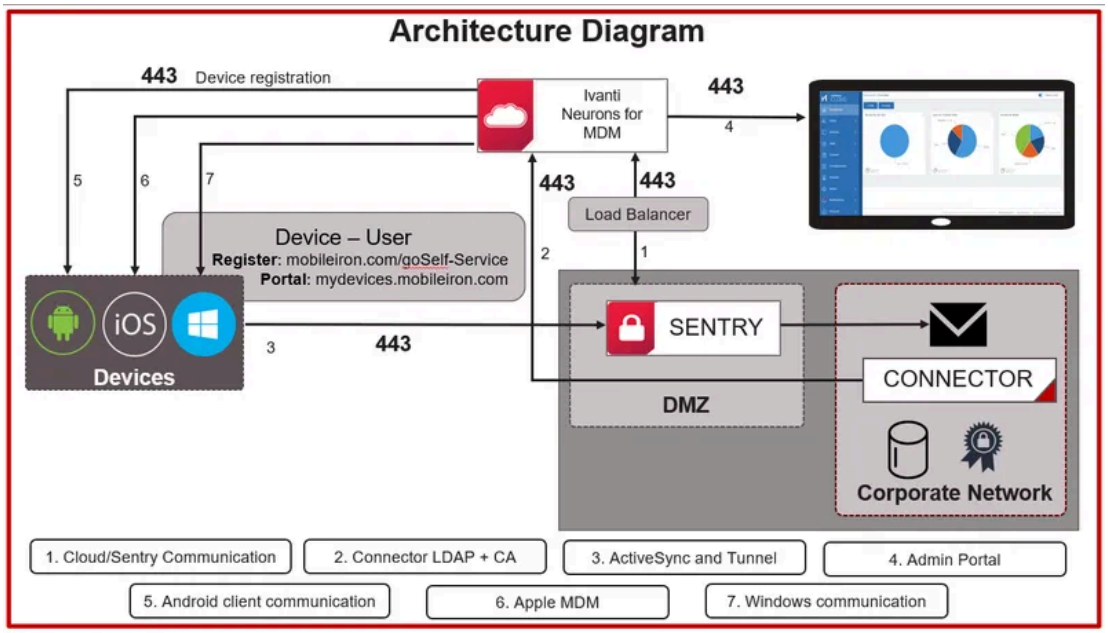
Funzioni chiave

La piattaforma Ivanti Neurons per MDM offre la visibilità e i controlli IT essenziali per proteggere, gestire e monitorare qualsiasi dispositivo mobile e desktop aziendale o di proprietà dei dipendenti che acceda a dati aziendali importanti. Ivanti Neurons per MDM consente alle organizzazioni di proteggere una vasta gamma di dispositivi dei dipendenti utilizzati all'interno dell'organizzazione gestendo al tempo stesso l'intero ciclo di vita del dispositivo, eseguendo attività quali:

- Gestione e applicazione della configurazione di policy
- Gestione e distribuzione delle applicazioni
- Gestione e distribuzione di script per dispositivi desktop
- Azioni relative ai dispositivi
- Controllo degli accessi e autenticazione a più fattori
- Rilevamento e correzione delle minacce

Diagramma dell'architettura

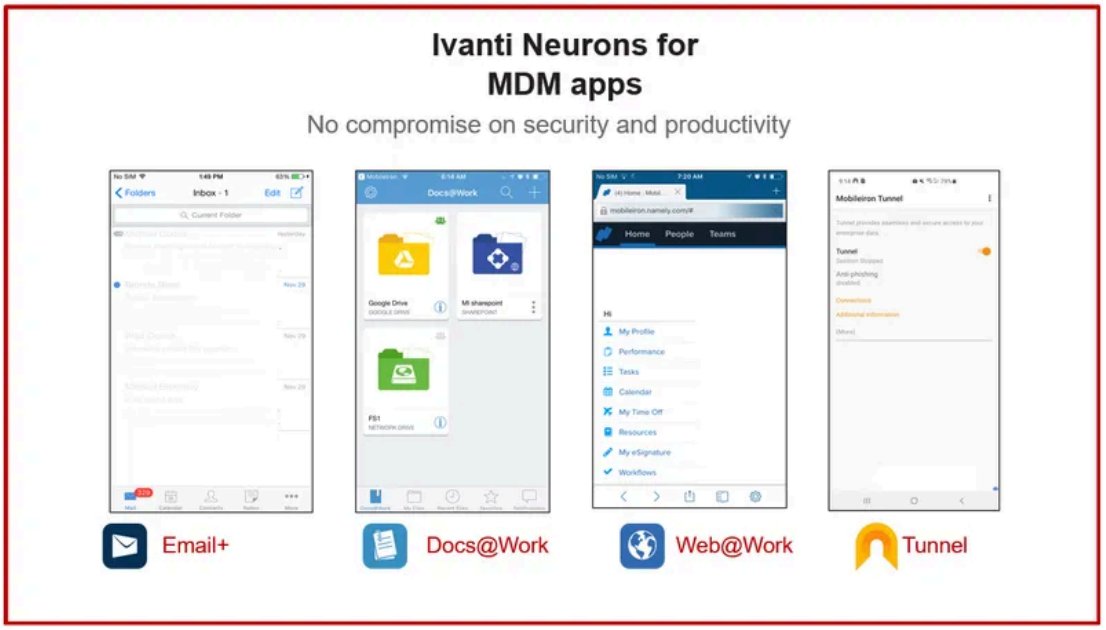
Il seguente schema mostra la panoramica dell'architettura della piattaforma UEM di Ivanti Neurons per MDM:



Applicazioni Ivanti Neurons per MDM

- **App Catalog**: l'App Catalog è una vetrina di app aziendali personalizzabili. Gli amministratori IT possono pubblicare direttamente app private o interne per i dispositivi dei propri utenti finali. L'App Catalog può essere combinato anche con l'Apple Volume Purchase Program per facilitare una distribuzione sicura di app mobili su dispositivi iOS. Inoltre, Ivanti può usufruire delle funzionalità delle app gestite da iOS e di quelle di Android Enterprise. Questo permette una facile configurazione all'interno della piattaforma Ivanti Neurons per MDM UEM delle impostazioni a livello di app e dei criteri di sicurezza per entrambe le funzioni avanzate di sicurezza delle app.
- **Email+**: un'applicazione PIM multipiattaforma sicura per iOS e Android. Email+ fornisce e-mail, calendario, contatti e attività sicure su dispositivi aziendali e personali comunicando con un server ActiveSync nell'azienda.
- **Docs@Work** - Consente agli utenti di accedere, creare, modificare, contrassegnare e condividere contenuti in modo sicuro da archivi come Microsoft Share Point e servizi cloud come Box e Dropbox. Ciò è importante affinché gli utenti possano ottimizzare la produttività ovunque si trovino.
- **Web@Work**: è un browser protetto che consente agli utenti aziendali di accedere in modo sicuro ai contenuti Web nella propria Intranet aziendale. Web@Work consente di limitare l'accesso ai dati aziendali agli utenti autorizzati. Se Web@Work viene distribuito insieme ad App Tunnel, è possibile proteggere i dati aziendali ovunque. Grazie a Web@Work, gli utenti possono accedere rapidamente e facilmente a risorse Web interne.

La seguente immagine mostra le applicazioni Ivanti Neurons per MDM:



Ruoli

Amministratore: l'amministratore aziendale è responsabile delle attività indicate di seguito.

- Fornire agli utenti aziendali l'accesso semplice e sicuro a e-mail, applicazioni e configurazioni dell'area di lavoro, nonché a strumenti di connettività quali Wi-Fi e VPN.
- Separare i dati personali dai dati aziendali sui dispositivi dei dipendenti affinché i dati aziendali non trapelino nelle app personali e i dati personali non siano inavvertitamente accessibili dall'IT.

Utente: in qualità di utente aziendale, è possibile accedere facilmente ad applicazioni aziendali e dati personali da dispositivi mobili, desktop e servizi cloud sicuri moderni. Per ulteriori informazioni sulle varie attività che si possono eseguire come utente, vedere Utenti. e Gestione dei ruoli.

Introduzione

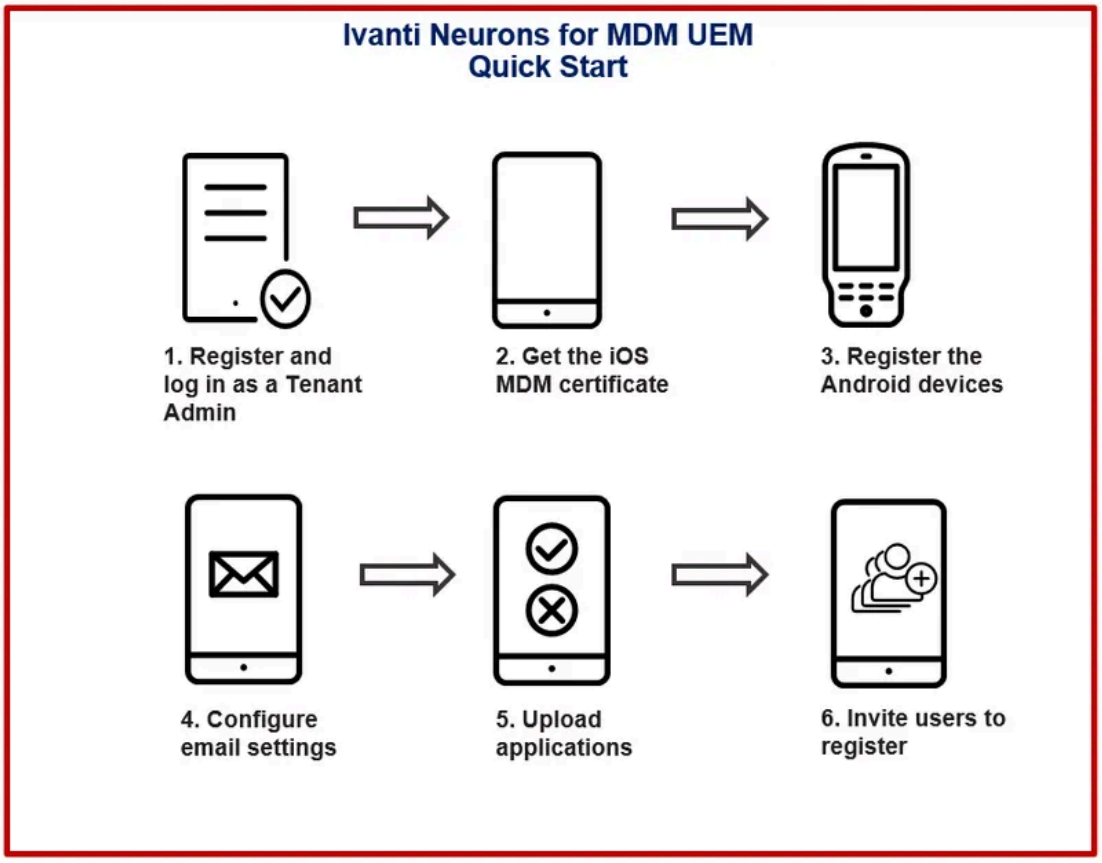
I nuovi utenti registrati possono eseguire la procedura descritta in questa sezione per iniziare a utilizzare i servizi Ivanti Neurons per MDM.

Dopo la sottoscrizione alla piattaforma Ivanti Neurons per MDM, Ivanti crea un tenant Ivanti Neurons per MDM per l'utente. L'utente riceve quindi un messaggio e-mail all'indirizzo registrato contenente un PDF con le seguenti informazioni sul tenant creato per l'azienda:

- Informazioni sul bundle software acquistato
- URL e credenziali di accesso amministratore avanzato del tenant
- Come accedere alla community di supporto e alle Domande frequenti per Ivanti Neurons per MDM
- Dove accedere alla documentazione tecnica e scaricare il software

> Ivanti, Inc non fornisce chiavi software. Se si accede al proprio tenant Ivanti Neurons per MDM con le credenziali di amministratore avanzato e si accettano le Condizioni per l'utilizzo del servizio, il prodotto Ivanti Neurons per MDM viene attivato.

Il seguente schema mostra la procedura per iniziare a utilizzare Ivanti Neurons per MDM:



Procedura

1. Fare clic sull'URL fornito nel messaggio e-mail di registrazione del tenant. Viene visualizzata la richiesta di reimpostazione della password.
2. Modificare la password.
3. Effettuare l'accesso all'account del tenant utilizzando l'ID e la password. Viene visualizzata la procedura guidata di benvenuto.
4. Completare i dettagli nel modulo di **Benvenuto**, accettare le condizioni e il contratto, quindi fare clic su **Continua**.
5. Per installare il certificato MDM iOS, consultare **Installa certificato MDM**.

Se si desidera gestire i propri dispositivi iOS in un secondo momento, è possibile saltare l'installazione del certificato MDM iOS. Quindi la procedura guidata chiederà di registrare i dispositivi Android dell'azienda. Se si salta l'installazione del certificato MDM iOS, non è possibile registrare i dispositivi iOS. Viene visualizzato un messaggio che indica che la registrazione del dispositivo iOS non è stata abilitata.

6. Per registrare i dispositivi Android in modalità Android Enterprise (AE), consultare **Account Google Play gestiti (account Android Enterprise)**. La procedura guidata chiederà quindi di configurare gli account e-mail.

Se si desidera gestire i propri dispositivi Android in un secondo momento, è possibile saltare la registrazione degli account Google Play gestiti da Android. Se si salta la registrazione degli account Google Play gestiti, non sarà possibile registrare i dispositivi Android Enterprise. È comunque possibile registrare i dispositivi Android con l'opzione Amministratore del dispositivo, tuttavia non sarà possibile utilizzare le funzionalità principali come Google Play gestito e Configurazione app.

7. Per configurare le impostazioni e-mail e ActiveSync, consultare **Configurazione di Exchange** e **Configurazione delle e-mail**.

8. Fare clic su **Continua**. Viene visualizzata la richiesta di creazione del passcode.
9. Selezionare un tipo di passcode, quindi fare clic su **Continua**.
10. Selezionare le applicazioni che si desidera caricare, quindi fare clic su **Continua**.
11. Specificare gli indirizzi e-mail degli utenti, quindi fare clic su **Continua**. Gli utenti riceveranno un messaggio e-mail per registrare i propri dispositivi mobili. Viene visualizzato un riepilogo della configurazione.
12. Fare clic su **Operazione completata**. Viene visualizzata la pagina Dashboard.
13. Per esplorare ulteriormente, procedere come segue:
    - Andare su **Utenti**. Vengono elencati tutti gli utenti invitati.
    - Andare ad **App**. Vengono elencate tutte le applicazioni caricate.
    - Accedere a **Configurazioni**. Vengono elencate tutte le configurazioni inviate durante la registrazione.

Per ulteriori informazioni sulle diverse attività che è possibile eseguire come amministratore, consultare la sezione **Amministratore**.

Impostazione della lingua preferita in un browser

Se per il browser l'utente ha impostato una lingua non supportata, può impostare en_US (English, United States) come lingua predefinita per il portale.

Per impostare la preferenza relativa alla lingua in un browser Safari su un dispositivo macOS 10.15 o versione successiva, è possibile procedere come segue:

1. Sul dispositivo macOS accedere a **System Preference** (Preferenze di sistema).
2. Accedere a **Lingua e regione > Generale**.
3. Impostare **en_US** (o qualsiasi altra lingua) come **Lingua preferita**.

Interfaccia di navigazione unificata per Ivanti Neurons for MDM e Access

Per i nuovi clienti in alcuni cluster, Access è disponibile come interfaccia di navigazione unificata con Ivanti Neurons per MDM. Effettuare l'accesso con le credenziali amministrative di Ivanti Neurons per MDM. Le opzioni di Access sono disponibili nel riquadro di navigazione a sinistra come scheda separata. Visitare la pagina della **documentazione dei prodotti** e fare clic su Access per ulteriori informazioni su Access e su come configurarlo.

L'interfaccia di navigazione unificata include le seguenti funzionalità:

- Accesso unificato per Ivanti Neurons per MDM e Access.
- Selezione di prodotti nel riquadro di navigazione a sinistra per alternare prodotti Ivanti Neurons per MDMe Access.
- Memoria di selezione prodotto: al primo accesso, viene visualizzato il portale Amministratori di Ivanti Neurons per MDM. Agli accessi successivi, viene visualizzato Ivanti Neurons per MDM o Access, a seconda del prodotto prescelto al momento del primo accesso.
- Riquadro di navigazione a sinistra per Ivanti Neurons per MDM e Access.
- Riquadro delle impostazioni dell'account unificato con collegamenti a opzioni quali Opzioni di aggiornamento, Documentazione, Portale di supporto, Modifica password e Disconnetti.

Modalità Amministratore dispositivo (DA) per la gestione di dispositivi Android - Deprecata

La modalità Amministratore del dispositivo (DA) per la gestione dei dispositivi Android è stata deprecata nella modalità per fasi a partire da Ivanti Neurons per MDM 78.

Qualsiasi nuovo utente con un nuovo tenant creato su Ivanti Neurons per MDM 78 non sarà in grado di registrare alcun dispositivo (Android 6 o versione successiva) in modalità DA. Qualsiasi nuovo tenant che deve abilitare la registrazione DA per Android da 6 a 9 deve contattare il supporto Ivanti.

- La registrazione nella modalità DA dei dispositivi con Android 10 e versioni successive continuerà a essere bloccata.
- Per gli utenti esistenti (con o senza deployment DA esistenti), non sono previste modifiche in termini di gestione dei dispositivi DA esistenti (da Android 6 ad Android 11). Tuttavia, con l'aggiornamento a Ivanti Neurons per MDM 78, i nuovi dispositivi registrati con Android 10+ sui tenant esistenti non potranno funzionare in modalità DA. I tenant esistenti potranno solo registrare dispositivi dalle versioni di Android dalla 6 alla 9 in modalità DA.
- Se gli utenti intendono migrare i dispositivi DA da un'istanza Core a Ivanti Neurons per MDM R78, assicurarsi che Android Enterprise sia abilitato e che almeno una configurazione di sistema sia distribuita al set di destinazione: PO, DO o COPE prima di avviare la migrazione. Questa fase è essenziale per evitare il ritiro dei dispositivi dopo la migrazione.

Tipo di registrazione DA	Tenant esistente (aggiornato a 78)	Nuovo tenant
Nuova registrazione DA del dispositivo con SO >=10	Non consentito	Non consentito
Nuova registrazione DA del dispositivo con SO < 10	Consentito	Non consentito
Dispositivi DA esistenti con SO >= 10	Rimarranno attivi	ND
Dispositivi DA esistenti con SO < 10	Rimarranno attivi	ND
Dispositivi DA migrati con SO >= 10	Saranno dismessi	Saranno dismessi
Dispositivi DA migrati con SO < 10	Rimarranno attivi	Saranno dismessi

4.1. Configurazione dei dispositivi macOS

Questo articolo fornisce un elenco delle procedure comuni e altri contenuti relativi alla configurazione dei dispositivi macOS in Ivanti Neurons per MDM. È possibile accedere a tutti gli argomenti relativi a macOS nella Ivanti Neurons per MDM *Guida per l'amministratore*.

Contenuti

- Registrazione dei dispositivi
- Configurazione del modello di invito utente
- Configurazione delle funzionalità Zero Sign-On
- Configurazione di Mobile@Work per il client macOS
- Configurazione degli script della shell di macOS
- Impostazione delle configurazioni macOS
- Configurazione delle policy di macOS

Registrazione dei dispositivi

La maggior parte degli utenti inizia con la registrazione di un dispositivo. Per avviare il processo di registrazione, è possibile seguire uno degli approcci che seguono:

- Inviare un invito a uno o più utenti finali (registrazione iReg). Per ulteriori informazioni, consultare l'argomento *Registrazione dispositivo macOS* nella sezione **Registrazione del dispositivo**.
- **Registrazione dispositivi** e **Registrazione utenti con Apple Business Manager**

Per ulteriori informazioni, vedere Registrazione del dispositivo.

Configurazione del modello di invito utente

È possibile personalizzare l'invito per e-mail inviato all'utente finale per ottenere un aspetto più familiare. Per ulteriori informazioni, vedere **Personalizzazione dei modelli di e-mail**.

È possibile personalizzazione il processo di registrazione dei dispositivi mediante l'utilizzo di nomi e loghi riconoscibili dagli utenti. Per ulteriori informazioni, vedere **Personalizzazione degli utenti**.

Per ulteriori informazioni, vedere **Configurazione e utilizzo di messaggi e-mail di conferma della registrazione**.

Configurazione delle funzionalità Zero Sign-On

Per la documentazione relativa a Zero Sign-On, vedere Zero Sign-on con Access nella *Guida di Access*.

Per la registrazione automatica zero-touch, vedere il passaggio 13 della sezione Configurazione delle impostazioni per le nuove registrazioni di dispositivi nell'argomento Impostazioni utente.

Configurazione di Mobile@Work per il client macOS

Mobile@Work per l'app macOS offre:

- funzionalità di creazione script su dispositivi macOS

- App Catalog per gli utenti finali
- Notifiche push
- schermata di onboarding utente (benvenuto/stato) per le registrazioni automatiche del dispositivo

Prima di inviare Mobile@Work agli utenti finali, assicurarsi che la **Mobile@Work for macOS Configuration.htmMobile@Work per macOS** venga creata e sia impostata per essere distribuita ai dispositivi macOS di destinazione.

È possibile attivare l'onboarding degli utenti per i dispositivi macOS durante il processo **Registrazione dispositivi** automatizzato. Al termine del processo Registrazione dispositivi, Mobile@Work per macOS viene inviato al dispositivo insieme ai profili, alle configurazioni e alle app.

Configurazione degli script della shell di macOS

Ivanti Neurons per MDMconsente di creare i propri script della shell macOS, che è quindi possibile caricare in Ivanti Neurons per MDM ed eseguire sui dispositivi macOS gestiti. È possibile configurare gli script che utilizzano la configurazione degli script di Mobile@Work per macOS. Mobile@Work restituisce i risultati di esecuzione dello script a Ivanti Neurons per MDM, che vengono visualizzati nei registri del dispositivo. È possibile verificare i registri del dispositivo nella pagina dei dettagli del dispositivo macOS, nella scheda **Registri**. Per ulteriori informazioni sulle attività di creazione, caricamento e gestione del repository di script, vedere **Tutti gli script**.

Prima di poter eseguire gli script della shell sui dispositivi macOS, assicurarsi che gli utenti stiano eseguendo l'app Mobile@Work per macOS sui dispositivi e che una configurazione Mobile@Work per macOS sia inviata ai dispositivi. Gli script possono essere eseguiti una volta o su base ricorrente. La creazione di script su Ivanti Neurons per MDM consente inoltre agli amministratori di raccogliere informazioni da un dispositivo e quindi conservarle in Ivanti Neurons for MDM come attributo personalizzato. Per esempio, per conoscere la versione Java su un dispositivo macOS, è possibile raccogliere queste informazioni e conservarle per ogni dispositivo in un attributo del dispositivo personalizzato. Per ulteriori informazioni, vedere *Creazione di una configurazione di script Mobile@Work per macOS* in **Mobile@Work per macOS**.

Impostazione delle configurazioni macOS

Le **configurazioni** sono delle raccolte di impostazioni inviate ai dispositivi. Ad esempio, è possibile utilizzare le configurazioni per impostare automaticamente le impostazioni VPN e i requisiti del passcode su tali dispositivi. Utilizzare la pagina **Configurazioni** per selezionare, configurare e distribuire le configurazioni. Sono presenti numerosi **tipi di configurazioni** disponibili. Nella **pagina**, è possibile visualizzare un elenco di configurazioni macOS disponibili, che include le configurazioni seguenti:

- **Wi-Fi**
- **Passcode**
- **VPN**
- **DNS cifrato**
- **FileVault 2**
- **Chiave di ripristino di FileVault**
- **Firewall macOS**
- **Restrizioni di macOS**
- **Restrizioni dell'App Store di macOS**
- **Impostazioni Finder in macOS**
- **Policy di estensione kernel di macOS**
- **Active Directory (macOS)**

- Creazione automatica dell'account Office 365 (macOS)

È possibile usare configurazioni personalizzate per importare e distribuire un file di configurazione predefinito.

Configurazione delle policy di macOS

I criteri consentono di definire i requisiti per i dispositivi, oltre alle situazioni che si verificano se un dispositivo non è conforme a tali requisiti. Ciascun criterio è composto da una regola e da un'azione di conformità (ciò che accade in caso di violazione della regola). Utilizzare la pagina **Policy** per selezionare, configurare e distribuire le policy. Protezione dati/cifratura disabilitate e App consentite sono policy relative a macOS. È possibile utilizzare policy personalizzate per creare una policy personalizzata in base agli attributi dei dispositivi e degli utenti, ai criteri di selezione, ai valori e alle azioni di conformità specificate.

Distribuzione di app macOS

Ivanti Neurons per MDM supporta la distribuzione di app macOS tramite il protocollo MDM di Apple e utilizzando l'app Mobile@Work. Gli amministratori possono scegliere di utilizzare uno o entrambi dei seguenti approcci:

- Protocollo MDM di Apple - Gli amministratori possono caricare solo formati PKG specifici (formato di distribuzione), come le app interne, e può anche distribuire le app dal Mac App Store (il supporto per le licenze App e libri è incluso). Tuttavia, questo approccio non consente agli amministratori di distribuire DMG e altri formati PKG.
- Mobile@Work per app macOS - Come metodo per distribuire le app agli utenti, gli amministratori possono utilizzare l'app MobileIron Packager (MIP) per convertire qualsiasi file PKG, DMG o .app in un file MIP. Caricare il file MIP in Ivanti Neurons for MDM come app in-house.

> È possibile scaricare lo strumento Ivanti Neurons per MDM Mac Packager tramite i download di software MobileIron.

Gli amministratori possono utilizzare Mobile@Work per distribuire le app interne nel formato DMG, PKG o .app. Per le app che sono disponibili solo nel Mac App Store, gli amministratori possono continuare a utilizzare le funzionalità MDM native di Apple, che comprendono le licenze App e libri di Apple.

4.2. Configurazione e utilizzo di messaggi e-mail di conferma della registrazione

Gli amministratori possono configurare e attivare il servizio e-mail per gli utenti che hanno completato la registrazione. I messaggi e-mail possono contenere, ad esempio, istruzioni aggiuntive per gli utenti registrati. Gli amministratori possono abilitare l'invio di questi messaggi e-mail durante gli inviti agli utenti.

Processo:

- **Configurazione della funzionalità:**
  - Configura modello e-mail: per impostazione predefinita, il modello e-mail in inglese è simile a quello riportato di seguito, ma è possibile modificarlo per adattarlo meglio ai propri scopi seguendo le istruzioni fornite nella pagina **Personalizzazione di un modello e-mail** in **Personalizzazione dei modelli e-mail**.

  - Attivare l'invio del messaggio e-mail di conferma della registrazione. Consultare la sezione **Configurazione delle e-mail di conferma della registrazione degli utenti** in **Impostazioni utente**.
- **Utilizzare la funzionalità per:**
  - Inviare all'utente l'invito per la registrazione, come descritto nella sezione **Invio di inviti agli utenti**. Una volta completata la registrazione, Ivanti Neurons for MDM invia all'utente il messaggio e-mail di conferma della registrazione.

4.3. Configurazione e utilizzo di e-mail di notifica sulla conformità delle policy

Gli amministratori possono includere un modello e-mail di notifica sulla conformità delle policy nei messaggi e-mail inviati mediante le azioni di invio e-mail di una policy personalizzata o una policy App consentite agli utenti di dispositivi non conformi. La procedura di configurazione è descritta di seguito:

- **Configurazione della funzionalità:**
  - **Configurare il modello e-mail**.
    Per impostazione predefinita, il modello e-mail in inglese è simile a quello riportato di seguito, ma è possibile modificarlo per adattarlo meglio ai propri scopi seguendo le istruzioni fornite nella pagina **Personalizzazione di un modello e-mail** in **Personalizzazione dei modelli e-mail**:
    
  - **Attivare il modello di notifica sulla conformità delle policy**. Questo modello viene utilizzato insieme al messaggio creato dall'utente mediante le azioni di invio e-mail di una policy personalizzata o una policy App consentite. Ivanti Neurons for MDM inserisce le informazioni specificate nelle azioni e-mail all'interno del modello di notifica sulla conformità delle policy. È possibile attivare il modello e-mail sulla conformità delle policy durante la creazione o la modifica di una policy personalizzata o una policy App consentite. Per ulteriori informazioni sulle istruzioni relative all'abilitazione del modello di notifica sulla conformità delle policy per una policy personalizzata o a una policy App consentite, consultare rispettivamente le sezioni **Aggiunta di una policy personalizzata** e **Creazione di un criterio App consentite**.
- **Utilizzare la funzionalità per:**
  - Se un dispositivo non è conforme a una policy personalizzata o a una policy App consentite con il modello di notifica delle policy abilitato, Ivanti Neurons for MDM invia un messaggio e-mail al proprietario del dispositivo, inserendo prima il messaggio e-mail nel modello di notifica delle policy. L'utente deve solo configurare la funzione come indicato in precedenza, le altre operazioni vengono eseguite automaticamente da Ivanti Neurons for MDM.

4.4. Funzionalità on-demand

Ivanti Neurons per MDM include alcune funzionalità on-demand che sono disattivate per impostazione predefinita. Tali funzionalità potrebbero influire sulle prestazioni e potrebbero non essere completamente pronte per la distribuzione in produzione.

Gli amministratori possono contattare il **Supporto** se desiderano attivare una o più funzionalità on-demand sui propri tenant disattivate per impostazione predefinita.

La tabella seguente include l'elenco delle caratteristiche on-demand documentate:

Funzionalità	Descrizione	Piattaforme	Licenza
Funzionalità per Windows 10	Funzionalità valide per i dispositivi Windows 10.	Windows 10	• Legacy: Gold • Attuale: Secure UEM Vedere **Pacchetti** per ulteriori informazioni sulle offerte legacy e attuali.
Copia dell'URL del Catalogo app negli appunti	Permette agli amministratori di copiare l'URL del Catalogo app negli appunti per le app. È possibile distribuire questo URL agli utenti via e-mail. Se l'utente fa clic sul collegamento da un dispositivo registrato, il Catalogo app con l'app verrà aperto nel browser. Qui l'utente può scegliere di installare l'app. Gli amministratori sono responsabili della limitazione della distribuzione di questo URL agli utenti interessati.	• iOS • macOS	ND (in base a tenant)
Configurare una clip Web come app	Configurare una **clip Web** come un'app nel catalogo app per rendere disponibile l'applicazione Web agli utenti in questo catalogo. La clip Web può essere definita come configurazione, ma le configurazioni possono essere inviate esclusivamente dall'amministratore. Gli utenti possono scegliere di installare l'applicazione Web sui propri dispositivi o disattivarla, mentre non possono disattivare la configurazione di una clip Web.	iOS	ND (in base a tenant)
Attiva registrazione dei dispositivi consentiti	Permettere la registrazione dei dispositivi sulla base dei numeri di serie consentiti in Utenti > **Impostazioni utente** > Impostazione predefinita registrazione del dispositivo.	• iOS • macOS	ND (in base a tenant)
Autenticazione basata su certificati	La funzionalità **Autenticazione basata su certificati** consente agli amministratori di effettuare l'accesso utilizzando certificati digitali e un nome host specificato del tenant o un nome host vanity. Questa impostazione di autenticazione può essere configurata mediante la configurazione vanity host nella scheda **Amministratore**.	Questa funzionalità non è specifica per la piattaforma.	ND (in base a tenant) Questa funzionalità è disponibile solo su ambienti cluster NA3, e solo se abilitata dal supporto.
Creare una configurazione di dispositivi dedicati (monouso di	Gli amministratori possono configurare dispositivi dedicati, che possono essere utilizzati per uno scopo specifico utilizzando Android Enterprise e la configurazione dei dispositivi dedicati (monouso di proprietà dell'azienda o COSU). La **configurazione COSU** viene distribuita ai dispositivi di lavoro gestiti (modalità	Android Enterprise	Silver

Funzionalità	Descrizione	Piattaforme	Licenza
proprietà dell'azienda o COSU)	Proprietario del dispositivo) al fine di mettere una sola app a disposizione degli utenti in modalità tutto schermo.		
Periodo di inattività del dashboard	Per impostazione predefinita, il periodo di inattività del dashboard è impostato su 15 giorni. Ciò può essere aggiornato in base alle esigenze del tenant e per un massimo di 30 giorni. Se si richiede un periodo di inattività più lungo, contattare il team di **Supporto**.	Questa funzionalità non è specifica per la piattaforma.	

4.5. Preparazione per il supporto dei dispositivi Android Enterprise

Questa sezione descrive i requisiti minimi di rete per i dispositivi Android Enterprise. I dispositivi Android generalmente non richiedono l'apertura di porte in entrata sul firewall al fine di funzionare correttamente. Tuttavia, ci sono una serie di connessioni in uscita di cui gli amministratori devono essere consapevoli quando impostano i loro ambienti di rete per i dispositivi Android Enterprise.

L'elenco delle modifiche di rete fornito nella tabella seguente non è esaustivo e può variare. Presenta gli endpoint noti per le versioni attuali e precedenti di app GMS e API di gestione aziendale.

> Oltre alle porte elencate nella seguente tabella, i dispositivi Android Enterprise richiedono l'accesso a Ivanti Neurons per MDM.

Per informazioni sui requisiti dei dispositivi Android Enterprise, vedere **Requisiti di rete Android Enterprise** dalla Guida di Android Enterprise.

Google non fornisce IP specifici, pertanto si dovrebbe consentire al firewall di accettare le connessioni in uscita verso tutti gli indirizzi IP contenuti nei blocchi IP indicati nell'ASN 15169 di Google disponibile all'indirizzo **http://bgp.he.net/AS15169#_prefixes**.

> Gli indirizzi IP dei nodi edge e dei peer Google non sono elencati nei blocchi AS15169. Consultare la pagina **https://peering.google.com/** per ulteriori informazioni su Google Edge Network.

5. Dashboard

Nel dashboard vengono visualizzate delle statistiche importanti sugli utenti e i dispositivi registrati. Ogni sezione del dashboard viene chiamata widget. Per ciascun widget si definisce:

- la categoria dei dati visualizzati (come ad esempio dispositivi o utenti)
- la modalità di raggruppamento dei dati (ad esempio in base alla versione build di sistema operativo o al modello)
- la modalità in cui i dati vengono filtrati (ad esempio se vengono visualizzati soltanto i dispositivi iOS o la versione build sistema operativo)
- la modalità di visualizzazione dei dati (ad esempio come grafico a torta o a barre)

Verifica dei report e altre informazioni

Nel **dashboard** vengono visualizzate informazioni statistiche importanti sugli utenti e i dispositivi registrati. Ogni sezione del dashboard viene chiamata widget.

È possibile verificare ulteriori informazioni come segue:

- **Controllare le notifiche**: andare alla pagina **Dashboard > Notifiche** (o fare clic sull'icona della campana (in alto a destra)) per controllare le notifiche e intraprendere azioni se necessario.
- **Report**: andare alla pagina **Dashboard > Report** per accedere ai dati del proprio sistema Unified Endpoint Management (UEM).
- **Audit trail**: andare alla pagina **Dashboard > Audit Trail** per accedere al set cronologico di record che mostra le attività eseguite su tutte le entità all'interno di Ivanti Neurons for MDM. Per attivare questa funzione, andare alla pagina **Amministratore > Infrastruttura > Audit trail** e fare clic su **Attiva Audit trail**.
- App Insights: andare alla pagina **Dashboard > App Insights** per visualizzare e analizzare la distribuzione di app e altri dettagli delle app.

Argomenti della sezione:

- Utilizzo di widget
- Approfondimenti app
- Utilizzo di report pianificati
- Utilizzo di report personalizzati

5.1. Utilizzo di widget

Argomenti della sezione:

- Aggiunta di un widget
- Organizzazione dei widget
- Modifica di un widget
- Controllo delle notifiche
- Report
- Audit trail

Nel dashboard vengono visualizzate delle statistiche importanti sugli utenti e i dispositivi registrati. Ogni sezione del dashboard viene chiamata widget. Per ciascun widget si definisce:

- la categoria dei dati visualizzati (come ad esempio dispositivi o utenti)
- la modalità di raggruppamento dei dati (ad esempio in base alla versione di sistema operativo o al modello)
- la modalità in cui i dati vengono filtrati (ad esempio se vengono visualizzati soltanto i dispositivi iOS)
- la modalità di visualizzazione dei dati (ad esempio come grafico a torta o a barre)

Aggiunta di un widget

1. Fare clic su **Aggiungi** (in alto a destra).
2. Assegnare un nome al widget.
3. Selezionare una categoria per i dati.
4. Completare le opzioni relative ai filtri in base all'ordine di visualizzazione.
5. Selezionare il tipo di visualizzazione predefinito (grafico a torta, a barre, a linee).
6. Fare clic su **Fine**.

Organizzazione dei widget

I widget vengono sempre visualizzati in tre per ogni riga. Tuttavia, è possibile modificarne l'ordine di visualizzazione:

1. Fare clic su **Disponi** (in alto a destra).
2. Trascinare le caselle nell'ordine in cui si desidera che vengano visualizzati i widget.
3. Fare clic su **OK**.

Modifica di un widget

1. Fare clic sull'icona delle impostazioni del widget (in alto a destra).
2. Selezionare **Modifica**.
3. Apportare le modifiche desiderate.
4. Fare clic su **Fine**.

Controllo delle notifiche

Fare clic sull'icona a forma di campana (in alto a destra) oppure andare alla pagina **Dashboard > Notifiche** per controllare le notifiche e scegliere l'azione necessaria in base ai seguenti criteri:

- Tipo di componente
  - APP
  - LDAP
  - Entra ID
  - Elenco dei dispositivi consentiti
  - App e libri
  - iOS
  - Android
  - macOS
  - visionOS
  - watchOS
  - tvOS
  - Tenant
  - CA
  - Connettore
  - Sentry
  - Token del server Registrazione dispositivi

Tipo di notifica

  - Scadenza
  - Sincronizzazione dati
  - Limite di utilizzo
  - Azione amministrativa
  - Errore di autenticazione del server
  - Errore di convalida
  - Modifica dello stato

Gravità

  - Cancellata
  - Informazioni
  - Critica
  - Avviso

Gli amministratori possono selezionare il componente APP per controllare rapidamente tutte le notifiche relative all'app nella pagina Notifiche, così come nella sezione delle notifiche con l'icona a forma di campana. Se sono presenti nuove autorizzazioni da accettare per le app di Google Play, gli amministratori possono accettarle facendo clic sulle notifiche invece di visitare la pagina di ciascuna app.

> Ivanti Neurons per MDM i clienti/tenant otterranno le notifiche di approvazione dell'applicazione Android Go anche se l'applicazione Android Go non è stata importata nel Catalogo app.

Revisione della scadenza della password per l'utente e notifiche di modifica all'ID

Gli amministratori possono rivedere la prossima scadenza della password nella pagina **Notifiche**. Gli amministratori ricevono notifiche da due settimane a un giorno prima della scadenza delle password, inclusi i collegamenti ai file dei report CSV che contengono l'elenco degli utenti corrispondenti. Dopo la scadenza della password le notifiche non vengono più generate.

Gli amministratori possono inoltre esaminare una notifica con l'elenco degli utenti i cui ID (UID) sono stati modificati durante l'ultima sincronizzazione LDAP.

Cancellazione di una notifica

Ogni volta che è necessario, dalla pagina Notifiche è possibile cancellare manualmente le **notifiche** con qualsiasi livello di gravità.

1. Nella pagina **Notifiche**, fare clic sull'icona nella colonna **Azioni** corrispondente alla notifica che si desidera cancellare. Viene visualizzata la finestra **Conferma cancellazione notifica**.
2. Fare clic su **Cancella notifica**. Dopo la cancellazione, lo stato della notifica cambia in **Cancellata** nella colonna **Stato**.

> Il conteggio totale delle notifiche cancellate viene visualizzato nella pagina **Notifiche**.

Report

Nella pagina **Dashboard > Report** è possibile accedere ai dati del proprio sistema di gestione unificata degli endpoint (UEM). Per esempio, gli amministratori possono aggiungere informazioni come Nome spazio dispositivo e Attributi personalizzati dispositivo ai report utilizzando l'opzione di filtro corrispondente durante la creazione dei report Dispositivi e Dispositivi bloccati. Di conseguenza, questi report includeranno rispettivamente le colonne denominate Nome spazio dispositivo e Attributi personalizzati dei dispositivi. Gli attributi personalizzati dei dispositivi sono disponibili nelle opzioni di filtro durante la creazione di un report. Gli amministratori possono selezionare un'opzione dall'elenco di chiavi degli attributi dei dispositivi personalizzate e selezionare gli operatori disponibili.

A partire da Ivanti Neurons per MDM 76, gli operatori di tutti i modelli di report presentano operatori standard. Gli operatori dei seguenti modelli sono standardizzati in questa versione:

- Dashboard > Report > Crea report

Di seguito è indicato il flusso di lavoro di un report:

1. Scegli: selezionare un modello di report predefinito.
2. Definisci ambito: impostare un intervallo di tempo per i dati del report.
3. Imposta dettagli: assegnare un nome al report e personalizzarlo.
4. Esegui o pianifica: eseguire il report immediatamente o creare una pianificazione.
5. Condividi: specificare i destinatari del report.

Argomenti correlati:

- **Dashboard > Report (pianificati)**
- **Dashboard > Report (personalizzati)**

Ricerca rapida: andare alla scheda Report. Il campo Ricerca rapida consente di effettuare ricerche dalle colonne seguenti, anche se si includono spazi o caratteri speciali:

- NOME
- DESCRIZIONE
- NOME MODELLO

Audit trail

Gli **Audit trail** forniscono un record cronologico delle attività eseguite in Ivanti Neurons per MDM. Questi record includono azioni eseguite da amministratori, utenti finali e componenti di sistema.

Gli amministratori utilizzano gli **Audit trail** per rivedere le modifiche, verificare le azioni, risolvere i problemi e supportare i controlli di conformità. Gli **Audit trail** tracciano azioni come l'aggiunta, l'aggiornamento e l'eliminazione di entità gestite, inclusi i dispositivi. Per ulteriori informazioni, vedere Registrazione del dispositivo (iOS, macOS e Android).

Attivazione della funzionalità Audit trail

È necessario abilitare l'opzione **Audit Trail** per acquisire le attività eseguite all'interno di Ivanti Neurons per MDM.

Procedura

1. Andare in **Amministratore** > **Infrastruttura** > **Audit Trail**.
   Viene visualizzato il riquadro **Audit Trail**.
2. Selezionare e impostare il pulsante di commutazione **Esporta Audit Trail** su ON.

> Non è possibile disattivare la funzionalità Audit Trail dopo averla attivata. Per disabilitarla, contattare il supporto Ivanti.

Visualizzazione degli Audit Trail

Seguire i passaggi per visualizzare ulteriori dettagli sugli **Audit Trail:**

Procedura

1. Andare in **Dashboard** > **Audit Trail**.

Viene visualizzato il riquadro **Audit Trail**.

2. Le seguenti tabelle elencano i dati visualizzati nel riquadro **Audit Trail**:

Impostazione	Descrizione
Icona	Mostra l'icona dell'attività per l'evento di audit.
Attività	Mostra l'azione che si è verificata, come il check-in del dispositivo o l'accesso amministratore.
Stato	Mostra se l'attività è riuscita o non riuscita. Se un report non riesce, è possibile riprovare il processo report dalla **Cronologia report**. Utilizzare questa opzione per rieseguire il processo non riuscito senza creare una nuova pianificazione report.
Eseguito da	Mostra l'amministratore o l'utente che ha eseguito l'attività.
Eseguito alle	Mostra la data e l'ora in cui si è verificata l'attività.
Eseguito il	Mostra il dispositivo, l'account o l'oggetto interessato dall'attività.
Dettagli	Mostra ulteriori informazioni sull'attività.
Tipo	Mostra il tipo di attività, ad esempio Azione dispositivo o Account.
Categoria	Mostra l'area funzionale correlata all'attività, ad esempio Gestione dispositivo o Accesso al portale di amministrazione.

3. Fare clic sul pulsante **Azioni** per eseguire le seguenti opzioni:

- **Configura impostazioni Audit Trail**: selezionare questa opzione per visualizzare la configurazione degli **Audit Trail** in **Amministratore** > **Infrastruttura** > **Audit Trail.**
- **Esporta in CSV**: selezionare questa opzione per esportare e scaricare gli **Audit Trail**.

4. (Facoltativo) È possibile utilizzare i **Filtri** per visualizzare **Audit Trail** specifici.

Visualizzazione dettagli attività

L'icona **Modifiche - Prima e dopo** viene visualizzata nella colonna **Dashboard** > **Audit Trail** > **Dettagli**. Consente di confrontare i valori degli attributi prima e dopo un'azione verificata. Questo confronto rende più semplice l'identificazione di ciò che è cambiato, la verifica dell'attività dell'utente o del sistema e la risoluzione dei problemi di aggiornamento della configurazione.

Fare clic sull'icona per visualizzare i dettagli del confronto dell'Audit Trail nel riquadro **Modifiche Audit Trail - Prima e dopo** e visualizzare i seguenti dati:

Impostazione	Descrizione
Attributo	Mostra il nome dell'attributo modificato. Ad esempio `creato in`.
Prima	Visualizza il valore dell'attributo prima che l'azione sia stata eseguita. Evidenziazioni in colore rosso.
Dopo	Visualizza il valore dell'attributo dopo l'esecuzione dell'azione. Evidenziazioni in colore verde.

Utilizzo di Ricerca avanzata per Audit Trail

Utilizzare l'opzione Ricerca avanzata per cercare gli Audit Trail in base alle regole. Definire criteri specifici per identificare e visualizzare le attività. È possibile utilizzare i seguenti attributi per eseguire la ricerca avanzata:

- **Attività**
- **Categoria**
- **Creato alle**
- **Eseguito da**
- **Eseguito il**
- **Nome spazio**
- **Stato**
- **Tipo**

Creazione di report per Audit Trail

È possibile pianificare l'esecuzione dei report **Audit Trail** ogni 12 ore o 24 ore o generare report personalizzati. Inoltre, è possibile eseguire report **Audit Trail** su richiesta. I report su richiesta non sono pianificati e includono i dati **Audit Trail** delle ultime 24 ore.

È possibile generare un report Audit Trail in uno dei seguenti formati:

- CSV
- JSON
- CEF

Inoltre, durante la creazione di un report per **Audit Trail** > **Distribuzione report**, è possibile selezionare l'opzione **Esporta SFTP** per esportare e caricare tutte le informazioni dell'Audit Trail in una posizione specifica del server. L'esportazione Audit Trail utilizza il protocollo di trasferimento file Secure Shell (SFTP). Il server deve essere accessibile tramite la porta predefinita. È possibile configurare le impostazioni di **Esportazione Audit Trail** per caricare automaticamente gli archivi dell'Audit Trail in una posizione specifica ogni giorno. Per ulteriori informazioni, vedere **Esportazione degli Audit trail**.

Per maggiori informazioni sulla creazione di un report, vedere **Utilizzo di report pianificati** e **Utilizzo di report personalizzati**.

5.2. Approfondimenti app

Argomenti della sezione:

- Visualizzazione della distribuzione delle app
- Visualizzazione dei dettagli delle app
- Aggiunta di grafici di distribuzioni single app
- Aggiunta di un grafico di app iOS non gestite
- Aggiunta delle principali 10 app gestite installate
- Aggiunta delle principali 5 app interne valutate

Approfondimenti app è una funzionalità del Dashboard che aiuta a visualizzare e analizzare la distribuzione delle app seguenti:

- distribuzione di app interne che richiedono l'installazione
- distribuzione di app pubbliche che richiedono l'installazione
- App iOS non gestiste
- Principali 10 app gestite installate
- Migliori 5 app interne

Analisi delle 5 principali app che richiedono l'installazione: si tratta di app interne o pubbliche che sono state distribuite a un alto numero di utenti ma hanno in proporzione tassi di installazione bassi. Il grafico delle app iOS non gestite fornisce informazioni sulle app non gestite sui dispositivi. L'utente avrà la possibilità di vedere l'elenco delle app non gestite, su quali dispositivi sono installate e intraprendere le azioni necessarie per convertire un'app in un'app gestita. Queste sono le distribuzioni di app che richiedono l'attenzione di un amministratore o un'azione per migliorare la distribuzione. Questi grafici rappresentano i dispositivi su cui le app sono già installate. Il grafico a ciambella fornisce una panoramica di alto livello della distribuzione di app interne e pubbliche che non solo aiuta ad analizzare il numero di dispositivi che necessitano l'installazione di app, ma consente anche di eseguire un'analisi più approfondita per ottenere informazioni più specifiche sulle app facendo clic su un'area specifica del grafico. È inoltre possibile aggiungere il grafico di una singola distribuzione che rappresenta la distribuzione specifica per la versione di una singola app.

> Nel dashboard vengono visualizzate solo le informazioni relative ai dispositivi sottoposti a check-in negli ultimi 15 giorni.

Visualizzazione della distribuzione delle app

Nella pagina **App**, in **Dashboard** è possibile visualizzare i seguenti grafici:

- Distribuzione delle app interne che richiedono l'installazione
- Distribuzione delle app pubbliche che richiedono l'installazione
- App iOS non gestiste

I grafici di 5 app interne, 5 app iOS non gestite e pubbliche vengono visualizzati per impostazione predefinita. I grafici sono ordinati da sinistra a destra cominciando con l'app con il tasso di disinstallazione più alto.

Nei grafici a ciambella vengono visualizzati 2 colori che rappresentano lo stato dell'installazione. Il colore blu indica il numero di dispositivi in cui l'app è installata. Il colore rosso indica il numero di dispositivi che richiedono l'installazione. Il conteggio dei dispositivi viene visualizzato se si passa il puntatore del mouse sopra ciascuna area di colore.

È possibile eliminare un grafico facendo clic sull'opzione Elimina nell'angolo in alto a destra del grafico.

Visualizzazione dei dettagli delle app

Nel centro del grafico a ciambella viene visualizzato anche il numero di dispositivi che richiedono l'installazione. Esempio: 750/1000 che significa 750 su 1.000 dispositivi richiedono l'installazione.

Nei grafici a ciambella vengono visualizzati 3 colori che rappresentano la distribuzione dell'app.

- Il colore blu indica il numero di dispositivi in cui l'applicazione è installata. Facendo clic sull'area blu del grafico è possibile spostarsi alla pagina **Dispositivi**. Nella pagina **Dispositivi**, nella colonna **Versione app** viene visualizzata la versione installata e la data di installazione dell'app.

> È inoltre possibile visualizzare i dispositivi in base alle versioni delle app installate, selezionando le opzioni nella sezione **Versioni** del pannello a sinistra.

- Il colore rosso indica il numero di dispositivi che richiedono l'installazione di app. Facendo clic sull'area rossa del grafico è possibile spostarsi alla pagina **Dispositivi**. Nella pagina **Dispositivi**, è possibile visualizzare i dispositivi che richiedono l'installazione di app.

L'icona di un'app viene visualizzata al centro del grafico. Quando si fa clic sull'icona, si naviga fino alla pagina dei dettagli dell'app in **App > App Catalog**.

In questa pagina, fare clic sulla scheda **Dispositivi con app installata** per visualizzare un elenco di dispositivi per l'app selezionata.

Fare clic sulla scheda **Dispositivi senza app installata** per visualizzare un elenco di dispositivi in cui l'app selezionata non è installata.

Aggiunta di grafici di distribuzioni single app

È possibile aggiungere grafici a ciambella di singole distribuzioni per una specifica versione di un'app nella pagina App. Il colore rosso indica l'elenco dei dispositivi idonei che dovrebbero avere l'app installata. Questi grafici rappresentano graficamente i seguenti dettagli della distribuzione di app:

- dispositivi con una specifica versione dell'app installata
- dispositivi con altre versioni dell'app installate
- dispositivi su cui l'app non è installata

Procedura

1. Fare clic su **+Aggiungi** nella pagina **App**. Viene visualizzata la finestra **Aggiungi grafico di app**.
2. Nell'elenco a discesa **Tipo di grafico** selezionare **Distribuzione app singola**.
3. Selezionare la casella di controllo per l'elenco delle app di cui si desidera visualizzare il grafico di distribuzione di app singola.

> In alternativa è possibile cercare un'app specifica digitando il nome dell'app nel campo di ricerca delle app.

4. Fare clic su **Aggiungi grafico**. I grafici di distribuzione di app singole vengono visualizzati nella pagina App.

> È possibile selezionare al massimo 9 app dall'elenco.

Il centro del grafico visualizza il numero di dispositivi su cui è installata la versione specifica dell'app.

Esempio: 5/10 che indica che 5 su 10 dispositivi hanno installata la versione specifica dell'app.

Nei grafici a ciambella vengono visualizzati 3 colori che rappresentano la distribuzione dell'app.

- Il colore verde indica il numero di dispositivi in cui la versione specifica dell'app è installata. Facendo clic sull'area verde del grafico è possibile spostarsi alla pagina **Dispositivi** che mostra l'elenco dei dispositivi su cui è installata la versione specifica dell'app. È possibile anche visualizzare i dispositivi in base alle altre versioni di app installate selezionando le opzioni nella sezione **Versione app** del pannello a sinistra.
- Il colore vere chiaro indica il numero di dispositivi in cui sono installate altre versioni dell'app. Facendo clic sull'area verde del grafico è possibile spostarsi alla pagina **Dispositivi** in cui viene visualizzato l'elenco dei dispositivi in cui sono installate altre versioni dell'app. È possibile anche visualizzare i dispositivi in base alle altre versioni dell'app installate selezionando le opzioni di versione nella sezione **Versione app** nel pannello a sinistra.
- Il colore rosso indica il numero di dispositivi in cui l'app non è installata. Il conteggio dei dispositivi viene visualizzato se si passa il puntatore del mouse sopra ciascuna area di colore. Facendo clic sull'area rossa del grafico è possibile spostarsi alla pagina **Dispositivi** dove è possibile visualizzare i dispositivi su cui l'app non è installata. Nel pannello di sinistra viene visualizzata anche la data da quando l'app è disponibile in App Catalog.

L'icona di un'app viene visualizzata al centro del grafico. Quando si fa clic sull'icona, si naviga fino alla pagina dei dettagli dell'app in **App > App Catalog**. In questa pagina, fare clic sulla scheda **Dispositivi con app installata** per visualizzare un elenco di dispositivi per l'app selezionata. Fare clic sulla scheda **Dispositivi senza app installata** per visualizzare un elenco di dispositivi in cui l'app selezionata non è installata.

È possibile eliminare un grafico facendo clic sull'opzione Elimina nell'angolo in alto a destra del grafico.

Aggiunta di un grafico di app iOS non gestite

È possibile identificare e visualizzare l'elenco delle app non gestite aggiungendo il grafico delle app iOS non gestite nella pagina App. Il grafico viene visualizzato automaticamente quando un amministratore aggiunge un'app iOS non gestita al catalogo. L'amministratore può eliminare o aggiungere questo grafico secondo necessità.

Procedura

1. Fare clic su **+Aggiungi** nella pagina **App**. Viene visualizzata la finestra **Aggiungi grafico di app**.
2. Nell'elenco a discesa **Tipo di grafico** selezionare **App iOS non gestite**.
3. Fare clic su **Aggiungi grafico**. Il grafico delle app iOS non gestite viene visualizzato nella pagina **App**.

Il grafico mostra il numero di app presenti nell'App Catalog che non sono gestite. Nella parte inferiore del grafico vengono visualizzate 3 colonne con i seguenti dettagli:

- **Dispositivi con app iOS non gestite** - Indica il numero di app iOS non gestite. Fare clic sul collegamento per visualizzare l'elenco dei dispositivi con app non gestite nella finestra Dispositivi con app iOS non gestite.
- **Numero totale di app nell'App Catalog** - Mostra il numero totale di app disponibili nell'App Catalog.
- **App iOS non gestite (%)** - Indica le app iOS non gestite in percentuale.

Se un'app è già installata da iTunes App Store, è possibile convertire l'app e i relativi dati in un'app gestita. Per convertire tale app in un'app gestita:

1. Fare clic sul collegamento con numero nella **colonna Dispositivi con app iOS non gestite**. Viene visualizzata la finestra **App iOS non gestite**.
2. Selezionare una o più app non gestite dall'elenco e fare clic sul collegamento al numero sotto App iOS non gestite. Le app selezionate verranno convertite in app gestite e lo stato verrà aggiornato al successivo check-in del dispositivo.

È possibile esportare i dati delle app non gestite in formato CSV facendo clic sul collegamento **Esporta in CSV**.

Aggiunta delle principali 10 app gestite installate

È possibile identificare e visualizzare l'elenco delle principali 10 app gestite installate utilizzando il grafico delle principali 10 app gestite installate nella pagina App. L'amministratore può eliminare o aggiungere questo grafico come e quando richiesto.

Per impostazione predefinita, il grafico delle principali 10 app gestite installate è disponibile nella pagina **App** . Se il grafico viene eliminato, l'amministratore può aggiungerlo dalla pagina **App** .

Procedura

1. Fare clic su **+Aggiungi** nella pagina **App**. Viene visualizzata la finestra **Aggiungi grafico di app**.
2. Nell'elenco a discesa **Tipo di grafico** selezionare **Principali 10 app gestite installate**.
3. Fare clic su **Aggiungi grafico**. Il grafico Principali 10 app gestite installate viene visualizzato nella pagina **App**.

È possibile visualizzare le principali 10 app gestite installate in base alla categoria selezionata sotto l'elenco a discesa **Mostra** . Le categorie disponibili sono:

- **Tutte le app** (selezionata per impostazione predefinita)
- **App interne**
- **App pubbliche**

Ciascuna barra del grafico viene visualizzata per rappresentare ciascuna app specifica e il relativo nome. Passare il puntatore del mouse su ciascuna barra per visualizzare la piattaforma (Android, iOS o Windows) e il numero di dispositivi in cui l'app è installata.

Facendo clic sulla barra di un'app specifica è possibile spostarsi alla pagina **Dispositivi** che mostra i dettagli dei dispositivi in cui l'app è installata. Il pannello di sinistra nella pagina Dispositivi indica il numero di dispositivi in cui l'app è installata. Facendo clic sul pulsante X nel pannello di sinistra è possibile tornare alla pagina **App** del dashboard.

È possibile eliminare un grafico facendo clic sull'opzione Elimina nell'angolo in alto a destra del grafico.

Aggiunta delle principali 5 app interne valutate

È possibile identificare e visualizzare l'elenco delle migliori 5 app interne utilizzando il grafico delle migliori 5 app interne nella pagina App. L'amministratore può eliminare o aggiungere questo grafico come e quando richiesto.

Di default, il grafico delle migliori 5 app interne è disponibile nella pagina **App**. Se il grafico viene eliminato, l'amministratore può aggiungerlo dalla pagina **App** .

Procedura

1. Fare clic su **+Aggiungi** nella pagina **App**. Viene visualizzata la finestra **Aggiungi grafico di app**.
2. Nell'elenco a discesa **Tipo di grafico** selezionare **Migliori 5 app interne**.
3. Fare clic su **Aggiungi grafico**. Il grafico Migliori 5 app interne viene visualizzato nella pagina **App**.

Questo grafico rappresenta i dati con un logo per l'app e le stelle di valutazione. Le stelle di valutazione sono rappresentate con immagini di stelle e la rappresentazione di un numero intero (per un punteggio massimo di 5). Viene visualizzato anche il numero di utenti che hanno votato l'app.

> Il numero di valutazioni per un'app non è limitato ai dispositivi di un determinato amministratore e di una determinata area, ma si basa sulla valutazione di tutti gli utenti dell'app. La valutazione è data dalla media di tutte le valutazioni per quell'app considerati i diversi utenti che hanno visualizzato l'app da Apps@Work sui propri dispositivi registrati.

Per passare alla pagina **Dettagli app** che mostra informazioni specifiche dell'app, fare clic sull'app specifica.

È possibile eliminare un grafico facendo clic sull'opzione Elimina nell'angolo in alto a destra del grafico.

5.3. Utilizzo di report pianificati

Licenza: Silver

La funzionalità Report pianificati consente di pianificare e generare report basati su diverse metriche con modelli predefiniti pronti all'uso. Per accedere a questa funzionalità è necessario disporre del ruolo di Amministratore di sistema o Sistema di sola lettura. Attualmente è possibile creare un massimo di 40 report.

> Il report sulle violazioni delle policy può contenere più record per lo stesso dispositivo, se per quest'ultimo sono state create più istanze di Tunnel. Questo vale sia per i report standard che per quelli personalizzati.

Generazione di un report

È possibile pianificare e generare un report.

Procedura

1. Andare in **Dashboard** > **Report**.
2. Fare clic su **Crea un report** per visualizzare la pagina Scegli un modello di report.
3. Scegliere un modello di report dalle opzioni configurate.
   - **Dispositivi bloccati**: segnala i dispositivi attualmente bloccati da Sentry.
   - **Dispositivi**: segnala i dispositivi di tutte le partizioni del sistema.
   - **Violazioni dei criteri**: segnala le violazioni dei criteri nel sistema.
   - **Utenti**: segnala gli utenti del sistema
   - **Stato scadenza password utente**: segnala lo stato di scadenza della password degli utenti del sistema.
   - **App più installate**: segnala tutte le applicazioni presenti nel sistema, ordinate in base al numero di volte in cui ciascuna applicazione è stata installata.
   - **App non gestite**: segnala le applicazioni non gestite nel sistema.
   - **Tutte le applicazioni**: segnala tutte le applicazioni nei dispositivi gestiti dall'utente.
   - **Audit trail**: segnala tutte le attività svolte su tutte le entità all'interno di Ivanti Neurons for MDM.
4. Fare clic su **Avanti**.
   Viene visualizzata la pagina **Dettagli report**.
   - Immettere un **nome per il report**.
   - (Facoltativo) Immettere una **descrizione** per il report.

Selezionare l'**Intervallo eventi** dalle opzioni seguenti:
Per i report esistenti:

- **Tutti gli eventi**
- **Giorno precedente**
- **Settimana precedente**
- **Mese precedente**
- **Intervallo precedente** - Visualizza il report creato utilizzando il cursore dell'intervallo dalla release precedente del portale amministrativo Ivanti Neurons per MDM. Se l'amministratore seleziona e salva una delle opzioni di cui sopra per un report,

l'opzione Intervallo precedente non verrà visualizzata. Il valore dell'intervallo è visibile nella pagina di riepilogo del report.

Per i nuovi report:

- **Tutti gli eventi**
- **Giorno precedente**
- **Settimana precedente**
- **Mese precedente**

Fare clic su **Avanti**. Viene visualizzata la pagina Dati report.

6. Fare clic su **Personalizza colonne** per aggiungere, rimuovere o riordinare le colonne nella sezione **Colonne report**. In alternativa, fare clic sul nome della colonna per rimuovere la colonna aggiunta.
7. (Facoltativo) Utilizzare la casella di controllo **Seleziona tutte le colonne** per selezionare tutte le colonne visualizzate nell'elenco.
8. Fare clic su **Ripristina valori predefiniti** per ripristinare le colonne generate in precedenza. Per ripristinare le colonne senza applicare personalizzazioni, è possibile scegliere uno dei modelli dalla pagina **Scegli un modello di report**.
9. Creare filtri basati su regole specifiche nella sezione **Filtro avanzato**.

> Non tutte le opzioni di filtro sono disponibili per tutti i report. Per ulteriori informazioni sull'elenco dei filtri disponibili, consultare l'argomento **Filtri** sotto questa procedura.

> Durante la creazione dei report sono disponibili i seguenti nuovi attributi hardware per i dispositivi Windows: crittografia BitLocker, edizione del sistema operativo, versione del sistema, produttore della scheda madre, prodotto della scheda madre, stato della scheda madre, produttore del BIOS, versione del BIOS, partizioni del disco rigido, tipo di unità ottica, nome della CPU e stato della CPU.

10. (Opzionale) fare clic sull'icona **+** per aggiungere un'altra regola o fare clic sull'icona **Aggiungi gruppo** per aggiungere un altro gruppo di regole.
11. Fare clic su **Avanti**. Viene visualizzata la pagina Pianificazione report.
12. Per scaricare il report, selezionare *uno* dei seguenti formati:
    - CSV
    - PDF
    - **CSV e PDF**
      Per i file di report in formato PDF sono consentite al massimo 10 colonne. Nella sezione Grafici report vengono mostrati i due tipi di grafici inclusi nei report in PDF.
      Il report Tutte le applicazioni supporta solo il formato CSV.

Fare clic su **Pianificazione automatica** per impostare l'esecuzione automatica di un report impostando la ricorrenza. In alternativa, fare clic su **Manuale** per eseguire il report una volta e inviarlo via e-mail.

- Selezionare *una* delle opzioni **Report ricorrente**:
  - **Quotidiano**
  - **Settimanale**
  - **Mensile**
  - **Schema precedente** - Per i report esistenti

- Selezionare la **Data di inizio** e la **Data di fine** (opzionale).

14. Fare clic su **Avanti**. Viene visualizzata la pagina Distribuzione report. Selezionare i destinatari del report.
15. (Facoltativo) aggiungere ID e-mail esterni facendo clic sul link **Aggiungi e-mail esterna** .
16. Fare clic su **Fine**. Viene visualizzata la schermata **RiepilogoDistribuzione report**.
17. (Opzionale) fare clic su **Modifica** per modificare il proprio report.
18. Fare clic su **Salva**.
19. Fare clic sull'icona Download per selezionare il formato del report. Un'e-mail contenente un pulsante **Scarica report** per scaricare il report viene inviata ai destinatari del report.

Filtri

Opzioni regole	Descrizione
Blocco attivazione abilitato	Regole basate sul blocco di attivazione abilitato come **Sì** o **No**. Esempio di regola: "Blocco di attivazione abilitato è uguale a Sì".
Stato Tunnel app	Regola per stato Tunnel app come **BLOCCA** o **CONSENTI**. Esempio di regola: "Stato Tunnel app è uguale a Blocca".
Livello batteria	Valore del livello della batteria del dispositivo. Esempio di regola: "Livello batteria è uguale a 1080". Il valore specificato per il livello della batteria deve essere espresso in secondi.
Ultimo check-in del client	Regola basata sull'ultimo check-in del client entro l'intervallo di date. Esempio di regola: "L'ultimo check-in del client è compreso nell'intervallo 04/02/2019 06:00:00,04/05/2019 17:00:00".
Stato di conformità	Regola basata sullo stato di conformità come **Sì** o **No**. Esempio di regola: "Lo stato di conformità è uguale a Sì".
Nome paese attuale	Inserire il nome del paese attuale. Esempio di regola: "Lo stato di conformità è uguale a Francia".
MCC attuale	Regola basata sul Mobile Country Code (MCC) attuale. Esempio di regola: "MCC attuale è uguale a 410".
MNC attuale	Regola basata sul Mobile Network Code (MNC) attuale. Esempio di regola: "MNC attuale è uguale a 06".
Registrazione dispositivi abilitato	Regola basata su Registrazione dispositivi abilitato come **Sì** o **No**. Esempio di regola: "Registrazione dispositivi abilitato corrisponde a Sì"
Stato nativo anti-phishing	Selezionare una delle seguenti opzioni di Stato nativo anti-phishing: • è uguale a • non è uguale a I valori possibili sono: • Non abilitato • N/A • Attivato • Sconosciuto
Stato VPN anti-phishing	Selezionare una delle seguenti opzioni di Stato VPN anti-phishing: • è uguale a • non è uguale a I valori possibili sono: • Non abilitato • N/A • Attivato

Opzioni regole	Descrizione
	• Sconosciuto
Registrato in Registrazione dispositivi	Regola basata su Registrato in Registrazione dispositivi come **Sì** o **No**. Esempio di regola: "Registrato in Registrazione dispositivi corrisponde a Sì"
Protezione dati	Indica se sul dispositivo è abilitata la protezione dati. I valori possibili sono **Sì** e **No**. Esempio di regola: "Protezione dati è uguale a Sì".
Roaming dati attivato	Regola basata sul roaming dati abilitato come **Sì** o **No**. Esempio di regola: "Roaming dati abilitato è uguale a Sì"
Stato di blocco del dispositivo	Regola basata sullo stato di blocco del dispositivo. Esempio di regola: "Stato di blocco del dispositivo è uguale a Blocca".
ID dispositivo	Regola per un ID dispositivo specifico o all'interno di una serie di ID dispositivo. Esempio di regola: "L'ID dispositivo è maggiore di 45". X
MCC nazionale	Regola basata sul Mobile Country Code (MCC) nazionale. Esempio di regola: "MCC nazionale è uguale a 310".
MNC nazionale	Regola basata sul Mobile Network Code (MNC) nazionale. Esempio di regola: "MNC nazionale è uguale a 510".
IMEI	Regola per un valore IMEI specifico. Esempio di regola: "Il valore IMEI inizia con 9900"
Stato di invito	Selezionare una delle seguenti opzioni di Stato di invito: • Nessuno • In sospeso • Scaduto • **Completato** Esempio di regola: "Lo stato di invito è uguale a In sospeso".
Servizio di localizzazione abilitato	Regola basata sul Servizio di localizzazione abilitato come **Sì** o **No**. Esempio di regola: "Servizio di localizzazione abilitato è uguale a Sì"
Stato attivazione MTD	Selezionare una delle seguenti opzioni di Stato di attivazione MTD: • è uguale a • non è uguale a I valori possibili sono: • N/A • Errore • In sospeso • Protetto
Stato di quarantena	Regola basata sul Servizio di localizzazione abilitato come **Sì** o **No**. Esempio di regola: "Stato di quarantena è uguale a Sì".

Opzioni regole	Descrizione
Registrato alle	Regola per selezionare l'intervallo di data e ora da quando il dispositivo è stato registrato. Esempio di regola: "Registrato alle è compreso nell'intervallo 10/03/2017 09:00:00,10/20/2017 17:00:00".
Roaming	Regola basata sul roaming come **Sì** o **No**. Esempio di regola: "Roaming è uguale a Sì"
Stato	Selezionare una delle seguenti opzioni di Stato di invito: • Attivo • Disattiva gli elementi in sospeso • Disattiva gli elementi inviati • Disattivato • Disattiva gli elementi annullati • Cancella gli elementi in sospeso • Cancella gli elementi inviati • Cancellato • Cancella gli elementi annullati Esempio di regola: "Lo stato è uguale a Disattiva gli elementi in sospeso".
Chiamate in roaming abilitate	Regola basata sulle chiamate in roaming abilitate come **Sì** o **No**. Esempio di regola: "Chiamate in roaming abilitate è uguale a Sì"
Indirizzo Mac Wi-Fi	Inserire un valore di indirizzo Mac specifico. Esempio di regola: "L'indirizzo Mac Wifi non è uguale a 00-14-22-01-23-45".
Backup su iCloud abilitato	Regola basata su Backup su iCloud abilitato come **Sì** o **No**. Esempio di regola: "Backup su iCloud abilitato è uguale a Sì".
Stato attivazione dell'account iTunes Store	Regola basata sullo Stato attivazione dell'account iTunes come **Sì** o **No**. Esempio di regola: "Stato attivazione dell'account iTunes non è uguale a No".
Tipo di piattaforma	Applicabile al report per tutte le applicazioni.
Origine	Applicabile al report per tutte le applicazioni.
Attributi personalizzati	Applicabile al report per tutte le applicazioni.
Gestito	Applicabile a tutte le applicazioni e al report sulle applicazioni più utilizzate.
Identificatore app	È predefinito per il report Tutte le applicazioni.
Meid	Applicabile al report sulle applicazioni non gestite.

Esecuzione di azioni su un report dalla pagina Report pianificati

È possibile eseguire varie azioni dalla pagina Report pianificati.

Procedura

1. Andare in **Dashboard** > **Report**.
2. Nella pagina **I miei report pianificati**, fare clic sul menu a discesa **Azioni** e selezionare una delle seguenti opzioni:

Opzioni di Azioni	Azione eseguita
Vista	Consente di visualizzare il report.
Modifica	Consente di modificare il report. Il report consente anche di visualizzare l'intervallo selezionato nell'ultima versione come Intervallo precedente.
Esegui ora	Esegue il report.
Scarica CSV	Consente di scaricare il report in formato CSV.
Scarica PDF	Scarica il report in formato PDF.
Elimina	Consente di eliminare il report.

Visualizzazione dei dettagli del report

È possibile visualizzare i dettagli del report ed eseguire alcune azioni sul report creato.

Procedura

1. Andare in **Dashboard** > **Report**.
2. Nella pagina **I miei report pianificati**, fare clic sul nome del report per visualizzare i dettagli del report. Si apre la pagina Report.
3. In questa pagina è possibile visualizzare il riepilogo e la cronologia dei report.

Argomenti correlati:

- Per assegnare un ruolo personalizzato a un utente, vedere **Assegnazione di ruoli**.
- Vedere **Ruoli utente** per un elenco dei ruoli predefiniti.
- **Gestione dei ruoli**
- **Utilizzo di report personalizzati**

5.4. Utilizzo di report personalizzati

Licenza: Gold

La funzionalità Report personalizzati consente di personalizzare e generare report basati su diverse metriche con modelli pronti all'uso. Per accedere a questa funzionalità è necessario disporre del ruolo di Amministratore di sistema o Sistema di sola lettura. Attualmente è possibile creare un massimo di 40 report.

Argomenti della sezione:

[Generazione di un report]

[Esecuzione di azioni su un report]

[Visualizzazione dei dettagli del report]

Generazione di un report

È possibile pianificare e generare un report dal portale amministrativo Ivanti Neurons per MDM.

Procedura

1. Andare in **Dashboard** > **Report**.
2. Fare clic su **Crea un report** per visualizzare la pagina Scegli un modello di report.
3. Scegliere un modello di report dalle opzioni configurate.
   - **Dispositivi bloccati**: segnala i dispositivi attualmente bloccati da Sentry.
   - **Dispositivi**: segnala i dispositivi di tutte le partizioni del sistema.
   - **Violazioni dei criteri**: segnala le violazioni dei criteri nel sistema.
   - **Utenti**: segnala gli utenti del sistema
   - **Stato scadenza password utente**: segnala lo stato di scadenza della password degli utenti del sistema.
   - **App più installate**: segnala tutte le applicazioni presenti nel sistema, ordinate in base al numero di volte in cui ciascuna applicazione è stata installata.
   - **App non gestite**: segnala le applicazioni non gestite nel sistema.
   - **Tutte le applicazioni**: segnala tutte le applicazioni nei dispositivi gestiti dall'utente.
   - **Audit trail**: segnala tutte le attività svolte su tutte le entità all'interno di Ivanti Neurons for MDM.
4. Fare clic su **Avanti**. Viene visualizzata la pagina Dettagli report.
5. Immettere un **nome per il report**.
6. (Facoltativo) Immettere una **descrizione** per il report.
7. Selezionare l'**Intervallo eventi** dalle opzioni seguenti:
   Per i report esistenti:
   - **Tutti gli eventi**
   - **Giorno precedente**
   - **Settimana precedente**
   - **Mese precedente**

- **Intervallo precedente** - Visualizza il report creato utilizzando il cursore dell'intervallo dalla release precedente del portale amministrativo Ivanti Neurons per MDM. Se l'amministratore seleziona e salva una delle opzioni di cui sopra per un report, l'opzione Intervallo precedente non verrà visualizzata. Il valore dell'intervallo è visibile nella pagina di riepilogo del report.

Per i nuovi report:

- **Tutti gli eventi**
- **Giorno precedente**
- **Settimana precedente**
- **Mese precedente**

Fare clic su **Avanti**. Viene visualizzata la pagina Dati report.

9. Fare clic su **Personalizza** per generare un report personalizzato:

> Nella pagina **Dashboard > Report** la colonna Nome modello visualizza "personalizzato" tra parentesi per indicare che il report è personalizzato.

10. Fare clic su **Personalizza colonne** per aggiungere, rimuovere o riordinare le colonne nella sezione **Colonne report**. In alternativa, fare clic sul nome della colonna per rimuovere la colonna aggiunta.
11. (Facoltativo) Utilizzare la casella di controllo **Seleziona tutte le colonne** per selezionare tutte le colonne visualizzate nell'elenco.
12. Fare clic su **Ripristina valori predefiniti** per ripristinare le colonne generate in precedenza. Per ripristinare le colonne senza applicare personalizzazioni, è possibile scegliere uno dei modelli dalla pagina **Scegli un modello di report**. Le colonne predefinite sono indicate con un'icona a forma di lucchetto.
13. Creare filtri basati su regole specifiche nella sezione **Filtro avanzato**.

> Non tutte le opzioni di filtro sono disponibili per tutti i report. Per ulteriori informazioni sull'elenco dei filtri disponibili, consultare l'argomento **Filtri** sotto questa procedura.

> Durante la creazione dei report sono disponibili i seguenti nuovi attributi hardware per i dispositivi Windows: crittografia BitLocker, edizione del sistema operativo, versione del sistema, produttore della scheda madre, prodotto della scheda madre, stato della scheda madre, produttore del BIOS, versione del BIOS, partizioni del disco rigido, tipo di unità ottica, nome della CPU e stato della CPU.

14. (Opzionale) fare clic sull'icona **+** per aggiungere un'altra regola o fare clic sull'icona **Aggiungi gruppo** per aggiungere un altro gruppo di regole.
15. Fare clic su **Avanti**. Viene visualizzata la pagina Pianificazione report.
16. Per scaricare il report, selezionare *uno* dei seguenti formati:
    - **CSV**
    - **PDF**
    - **CSV e PDF**
      Per i file di report in formato PDF sono consentite al massimo 10 colonne. Nella sezione Grafici report vengono mostrati i due tipi di grafici inclusi nei report in PDF.
      Il report Tutte le applicazioni supporta solo il formato CSV.

Fare clic su **Pianificazione automatica** per impostare l'esecuzione automatica di un report impostando la ricorrenza. In alternativa, fare clic su **Manuale** per eseguire il report una volta e inviarlo via e-mail.

- Selezionare *una* delle opzioni **Report ricorrente**:
  - **Quotidiano**
  - **Settimanale**
  - **Mensile**
  - **Schema precedente** - Per i report esistenti
- Selezionare la **Data di inizio** e la **Data di fine** (opzionale).

> L'opzione Esegui ora genera un report unico. È possibile utilizzare lo stesso modello per generare report pianificati. Nella pagina **Dashboard > Report**, verrà mostrato lo stato Non pianificato per questi report nelle colonne Frequenza e Prossima pianificazione.

18. Fare clic su **Avanti**. Viene visualizzata la pagina Distribuzione report. Selezionare i destinatari del report.
19. (Facoltativo) aggiungere ID e-mail esterni facendo clic sul link **Aggiungi e-mail esterna** .
20. Fare clic su **Fine**. Viene visualizzata la schermata **RiepilogoDistribuzione report**.
21. (Opzionale) fare clic su **Modifica** per modificare il proprio report.
22. Fare clic su **Salva**.
23. Fare clic sull'icona Download per selezionare il formato del report. Un'e-mail contenente un pulsante **Scarica report** per scaricare il report viene inviata ai destinatari del report.

Filtri

Opzioni regole	Descrizione
Blocco attivazione abilitato	Regole basate sul blocco di attivazione abilitato come **Sì** o **No**. Esempio di regola: "Blocco di attivazione abilitato è uguale a Sì".
Stato Tunnel app	Regola per stato Tunnel app come **BLOCCA** o **CONSENTI**. Esempio di regola: "Stato Tunnel app è uguale a Blocca".
Livello batteria	Valore del livello della batteria del dispositivo. Esempio di regola: "Livello batteria è uguale a 1080". Il valore specificato per il livello della batteria deve essere espresso in secondi.
Ultimo check-in del client	Regola basata sull'ultimo check-in del client entro l'intervallo di date. Esempio di regola: "L'ultimo check-in del client è compreso nell'intervallo 04/02/2019 06:00:00,04/05/2019 17:00:00".
Stato di conformità	Regola basata sullo stato di conformità come **Sì** o **No**. Esempio di regola: "Lo stato di conformità è uguale a Sì".
Nome paese attuale	Inserire il nome del paese attuale. Esempio di regola: "Lo stato di conformità è uguale a Francia".
MCC attuale	Regola basata sul Mobile Country Code (MCC) attuale. Esempio di regola: "MCC attuale è uguale a 410".
MNC attuale	Regola basata sul Mobile Network Code (MNC) attuale. Esempio di regola: "MNC attuale è uguale a 06".
Registrazione dispositivi abilitato	Regola basata su Registrazione dispositivi abilitato come **Sì** o **No**. Esempio di regola: "Registrazione dispositivi abilitato corrisponde a Sì"
Stato nativo anti-phishing	Selezionare una delle seguenti opzioni di Stato nativo anti-phishing: • è uguale a • non è uguale a I valori possibili sono: • Non abilitato • N/A • Attivato • Sconosciuto
Stato VPN anti-phishing	Selezionare una delle seguenti opzioni di Stato VPN anti-phishing: • è uguale a • non è uguale a I valori possibili sono: • Non abilitato • N/A • Attivato

Opzioni regole	Descrizione
	• Sconosciuto
Registrato in Registrazione dispositivi	Regola basata su Registrato in Registrazione dispositivi come **Sì** o **No**. Esempio di regola: "Registrato in Registrazione dispositivi corrisponde a Sì"
Protezione dati	Indica se sul dispositivo è abilitata la protezione dati. I valori possibili sono **Sì** e **No**. Esempio di regola: "Protezione dati è uguale a Sì".
Roaming dati attivato	Regola basata sul roaming dati abilitato come **Sì** o **No**. Esempio di regola: "Roaming dati abilitato è uguale a Sì"
Stato di blocco del dispositivo	Regola basata sullo stato di blocco del dispositivo. Esempio di regola: "Stato di blocco del dispositivo è uguale a Blocca".
ID dispositivo	Regola per un ID dispositivo specifico o all'interno di una serie di ID dispositivo. Esempio di regola: "L'ID dispositivo è maggiore di 45". X
MCC nazionale	Regola basata sul Mobile Country Code (MCC) nazionale. Esempio di regola: 'MCC nazionale è uguale a 310'.
MNC nazionale	Regola basata sul Mobile Network Code (MNC) nazionale. Esempio di regola: "MNC nazionale è uguale a 510".
IMEI	Regola per un valore IMEI specifico. Esempio di regola: "Il valore IMEI inizia con 9900"
Stato di invito	Selezionare una delle seguenti opzioni di Stato di invito: • Nessuno • In sospeso • Scaduto • **Completato** Esempio di regola: "Lo stato di invito è uguale a In sospeso".
Servizio di localizzazione abilitato	Regola basata sul Servizio di localizzazione abilitato come **Sì** o **No**. Esempio di regola: "Servizio di localizzazione abilitato è uguale a Sì"
Stato attivazione MTD	Selezionare una delle seguenti opzioni di Stato di attivazione MTD: • è uguale a • non è uguale a I valori possibili sono: • N/A • Errore • In sospeso • Protetto
Stato di quarantena	Regola basata sul Servizio di localizzazione abilitato come **Sì** o **No**. Esempio di regola: "Stato di quarantena è uguale a Sì".

Opzioni regole	Descrizione
Registrato alle	Regola per selezionare l'intervallo di data e ora da quando il dispositivo è stato registrato. Esempio di regola: "Registrato alle è compreso nell'intervallo 10/03/2017 09:00:00,10/20/2017 17:00:00".
Roaming	Regola basata sul roaming come **Sì** o **No**. Esempio di regola: "Roaming è uguale a Sì"
Stato	Selezionare una delle seguenti opzioni di Stato di invito: • Attivo • Disattiva gli elementi in sospeso • Disattiva gli elementi inviati • Disattivato • Disattiva gli elementi annullati • Cancella gli elementi in sospeso • Cancella gli elementi inviati • Cancellato • Cancella gli elementi annullati Esempio di regola: "Lo stato è uguale a Disattiva gli elementi in sospeso".
Chiamate in roaming abilitate	Regola basata sulle chiamate in roaming abilitate come **Sì** o **No**. Esempio di regola: "Chiamate in roaming abilitate è uguale a Sì"
Indirizzo Mac Wi-Fi	Inserire un valore di indirizzo Mac specifico. Esempio di regola: "L'indirizzo Mac Wifi non è uguale a 00-14-22-01-23-45".
Backup su iCloud abilitato	Regola basata su Backup su iCloud abilitato come **Sì** o **No**. Esempio di regola: "Backup su iCloud abilitato è uguale a Sì".
Stato attivazione dell'account iTunes Store	Regola basata sullo Stato attivazione dell'account iTunes come **Sì** o **No**. Esempio di regola: "Stato attivazione dell'account iTunes non è uguale a No".
Tipo di piattaforma	Applicabile al report per tutte le applicazioni.
Origine	Applicabile al report per tutte le applicazioni.
Attributi personalizzati	Applicabile al report per tutte le applicazioni.
Gestito	Applicabile a tutte le applicazioni e al report sulle applicazioni più utilizzate.
Identificatore app	È predefinito per il report Tutte le applicazioni.
Meid	Applicabile al report sulle applicazioni non gestite.

Esecuzione di azioni su un report

È possibile eseguire varie azioni dalla pagina Report pianificati.

Procedura

1. Andare in **Dashboard** > **Report**.
2. Nella pagina **I miei report pianificati**, fare clic sul menu a discesa **Azioni** e selezionare una delle seguenti opzioni:

Opzioni di Azioni	Azione eseguita
Vista	Consente di visualizzare il report.
Modifica	Consente di modificare il report.
Esegui ora	Esegue il report.
Scarica CSV	Consente di scaricare il report in formato CSV.
Scarica PDF	Scarica il report in formato PDF.
Elimina	Consente di eliminare il report.

Visualizzazione dei dettagli del report

È possibile visualizzare i dettagli del report ed eseguire alcune azioni sul report creato.

Procedura

1. Andare in **Dashboard** > **Report**.
2. Nella pagina **I miei report pianificati**, fare clic sul nome del report per visualizzare i dettagli del report. Si apre la pagina Report.
3. Selezionare una delle seguenti opzioni

Opzioni di Azioni	Azione eseguita
Attiva/disattiva	Consente di abilitare o disabilitare il report.
Esegui ora	Esegue il report.
Vista	Consente di visualizzare i dettagli del report. Utilizzare il menu a discesa Azioni per eseguire una delle seguenti attività: • **Disattiva** • **Scarica CSV/PDF più recente** (in base al tipo di report selezionato può essere CSV, PDF o CSV e PDF, mostra l'opzione Download) • **Cronologia** • **Elimina**
Elimina	Consente di eliminare il report.

Argomenti correlati:

- Per assegnare un ruolo personalizzato a un utente, vedere **Assegnazione di ruoli**.

- Vedere **Ruoli utente** per un elenco dei ruoli predefiniti.
- **Gestione dei ruoli**
- **Utilizzo di report pianificati**

6. Utenti

Prima di invitare un utente a registrare i dispositivi mobili, è necessario creare una relativa voce utente. È inoltre necessario creare un utente per chiunque debba utilizzare Ivanti Neurons for MDM per gestire i dispositivi o pubblicare contenuti (amministratori).

Argomenti della sezione:

- **Gruppi di utenti**
- **Impostazioni utente**
- **Personalizzazione degli utenti**
- **Registrazione utenti con Apple Business Manager**
- **Registrazione degli utenti basata su account**
- **Licenze utente**
- **Gestione degli utenti**

6.1. Aggiunta di utenti

Argomenti della sezione:

- Aggiunta di utenti
- Aggiunta di più utenti
- Aggiunta di più utenti caricando un file
- Aggiunta di un amministratore
- Utente Nessuno
- Visualizzazione delle informazioni del PIN di registrazione dispositivi

È possibile aggiungere un singolo utente o più utenti contemporaneamente. Dopo aver aggiunto più utenti, è consigliabile filtrare la visualizzazione in modo che vengano visualizzati soltanto gli utenti a cui si è interessati.

Tra le altre operazioni che è possibile svolgere con gli utenti in questa pagina, sono incluse le attività seguenti:

- assegnazione a/ rimozione da un gruppo di utenti
- invio di messaggi
- invito alla registrazione
- assegnazione di ruoli
- modifica password
- elimina
- genera un pin

Tutti i profili Proprietario del dispositivo vengono assegnati a un account dispositivo. Non esistono limitazioni per il numero di dispositivi che possono essere assegnati a un account dispositivo. I profili di lavoro (di proprietà del dipendente) vengono assegnati agli account utente.

Aggiunta di utenti

Procedura

1. Andare a **Utenti**.
2. Fare clic su **+ Aggiungi** (in alto a destra).
3. Selezionare **Utente unico**.
4. Compilare il modulo con le informazioni sull'utente:
    - Indirizzo e-mail (obbligatorio)
    - Nome
    - Cognome

> Nel campo Nome utente viene visualizzato l'indirizzo e-mail immesso. Nella maggior parte dei casi si sconsiglia di modificare questa impostazione predefinita. Per ulteriori informazioni, consultare la sezione Quando modificare un nome utente.

    - Nome visualizzato

> Se si desidera cambiare il nome visualizzato dell'utente, modificare il testo predefinito nel campo **Nome visualizzato**.

5. Se si desidera assegnare una password, immetterla nei campi **Password** e **Conferma password**.
    - Se viene assegnata una password, è necessario comunicarla all'utente per la registrazione del dispositivo.
    - Se non si assegna una password, l'utente dovrà crearne una durante la registrazione del dispositivo.
6. Selezionare **Impostazioni locali** dall'elenco a discesa.
7. Immettere l'**ID Apple gestito**. È possibile includere "appleid" come sottodominio per l'ID Apple gestito allo scopo di evitare conflitti con ID Apple esistenti. Ad esempio, utente@appleid.propriodominio.com. Il sottodominio deve essere valido e verificato su Apple Business Manager.

> L'account non può essere aggiornato con un ID Apple gestito diverso, se è presente un dispositivo Registrazione utenti attivo con l'ID Apple gestito dell'account corrente.

(Opzionale) Assegnare uno o più gruppi di utenti. L'ID Apple gestito non può essere aggiornato quando è presente un dispositivo con lo stato "Attivo" e "Dismissione in sospeso".

10. Se si desidera configurare altre funzioni prima di invitare l'utente, deselezionare l'opzione **Invia invito ora**. Altrimenti, l'e-mail di invito verrà inviata dopo aver fatto clic su **Fine**.
11. Fare clic su **Fine** per aggiungere l'utente.

Per i dispositivi Android, gli account dei dispositivi sono progettati per i dispositivi monouso gestiti in cui un singolo account di servizio locale può essere utilizzato per registrare un alto numero di dispositivi. Durante la creazione di un nuovo utente, deve essere abilitato l'Account dispositivo aziendale Android disponibile in **Amministratore > Google > Android Enterprise**. Gli account dispositivo sono abilitati per impostazione predefinita (invece degli account utente) per le registrazioni di account Google Play gestiti dal proprietario del dispositivo.

Selezionare la casella di controllo **Account dispositivi Android enterprise** per consentire che alle registrazioni di dispositivi gestiti dal lavoro Android Enterprise collegati a questo account venga assegnato automaticamente un account dispositivo Google.

Durante la modifica di un utente locale o LDAP per i dispositivi Android, ai dispositivi Account Google Play gestito dal proprietario del dispositivo aziendale Android verranno assegnati gli account dispositivo al successivo check-in del dispositivo, purché siano soddisfatte le seguenti condizioni:

- Viene abilitata la funzione selezionando la casella di controllo **Account dispositivi Android enterprise**.
- La versione dell'app Go del dispositivo Android è 47 o successiva.

Aggiunta di più utenti

Procedura:

1. Andare a **Utenti**.
2. Fare clic su **+ Aggiungi** (in alto a destra).
3. Selezionare **Utenti multipli**.
4. Per impostazione predefinita, è possibile inserire gli indirizzi e-mail **Manualmente**. Digitare o incollare gli indirizzi e-mail degli utenti, separati da virgole.
5. Esempio: jdoe@lamiaazienda.com, jsmith@lamiaazienda.com, tjones@lamiaazienda.com
   Se si desidera configurare altre funzioni prima di invitare l'utente, deselezionare l'opzione **Invia invito ora**.

6. Altrimenti, l'e-mail di invito verrà inviata dopo aver fatto clic su **Fine**.
   Fare clic su **Fine** per aggiungere gli utenti.

Aggiunta di più utenti caricando un file

Procedura:

1. Andare a **Utenti**.
2. Fare clic su **+ Aggiungi** (in alto a destra).
3. Selezionare **Utenti multipli**.
4. Selezionare **Carica CSV**.
5. Fare clic su **Scarica modello CSV**.
6. Modificare il modello con le seguenti informazioni per ciascun utente:
   - ID utente (obbligatorio)
   - Indirizzo e-mail (obbligatorio)
   - Password
   - Nome
   - cognome
   - nome visualizzato
   - gruppi di utenti
   - attributi personalizzati
7. Si tratta delle stesse informazioni da immettere quando si **aggiunge un singolo utente**. Il file non può contenere più di 10.000 voci.
   Salvare il file.
8. Trascinare il file nell'area di caricamento o selezionare **Carica CSV** e scegliere il file.
9. Una volta che le informazioni caricate sono visibili, apportare le modifiche desiderate.
10. Fare clic su **Avanti** (in basso a destra).
11. Se non si desidera inviare subito degli inviti, selezionare **Non inviare inviti**.
12. Fare clic su **Fine**.

Aggiunta di un amministratore

Procedura:

1. Fare clic su **Aggiungi** (in alto a destra).
2. Selezionare **Utente unico**.
3. Compilare il modulo con le informazioni sull'utente:
   - Indirizzo e-mail
   - Nome
   - Cognome
4. Nel campo **Nome utente** viene visualizzato l'indirizzo e-mail immesso.
   Se si desidera cambiare il nome visualizzato dell'utente, modificare il testo predefinito nel campo **Nome visualizzato**.

5. Assegnare una password nel campo **Password**.
6. Immettere nuovamente la password nel campo **Conferma password**.
7. Fare clic su **Fine** per aggiungere l'utente.
8. Comunicare la password all'utente di supporto per la gestione dei dispositivi.

Utente Nessuno

L'utente nessuno è un utente predefinito che non è possibile eliminare. Il servizio applica questo utente a dispositivi senza utenti associati come i dispositivi ritirati.

Visualizzazione delle informazioni del PIN di registrazione dispositivi

Se l'opzione Tipo di autenticazione della registrazione dispositivi è impostata su Solo PIN, durante l'aggiunta di nuovi utenti vengono mostrate agli amministratori le informazioni sul PIN di registrazione generato. Queste informazioni possono essere utili per assistere gli utenti nella registrazione dei dispositivi.

- In caso di singoli utenti, il PIN viene mostrato mediante l'azione **Utenti > Invita l'utente a effettuare la registrazione** oppure nella sezione Informazioni PIN della pagina Dettagli utente.
- In caso di più utenti, i PIN vengono mostrati in una colonna nella pagina Elenco utenti, insieme alle colonne Stato PIN (Valido o Scaduto), PIN emesso, e Scadenza PIN.

Se non è possibile eseguire le attività indicate nella pagina **Utenti**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione sistemi
- Gestione utenti

6.2. Gruppi di utenti

Argomenti della sezione:

- Creazione di un gruppo di utenti gestito dinamicamente
- Creazione di un gruppo di utenti gestito manualmente
- Creazione di un gruppo di utenti da uno dei gruppi di utenti duplicati
- Creazione di un gruppo di utenti tramite caricamento di un file CSV

Creare un gruppo di utenti per assegnare app e ruoli a più utenti. Ad esempio, è possibile creare un gruppo Manager se si desidera che tutti i manager dei reparti siano gli amministratori delle app e del contenuto.

È possibile creare un gruppo di utenti da gestire in uno dei modi seguenti:

- **Gestione dinamica (Più comune):** gli utenti locali e LDAP vengono aggiunti/rimossi dinamicamente a/da un gruppo in base a determinate regole e/o attributi.
- **Gestione manuale (Scopo limitato):** consente di aggiungere/rimuovere manualmente gli utenti a/da un gruppo. I gruppi gestiti manualmente sono consigliati unicamente per scopi di testing che richiedono meno autorizzazioni.

È possibile immettere del testo nel campo di **ricerca** per visualizzare un elenco di tutti i gruppi di utenti i cui nomi iniziano con il testo immesso.

- I risultati della ricerca vengono visualizzati in tempo reale durante l'immissione del testo, come elenco delle possibili corrispondenze.
- Selezionare il nome del gruppo di utenti desiderato dall'elenco delle possibili corrispondenze, per eseguire l'azione successiva.
- Il confronto eseguito dalla funzione di ricerca rileva la distinzione tra maiuscole e minuscole.

Creazione di un gruppo di utenti gestito dinamicamente

> La seguente procedura non è applicabile ai Gruppi di utenti dinamici.

Procedura

1. Fare clic su **+Aggiungi**.
2. Immettere un nome per il gruppo di utenti nel campo **Nome**.
3. (Facoltativo) Fare clic su **Aggiungi descrizione** per aggiungere una descrizione del gruppo di utenti.
4. Fare clic sull'opzione **Gestione dinamica (Più comune)**.
5. Impostare regole e/o attributi in base ai propri requisiti. Di seguito sono indicate le opzioni delle regole disponibili:
    - Attributo LDAP personalizzato
        - msExchPoliciesIncluded
        - msExchMailboxGrid
        - mailNickname

    Attributo LDAP predefinito

        - samAccountName

- userPrincipalName

Attributo utente predefinito

- email_address
- distinguished_name
- last_name
- display_name
- first_name
- Gruppo di utenti
- Attributo utente personalizzato

DN gruppo di utenti

- GUID gruppo di utenti
- Nome gruppo di utenti

6. Per ciascuna regola, scegliere tra utenti locali e LDAP. È possibile includere o escludere un sottogruppo utilizzando i criteri del filtro **Gruppo di utenti**.
7. Aggiungere altre regole facendo clic sull'icona più (+).
   È possibile impostare i filtri condizionali **QUALUNQUE** o **TUTTI** per le regole aggiunte.
8. Creare un gruppo di regole facendo clic sull'icona della gerarchia accanto all'icona più (+).
9. Controllare le regole e gli attributi del gruppo di utenti nella query di testo sotto le opzioni di selezione delle regole.
10. Nella sezione **Risultati**, verificare i dettagli degli utenti che corrispondono ai criteri configurati. Quando si aggiunge o si modifica una regola o un attributo, è possibile osservare che gli utenti corrispondenti sono visualizzati, se esistono.
11. Fare clic su **Salva** per salvare il gruppo di utenti configurato.

Creazione di un gruppo di utenti gestito manualmente

1. Fare clic su **+Aggiungi**.
2. Immettere un nome gruppo.
3. (Facoltativo) Fare clic su **Aggiungi descrizione** per aggiungere una descrizione.
4. Selezionare l'opzione **Gestione manuale (Scopo limitato)**.
5. Nel campo **Cerca utenti**, digitare l'indirizzo e-mail di ciascun utente da includere nel gruppo.
   Mentre si digita, gli utenti corrispondenti vengono individuati e visualizzati, se esistono.
6. Selezionare gli utenti che si desidera aggiungere al gruppo. È possibile cercare e aggiungere altri utenti, come richiesto.
7. Fare clic su **Salva**.

> È possibile creare un gruppo di utenti gestito manualmente e aggiungerlo poi a un gruppo di utenti gestito dinamicamente. In questo scenario, la modifica del gruppo di utenti gestito manualmente non infrange la regola del gruppo di utenti gestito dinamicamente. Non sarà possibile eliminare un gruppo di utenti gestito manualmente se è stato aggiunto a un gruppo di utenti gestito dinamicamente.

Creazione di un gruppo di utenti da uno dei gruppi di utenti duplicati

A partire da Neurons for MDM 127, il portale amministratore visualizza il numero di gruppi di utenti duplicati e il numero corrispondente di GUID per identificare gruppi duplicati quando si seleziona l'attributo "Nome gruppo di utenti" nel Generatore di regole. Inoltre, una tabella sotto questa regola visualizza l'elenco di gruppi di utenti duplicati e i relativi dettagli, ad esempio Nome gruppo di utenti, GUID, Origine e Nome distinto (DN).

Procedura

1. Accedere al portale amministratore di Ivanti Neurons for MDM.
2. Andare a **Utenti**, **Gruppi di utenti**.
3. Fare clic su **+Aggiungi**. Viene aperta la procedura guidata Crea gruppo di utenti.
    1. Specificare il nome nel campo **Nome**.
    2. Selezionare **Nome gruppo utenti** nel Generatore di regole, selezionare **è uguale a**, quindi selezionare *uno* dei nomi gruppo duplicati.
    3. Fare clic sull'icona del segno più **+** per aggiungere più regole.
    4. Selezionare **GUID gruppo utenti**, **è uguale a**.
    5. Copiare e incollare il GUID nella tabella che visualizza l'elenco di nomi di gruppi di utenti duplicati e GUID. Il risultato visualizza gli utenti associati che verranno aggiunti al nuovo gruppo.
    6. Fare clic su **Salva**. Gli utenti indicati ora vengono aggiunti al nuovo gruppo di utenti creato.

Se non è possibile eseguire le attività indicate nella pagina **Gruppi di utenti**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione sistemi
- Gestione utenti

Creazione di un gruppo di utenti tramite caricamento di un file CSV

La nuova funzione consente agli amministratori di creare gruppi di utenti e di aggiungere utenti ai gruppi creati utilizzando un file CSV.

Procedura

1. Accedere al portale amministratore di Ivanti Neurons for MDM.
2. Andare a **Utenti**, **Gruppi di utenti**.
3. Fare clic su **+Aggiungi**.
4. Selezionare **Importa gruppi di utenti da CSV**. Viene aperta la procedura guidata Importa gruppo di utenti.
    1. Nella sezione Scarica CSV fare clic su **Scarica modello CSV** per scaricare il modello CSV. Utilizzando il modello, è possibile modificare il file per creare gruppi di utenti e aggiungere gli utenti ai gruppi di utenti nuovi/esistenti.
    2. Dopo aver modificato e salvato il file CSV, fare clic su **Scegliere un file** per caricare il file CSV.
    3. Fare clic su **Carica**. Viene visualizzato un messaggio di conferma relativo alla riuscita del caricamento.

Proprietà	Descrizione
Limitazione delle dimensioni del file CSV	La dimensione massima del file CSV per l'importazione è limitata a 2 MB.
Requisiti del formato file CSV	I file CSV devono contenere esattamente 2 colonne: accountUid e groupName. • Entrambi i valori accountUid e groupName sono obbligatori. • I record che non soddisfano questi criteri saranno scartati durante l'importazione. Gli amministratori possono scaricare un file CSV di esempio dalla sezione Importazione come riferimento.
Gestione degli errori durante l'importazione	Se durante l'importazione di CSV si verificano errori o malfunzionamenti, viene generato un file di errore. • Gli amministratori possono scaricare questo file di errore per esaminare le righe CSV non riuscite e capire le ragioni della mancata riuscita. • Il file di errore include la riga CSV specifica che non è riuscita e fornisce una spiegazione dell'errore.
Condizioni per l'importazione riuscita	L'importazione di utenti in gruppi di utenti ha successo solo se il gruppo di utenti è locale e gestito manualmente. • L'utente deve esistere nel sistema perché l'importazione vada a buon fine.

Condizioni per la creazione di un gruppo di utenti e l'aggiunta di un utente con un file CSV di esempio

Esempio di file CSV dettagliato

accountUid: test_user_1@org.com

groupName: test_group_1

Condizioni	Descrizione
Gruppo esistente	Se il gruppo test_group_1 esiste già, l'utente test_user_1@org.com sarà associato al gruppo.
Gruppo non esistente	Se il gruppo test_group_1 non esiste, verrà creato un nuovo gruppo con il nome test_group_1 e l'utente test_user_1@org.com verrà associato al gruppo.
Gruppo non locale	Se il gruppo test_group_1 esiste ma non è un gruppo locale, questo record verrà incluso nel file CSV degli errori con il motivo "Il gruppo non è locale".
Gruppo non gestito manualmente	Se il gruppo test_group_1 esiste ma non è un gruppo gestito manualmente, questo record verrà incluso nel file CSV degli errori con il motivo "Il gruppo non è gestito manualmente".
Utente non esistente	Se l'utente test_user_1@org.com non esiste, questo record verrà incluso nel file CSV degli errori con il motivo "Utente non trovato".
Utente e gruppo non esistente	Se l'utente test_user_1@org.com e il gruppo test_group_1 non esistono, verrà creato un nuovo gruppo con il nome test_group_1 e questo record verrà incluso nel file CSV degli errori con il motivo "Utente non trovato".

6.3. Impostazioni utente

Argomenti della sezione:

- Modifica delle impostazioni predefinite
- Aggiunta di un'impostazione personalizzata
- Eliminazione di un'impostazione personalizzata
- Configurazione delle impostazioni per la registrazione di nuovi dispositivi
- Configurazione del limite di dispositivi per utente
- Configurazione del limite di cancellazione dei dispositivi
- Impostazioni utente
- Configurazione dell'autenticazione al portale self-service
- Impostazione della complessità della password
- Definizione delle condizioni per l'utilizzo del servizio
- Configurazione delle e-mail di promemoria per gli inviti degli utenti
- Configurazione delle e-mail di conferma della registrazione degli utenti
- Configurazione dell'impostazione Pianificazione lavoro utente
- Configurazione delle impostazioni di autenticazione del portale Amministratori

Su Impostazioni utente è possibile definire le opzioni di registrazione del dispositivo. Sono disponibili diverse opzioni:

- **Impostazione registrazione dispositivo**: imposta l'autenticazione tramite password, PIN o entrambi; il tipo di registrazione Apple e la proprietà del dispositivo.
    - Nelle versioni precedenti, se si imposta Autenticazione SAML/IdP, l'autenticazione SAML viene utilizzata sia per la registrazione del dispositivo che per l'autenticazione nel portale.
    - **Impostazioni registrazione dispositivi della piattaforma** - Gli amministratori possono ora controllare la registrazione dei dispositivi a livello di sistema operativo limitando la registrazione di specifiche piattaforme Apple, Android e Windows al sistema. Questa nuova impostazione di restrizione a livello di sistema operativo viene applicata come controllo di registrazione padre e, quando è attivata per una piattaforma, le restrizioni di registrazione correlate per tale piattaforma vengono disabilitate in automatico. Ciò aiuta le aziende a far rispettare i criteri di registrazione e a impedire la registrazione delle piattaforme del dispositivo non supportate.

Impostazione limite dispositivi: imposta un numero massimo di dispositivi che un utente può registrare.

- **Impostazione limite di cancellazione**: imposta il limite per il numero massimo di dispositivi che possono essere eliminati alla volta.
- **Impostazione Autenticazione al portale self-service:** impostare il tipo di autenticazione password per il portale self-service.
- **Impostazione complessità password**: impostare la complessità della password e i parametri di policy per gli account locali utilizzati per la registrazione dei dispositivi, oltre che per l'accesso al portale Amministratori e ai portali self-service.
- **Impostazione termini di servizio**: imposta i termini di servizio visualizzati all'utente per ogni registrazione di un dispositivo.
- **Impostazione promemoria invito utente:** consente di impostare le date e la frequenza di invio delle e-mail di promemoria invito utente.

- **Impostazione conferma registrazione utente:** consente di impostare l'invio di un messaggio e-mail di conferma della registrazione utente. Vedere la sezione **Configurazione e utilizzo di messaggi e-mail di conferma della registrazione** per una panoramica della soluzione e la sezione **Configurazione delle e-mail di conferma della registrazione degli utenti** di seguito per le istruzioni relative a specifiche impostazioni utente.
- **Impostazione Pianificazione lavoro utente**: controlla la possibilità di configurare una pianificazione di lavoro utente che blocca tutte le comunicazioni da Sentry, per i dispositivi gestiti, durante le ore non lavorative stabilite. Utile per i paesi che prevedono leggi per il "diritto alla disconnessione".
- **Impostazione Autenticazione al portale Amministratori:** determina se Ivanti Neurons for MDM deve richiedere all'amministratore solamente la password oppure la password e il PIN.

È possibile modificare le impostazioni predefinite per il gruppo **Tutti gli utenti** o aggiungere impostazioni personalizzate e assegnarle ad altri gruppi utente.

Modifica delle impostazioni predefinite

Fare clic sul collegamento **Modifica** per l'impostazione con l'icona a forma di lucchetto. Non è possibile eliminare un'impostazione predefinita.

Aggiunta di un'impostazione personalizzata

Fare clic sul collegamento **Aggiungi impostazione per specifici gruppi utente**.

Eliminazione di un'impostazione personalizzata

Fare clic sull'icona X.

Configurazione delle impostazioni per la registrazione di nuovi dispositivi

Per registrare nuovi dispositivi, è possibile configurare la proprietà del dispositivo, il tipo di autenticazione e la versione minima del sistema operativo. L'URL di registrazione del dispositivo generato nelle versioni precedenti di Ivanti Neurons for MDM non funziona con la versione corrente. L'amministratore dovrà rigenerare l'URL di registrazione del dispositivo per registrarlo.

Registrazione dispositivo Allowlist

L'opzione per la registrazione dei dispositivi dei produttori consentiti non è disponibile per le impostazioni utente personalizzate, ma solo nelle impostazioni utente predefinite. Utilizzando il modello, è possibile caricare un file CSV contenente i numeri di serie e gli attributi personalizzati del dispositivo, da utilizzare per inserire alcuni dispositivi nell'elenco degli elementi consentiti. Per creare l'elenco degli elementi consentiti è possibile includere uno o più attributi personalizzati del dispositivo. Questo permetterà di assegnare gli attributi a spazi o a gruppi di dispositivi dopo la registrazione.

Per creare attributi personalizzati, andare a **Amministrazione > Attributi**. Se la funzionalità Elenco dispositivi consentiti è attivata e il numero di serie del dispositivo non è incluso nel file CSV, i dispositivi iOS e macOS non possono essere registrati tramite iReg. Se il file CSV contiene un numero di serie duplicato, per l'assegnazione del dispositivo durante la fase di registrazione vengono considerati l'ultima voce nel file CSV e gli attributi personalizzati del dispositivo associati a questa voce.

Se l'opzione **Allowlist dispositivi** è attivata, solo i dispositivi presenti in elenco saranno autorizzati a registrarsi con Ivanti Neurons per MDM. Questa funzione è applicabile solo ai dispositivi che si registrano tramite la procedura di registrazione via web. Questo non influisce sui dispositivi già registrati su Ivanti Neurons per MDM. Dopo la registrazione, se il numero di serie del dispositivo viene rimosso dal file CSV, il dispositivo non verrà dismesso. L'utente menzionato nel file CSV è opzionale e verrà assegnato solo se è un utente valido.

Se si desidera caricare un nuovo file CSV, è possibile eliminare quello esistente e caricarne uno nuovo. L'utilizzo degli elenchi di dispositivi consentiti è supportato solo con iReg. Se è necessario il client Go, scegliere la registrazione zero-touch. Per il corretto funzionamento di funzioni come AppConnect e Threat Defense, il client Go deve essere installato sul sistema. Poiché la registrazione in-app non è supportata, l'utente può registrare prima il dispositivo tramite iReg. In seguito, l'app Go può essere inviata ai dispositivi dall'App Catalog. Quando l'utente accetta l'installazione dell'app, il dispositivo diventa un dispositivo gestito e tutte le funzioni continueranno a funzionare dopo la registrazione. Impossibile utilizzare la configurazione Zero-touch su dispositivi in cui lo stato di AppConnect è Attivo o Inattivo. Può essere utilizzata solo quando lo stato di AppConnect è Nessuno. Lo stato di AppConnect rimane impostato su Nessuno finché non viene avviato il client Go sul dispositivo dopo la registrazione con iReg.

Procedura

1. Accedere a Ivanti Neurons per MDM.
2. Andare in **Utenti** > **Impostazioni utenti**.
3. Sotto **Impostazioni di registrazione del dispositivo** fare clic su **+Aggiungi impostazione per gruppi di utenti specifici**.
4. Modificare l'impostazione predefinita **Tipo di autenticazione della registrazione dispositivi** o aggiungerne una nuova.
5. Inserire un nome nel campo **Nome**.
6. (Opzionale) Inserire una descrizione dell'impostazione.
7. Nella sezione **Impostazioni del sistema operativo**, definire la versione minima del sistema operativo per iOS, macOS e Windows:
8. Selezionare il pulsante di attivazione/disattivazione **Abilita versione minima**, quindi selezionare una versione del sistema operativo dall'elenco a discesa.

> L'impostazione Abilita versione minima non è applicabile alle registrazioni dei dispositivi DEP.

Per **Android**:

- Abilitare l'opzione **Livello di patch di sicurezza minimo** (solo Android) e specificare il periodo selezionando il tipo di durata tra le seguenti opzioni dell'elenco a discesa:
  - **giorno/i**
  - **mese/i**
  - **anno/i**

  Abilitare l'opzione **Produttori consentiti/non consentiti** e selezionare una delle opzioni seguenti:
  - **Crea elenco di produttori consentiti**: se si desidera consentire la registrazione solo per i dispositivi dei produttori specificati.
  - **Crea elenco di produttori non consentiti**: per impedire la registrazione dei dispositivi dei produttori specificati.
    Per aggiungere un produttore:
    1. Fare clic su **Aggiungi produttore**.
    2. Immettere il nome del produttore nel campo **Nome produttore**.
    3. Fare clic su **Salva**. Il nome del produttore aggiunto viene visualizzato nella tabella.

    > Il nome del produttore effettua la distinzione tra lettere maiuscole e minuscole. Per modificare o eliminare il nome del produttore aggiunto, fare clic sull'opzione **Modifica** o **Elimina** relativa al produttore.

Nella sezione Registrazione Apple, selezionare il tipo di registrazione Apple:

- **Registrazione dispositivo**
- **Registrazione utenti**: per impostazione predefinita, Registrazione utenti è applicabile a dispositivi iOS e iPadOS.
- (Facoltativo) **Includi dispositivo macOS (macOS 10.15+)**: selezionare questa opzione per consentire l'applicazione di Registrazione utenti anche ai dispositivi macOS.

Nella sezione **Metodo di invito alla registrazione (solo iOS e Android)**, abilitare **Registrazione Solo MAM**.

> Questa opzione deve essere abilitata per le registrazioni di dispositivi Solo MAM, dopodiché gli utenti vengono reindirizzati all'App Store pubblico per scaricare l'app client AppStation.

11. Nella sezione **Tipo di autenticazione per la registrazione del dispositivo**, selezionare una delle seguenti opzioni di tipo di registrazione dal menu a discesa **Seleziona tipo di registrazione**. Se si utilizza Registrazione dispositivo, assicurarsi che la configurazione di Registrazione dispositivo corrisponda alla scelta effettuata.
    - **Solo password**
    - **Solo PIN** Quando si seleziona questa opzione, il pulsante di attivazione/disattivazione Ignora autenticazione registrazione dispositivo IdP è bloccato.
    - **Password e PIN**

      > Gli utenti possono comunque ricevere un PIN per completare l'attivazione dell'account.

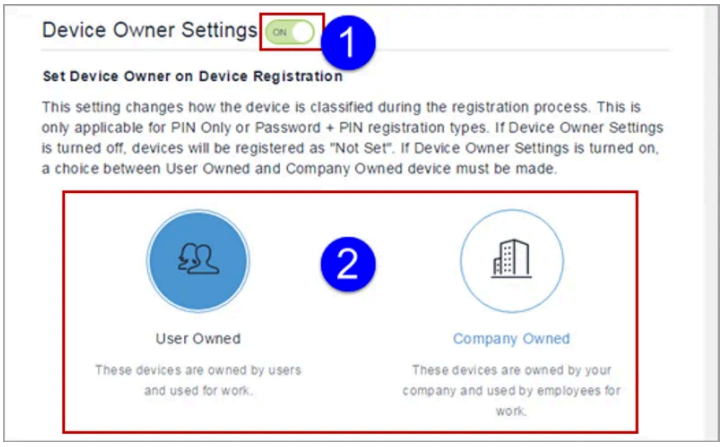
> Questa impostazione interessa sia la registrazione normale, sia la registrazione Registrazione dispositivi.

Per i PIN, specificare quanto segue. Durante la registrazione di un dispositivo, l'utente può fare clic su **Reinvia PIN**, se necessario.

- **Durata PIN**: periodo di validità del PIN (1-30 giorni).
- **Lunghezza PIN**: il numero di caratteri (4-12).
- **Consenti a utenti di richiedere nuovo PIN**: in caso di dimenticanza o dopo la scadenza.

Facoltativamente, attivare **Impostazioni del proprietario del dispositivo**, quindi fare clic su **Di proprietà dell'utente** o **Di proprietà dell'azienda**. Questa impostazione modifica il modo in cui il dispositivo viene classificato durante il processo di registrazione.

- Se **Impostazioni del proprietario del dispositivo** è attivato e l'amministratore ha contrassegnato il dispositivo come Di proprietà dell'utente, all'utente verrà presentata l'opzione di contrassegnare il dispositivo come Di proprietà dell'utente o Di proprietà dell'azienda durante la registrazione e anche dal portale self-service. Per i dispositivi registrati in User Enrolled, l'impostazione predefinita del proprietario del dispositivo sarà "Di proprietà dell'utente" a prescindere dalla scelta fatta dall'amministratore.
- Per i dispositivi supervisionati, l'opzione Impostazioni del proprietario del dispositivo sarà "Di proprietà dell'azienda."



Fare clic su **+Aggiungi** per almeno un gruppo utente al quale si desidera distribuire l'impostazione.

15. (Funzionalità on-demand solo per dispositivi iOS e macOS) Facoltativamente, attivare l'opzione **Elenco dispositivi consentiti** per consentire la registrazione dei dispositivi in base ai numeri di serie consentiti.
16. Fare clic su **Avanti**. Si apre la pagina Distribuzione impostazione utente.
17. Selezionare la distribuzione del gruppo di utenti.
18. Fare clic su **Fine**.
19. Inviare un invito agli utenti. Per ulteriori informazioni, vedere Invio di inviti agli utenti.

Tenere presenti i seguenti punti:

> Se un dispositivo utente è registrato utilizzando l'opzione solo PIN, l'utente riceve un'e-mail di conferma della registrazione con un PIN per l'autenticazione.

- Viene inviato un PIN all'ID e-mail dell'utente.
- L'utente immette il PIN nella pagina di registrazione del dispositivo.
- Se il PIN è corretto, l'utente viene indirizzato a completare il processo di registrazione.

Per gli utenti configurati con un provider di identità (IdP) basato su SAML, Ivanti Neurons per MDM supporta l'autenticazione basata su PIN durante la registrazione del dispositivo. L'opzione Tipo di autenticazione per registrazione dispositivi deve essere impostata su PIN o PIN e password. La funzione PIN e password agisce come autenticazione a due fattori per una maggiore sicurezza. In questo caso, quando un utente cerca di registrare un dispositivo:

- Viene inviato un PIN all'ID e-mail dell'utente.
- L'utente immette il PIN nella pagina di registrazione del dispositivo.
- Se il PIN è corretto, l'utente viene reindirizzato alla pagina di accesso dell'IdP, in cui l'utente immette il nome utente e la password per l'IdP.
- Se le credenziali dell'IdP sono corrette, l'utente viene reindirizzato al dispositivo per completare il processo di registrazione.

Configurazione del limite di dispositivi per utente

Procedura

1. Modificare l'impostazione predefinita **Limite dispositivi** o aggiungerne una nuova.

2. (Facoltativo) Fare clic su **+ Aggiungi impostazione per gruppi di utenti specifici** per configurare il limite del dispositivo per gruppi di utenti specifici.
3. Modificare o assegnare un nome per identificare l'impostazione.
4. Inserire una descrizione facoltativa dell'impostazione.
5. Dal menu a discesa **Numero massimo di dispositivi attivi**, selezionare il limite di dispositivi Apple attivi.
6. Dal menu a discesa **Numero massimo di dispositivi Apple watchOS da associare a un iPhone**, selezionare il limite di dispositivi Apple watchOS attivi da associare all'iPhone.
7. (Facoltativo) Se è selezionato **+ Aggiungi impostazione per gruppi di utenti specifici**, fare clic su **Avanti** e selezionare almeno un gruppo di utenti per la distribuzione di questa impostazione.
8. Fare clic su **Fine**.

Configurazione del limite di cancellazione dei dispositivi

Procedura

1. Modificare l'impostazione predefinita **Limite di cancellazione dei dati dei dispositivi**.
2. Attivare l'opzione **Abilita limite di cancellazione dei dati per tutti gli utenti (inclusi ruoli predefiniti)**.
3. Nel campo **Numero massimo di dispositivi che un utente può cancellare contemporaneamente**, digitare il numero massimo dei dispositivi che possono essere cancellati contemporaneamente. Il valore predefinito è 1. È possibile impostare un valore massimo di 200 come limite di cancellazione dei dispositivi.
4. Fare clic su **Fine**.

Configurazione dell'autenticazione al portale self-service

Procedura

1. Per modificare l'impostazione predefinita **Autenticazione al portale self-service** o aggiungere una nuova, fare clic su **+ Aggiungi impostazioni per gruppi specifici di utente**.
2. Modificare o assegnare un nome per identificare l'impostazione.
3. Inserire una descrizione facoltativa dell'impostazione.
4. Selezionare una voce dall'elenco a discesa **Tipo di autenticazione al portale self-service**. Sono disponibili le opzioni seguenti:
   - Password
   - Certificato
5. Fare clic su **Avanti**.
6. Selezionare uno o più gruppi per cui verrà distribuita questa configurazione.
7. Fare clic su **Fine**.

Impostazione della complessità della password

È possibile impostare la complessità della password e i parametri di policy per gli account locali utilizzati per la registrazione dispositivi, nonché per accedere al portale Amministratori e ai portali self-service.

> La lunghezza, le caratteristiche e le policy per la password impostate di seguito definiscono la sicurezza di una password.

Inoltre definiscono la difficoltà che può incontrare l'utente nel selezionare una password valida. Se si utilizza un account locale per gli utenti finali e si desidera disporre di password sicure per l'accesso al portale Amministratori, valutare la possibilità di utilizzare un PIN per la registrazione dei dispositivi, per garantire che la complessità della password non interferisca con la registrazione del dispositivo. Utilizzare l'impostazione "Tipo di autenticazione per registrazione dispositivi" per selezionare la modalità di autenticazione per la registrazione del dispositivo in **Impostazioni utente > Impostazione registrazione del dispositivo**.

Procedura

1. Modificare le impostazioni predefinite **Complessità password**.
2. Definire le seguenti impostazioni della complessità della password:

Impostazione	Operazione da eseguire
Lunghezza minima della password	Spostare il cursore per specificare la lunghezza minima di una password per impedire agli utenti di creare password corte e non sicure. Il numero è compreso tra 8 e 32.
Caratteristiche richieste	Specificare il numero di caratteristiche della password da soddisfare quando gli utenti selezionano una password. Il numero minimo di caratteristiche che devono essere soddisfatte è 3 (4 per i clienti federali).
Caratteri speciali richiesti (simboli)	Specificare il numero di caratteri non alfanumerici che una password deve contenere.
Caratteri maiuscoli richiesti	Specificare il numero di caratteri alfabetici maiuscoli che una password deve contenere.
Caratteri minuscoli richiesti	Specificare il numero di caratteri alfanumerici minuscoli che una password deve contenere.
Caratteri numerici richiesti	Specificare il numero di caratteri numerici che una password deve contenere.
Convalide delle password	
Sequenza numerica consentita	Selezionare il numero di numeri ripetuti in una sequenza. Esempio: 123.
Caratteri ripetuti consentiti	Selezionare il numero di caratteri alfabetici ripetuti. Esempio: bbc.

3. Configurare la seguente impostazione di policy delle password per personalizzare il comportamento.

Impostazione	Operazione da eseguire
Cronologia password conservate	Spostare il cursore per selezionare il numero di nuove password che devono essere associate a un account utente prima di poter utilizzare una vecchia password. Il numero è compreso tra 3 e 36.
Periodo di scadenza password	Spostare il cursore per selezionare la durata della scadenza della password in giorni. Il numero è compreso tra 30 e 365 giorni.
Timeout di inattività	Spostare il cursore per specificare il periodo di tempo per cui un utente può rimanere inattivo prima che si verifichi un timeout della sessione di un portale Amministratori o self-service. Il numero varia da 5 a 60 (minuti).
Soglia di accessi non riusciti	Spostare il cursore per selezionare il numero di tentativi di accesso non riusciti prima che il blocco di 5 minuti dell'account abbia effetto. Il numero è compreso tra 2 e 5. Quando i tentativi falliti sono entro il valore limite, viene visualizzato un messaggio per l'utente che informa del blocco e di tentare l'accesso più tardi. Quando i tentativi falliti superano il valore limite, viene visualizzato un messaggio per l'utente che informa del blocco e di tentare l'accesso dopo un periodo di tempo specificato (in minuti).

4. Fare clic su **Fine**. Se si è cambiata l'impostazione predefinita della complessità della password, la password precedente dell'account locale esistente rimane invariata. Alla scadenza, all'utente verrà richiesto di rinnovare la password. Gli amministratori che tentano di accedere al portale Amministratori possono contattare l'Help Desk che potrà fornire assistenza per la reimpostazione della password.

> Per la registrazione di un dispositivo, l'approccio consigliato è quello di utilizzare modalità di registrazione con solo PIN.

Definizione delle condizioni per l'utilizzo del servizio

Procedura

1. Creare una nuova impostazione delle **Condizioni per l'utilizzo del servizio**.
2. Assegnare un nome per identificare l'impostazione.
3. Inserire una descrizione facoltativa dell'impostazione.
4. Selezionare **Chiedere all'utente**... .
5. Inserire un titolo e un testo da visualizzare.
6. Fare clic su **+Aggiungi** per almeno un gruppo utente al quale si desidera distribuire l'impostazione.
7. Fare clic su **Salva**.

> Una volta accettati, i termini del servizio non possono essere eliminati. Tuttavia, è possibile disattivare le richieste di nuova registrazione deselezionando l'opzione **Chiedere all'utente**... .

Configurazione delle e-mail di promemoria per gli inviti degli utenti

Gli amministratori possono promuovere le registrazioni dei dispositivi utilizzando questa impostazione per inviare e-mail di promemoria invito utente.

Procedura

1. Modificare un'**Impostazione promemoria invito utente** esistente o aggiungerne una nuova.
2. Modificare o assegnare un nome per identificare l'impostazione.
3. Inserire una descrizione facoltativa dell'impostazione.
4. Assicurarsi che l'opzione **Promemoria invito utente** sia attivata.
5. Nella regione Definisci date di inizio e di fine, scegliere le date di inizio e interruzione dell'invio di e-mail di promemoria.

> Il numero massimo di e-mail che possono essere inviate è 30. Per reimpostare questo limite, l'amministratore deve inviare nuovamente l'invito.

6. Nella regione Definisci frequenza, scegliere la frequenza con cui inviare le e-mail di promemoria.
7. Fare clic su **Avanti**.
8. Selezionare una distribuzione per la configurazione.
9. Fare clic su **Fine**.

Configurazione delle e-mail di conferma della registrazione degli utenti

Gli amministratori possono inviare messaggi e-mail a nuovi utenti che hanno completato la registrazione.

Procedura

1. Modificare l'**Impostazione conferma registrazione utente** esistente o aggiungerne una nuova.
2. Modificare o assegnare un nome per identificare l'impostazione.
3. Inserire una descrizione facoltativa dell'impostazione.
4. Assicurarsi che l'opzione **Invia e-mail di conferma registrazione utente** sia attivata.
5. Fare clic su **Avanti**.
6. Selezionare una distribuzione per la configurazione.
7. Fare clic su **Fine**.

Configurazione dell'impostazione Pianificazione lavoro utente

Gli amministratori possono configurare una pianificazione di lavoro per gli utenti che blocca tutte le comunicazioni da Sentry per i dispositivi gestiti durante le ore non lavorative stabilite. Utile per gli utenti dei paesi che prevedono leggi per il "diritto alla disconnessione".

Procedura

1. Selezionare **Utenti**.
2. Selezionare **Impostazioni utente**.
3. Nella sezione, **Impostazione Pianificazione lavoro utente**, selezionare **+Aggiungi impostazione per specifici gruppi utente**.
4. Fornire un nome per l'impostazione.
5. Attivare l'impostazione.

6. Selezionare il fuso orario.
7. Configurare le ore durante le quali Ivanti Neurons for MDM blocca il protocollo Exchange ActiveSync, le app compatibili con AppConnect e le app gestite.
8. Fare clic su **Avanti**.
9. Configurare la distribuzione, quindi fare clic su **Fatto**.

> Le modifiche applicate potrebbero richiedere fino a 1 ora e 15 minuti per avere effetto sul dispositivo.

Configurazione delle impostazioni di autenticazione del portale Amministratori

Gli amministratori possono impostare il tipo di autenticazione per l'accesso degli utenti. Questa impostazione determina se agli utenti verrà richiesto di immettere solo la password oppure sia la password che il PIN.

Procedura

1. Modificare un'**impostazione di autenticazione del portale Amministratori** esistente o aggiungerne una nuova.
2. Modificare o assegnare un nome per identificare l'impostazione.
3. Inserire una descrizione facoltativa dell'impostazione.
4. In **Tipo di autenticazione portale Amministratori**, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Password	Selezionare questa opzione per autenticare l'accesso solo tramite password. Gli utenti possono comunque ricevere un PIN per completare l'attivazione dell'account.
Password e PIN	Selezionare questa opzione per autenticare l'accesso tramite password e PIN. Quando si seleziona questa opzione vengono visualizzati i seguenti campi aggiuntivi: • **Durata del PIN**: selezionare la durata del PIN in minuti dall'elenco a discesa. Il valore deve essere compreso tra 1 e 15 minuti. • **Lunghezza del PIN**: selezionare il numero di caratteri del PIN dall'elenco a discesa. La lunghezza del PIN deve essere compresa tra 4 e 12 caratteri. Questa opzione è applicabile solo per gli account locali e non per gli account di amministrazione LDAP.
Consentire all'utente di richiedere un nuovo PIN	Selezionare questa opzione per consentire agli utenti di richiedere un nuovo PIN.

5. Fare clic su **Avanti**.
6. Selezionare una distribuzione per la configurazione.
7. Fare clic su **Fine**.

Per gli utenti configurati con un **Provider di identità** (IdP) basato su SAML, Ivanti Neurons per MDM supporta l'autenticazione basata su PIN al portale di amministrazione. L'opzione Tipo di autenticazione portale Amministratori deve essere impostata su PIN e password. Questa funzione opera come autenticazione a due fattori, per aumentare il livello di sicurezza. In questo caso, quando tale utente tenta di accedere al portale:

- Viene inviato un PIN all'ID e-mail dell'utente.

- L'utente immette il PIN nella pagina di accesso del portale amministrativo.
- Se il PIN è corretto, l'utente viene reindirizzato alla pagina di accesso dell'IdP, in cui l'utente immette il nome utente e la password per l'IdP.
- Se le credenziali dell'IdP sono corrette, l'utente viene reindirizzato al portale amministrativo.

Quando accede al portale amministrativo, l'utente può fare clic su **Password dimenticata** per reimpostare la password. Nella schermata successiva l'utente può immettere la nuova password e il PIN (richiesto in base alle impostazioni precedenti relative alla modalità di autenticazione degli utenti) viene inviato all'indirizzo e-mail dell'utente. Se necessario, fare clic su **Reinvia PIN**. L'utente deve attendere quindici minuti tra una richiesta di password dimenticata e l'altra.

> Quando questa configurazione viene distribuita ai dispositivi, se l'utente effettua vari tentativi di accesso non riusciti consecutivi (valore predefinito: 5 tentativi) utilizzando la password o il PIN, l'account viene bloccato e al momento del blocco viene visualizzato un messaggio per l'utente.

6.4. Personalizzazione degli utenti

Personalizzazione utenti consente di personalizzare il processo di registrazione dei dispositivi mediante l'utilizzo di nomi e loghi riconoscibili dagli utenti. È possibile personalizzare il branding lato utente come segue:

- Impostare un nome host personalizzato per l'URL di registrazione
- Visualizzare il proprio logo nell'e-mail e nella schermata di registrazione
- Visualizzare un'icona preferita personalizzata durante le attività di registrazione

> L'aggiornamento delle impostazioni sopra indicate modifica il valore a cui fa riferimento **$**.

Licenza: Gold

Prerequisito:

- Decidere quale nome host utilizzare nell'URL personalizzato. Il nome host deve soddisfare i seguenti requisiti:
  - Non deve contenere spazi
  - Non deve contenere caratteri speciali

Ottenere un file del logo che soddisfi i seguenti requisiti:

  - Formato PNG
  - 580 x 80 pixel

Ottenere un file dell'icona preferita che soddisfi i seguenti requisiti:

  - Formato PNG
  - 64 x 64 pixel

Procedura:

1. Andare a **Utenti > Personalizzazione utenti**.
2. Fare clic su **Personalizza** (in alto a destra).
3. Nel campo **Nome host** digitare un nome breve da utilizzare come nome host nell'URL.
4. Fare clic su **Verifica disponibilità** per confermare che il nome host immesso non è stato utilizzato da altri.
5. Se il nome host non è disponibile, immettere un altro nome.
6. Notare l'URL di registrazione risultante in **Anteprima URL**.
7. Fare clic su **Avanti**.
8. In **Logo**, fare clic su **Scegli file** per caricare il logo da utilizzare nell'e-mail e nella schermata di registrazione.
9. Fare clic su **Avanti**.
10. In **Favicon**, fare clic su **Scegli file** per caricare il favicon da mostrare al posto del favicon di Ivanti Neurons for MDM durante le attività di registrazione.
11. Fare clic su **Fine**.

6.5. Registrazione utenti con Apple Business Manager

Argomenti della sezione:

Applicabile a:

- Dispositivi non supervisionati con iOS 13.0 fino all'ultima versione supportata da Ivanti Neurons per MDM.
- Dispositivi con macOS 10.15 o versioni più recenti supportate Ivanti Neurons per MDM.

Apple Business Manager è uno strumento mediante cui i team IT possono automatizzare il deployment dei dispositivi, acquistare e distribuire contenuti e gestire i ruoli all'interno delle proprie organizzazioni. Apple Business Manager implementa Registrazione utenti, un'opzione di registrazione pensata per le aziende che implementano BYOD (Bring Your Own Device). Registrazione utenti è una versione modificata del protocollo MDM con una maggiore attenzione alla privacy degli utenti, implementata con un livello di sicurezza che riflette le esigenze dell'azienda.

La registrazione dell'utente consente all'amministratore di effettuare le seguenti operazioni:

- installare e rimuovere applicazioni gestite
- installare e rimuovere configurazioni di rete
- installare una VPN parziale nell'ambito delle app e degli account gestiti
- richiedere l'utilizzo di una password

Requisiti per l'attivazione di Registrazione utenti

Di seguito sono indicati i requisiti per l'attivazione di Registrazione utenti. Se uno di essi non viene soddisfatto, il tipo di registrazione sarà in base al dispositivo.

- Dispositivi non supervisionati con iOS 13.0 fino all'ultima versione supportata da Ivanti Neurons per MDM o dispositivi con macOS 10.15 o versioni successive supportate da Ivanti Neurons per MDM.
- L'impostazione utente per il campo Tipo di registrazione Apple deve essere "Registrazione utenti".
- Un account Apple Business Manager.
    - L'account di licenza delle app Apple deve essere parte dello stesso account Apple Business Manager.
    - All'interno di Apple Business Manager, se si dispone di un account in Posizioni, è necessario che la funzione App e libri sia abbinata alla stessa posizione. Potrebbe essere necessario aggiungere una nuova posizione (ad esempio, West Coast).

ID Apple gestito: ID Apple gestito da associare a ciascun dispositivo registrato.

    - Questo ID Apple gestito fornisce l'autenticazione per le licenze delle app e la gestione MDM.
    - Quando la soluzione MDM distribuisce app e media, le licenze Apple necessarie vengono assegnate all'ID Apple gestito associato al dispositivo.
    - Nell'ambito della conformità al GDPR, gli ID Apple gestiti sono mascherati nell'elenco degli utenti e nelle pagine con i dettagli degli utenti considerando l'ID Apple un dato relativo all'utente.
    - Gli ID Apple gestiti sono stati utilizzati inizialmente da Apple School Manager e sono ora utilizzati da Apple Business Manager per Registrazione utenti.

> L'ID Apple gestito e il token della posizione di App and Books del dispositivo devono provenire dalla stessa organizzazione dell'account Apple Business Manager.

Se sono diversi, viene visualizzata una notifica nel portale Amministratori di Ivanti Neurons per MDM quando l'assegnazione della licenza non va a buon fine per un'app.

Microsoft Entra ID configurato per Autenticazione federata o un ID Apple creato manualmente in Apple Business Manager con un dominio convalidato.

- Per istruzioni sull'utilizzo della funzione di autenticazione federata, vedere la **Guida per l'utente di Apple Business Manager** sul sito web di Apple. È richiesto l'accesso.

Gli utenti del dispositivo che vengono sincronizzati con LDAP devono essere assegnati a un ruolo di gestione dei dispositivi e associati a un ID Apple gestito.

Nella pagina dell'elenco **Utenti** e nella pagina dell'elenco **Dispositivi** è possibile aggiungere la colonna ID Apple gestito, che potrà essere visualizzata da tutti gli utenti. Nella pagina **Dispositivi**, è possibile aggiungere la colonna Registrazione utente completata per visualizzare lo stato dei dispositivi con Registrazione utenti. Queste colonne sono inoltre incluse nelle esportazioni degli utenti e dei dispositivi in formato CSV.

Priorità delle registrazioni

- La registrazione utenti è supportata dal client Go for iOS e da iReg. Apple non supporta più la Registrazione utenti tramite Ivanti Go per iOS e iReg. **Registrazione utenti guidata dall'account** è disponibile solo nell'account Lavoro o Scuola del dispositivo.
- Le registrazioni Registrazione automatica dispositivo e Apple Configurator saranno sempre in base al dispositivo.
- Se a un dispositivo viene applicata la configurazione MAM, la registrazione MAM ha la precedenza sulla registrazione utente.
- Se sono soddisfatti entrambi i requisiti Sola autorizzazione e Registrazione utenti, Registrazione utenti ha la precedenza.
- Se si registra nuovamente un dispositivo da Go per il client iOS, verrà applicato lo stesso tipo di registrazione utilizzato durante la registrazione del dispositivo, indipendentemente dalla modifica del tipo di registrazione in Ivanti Neurons per MDM. Ad esempio, se un dispositivo è stato registrato dall'utente, modificare il tipo in Registrazione dispositivi in Ivanti Neurons per MDM e registrare nuovamente il dispositivo dal client Go. Il dispositivo sarà ancora registrato dall'utente e non dal dispositivo.

Differenza tra registrazione MDM standard e Registrazione utenti

Questa sezione descrive la differenza tra la registrazione MDM standard e Registrazione utenti con Apple Business Manager.

Registrazione MDM standard

Nell'elenco seguente vengono indicate le attività che un server Ivanti Neurons per MDM non può eseguire nella modalità Registrazione utenti, ma può svolgere nell'ambito di una registrazione MDM standard.

Il server MDM:

- non può eliminare il dispositivo
- non vede le app personali che l'utente ha installato sul dispositivo
- non può convertire le app installate dall'utente in app gestite da MDM
- Impossibile cancellare il passcode del dispositivo (p. es. sbloccare il dispositivo).
- non può impostare un requisito lungo e complesso per il passcode del dispositivo

- non può configurare una VPN o un proxy Wi-Fi a livello di dispositivo, né può gestire in alcun modo la funzionalità dello smartphone
- non può vedere gli identificatori di dispositivo come UDID, numero di serie o IMEI
- non può applicare molte restrizioni a livello di dispositivi (come ad esempio limitare la classificazione dei contenuti delle app), bloccare iCloud e applicare eventuali restrizioni supervisionate

Registrazione utenti con Apple Business Manager

In Registrazione utenti, il server MDM può ancora fare tutto il necessario per gestire le app, gli account e i dati aziendali.

Con Registrazione utenti è possibile:

- installare app o app in-house tramite licenze App e libri basate su utente (Apple).
  - Le licenze sono applicate in base all'ordine di arrivo delle richieste e sono utilizzate dagli ID Apple gestiti.
  - La licenza utilizzata da un'app installata sul dispositivo registrato dall'utente sarà diversa dalla licenza utilizzata dalla stessa app installata sul dispositivo con registrazione dispositivo.
  - Controllare il tipo di licenza per le app App e libri di Apple nella pagina dei dettagli utente tramite la scheda Utilizzo licenze; il tipo di registrazione viene visualizzato come Registrazione utenti o Registrazione dispositivi.

Applicare le impostazioni payload del passcode. Ad esempio:

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

eseguire query sui dati correlati ad app, certificati e profili gestiti a livello aziendale

- configurare una VPN per-app per app, posta elettronica, contatti e calendari che sono stati installati da MDM
- imporre alcune restrizioni, come la funzionalità "Apri in" gestita, contatti gestiti e dati gestiti nella schermata di blocco e molte altre ancora

I dati aziendali vengono memorizzati in un volume APFS (Apple File System) separato, che viene creato al momento della registrazione e crittografato separatamente dai dati utente del dispositivo. Questo volume contiene i dati memorizzati da app gestite, note aziendali, documenti iCloud Drive aziendali, voci portachiavi aziendali, allegati e testi e-mail gestiti e allegati del calendario. L'annullamento della registrazione da MDM elimina il volume e le chiavi.

Tutte le app di terze parti possono essere solo un'app personale o un'app gestita tramite Ivanti Neurons for MDM. Il servizio MDM non può iniziare a gestire le app che l'utente del dispositivo ha già installato. In questo caso, l'amministratore dovrà richiedere all'utente del dispositivo di eliminare l'app personale prima di installare l'app tramite MDM. Il servizio MDM non può iniziare a gestire le app che l'utente ha già installato. Tuttavia, alcune app di sistema come Note e File supporteranno sia gli account di lavoro sia quelli personali.

Registrazione utenti per dispositivi macOS

Registrazione utenti è supportato per i dispositivi con macOS 10.15 o versioni successive supportate da Ivanti Neurons per MDM.

- Mobile@Work per macOS non è supportata per i dispositivi macOS registrati in Registrazione utenti.
  - Anche se l'app è distribuita nel dispositivo macOS registrato in Registrazione utenti, l'app non verrà inviata al dispositivo da MDM.

- Pertanto le funzionalità di Mobile@Work, come la gestione degli script e la gestione delle app per le app MobileIron Packager (MIP), non sono supportate per i dispositivi macOS registrati in Registrazione utenti.

Dipendenza delle app e cambiamenti comportamentali nei dispositivi macOS registrati in Registrazione utenti.

- Nei dispositivi macOS registrati in Registrazione utenti, la dipendenza delle app funziona al meglio delle proprie possibilità poiché MDM non conosce (non può confermare) lo stato di installazione delle app prerequisito prima di distribuire l'app principale.
- Le app e le configurazioni possono essere distribuite agli utenti e ai gruppi di utenti che appartengono ai dispositivi macOS registrati in Registrazione utenti. Tuttavia, nelle app viene sempre visualizzato il pulsante **Installa**, anziché "Installato", perché MDM non può visualizzare lo stato di installazione delle app nei dispositivi macOS registrati con Registrazione utenti.
- Le app installate sono indicate come App richieste nella pagina **Dispositivi > Inventario delle app**, poiché i dispositivi macOS registrati con Registrazione utenti non indicano al serverIvanti Neurons per MDM se le app sono installate o meno nel report dell'inventario.

Nel filtro di distribuzione delle app, gli attributi Registrazione Registrazione utenti e Registrazione Automated Registrazione dispositivi possono essere utilizzati per la distribuzione personalizzata, secondo le esigenze.

- Le licenze basate sull'utente sono supportate utilizzando gli ID Apple per installare le app App e libri di Apple. Le licenze basate su dispositivo non sono consentite. Il Catalogo app mostra solo le applicazioni App e libri di Apple.
- Non tutte le configurazioni, policy e azioni sono consentite. Vedere l'elenco completo delle configurazioni e delle policy che seguono questa procedura.
  - Se le configurazioni non supportate sono distribuite in un dispositivo macOS registrato in Registrazione utenti, non saranno distribuite o applicate al dispositivo e potrebbe essere visualizzato un messaggio del tipo "Limitazioni - questo non è un tipo di richiesta valido".
  - Allo stesso modo, le azioni non supportate dell'amministratore sul dispositivo saranno descritte nell'interfaccia utente di Ivanti Neurons per MDM.
  - I report non supportati non verranno inviati da Ivanti Neurons per MDM.

Di seguito vengono indicate le configurazioni e le policy non supportate da distribuire ai dispositivi macOS registrati in Registrazione utenti:

- Passcode
- Tunnel
- Tunnel (on demand)
- Configurazioni VPN
- Creazione automatica dell'account Office 365
- Policy di estensione kernel di macOS
- Preferenze privacy
- Restrizioni di macOS
- Aggiornamenti software
- AirPrint
- Privacy client dell'istanza gestita
- FileVault 2
- Chiave di ripristino di FileVault

- Firewall
- Regola policy di sistema
- Preferenza certificato
- Controllo policy di sistema
- Gestito dalle policy di sistema
- Restrizioni dell'App Store di macOS
- Restrizioni della masterizzazione dischi in macOS
- Impostazioni Finder in macOS
- Mobile@Work per macOS
- Script di Mobile@Work per macOS
- Controllo supporti multimediali consentito
- Server di riferimento orario
- Policy app consentita

Differenza tra Registrazione utenti e Registrazione dispositivi

Questa sezione illustra la differenza tra Registrazione utenti e Registrazione dispositivi.

Registrazione utenti si applica ai dispositivi con iOS 13.0 e macOS 10.15 fino all'ultima versione supportata. I dispositivi con versione inferiore a iOS 13.0 e macOS 10.15 saranno considerati "Registrazione dispositivi" indipendentemente dal fatto che l'utente del dispositivo sia stato abilitato per Registrazione utenti.

> Registrazione utenti per Apple Business Manager non consente di eseguire azioni di cancellazione o di sblocco. Tuttavia, nel portale utente tali opzioni saranno ancora disponibili, anche se non funzioneranno.

Differenza tra Registrazione utenti e Registrazione dispositivi			
Funzionalità	Registrazione utente	Mobile Application Management (MAM)	Registrazione dispositivo
Cancellare il dispositivo e vedere le app personali degli utenti	✗	✗	✓
Convertire un dispositivo da gestito a non gestito o viceversa	✗	✗	✓
Cancellare il passcode del dispositivo, configurare una VPN o un proxy Wi-Fi lato dispositivo o gestire la funzionalità cellulare	✗	✗	✓
Vedere gli identificatori di dispositivo come il numero di serie, IMEI	✗	✗	✓
Applicare restrizioni supervisionate	✗	✗	✓ (Solo dispositivi supervisionati)
È possibile installare e configurare app e account	✓	✓	✓
È possibile configurare una VPN per-app per le app, la posta elettronica, i contatti e i calendari che sono stati installati da MDM	✓	✗	✓
È possibile imporre alcune restrizioni, come la funzionalità "Apri in" gestita, contatti gestiti e dati gestiti nella schermata di blocco e molte altre	✓	✗	✓
È possibile eseguire query sui dati correlati ad app, certificati e profili gestiti a livello aziendale	✓	✗	✓

Connessione di Ivanti Neurons for MDM a Apple Business Manager

In questa sezione viene descritto come consentire Registrazione utenti per Apple Business Manager.

Prerequisiti

- È necessario disporre di un account Apple Business Manager. Vedere **https://business.apple.com/** .
- Per gestire i dispositivi iOS, è necessario richiedere e installare un **certificato MDM** Apple.

Creazione di utenti locali per l'abilitazione di Registrazione utenti

Questa sezione descrive la creazione di utenti locali e LDAP e l'impostazione di Registrazione utenti utente per i dispositivi Apple senza supervisione. Registrazione utenti non funzionerà sui dispositivi supervisionati o sui dispositivi registrati al programma Registrazione dispositivi di Apple.

Creazione di un gruppo di utenti gestito manualmente (statico)

Questa è una procedura che viene eseguita una sola volta. Se questo gruppo è già stato creato, passare alla sezione "Creazione di utenti per Registrazione utenti".

Procedura

1. Andare a **Utenti >** Gruppi di utenti.
2. Creare un gruppo di utenti gestito manualmente (statico), come ad esempio Gruppo registrazione utente, per aggiungere utenti con il tipo di registrazione dispositivo Registrazione utenti.
3. Fare clic su **Salva**.

Creazione di un'impostazione del tipo di registrazione dispositivo

Questa è una procedura che viene eseguita una sola volta. Se questo gruppo è già stato creato, passare alla sezione "Creazione di utenti per Registrazione utenti". Per i dispositivi registrati in Registrazione utenti, l'impostazione predefinita del proprietario del dispositivo sarà "Di proprietà dell'utente".

Procedura

1. Andare in **Utenti >** Impostazioni utenti.
2. Nella sezione Impostazioni registrazione dispositivo, fare clic **+ Aggiungi impostazione per specifici gruppi utente**.
3. Creare una nuova impostazione, come Registrazione UE, per gli utenti con tipo di registrazione del dispositivo come Registrazione utenti.
4. Nella sezione Registrazione Apple, selezionare **Registrazione utenti** come tipo di registrazione Apple.
5. Fare clic su **Avanti**.
6. Nella pagina Distribuzione impostazioni utente, selezionare il gruppo di utenti appena creato, come ad esempio Gruppo registrazione utenti.
7. Fare clic su **Fine**.

Creazione di un utente locale per Registrazione utenti

Come prerequisito, creare un gruppo di utenti gestito manualmente e un'impostazione di registrazione dispositivo per Registrazione utenti.

Procedura

1. Andare a Utenti.
2. Fare clic su +**Aggiungi** >**Utente singolo** .
   Inserire le informazioni sul nuovo utente e aggiungerlo al gruppo di utenti appena creato, come ad esempio Gruppo registrazione utenti. Per ulteriori informazioni, vedere *Aggiunta di un utente* nell'argomento Utenti.

Importazione di utenti LDAP per consentire Registrazione utenti

Prerequisiti

- Come prerequisito, impostare un connettore di Ivanti Neurons per MDM per accedere alle risorse LDAP.
- Assicurarsi che l'impostazione **ID apple gestito** sia impostata su **Modello** (indirizzo e-mail dell'utente). Assicurarsi che il modello dell'ID Apple gestito sia unico. In caso contrario, l'account non verrà aggiornato con l'ID Apple gestito se lo stesso ID Apple

gestito esiste in un altro account.
- (Facoltativo) Includere il sottodominio "appleid" per evitare conflitti con gli ID Apple esistenti.
- È possibile importare gli utenti da LDAP e invitarli per Registrazione utenti. Gli utenti LDAP importati avranno i propri ID Apple gestiti sincronizzati con Ivanti Neurons per MDM, che è un requisito per Registrazione utenti.

Procedura

1. Andare a **Utenti**.
2. Fare clic su **+Aggiungi > Invita utenti da LDAP**.
3. Fare clic su **Seleziona utenti** alla voce del server LDAP.
4. Nella pagina Aggiungi utenti LDAP, immettere il nome dell'utente, gruppo o unità organizzativa nella casella di ricerca.
5. Per aggiungere nuovi utenti o gruppi, fare clic su **+Aggiungi** accanto alla voce che si desidera aggiungere.
6. Fare clic su **Fine**.

Importazione di utenti Entra ID per consentire Registrazione utenti

Come prerequisito, collegare Ivanti Neurons per MDM con Microsoft Entra ID (Entra ID).

È possibile invitare gli utenti Entra ID per Registrazione utenti. Gli utenti Entra ID importati avranno i propri ID Apple gestiti sincronizzati con Ivanti Neurons per MDM, che è un requisito per Registrazione utenti.

Procedura

1. Andare in **Amministratore >** Origine utente Entra ID.
2. Modificare le impostazioni.
3. Selezionare **Attiva questo Entra ID**.
4. Nell'impostazione ID Apple gestito, selezionare una delle seguenti opzioni:
    - **Modello**
        - **Indirizzo e-mail dell'utente** - Assicurarsi che il modello per l'ID Apple gestito sia unico. In caso contrario, l'account non verrà aggiornato con l'ID Apple gestito se lo stesso ID Apple gestito esiste in un altro account.
        - In alternativa, selezionare **userUPN**.
5. (Facoltativo), Includere il sottodominio "appleid" per evitare conflitti con gli ID Apple esistenti.
6. Selezionare **Invita gli utenti importati da Entra ID automaticamente**. Gli utenti importati da Entra ID a Ivanti Neurons per MDM vengono invitati automaticamente a registrarsi tramite e-mail.
7. Fare clic su **Salva**.

Istruzioni per gli utenti del dispositivo per la registrazione con Registrazione utenti

Questa sezione descrive le azioni che l'utente del dispositivo deve intraprendere per la registrazione tramite Registrazione utenti di Apple.

Procedura

1. Sul dispositivo iOS che si desidera registrare, aprire l'e-mail di invito che contiene un collegamento e le istruzioni che indirizzano l'utente finale a un link di registrazione, come mobileiron.com/go.
2. Aprire il link di registrazione in Safari.

3. Viene visualizzata la pagina di accesso. L'utente del dispositivo deve effettuare l'accesso utilizzando le proprie credenziali di utente locale o le credenziali LDAP.
   Viene visualizzata la pagina di registrazione con un messaggio che informa che il profilo è stato scaricato.
   Toccare Impostazioni. Viene visualizzata la pagina delle impostazioni.
4. Toccare Registrati a [Nome azienda].
5. Viene visualizzata la pagina Registrazione utenti.
6. Toccare Registra il mio [dispositivo dell'utente]. Ad esempio, toccare Registra il mio iPhone.
   Se si tocca Annulla ed Elimina profilo, si dovrà ricominciare il processo di registrazione da capo.
   Verrà visualizzato un accesso per Apple o l'account federato. Immettere la password per l'ID Apple gestito. (L'ID Apple gestito verrà visualizzato nella parte superiore della pagina di accesso).
   Può essere visualizzata l'opzione di rimanere connessi, effettuare una selezione.
   In una pagina viene visualizzato il messaggio "La registrazione è riuscita".

Utilizzo dei registri del dispositivo per la risoluzione dei problemi

Per risolvere errori o problemi relativi a un dispositivo registrato dall'utente, iniziare rivedendo i registri dei dispositivi.

Procedura

1. Andare su Dispositivi.
2. Fare clic sul dispositivo per visualizzare la pagina dei dettagli del dispositivo. È possibile verificare i campi Registrazione utente completata e ID Apple gestito registrato.
3. Selezionare la scheda Registri.
4. Nell'area Filtri, limitare il numero di registri dei dispositivi applicando filtri basati sui nomi delle azioni (ad esempio Checkout, Nome dispositivo, Imposta token bootstrap, Ottieni token bootstrap e così via), stato, data di inizio e data di fine.
5. Nella colonna Azioni, fare clic sull'icona dell'occhio per visualizzare i dettagli dei registri del dispositivo, come ad esempio l'ID di registrazione.
6. Fare clic su **OK**.

6.6. Licenze utente

Le licenze di Ivanti Neurons per MDM basate sull'utente definiscono il numero di utenti che è possibile registrare, il numero di dispositivi consentiti per licenza utente, la quantità di contenuti che è possibile configurare per la distribuzione ai dispositivi e le funzionalità disponibili. Se si raggiunge il limite di utenti, viene visualizzato un triangolo rosso nella pagina Amministratore. Se si raggiunge il limite di contenuto, il servizio impedirà l'aggiunta di ulteriori contenuti e visualizzerà un messaggio per segnalare il raggiungimento del limite.

Per determinare il numero di licenze utente, occorre considerare i seguenti punti:

- Ogni licenza utente acquistata nell'ambito del pacchetto Secure UEM or Secure UEM Premium consente la registrazione di un massimo di cinque dispositivi.
- Dopo aver registrato più di cinque dispositivi, viene richiesta un'altra licenza utente.
- Non è presente nessun limite stabilito per il numero di licenze utente che un utente può richiedere.
- Le licenze vengono rilasciate al momento della disattivazione o della cancellazione dei dispositivi.

Ad esempio, quando Utente1 registra il telefono aziendale il primo giorno di lavoro, richiede una licenza utente. La settimana successiva, registra due suoi telefoni personali e un tablet con la stessa licenza. Quando registra un altro tablet, dispone di cinque dispositivi e pertanto richiede una seconda licenza utente. Se le viene rubato il telefono personale, cancella il dispositivo, che rilascerà la seconda licenza utente.

Visualizzazione del numero di dispositivi/ licenze per un utente

Procedura:

1. Andare a **Utenti**.
2. Fare clic sul collegamento relativo all'utente.

Nel riquadro a sinistra vengono elencati i dettagli utente, incluso l'utilizzo della licenza.

6.7. Gestione degli utenti

Argomenti della sezione:

- Aggiunta di un utente API per operazioni Cisco ISE
- Assegnazione di ruoli
- Ruoli utente
- Ricerca e applicazione di filtri agli utenti
- Assegna utenti
- Invio di inviti agli utenti
- Attivazione e disattivazione di utenti
- Gestione di accessi multipli dell'amministratore
- Modifica password
- Invio di messaggi
- Rimozione di utenti dai gruppi di utenti
- Eliminazione di un utente
- Esportazione di utenti
- Assegnazione di attributi personalizzati agli utenti
- Rimozione di attributi personalizzati dagli utenti
- Modifica delle impostazioni locali degli utenti
- Modifica di un nome utente
- Interruzione della raccolta di dati sulla posizione
- Informazioni sul timeout
- Disattivazione dell'analisi di utilizzo del sistema
- Registrazione dispositivo tramite generazione PIN

6.7.1. Aggiunta di un utente API per operazioni Cisco ISE

È possibile aggiungere un utente API con il ruolo "Operazioni Cisco ISE" che consente a Cisco ISE di interagire con le API Cisco ISE in Ivanti Neurons per MDM. Dopo aver creato questo utente, si utilizzano le sue credenziali utente da Cisco ISE per autenticare le chiamate API in Ivanti Neurons per MDM. Queste API consentono a Cisco ISE di ottenere informazioni sui dispositivi; eseguire azioni sui dispositivi, ad esempio, cancellazione di tutti i dati, cancellazione di dati aziendali e blocco del PIN, e di inviare messaggi ai dispositivi.

> L'utente API non sarà in grado di accedere al portale Amministratori. L'utente può solo abilitare l'utilizzo delle API.

> Il ruolo Operazioni Cisco ISE può essere assegnato per impostazione predefinita solo al super amministratore di un tenant. Il super amministratore deve scegliere esplicitamente gli altri utenti nel sistema che devono avere questo ruolo e assegnarlo loro. Gli utenti a cui viene assegnato il ruolo Operazioni Cisco ISE possono assegnare a loro volta tale ruolo ad altri utenti idonei nel sistema.

Procedura

1. Andare in **Utenti** > **Utenti**.
2. Fare clic su **Aggiungi**.
3. Selezionare **Utente API**.
4. Compilare il modulo risultante con le informazioni dell'utente:
    - Indirizzo e-mail
    - Nome
    - Cognome

> Nel campo Nome utente viene visualizzato l'indirizzo e-mail immesso. Nella maggior parte dei casi si sconsiglia di modificare questa impostazione predefinita. Consultare **Quando modificare un nome utente**.

Se si desidera cambiare il nome visualizzato dell'utente, modificare il testo predefinito nel campo **Nome visualizzato**.

6. Assegnare una password inserendola nei campi **Password** e **Conferma password**.
7. Lasciare selezionato il ruolo **Operazioni Cisco ISE Gestione API** nella sezione **Assegna ruoli**.
8. Fare clic su **Fine** per aggiungere l'utente.

Se non è possibile eseguire le attività indicate nella pagina **Utenti**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione sistemi
- Gestione utenti

6.7.2. Assegnazione di ruoli

È possibile fornire agli utenti accesso ai dati e alle funzionalità di Ivanti Neurons per MDM assegnando **ruoli**. È possibile assegnare i ruoli direttamente agli utenti o ai gruppi di utenti. Se viene assegnato un ruolo a un {{gruppo di utenti}}, tale ruolo sarà valido per tutti gli utenti del gruppo.

> Il ruolo Utente di sola lettura non è assegnato agli utenti per impostazione predefinita.
> La pagina dei ruoli e le opzioni associate sono nascoste per i tenant che hanno accesso sia a Ivanti Neurons for UEM che a Ivanti Neurons per MDM.

Gli utenti non possono assegnare autorizzazioni che non possiedono già. Le autorizzazioni e i ruoli che non sono stati assegnati agli utenti non vengono visualizzati per la selezione. In questo caso, compare un messaggio di errore. Quando un Amministratore Ivanti Neurons per MDM o un Amministratore partner tenta di assegnare ruoli a un Amministratore partner, Ivanti Neurons per MDM visualizza un messaggio che indica che un Amministratore partner deve eseguire questa operazione sul Portale service provider.

Per ulteriori informazioni sui ruoli, vedere **Gestione dei ruoli.htm**.

Procedura:

1. Andare a:
    - **Utenti > Utenti** *o*
    - Utenti > Gruppi di utenti.

Selezionare uno o più utenti o gruppi di utenti.

3. Fare clic su **Azioni**.
4. Dalla pagina Dettagli utente o Dettagli gruppo di utenti, fare clic su **Assegna ruoli** *o su*
   Dalla pagina Elenco utenti o Elenco gruppi di utenti, selezionare **Allega ruoli**.
5. Selezionare una o più delle regole seguenti che si desidera assegnare.
    - Gestione sistema | Tra gli spazi
    - Sistema di sola lettura | Tra gli spazi
    - Gestione utenti | Tra gli spazi
    - Utente di sola lettura | Tra gli spazi
    - Importazione e invito utente LDAP | Tra gli spazi
    - Gestione dispositivi | Specifico per lo spazio
    - Dispositivo di sola lettura | Specifico per lo spazio
    - Gestione app e contenuti | Specifico per lo spazio
    - App e contenuti di sola lettura | Specifico per lo spazio
    - Azioni relative ai dispositivi | Specifico per lo spazio
    - Operazioni Cisco ISE | Specifico per lo spazio
    - Gestione attività pianificate | Specifico per lo spazio
    - Servizi piattaforma comuni (CPS) | Specifico per lo spazio
    - Gestione Migrazione a basso impatto utente | Specifico per lo spazio
    - Registrazione personalizzata dispositivo | Specifico per lo spazio

- Modifica Microsoft Graph | Specifico per lo spazio
- Invia/Annulla cancellazione | Tra gli spazi
- Visualizza Microsoft Graph | Specifico per lo spazio
- Gestisci integrazione di Access | Tra gli spazi

Fare clic su **Avanti**.

7. Se i ruoli selezionati hanno un vincolo di Spazio, selezionare gli spazi per tutti i ruoli legati allo Spazio.

> Se è disponibile un solo spazio (Spazio predefinito), quando si assegna un ruolo vincolato allo spazio viene saltato il passaggio di specificazione dello spazio.

La pagina di riepilogo mostra il nome dello spazio relativo al ruolo vincolato allo spazio come Spazio predefinito.
Rivedere il riepilogo dei ruoli da assegnare e fare clic su **Fine**.

Consentire al personale dell'assistenza tecnica di utilizzare le azioni base del dispositivo

Gli addetti all'assistenza tecnica di solito possono visualizzare i dati. Tuttavia, alcune aziende preferiscono includere le azioni di base del dispositivo:

- Forza il check-in
- Blocca
- Sblocca
- Invia messaggio
- Ritira
- Cancella

Procedura

È possibile fornire un'autorizzazione alle azioni.

1. Passare a **Utenti > Utenti*** o**** Utenti > Gruppi di utenti**.
2. Selezionare uno o più utenti o gruppi di utenti.
3. Fare clic su **Azioni**.
4. Dalla pagina Dettagli utente o Dettagli gruppo di utenti, selezionare **Assegna ruoli** *o*
   Dalla pagina Elenco utenti o Elenco gruppi di utenti, selezionare **Allega ruoli**.
5. Selezionare **Dispositivo di sola lettura**.
6. Selezionare **Azioni relative ai dispositivi**.
7. Fare clic su **Fine**.

> Assicurarsi di selezionare Solo lettura del dispositivo prima di selezionare Azioni del dispositivo affinché gli utenti abbiano le autorizzazioni previste.

6.7.3. Ruoli utente

I ruoli utente determinano le pagine che gli utenti possono vedere in Ivanti Neurons for MDM e le cose che gli utenti possono fare. Nella tabella seguente vengono elencati i ruoli che è possibile assegnare e i relativi significati.

Ruolo	Descrizione	Specifico per lo spazio
Gestione sistemi	Consente a un amministratore di gestire le impostazioni a livello tenant, quali i certificati MDM, le impostazioni dell'App Catalog e altro.	No
Sistema di sola lettura	Consente a un amministratore di visualizzare le impostazioni a livello tenant, quali i certificati MDM, le impostazioni dell'App Catalog e altro.	No
Gestione utenti	Consente a un amministratore di aggiungere e rimuovere utenti, assegnare ruoli e aggiungere utenti a gruppi di utenti.	No
Utente di sola lettura	Consente a un amministratore di visualizzare gli utenti e i gruppi di utenti, nonché i cataloghi delle app e dei contenuti.	No
Gestione dispositivi	Consente a un amministratore di gestire gruppi di dispositivi, configurazioni e policy, così come tutte le azioni relative ai dispositivi.	Sì
Dispositivo di sola lettura	Consente a un amministratore di visualizzare gruppi di dispositivi, configurazioni e policy.	Sì
Gestione app e contenuti	Consente a un amministratore di aggiungere, distribuire e rimuovere app e contenuti.	Sì
App e contenuti di sola lettura	Consente di visualizzare tutte le attività in Utenti, App, Contenuti, incluse le attività AppConnect	Sì
Azioni relative ai dispositivi	Consente a un amministratore di avviare azioni relative ai dispositivi, quali: • Forza il check-in • Blocca • Sblocca • Invia messaggio • Ritira • Cancella È necessario selezionare Dispositivo di sola lettura prima di selezionare Azioni relative ai dispositivi. Altrimenti, gli utenti non avranno le autorizzazioni previste.	Sì
Importazione e invito utente LDAP	Consente a un amministratore di registrare gli utenti LDAP e di inoltrare inviti per la registrazione dei dispositivi.	No
Operazioni Cisco ISE	Consente a un amministratore di richiamare le API necessarie per l'integrazione Cisco ISE.	No
Gestione attività pianificate	Consenti a un amministratore di creare e gestire le attività pianificate per varie operazioni di amministrazione.	No
Servizi piattaforma comuni (CPS, Common Platform	Consente a un amministratore di utilizzare Servizi piattaforma comuni.	No

Ruolo	Descrizione	Specifico per lo spazio
Services)		
Gestione Migrazione a basso impatto utente	Consente a un amministratore di gestire le impostazioni di migrazione a basso impatto utente.	No
Registrazione personalizzata dispositivo	Consente a un amministratore di registrare un dispositivo tramite la funzione di registrazione personalizzata dispositivo.	No
Modifica Microsoft Graph	Consente a un amministratore di modificare le impostazioni API di Microsoft Graph utilizzate per la protezione app di Office 365.	No
Visualizza Microsoft Graph	Consente a un amministratore di visualizzare le impostazioni API di Microsoft Graph utilizzate per la protezione app di Office 365.	No
Invia/Annulla cancellazione	Consente a un amministratore di inviare un comando di cancellazione a un dispositivo o di annullare un comando di cancellazione emesso prima che venga eseguito.	No
Gestisci integrazione di Access	Consente a un amministratore di gestire l'integrazione di Access.	No

Per ulteriori informazioni, vedere **Assegnazione di ruoli**

6.7.4. Ricerca e applicazione di filtri agli utenti

Argomenti della sezione:

Ricerca di un utente

In seguito all'aggiunta di più utenti, l'utilizzo di filtri o di funzionalità di ricerca potrebbe essere utile per individuare rapidamente una voce relativa a un utente.

Procedura

1. Andare a **Utenti**.
2. Digitare i caratteri nella casella di ricerca.

Utilizzo di Ricerca avanzata per gli utenti

È possibile utilizzare l'opzione Ricerca avanzata per cercare utenti in base a regole per identificare e visualizzare gli utenti con criteri specifici. Le opzioni delle regole possono essere nidificate insieme utilizzando le opzioni QUALSIASI (O) o TUTTO (E). Gli utenti che soddisfano le regole vengono visualizzati sotto la sezione. Le regole possono essere costruite utilizzando i seguenti operatori:

- inizia con
- termina con
- contiene
- non contiene
- non inizia con
- non termina con
- è inferiore a
- è superiore a
- è compreso nell'intervallo
- è uguale a
- non è uguale a

A partire da Neurons for MDM 127, l'Amministratore Ivanti Neurons per MDM visualizza il numero di gruppi di utenti duplicati e il numero corrispondente di GUID per identificare i gruppi duplicati, quando l'attributo Nome gruppo utente è selezionato nel Generatore di regole. Inoltre, una tabella sotto questa regola visualizza l'elenco di gruppi di utenti duplicati e i relativi dettagli, ad esempio Nome gruppo di utenti, GUID, Origine e Nome distinto (DN).

Procedura

1. Nella pagina Utenti, fare clic sul collegamento **Ricerca avanzata**.
2. Fare clic su **Qualsiasi** se gli utenti devono soddisfare almeno una delle regole oppure fare clic su **Tutto**, se gli utenti devono soddisfare tutte le regole.
3. Creare una regola che definisce i criteri di ricerca, come ad esempio Gruppo utente, Attributo utente personalizzato e Attributo LDAP personalizzato.
4. (Opzionale) Fare clic su + per creare altre regole, se necessario.
5. (Opzionale) Fare clic **Salva** per salvare la query.

6. Fare clic su **Cerca**. L'elenco degli utenti che soddisfano i criteri di ricerca viene visualizzato nella pagina.

Caricamento delle query di ricerca per gli utenti

Procedura

1. Nella pagina Utenti, fare clic sul collegamento **Ricerca avanzata**.
2. Fare clic sull'icona "Cartella". Viene visualizzata la finestra **Ricerca avanzata**. L'elenco delle query di ricerca create viene visualizzato nella sezione **Carica query**. In questa sezione vengono visualizzati i seguenti dettagli:
   - **Nome query**: nome della query caricata.
   - **Contenuto query**: mostra il contenuto delle regole che definiscono la query di ricerca.
   - **Azioni**: selezionare l'azione da eseguire per la query.
3. Fare clic su **Carica query** nella colonna **Azioni** per visualizzare l'elenco degli utenti che soddisfano i criteri della query caricata. Per eliminare una query caricata, fare clic sull'icona Elimina.

Come applicare i filtri agli utenti

La barra di navigazione laterale Filtri elenca varie sezioni che consentono di ricercare un utente specifico dall'intero elenco di utenti. La procedura guidata Gestisci filtri contiene l'elenco di tutte le sezioni selezionabili per visualizzarle nella barra di navigazione Filtri.

Procedura

1. Andare a **Utenti**.
2. Fare clic sulle caselle di controllo rilevanti dalle sezioni elencate nella procedura guidata Gestisci filtri. È possibile ricercare dalle seguenti sezioni:
   - Amministratori
   - Stato di Google
   - Stato dell'invito
     - Completato (L'utente ha ricevuto l'invito e ha risposto.)
     - Scaduto (L'utente non ha risposto in tempo.)
     - Non invitato (L'utente non è stato invitato.)
     - In attesa (in attesa della risposta dell'utente)

   Scadenza password

     - Scade (utenti con opzione di scadenza password impostata su una data specifica).
     - Mai (utenti con opzione di scadenza password impostata su Mai).
   - Gruppo di utenti (selezionare il {{gruppo di utenti}} desiderato).
   - Origine utente
     - LDAP
     - Entra ID
     - Roster
     - Salesforce
     - Locale

- Sincronizza
  - Sincronizzazione diretta - Elenca gli utenti che sono stati sincronizzati direttamente dal server LDAP.
  - Nessuna sincronizzazione - Elenca gli utenti che sono stati rimossi dal server LDAP.
  - Sincronizzazione indiretta - Elenca gli utenti che sono stati sincronizzati indirettamente dal server LDAP.
  - N/A

3. (Opzionale) Fare clic su **Ripristina predefiniti** per ripristinare la selezione dei filtri predefiniti. La barra di navigazione Filtri visualizza le sezioni selezionate. Se si deselezionano tutte le caselle di controllo della procedura guidata Gestisci filtri, la barra di navigazione laterale Filtri visualizza tutte le sezioni.
4. Fare clic su un punto qualsiasi della procedura guidata di Gestisci filtri per uscire dalla procedura guidata.
5. Fare clic sull'icona x per chiedere la barra di navigazione laterale Filtri e fare clic su **Filtri** per riaprire la barra di navigazione laterale.

6.7.5. Assegna utenti

Argomenti della sezione:

- Assegnazione di utenti dalla pagina Utenti
- Assegnazione di utenti dalla pagina Gruppi di utenti

Assegnare utenti a gruppi di utenti è il modo ideale per ridurre al minimo la ripetizione di attività come:

- la distribuzione di app
- assegnazione di ruoli

Assegnazione di utenti dalla pagina Utenti

1. Andare a **Utenti**.
2. Selezionare gli utenti con cui si desidera collaborare.
3. Fare clic su **Azioni**.
4. Selezionare **Assegna a gruppo**.
5. Selezionare i gruppi o fare clic su **Crea nuovo** per creare un nuovo gruppo.
6. Fare clic su **Salva**.

Assegnazione di utenti dalla pagina Gruppi di utenti

1. Andare a **Utenti > Gruppi di utenti**.
2. Selezionare i gruppi di utenti con cui si desidera collaborare.
3. Fare clic su **Azioni** (in alto a destra).
4. Selezionare **Assegna utenti**.
5. Digitare l'indirizzo e-mail di ciascun utente.
6. Fare clic su **Assegna utenti**.

6.7.6. Invio di inviti agli utenti

Quando si aggiunge un utente, è possibile invitare quest'ultimo a registrare dei dispositivi. Quest'opzione è selezionata per impostazione predefinita. L'utente invitato riceve un messaggio e-mail con le informazioni necessarie per la registrazione. È possibile anche invitare (o invitare nuovamente) gli utenti dalla pagina **Utenti > Utenti**.

Procedura

1. Andare a **Utenti**.
2. Selezionare gli utenti che si desidera invitare.
3. Selezionare **Azioni > Invia invito**. Viene visualizzata l'Anteprima invito e un'opzione per impostare la proprietà del dispositivo su **Possedutodall'utente** o **Posseduto dall'azienda**.

4. Facoltativamente, attivare **Impostazioni proprietario dispositivo**.
5. Fare clic su **Di proprietà dell'utente** o su **Di proprietà dell'azienda**. Questa impostazione modifica il modo in cui il dispositivo viene classificato durante il processo di registrazione. Valido solo per i tipi di registrazione Solo PIN o Password + PIN. Se **Impostazioni proprietario dispositivo** è disattivato, i dispositivi saranno registrati come "Non impostati". Per i dispositivi supervisionati, l'impostazione del proprietario del dispositivo sarà "Posseduto dall'azienda".
6. Fare clic su **Invia**. Se è stata eseguita una registrazione del dispositivo basata su PIN, l'utente riceverà un PIN al suo indirizzo e-mail registrato. Se è impostata una registrazione basata sul codice QR, l'utente riceverà un codice QR.
7. Fare clic su **Ok**.

> Se la funzionalità e-mail di conferma registrazione è abilitata come descritto in **Configurazione e utilizzo di messaggi e-mail di conferma della registrazione**, viene visualizzato anche un promemoria per ricordare all'utente che riceverà un messaggio e-mail di conferma al completamento della registrazione. Per ricevere il messaggio e-mail, l'utente deve essere stato incluso nell'elenco di distribuzione specificato nella sezione **Configurazione delle e-mail di conferma della registrazione degli utenti** in **Impostazioni utente**.

Per ulteriori informazioni, vedere **Importazione di utenti LDAP**.

6.7.7. Attivazione e disattivazione di utenti

Argomenti della sezione:

- Attivazione e disattivazione di utenti locali
- Attivazione e disattivazione di utenti LDAP

Gli utenti locali e LDAP possono essere attivati o disattivati. In base al loro stato, è possibile creare policy personalizzate utilizzando la condizione Utente abilitato e impostando un'azione per la condizione nel Generatore di regole. Ad esempio, è possibile generare una regola della policy personalizzata per dismettere i dispositivi appartenenti a utenti LDAP/locali disattivati.

Attivazione e disattivazione di utenti locali

Per impostazione predefinita, quando viene creato un utente locale, l'utente viene attivato.

Procedura

1. Andare a **Utenti**.
2. Fare clic sul nome visualizzato dell'utente.
3. Fare clic su **Modifica**. Viene visualizzata la finestra **Autenticazione richiesta**.
4. Immettere la password dell'amministratore e fare clic su **Autentica**.

> Quando vengono inserite più voci errate della password e se viene superato il "limite dei tentativi non riusciti" impostato nell'opzione "Impostazioni complessità della password", l'account verrà bloccato e l'utente verrà disconnesso dalla sessione corrente.

5. Selezionare o deselezionare l'opzione **Attivo** per attivare o disattivare rispettivamente l'utente locale.
6. Fare clic su **Salva**.

Attivazione e disattivazione di utenti LDAP

È possibile attivare o disattivare gli utenti LDAP solo per Microsoft Active Directory. Dopo avere aperto le proprietà per un account utente in Microsoft Active Directory, fare clic sulla scheda **Account**, quindi selezionare o deselezionare le caselle di controllo nella finestra di dialogo delle opzioni **Account**. Vengono assegnati valori numerici all'attributo **UserAccountControl**. Il valore assegnato all'attributo indica a Windows quali opzioni sono state attivate. Dopo avere assegnato un valore all'attributo UserAccountControl, lo stato dell'utente verrà aggiornato dopo la sincronizzazione LDAP con Ivanti Neurons for MDM.

I valori che possono essere assegnati sono i seguenti:

- 512 - Attivo
- 514 - Disabilitato
- 66048 - Attivo, password senza scadenza
- 66050 - Disabilitato, password senza scadenza

Visualizza account utente

Procedura

1.	Fare clic su **Avvia**.	
2.	Passare a **Programmi**.	
3.	Passare a **Strumenti amministrativi**.	
4.	Fare clic su **Utenti e computer Active Directory**.	

Per ulteriori informazioni, vedere **https://support.microsoft.com/en-in/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-pro**.

È possibile visualizzare e modificare gli attributi utilizzando lo strumento Ldp.exe o lo snap-in Adsiedit.msc. L'utilizzo di questi strumenti per modificare Active Directory è consigliato solo agli amministratori esperti. Entrambi gli strumenti sono disponibili dopo avere installato Support Tools dal supporto di installazione Windows originale.

6.7.8. Gestione di accessi multipli dell'amministratore

Sono supportate sessioni multiple del portale Amministratori di Ivanti Neurons per MDM, in modo che l'amministratore possa visualizzare contemporaneamente diverse pagine del portale. Può visualizzare la data dell'ultimo accesso per tenere traccia degli accessi multipli.

Visualizza l'ultimo accesso dell'amministratore

Procedura

1. Fare clic sull'icona **Account**.
2. Visualizzare la voce **Utente ultimo accesso:**.

6.7.9. Modifica password

Argomenti della sezione:

- Modifica della password nella scheda Utenti
- Applicazione di una password senza scadenza
- Rimozione dell'impostazione Password senza scadenza

> Se un utente ha un ruolo di gestione del sistema, solo un superutente o un utente attualmente connesso può vedere l'opzione **Cambia password**.

È possibile cambiare la password di Ivanti Neurons per MDM. È inoltre possibile modificare la password di un altro utente, se si dispone dell'autorizzazione.

Procedura

1. Fare clic sull'icona Account (in alto a destra).
2. 
   Selezionare **Modifica password** dal menu a discesa.
3. Immettere la password corrente.
4. Immettere la nuova password.
5. Reimmettere la nuova password.
6. Per impostare la password senza scadenza, selezionare **Imposta la password senza scadenza**.

> L'impostazione della password senza scadenza sovrascrive l'impostazione **Periodo di scadenza password** definita in Utenti > Impostazioni utente > Impostazioni complessità della password.

7. Fare clic su **Fine**.

> Per reimpostare la password dell'account locale in modo che scada, deselezionare **Imposta la password senza scadenza**. Quando questa opzione viene deselezionata, una finestra pop-up mostra la data di scadenza della password precedentemente applicata all'utente.

Modifica della password nella scheda Utenti

Procedura

1. Andare a **Utenti**.
2. Fare clic sul nome visualizzato dell'utente.
3. Fare clic su **Modifica** (in alto a sinistra). Viene visualizzata la finestra **Autenticazione richiesta**. Agli amministratori (che sono utenti locali o utenti LDAP) viene richiesto di autenticarsi inserendo la password di amministratore prima di modificare l'utente.
4. Immettere la password dell'amministratore e fare clic su **Autentica**.

> Quando vengono inserite più voci errate della password e se viene superato il "limite dei tentativi non riusciti" impostato nell'opzione "Impostazioni complessità della password", l'account verrà bloccato e l'utente verrà disconnesso dalla sessione corrente.

5. Immettere la password attuale nel campo **Password attuale**.

> Questo campo non verrà visualizzato se si modifica la password di un altro utente.

6. Immettere la nuova password nel campo **Modifica password**.
7. Confermare la nuova password.
8. Fare clic su **Salva** (in alto a sinistra).

Applicazione di una password senza scadenza

1. Andare a **Utenti**.
2. Selezionare uno o più utenti.
3. Fare clic su **Azioni**.
4. Selezionare **Assegna Password senza scadenza**. Viene visualizzata la finestra **Imposta la password dell'account locale senza scadenza**.
5. Fare clic su **Invia**.

Rimozione dell'impostazione Password senza scadenza

1. Andare a **Utenti**.
2. Selezionare uno o più utenti.
3. Fare clic su **Azioni**.
4. Selezionare **Rimuovi Password senza scadenza**. Viene visualizzata la finestra **Rimuovi Password dell'account locale senza scadenza**.
5. Fare clic su **Invia**. Dopo la rimozione di questa impostazione, agli utenti viene applicata la data di scadenza password precedente.

6.7.10. Invio di messaggi

Argomenti della sezione:

- Invio di un messaggio a utenti
- Invio di un messaggio a dispositivi

È possibile inviare un messaggio a qualsiasi utente conosciuto. I messaggi possono essere e-mail o {{notifiche push}}. Soltanto gli utenti dei dispositivi registrati possono ricevere le notifiche push.

Prerequisiti

- Per i dispositivi iOS, assicurarsi che il client Go sia installato.
- Per i dispositivi macOS, assicurarsi che il client Mobile@Work sia installato.

Invio di un messaggio a utenti

1. Andare in **Utenti > Utenti**.
2. Selezionare gli utenti a cui si desidera inviare il messaggio.
3. Fare clic su **Azioni** (in alto a destra).
4. Fare clic su **Invia messaggio**.
5. Se non si desidera inviare un'e-mail, deselezionare la casella **Invia un messaggio e-mail**.
6. Se si desidera inviare un'e-mail, immettere un oggetto e il testo del messaggio.
7. Se si sta inviando una notifica push, selezionare la casella **Invia una notifica push** e immettere il testo del messaggio.
8. Fare clic su **Invia**.

Invio di un messaggio a dispositivi

1. Andare in **Dispositivi > Dispositivi**.
2. Selezionare i dispositivi a cui si desidera inviare il messaggio.
3. Fare clic su **Azioni** (in alto a destra).
4. Fare clic su **Invia messaggio**.
5. È possibile fare clic sul collegamento del nome del dispositivo per andare alla pagina Informazioni sul dispositivo e fare clic sull'icona **Invia messaggio** .
6. Se non si desidera inviare un'e-mail, deselezionare la casella **Invia un messaggio e-mail**.
7. Se si desidera inviare un'e-mail, immettere un oggetto e il testo del messaggio.
8. Se si sta inviando una notifica push, selezionare la casella **Invia una notifica push** e immettere il testo del messaggio.

> Il messaggio di una notifica push può includere anche URL a cui gli utenti possono accedere.

9. Fare clic su **Invia**.
   Quando una notifica push viene inviata all'utente, l'utente sarà in grado di vedere l'icona di una campana nella barra degli strumenti sullo schermo del dispositivo. Toccando l'icona a forma di campana, l'utente può visualizzare la cronologia delle notifiche ricevute e può eseguire un'azione o eliminare una notifica.

Disponibile all'interno delle pagine **Dispositivi** e **Utenti**, gli amministratori possono inserire attributi specifici del dispositivo o dell'utente in messaggi che vengono quindi messi in coda per la consegna all'utente finale.

6.7.11. Rimozione di utenti dai gruppi di utenti

Argomenti della sezione:

- Rimozione di utenti dalla pagina Utenti
- Rimozione di utenti dalla pagina Gruppi di utenti

Rimozione di un utente di un gruppo di utenti vuol dire:

- l'utente non potrà più usufruire dei ruoli assegnati al gruppo
- le app assegnate al gruppo non saranno più disponibili nell'{{App Catalog}} dell'utente
- le app configurate come rimovibili vengono rimosse dai dispositivi dell'utente

Rimozione di utenti dalla pagina Utenti

1. Selezionare l'utente con cui si desidera collaborare.
2. Fare clic su **Azioni** (in alto a destra).
3. Selezionare **Rimuovi da gruppo**.
4. Selezionare i gruppi.
5. Fare clic su **Rimuovi**.

Rimozione di utenti dalla pagina Gruppi di utenti

1. Fare clic sul gruppo di utenti per visualizzarne i dettagli.
2. Fare clic su **Modifica** (in alto a destra).
3. Fare clic sul collegamento **Rimuovi** accanto all'utente che si desidera rimuovere.
4. Fare clic su **Salva** (in alto a destra).

6.7.12. Eliminazione di un utente

Argomenti della sezione:

- Cosa succede quando si elimina un utente locale
- Informazioni relative agli utenti LDAP

Procedura

1. Andare in **Utenti > Utenti**.
2. Selezionare la voce relativa all'utente.
3. Fare clic su **Azioni** (in alto a destra).
4. Selezionare **Elimina**.

Quando un Amministratore Ivanti Neurons per MDM o un Amministratore partner tenta di eliminare un Amministratore partner, Ivanti Neurons per MDM visualizza un messaggio che indica che un Amministratore partner deve eseguire questa operazione sul Portale service provider.

> Se un utente ha alcuni dispositivi associati al proprio account, è necessario prima ritirare ed eliminare i dispositivi e poi eliminare l'utente. Se l'utente non ha dispositivi, le informazioni utente possono essere eliminate quando viene eliminato l'utente

Cosa succede quando si elimina un utente locale

- Tutte le informazioni relative all'utente eliminato vengono eliminate dal sistema.
- I dispositivi associati all'utente vengono ritirati.
- Il contenuto caricato dall'utente rimane.
- Non saranno consentite ulteriori registrazioni di dispositivi per l'account dell'utente.

Informazioni relative agli utenti LDAP

- Se il server LDAP è stato disabilitato, non è possibile eliminare in modo permanente un utente LDAP. La sincronizzazione successiva dei dati LDAP ripristinerà l'utente LDAP eliminato.
- Se è stato eliminato il server o gruppo LDAP, gli utenti LDAP diventano utenti locali e possono essere eliminati.
- Quando un utente viene eliminato da LDAP, non viene eliminato da Cloud. Lo stato di sincronizzazione passa a "NO_SYNC", ma l'utente non viene rimosso.

6.7.13. Esportazione di utenti

Come amministratore, è possibile esportare un elenco di utenti da Ivanti Neurons per MDM.

> Quando il PIN di registrazione del dispositivo dell'utente viene esportato in un file CSV, il PIN viene mascherato come "" invece del PIN effettivo per motivi di sicurezza.

Procedura

1. Andare in **Utenti > Utenti**.
2. Selezionare uno o più utenti dall'elenco.
3. Fare clic su **Esporta in CSV**.

Verrà mostrato un pop-up che informa che il report di esportazione richiederà del tempo per essere elaborato. Dopo aver inviato la richiesta, è necessario attendere che la richiesta sia completata prima di inviarne un'altra. Una volta che il report è pronto, all'utente verrà mostrato un messaggio per scaricare o eliminare il report generato. Si riceverà anche un'e-mail contenente un link per scaricare il report.

> I dettagli degli attributi **Utente personalizzato** e **LDAP** possono anche essere esportati in un file CSV insieme ad altri dettagli.

> Quando si aggiunge un utente con un valore di campo che contiene i caratteri +, -, = o @, i dati dell'utente nel file CSV esportato saranno automaticamente preceduti da una virgoletta singola (') e il simbolo pipe (|) sarà aggiunto con un backslash (\). Ciò avviene per prevenire la vulnerabilità di injection di Excel.

6.7.14. Assegnazione di attributi personalizzati agli utenti

È possibile assegnare attributi personalizzati, come Reparto, a uno o più utenti. Ciascun attributo dispone di un valore che è possibile utilizzare per attività quali la creazione di configurazioni e gruppi di utenti. È possibile assegnare attributi personalizzati a uno o più utenti.

Procedura

1. Andare su **Amministratore > Sistema > Attributi** per creare nuovi attributi personalizzati, se necessario.
2. Andare a **Utenti**.
3. Selezionare uno o più utenti.
4. Fare clic su **Azioni**.
5. Selezionare **Assegna attributi personalizzati**.
6. Selezionare una delle seguenti opzioni:
    - Consente di forzare l'assegnazione (la sovrascrittura) di tutti gli attributi, anche in presenza di valori esistenti.
    - Consente di sovrascrivere solo se il valore è vuoto e di ignorare gli attributi con valori esistenti.

Selezionare gli attributi che si desidera assegnare e immettere i relativi valori (non sono consentiti campi vuoti).

8. Fare clic su **Assegna**.

Argomenti correlati:

- Attributi
- Variabili

6.7.15. Rimozione di attributi personalizzati dagli utenti

È possibile rimuovere attributi personalizzati da uno o più utenti.

> Si tenga presente che questa azione non può essere annullata.

Procedura

1. Andare a **Utenti**.
2. Selezionare uno o più utenti.
3. Fare clic su **Azioni**.
4. Selezionare **Rimuovi attributi personalizzati**.
5. Selezionare gli attributi da rimuovere.
6. Fare clic su **Rimuovi**.

Argomenti correlati:

- Attributi
- Variabili

6.7.16. Modifica delle impostazioni locali degli utenti

Per impostazione predefinita, il locale dell'utente è impostato sul locale del tenant. Se necessario, è possibile modificare il locale per un singolo utente.

Procedura

1. Andare a **Utenti**.
2. Fare clic sul nome visualizzato dell'utente.
3. Fare clic su **Modifica**. Viene visualizzata la finestra **Autenticazione richiesta**.
4. Immettere la password dell'amministratore e fare clic su **Autentica**.

> Quando vengono inserite più voci errate della password e se viene superato il "limite dei tentativi non riusciti" impostato nell'opzione "Impostazioni complessità della password", l'account verrà bloccato e l'utente verrà disconnesso dalla sessione corrente.

5. Nel campo Impostazioni locali, fare clic su **Cambia**.
6. Nella finestra **Cambia locale utente**, selezionare il locale richiesto dall'elenco a discesa **Cambia locale utente in:**.
7. Fare clic su **Fine**.
8. Fare clic su **Salva**.

6.7.17. Modifica di un nome utente

Quando si aggiunge un utente, il testo inserito per l'indirizzo e-mail viene automaticamente utilizzato come nome utente. Nella maggior parte dei casi si consiglia di non modificare il nome utente predefinito poiché:

- È richiesto un nome utente nel formato di indirizzo e-mail.
- È consigliabile utilizzare la **variabile** del nome utente nelle configurazioni, ma è possibile utilizzare anche l'indirizzo e-mail.

La modifica del nome utente può verificarsi unicamente nel raro caso di conflitto tra i nomi utente, poiché è necessario che ogni nome utente sia univoco in tutto il sistema di gestione dei dispositivi. Un conflitto potrebbe verificarsi, ad esempio, nel caso in cui due dipartimenti facenti parte di un'unica azienda si iscrivano al sistema di gestione dei dispositivi.

Se si verifica un conflitto tra nomi utente

Se non è possibile aggiungere un utente a causa di un conflitto tra nomi utente, inserire un nome utente diverso utilizzando il formato dell'indirizzo e-mail. L'indirizzo e-mail non deve corrispondere a un account e-mail reale. Ad esempio, è possibile cambiare il seguente indirizzo e-mail:

ksmith@mycompany.com

a

ksmith21@mycompany.com

Se si modifica il nome utente, qualsiasi configurazione che include il nome utente come variabile non funzionerà per il relativo utente. In alternativa, creare configurazioni alternate che utilizzano la variabile dell'indirizzo e-mail.

6.7.18. Interruzione della raccolta di dati sulla posizione

Argomenti della sezione:

- Per dispositivi iOS
- Per dispositivi Android

Se viene applicata una configurazione della privacy per abilitare la raccolta dei dati sulla posizione, l'utente del dispositivo può annullare la configurazione.

Per dispositivi iOS

Gli utenti di dispositivi iOS possono disattivare i servizi di localizzazione per impedire l'invio dei dati sulla posizione al sistema di gestione del dispositivo dalla seguente impostazione:

Impostazioni > Privacy > Servizi di posizione

Per dispositivi Android

Gli utenti di dispositivi Android possono disattivare l'impostazione di localizzazione per impedire la raccolta dei dati sulla posizione. Il percorso dell'impostazione varia in base al produttore. Agli utenti di dispositivi Android viene chiesto di accettare la richiesta di raccolta di dati sulla posizione.

6.7.19. Informazioni sul timeout

Il timeout per inattività del portale amministrativo è compreso tra 5 e 60 minuti, mentre il timeout della sessione si verifica dopo 24 ore.

Procedura

1. Andare in **Utenti > Impostazioni utenti**.
2. Modificare le impostazioni predefinite **Complessità password**.
3. Nella sezione Policy delle password spostare il cursore **Timeout di inattività** per specificare il periodo di tempo per cui un utente può rimanere inattivo prima che si verifichi un timeout della sessione di un portale Amministratori o self-service. Il numero varia da 5 a 60 (minuti).
4. Fare clic su **Fine**.

6.7.20. Disattivazione dell'analisi di utilizzo del sistema

Vengono raccolti dati anonimi relativi alla diagnosi e all'utilizzo dei prodotti al fine di migliorare i prodotti.

Se si desidera che i dati di utilizzo rimangano riservati, è possibile rinunciare all'invio di dati analitici sull'utilizzo del sistema.

Procedura

1. Fare clic sul link **Dati utilizzo** in fondo alla pagina nel portale amministrativo Ivanti Neurons per MDM. Viene visualizzata la finestra **Dati di utilizzo**.
2. Rimuovere il segno di spunta dalla casella **Invia dati diagnostici e di utilizzo**.
3. Fare clic su **Salva**.

6.7.21. Registrazione dispositivo tramite generazione PIN

Argomenti della sezione:

- Per utenti singoli o multipli dalla pagina di destinazione utenti
- Per un singolo utente da Dettagli utente

È possibile generare PIN di registrazione del dispositivo per gli utenti senza inviare un'e-mail di invito, semplificando la procedura di registrazione del dispositivo.

Per utenti singoli o multipli dalla pagina di destinazione utenti

1. Andare in **Utenti** > **Utenti**.
2. Selezionare gli utenti per i quali si desidera generare un PIN di registrazione. È possibile selezionare uno o più utenti.
3. Fare clic sul pulsante **Azioni**.
4. Selezionare **Genera PIN** dal menu a discesa.
5. I PIN generati vengono visualizzati nella colonna **PIN DI REGISTRAZIONE**.
6. Per visualizzare i PIN, fare clic su **Visualizza PIN**.

Per un singolo utente da Dettagli utente

1. Andare in **Utenti** > **Utenti**.
2. Fare clic sul nome utente per il quale si desidera generare un PIN di registrazione per aprire i dettagli dell'utente.
3. Nella sezione Informazioni utente, fare clic su **Genera PIN**.
4. Fare clic su **Visualizza PIN** per visualizzare il PIN generato.

> Assicurarsi di avere le autorizzazioni appropriate per generare i PIN di registrazione per gli utenti. L'opzione Genera PIN è abilitata solo per gli utenti il cui stato di registrazione del dispositivo è "Password e PIN".

7. Dispositivi

Argomenti della sezione:

- Introduzione all'uso di dispositivi
- Gruppi di dispositivi
- Inventario delle applicazioni
- Gestione dei dispositivi

7.1. Introduzione all'uso di dispositivi

Argomenti della sezione:

- Gestione dei dispositivi
- Esecuzione di azioni su un dispositivo
- Impostazione fuso orario per un dispositivo
- Dispositivi elencati in base ai criteri
- Visualizzazione di informazioni dettagliate sul dispositivo
- Assegna in blocco o modifica utenti e attributi personalizzati per i dispositivi
- Esportazione di dispositivi in un file CSV
- Ricerca dei registri dei dispositivi

Ciascuna voce nella pagina **Dispositivi** rappresenta un dispositivo mobile registrato con Ivanti Neurons per MDM e include informazioni importanti relative al dispositivo. La pagina Dispositivi visualizza i dispositivi con informazioni quali:

- Nome
- Indirizzo e-mail
- N. di telefono
- Sistema operativo
- Tipo di dispositivo
- Stato
- Ultimo check-in
- Conteggio violazioni
- Spazio
- Proprietario legale (per iPad condivisi)

L'indirizzo IP Wi-Fi viene segnalato al server Ivanti Neurons per MDM. Qualsiasi modifica dell'indirizzo IP viene segnalata a ogni check-in. L'opzione per l'indirizzo IP conforme al GDPR è disponibile nella pagina con l'elenco dei dispositivi e nei dettagli del dispositivo. Questa funzione richiede che i dispositivi siano registrati tramite Go 5.5 per iOS o versioni successive, e Go 72 per Android o versioni successive, come supportato da Ivanti Neurons for MDM.

> Poiché nelle nuove versioni di Ivanti Neurons per MDM sono stati aggiunti ulteriori campi correlati al GDPR (come Indirizzo IP e ID eSIM), gli amministratori che hanno già configurato le opzioni per il GDPR devono modificare il profilo GDPR, se desiderano nascondere i nuovi campi.

L'identificatore delle apparecchiature (EID) viene visualizzato come attributo IOS quando un elenco di dispositivi viene esportato nel formato foglio di calcolo (CSV). L'EID e l'EID per dispositivi mobili (MEID), quando presenti, sono precedute da una stringa EID o MEID, rispettivamente.

> Il server Ivanti Neurons per MDM non è in grado di gestire l'elaborazione dello stesso dispositivo con identificatori di client diversi e registrato su tenant differenti. Il server può gestire esclusivamente l'istanza in cui lo stesso dispositivo con identificatori di client diversi è registrato sullo stesso tenant.

Gestione dei dispositivi

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Andare su **Dispositivi**.
3. Selezionare uno o più dispositivi.
4. Selezionare un'azione dall'elenco a discesa **Azioni**.

La seguente tabella elenca le azioni disponibili dalla pagina Dispositivi:

Categoria	Azione
Comune	• Aggiungi al gruppo • Sblocco di AppConnect> • Assegna attributi personalizzati • **Assegna a utente** • Sincronizzazione stato di conformità dispositivo • Disattiva Desktop remoto • Attiva Desktop remoto • Attiva/Disattiva Bluetooth • **Forza il check-in** • **Blocca** • Rimuovi attributi personalizzati • Riavvia/Arresta • Sincronizzazione stato di conformità dispositivo • **Dismissione dispositivo** • **Invia messaggio** • Imposta proprietà • **Sblocca** • **Cancella**
iOS	• **Assegna al proprietario legale** (solo iPad condivisi) • Reinstalla app del sistema iOS • Imposta fuso orario
macOS	• Imposta password amministratore automatica per macOS • Imposta/modifica password del firmware • Imposta/Modifica blocco di ripristino
Android	• Passa in modalità tutto schermo • Esci dalla modalità tutto schermo
Windows	Script e azioni tramite Ivanti Bridge

Esecuzione di azioni su un dispositivo

Il menu Azioni (pulsante puntini di sospensione) consente di eseguire svariate azioni su un dispositivo selezionato.

Procedura

1. Fare clic sul nome di un dispositivo. Si apre la pagina Dettagli dispositivo.
2. In questa pagina, fare clic sul menu Azioni (puntini di sospensione) per eseguire una delle seguenti azioni del dispositivo:
    - Modifica nome dispositivo

- Elimina dispositivo
- Modifica appartenenza al gruppo
- Attiva/Disattiva Bluetooth
- Script e azioni tramite Ivanti Bridge
- Estrai registro di Ivanti Bridge
- Rinuncia alla proprietà
- Richiedi registri di debug
- Riavvia/Arresta dispositivo
- Ritira
- Imposta proprietà
- Imposta/Modifica blocco di ripristino
- Cancella
- Sincronizzazione stato di conformità dispositivo

Impostazione fuso orario per un dispositivo

Applicabile a: dispositivi iOS 14.0 e versioni successive e tvOS 14.0 e versioni successive

Questa azione non richiede servizi di localizzazione. L'azione di impostazione del fuso orario del dispositivo viene visualizzata anche nella pagina dettagli del dispositivo di un dispositivo. Le modifiche apportate al fuso orario nel dispositivo si rifletteranno anche sul Ivanti Neurons per MDMserver.

> Questa azione del dispositivo genera un errore se è attivata la restrizione **Forza data e ora automatiche** in Configurazione delle restrizioni per iOS.

Procedura

1. Selezionare uno o più dispositivi.
2. Fare clic su **Azioni** > **Imposta fuso orario** per i dispositivi selezionati.
3. Inserire la stringa del fuso orario nel formato ID fuso orario di Olson. Ad esempio, Pacific/ Midway.
4. Fare clic su **Imposta fuso orario**.

Dispositivi elencati in base ai criteri

È possibile utilizzare la barra di navigazione laterale Filtri per ricercare e visualizzare dispositivi specifici dall'intero elenco di dispositivi. Utilizzare l'elenco a discesa Spazio per selezionare tutti gli spazi o spazi specifici per visualizzare i dispositivi e le relative informazioni correlate. È possibile cercare utilizzando la versione visualizzata o la versione in bundle. La pagina Dispositivi mostra sia la versione in bundle sia la versione visualizzata dei dispositivi.

> Quando si naviga dalla pagina Gruppo di dispositivi e si fa clic sul numero elencato sotto la colonna **N. di dispositivi** o dalla colonna **#Installed** nella pagina **Inventario app**, viene visualizzato un messaggio che indica il nome dello spazio per il quale vengono elencati i dispositivi nella pagina.

Visualizzazione di informazioni dettagliate sul dispositivo

Fare clic sul collegamento nella colonna Nome di una voce per visualizzare la pagina Informazioni del dispositivo. La pagina Informazioni del dispositivo contiene diverse schede in cui sono disponibili le informazioni seguenti:

- **Panoramica** - La tabella seguente elenca tutti i dettagli visualizzati nella scheda Panoramica:
- **Configurazioni**: mostra i dettagli delle configurazioni applicate Per ulteriori informazioni, vedere **Utilizzo delle configurazioni**.

Nome sezione	Descrizione
Generale	• Posizione del dispositivo • Produttore • Indirizzo MAC Wi-Fi • Indirizzo IP Wi-Fi (dispositivi Android) • Condivisione della rete tramite Tethering (dispositivi iOS) • È dotato di batteria - (Solo per macOS 13.3+) • Indirizzo IP • Indirizzo IP pubblico - Visualizza l'indirizzo IP del dispositivo per Android o ChromeOS. Se il dispositivo si connette a un server VPN o proxy, mostra l'indirizzo IP WAN del proxy. • Numero di modello - (macOS 13.3+ e iOS 16.4+) • Numero di serie • Numero di serie alternativo (dispositivi Android): numero di serie specifico del fornitore e applicabile ai dispositivi Samsung nella modalità Amministratore del dispositivo o Proprietario dispositivo. • PIN di blocco - Gli amministratori possono bloccare in remoto un dispositivo gestito e generare un PIN univoco per sbloccarlo manualmente. Selezionare **Visualizza** per visualizzare il PIN nella pagina **Dettagli dispositivo** per gli utenti con privilegi di amministratore. Applicabile solo ai dispositivi macOS. • Utilizzo dello spazio di archiviazione: spazio di archiviazione interna utilizzato (tranne Windows) e disponibile sui dispositivi • Batteria disponibile (Android) • Stato batteria (Android) - In carica, In scaricamento, Piena e Non in carica • Carica rimanente batteria stimata (Windows) • Runtime batteria stimato (Windows) • Aggiornamento disponibile (macOS) • Nome aggiornamento disponibile (macOS) • Versione SO • Versione build sistema operativo • Versione di build supplementare • Sistema operativo/Versione supplementare Extra • Dispositivo con processore Apple • Versione firmware • Origine dispositivo • Proprietario legale • Modalità multiutente • Fuso orario • Ultimo passcode di sblocco dispositivo noto

Nome sezione	Descrizione
	• Modalità blocco sicurezza • Aggiornamento sistema (dispositivi Android) • Versione patch Zebra (dispositivi Android) • ID ultimo hotfix - (dispositivi Windows) • Data installazione ultimo hotfix - (dispositivi Windows) • Tipo di registrazione MDM • Ritorno in servizio MDM (iOS 27.0+ e visionOS 27.0+)
Impostazioni	• Nome dispositivo • Identificatore dispositivo • GUID dispositivo • Dispositivo Registrazione dispositivi (dispositivi Apple) • Registrazione Registrazione dispositivi (dispositivi Apple) • Automated Registrazione dispositivi abilitato • Registrato con Registrazione automatica dispositivo • Registrazione Registrazione utenti (dispositivi Apple) • Registrazione ID Apple gestito (dispositivi Apple) • Gruppi di dispositivi • Lingua • Identificatori dispositivo MDM • ID client dispositivi • Versione dell'applicazione client • BundleID dell'applicazione del client • Client registrato • Identificatori dispositivo EAS • Blocco attivazione abilitato • Gestione dichiarativa Apple abilitata • App Apple DDM abilitata • Codice bypass di Blocco attivazione • Termini di servizio • Proprietà • Account iTunes attivo • Servizio di localizzazione dispositivo abilitato • In quarantena • Sentry bloccato • Accesso bloccato

Nome sezione	Descrizione

	• Azione di conformità bloccata
	• Supporto APNS
	• Modalità di supervisione (dispositivi iOS e macOS) - Identifica un dispositivo supervisionato. Il dispositivo rimane sotto il controllo diretto del team IT. La modalità di supervisione consente ulteriori funzioni sul dispositivo (ad esempio, distribuzioni di servizi sul campo, dispositivi Point-Of-Sale al dettaglio), dispositivi "in prestito" utilizzati nei settori dei servizi e dell'ospitalità e dispositivi condivisi tra studenti nei laboratori.
	• Cancella PIN - Fare clic su **Visualizza** per visualizzare il PIN.
	• Utente amministratore macOS gestito (dispositivi macOS)
	• Password amministratore macOS locale (dispositivi macOS) - Selezionare **Visualizza**, per vedere le informazioni **Password amministratore**, **Ultima rotazione password**, **Prossima rotazione** e **Motivo** sui dispositivi registrati e gestiti mediante Registrazione automatizzata dispositivi.
	Dopo che l'amministratore ha visualizzato la password, potrebbe essere necessaria un'altra ora (al prossimo check-in) affinché la password venga ruotata dall'orario **Prossima rotazione** mostrato.
	• Stato di cifratura del dispositivo (dispositivi macOS)
	  ◦ Abilitata crittografia di FileVault
	  ◦ Utilizzata chiave di ripristino personale
	  ◦ Utilizzata chiave di ripristino istituzionale
	• Token bootstrap disponibile
	• Protezione di integrità del sistema attivata
	• Password firmware
	  ◦ Password
	  ◦ Modifica in sospeso
	  ◦ Stato comando
	  ◦ Consenti ROM opzione
	• Blocco di ripristino
	  ◦ Password
	  ◦ Blocco di ripristino abilitato
	• Script via Mobile@Work per macOS
	• Impostazioni del firewall (dispositivi macOS)
	  ◦ Firewall attivato
	  ◦ Blocca tutti gli elementi in ingresso
	  ◦ Modalità mascheramento
	• Stato del firewall dell'applicazione (dispositivi macOS)
	• Stato del firewall (dispositivi Windows)
	• Ultimo backup su iCloud (dispositivi iOS)

Nome sezione	Descrizione
	• Periodo di tolleranza per il blocco del passcode (dispositivi iOS) • ID Android • Livello di patch di sicurezza di Android (dispositivi Android) • Modalità tutto schermo (dispositivi Android) • Tipo di attestazione SafetyNet di Android (dispositivi Android) • Compatibile con Android Enterprise (dispositivi Android) • Android for Work abilitato (dispositivi Android) • Compatibile con Samsung SAFE (dispositivi Android) • Dispositivi di lavoro gestiti Android (proprietario del dispositivo) abilitati • Profilo di lavoro Android su dispositivo di proprietà dell'azienda abilitato • Stato nativo anti-phishing • Stato anti-phishing • Stato VPN anti-phishing • Dispositivo gestito Android con profilo di lavoro • Blocco del Profilo di lavoro Android su dispositivo di proprietà dell'azienda abilitato • Help@Work disponibile • Abilitato per Zebra • Stato Secure Apps • Stato crittografia Secure Apps • Modalità di crittografia applicazioni protette • FCM abilitato • Stato attivazione MTD
Protezione delle informazioni di Windows (dispositivi Windows)	• WIP • Raccoglitore app configurato • Impostazioni EDP obbligatorie
Telefonia	**Sottoscrizioni ai servizi del dispositivo** • Numero di telefono • Tecnologia cellulare • IMSI • ICCID • IMEI • IMEI 2 - (Solo su dispositivi Android con porta per doppia SIM, applicabile ad Android 8.0 e versioni successive) • MEID • Posizione del dispositivo

Nome sezione	Descrizione
	• Gestore telefonico • MCC nazionale • MNC nazionale • Nome paese attuale • Nome paese principale • Tecnologia cellulare • Roaming • Operatore attuale • MCC attuale • MNC attuale • Roaming dati • Chiamate in roaming • EID - (applicabile per i dispositivi Android supportati) **Abbonamenti al servizio SIM** - (applicabile per i dispositivi iOS supportati) Per i dispositivi iOS supportati, queste proprietà sono visualizzate per più sottoscrizioni al servizio attivo eSIM. • Versione impostazione gestore telefonico • Rete impostazione gestore telefonico • MCC attuale • MNC attuale • EID • ICCID • IMEI • Dati preferiti • Voce preferita • Etichetta • ID etichetta • Numero di telefono • Slot SIM • È Roaming • Rete gestore telefonico sottoscrittore **Abbonamenti al servizio SIM** - (applicabile per i dispositivi Android supportati) Per i dispositivi Android supportati, queste proprietà sono visualizzate per più sottoscrizioni al servizio attivo. • Versione impostazione gestore telefonico • MCC attuale • MNC attuale

Nome sezione	Descrizione
	• ICCID • Dati preferiti • Voce preferita • ID abbonamento • Numero di telefono • Slot SIM • È incorporato • È gestito
Conformità dispositivo Azure	• Identificatore dispositivo Azure • Stato di conformità dispositivo Azure • Codice stato client Azure • Ora report di conformità dispositivo Azure • UPN utente dispositivo Azure Intune
Conformità dispositivi Google BeyondCorp	• Identificatore dispositivo • Stato conformità • Ora report conformità • Utente
Informazioni batteria	• Livello batteria - Visualizza il livello di carica della batteria corrente come segnalato dal sistema operativo Android • Stato integrità batteria - Come segnalato dai dispositivi con sistema operativo Android, Mac, iOS e iPad. • Stato carica batteria - Come segnalato dal sistema operativo Android • Percentuale integrità batteria (specifico per OEM) - Integrità batteria in percentuale per i produttori di dispositivi supportati come i dispositivi Zebra • Data di produzione batteria (OEM) - Dat di produzione della batteria per i produttori di dispositivi supportati come i dispositivi Zebra • Cicli di carica della batteria (OEM) - Numero di cicli completati in totale per i produttori di dispositivi supportati come i dispositivi Zebra
Integrità dei componenti del dispositivo (applicabile per dispositivi supervisionati iOS 27.0+ e macOS 27.0+)	• **Banda base**: indica lo stato di integrità della banda base del dispositivo. • **Videocamera**: indica lo stato di integrità della videocamera del dispositivo. • **Display**: indica lo stato di integrità del display del dispositivo. • **Face ID**: indica lo stato di integrità Face ID del dispositivo. • **Near Field**: indica lo stato di integrità della Comunicazione near field (NFC) del dispositivo. • **Touch ID**: indica lo stato di integrità Touch iD del dispositivo. • **Banda ultra larga**: indica lo stato di integrità della banda ultra larga del dispositivo.

- **App installate** - Visualizza i dettagli delle applicazioni installate sul dispositivo. La data di installazione della versione corrente dell'app installata viene visualizzata nella colonna **Data segnalazione app**. Ricercare le app installate per il dispositivo come indicato di seguito:
- Nome app
- ID bundle o pacchetto

> La data di installazione delle app dei dispositivi rimossi dalla quarantena è la data di fine della quarantena.

> Nel caso dei dispositivi Android Enterprise, è possibile visualizzare i dettagli di utilizzo delle app installate ordinati per giorno, settimana, mese o anno. Per visualizzare questi dettagli, è necessario aver selezionato l'opzione **Abilita raccolta dati utilizzo app** disponibile nella sezione **Impostazione configurazione** e quindi è possibile selezionare le opzioni **Utilizzo app - giorno**, **Utilizzo app - settimana**, **Utilizzo app - mese**, **Utilizzo app - anno** per visualizzare i dettagli sull'utilizzo delle app.

- **App disponibili** - Visualizza i dettagli delle applicazioni disponibili per il dispositivo. Ricercare le app disponibili per il dispositivo come indicato di seguito.
- Nome app
- ID bundle o pacchetto

Nella colonna **Configurazioni app**, quando si seleziona **Nome configurazione**, si viene indirizzati alla scheda **Configurazione app** del catalogo app per esaminare le opzioni di configurazione app. Se necessario, è possibile modificare le configurazioni dell'app per il dispositivo nella pagina **Riepilogo configurazioni app**. Per ulteriori informazioni sulla configurazione di un'app, vedere **Configurazione dell'app**.

Nella colonna **Configurazioni app**, quando si seleziona **Nome configurazione**, si viene indirizzati alla scheda **Configurazione app** del catalogo app per esaminare le opzioni di configurazione app. Se necessario, è possibile modificare le configurazioni dell'app per il dispositivo nella pagina **Riepilogo configurazioni app**. Per ulteriori informazioni sulla configurazione di un'app, vedere **Configurazione dell'app**.

> Assicurarsi di ricordare il nome e il tipo di configurazione dell'app specifica per il dispositivo assegnato nella pagina **Configurazioni app**.

> La colonna **Stato** indica lo stato di installazione dell'applicazione sul dispositivo. Lo stato di installazione delle app viene acquisito solo per le applicazioni gestite. Lo stato di installazione delle applicazioni non gestite viene visualizzato come Non installato. È necessario convertire l'applicazione in Gestita per visualizzare lo stato di installazione corretto.

- **App AppConnect** - Dettagli sulle app AppConnect installate.
- **Criteri** - Dettagli sui criteri applicati. Per i dispositivi compromessi, verificare la motivazione della violazione nella colonna Violazione. Se è stata violata la root del dispositivo, il sistema visualizza la motivazione riportata nella colonna **Violazione**:

Priorità (1 = più elevata)	Violazione
1	Plugin compromesso
2	Client manomesso
3	Produttore dispositivo sconosciuto: sconosciuto
4	Rilevata cartella sospetta: [percorso]
5	File binario sospetto trovato in: [percorso]
6	Cartella/dati sfogliabili O cartella /dati/dati sfogliabili
7	Trovato/sistema/app/Superuser.apk
8	Gestione pacchetto compromessa
9	Trovata app sospetta: [pacchetto]

- **Certificati**: dettagli dei certificati installati.
  Per l'utilizzo del certificato, controllare la colonna Tipo di utilizzo. Se il certificato è specifico per dispositivo, viene visualizzato il tipo "dispositivo". Se il certificato è specifico per utente, viene visualizzato il tipo "utente".
- **Sentry** - Informazioni su Sentry (associazioni ActiveSync)
- **Attributi** - Attributi personalizzati e attributi del dispositivo
- **Utenti**: mostra l'elenco degli utenti attivi per dispositivo macOS supervisionato.

> La scheda **Utenti** è stata migliorata e mostra l'ID apple gestito come collegamento ipertestuale. Se si fa clic su di esso, si viene reindirizzati alla pagina dei dettagli dell'account utente in iPad condiviso.

- **Registri** - Visualizza e personalizza i filtri del dispositivo. È possibile eseguire le seguenti operazioni dai Filtri:
  - Selezionare il nome dell'azione per filtrare i dispositivi in base alle azioni dell'applicazione.
  - Selezionare lo stato.
  - Specificare la data di inizio e la data di fine.
- **Hardware**: dettagli dell'inventario hardware (sistema, scheda madre, BIOS, disco rigido, CD ROM, processore e memoria fisica)

Assegna in blocco o modifica utenti e attributi personalizzati per i dispositivi

È possibile utilizzare l'opzione Assegnazione in blocco tramite l'icona Carica per caricare un file CSV al fine di assegnare o modificare utenti e/o attributi personalizzati per i dispositivi in blocco.

Procedura

1. Dalla pagina Dispositivi, fare clic sull'icona **Assegnazione in massa tramite upload** (accanto al pulsante Azioni).
2. (Facoltativo) Fare clic su **Scarica modello** per salvare un file di un modello CSV che è possibile modificare e caricare.
3. Una volta pronto il file CSV, fare clic su **Scegli file** per passare alla posizione del file CSV oppure trascinare e rilasciare il file CSV nella sezione dati del file.
4. Selezionare una delle seguenti opzioni:

- **Forza l'assegnazione (la sovrascrittura) di tutti gli attributi, anche in presenza di valori esistenti**
- **Sovrascrivi solo se il valore è vuoto e ignora gli attributi con valori esistenti**

Fare clic su **Carica**.

Esportazione di dispositivi in un file CSV

È possibile esportare i dettagli dei dispositivi di un dispositivo specifico usando l'opzione **Esporta in CSV** dalla pagina **Dispositivi**.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare tutti o più spazi per visualizzare le informazioni correlate a spazi specifici.
3. Fare clic sul collegamento di conteggio dei dispositivi. Viene visualizzata la pagina Elenco dispositivi correlata allo spazio selezionato.
4. Fare clic sull'opzione **Esporta in CSV** per esportare l'elenco di dispositivi e i dettagli correlati in un file CSV. Viene visualizzato un messaggio pop-up che informa che l'elaborazione del report di esportazione richiederà del tempo. Attendere il completamento della richiesta prima di inviarne un'altra. Una volta che il report è pronto, all'utente verrà mostrato un messaggio per scaricare o eliminare il report.
5. Fare clic su **Download**. Si riceverà anche un'e-mail contenente un link per scaricare il report.
6. (Opzionale) Fare clic su **Elimina** per eliminare il report.

Ricerca dei registri dei dispositivi

Procedura

1. Passare a **Dispositivi** > **Dispositivi**, fare clic sul collegamento della colonna **Nome** di una voce.
2. Fare clic sulla scheda **Registri**.
3. Utilizzare i filtri Azione, Stato, Data di inizio e Data di fine per restringere i dispositivi visualizzati. È possibile eseguire le seguenti operazioni dai Filtri:
    1. Selezionare il nome dell'azione per filtrare i dispositivi in base alle azioni dell'applicazione.
    2. Selezionare lo stato.
    3. Specificare la data di inizio e la data di fine.
4. La colonna Dettagli dispositivo visualizza lo stato dell'applicazione come segue:
   Per tutti i dispositivi lo stato mostra i seguenti dettagli:
    - Nome app, versione app, bundle o ID del pacchetto
    - Stato dell'installazione
    - Eventuali errori e motivo dell'errore
      Ad esempio - appOrConfigName=Nome:<app name>;Identificatore=<bundleid>;iTunesStoreId:<itunesid>;Stato:<status or error reason from Apple>versione: <app version>

Per tutti i dispositivi Windows lo stato mostra i seguenti dettagli:

- Includere l'ID del bundle o del pacchetto, lo stato e gli errori
  Ad esempio -
- Per il tipo - inventario e stato dell'applicazione - conferma - visualizza - appType

- Per il tipo - inventario e stato dell'applicazione - invio - Non visualizza nulla
- Per il tipo - installazione/disinstallazione e lo stato - riuscita/non riuscita/invio - visualizza l'ID del bundle o del pacchetto, lo stato, il nome, la versione e gli errori

Se non è possibile visualizzare la pagina **Dispositivi**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione dispositivi
- Dispositivo di sola lettura

7.2. Gruppi di dispositivi

Argomenti della sezione:

- Aggiunta di un gruppo di dispositivi
- Rimozione di un gruppo di dispositivi
- Esportazione di dispositivi in un file CSV
- Assegna attributi personalizzati a gruppi di dispositivi

Nella pagina **Gruppi di dispositivi**, è possibile creare elenchi di dispositivi da trattare nello stesso modo. È possibile definire e assegnare criteri e configurazioni ai gruppi di dispositivi. I seguenti rappresentano i gruppi di dispositivi predefiniti creati da Ivanti Neurons per MDM:

- Tutti i dispositivi
- Dispositivi Android
- Dispositivi Android enterprise
- Dispositivi iOS
- Tipo di dispositivo (Apple)
- Dispositivi tvOS
- Dispositivi macOS
- Dispositivi visionOS
- Dispositivi watchOS
- Dispositivi Windows

I dettagli delle app assegnate a un gruppo specifico di dispositivi vengono visualizzati nella scheda **App** del gruppo di dispositivi specifico.

Aggiunta di un gruppo di dispositivi

> L'aggiunta di un gruppo di dispositivi non è applicabile ai gruppi di utenti dinamici.

A seconda del tipo di licenza di cui si dispone, è possibile aggiungere un nuovo gruppo di dispositivi basato su regole per identificare i dispositivi con criteri specifici. I dispositivi che soddisfano le regole vengono visualizzati sotto la sezione Generatore di regole. Le regole possono essere nidificate insieme utilizzando le opzioni QUALSIASI (OR) o TUTTO (AND). Le regole possono essere costruite utilizzando i seguenti operatori:

- inizia con
- termina con
- contiene
- non contiene
- non inizia con
- non termina con
- è inferiore a

- è superiore a
- è compreso nell'intervallo
- è uguale a
- non è uguale a
- non è vuoto
- è vuoto

Il portale amministratore di Ivanti Neurons per MDM visualizza il numero di gruppi di utenti duplicati e il numero corrispondente di GUID per identificare gruppi duplicati quando si seleziona l'attributo Nome gruppo di utenti nel Generatore di regole. Inoltre, una tabella sotto questa regola visualizza l'elenco di gruppi di utenti duplicati e i relativi dettagli, ad esempio Nome gruppo di utenti, GUID, Origine e Nome distinto (DN).

Licenza Bronze:

Le regole consentono di identificare i dispositivi mediante i criteri seguenti:

- Tipo di dispositivo
- SO: sistema operativo (precompilato)
- Versione SO
- Sistema operativo con versione
- Gruppo di utenti

Licenza Silver:

Le regole consentono di identificare i dispositivi mediante i criteri seguenti:

- Entra ID registrato
- Numero di serie alternativo (solo Android, applicabile ai dispositivi Samsung nella modalità Amministratore del dispositivo o Proprietario dispositivo)
- Dispositivi dedicati Android
- Compatibile con Android enterprise
- Dispositivo gestito Android con profilo di lavoro
- Tipo di attestazione SafetyNet di Android
- Android for Work abilitato
- Livello di patch di sicurezza di Android (dispositivi Android)
- Dispositivi di lavoro gestiti Android (proprietario del dispositivo) abilitati
- Profilo di lavoro Android abilitato
- Profilo di lavoro Android su dispositivi di proprietà dell'azienda abilitato
- Stato nativo anti-phishing
- Stato anti-phishing
- Stato VPN anti-phishing
- Supporto APNS
- Dispositivo con processore Apple
- Automated Registrazione dispositivi abilitato

- Registrato con Registrazione automatica dispositivo
- Identificatore dispositivo Azure
- Stato di conformità dispositivo Azure
- Codice stato client Azure
- Ora report di conformità dispositivo Azure
- Stato di integrità banda base
- Crittografia BitLocker
- Sentry bloccato
- Accesso bloccato
- Token bootstrap disponibile
- Tipo di provisioning in blocco (Configuratore Apple o Nessuno)
- Gestore telefonico
- Stato integrità videocamera
- Ultimo check-in del client
- Client registrato
- Conformità
- Azione di conformità bloccata
- Nome paese attuale (selezionare il nome del paese attuale dall'elenco a discesa)
- MCC attuale
- MNC attuale
- Attributo dispositivo personalizzato
- Attributo LDAP personalizzato
- Attributo utente personalizzato
- Roaming dati
- Nome dispositivo
- Dispositivo registrato
- Origine dispositivo
- Tipo di dispositivo
- Nome visualizzato
- Visualizza stato di integrità
- Crittografia abilitata
- Stato integrità Face ID
- Partizioni del disco rigido
- Nome paese principale (selezionare il nome del paese principale dall'elenco a discesa)
- MCC nazionale
- MNC nazionale
- IMEI

- IMEI2 (solo su dispositivi Android con doppia porta SIM e applicabile a dispositivi Android 8.0 o superiori)
- Chiave recupero istituzionale abilitata
- Indirizzo IP
- Modalità tutto schermo
- Ultimo check-in
- Solo MAM
- Produttore
- Tipo di registrazione MDM
- Ritorno in servizio MDM (iOS 27.0+ e visionOS 27.0+)
- Modalità multiutente (iOS 27.0+)
- Stato attivazione MTD
- Stato di integrità NFC
- Sistema operativo
- Versione build sistema operativo
- Edizione sistema operativo
- Versione SO
- Sistema operativo con versione
- Proprietà
- N. di telefono
- Indirizzo IP pubblico (dispositivi Android o ChromeOS)
- Chiave di recupero personale abilitata
- In quarantena
- Blocco di ripristino abilitato
- Roaming
- Stato Secure Apps
- Modalità blocco sicurezza
- Numero di serie
- Stato
- Supervisionato
- Versione sistema
- Capacità totale del dispositivo
- Memoria totale MB
- Versione TPM
- Toccare stato integrità ID
- Token di sblocco disponibile (iOS)
- Registrazione utenti abilitato
- Gruppo di utenti`

- Stato di integrità radio a banda ultra larga
- Chiamate in roaming
- Chiave di ripristino personale macOS depositata
- Tipo chiave di ripristino macOS

Procedura

1. Fare clic su **Aggiungi**.
2. Inserire un nome per il gruppo.
3. Inserire una descrizione opzionale per il gruppo.
4. Selezionare il tipo di gruppo di dispositivi che si desidera creare.
   - **Gestione dinamica**: consente di utilizzare le regole per definire i dispositivi da inserire nel gruppo.
     - **Carica da Ricerca avanzata**: selezionare questa opzione per aprire una libreria delle ricerche salvate. La scelta di una query popolerà in automatico il nome del gruppo di dispositivi e i criteri delle regole in base alla ricerca selezionata.

     > È possibile creare e salvare queste query navigando in **Dispositivi** > **Dispositivi** > **Ricerca avanzata**. Qualsiasi query salvata sarà automaticamente disponibile per il caricamento qui.

   Gestione manuale: consente di inserire gli utenti i cui dispositivi devono essere inclusi nel gruppo.
5. Per i gruppi gestiti dinamicamente:
   1. Creare una regola che definisca il gruppo.
   2. **Ad esempio**: il sistema operativo è iOS
      Fare clic su **+** per creare altre regole, se necessario.
   3. **Ad esempio**: il dispositivo è iPhone 5S
      Fare clic su **Qualsiasi** se è necessario che i dispositivi soddisfino almeno una delle regole.
   4. Fare clic su **Tutte** se è necessario che i dispositivi soddisfino tutte le regole.
6. Per i gruppi gestiti manualmente:
   1. Digitare il nome dell'utente di cui si desidera aggiungere il dispositivo.
   2. Selezionare il dispositivo dall'elenco visualizzato.
   3. Ripetere i passaggi a e b finché non sono presenti tutti i dispositivi nell'elenco.

Fare clic su **Salva**.

Rimozione di un gruppo di dispositivi

Procedura

1. Andare a **Dispositivi** > **Gruppi di dispositivi**.
2. Fare clic sulla casella del gruppo di dispositivi che si desidera rimuovere.
3. Fare clic su **Elimina gruppo di dispositivi**.

Esportazione di dispositivi in un file CSV

È possibile esportare i dettagli dei dispositivi di un gruppo specifico di dispositivi usando l'opzione **Esporta in CSV** dalla pagina **Gruppi di dispositivi**.

Procedura

1. Andare a **Dispositivi** > **Gruppi di dispositivi**.
2. Selezionare tutti o più spazi per visualizzare le informazioni correlate a spazi specifici.
3. Fare clic sul collegamento di conteggio del gruppo di dispositivi. Viene visualizzata la pagina Elenco dispositivi correlata allo spazio selezionato.
4. Fare clic sull'opzione **Esporta in CSV** per esportare l'elenco di dispositivi e i dettagli correlati in un file CSV. Viene visualizzato un messaggio pop-up che informa che l'elaborazione del report di esportazione richiederà del tempo. Attendere il completamento della richiesta prima di inviarne un'altra.
5. Fare clic su **Download**. Si riceverà un'e-mail contenente un link per scaricare il report.
6. (Opzionale) Fare clic su **Elimina** per eliminare il report.

Se non è possibile visualizzare la pagina **Gruppi di dispositivi**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli seguenti**:

- Gestione dispositivi
- Dispositivo di sola lettura

Assegna attributi personalizzati a gruppi di dispositivi

Gli amministratori possono ora assegnare attributi personalizzati direttamente ai gruppi di dispositivi. Qualsiasi dispositivo che diventa membro di un gruppo di dispositivi eredita in modo automatico i valori di attributo personalizzati configurati, eliminando la necessità di assegnare manualmente gli attributi ai singoli dispositivi dopo la registrazione. Utilizzare i gruppi di dispositivi per assegnare in modo automatico valori di attributo personalizzati ai dispositivi che diventano membri del gruppo.

Procedura

1. Andare a **Dispositivi** > **Gruppi di dispositivi**.
2. Selezionare un gruppo esistente o crearne uno.
3. Nella pagina Dettagli gruppo di dispositivi, fare clic su **Attributi**.
4. Fare clic su **Aggiungi nuovo**.
5. Scegliere l'attributo personalizzato e specificare il valore richiesto.

7.3. Dispositivi non gestiti

Argomenti della sezione:

- Blocco di un dispositivo
- Sblocco di un dispositivo
- Cancellazione di un dispositivo dall'elenco di dispositivi

Licenza: Silver

Se è stato configurato il controllo dell'accesso e-mail di Sentry, i dispositivi non registrati che eseguono l'accesso al sistema di posta elettronica in uso vengono denominati dispositivi non gestiti. Definire se i dispositivi non gestiti devono disporre dell'accesso e-mail per impostazione predefinita al momento della configurazione di un Sentry. Quindi, è possibile consentire o bloccare manualmente l'accesso e-mail per tali dispositivi.

> La pagina Dispositivi non gestiti viene aggiornata ogni 5 minuti. Pertanto, le modifiche apportate alla gestione non vengono visualizzate immediatamente.

Blocco di un dispositivo

Procedura

1. Selezionare il dispositivo.
2. Selezionare **Azioni > Blocca**.

Il dispositivo rimane bloccato finché non si seleziona **Azioni > Consenti** o **Azioni > Elimina**.

Sblocco di un dispositivo

Procedura

1. Selezionare il dispositivo.
2. Selezionare **Azioni > Consenti**.

Il dispositivo continua a disporre dell'accesso e-mail finché non si seleziona **Azioni > Blocca** o **Azioni > Elimina**.

Cancellazione di un dispositivo dall'elenco di dispositivi

Procedura

1. Selezionare il dispositivo.
2. Selezionare **Azioni > Elimina**.

Al successivo tentativo di accesso alle e-mail da parte del dispositivo, quest'ultimo verrà visualizzato nuovamente nell'elenco e sarà necessario ripetere l'azione Blocca o Consenti precedentemente applicata a tale dispositivo.

7.4. Inventario delle applicazioni

Argomenti della sezione:

- Come applicare filtri alla visualizzazione delle app
- Visualizzazione dei dispositivi installati per un'app
- Visualizzazione dell'elenco di app
- Visualizzazione delle applicazioni Win32 o Win32 Store installate su un dispositivo
- Creazione di un'autorizzazione di visualizzazione personalizzata
- Esportazione di un inventario app

L'inventario delle app è un elenco delle app rilevate sui dispositivi registrati. In quanto amministratore, è possibile utilizzare questa pagina per ottenere delle informazioni sulle app utilizzate dai dispositivi registrati. È possibile rispondere a domande come:

- Quali sono le app più popolari?
- I dispositivi iOS scaricano le app direttamente dall'App Store?
- Quanti utenti Android hanno scaricato un'{{app interna}} opzionale?
- Quanti dispositivi utilizzano una versione non aggiornata di un'app?

Come applicare filtri alla visualizzazione delle app

Nella pagina **Dispositivi > Inventario delle app**, vengono elencate tutte le app. Per restringere l'elenco a determinate app, utilizzare i filtri (riquadro a sinistra). Ad esempio, per restringere l'elenco in modo da visualizzare solo le app private di Google Play, selezionare **Privato** sotto la sezione **Origine**.

È possibile visualizzare l'inventario delle app nei dispositivi con tutti o più spazi selezionando più spazi dall'elenco a discesa. Quando si passa con il mouse sulle app visualizzate, viene visualizzato il numero dei dispositivi. È possibile fare clic sul numero di un'app per visualizzare tutti i dispositivi che contengono l'app. Ogni record dell'inventario delle app sarà raggruppato in base allo spazio.

È possibile effettuare ricerche utilizzando il Nome app o l'ID pacchetto/bundle.

Se sono stati selezionati più spazi, passando il mouse sul valore **Totale** nella colonna **# installazioni** si visualizza il conteggio delle installazioni per spazio del dispositivo.

Visualizzazione dei dispositivi installati per un'app

Fare clic sul numero **Gestiti**, **Non gestiti** o **Totale** elencato nella colonna **N. installati**.

Visualizzazione dell'elenco di app

Fare clic sulla voce **N. collegamenti richiesti** relativa all'app nell'inventario delle app per visualizzare i dispositivi che hanno richiesto l'app. Questa operazione si applica solo ai dispositivi Solo MAM.

Visualizzazione delle applicazioni Win32 o Win32 Store installate su un dispositivo

L'inventario app visualizza le app Win32 o Win32 Store su un dispositivo se la **configurazione della privacy** per quel dispositivo consente la raccolta di informazioni per tutte le app su quel dispositivo. È possibile configurare l'informativa sulla privacy per il dispositivo.

Procedura

1. Stabilire quale configurazione della privacy è valida per il dispositivo desiderato seguendo le istruzioni in **Dispositivi**.
2. Accedere a **Configurazioni**.
3. Per la configurazione della privacy registrata al passo 1:
    1. Selezionare la configurazione.
    2. Fare clic su Modifica.
    3. Sotto **Raccogli inventario app,** selezionare **Per tutte le app sul dispositivo**.
    4. Fare clic su **Fine**.

> Il CSP Win32AppInventory restituisce l'elenco di tutte le applicazioni Win32 e Win32 Store installate sul dispositivo ogni 24 ore dopo l'esecuzione delle scansioni di inventario sul dispositivo.

Creazione di un'autorizzazione di visualizzazione personalizzata

È possibile specificare le autorizzazioni di visualizzazione personalizzate per gli utenti.

Procedura

1. Andare in **Amministratore**.
2. Andare in **Gestione dei ruoli**.
3. Fare clic su **Aggiungi ruolo personalizzato**.
4. Selezionare l'opzione **Ruolo specifico per lo spazio**.
5. Immettere il nome utente nel campo **Nome**.
6. Nel menu **Dispositivi**, fare clic su **Inventario delle app**.
7. Selezionare la casella di controllo **Visualizza**.
8. Nel menu **Dispositivi**, fare clic su **Azioni relative ai dispositivi**.
9. Fare clic su **Salva**.
10. Andare in **Utenti** nel menu principale.
11. Fare clic sul nuovo utente creato.
12. Fare clic su **Assegna ruoli**.
13. Selezionare la casella di controllo **Specifico per lo spazio | app**, quindi fare clic su **Avanti**.
14. La pagina **Riepilogo** mostra le autorizzazioni assegnate al ruolo creato.
15. Fare clic su **Fine**.
16. Accedere come nuovo utente.
17. Fare clic su **Dispositivi** nel menu principale.
18. Fare clic su **Inventario delle app**.
19. La pagina **Inventario delle app** ora mostra solo le applicazioni consentite per l'utente.

Esportazione di un inventario app

In qualità di amministratore, è possibile richiedere i report dell'Inventario app mediante l'opzione **Esporta in CSV**.

Procedura

1. Passare a **Dispositivi > Inventario app**.
2. Selezionare un inventario dall'elenco.
3. Fare clic su **Esporta in CSV**.
4. Selezionare una delle seguenti opzioni:

- **Esporta app in CSV** per esportare tutte le applicazioni presenti nell'Inventario app.
- **Esporta dispositivi in CSV** per esportare un'applicazione specifica come da tabella seguente:

Opzione	Descrizione
ID bundle	Immettere l'ID bundle/pacchetto dell'applicazione.
Si desidera esportare	Selezionare una delle seguenti opzioni: • Totale installati • Gestito • Non gestiti • Richiesti (per dispositivi solo MAM)

5. Fare clic su **Esporta**.

All'amministratore verrà richiesto un pop-up che informa che il report di esportazione richiederà del tempo per essere elaborato. Dopo aver inviato la richiesta, l'amministratore deve aspettare che la richiesta sia completata per inviare un'altra richiesta. Una volta che il report è pronto, all'amministratore verrà mostrato un messaggio per scaricare o eliminare il report generato. L'amministratore riceverà anche un'e-mail contenente un link per scaricare il report.

Se non è possibile visualizzare la pagina **Inventario delle app**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione dispositivi
- Dispositivo di sola lettura

7.5. Gestione dei dispositivi

Argomenti della sezione:

- Distribuzione di dispositivi Windows
- Configurazione di Apple Remote Desktop su dispositivi macOS
- Registrazione del dispositivo (iOS, macOS e Android)
- Registrazione dei dispositivi (PC Windows versione 10 e successive e sistemi Microsoft Hololens 2)
- Registrazione dei pacchetti di provisioning con PIN
- Utilizzo della registrazione in blocco per i dispositivi Android
- Configurazione passcode
- Modifica del nome dispositivo
- Ricerca e applicazione di filtri ai dispositivi
- Utilizzo della modalità Proprietario del dispositivo
- Dispositivo gestito con profilo di lavoro
- Registrazione in blocco di dispositivi Android
- Registrazione in blocco utilizzando il caricamento file CSV
- Registrazione a Samsung Knox Mobile
- Registrazione di dispositivi Oculus
- Abilitazione di Bluetooth su un dispositivo
- Pianifica aggiornamento iOS
- Reinstallare le app del sistema iOS
- Assegnazione di un dispositivo a un nuovo utente
- Riassegnazione di un dispositivo Android
- Come forzare il check-in
- Individuazione di un dispositivo
- Blocco di un dispositivo
- Gestione dei dispositivi Apple in modalità smarrimento
- Richiesta registri di debug
- Disattivazione di un dispositivo
- Cessione della proprietà di un dispositivo
- Cancellazione di un dispositivo
- Eliminazione di dispositivi
- Sblocco di un dispositivo
- Riavvio o arresto dei dispositivi
- Cancellazione della password restrizioni (solo iOS)
- Eliminazione dell'associazione Sentry per un dispositivo
- Assegnazione di attributi personalizzati ai dispositivi

- Rimozione di attributi personalizzati dai dispositivi
- Sincronizzazione e recupero del feedback per un'app
- Impostazione della password del firmware
- Rilascio di una nuova chiave di ripristino personale
- Impostazione o modifica di un blocco di ripristino
- Gestione accessi Apple
- Registrazione criteri di gruppo

7.5.1. Distribuzione di dispositivi Apple

Ivanti Neurons for MDM supporta la gestione di tutti i dispositivi Apple. Si tratta di una soluzione completa per il provisioning, la gestione, l'aggiornamento e la sicurezza del parco macchine che offre all'utente finale la migliore esperienza d'uso.

Argomenti della sezione:

- Installazione del proprio certificato MDM Apple
- Registrazione di dispositivi Apple
- Ivanti Go per client iOS
- Gestione delle applicazioni per i dispositivi Apple
- Gestione delle configurazioni
- Gestione degli aggiornamenti software
- Impostazione dei dispositivi iOS/iPadOS
- Impostazione dei dispositivi watchOS
- Azioni del dispositivo supportate per i dispositivi watchOS
- Impostazione dei dispositivi visionOS
- Azioni del dispositivo supportate per i dispositivi visionOS
- Impostazione dei dispositivi macOS
- Impostazione dei dispositivi TvOS
- Supporto per la gestione dichiarativa dei dispositivi (DDM)

Installazione del proprio certificato MDM Apple

Al fine di gestire i dispositivi Apple, iniziare a richiedere e installare un certificato Apple MDM per gestire i dispositivi iOS. Rinnovare il certificato Apple MDM una volta all'anno. (L'account Apple utilizzato per creare il certificato riceve una notifica dal sito Apple quando la data di scadenza si avvicina). Usa la pagina del certificato MDM per aggiungere o rinnovare questo certificato.

Seguire i passaggi descritti in Installazione di un certificato MDM

Registrazione di dispositivi Apple

È possibile scegliere uno dei seguenti metodi per registrare i dispositivi:

- Registrazione dispositivi automatizzata
- Apple School Manager
- Apple Configurator

Ivanti Go per client iOS

Il passo successivo consiste nel selezionare il tipo di registrazione consentito dalla propria azienda per i propri dispositivi. Ivanti Neuros for MDM supporta attualmente:

- Registrazione del dispositivo (iOS, macOS e Android)
- Registrazione utenti con Apple Business Manager

- Registrazione degli utenti basata su account
- Impostazioni (Apple)

Gestione delle applicazioni per i dispositivi Apple

La pagina Catalogo app di Ivanti Neurons for MDM è un'interfaccia che consente agli amministratori di gestire in modo efficiente il proprio catalogo app. Questa funzionalità comprende l'orchestrazione delle applicazioni mobili disponibili per gli utenti finali, sia negli app store pubblici che in quelli destinati alla distribuzione tramite Ivanti Neurons for MDM.

App supportate:

La pagina Catalogo app aggrega vari tipi di app, tra cui le app dell'AppStore pubblico, le app personalizzate, le app sviluppate internamente, le app abilitate ad AppConnect, GoClient per iOS e M@W per macOS, semplificando la procedura di importazione per la successiva configurazione e distribuzione.

Sui dispositivi che operano solo con configurazioni Mobile Application Management (MAM), agli utenti iOS viene richiesto di selezionare un certificato di autenticazione quando accedono al Catalogo app. Questa fase di autenticazione è fondamentale per garantire l'accesso alle app elencate e per allinearsi a solide pratiche di sicurezza.

> I MacBook con chipset M1 di Apple offrono un supporto specializzato per le app VPP di iPhone e iPad all'interno di [il proprio prodotto software]. In particolare, solo gli amministratori hanno l'autorità di eseguire il push delle app VPP per iPhone e iPad supportate, impedendo agli utenti di installarle direttamente dall'app.

Per istruzioni dettagliate sull'implementazione e sulle opzioni di configurazione, consultare la documentazione completa disponibile nella Guida per l'amministratore e nelle risorse riportate di seguito:

- Gestione app
- Impostazioni catalogo app
- Configura Apple App e libri
- App Store Apps@Work aziendale
- Restrizioni dell'App Store di macOS

Gestione delle configurazioni

Le configurazioni sono delle raccolte di impostazioni che l'utente in quanto amministratore invia ai dispositivi. Ad esempio, è possibile utilizzare le configurazioni per specificare automaticamente le impostazioni VPN e i requisiti del passcode sui dispositivi. Le configurazioni esistenti del sistema in uso sono elencate nella pagina Configurazioni. È possibile selezionare più configurazioni nella pagina Configurazioni e inviarle a più dispositivi contemporaneamente. Tali configurazioni possono essere spinte ai dispositivi specifici degli spazi e i dispositivi negli altri spazi non ne sono influenzati. Le configurazioni possono essere inviate a un singolo spazio, a più spazi o a tutti gli spazi alla volta.

La maggior parte delle configurazioni di Ivanti Neurons for MDM è comune a tutte le piattaforme. Per ulteriori dettagli su come lavorare con le configurazioni, vedere Utilizzo delle configurazioni.

Alcune configurazioni sono supportate solo da piattaforme specifiche. È possibile rivedere l'elenco per piattaforma supportata su Tipi di configurazione

Gestione degli aggiornamenti software

È possibile iniziare impostando la configurazione di Aggiornamento software per i dispositivi iOS e MacOS.

> Quando si imposta una finestra programmata per l'aggiornamento del software, il comando di aggiornamento del sistema operativo verrà inviato ogni ora al dispositivo per assicurarsi che l'aggiornamento venga effettuato nei tempi previsti. Secondo il comportamento di Apple, ogni volta che il dispositivo riceve il comando di aggiornamento del sistema operativo, un pop-up avvisa l'utente di eseguire l'upgrade. L'utente può rinviare fino a tre volte. Alla terza volta, come previsto dal comportamento di Apple, il dispositivo imporrà l'upgrade.

I dispositivi MacOS hanno alcune regole specifiche che possono essere applicate. Vedere Configurazione delle regole di aggiornamento del software macOS

Comando di aggiornamento del sistema operativo per iOS

È anche possibile inviare un comando di aggiornamento una tantum a uno o più dispositivi dall'Elenco dispositivi o dalla Pagina dispositivi. Vedere Comando di aggiornamento del sistema operativo pianificato.

Impostazione dei dispositivi iOS/iPadOS

Le configurazioni seguenti sono supportate per iOS/iPadOS:

- **Limitazioni iOS/iPadOS**
- **Configurazione eSIM**
  - **Conserva piano dati**
- **Configurazioni rete mobile**
- **Abilita Modalità smarrimento**
- **Configurazione di un profilo MDM iOS**
- **Modalità App singola**
  - **Modalità app singola autonoma**
- **iPad condiviso per le aziende**
- **Configurazione formazione**
- **Configurazione personalizzata iOS**
- **Messaggio schermata di blocco**

Impostazione dei dispositivi watchOS

È ora possibile iscrivere i dispositivi Apple watchOS a Ivanti N-MDM durante l'associazione con i dispositivi iOS.

Questa funzione supporta attualmente: watchOS 10+.

ProcedureProcedura

1. È necessario registrare il dispositivo supervisionato iOS 17+.
2. Assegnare la configurazione della registrazione Apple Watch al dispositivo iOS.
3. Ora è possibile associare l'Apple Watch all'iPhone.

> È possibile associare l'Apple Watch dopo aver inviato la configurazione del Watch all'iPhone. Non è possibile abilitare la gestione remota per un Apple Watch se la configurazione del Watch viene inviata all'iPhone dopo che l'Apple Watch è stato associato con esso.

Le configurazioni seguenti sono supportate per i dispositivi watchOS:

- **Configurazione_rete mobile**
- **Configurazione dei certificati**
- **Trasparenza certificato**
- **Configurazione_certificato_identità**
- **Restrizioni iOS**
- **Impostazioni_passcode**
- **Configurazione_VPN_per-app**
- **Configurazione_Wi-Fi**

Azioni del dispositivo supportate per i dispositivi watchOS

Le azioni seguenti dei dispositivi sono supportate per i dispositivi watchOS:

- Cancella passcode
- Blocca Apple watch
- Cancella Apple watch
- Annulla registrazione Apple watch da Ivanti Neurons per MDM

> L'annullamento della registrazione del dispositivo iOS associato resetterà l'orologio e ne rimuoverà l'associazione con il dispositivo iOS.

Impostazione dei dispositivi macOS

Le configurazioni seguenti sono supportate per macOS:

- **Restrizioni di macOS**
- **Configurazione dei dispositivi macOS**
- **Lavorare con gli script e il client Mobile@Work**
- **Configurare un profilo MDM di macOS**
- **Impostazione della password del firmware**
- **Abilita FileVault**
  - **Chiave di ripristino di FileVault**
  - **Configurazione Opzioni FileVault**
- **Piattaforma e SSO estensibile**
- **macOS Active Directory**
- **Firewall**

- Ethernet
- Creazione account Office 365
- Estensioni di sistema macOS
- Limitazioni masterizzazione dischi supporto
- Impostazioni sulla privacy

Impostazione dei dispositivi TvOS

Le configurazioni seguenti sono supportate per tvOS:

- Configurazione di Apple TV
- Limitazioni Apple TV
- Visualizzazione Sala conferenze
- Mirroring di AirPlay

Impostazione dei dispositivi visionOS

È ora possibile registrare i dispositivi Apple visionOS in Ivanti Neurons per MDM.

Questa funzione supporta attualmente: visionOS 1.1+

È possibile registrare i dispositivi visionOS utilizzando uno dei seguenti metodi:

- Registrazione dispositivi guidata dall'account
- Registrazione degli utenti basata su account
- Registrazione dispositivo

Le configurazioni seguenti sono supportate per i dispositivi visionOS:

- Configurazione CalDAV
- CardDAV
- Configurazione dei certificati
- Configurazione della verifica della revoca dei certificati
- Trasparenza certificato
- Creazione della configurazione del proxy DNS
- DNS cifrato
- Configurazione delle e-mail
- Configurazione di Exchange
- Configurazione di Google
- Certificato di identità
- Restrizioni iOS
- Configurazione LDAP
- Domini gestiti
- Configurazione relay di rete

- Configurazione VPN per-app
- Configurazione Single Sign-On
- Configurazione del calendario sottoscritto
- Configurazione VPN
- Filtro contenuto Web
- Configurazione Wi-Fi

Azioni del dispositivo supportate per i dispositivi visionOS

Le azioni seguenti dei dispositivi sono supportate per i dispositivi visionOS:

- Cancella Apple Vision Pro
- Ritira Apple Vision Pro
- Sblocca Apple Vision Pro

Supporto per la gestione dichiarativa dei dispositivi (DDM)

La Gestione dichiarativa dei dispositivi di Apple è un protocollo di gestione moderno che consente ai dispositivi gestiti di applicare in modo proattivo e autonomo le proprie impostazioni di gestione con meno comunicazioni. La Gestione dichiarativa dei dispositivi viene attivata sui nuovi dispositivi registrati durante la registrazione o durante il check-in per i dispositivi già registrati.

La Gestione dichiarativa dei dispositivi è abilitata automaticamente sui seguenti dispositivi idonei:

- Computer con macOS 13 o versione successiva
- Dispositivi con iOS 16 o iPadOS 16 o successivo
- I dispositivi registrati tramite Registrazione utenti supportano la gestione dichiarativa dei dispositivi su iOS o iPadOS 15 o successivi.
- Dispositivi Apple TV con tvOS 16 o versione successiva
- Dispositivi Apple Watch con watchOS 10 o successivo
- Dispositivi Apple Vision Pro con visionOS 1.1 o successivo

Funzionalità di Gestione dichiarativa attualmente supportate:

- **Canali di stato**:
  - Modifiche alla versione del sistema operativo
  - Conformità passcode
  - Passcode presente
- **Configurazione**:
  - Configurazione di gestione dichiarativa

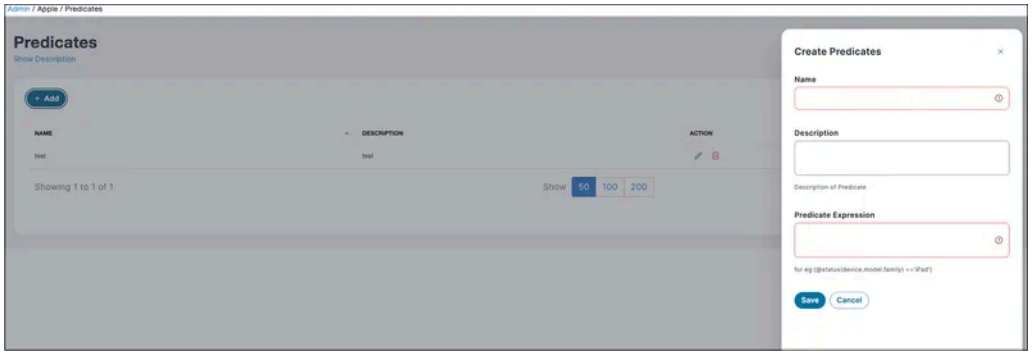
Predicati nelle configurazioni DDM

I predicati sono espressioni del linguaggio Cocoa che possono fornire flessibilità e granularità all'attivazione di una configurazione di un dispositivo. L'espressione risiede sul dispositivo e verrà applicata quando le condizioni di questo predicato sono soddisfatte. Abbiamo aggiunto una nuova funzione che consente di creare, salvare e applicare i predicati a qualsiasi configurazione DDM.

La configurazione del DDM visualizza una nuova opzione nella pagina Distribuzione per applicare un Predicato. I predicati già creati si trovano nell'elenco a discesa di questa sezione.

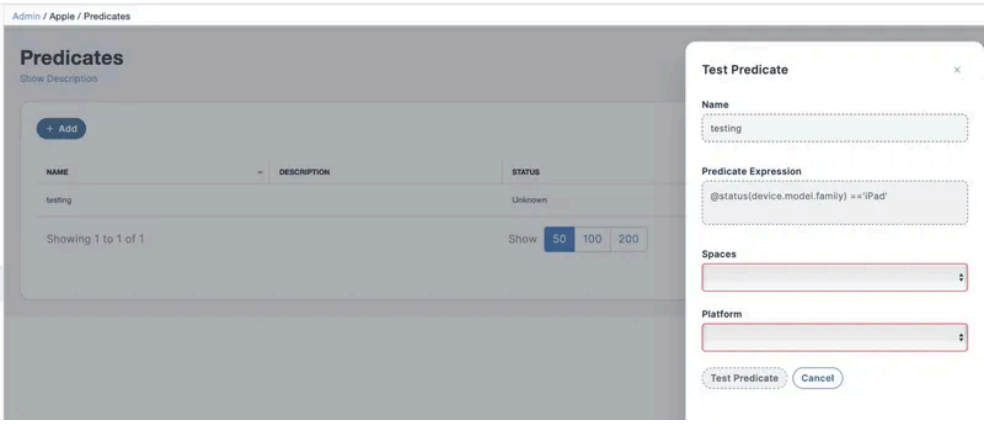
Creazione di un predicato

1. Andare in **Amministratore** > **Apple** > **Predicati**.
2. Fare clic su **Aggiungi**. Sullo schermo appare la finestra **Crea predicati**.
3. Immettere le informazioni seguenti:
   - **Nome** - Nome del predicato
   - **Descrizione** - Aggiungere una descrizione pertinente
   - **Espressione del predicato** - Espressione del predicato. Ad esempio, @status(device.model.family) =='iPad'



4. Fare clic su **Salva**. A schermo appare una finestra di dialogo che conferma la creazione del predicato.
5. Verificare la validità della sintassi del predicato aggiornando la pagina e osservando i valori nel campo STATUS (con i valori: **Sconosciuto**, **In corso**, **Valido**, **Non valido**).
   1. Fare clic su **Test**. Sullo schermo appare la finestra **Test predicato**.
   2. Immettere le informazioni seguenti:
      - **Nome** - Predefinito
      - **Espressione predicato** - Predefinito
      - **Spazi** – Spazio predefinito
      - **Piattaforma** – iOS/macOS
      - **Nome dispositivo** – Relativo all'espressione del predicato.

> Il campo **Nome dispositivo** apparirà sotto il campo **Piattaforma** solo dopo aver selezionato i dettagli dei campi **Spazi** e **Piattaforma** dai menu a discesa.



3. Fare clic su **Test predicato**.
4. A schermo appare una finestra di dialogo che conferma l'inizializzazione del test del predicato.
5. Aggiornare la pagina per trovare lo stato della sintassi del predicato.
    - Per un'espressione corretta del predicato, lo stato cambia da **Sconosciuto** > **In corso** > **Valido**.
    - Per un'espressione errata del predicato, lo stato cambia da **Sconosciuto** > **In corso** > **Non valido**.
6. Ripetere la procedura se si desidera creare più predicati utilizzando espressioni di predicato diverse.

Distribuzione dei predicati per una configurazione DDM

1. Creare una configurazione supportata dalla DDM.
2. Impostare l'interruttore "Attivazione con predicati" su ON e utilizzare i pulsanti + per includere i predicati (se necessario).



Per modificare o eliminare un predicato, andare in **Amministratore** > **Apple** > **Predicati**. L'elenco dei predicati disponibili è riportato in questa pagina. Fare clic su **Modifica** per apportare le modifiche al predicato esistente e salvarlo. Allo stesso modo, per eliminare un predicato esistente, selezionare il predicato e fare clic su **Elimina**.

> Non è possibile eliminare un predicato se è associato a una configurazione.

Proprietà di gestione per una configurazione DDM

L'amministratore può utilizzare quanto segue per creare i predicati:

- Variabili utente e dispositivo
- Attributi utente
- Attributi dispositivo

Esempio di utilizzo delle proprietà di gestione nei predicati (attributi personalizzati):

Predicato per verificare se il nome dell'utente è 'test' @property(userFirstName)=='test'

Altri esempi

- Famiglia hardware di un dispositivo: (Mac, iPhone, iPad, ecc.)
  @status(device.model.family) =='iPad'
  Se vero, sul dispositivo è presente un passcode. Se falso, sul dispositivo non è presente un passcode.
  @status(passcode.is-present)==true
- La famiglia del sistema operativo in uso sul dispositivo, come macOS o iOS.
  @status(device.operating-system.family)=='iPadOS'
- La versione del sistema operativo in uso sul dispositivo, come ad esempio 15.0
  @status(device.operating-system.version)=='18.2'
  @status(device.operating-system.version)<'18.3'
  @status(device.operating-system.version)>='18.2'
- Valore booleano che specifica lo stato di abilitazione del File Vault sul dispositivo
  @status(diskmanagement.filevault.enabled)==true
- Esempio di proprietà di gestione (attributi personalizzati):
  Predicato per verificare se il nome dell'utente è 'test'
  @property(userFirstName)=='test'

7.5.2. Distribuzione di dispositivi Windows

Argomenti della sezione:

- Panoramica
- Gestione dispositivi
- Iscrizione e registrazione dei dispositivi Windows
- Gestione aggiornamenti di Windows
- Gestione e distribuzione delle app
- Controllo app
- Configurazioni di gestione dispositivi Windows
- Conformità dei dispositivi Windows
- App Windows e inventario hardware

Panoramica

Ivanti Neurons for MDM aiuta a gestire tutti i portatili e i desktop Windows, incluso HoloLens 2, per la gestione del ciclo di vita del dispositivo end-end: dalla configurazione, l'iscrizione, il provisioning, la messa in sicurezza, l'applicazione, la gestione, il monitoraggio, gli aggiornamenti del software e del sistema operativo, fino al ritiro.

Gestione dispositivi

Dispositivi Windows supportati:

- Windows PC 10+
- Microsoft HoleLens 2

Per ulteriori informazioni sulla gestione dei dispositivi e sulla funzionalità di reporting, vedere Dispositivi

Iscrizione e registrazione dei dispositivi Windows

Ivanti Neurons per MDM supporta tutti i metodi di registrazione standard dei dispositivi Windows:

- Registrazione manuale
- Registrazione in blocco
- tramite SCCM e Ivanti EPM
- Windows Autopilot
- Registrazione Entra ID

Per ulteriori informazioni sui metodi di registrazione, vedere Utilizzo di Microsoft Azure

Per informazioni sul Supporto multi-utente, vedere Using_Microsoft_Azure.htm#Multi.

Gestione aggiornamenti di Windows

- Configurare e programmare gli aggiornamenti di Windows - Per configurare e programmare gli aggiornamenti di Windows, creare una configurazione usando Configurazione - Aggiornamenti software.

- Gestione aggiornamenti di Windows - È possibile visualizzare e approvare gli aggiornamenti segnalati dai dispositivi Windows che si desidera aggiornare tramite Gestione aggiornamenti di Windows. Utilizzando questa funzione, è possibile evitare che gli aggiornamenti che non sono necessari o non testati vengano installati sui dispositivi. Per ulteriori informazioni, vedere **Gestione aggiornamenti di Windows**.

Gestione e distribuzione delle app

Gli utenti possono gestire il ciclo di vita completo delle applicazioni (importazione, configurazione, pianificazione, distribuzione, aggiornamento e rimozione) per le applicazioni Windows.

Tipi di app supportate:

- In-house
- MSB
- Store pubblico

Estensioni app supportate:

- MSI
- MSIX
- APPX
- Bundle APPX
- EXE (Bridge)

Per maggiori dettagli sulla gestione delle applicazioni Windows, vedere **Configurazione dell'app**. Per automatizzare gli aggiornamenti delle app, vedere **Pianificazione delle app Windows** e **Utilizzo delle configurazioni**.

Controllo app

La configurazione Controllo app consente di classificare le app come "consentite" o "non consentite" a livello di dispositivo. Le app già installate non saranno visibili e non potranno essere avviate. Le app saranno ancora visibili nell'App Store, ma non sarà possibile scaricarle o avviarle. Qualsiasi dispositivo a cui venga distribuita la configurazione Controllo app la utilizzerà e ignorerà le impostazioni dei criteri App consentite. Questa configurazione Controllo app sostituirà eventuali criteri correlati alle app che si riferiscono alla stessa app sui dispositivi di destinazione.

Per maggiori dettagli, vedere **Configurazione del controllo delle app: controllo delle app installate per dispositivo**.

Configurazioni di gestione dispositivi Windows

Il supporto per PC Windows 10+ e Microsoft HoloLens 2 include le seguenti capacità:

- **Registrazione dei dispositivi (PC Windows versione 10 e successive e sistemi Microsoft Hololens 2)**
- **Impostazioni passcode**
- **Configurazione di Exchange**
- **Configurazioni**
- **Dispositivi**
- **App**
- **Pianificazione delle app Windows**

- Configurazione del controllo delle app: controllo delle app installate per dispositivo
- Gestione aggiornamenti di Windows
- Segnalazione stato dispositivi da Ivanti Neurons for MDM ad Azure
- Configurazione di profili Windows Autopilot
- Invio di SyncML su dispositivi con configurazioni personalizzate
- Criteri
- Restrizioni di Windows
- Certificati di identità
- Windows Hello for Business
- Profili Wi-Fi e VPN

> Le configurazioni distribuite ai dispositivi HoloLens non supportati da questo tipo di dispositivo non saranno segnalate come configurazioni distribuite nella scheda Configurazioni dei Dettagli dispositivo.

Caratteristiche di Windows (supportate solo per PC Windows):

- Ivanti Bridge
- Configurazione del BIOS di Windows
- Windows BitLocker
- Configurazione tutto schermo Windows
- Configurazione licenza Windows
- Configurazione Integrazione server EMA
- Impostazioni della stampante
- Configurazione Rimuovi Bloatware
- Browser ADMX (GPO)

Conformità dei dispositivi Windows

È possibile configurare Ivanti Neurons for MDM con Microsoft Azure per semplificare la registrazione degli utenti sui dispositivi desktop e tablet di Windows in cui viene eseguito Windows 10+. Per configurare l'integrazione Azure tenant per abilitare la conformità dei dispositivi Windows, vedere Utilizzo di Microsoft Azure.

App Windows e inventario hardware

Inventario delle app Windows

L'inventario delle app è un elenco delle app rilevate sui dispositivi registrati. Utilizzare questa pagina per ottenere delle informazioni sulle app utilizzate dai dispositivi registrati. Per ulteriori informazioni, vedere Inventario delle applicazioni.

> L'Inventario app visualizza le app Win32 o Win32 Store su un dispositivo se la configurazione della privacy per quel dispositivo consente di raccogliere le informazioni di tutte le app su quel dispositivo.

Configurazione degli intervalli dell'inventario app

È possibile impostare gli intervalli della raccolta inventario delle app di Windows 10 per più inventari tipo di origine delle app. Gli intervalli sono utilizzati quando la Configurazione della privacy è impostata per la raccolta di tutte le app dal dispositivo.

Per ulteriori informazioni, consultare **Configurazione degli intervalli dell'inventario app**.

Inventario hardware Windows

È possibile abilitare la raccolta di informazioni sull'hardware dai dispositivi Windows 10+. Questi dettagli vengono recuperati usando Bridge. Per ulteriori informazioni, vedere **Inventario hardware**.

7.5.3. Configurazione di Apple Remote Desktop su dispositivi macOS

Argomenti della sezione:

- Abilitazione di Apple Remote Desktop su dispositivi macOS
- Disabilitazione di Apple Remote Desktop su dispositivi macOS

Abilitazione di Apple Remote Desktop su dispositivi macOS

La funzione Desktop remoto Apple abilita la condivisione dello schermo e consente di gestire i dispositivi da remoto. La funzione Apple Remote Desktop è disponibile per dispositivi supervisionati macOS 10.14.4+.

Procedura

1. Andare in **Dispositivi** e selezionare uno o più dispositivi macOS supervisionati.
2. Fare clic su **Azioni** > **Abilita Desktop remoto** nei dispositivi.
3. Fare clic su **Abilita Remote Desktop** per confermare.

Disabilitazione di Apple Remote Desktop su dispositivi macOS

Procedura

1. Andare in **Dispositivi** e selezionare uno o più dispositivi macOS supervisionati.
2. Fare clic su **Azioni** > **Disabilita Desktop remoto** nei dispositivi. La funzionalità di condivisione schermo è disabilitata e non è possibile gestire in remoto i dispositivi.

7.5.4. Registrazione del dispositivo (iOS, macOS e Android)

Argomenti della sezione:

- Installazione manuale del profilo di gestione
- Invio di un invito (iOS, macOS e Android)
- Fornire agli utenti finali le istruzioni per scaricare l'app (iOS e Android)

La maggior parte degli utenti inizia con la registrazione di un dispositivo. Per avviare il processo di registrazione, è possibile seguire uno degli approcci che seguono:

- Inviare un invito a uno o più utenti finali (registrazione iReg)
- Fornire all'utente finale le istruzioni per scaricare l'app Go (registrazione in-app)

> Se la registrazione MDM di dispositivi iOS e macOS non riesce con il messaggio *Installazione profilo non riuscita. Il server SCEP ha restituito una risposta non valida*. errore, l'utente del dispositivo deve avviare nuovamente la procedura di registrazione del dispositivo dall'inizio. Ciò accade soprattutto quando l'utente del dispositivo impiega più tempo del previsto per completare la procedura di registrazione MDM del dispositivo iOS e macOS dopo che il profilo è stato scaricato sul dispositivo. Per ulteriori chiarimenti, contattare l'assistenza Ivanti.

Ivanti Neurons per MDM supporta la gestione a livello di utente di un singolo utente (utente locale o utente Active Directory (AD) registrato) sui dispositivi macOS. Gli amministratori possono gestire i dispositivi per gli utenti, applicare i profili dispositivo e i profili utente e di conseguenza utilizzare App Store, la distribuzione delle app, le configurazioni e le policy (inclusi Apps@Work, restrizioni, sicurezza).

Per gestire i dispositivi macOS con utente AD, l'utente AD deve essere l'utente che ha effettuato l'accesso durante la registrazione. Qualsiasi altro utente non registrato non può visualizzare i profili specifici degli utenti registrati (ad esempio, le certificazioni di identità, VPN). Tuttavia, le configurazioni a livello di dispositivo possono essere visualizzate e utilizzate da qualsiasi utente collegato.

> L'utente **finale deve disporre di un account** in Ivanti Neurons per MDM per potere iniziare la procedura di registrazione del dispositivo. Per gli utenti LDAP, questo significa che devono essere configurati un **Connettore** e un **server LDAP** e l'utente deve essere importato dal server LDAP. Per gli utenti locali, questo significa **aggiungere un utente**.

> L'URL di registrazione del dispositivo generato nelle versioni precedenti di Ivanti Neurons per MDM non funziona con la versione corrente. L'amministratore dovrà rigenerare l'URL di registrazione del dispositivo per registrarlo.

Installazione manuale del profilo di gestione

Applicabile a:

- iOS 12.2 fino alla versione più recente supportata da Ivanti Neurons per MDM.
- macOS 11.0 fino alla versione più recente supportata da Ivanti Neurons per MDM.

Registrazione dispositivi iOS

Durante la registrazione in-app su dispositivi iOS:

- Durante la registrazione del dispositivo usando Go app appare una pagina con le istruzioni per installare il profilo.
- Fare clic sull'opzione **Installa il profilo scaricato** e fare clic su **Ho capito**.
- Il profilo scaricato è valido per alcuni minuti, dopo cui è necessario effettuare nuovamente la registrazione.

Registrazione dispositivi macOS

Per la registrazione di un dispositivo macOS nel portale self-service, un utente deve effettuare le seguenti operazioni:

Procedura

1. Accedere con le proprie credenziali.
2. Nella pagina di installazione del profilo di gestione, il profilo viene scaricato nel sistema locale dell'utente.
3. Fare doppio clic sul profilo scaricato per renderlo visibile nelle Preferenze di sistema dell'utente.

> L'utente ha a disposizione un tempo limitato per installare il profilo prima che questo non sia più valido.

4. Aprire **Profili** nelle Preferenze di sistema. Quando il profilo viene scaricato sul dispositivo, gli utenti possono visualizzare una pagina Web con il link Profili. Fare clic su **Profili** per aprire l'app Impostazioni.
5. Fare clic su **Installa** per installare il profilo di gestione.
6. Continuare e completare la procedura di installazione. Inserire la password di sistema quando richiesto.

Invio di un invito (iOS, macOS e Android)

Avviare la procedura di registrazione inviando un invito. Ivanti Neurons per MDM fornisce i metodi seguenti per inviare agli utenti finali un invito per la registrazione del dispositivo:

- Nella **Procedura di configurazione guidata**
- Quando vengono **aggiunti uno o più utenti**
- Nella pagina Utenti (**Azioni > Invia invito**)

> Se gli utenti finali smarriscono l'invito, è possibile condividere l'URL elencato nell'invito. Assicurarsi di aggiungere **/go** alla fine dell'URL.

Gli utenti finali con un account Ivanti Neurons per MDM e una password impostata non hanno bisogno di un invito per iniziare la procedura di registrazione. È possibile inviare loro l'URL elencato nell'invito.

Fornire agli utenti finali le istruzioni per scaricare l'app (iOS e Android)

L'applicazione Go è disponibile per dispositivi Android e iOS. È possibile fornire istruzioni agli utenti finali su come scaricare l'applicazione da un app store pubblico e iniziare il processo di registrazione dall'app. L'invito via e-mail contiene le seguenti informazioni:

- Un collegamento alla pagina di registrazione
- Un PIN monouso (se impostato dall'amministratore)
- Istruzioni di base per i prossimi passi

Se si è già impostato un password per l'account, è possibile inviarla all'indirizzo e-mail aziendale dell'utente finale. Se si sta utilizzando LDAP per l'autenticazione, informare l'utente finale che saranno necessarie le credenziali di rete.

Se l'utente non completa l'installazione del profilo MDM durante la registrazione, Ivanti Neurons per MDM invia notifiche push periodiche al dispositivo per chiedere all'utente di completare la procedura di registrazione.

L'utente può usare Username e Password o scansionare il codice QR per iniziare la registrazione del dispositivo da Go app. I dettagli sono i seguenti:

- **Nome utente**: indirizzo e-mail
- **Password**: se specificato nelle **Impostazioni utente** e una password temporanea è definita dall'amministratore
- **Codice QR**: genera il codice QR dal portale autogestito Ivanti Neurons per MDM. Quando si tenta di scansionare il codice QR utilizzando l'opzione **Scansiona codice QR** appare un messaggio sullo schermo che richiede all'utente di concedere l'autorizzazione per accedere alla fotocamera del dispositivo. Una volta concessa l'autorizzazione, la fotocamera scansiona il codice QE e il dispositivo viene registrato. Questa opzione è supportata per Android 9 e versioni successive, iOS 14 e versioni successive.

In quanto utente finale, se si riceve un'e-mail di registrazione sul proprio dispositivo mobile, toccare il collegamento per avviare la procedura di registrazione. Se si ricevere l'e-mail su un computer desktop o portatile, inserire l'URL in un browser sul proprio dispositivo mobile per avviare la procedura di registrazione.

Se nell'account dell'utente finale non è definita una password per l'account utente Ivanti Neurons per MDM o se le **Impostazioni utente** richiedono un PIN di registrazione, viene incluso il PIN monouso. Dopo avere inserito il PIN, verrà richiesto all'utente finale di impostare una password per l'account se non è ancora esistente.

> Per i dispositivi Android Enterprise, quando la registrazione è completata, viene disinstallato qualsiasi certificato CA installato manualmente in un profilo di lavoro su un dispositivo di proprietà dell'azienda o un dispositivo gestito dal lavoro.

Nuova registrazione dei dispositivi iOS

Se si desidera registrare nuovamente il dispositivo, è possibile farlo come segue:

1. Avviare il client Go sul dispositivo.
2. Andare in **Impostazioni** > **Risoluzione dei problemi** > **Registra nuovamente dispositivo**. La procedura di nuova registrazione si avvia e visualizza alcune richieste di conferma.
3. Toccare **Sì** per confermare i messaggi di richiesta.

> Se si tocca **Annulla** durante l'installazione del profilo, il processo di registrazione si interrompe e il server Ivanti Neurons per MDM disattiva il dispositivo MDM.

Per riavviare la procedura di nuova registrazione è necessario reinstallare il profilo già scaricato. Il profilo scaricato è valido solo per pochi minuti, dopodiché è necessario eseguire la nuova registrazione dal client Go.

Nuova registrazione di dispositivi Android

L'amministratore può registrare nuovamente un dispositivo usando le operazioni ritira, cancella o elimina senza cancellare manualmente l'inserimento attivo esistente. Questo metodo è specificatamente più utile per le nuove registrazioni in cui la nuova voce e la voce esistente appartengono allo stesso tenant. La pagina Dispositivi visualizza lo stato del dispositivo sul portale amministrativo Ivanti Neurons per MDM nel modo seguente:

- **Attivo** - la registrazione del dispositivo è riuscita
- **Ritirato** - il dispositivo viene reimpostato e appare lo stato ritirato
- **Cancellato** - il dispositivo viene reimpostato e appare lo stato cancellato
- **Reimpostato** - il dispositivo viene reimpostato e rimarrà in stato attivo sul server fino alla successiva registrazione

La pagina Audit trail elenca gli stati di registrazione, nuova registrazione e ritirato per i dispositivi Android. Per maggiori informazioni, vedere **Utilizzo di widget**.

> Per Android 9.x e versioni precedenti, un singolo inserimento verrà mostrato dopo la nuova registrazione. In caso di Android 10.x e versioni successive, verranno visualizzati più inserimenti. Tuttavia, solo l'inserimento più recente sarà attivo, mentre gli inserimenti precedenti saranno in uno stato ritirato.

7.5.5. Registrazione dei dispositivi (PC Windows versione 10 e successive e sistemi Microsoft Hololens 2)

Argomenti della sezione:

La procedura di registrazione dei dispositivi può essere eseguita in due modi:

- Registrazione manuale
  - Su invito
  - Registrazione eseguita dall'utente finale
- Windows Autopilot
- Con SCCM e Ivanti EPM mediante una registrazione dei pacchetti di provisioning con PIN. Vedere **Registrazione dei pacchetti di provisioning con PIN**.
- **Registrazione in blocco**

Registrazione manuale

La maggior parte degli utenti inizia con la registrazione di un dispositivo. Per avviare il processo di registrazione, è possibile seguire uno degli approcci che seguono:

- Inviti tramite e-mail
- Indirizzare gli utenti all'URL per l'implementazione
- L'utente **finale deve disporre di un account** in Ivanti Neurons for MDM per potere inizializzare la procedura di registrazione del dispositivo. Per gli utenti LDAP, questo significa che devono essere configurati un **Connettore** e un **server LDAP** e l'utente deve essere importato dal server LDAP. Per gli utenti locali, questo significa **aggiungere un utente**.
- L'URL di registrazione del dispositivo generato nelle versioni precedenti di Ivanti Neurons for MDM non funziona con la versione corrente. L'amministratore dovrà rigenerare l'URL di registrazione del dispositivo per registrarlo.

Invio di un invito

Nella maggior parte dei casi, l'avvio del processo di registrazione segue l'invio di un invito. Ivanti Neurons for MDM fornisce i metodi seguenti per inviare agli utenti finali un invito per la registrazione del dispositivo:

- nella **Procedura di configurazione guidata**
- quando vengono **aggiunti uno o più utenti**
- nella pagina Utenti (**Azioni > Invia invito**)

Se l'utente finale perde l'invito, lo riceve su un computer fisso o portatile, o non riesce a riceverlo per qualsiasi ragione, è possibile indirizzarlo all'URL indicato nell'invito. È sufficiente aggiungere **\go** alla fine dell'URL del servizio.

Gli utenti finali con un account Ivanti Neurons for MDM e una password impostata non hanno bisogno di un invito per iniziare la procedura di registrazione. È possibile indirizzarli all'URL che sarebbe stato indicato nell'invito.

Completamento del processo di registrazione degli utenti finali

Spiegare agli utenti del dispositivo come completare il processo di registrazione. È possibile utilizzare le seguenti istruzioni come modello e apportare le modifiche necessarie:

Procedura

1. Aprire un browser sul PC con Windows versione 10 o successiva.
2. Andare su mobileiron.com/go.
   Si verrà reindirizzati a una nuova pagina che contiene un URL per l'iscrizione.
3. Copiare l'URL di registrazione negli appunti.
4. Toccare **Aggiungi account** nella parte inferiore della pagina **Impostazioni**.
5. Inserire l'indirizzo e-mail associato all'invito ricevuto.

> Se il nome utente dell'utente di Ivanti Neurons for MDM non corrisponde all'indirizzo e-mail dell'utente inserito in Ivanti Neurons for MDM, spiegare all'utente che deve immettere il nome utente quando viene richiesto l'indirizzo e-mail.

Incollare l'URL del server di Workplace nel campo di testo successivo.

7. Toccare **Accedi**.
8. Inserire la password nel campo successivo.
9. Lasciare gli altri campi vuoti.
10. Toccare **Accedi**.
11. Fare clic su **Fine** nella schermata di **AGGIUNTA DELL'ACCOUNT**.
    La schermata di avvio di Workplace indicherà che è stato aggiunto un account.

Windows Autopilot

Windows Autopilot è una funzione di Microsoft che consente agli amministratori di configurare e preconfigurare nuovi dispositivi per renderli subito operativi. La funzione Autopilot consente di eseguire un provisioning rapido, semplice e affidabile dei dispositivi Windows Desktop o HoloLens2. Inoltre, la funzione Autopilot consente di eseguire le seguenti attività:

- Unisce automaticamente i dispositivi a Entra ID (Entra ID)
- Registrare automaticamente dispositivi nei servizi MDM
- Creare e assegnare automaticamente dispositivi a gruppi di configurazioni in base al profilo del dispositivo
- Personalizzare l'esperienza di registrazione
- Applicare configurazioni e policy
- Installare applicazioni essenziali

Ivanti supporta tutte le modalità dei profili di Autopilot:

- Gestita dall'utente
- Gestita dall'utente con pre-provisioning, (precedentemente denominata White Glove)
- Modalità di distribuzione automatica

Per ulteriori informazioni, vedere **Configurazione di profili Windows Autopilot**.

Per motivi di sicurezza e al fine di evitare l'uso non autorizzato del dispositivo è possibile utilizzare la funzionalità CSP TenantLockdown, in modo da bloccare tutti i dispositivi Windows con Autopilot per un tenant. Per utilizzare questa funzione, è necessario registrare i dispositivi utilizzando l'opzione Autopilot. Questa configurazione viene applicata a livello di dispositivo. Vedere **CSP TenantLockdown**.

Registrazione standard Entra ID

Quando gli utenti vengono aggiunti al tenant Entra ID, possono registrare direttamente i loro dispositivi tramite l'account di lavoro.

Procedura

1. Su un dispositivo Windows, andare su **Impostazioni > Account > Accesso dal lavoro o dalla scuola**.
2. Selezionare Aggiungi account da lavoro o scuola e poi fare clic su **Connetti**.
3. Fornire l'indirizzo e-mail del proprio account di lavoro.

Il dispositivo viene registrato automaticamente a Ivanti Neurons for MDM.

7.5.6. Local Admin Password Solution (LAPS)

La **Local Administrator Password Solution (LAPS)** automatizza la gestione sicura delle password dei dispositivi Windows. LAPS impone modifiche casuali e regolari delle password e le memorizza in modo sicuro in una directory, riducendo il rischio di spostamenti laterali in caso di compromissione.

Modern LAPS si integra con Azure e con le più recenti piattaforme di gestione dei dispositivi Windows, consentendo l'archiviazione, il recupero e la configurazione sicura delle password con Ivanti Neurons for MDM e il portale Azure. Questo garantisce che le credenziali dell'amministratore rimangano protette e verificabili sia negli endpoint Windows legacy che in quelli gestiti dal cloud.

> Per utilizzare LAPS con Ivanti Neurons per MDM, gli amministratori di Azure devono assicurarsi che l'applicazione N-MDM sia aggiunta al proprio tenant Azure con l'autorizzazione LAPS richiesta (**DeviceLocalCredential.Read.All**).

> La configurazione di LAPS può specificare l'account amministratore locale a cui si applica utilizzando l'impostazione di criterio **Nome account amministratore**. Se il nome dell'account specificato nella configurazione non è presente sul dispositivo, il nome dell'account non può essere gestito. Tuttavia, quando l'opzione **Nome account amministratore** viene lasciata vuota, il criterio si basa sull'account amministratore locale integrato nel dispositivo, identificato dal suo noto identificatore relativo (RID).

> Quando si applica la configurazione LAPS, la password dell'account amministratore locale del dispositivo sarà gestita dall'amministratore e la password verrà generata in Azure Active Directory.

Altre funzionalità di LAPS

- Archiviazione delle password in Azure - Le password degli amministratori locali possono ora essere archiviate in modo sicuro nell'oggetto dispositivo di Azure.
- Recupero della password - Gli amministratori possono recuperare le password dei dispositivi direttamente attraverso il portale Azure.
- Impostazioni configurabili - Le impostazioni configurabili di LAPS possono essere gestite nel portale Ivanti Neurons per MDM.
- Rotazione delle password su richiesta: gli amministratori possono ruotare manualmente le password dei dispositivi dal portale Ivanti Neurons per MDM.
- Ripristino automatico della password al momento dell'utilizzo - Le password possono essere ripristinate automaticamente dopo l'accesso.

Creare la configurazione LAPS

Prerequisiti

- La soluzione LAPS deve essere abilitata per i dispositivi. Questa soluzione NON è disponibile per impostazione predefinita per tutti. Rivolgersi al team di supporto tecnico per ricevere assistenza.
- I dispositivi devono essere registrati in Azure Device Operations (ADO).

Procedura

1. Nella piattaforma di gestione della configurazione, avviare la creazione della configurazione LAPS.
2. **Impostare i parametri richiesti**:
    - **Directory di backup** - Selezionare Backup della password solo su Microsoft Entra ID.

- **Nome amministratore locale** - Specificare il nome dell'account amministratore del sistema (ad esempio, Admin).

3. **Configura impostazioni aggiuntive** - Impostare queste impostazioni in base ai criteri di sicurezza dell'organizzazione. Se non vengono specificati, verranno utilizzati i valori predefiniti.
   - **Giorni età password** - Numero di giorni prima della rotazione automatica della password dell'amministratore locale.
   - **Complessità password** - Specifica i requisiti di complessità della password (ad esempio, caratteri alfanumerici e speciali).
   - **Lunghezza password** - Imposta la lunghezza desiderata della password dell'amministratore locale.
   - **Azioni post autenticazione** - Definisce le azioni da eseguire dopo l'autenticazione.
   - **Ritardo ripristino post autenticazione** - Imposta il ritardo (in ore/minuti) per il ripristino della password dopo l'autenticazione.
4. **Distribuisci configurazione LAPS**
   - Assegnare il profilo di configurazione LAPS all'utente/dispositivo registrato in ADO.
   - Una volta applicata la configurazione, viene creata una password di amministratore locale casuale che viene memorizzata in modo sicuro in Microsoft Entra ID:
     Dispositivi → Gestione dei dispositivi → Recupero della password dell'amministratore locale.
5. **Rotazione password**
   - La password viene ruotata automaticamente in base al valore impostato in **Giorni età password**.
   - È possibile verificare lo stato di rotazione della password nei registri del dispositivo.

Rotazione password

Per forzare la rotazione immediata della password dell'amministratore locale, procedere come segue:

1. **Navigare nel dispositivo** - Accedere alla pagina dei dettagli del dispositivo nella console di gestione.
2. **Inizializza Rotazione password**
   - Fare clic sul menu a tre punti (...).
   - Selezionare **Ruota password locale amministratore**.
   - Confermare l'azione quando richiesto. In questo modo si invia una richiesta di rotazione della password.
3. **Check-in e conferma**
   - Il dispositivo elabora la modifica della password durante il successivo check-in imposto.
   - Aggiornare la pagina in Microsoft Entra ID per visualizzare la password aggiornata nella sezione di recupero della password.

7.5.7. Registrazione dei pacchetti di provisioning con PIN

L'amministratore può iscrivere i dispositivi gestiti da SCCM o Ivanti Endpoint Manager a Ivanti Neurons per MDM. Il Deployment Package Tool permette alle organizzazioni di semplificare la transizione dei dispositivi Windows al Ivanti Neurons per MDM Modern Management, senza tempi di inattività o interruzione dell'utente finale. La transizione diretta si ottiene scaricando un pacchetto di distribuzione unico dalla Ivanti Neurons per MDM Console, quindi distribuendolo attraverso lo strumento di gestione esistente o il dominio. Una volta eseguito, il pacchetto effettua la registrazione invisibile dell'endpoint in Ivanti Neurons per MDM per la gestione ordinaria. Questo approccio consente agli amministratori di eseguire prima una migrazione semplificata dei dispositivi, per poi configurarli in seguito over-the-air con la massima flessibilità. Quando un dispositivo completa la registrazione invisibile in Ivanti Neurons per MDM, viene aggiunto a MDM e viene gestito congiuntamente dalle due autorità di gestione. Dopo che l'amministratore ha configurato l'esperienza Windows desiderata in Ivanti Neurons per MDM, è possibile rimuovere la piattaforma di gestione legacy e lasciare Ivanti Neurons per MDM come singola autorità di gestione del dispositivo.

> C'è un'eccezione a questa regola se un dispositivo è in fase di transizione da Microsoft Endpoint Manager (MEM) o ex SCCM. Il client MEM esistente continua a funzionare in modalità di coesistenza (anziché di gestione congiunta) finché la piattaforma MEM non viene rimossa. Quando la modalità di coesistenza è abilitata, il MEM Client disabilita automaticamente alcune funzionalità a favore di Ivanti Neurons per MDM che fornisce quei carichi di lavoro. Per maggiori informazioni, consultare la **documentazione Microsoft's Coexistence**.

Per informazioni più precise sul comportamento previsto quando si utilizza MEM e altre piattaforme di gestione di terzi, Ivanti consiglia di testare prima lo strumento Pacchetto di distribuzione Ivanti Neurons per MDM nel proprio ambiente.

Prerequisiti

- Gli account utente devono essere importati su Ivanti Neurons per MDM usando LDAP, Entra ID (Entra ID), Upload di utenti locali o altre integrazioni di identità
- Tutti i dispositivi dovrebbero avere **Windows Configuration Designer** installato.
- Abilitare la registrazione basata su PIN su Ivanti Neurons per MDM
- Gli utenti non dovrebbero avere spazi nel loro nome utente, questo potrebbe causare la mancata riuscita della transizione di un dispositivo utente.
- Questo strumento può essere distribuito in ambienti che non sfruttano Entra ID.
- Gli elementi principali di Ivanti Neurons per MDM Modern Windows Management Suite non richiedono Entra ID. La co-gestione o la coesistenza possono richiedere che certi carichi di lavoro / configurazioni siano distribuiti al momento della registrazione invisibile all'utente, per evitare qualsiasi impatto durante la transizione.
- Il pacchetto di distribuzione è attualmente supportato solo per SCCM e Ivanti Endpoint Manager.

Procedura

1. Andare su **Amministratore>Windows>Pacchetto di distribuzione**.
2. Selezionare **Utente** o **Gruppi di utenti** per generare i PIN e fare clic su **Scarica Pacchetto di distribuzione** (file ZIP).
3. Il Pacchetto di distribuzione viene fornito agli amministratori di SCCM / Ivanti Endpoint Manager per decomprimere e trasferire i file ai rispettivi dispositivi gestiti da questi amministratori. Per informazioni su come eseguire questo passo, vedere **Pacchetti e programmi in Configuration Manager**.

4. Dopo il trasferimento, gli amministratori attivano da remoto lo script setup.ps1 sui dispositivi. Per informazioni sull'attivazione dello script, vedere **Creare e distribuire script da Configuration Manager**.
5. I dispositivi vengono registrati in Ivanti Neurons per MDM.

I PIN generati per gli utenti sono validi solo per 24 ore. Quando un PIN scade, è necessario generarne uno nuovo.

Il file che contiene i PIN viene rimosso dal dispositivo al termine del tentativo di registrazione.

Registrazione dei dispositivi SCCM in Ivanti Neurons per MDM

Procedura

1. Scaricare tutti i file correlati alla distribuzione da Ivanti Neurons per MDM per gli utenti selezionati.
2. Selezionare account o gruppi da registrare.
3. Distribuire i file del pacchetto ai dispositivi client usando SCCM:
    1. Verificare se i client richiesti sono presenti in SCCM. Se il Windows-configuration-designer non è presente sul client, l'amministratore dovrebbe spingere il designer e distribuirlo sul client.
    2. Sul server SCCM, creare una cartella e copiare il file zip di distribuzione ed estrarre il contenuto del file.
    3. Creare un file .bat che copierà il contenuto della cartella in cui sono stati estratti i file sul dispositivo client.
    4. In SCCM, andare su **Libreria software > Gestione applicazioni > Pacchetti** e creare un pacchetto per copiare il contenuto della cartella sul client. Inserire la cartella di destinazione in cui si desidera copiare il contenuto.
    5. Distribuire il pacchetto sul dispositivo o sulla posizione del dispositivo.
    6. Nella sezione Monitoraggio, è possibile monitorare lo stato di distribuzione e confermare che i file sono stati copiati nella cartella di destinazione del client.
4. Eseguire lo script per iscrivere un dispositivo:
    1. Andare su **Libreria Software > Script** e creare lo script.
    2. Inserire un nome per lo script e importare lo script PowerShell **setup.ps1** dalla cartella decompressa.
    3. Approvare lo script ed eseguire lo script sul dispositivo di destinazione.
    4. Selezionare **Avvia ora** e fare clic su **Salva**. Le attività Pianificate iniziano a eseguire lo script. In caso di esecuzione riuscita, la stato diventa Verde.
5. Per verificare la registrazione del dispositivo, **Impostazioni** > **Aggiungi o rimuovi un pacchetto di provisioning** > **Dettagli**.

Registrazione dei dispositivi Ivanti Endpoint Manager in Ivanti Neurons per MDM

Procedura

1. Scaricare tutti i file correlati alla distribuzione da Ivanti Neurons per MDM per gli utenti selezionati.
2. Selezionare account o gruppi da registrare.
3. **Caso 1**: un nome di dispositivo è considerato per registrare il dispositivo con lo stesso nome utente - In questo caso, l'indirizzo e-mail non è un indirizzo e-mail utente valido. Un'e-mail con il nome del dispositivo concatenato con il dominio AD è considerato come l'indirizzo e-mail di registrazione. L'amministratore deve impostare Account come LocalSystemAccount e utilizzare setup.ps1 come file primario per avviare l'esecuzione di PowerShell.
   Caso 2: un indirizzo e-mail utente valido è considerato per la registrazione del dispositivo e nessuna restrizione sulla modifica dei

file nella posizione del dispositivo - Usare l'indirizzo e-mail dell'utente memorizzato per la registrazione. Per abilitare questa registrazione, l'amministratore deve impostare Account come account utente corrente e utilizzare setup.ps1 come file primario per avviare l'esecuzione di PowerShell.

Caso 3: un indirizzo e-mail valido è considerato per la registrazione del dispositivo con restrizioni sulla modifica dei file nella posizione del dispositivo - Usare l'indirizzo e-mail dell'utente memorizzato per la registrazione. Questo caso ha due sottocasi:

- Utilizzando due script per la registrazione - Creare un pacchetto di distribuzione con **setupEPMCopyContentsToTempFolderStep1.ps1** ed eseguire come account utente corrente. I file vengono copiati in una posizione temporanea. Creare un altro pacchetto di distribuzione con **setupEPMCopyContentsToTempFolderStep2.ps1** ed eseguire come account di sistema locale.

> Se l'utente del dispositivo ha restrizioni sulla modifica della cartella contenente i file del pacchetto, copiare i file in una cartella temporanea, controllare l'id utente e creare un pacchetto PowerShell. Il pacchetto PowerShell è eseguito dallo script **setupEPMCopyContentsToTempFolderStep2.ps1**. Dopo l'installazione, la cartella temporanea verrà eliminata.

Disattiva/Attiva UAC

1. Aggiornare la voce di registro per disabilitare il controllo UAC e riavviare la macchina
2. Eseguire il pacchetto PowerShell come account dell'utente corrente e utilizzando setup.ps1
3. Aggiornare la voce di registro per abilitare il controllo UAC e riavviare la macchina

Creare il pacchetto PowerShell:

1. Verificare se i client richiesti sono presenti in Endpoint Manager.
2. Copiare i file in C:\Program Files\LANDesk\ManagementSuite\LANDesk\files\. Creare una sottocartella all'interno di questa cartella ed estrarre i file.
3. Creare il pacchetto: **Distribuzione > Pacchetti di distribuzione > Nuovo > Windows > PowerShell**.

> L'amministratore può distribuire i pacchetti a diversi dispositivi in base al livello di restrizioni impostato sui dispositivi.

4. Nella sezione Primary file, inserire il nome del pacchetto e caricare setup.ps1 dalla cartella che contiene i file copiati
5. Sotto la sezione File aggiuntivi, copiare i file rimanenti (diversi dallo script setup.ps1) usando **Aggiungi**.
6. Selezionare Account dell'utente corrente nella sezione Account.
7. Fare clic su **Salva**.

4. Creare Attività pianificata:
   1. Selezionare il pacchetto creato, fare clic con il pulsante destro del mouse e selezionare **Crea attività pianificata(e)**. Viene creata un'attività pianificata.
   2. Trascinare il dispositivo e aggiungerlo alla sezione dei pacchetti programmati.
   3. Sul pacchetto pianificato, fare clic con il pulsante destro del mouse e selezionare **Proprietà**.
   4. Verificare il pacchetto.
   5. Sotto Tipo di attività, selezionare **Push**.
   6. Selezionare **Avvia ora** e fare clic su **Salva**. Le attività Pianificate iniziano a eseguire lo script. In caso di esecuzione riuscita, la stato diventa Verde.
5. Per verificare la registrazione del dispositivo, **Impostazioni** > **Aggiungi o rimuovi un pacchetto di provisioning** > **Dettagli**. In alternativa, l'amministratore può verificare la registrazione di un dispositivo sotto i registri diagnostici del dispositivo.

7.5.8. Utilizzo della registrazione in blocco per i dispositivi Android

La funzionalità di registrazione in blocco consente di registrare velocemente numerosi dispositivi Android con Ivanti Neurons per MDM .

Prerequisiti:

- Gli account utente devono essere importati su Ivanti Neurons per MDM usando un Account Entra ID (Entra ID) Premium.
- Tutti i dispositivi dovrebbero avere **Windows Configuration Designer** installato.

Procedura:

1. Collegare i tenant Ivanti Neurons per MDM ed Entra ID. Vedere **Connessione di Entra ID a UEM per i dispositivi Windows 10.**
2. Aprire l'app **Windows Configuration Designer** e selezionare **Provisioning dispositivi desktop**. A schermo appare una finestra Nuovo progetto.
3. Immettere i seguenti dettagli:
    - Nome - Un nome univoco per il proprio progetto
    - Cartella di progetto - La posizione sul dispositivo in cui si desidera salvare il progetto
    - Descrizione - Descrizione opzionale del progetto

Fare clic su **Fine** per chiudere la finestra del nuovo progetto ed eseguire una sequenza di passaggi.

5. **Configura dispositivo**
   Inserire un nome univoco per i propri dispositivi. Il nome può includere un numero di serie (%SERIAL%) o un set casuale di caratteri.
6. In via opzionale è possibile inserire un codice prodotto se si sta aggiornando Windows, configurando il dispositivo per un uso condiviso o rimuovendo il software preinstallato.
7. **Configura rete**
   In via opzionale è possibile configurare i dispositivi da connettere alla rete Wi-Fi al primo avvio. Se i dispositivi di rete non sono configurati, all'avvio del dispositivo è necessaria una connessione di rete cablata.
8. **Gestione account**
   Selezionare **Registra in Entra ID**, inserire una data **Scadenza token in blocco**, quindi fare clic su **Ottieni token in blocco**.
9. Inserire le proprie credenziali Entra ID per ottenere un token in blocco.
10. Nella pagina **Mantieni l'accesso a tutte le tue app**, fare clic su **No, accedi solo a questa app**.
    - Fare clic su Avanti quando il token in blocco viene recuperato correttamente e creare il pacchetto.
    - Nel portale Azure viene creato un utente con il pacchetto di provisioning - Nome principale utente (come package_0ea893a5-1e93-4d21-a6b1-dc788946fd1d@miwinqe.onmicrosoft.com). Copiare il file (runtime ppkg tool) in un dispositivo di archiviazione.

> L'utente Entra ID per la creazione del token in blocco e l'utente del pacchetto non devono presentare l'MFA abilitata. Per verificare, è necessario eseguire l'unione OOBE + Entra ID su tale utente.

Ricreare o sincronizzare l'utente del pacchetto (creato in Azure) in Ivanti Neurons per MDM.

Iscrivere in blocco un dispositivo con una chiavetta contenente il pacchetto di provisioning. È anche possibile fare doppio clic sul dispositivo esistente per eseguire l'esperienza post-OOBE. Se il pacchetto non è stato installato al primo tentativo, non riuscirà nemmeno il secondo tentativo. Controllare se il nuovo dispositivo è stato creato in Ivanti Neurons per MDM e se Entra ID appartiene all'utente del pacchetto.

7.5.8.1. Ivanti Bulk Enrollment

L'amministratore può registrare più dispositivi Windows con un utente generico (tramite ppkg) che inizia con il prefisso **windows-bulkenroll**, e successivamente assegnare l'utente.

Prerequisiti:

- Su Ivanti Neurons per MDM, creare un account utente con prefisso **windows-bulkenroll**. Ad esempio, **windows-bulkenroll**-user1@abc.com, **windows-bulkenroll**-user2@abc.com.

Creazione del pacchetto PPKG con Windows Configuration Designer

1. Scaricare e installare **Windows Configuration Designer**.
2. Creare un nuovo progetto.
3. Fare clic su **Provision Desktop**.
4. Inserire il nome del progetto e selezionare un percorso.
5. Nella sezione **Imposta dispositivo**, inserire il nome del dispositivo.
6. Nella sezione **Imposta rete**, inserire il nome della rete (per impostare la rete, se necessario o se può essere disattivata).
7. Nella sezione **Gestione account**, selezionare **Registra in amministratore locale**. Inserire **Nome utente** e **Password**, quindi fare clic su **Avanti**.
8. Nella sezione **Aggiungi applicazioni**, fare clic su **Avanti**.
9. Nella sezione **Aggiungi certificati**, selezionare **Passa a editor avanzato**, quindi fare clic su **Procedi** > **Sì**.
10. Accedere a **Impostazioni Runtime** > **Registrazioni luogo di lavoro**. Immettere **UPN** (lo stesso utente creato su Ivanti Neurons per MDM nella sezione prerequisiti). Selezionare le opzioni seguenti:
    - AuthPolicy: in loco
    - Url completo servizio individuazione: https://login.mobileiron.com
    - Segreto: inserire la password

Fare clic su **File** > **Salva**.

12. Fare clic su **Esporta** > **Pacchetto di provisioning**.
13. Fare clic su **Avanti** nelle schermate successive, quindi fare clic su **Crea**.
    Il file ppkg viene salvato nella posizione specificata.

Eseguire il provisioning del dispositivo in modalità OOBE con ppkg

Eseguire il provisioning dei dispositivi con il file del pacchetto ppkg appena creato nella sezione precedente. Una volta che il dispositivo è stato registrato e il check-in è andato a buon fine, si troverà la voce del dispositivo sul server MDM con l'utente che ha come prefisso **windows-bulkenroll**.

Assegna dispositivo all'utente

1. Nella pagina Dispositivi, fare clic sull'utente che ha un prefisso come **windows-bulkenroll**.
2. Fare clic su **Assegna a utente**. Si apre la finestra Assegna a utente.
3. Selezionare o ricercare il dispositivo dall'elenco.
4. Selezionare il dispositivo richiesto.
5. Fare clic su **Assegna a utente**. Il dispositivo selezionato verrà assegnato all'utente.

Quando l'utente accede al dispositivo per la prima volta, è necessario cambiare la password.

> L'opzione Assegna a utente è disponibile solo per i dispositivi con Registrazione in blocco Ivanti.

> Solo le configurazioni e le applicazioni dell'ambito del dispositivo funzioneranno per i dispositivi iscritti in questa categoria. Le configurazioni e le applicazioni dell'ambito utente non sono supportate.

7.5.9. Configurazione passcode

Argomenti della sezione:

- Modifica della configurazione del passcode assegnata
- Assegnazione di una configurazione del passcode diversa

Utilizzare la Configurazione del passcode assegnata al dispositivo per modificare le impostazioni del passcode. È possibile:

- modificare le impostazioni relative alla configurazione assegnata

O

- assegnare una configurazione del passcode diversa

Le modifiche apportate alla configurazione saranno valide per tutti i dispositivi a cui è assegnata la configurazione.

Modifica della configurazione del passcode assegnata

Procedura

1. Andare su **Dispositivi**.
2. Cercare la voce relativa al dispositivo nell'elenco.
3. Fare clic sul collegamento nella colonna **Nome**.

> Se è stata assegnata una configurazione del passcode, quest'ultima verrà visualizzata nella scheda Configurazioni.

Nella scheda Configurazioni, fare clic sul collegamento **Configurazione passcode**.

5. Fare clic su **Modifica** (in alto a destra).
6. Apportare le modifiche.

Assegnazione di una configurazione del passcode diversa

Procedura

1. Assicurarsi che la configurazione di cui si necessita sia stata creata.
2. Andare su **Dispositivi**.
3. Cercare la voce relativa al dispositivo nell'elenco.
4. Fare clic sul collegamento nella colonna **Nome**.

7.5.10. Modifica del nome dispositivo

Gli amministratori possono modificare manualmente il nome di un dispositivo (anziché utilizzare la configurazione di modifica del nome dispositivo).

Applicabile a:

- Dispositivi iOS supervisionati
- Dispositivi tvOS supervisionati
- Dispositivi macOS 10.10 e versioni successive

Procedura

1. Andare su **Dispositivi**.
2. Cercare la voce relativa al dispositivo nell'elenco.
3. Eseguire una delle operazioni seguenti:
    - Se non è presente, aggiungere la colonna **Nome dispositivo**, facendo clic sull'icona delle impostazioni sulla destra e selezionando **Nome dispositivo**.
    - Fare clic sul collegamento nella colonna **Nome** per andare alla pagina dei dettagli del dispositivo.
4. Fare clic sull'icona a forma di matita **Modifica** accanto a Nome dispositivo.
5. Inserire un nuovo nome per il dispositivo e fare clic sull'icona a forma di segno di spunta.
6. Nella casella Sovrascrivi nome dispositivo, rivedere le note e fare clic su **OK**.

Le modifiche cambiate verranno inviate ai dispositivi al successivo check-in. Questa azione non può essere annullata.

> Se in precedenza era stata configurata un'impostazione Nome dispositivo predefinito, il nome impostato nella configurazione verrà sovrascritto.

7.5.11. Ricerca e applicazione di filtri ai dispositivi

Argomenti della sezione:

- Ricerca di un dispositivo
- Applicazione di filtri ai dispositivi
- Utilizzo di Ricerca avanzata
- Caricamento di query di ricerca

Ricerca di un dispositivo

Il portale amministratore di Ivanti Neurons per MDM visualizza il numero di gruppi di utenti duplicati e il numero corrispondente di GUID per identificare gruppi duplicati quando si seleziona l'attributo Nome gruppo di utenti nel Generatore di regole. Inoltre, una tabella sotto questa regola visualizza l'elenco di gruppi di utenti duplicati e i relativi dettagli, ad esempio Nome gruppo di utenti, GUID, Origine e Nome distinto (DN).

Procedura

1. Andare su **Dispositivi**.
2. Digitare nome dispositivo nel campo **Cerca**. Vengono elencati tutti i dispositivi che contengono i caratteri.

Applicazione di filtri ai dispositivi

La barra di navigazione laterale Filtri elenca varie sezioni che consentono di ricercare un dispositivo specifico dall'intero elenco di dispositivi. La procedura guidata Gestisci filtri contiene l'elenco di tutte le sezioni selezionabili per visualizzarle nella barra di navigazione Filtri.

Procedura

1. Andare su **Dispositivi**.
2. Fare clic sulle caselle di controllo rilevanti dalle sezioni elencate nella barra di navigazione laterale Filtri.
   Esempio:
   - Nella sezione **Utente abilitato**, selezionare **Sì** per visualizzare solo i dispositivi con utenti in stato attivo.
   - Se sono stati assegnati attributi personalizzati ai dispositivi, è possibile filtrare i dispositivi in base a tali attributi, facendo clic sull'icona delle impostazioni (in alto a destra).
   - Nella sezione **Stato**, selezionare **Disattivato** e **iOS** per visualizzare esclusivamente i dispositivi iOS dismessi.

(Opzionale) Fare clic su **Ripristina predefiniti** per ripristinare la selezione dei filtri predefiniti. La barra di navigazione Filtri visualizza le sezioni selezionate. Se si deselezionano tutte le caselle di controllo della procedura guidata Gestisci filtri, la barra di navigazione laterale Filtri visualizza tutte le sezioni.

4. Fare clic su un punto qualsiasi della procedura guidata di Gestisci filtri per uscire dalla procedura guidata.
5. (Opzionale) Fare clic sull'icona x per chiedere la barra di navigazione laterale Filtri e fare clic su **Filtri** per riaprire la barra di navigazione laterale.
   - Se si utilizza una delle parole non significative elencate nel file stopwords.txt, che fa parte della configurazione del server Apache SOLR, le parole non verranno indicizzate e di conseguenza le entità che contengono le parole non significative non verranno visualizzate nei risultati della ricerca.

- Esempi di entità sono dispositivi, utenti, gruppi, attributi, applicazioni, certificati, audit trail, contenuti e moduli di notifica.
- Esempi di parole non significative sono "circa", "con", "devo", "cui", ecc.

Utilizzo di Ricerca avanzata

È possibile utilizzare l'opzione Ricerca avanzata per cercare dispositivi in base a regole per identificare e visualizzare i dispositivi con criteri specifici. Le regole possono essere costruite utilizzando gli operatori applicabili, tra cui "inizia con", "termina con", "contiene", "non contiene", "non inizia con", "non termina con", "è inferiore a", "è superiore a", "è compreso" e "è uguale a" e "non è uguale a". Le opzioni delle regole possono essere nidificate insieme utilizzando le opzioni QUALSIASI (O) o TUTTO (E). I dispositivi che soddisfano le regole vengono visualizzati sotto la sezione.

Il portale amministratore di Ivanti Neurons per MDM visualizza il numero di gruppi di utenti duplicati e il numero corrispondente di GUID per identificare gruppi duplicati quando si seleziona l'attributo Nome gruppo di utenti nel Generatore di regole. Inoltre, una tabella sotto questa regola visualizza l'elenco di gruppi di utenti duplicati e i relativi dettagli, ad esempio Nome gruppo di utenti, GUID, Origine e Nome distinto (DN).

Procedura

1. Nella pagina Dispositivi, fare clic sul collegamento **Ricerca avanzata**. Si apre la procedura guidata Ricerca avanzata.
2. Fare clic su una delle seguenti opzioni:
   - Fare clic su **Qualsiasi** se è necessario che i dispositivi soddisfino almeno una delle regole
   - **Tutto**: se è necessario che i dispositivi soddisfino tutte le regole

Creare una regola che definisca i criteri di ricerca. **Ad esempio**: Supporto APNS uguale a Sì.

4. (Opzionale) Fare clic su **+** per creare altre regole.
5. Fare clic su **Cerca**. L'elenco dei dispositivi che soddisfano i criteri di ricerca è visualizzato nella pagina.
   - Per i dispositivi iOS 14.0 e versioni successive, l'ID eSIM (EID) del dispositivo è disponibile nella relativa pagina dei dettagli. L'ID eSIM (EID) consente ai gestori telefonici di assegnare la SIM a un dispositivo specifico. Il campo ID eSIM (EID) è conforme al GDPR.
   - Poiché nelle nuove versioni di Ivanti Neurons per MDM sono stati aggiunti ulteriori campi correlati al GDPR (come Indirizzo IP e ID eSIM), gli amministratori che hanno già configurato le opzioni per il GDPR devono modificare il profilo GDPR, se desiderano nascondere i nuovi campi.
   - L'opzione Ricerca avanzata mostra lo stato del blocco di ripristino di un dispositivo.

Caricamento di query di ricerca

È possibile visualizzare l'elenco delle query di ricerca salvate.

Procedura

1. Fare clic su Ricerca avanzata e quindi fare clic sull'icona cartella. L'elenco delle query di ricerca create viene visualizzato nella sezione **Carica query** e vengono mostrati i seguenti dettagli.
   - **Nome query**: nome della query caricata.
   - **Contenuto query**: mostra il contenuto delle regole che definiscono la query di ricerca.
   - **Azioni**: selezionare l'azione da eseguire per la query.
2. Fare clic su **Carica query** nella colonna **Azioni** per visualizzare l'elenco di dispositivi che soddisfano i criteri nella query caricata.

3. Fare clic su **Elimina** per eliminare una query caricata.

7.5.12. Utilizzo della modalità Proprietario del dispositivo

Argomenti della sezione:

- **Provisioning dei dispositivi Android Enterprise tramite codice QR o NFC Bump**
- **Provisioning dei dispositivi Android Enterprise tramite token client**

Licenza: Gold

Dopo la registrazione, è possibile designare i dispositivi come di proprietà dell'azienda o di proprietà del dipendente. Tale designazione consente di gestire i criteri che variano a seconda che l'utente sia proprietario di un dispositivo personale o di proprietà dell'azienda. Con la licenza corretta, è quindi possibile usare la proprietà nelle regole per la creazione di gruppi di dispositivi.

Con un dispositivo nuovo o ripristinato alle impostazioni predefinite utilizzare l'app **Provisioner** per eseguire il provisioning in modalità Proprietario del dispositivo selezionando una delle seguenti opzioni:

- Trasferimento dati tramite NFC (Near Field Communication)
- Scansione del codice QR

Per trasferire dati tramite NFC è necessario toccare un dispositivo nuovo, o ripristinato alle impostazioni predefinite, con il dispositivo principale o modello, allo scopo di eseguire il provisioning.

Una scansione del codice QR presuppone il tocco dello schermo di un dispositivo nuovo o ripristinato alle impostazioni predefinite, la configurazione di una rete Wi-Fi e la scansione del codice quando il dispositivo è pronto per il provisioning.

Mentre si esegue il provisioning della modalità Proprietario dispositivo utilizzando NFC o il codice QR code, l'app Provisioner accetta un token di registrazione. Al momento della registrazione, il token di registrazione viene inviato al server. Se è presente nel server e il dispositivo è assegnato a un utente, il dispositivo è stato registrato correttamente.

Il client Go controlla il dispositivo quando si trova nella modalità Proprietario del dispositivo e blocca lo schermo fino a quando il dispositivo non viene registrato con Ivanti Neurons for MDM, per impedire agli utenti di abbandonare il processo di provisioning. La modalità Proprietario del dispositivo supporta inoltre la modalità tutto schermo. Per le informazioni di configurazione andare a: **Configurazione blocco e tutto schermo**.

Importante

- Se si disattiva un dispositivo in modalità Proprietario del dispositivo, il dispositivo viene ripristinato alle impostazioni predefinite.
- Facoltativamente, tutti i dispositivi in modalità Proprietario del dispositivo possono avere tutte le app di sistema abilitate.
- Un dispositivo può avere attiva una sola modalità Proprietario del dispositivo alla volta.
- Solo i dispositivi compatibili con Android Enterprise possono essere forniti in modalità proprietario dispositivo.
- Per i dispositivi Samsung Knox Standard che sono in modalità Proprietario del dispositivo, agli utenti verrà chiesto di attivare la licenza Samsung ELM. Questa richiesta viene visualizzata anche nei dispositivi Samsung in modalità Proprietario del dispositivo quando l'app del client Go viene aggiornata da una versione precedente a una più recente supportata da Ivanti Neurons for MDM. Dopo l'attivazione, il numero di serie viene visualizzato nella pagina Dettagli dispositivo, che corrisponderebbe al campo Dispositivo > Impostazioni > Numeri di serie.

Provisioning dei dispositivi Android Enterprise tramite codice QR o NFC Bump

Per eseguire il provisioning dei dispositivi Android Enterprise utilizzando il codice QR o il bump NFC è necessario scaricare e installare l'app Provisioner da Google Play sul dispositivo master.

Componenti compatibili

Versione di Provisioner: 1.3.0.

Provisioner è compatibile o funziona con i seguenti componenti:

Elemento	Versione
Sistema operativo Android (sul dispositivo di cui eseguire il provisioning) Sistema operativo Android (sul dispositivo principale)	• Se si utilizza NFC, è necessaria la versione 5.0 o una versione supportata più recente. • Se si utilizzano i codici QR, è necessaria la versione 7.0 o una versione supportata più recente. Il dispositivo deve essere compatibile con Android Enterprise. Dalla 5.1 alla versione supportata più recente. Il dispositivo deve disporre della tecnologia NFC per effettuare il trasferimento dati mediante NFC. Non è richiesta per il codice QR.
Prodotto server UEM, abilitato per Android Enterprise	Una delle opzioni seguenti: Ivanti Neurons for MDM, o Allow-labeled Ivanti Neurons for MDM.
App client Android	La versione dell'applicazione client più recente viene installata automaticamente sul dispositivo con provisioning dal Provisioner.

Prerequisiti

Per impostare un dispositivo Android Enterprise come dispositivo gestito dal lavoro, è necessario:

- Assicurarsi che la configurazione richiesta relativa ad Android Enterprise sia definita e venga applicata al dispositivo registrato.

> La configurazione predefinita di Android Enterprise: Dispositivo gestito dal lavoro deve essere abilitata per il dispositivo.

Abilitare Android Enterprise sul server.

- Disporre di un dispositivo Android con NFC (solo se si utilizza NFC) come dispositivo principale, con l'app Provisioner installata.
- Disporre di dispositivi compatibili con Android Enterprise per il provisioning.

Per abilitare Android Beam per l'utilizzo del trasferimento dati tramite NFC:

Procedura

1. Dal dispositivo, andare a **Impostazioni**
2. Andare a **Reti > Wireless e reti**.
3. Nella **sezione Connettività**, selezionare **Condividi e connetti**.
4. Spostare l'interruttore **NFC** su **Attivato**.
5. Spostare l'interruttore **Android Beam** su **Attivato**.

I passaggi per abilitare NFC e Android Beam possono variare da un dispositivo all'altro.

Eseguire il provisioning dei dispositivi Android Enterprise per farli diventare dispositivi gestiti dal lavoro

Procedura

1. Dal dispositivo principale Android, scaricare l'app Provisioner da Google Play e installarla.
2. Avviare l'app Provisioner sul dispositivo principale.
3. Selezionare NFC o codice QR per il metodo di provisioning.
4. Toccare **App per il provisioning** e scegliere l'app client da installare sul dispositivo sottoposto a provisioning:

Selezionare questa app client:	Per registrarsi con questo server UEM:
Vai	Ivanti Neurons per MDM
At Work UEM	(Allow labeled) Ivanti Neurons for MDM

5. Compilare i campi rimanenti nell'app Provisioner. Nel caso in cui sia presente un tipo di Wi-Fi supportato, è possibile che alcuni campi vengano compilati in modo automatico. I campi Wi-Fi non sono mostrati se è selezionato il codice QR. Utilizzare queste linee guida:

Campo	Valore
Selezionare l'app per il provisioning	Go o At Work
Fuso orario	Immettere il fuso orario da configurare sul dispositivo
Impostazioni locali	Immettere le impostazioni locali da configurare sul dispositivo
Abilita tutte le app di sistema	Fare clic sulla casella di controllo per abilitare tutte le app di sistema
SSID rete Wi-Fi	Immettere l'SSID Wi-Fi che utilizzerà il dispositivo principale
Tipo di protezione Wi-Fi	Immettere il tipo di protezione Wi-Fi
Password Wi-Fi	Immettere la password per il Wi-Fi
Registrazione in blocco	La funzione di registrazione in blocco è facoltativa. Per utilizzare la registrazione in blocco, è richiesto un nome host. Facoltativamente, è possibile immettere un nome utente e selezionare l'opzione di avvio rapido. Per ignorare la funzione di registrazione in blocco, lasciare vuoti questi campi.

6. Toccare **Continua**.
7. Se è stato selezionato **NFC**, toccare **Continua**. La schermata **Bump the devices!** appare sul dispositivo principale. Continuare con la sezione **Trasferimento dati tramite NFC** sotto.
8. Se si è selezionato **Codice QR**, la schermata **Scansionare questo codice QR!** appare sul dispositivo principale. Continuare con la sezione **Codice QR** sotto.

Per eseguire un trasferimento dati tramite NFC, attenersi alla procedura riportata di seguito

Verificare che sul dispositivo di destinazione sia visualizzata la schermata di benvenuto di Android.

9. Premere il retro del dispositivo principale sul retro del dispositivo di destinazione per avviare il trasferimento mediante NFC. Se il trasferimento NFC avviene correttamente, è possibile che il dispositivo di destinazione emetta un suono; procedere quindi con il download dell'app client. Se non è possibile stabilire una connessione Wi-Fi o se il dispositivo non in grado di scaricare l'app client, il dispositivo verrà reimpostato automaticamente alle impostazioni predefinite.
10. Se viene emesso un suono o viene mostrata una schermata diversa da quella di benvenuto, è possibile separare i dispositivi. Generalmente sono necessari alcuni secondi. Se il dispositivo non è crittografato, prima di avviare il download, viene avviato il processo di crittografia.
11. È possibile continuare il provisioning di altri dispositivi trasferendo i dati dei dispositivi al dispositivo principale. Il dispositivo di destinazione deve mostrare la schermata di benvenuto e il dispositivo principale deve mostrare la schermata "Bump the devices!".

Per eseguire il provisioning tramite codice QR, attenersi alla procedura riportata di seguito

Verificare che sul dispositivo di destinazione sia visualizzata la schermata di benvenuto di Android.

12. Toccare 6 volte lo stesso punto della schermata di benvenuto di Android sul dispositivo di destinazione.
13. Verrà chiesto di configurare una rete Wi-Fi in modo che l'installazione guidata possa scaricare un lettore di codici QR sul dispositivo di destinazione.
14. Dopo avere scaricato il lettore di codici QR, viene avviata la fotocamera.
15. Tenere il dispositivo di destinazione pochi centimetri sopra il dispositivo principale finché non viene eseguita correttamente la scansione del codice QR. L'installazione guidata procede quindi con il download dell'app client. Se non è in grado di scaricare l'app client, eseguirà automaticamente un ripristino delle impostazioni predefinite.
16. È possibile continuare il provisioning di altri dispositivi eseguendo la scansione del codice QR sul dispositivo principale. Il dispositivo di destinazione deve avere una fotocamera pronta per la scansione, e il dispositivo principale deve mostrare la schermata "Scansionare questo codice QR!".
17. È inoltre possibile esportare il codice QR toccando l'icona Condividi. Le opzioni per l'esportazione variano a seconda del dispositivo.

Provisioning dei dispositivi Android Enterprise tramite token client

È possibile eseguire il provisioning di un dispositivo Android Enterprise in modalità Proprietario dispositivo utilizzando un token client di marca invece di utilizzare i metodi NFC bump o codice QR. Questo metodo permette di accedere a un dispositivo con un token semplificando l'installazione automatica del client Go o At Work e il provisioning in modalità Proprietario del dispositivo:

> I token client con marchio sono supportati sui dispositivi dotati i account Google gestiti che utilizzano Android 6 o una versione supportata più recente. Per ulteriori dettagli, vedere la guida per gli sviluppatori UEM di Android. https://developers.google.com/android/work/prov-devices#Key_provisioning_differences_across_android_releases.

Requisiti per l'utilizzo di questo metodo:

- È necessario essere registrati con un account Android Enterprise.
- Il dispositivo deve essere compatibile con Android Enterprise.
- Il dispositivo deve utilizzare Android 6 o una versione rilasciata più recente.
- Il dispositivo deve essere nuovo o ripristinato alle impostazioni predefinite.

Configurazione (per dispositivi che eseguono Android 5.0 e versioni successive)

Procedura

1. Nel Ivanti Neurons per MDMportale, andare a **Configurazioni**.
2. Fare clic su **+Aggiungi**.
3. Selezionare **Blocco e Chiosco: Android Enterprise**.
4. Viene visualizzata la pagina **Crea Blocco e Chiosco: Configurazione di Android Enterprise**.

Immettere un nome e una descrizione della configurazione.

5. Scegliere un tipo di blocco.

Fare clic su **Dispositivi di lavoro gestito (Proprietario del dispositivo)**.

6. Vengono visualizzate le opzioni delle impostazioni di blocco proprietario del dispositivo Android.

È possibile, scegliere

- Disattiva Wi-Fi o impostazioni Wi-Fi
- Disattiva fotocamera
- Disattiva Bluetooth
- Non consentire impostazioni Bluetooth
- Disattiva Acquisizione schermo
- Disattiva volume master
- Non consentire Controllo app
- Non consentire credenziali
- Non consentire broadcast di emergenza
- Non consentire reti mobili
- Non consentire tethering
- Non consentire VPN
- Non consentire ripristino delle impostazioni predefinite
- Abilita protezione ripristino delle impostazioni predefinite.

> È possibile specificare facoltativamente un elenco di ID di account Google autorizzati (un valore intero) che possono eseguire il provisioning del dispositivo dopo la reimpostazione delle impostazioni di fabbrica o posizionare il cursore del mouse sopra l'icona della Guida in linea per visualizzare le istruzioni per il recupero degli ID di account autorizzati).

Non consentire Modifica account

- Disattivare NFC (raggio in uscita)
- Non consentire chiamate in uscita
- Non consentire modalità provvisoria
- Non consentire Condividi la posizione
- Non consentire Funzioni di debug
- Assicura Verifica app
- Non consentire SMS
- Non consentire Riattiva microfono
- Disattiva ora automatica
- Disattiva fuso orario automatico
- Disattiva roaming dati
- Disattiva sospensione Wi-Fi
- Limita metodi di input
- Limita servizi di accessibilità
- Disattiva trasferimento file tramite USB
- Disattiva supporti esterni
- Disattiva keyguard (non sarà effettivo se è impostato il PIN/passcode)
- Mantieni lo schermo attivo quando il dispositivo è collegato all'alimentazione
- Non consentire la creazione di finestre
- Salta suggerimenti primo utilizzo

Nella sezione **Abilita/Disabilita app di sistema**, è facoltativamente possibile scegliere di consentire la disattivazione delle app di sistema seguenti:

7. È possibile scegliere di attivare la **modalità tutto schermo**.

Elemento	Versione
Preimposta app di sistema **Fotocamera incorporata** **Telefono integrato**	Fare clic sull'interruttore per **attivare** o **disattivare** l'app della fotocamera incorporata. Fare clic sull'interruttore per **attivare** o **disattivare** l'app del telefono incorporata.
Nome pacchetto app di sistema	Per attivare o disattivare qualsiasi altra app di sistema diversa dalle app di sistema predefinite, fare clic sull'icona + (più) e aggiungere il nome pacchetto app di sistema. Per rimuovere l'app di sistema, fare clic sull'icona -(meno).

Vengono visualizzate le seguenti impostazioni:

- Abilita la modalità di blocco delle attività

- Passa a tutto schermo automaticamente (solo durante la configurazione iniziale)
- Disabilita impostazioni rapide
- Consenti all'utente di accedere alle impostazioni Wi-Fi
- Consenti all'utente di accedere alle impostazioni Bluetooth
- Consenti all'utente di accedere a Impostazioni posizione
- Consenti all'utente di ritardare gli aggiornamenti delle applicazioni
- Consenti all'utente di accedere alle impostazioni di ora e data
- Consenti all'utente di accedere alle impostazioni della rete mobile
- Consenti la selezione della lingua da parte dell'utente
- Abilita dispositivo condiviso (selezionare una qualsiasi delle seguenti opzioni)
  - Abilita accesso
  - Abilita disconnessione (fornire l'impostazione di timeout in ore)

Selezionare facoltativamente le opzioni di personalizzazione predefinite o personalizzate dall'elenco a discesa.

8. Facoltativamente, creare un PIN di uscita da tutto schermo da utilizzare per uscire dalla modalità tutto schermo.
9. Se si desidera, è possibile creare un elenco di app consentite da mettere a disposizione dell'utente in modalità tutto schermo.

Provisioning del dispositivo

Procedura

1. Accendere il dispositivo e immettere la password Wi-Fi. Il dispositivo potrebbe richiedere una password diversa.
2. Nella schermata **Verifica il tuo account** inserire il token Android Enterprise. Fare clic su **Avanti**.
3. Nella schermata **Google Services**, fare clic su **Installa**.
4. Accettare i termini e condizioni.
5. Nella schermata Configura dispositivo di lavoro, fare clic su **Avanti**. Il client Go o At Work viene scaricato e installato sul dispositivo. Il dispositivo entra in modalità Proprietario del dispositivo.

Argomenti correlati

- Registrazione in blocco di dispositivi Android
- Gruppi di dispositivi

7.5.13. Dispositivo gestito con profilo di lavoro

Dispositivo gestito con Profilo di lavoro su dispositivo di proprietà dell'azienda è una modalità in cui il dispositivo Android Enterprise è un dispositivo di proprietà aziendale con dati personali separati dagli altri dati. Questa modalità supporta due profili, grazie alla quale è possibile distribuire le app di lavoro nel profilo gestito e fare in modo che l'utente abbia una sezione personale. La modalità Dispositivo gestito con Profilo di lavoro su dispositivo di proprietà dell'azienda viene creata distribuendo una configurazione Dispositivo gestito con Profilo di lavoro in un dispositivo di cui è stato eseguito il provisioning in modalità proprietario del dispositivo.

Per altre informazioni sui dispositivi gestiti con impostazioni di blocco del profilo di lavoro, vedere **Blocco e tutto schermo: Android Enterprise**.

> Questa modalità richiede Android 8.0 o una versione rilasciata più recente.

Le configurazioni dell'app, i widget di condivisione delle app tra i profili, gli alias del certificato client e i certificati di ID possono essere applicati al Dispositivo gestito con Profilo di lavoro.

Le configurazioni seguenti sono applicabili ai dispositivi Dispositivo gestito con profilo di lavoro:

- Passcode avanzata
- VPN sempre attiva
- Certificato
- Certificato di identità
- Account Google
- Passcode
- Restrizioni per telefoni Samsung
- Difesa dalle minacce
- Wi-Fi
- Autorizzazioni di runtime delle app predefinite
- Attestazione SafetyNet
- Passcode
- Azioni locali di Threat Defense

7.5.14. Registrazione in blocco di dispositivi Android

La funzionalità di registrazione in blocco consente di registrare velocemente numerosi dispositivi Android con Ivanti Neurons for MDM.

Licenza: Silver

Prima di utilizzare la registrazione in blocco, eseguire le seguenti attività:

1. Installare Android SDK, che include Android Debug Bridge (adb), sul computer utilizzato per registrare i dispositivi.
   Per ulteriori informazioni su Android Debug Bridge, vedere: **http://developer.android.com/tools/help/adb.html**.
2. Abilitare il debug USB.
   La procedura per abilitare il debug USB sui dispositivi Android varia in base alla versione. Per ulteriori informazioni su come abilitare il debug USB, vedere **http://developer.android.com/tools/device.html**.
3. Installare il client Go su ogni dispositivo.
4. Connettere i dispositivi tramite cavo USB al computer di provisioning da utilizzare per la registrazione.

È possibile avviare e registrare Go su un server tramite la shell Android Debug Bridge (adb). Android Debug Bridge è uno strumento che può essere utilizzato dalla riga di comando in Windows o nell'utilità Terminale in iOS. Consente di comunicare con un dispositivo Android connesso. Dalla shell adb, il formato del comando è:

> 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

> Il protocollo di registrazione (**mirp**) è usato per codificare i dati rilevanti per la registrazione.

Le chiavi e i valori validi sono:

Chiave	Valore
utente	L'indirizzo e-mail dell'utente che verrebbe inserito nel campo del nome utente tramite iReg. Necessario.
Password	Password dell'utente
pin	PIN di registrazione per l'utente
quickStart	**Quando impostato su VERO:** viene visualizzata la schermata iniziale, ma non per esteso. Nella schermata di benvenuto, quando l'indicatore viene sostituito dal pulsante Continua, la schermata continua a essere visualizzata automaticamente anche senza toccare Continua. Inoltre, questo flusso di provisioning semplificato si verifica su tutti i dispositivi. • Le richieste di riservatezza e di scelta rapida per l'utente vengono saltati. • Sui dispositivi Zebra, il client concede privilegi di amministratore a se stesso, senza una richiesta utente Richiede una versione minima di Zebra MX 4.3. **Se impostato su FALSO:** la schermata iniziale viene visualizzata normalmente e l'utente deve toccare Continua nella schermata di benvenuto. Opzionale, l'impostazione predefinita è FALSO.

> Per effettuare una registrazione in blocco, è necessario utilizzare una password, un PIN o un token.

Questo comando di esempio specifica server, utente, password, PIN e quickstart:

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

Script di esempio di registrazione in blocco

È possibile utilizzare questo script come esempio quando si progetta il proprio script di registrazione in blocco. Questo script di esempio registra tutti i dispositivi collegati alla macchina di provisioning con gli stessi utente e password.

for i in `adb devices | grep -v devices |

do

echo "Registering $i"

adb -s $i shell "am start -a android.intent.action.MAIN -d \"mirp://<servername?user=user email addresspassword=password

done

Messaggi di errore potenziali

Ecco alcuni potenziali errori che si possono incontrare usando la registrazione di massa:

Errore	Risoluzione
schema mirp non trovato	Comando di esempio per schema mirp🇦🇲 am start -a android.intent.action.MAIN -d "xxxmirp://?
URL non valido	Si verifica se non viene inviata alcuna stringa di dati. Verificare che l'URL sia corretto.
informazioni sul server non trovate	Informazioni sul server mancanti o immesse in modo non corretto.
informazioni sull'utente non trovate	Verificare che la chiave utente sia stata immessa.
Informazioni su password/PIN non trovate	Verificare che la chiave del PIN O della password sia stata immessa.

> Quando vengono creati più profili per la Registrazione in blocco:

- Un dispositivo Android Enterprise completamente gestito e registrato in modo nativo riceve l'attributo personalizzato creato con il primo profilo.
- Durante il trasferimento dei dispositivi, se il dispositivo è presente in un profilo di registrazione in blocco, gli attributi personalizzati definiti per il dispositivo da trasferire nel profilo di registrazione in blocco saranno applicati al dispositivo durante il trasferimento. Questo comportamento è lo stesso per i dispositivi Android Enterprise migrati completamente gestiti, perché riceve l'attributo personalizzato del primo profilo.

Inoltre, tutti i profili creati per quel particolare dispositivo vengono visti come attivi.

7.5.15. Registrazione in blocco utilizzando il caricamento file CSV

La registrazione in blocco consente di registrare più dispositivi Android tramite i relativi identificatori. È possibile caricare un file CSV per aggiungere dispositivi in blocco.

Procedura

1. Nella pagina **Dispositivi** fare clic sulla scheda **Registrazione in blocco**. Viene visualizzata la pagina **Registrazione in blocco**.
2. Fare clic su **Aggiungi**.
3. Nel campo di testo **Nome profilo**, inserire il nome del Profilo. Facoltativamente, fare clic su **+Aggiungi descrizione** per aggiungere una descrizione per il file CSV.
4. Nella sezione **Carica CSV** fare clic su **Scarica modello CSV** per scaricare il modello CSV. Utilizzando il formato esistente, è possibile modificare il file per aggiungere dispositivi.

> Consente di registrare fino a 200.000 righe alla volta in CSV.

5. Dopo aver modificato e salvato il file CSV, fare clic su **Carica CSV** per caricare il file CSV. Viene visualizzato un messaggio di conferma relativo alla riuscita del caricamento.

> Le righe con informazioni inadeguate possono causare il mancato caricamento del CSV. Ogni record deve includere almeno il numero di serie e le informazioni sul produttore o il valore IMEI.

> Per rimuovere il file CSV aggiunto, fare clic sull'icona del segno meno (-). Per scegliere un altro file CSV da caricare, fare clic sul collegamento **Scegli un file diverso**.

6. Opzionale: selezionare **Assegna attributi personalizzati senza token** per registrare in blocco tutti i tipi di dispositivi senza generare un token. Questa opzione non è selezionata per impostazione predefinita.

La registrazione in blocco senza token può essere applicata anche quando l'IMEI o la combinazione di numero di serie e produttore (con o senza attributi personalizzati) viene fornita nel file CSV caricato. Tuttavia la registrazione del dispositivo dipende dalla correttezza dei valori degli attributi caricati nel file CSV. La tabella seguente illustra gli scenari in base ai risultati secondo la combinazione dei valori degli attributi immessi per l'iscrizione in blocco:

Scenario	Valori degli attributi immessi			Stato registrazione dispositivo
	IMEI	**Numero di serie**	**Produttore**	
1	Corretto	Non corretto	Non corretto	Il dispositivo è registrato
2	Non corretto	Corretto	Corretto	Il dispositivo è registrato
3	Non corretto	Non corretto	Corretto	Il dispositivo non è registrato
4	Non corretto	Corretto	Non corretto	Il dispositivo non è registrato

> Il nome del produttore non effettua la distinzione tra lettere maiuscole e minuscole.

7. Nel campo **Seleziona utente**, selezionare un utente.
   Il token di registrazione viene visualizzato nella colonna Registrazione token. Per aggiornare il token di registrazione, fare clic su **Aggiorna**.
   La data di scadenza del token viene visualizzata nella sezione **Scadenza token**. Per estendere il periodo di scadenza del token, fare clic su **Estendi**. Nel campo **Estendi fino a** immettere il numero di giorni per cui si desidera estendere la scadenza del token.

> Il numero di giorni specificato deve essere compreso tra 7 e 999. La scadenza predefinita del token è di 7 giorni.
> Se l'opzione **Assegna attributi personalizzati senza token** è selezionata, questa pagina non viene visualizzata.

8. Fare clic su **Fine**.

Dopo il caricamento, in una tabella nella pagina **Profili di registrazione in blocco** sono visualizzati i seguenti dettagli relativi al file CSV caricato.

Impostazione	Descrizione
Nome profilo	Il nome del Profilo.
Descrizione	Una qualche descrizione del profilo.
Ultima modifica	Data dell'ultima modifica apportata al file CSV.
TIPO	Per i profili gestiti autonomamente → Gestiti autonomamente
N. di dispositivi	Numero di dispositivi da registrare in blocco.
Utente associato	Nome dell'utente associato.
Nome utente	Consente di specificare l'utente associato al dispositivo. Richiesto quando è attivato il mapping da dispositivo a utente. L'utente deve esistere in Ivanti Neurons per MDM.
Azioni	È possibile eseguire una delle azioni seguenti: **Scarica inventario esistente** - Fare clic su questo pulsante per scaricare i dettagli su tutti i dispositivi disponibili nel profilo. **Visualizza** - Fare clic su questo collegamento per visualizzare i dettagli dei dispositivi caricati in blocco per la registrazione. **Modifica** - Fare clic su questo pulsante per modificare i dettagli del profilo. Questa opzione è disponibile solo quando viene selezionata l'opzione dispositivo singolo. **Elimina** - Fare clic su questo collegamento per eliminare il profilo. Nella finestra di conferma fare clic su **Sì** per confermare l'eliminazione del profilo caricato.

Per la registrazione è necessario utilizzare il token generato durante il caricamento del file CSV. L'immissione di un token non corretto determina il reindirizzamento al flusso normale di iReg, che richiede l'immissione di ID/password.

Azioni

Quando si visualizzano i profili di Registrazione in blocco dalla sezione Visualizza dettagli profilo, è possibile eseguire altre attività dalla scheda Azioni, presente nella pagina Visualizza dettagli profilo.

- **Aggiungi ulteriori dispositivi** - Utilizzare questa opzione per aggiungere più dispositivi a un profilo. È necessario fornire il **Numero IMEI** o il **Numero di serie**, o entrambi, il **Produttore** e, facoltativamente, le informazioni sugli **Attributi personalizzati** e quindi fare clic su **Salva**.
- **Modifica configurazione** - Utilizzare questa opzione per modificare una configurazione esistente. È possibile aggiungere **Chiavi specifiche Ivanti**, effettuare modifiche agli **Extra del sistema Android predefiniti** o alle **Chiavi personalizzate del sistema Android** e fare quindi clic su **Aggiorna**.
- **Genera QR code** - Utilizzare questa opzione per generare un QR code per la Registrazione in blocco dei profili.
- **Aggiorna token** - Utilizzare questa opzione per aggiornare un token o estenderne la validità. La validità può essere impostata in un intervallo compreso tra 7 e 999 giorni oppure può essere impostata su **Non scade mai**.
- **Modifica utente associato** - Utilizzare questa opzione per modificare un utente associato. È necessario cercare e selezionare l'utente dal popup **Cambia utente associato** e fare clic su **Applica**.
- **Modifica** - Utilizzare questa opzione per modificare i dispositivi dal profilo selezionato. È necessario selezionare i dispositivi e fare clic sul pulsante **Modifica**.
- **Elimina** - Utilizzare questa opzione per eliminare i dispositivi dal profilo selezionato. Una volta selezionati i dispositivi e fatto clic sul pulsante Elimina, a schermo apparirà un messaggio pop-up di conferma. Fare clic su **Elimina**.

I dispositivi gestiti autonomamente hanno stati diversi. È possibile trovare ulteriori dettagli Registrazione a Samsung Knox Mobile.

7.5.16. Device_to_User_BulkEnrollment

File not found!

7.5.17. Registrazione a Samsung Knox Mobile

Samsung Knox Mobile Enrollment consente agli amministratori di registrare i dispositivi Samsung qualificati in Ivanti Neurons for MDM. Utilizzando Knox Mobile Enrollment, un dispositivo può essere spedito direttamente da un rivenditore approvato a un utente finale e il client Go Android verrà scaricato automaticamente con i dati di registrazione precompilati. Per ulteriori informazioni, consultare **Registrazione di Samsung Knox Mobile per Android Enterprise**.

Requisiti

- Elenco dispositivi per IMEI
- File CSV contenente un elenco di dispositivi con un numero IMEI o di serie e, facoltativamente, un nome utente e una password di registrazione.
- Ivanti Neurons for MDM (versione attuale).
- L'account Samsung Knox è stato approvato per la registrazione mobile
- Dispositivi Samsung supportati. Un elenco dei dispositivi Samsung supportati è disponibile **qui**.

7.5.18. Registrazione di dispositivi Oculus

Ivanti Neurons per MDM può ora gestire i dispositivi Quest for Business (dispositivi Oculus). Attualmente, Meta supporta i dispositivi Oculus for Business (OFB) e Quest for Business (QFB) per MDM. È necessario eseguire alcune operazioni di base sulla console Meta per rendere i dispositivi MDM-ready e quindi registrarsi per Ivanti Neurons for MDM.

È possibile iscrivere il parco dispositivi Oculus nella Gestione dispositivi sotto la console Meta Workplace. È necessario accedere a Oculus Business Workplace utilizzando le credenziali condivise nell'e-mail registrata. Nella pagina iniziale, le informazioni su Tutti i dispositivi vengono visualizzate nella sezione Parco dispositivi. La sezione Parco dispositivi offre una panoramica di tutti i dispositivi disponibili in Gestione dispositivi. Questi dettagli includono il nome del dispositivo, lo stato del dispositivo, il sistema operativo (OS), il modello, ecc.

Argomenti della sezione:

- Prerequisiti per la registrazione di dispositivi Oculus
  - **Configurazione di un'app MDM in Gestione dispositivi**
  - **Configurazione del dispositivo Oculus**

Registra un dispositivo OFB con MobileIron Go

  - **Sulla console Ivanti Neurons per MDM**
  - **Client On Go**

Prerequisiti per la registrazione di dispositivi Oculus

Configurazione di un'app MDM in Gestione dispositivi

I Dispositivi / Visori vengono forniti e aggiornati ad almeno la **v28** di **Oculus for Business**. Nella Meta Console, l'amministratore deve impostare un MDM in Gestione dispositivi e mappare i dispositivi Oculus su questo specifico servizio MDM.

Procedura

1. Sulla pagina home di **Oculus Business Workplace**, selezionare **App**.
2. Sotto la **Libreria app**, fare clic sull'app MDM di terze parti che si desidera installare, quindi fare clic su **Aggiorna**.
3. Selezionare l'MDM appropriato per l'app dall'elenco sotto **Gestione dispositivi mobili** e fare clic su **Aggiorna app**.
4. Fare clic sul visore del dispositivo Oculus su cui si desidera installare MDM. A schermo appariranno le informazioni sul dispositivo.
5. Sotto la scheda **Informazioni**, scorrere in basso fino a **Gestione dispositivi mobili**.
6. Fare clic sul pulsante **Modifica** accanto all'opzione **Autorità MDM**.

> Per impostazione predefinita, verrà selezionata l'opzione Gestione dispositivi Oculus. È necessario selezionare l'app MDM Authority e selezionare **MobileIron Go** dall'elenco App MDM Authority.

Fare clic su **Salva**. Il Dispositivo si reimposta automaticamente, dopodiché sarà necessario configurare il dispositivo Oculus usando l'app di configurazione.

Configurazione del dispositivo Oculus

È possibile aggiungere i dispositivi Visore Oculus Quest 2 usando l'app Configurazione dispositivo. Questa app deve essere condivisa con gli utenti richiesti, in modo che gli utenti possano scaricare e installare l'app sui loro dispositivi Android.

Procedura

1. Sotto la sezione **Parco dispositivi**, fare clic su **Dispositivi non configurati**.
2. Fare clic su **Ottieni app configurazione**. La pagina **Invia link di download** appare a schermo.
3. Selezionare uno o più membri del team dall'elenco o fare clic su **Aggiungi destinatario** per selezionare dall'elenco.
4. Fare clic su **Invia collegamento**. Gli utenti selezionati riceveranno un'e-mail con un collegamento per installare l'app **Configurazione dispositivi**.
5. Fare clic sul collegamento **Scarica app configurazione dispositivi** nell'e-mail per installare l'**App configurazione dispositivi** sul proprio dispositivo Android.

> Dopo il download, questa app non apparirà nell'App Store del proprio dispositivo. Sarà necessario ottenerla dalla sezione Download del proprio dispositivo e provvedere quindi a installarla.

Aprire l'app **Oculus for Business** dal proprio dispositivo Android.

7. Accendere i dispositivi Oculus premendo il pulsante di accensione per 2 secondi.
8. Attivare il Bluetooth e posizionare il proprio dispositivo Android vicino ai dispositivi Oculus fino al termine della configurazione.
9. Ricercare i dispositivi Oculus usando il Bluetooth del proprio dispositivo Android.
10. Una volta trovato il dispositivo Oculus richiesto, sarà necessario connetterlo a una rete Wi-Fi per completare la configurazione.
11. Fare clic su **Inserisci Informazioni Wi-Fi** e fornire il Nome di rete e la Password, quindi fare clic su **Salva**. Ora, il dispositivo Oculus viene connesso alla rete Wi-Fi.
12. Fare clic su **Avvia configurazione**. A schermo appare una notifica relativa all'avanzamento della configurazione; in questa fase non chiudere l'app né maneggiare il visore.
    Appare una conferma a schermo. È possibile continuare a ricercare ulteriori dispositivi usando il pulsante **Trova altri dispositivi**.

Registrazione di un dispositivo OFB con MobileIron Go

Sulla console Ivanti Neurons per MDM

Un dispositivo OFB può essere registrato con MobileIron Go su Ivanti Neurons per la console MDM. Tuttavia, la configurazione Dispositivo di lavoro gestito in modalità non GMS (AOSP) (in **Configurazioni**) deve essere distribuita a questi gruppi di dispositivi OFB.

Client On Go

Un dispositivo OFB può essere registrato sul client MobileIron Go. Per registrare il dispositivo OFB, è necessario eseguire le seguenti operazioni:

- Dopo aver completato l'impostazione tramite l'app OFB Setup, continuare a seguire le istruzioni sullo schermo del visore OFB e completare l'impostazione del dispositivo.
- L'app MobileIron Go si avvia automaticamente e occorre fornire le credenziali di accesso e completare la registrazione seguendo le istruzioni MDM.

Ora il dispositivo viene fornito in modalità DO ed è impostato per essere gestito dall'MDM.

7.5.19. Abilitazione di Bluetooth su un dispositivo

Applicabile a:

- iOS 11.3 e versioni successive
- macOS 10.13.4 e versioni successive

È possibile abilitare o disabilitare Bluetooth su un dispositivo.

Procedura

1. Accedere al dispositivo nella pagina **Dispositivi**.
2. Eseguire una delle operazioni seguenti:
    - Selezionare i dispositivi nell'elenco.
    - Fare clic sul nome del dispositivo per visualizzare la pagina delle informazioni del dispositivo.
3. Nel menu **Azioni**, fare clic su **Abilita/Disabilita Bluetooth**.
4. Fare clic su **OK**.

Le modifiche verranno inviate ai dispositivi al successivo check-in.

7.5.20. Pianifica aggiornamento iOS

Applicabile a:

- Dispositivi Registrazione dispositivi supervisionati iOS 9.0 e versioni successive
- Dispositivi iOS 10.3 supervisionati e versioni successive.

È possibile pianificare l'aggiornamento all'ultima versione iOS disponibile. L'opzione di menu **Dispositivo** > **Azioni Aggiorna versione sistema operativo** per i dispositivi iOS supervisionati visualizza un elenco di solo quelle versioni iOS applicabili al dispositivo.

Procedura

1. Accedere al dispositivo nella **pagina Dispositivi**.
2. Fare clic sul nome del dispositivo per visualizzare la pagina delle informazioni del dispositivo.
3. Dal menu **Azioni**, fare clic su **Aggiorna versione SO**.
4. Sulla procedura guidata **Aggiorna versione sistema operativo**, esaminare la versione iOS e selezionare la versione OS dall'elenco a discesa **Aggiorna alla versione**.

> Se inserisci una versione uguale o precedente, appare un messaggio di errore che indica che la versione di iOS di destinazione deve essere maggiore di quella attuale.

5. Fare clic su **Aggiorna**.

Il dispositivo iOS sarà programmato per aggiornarsi all'ultima versione iOS disponibile quando il dispositivo esegue il check-in. Se il dispositivo ha un passcode, dopo che MDM avrà inviato l'aggiornamento al dispositivo, quest'ultimo mette in coda l'aggiornamento e all'utente viene richiesto di inserire il passcode per avviare l'installazione. Per ulteriori informazioni, vedere **Aggiornamenti_software**.

7.5.21. Reinstallare le app del sistema iOS

Applicabile a:

- Dispositivi iOS 11.3 e versioni successive.

Reinstallare le app del sistema iOS eliminate su dispositivi iOS.

Procedura

1. Andare alla **pagina Dispositivi**. In alternativa è possibile fare clic sul nome del dispositivo ed eseguire questa azione dalla pagina dei dettagli del dispositivo.
2. Selezionare uno o più dispositivi iOS.
3. Dal menu **Azioni** , fare clic su **Reinstalla app del sistema iOS**.
4. Nella casella Reinstalla app del sistema iOS, selezionare una o più app del sistema disponibili per l'installazione sui dispositivi.
5. Fare clic su **Reinstalla app**.

Le applicazioni saranno installate sui dispositivi iOS selezionati e compatibili quando i dispositivi eseguono il check-in. Le app di sistema installate in questo modo non saranno considerate app gestite. Se non ci sono dispositivi compatibili selezionati, verrà visualizzato un messaggio che informa che le app di sistema non verranno installato su tali dispositivi.

Per ulteriori informazioni, vedere **Aggiornamenti_software**.

7.5.22. Assegnazione di un dispositivo a un nuovo utente

Potrebbe essere necessario eseguire nuovamente il provisioning di un dispositivo registrato esistente per un nuovo utente, in caso di modifica del ruolo dell'utente o se è stata modificata la relazione precedente dell'utente nei confronti dell'azienda. Questi passaggi consentono di evitare la disattivazione del dispositivo e di ripeterne la registrazione.

Procedura:

1. Accedere al dispositivo nella pagina **Dispositivi**.
2. Fare clic sul nome del dispositivo per visualizzare la pagina delle informazioni del dispositivo.
3. Fare clic sull'icona **Assegna a utente** .

> In alternativa, è possibile selezionare un dispositivo dalla pagina **Dispositivi** e fare clic sull'opzione **Assegna a utente** dal menu **Azioni**.

Iniziare a inserire il nome dell'utente nel campo **Cerca utente**... .

5. Selezionare l'utente desiderato.
6. Fare clic su **Assegna a utente**.
   Verrà eseguito il provisioning del dispositivo per l'utente specificato.

> Negli scenari basati sull'utente o sulla licenza, è possibile assegnare un dispositivo a un utente che ha superato il numero massimo di dispositivi assegnati. Ciò è dovuto al fatto che lo scopo della funzionalità di numero massimo di dispositivi è limitare la registrazione dei dispositivi a supporto degli scenari Bring Your Own Device (BYOD).

Nel caso di licenze basate su dispositivo e sull'utente, l'applicazione del numero massimo di dispositivi non è consequenziale. Nel caso di licenze basate su dispositivo, il costo per il cliente finale non cambia, perché il numero totale di dispositivi nel sistema resta invariato. Nel caso di licenze basate sull'utente, la mancanza di questo controllo rappresenta in effetti un vantaggio per il cliente. Ad esempio, si considerino cinque utenti, da U1 a U5 con 5 dispositivi ciascuno. Con licenze basate sull'utente, ciò implicherebbe il consumo di cinque licenze. Se, al contrario, due dispositivi vengono spostati da U4 e U5 a U1 e U2, il consumo di licenze si RIDUCE da cinque a tre.

7.5.23. Riassegnazione di un dispositivo Android

L'amministratore può trasferire la proprietà di un dispositivo Android da un utente a un altro. Durante la procedura di riassegnazione, il profilo di gestione del dispositivo verrà riconfigurato o rimappato dall'utente corrente al nuovo utente in modalità Android Enterprise. La riassegnazione può essere effettuata su tutti i dispositivi Android Enterprise, ad eccezione dei dispositivi Android Management API (AMAPI) e non può essere effettuata sui dispositivi Android Enterprise del dominio Google.

> La riassegnazione del dispositivo può essere effettuata solo con i dispositivi nella stessa modalità. Ad esempio, un dispositivo in modalità Dispositivo gestito dal lavoro può essere riassegnato a un altro utente nella stessa modalità.

La procedura di riassegnazione del dispositivo avrà i seguenti stati:

- Inizializzato
- Riuscito
- Non riuscito
- In sospeso

È possibile visualizzare lo stato di ultima riassegnazione di un dispositivo nella pagina **Dettagli dispositivo** → scheda **Panoramica** -> **Stato ultima riassegnazione**.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare uno o più dispositivi dall'elenco.
3. Dall'elenco **Azioni**, fare clic su **Assegna all'utente**.
4. In alternativa, è possibile fare clic sul nome di qualsiasi dispositivo. Si apre la pagina **Dettagli dispositivo**. Fare clic sull'icona **Assegna a utente** per visualizzare la schermata Assegna a utente e selezionare l'utente desiderato.
5. Fare clic su **Assegna a utente**. Le opzioni selezionate saranno convalidate per verificare se i dispositivi selezionati possono essere riassegnati agli utenti selezionati o meno.
   Dopo la convalida e la riassegnazione, sullo schermo appare un messaggio di conferma.

> Se è stato selezionato un numero massimo di 10 dispositivi, sullo schermo appare il messaggio "Assegnazione avviata". Se sono stati selezionati 11 o più dispositivi, sullo schermo appare il pop-up "Convalida in corso".

> Riassegnazione dispositivo Android è una soluzione innovativa costruita in modo unico con l'obiettivo di eliminare i dati lasciati dal precedente utente registrato ed è disponibile solo nella SKU SUEM-Premium.

7.5.24. Come forzare il check-in

I dispositivi devono contattare Ivanti Neurons for MDM (check-in) per fornire e ricevere informazioni. I check-in vengono programmati a intervalli regolari. È inoltre possibile richiedere a un dispositivo di eseguire un check-in su richiesta. Forzare il check-in di un dispositivo può accelerare la procedura di applicazione delle configurazioni, l'aggiornamento delle policy e così via.

Procedura

1. Andare in **Dispositivi > Dispositivi**.
2. Selezionare i dispositivi.
3. Fare clic su **Azioni**.
4. Selezionare **Forza il check-in**.
5. È possibile fare clic sul collegamento del nome del dispositivo per andare alla pagina dei dettagli del dispositivo e fare clic sull'icona **Forza il check-in**  e quindi su **OK**.

> Se durante l'elaborazione del comando di installazione della configurazione durante un check-in si verifica un errore nel dispositivo, Ivanti Neurons for MDM non tenta automaticamente di installare la configurazione nel dispositivo durante i successivi check-in. L'amministratore deve riprovare a installare la configurazione manualmente dalla pagina dei dettagli del dispositivo. A questo scopo, andare alla scheda Configurazione e selezionare la configurazione con errore e fare clic su **Riprova installazione**.

7.5.25. Individuazione di un dispositivo

Se la funzione per l'individuazione di un dispositivo è attivata, è possibile visualizzare l'ultima posizione conosciuta del dispositivo. Per attivare questa funzionalità, è necessario modificare la **configurazione della privacy** per abilitare la raccolta dei dati di posizione e applicare la configurazione al dispositivo. Il dispositivo deve inoltre supportare questa funzionalità e gli utenti devono acconsentire alla condivisione dei dati relativi alla posizione.

Procedura

1. Accedere al dispositivo nella pagina **Dispositivi**.
2. Fare clic sul collegamento nella colonna **Nome**.
3. Nella scheda **Panoramica**, fare clic sul collegamento sotto **Posizione del dispositivo**.

Sulla pagina vengono visualizzati i dettagli seguenti:

Nome del campo	Descrizione
Ultima posizione rilevata in data	Vengono visualizzate la data e l'ora di quando il dispositivo è stato individuato.
Coordinate	Vengono visualizzate la latitudine (posizione nord-sud) e la longitudine (posizione est-ovest) del dispositivo.

Sulla pagina è inoltre possibile trovare una mappa con la posizione del dispositivo.

7.5.26. Blocco di un dispositivo

È possibile attivare o disattivare il blocco schermo su un dispositivo. La funzione di blocco funziona in modo diverso in base ai dispositivi in uso.

Procedura

1. Andare in **Dispositivi > Dispositivi**.
2. Selezionare il dispositivo.
3. Fare clic su **Azioni**.
4. Selezionare **Blocca**.
5. In alternativa, fare clic sul collegamento del nome del dispositivo per andare alla pagina Dettagli dispositivo e fare clic sull'icona **Blocca**  e su **OK**.
6. Per le app Android AppConnect, il comando Blocca blocca l'utente fuori dal contenitore e blocca anche il dispositivo. Gli utenti possono accedere nuovamente al dispositivo e all'app AppConnect utilizzando rispettivamente il passcode del dispositivo e il passcode di AppConnect.
7. Per i dispositivi con iOS 7, è possibile immettere un messaggio da visualizzare e un numero di telefono (facoltativo). Queste opzioni forniscono agli utenti del dispositivo delle informazioni sul perché quest'ultimo è stato bloccato e il codice da comporre per sbloccarlo.
8. Per i dispositivi macOS, all'utente viene chiesto di immettere un PIN a 6 cifre come passcode per accedere al dispositivo. Per procedere al blocco dello schermo, l'utente del dispositivo deve:
    1. Immettere il PIN.
    2. Selezionare la casella di controllo per confermare il blocco del dispositivo.
    3. Fare clic su **Sì, invia comando di blocco**.

> In macOS, l'utente può aggiungere facoltativamente un messaggio schermata di blocco e un numero di telefono durante l'impostazione del passcode di blocco del dispositivo.

9. Per i dispositivi ChromeOS, quando si esegue un'operazione di blocco, viene visualizzata una finestra pop-up "Il blocco di un dispositivo potrebbe richiedere all'utente di inserire un codice di accesso per accedere al dispositivo". Fare clic su **Blocca** e lo stato del dispositivo verrà aggiornato a **Disabilita inviato**, mentre lo stato aggiornato del dispositivo sarà visibile dopo la sincronizzazione periodica del dispositivo.

Metodi alternativi di blocco di un dispositivo:

- L'utente di un dispositivo può eseguire l'azione di blocco dal portale self-service.
- Un amministratore può eseguire l'azione di blocco dal portale di amministrazione.

7.5.27. Gestione dei dispositivi Apple in modalità smarrimento

Argomenti della sezione:

- Abilitazione Modalità smarrimento
- Esecuzione di azioni in modalità di smarrimento
- Disabilitazione Modalità smarrimento

Applicabile a: dispositivi supervisionati con iOS 10.3 e versioni successive

È possibile impostare la modalità di smarrimento su un dispositivo supervisionato mediante Ivanti Neurons for MDM. Ciò significa che si può segnalare un dispositivo come smarrito ai server di Apple, recuperando così l'ultima posizione registrata del dispositivo e disattivando la modalità di smarrimento quando il dispositivo viene ritrovato.

Abilitazione Modalità smarrimento

È possibile segnalare ai server Apple lo smarrimento di un dispositivo impostandolo in modalità di smarrimento. Dopo avere impostato il dispositivo in modalità di smarrimento:

- Se il dispositivo viene disattivato, non è possibile disattivare la modalità di smarrimento.
- Se vengono cancellati i dati del dispositivo, non è possibile localizzarlo o monitorarlo.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare la voce relativa al dispositivo.
3. Selezionare **Azioni** > **Comune** > **Abilita modalità smarrimento**.
4. In alternativa, accedere alla pagina **Dettagli dispositivo** selezionando il link del nome del dispositivo. Fare clic sull'icona di azione del dispositivo e selezionare **Abilita modalità smarrimento**.

Esecuzione di azioni in modalità di smarrimento

Dopo avere attivato la modalità di smarrimento, è possibile eseguire le seguenti azioni dalla sezione Modalità dispositivo smarrito:

- Inviare un messaggio/numero di telefono all'iPhone
  - Immettere un messaggio da mostrare sulla schermata di blocco del dispositivo smarrito.
  - Immettere un numero di contatto da mostrare sulla schermata di blocco del dispositivo smarrito. Se qualcuno trova il dispositivo, può chiamare il numero per segnalarlo.

Blocca dispositivo

- **Aggiornare la posizione del dispositivo**

> Se vengono cancellati i dati del dispositivo, non è possibile individuarlo.

- **Riproduci suono per modalità di smarrimento**

> Il suono viene riprodotto finché il dispositivo non viene rimosso dalla modalità di smarrimento o finché un utente non disabilita il suono sul dispositivo.

- **Aggiorna posizione**
  L'opzione **Aggiorna posizione** è stata aggiunta alla **Modalità smarrimento** per visualizzare la posizione del dispositivo. Vengono visualizzati i seguenti dettagli:
  - **Latitudine**: la latitudine della posizione del dispositivo.
  - **Timestamp**: viene visualizzato il timestamp della data e dell'ora del payload.
  - **Longitudine**: la longitudine della posizione del dispositivo.

Disabilitazione Modalità smarrimento

Se il dispositivo in modalità di smarrimento viene recuperato o se la modalità è stata attivata per errore, è possibile disattivarla.

> Se il dispositivo smarrito viene ritirato da Ivanti Neurons per MDM, la disabilitazione della modalità smarrito non funziona.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare la voce relativa al dispositivo.
3. Selezionare **Azioni** > **Comune** > **Disabilita modalità smarrimento**.
4. In alternativa, navigare nella pagina **Dettagli dispositivo** selezionando il link del nome del dispositivo e selezionare **Modalità smarrimento dispositivo: Abilitata** > **Disabilita modalità smarrimento**.

7.5.28. Gestione dispositivi Android in Modalità smarrimento

Argomenti della sezione:

- Abilitazione Modalità smarrimento
- Disabilitazione Modalità smarrimento

Abilitazione Modalità smarrimento

Applicabile a: dispositivi Android 8+

È possibile collocare più dispositivi Android contemporaneamente in Modalità smarrimento attraverso Ivanti Neurons for MDM. Ciò significa che è possibile segnalare un dispositivo smarrito a Ivanti Neurons for MDM mettendo il dispositivo o i dispositivi in Modalità smarrimento, che consente di visualizzare sullo schermo un messaggio personalizzato, un numero di telefono e una nota a piè di pagina, oltre all'opzione di riproduzione di un suono.

> Questa funzionalità supporta solo i dispositivi completamente gestiti, compresi quelli non GMS.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare la casella di controllo relativa ai dispositivi.
3. Selezionare **Azioni > Abilita modalità di smarrimento**.
4. In alternativa, fare clic sul collegamento del nome del dispositivo per andare alla pagina Dettagli dispositivo e fare clic sull'icona ⋮. Selezionare **Abilita modalità di smarrimento**.
5. Immettere un messaggio della schermata di blocco o un numero di telefono o entrambi da visualizzare sulla schermata di blocco dei dispositivi smarriti. Gli amministratori possono anche selezionare le opzioni di nota a piè di pagina e **Riproduci suono modalità smarrimento**. Se qualcuno trova i dispositivi, può chiamare il numero per segnalarlo.

> Per attivare l'opzione **Abilita modalità di smarrimento** è necessario inserire un messaggio o un numero di telefono nei rispettivi campi.

> Il suono della modalità di smarrimento viene emesso per 5 minuti, a meno che il telefono non venga sbloccato, che non venga premuto il tasto di chiamata o che l'amministratore non disattivi la modalità di smarrimento entro tale periodo. Per riprodurre un suono, riattivare la modalità smarrimento sui dispositivi.

6. Selezionare **Abilita Modalità smarrimento** per collocare il dispositivo o i dispositivi Android in Modalità smarrimento.

L'attivazione della Modalità smarrimento disabilita le seguenti azioni:

- Sblocca
- Accesso/Uscita dal chiosco
- Imponi disconnessione per il chiosco condiviso
- Assegna a utente

- Invia messaggio
- Imposta proprietà

> Una volta abilitata la modalità Smarrimento in un dispositivo, l'opzione modalità Smarrimento nel server sarà disabilitata.

Disabilitazione Modalità smarrimento

Se il dispositivo in Modalità smarrimento viene recuperato o se la Modalità smarrimento è stata attivata per errore, è possibile disabilitarla.

> Se il dispositivo smarrito viene cancellato da Ivanti Neurons per MDM, la disabilitazione della Modalità smarrimento non funziona.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare la casella di controllo relativa ai dispositivi.
3. Selezionare **Azioni > Disabilita modalità di smarrimento**.
4. In alternativa, fare clic sul link del nome del dispositivo per accedere alla pagina dei dettagli del dispositivo e selezionare **Modalità smarrimento dispositivo: Abilitato > Disabilita modalità smarrimento**.

> Nella sezione **Dettagli**, **Disabilita modalità smarrimento** diventa visibile solo dopo l'attivazione di **Abilita modalità smarrimento**. Una volta attivato **Disabilita modalità smarrimento**, il campo **Modalità smarrimento dispositivo: Abilitata**, che include l'opzione **Disabilita modalità smarrimento**, scompare.

> I dispositivi che si trovavano precedentemente in modalità Chiosco dovranno essere reinseriti in Chiosco dopo la disattivazione della modalità smarrimento.

7.5.29. Richiesta registri di debug

Per recuperare i registri debug per la risoluzione dei problemi dei dispositivi, è possibile inviare una richiesta ai dispositivi di lavoro gestiti iOS, macOS e Android. Utilizzare il comando "Richiesta di registri debug" nella pagina Dispositivi; nei registri debug sono riportati le azioni, le operazioni completate e gli errori relativi a ogni evento.

Questa funzionalità necessita dei seguenti client:

- I dispositivi iOS richiedono Go 5.3.0 per iOS o una versione successiva supportata. Per i dispositivi migrati da Ivanti EPMM a Ivanti Neurons per MDM, questa funzione richiede Mobile@Work 12.2.0 per iOS o versioni più recenti supportate.
- I dispositivi macOS richiedono Mobile@Work 1.5 per macOS o una versione successiva supportata.
- I dispositivi gestiti da Android richiedono Go 65 per Android o una versione più recente supportata.

Procedura

1. Andare in **Dispositivi > Dispositivi**.
2. Selezionare il dispositivo e fare clic sul nome del dispositivo per andare alla pagina dei dettagli del dispositivo.
3. Fare clic sull'icona ⋮.
4. Selezionare **Richiedi registri debug** e fare clic su **OK**.

Quando la richiesta è stata inviata e i registri sono pronti sul dispositivo, una notifica viene inviata all'amministratore e visualizzata nei registri dei dispositivi. È inoltre possibile scaricare i registri dei dispositivi facendo clic sul collegamento.

7.5.30. Apple_Enhanced_Logging

File not found!

7.5.31. Disattivazione di un dispositivo

Il ritiro di un dispositivo pone fine alla sua relazione con Ivanti Neurons for MDM. È possibile disattivare un dispositivo se:

- l'utente non lavora più in azienda
- l'utente ha sostituito il dispositivo
- è necessario annullare le attività di gestione completate (ricominciare)

Procedura

1. Andare in **Dispositivi > Dispositivi**.
2. Selezionare il dispositivo.
3. Fare clic su **Azioni** (in alto a destra).
4. Selezionare **Disattiva**.
5. È possibile fare clic sul collegamento del nome del dispositivo per andare alla pagina Informazioni sul dispositivo e fare clic sull'icona ⋮.
6. Selezionare **Disattiva** e fare clic su **OK**.

Quando si esegue un'Operazione di ritiro su un dispositivo in stato Attivo, il dispositivo viene ritirato immediatamente.

7.5.32. Cessione della proprietà di un dispositivo

Si applica ai dispositivi Android in modalità Profilo di lavoro su dispositivo di proprietà dell'azienda.

Rinunciare alla proprietà di un dispositivo nella modalità Profilo di lavoro su dispositivo di proprietà dell'azienda consente di rimuovere il profilo di lavoro e di dismettere il dispositivo da Ivanti Neurons for MDM, senza compromettere le app e i dati personali. L'utente finale può quindi utilizzare il dispositivo come un dispositivo personale, con pieno accesso a tutti i controlli e le impostazioni del dispositivo.

> Il dispositivo deve essere rimosso dal portale Registrazione Google Zero Touch o Knox Mobile.

L'utente può alla proprietà di un dispositivo se:

- l'utente non lavora più in azienda
- l'utente ha sostituito il dispositivo

Procedura

1. Andare in **Dispositivi > Dispositivi**.
2. Selezionare il dispositivo.
3. Fare clic sulla **pagina dei dettagli dispositivo** e fare clic sull'icona ⋮.
4. Selezionare **proprietà**.

7.5.33. Cancellazione di un dispositivo

La cancellazione di un dispositivo determina la rimozione di tutti i dati e riporta il dispositivo alle impostazioni predefinite.

Procedura

1. Andare in **Dispositivi > Dispositivi**.
2. Selezionare il dispositivo.
3. Fare clic su **Azioni** (in alto a destra).
4. Selezionare **Cancella**.
5. In alternativa, fare clic sul collegamento del nome del dispositivo per andare alla pagina Dettagli dispositivo e fare clic sull'icona ⋮. Selezionare **Cancella** e fare clic su **OK**.
6. Per impostazione predefinita, è selezionata l'opzione **Preserva piano dati**.
   (Facoltativo, applicabile a dispositivi iOS 11.3+) Selezionare l'opzione **Salta configurazione di prossimità**.
7. Selezionare l'opzione **Riporta in servizio** per effettuare una nuova registrazione in modo automatico dopo la cancellazione dei dati, così da non dover registrare di nuovo manualmente il dispositivo dopo una cancellazione. Applicabile solo per dispositivi iOS 17+ registrati in modalità DEP.
   1. Selezionare la **Configurazione Wi-Fi** dal menu a discesa. L'utente deve disattivare tutti i blocchi di attivazione. Applicabile solo per dispositivi iOS 17+ registrati in modalità DEP.
   2. (facoltativo) Selezionare l'opzione **Preserva app** se si desidera che i dispositivi tornino in servizio con le app esistenti preservate. Verranno preservate solo le app installate utilizzando Ivanti N-MDM con priorità elevata. Applicabile solo per dispositivi iOS 26+.
8. Per i dispositivi macOS è possibile inviare al dispositivo un PIN a 6 cifre come passcode. Sul dispositivo, all'utente viene richiesto di immettere il PIN per accedere al dispositivo. Per continuare con l'azione di cancellazione, l'utente del dispositivo deve:
   1. Immettere il PIN.
   2. Selezionare la casella di controllo per confermare l'azione di cancellazione del dispositivo.
   3. Fare clic su **Sì, cancella il dispositivo**.
9. Per i dispositivi ChromeOS, quando si esegue un'operazione di cancellazione dalla pagina **Dettagli dispositivo** o **Elenco dispositivo** viene visualizzata una finestra pop-up "La cancellazione di un dispositivo lo riporta alle impostazioni di fabbrica, il che può comportare la perdita di dati sul dispositivo". L'azione Cancella varia a seconda della piattaforma.".
   1. Selezionare la casella di controllo "Sono consapevole che la cancellazione non può essere annullata" per confermare l'azione di cancellazione del dispositivo.
   2. Fare clic su **Cancella** per cancellare il dispositivo.

Lo stato del dispositivo cambia in "**Cancellazione inviata**". Lo stato aggiornato del dispositivo sarà visibile dopo una sincronizzazione periodica del dispositivo.

Sui dispositivi Android Enterprise, è possibile eseguire l'azione del dispositivo **Cancella** anche dopo che il dispositivo è stato riavviato ed è rimasto bloccato.

I dispositivi Android che si trovano in stato **Cancellazione in corso** possono essere eliminati usando l'opzione **Elimina dispositivo** presente sulla pagina **Dettagli dispositivo**. Una volta eliminato, il dispositivo perde la connessione al server e diventa non conforme. L'utente deve quindi registrare nuovamente il dispositivo dopo aver eseguito il ripristino di fabbrica.

7.5.34. Eliminazione di dispositivi

Una volta disattivato il dispositivo, è possibile eliminarlo. La sua eliminazione lo rimuoverà da tutte le pagine. È possibile eliminare un dispositivo solo se il suo stato è Ritirato, In attesa di ritiro, Cancellato o In attesa di cancellazione.

Procedura

1. Andare in **Dispositivi > Dispositivi**. A schermo appare l'elenco dei dispositivi.
2. Selezionare i dispositivi che si desidera eliminare.
3. Fare clic su **Azioni**.
4. Sotto la sezione **Comune**, selezionare l'opzione **Elimina dispositivi**. A schermo appare un pop-up.
5. Selezionare l'opzione "Sono consapevole che l'eliminazione non può essere annullata", quindi fare clic su **Elimina dispositivi**.
6. In alternativa, è possibile eliminare un dispositivo seguendo la procedura descritta di seguito:
    - Andare in **Dispositivi** > **Dispositivi**.
    - Nella colonna **Nome visualizzato utente**, fare clic su un link qualsiasi. A schermo appare la pagina **Dettagli dispositivo**. Fare clic su **Dettagli dispositivo**. A schermo appare un messaggio, se si accetta l'avviso e si fa clic su **OK**, il dispositivo specifico viene eliminato.

Eliminazione di più dispositivi

È possibile eliminare più dispositivi selezionando tutti i dispositivi che si desidera eliminare.

Procedura

1. Andare in **Dispositivi > Dispositivi**.
2. Selezionare i dispositivi dall'elenco dei dispositivi disponibili.
3. Fare clic sulla scheda **Azioni**, sotto la voce **Comune** selezionare l'opzione **Elimina dispositivi**.
4. Nella finestra **Elimina dispositivo(i)**:
    1. Selezionare la casella di controllo **Sono consapevole che l'eliminazione non può essere annullata**.
    2. Fare clic su **Elimina i dispositivi validi**, per eliminare i dispositivi selezionati.

7.5.35. Sblocco di un dispositivo

Argomenti della sezione:

- Sblocco di dispositivi Android
- Sblocco di AppConnect per app Android
- Sblocco di un dispositivo iOS
- Sblocco dispositivi ChromeOS

Per sbloccare un dispositivo:

È possibile cancellare il blocco schermo di un dispositivo. Lo sblocco funziona in modo diverso in base ai diversi modelli di dispositivi.

Procedura

1. Andare in **Dispositivi > Dispositivi**.
2. Selezionare i dispositivi.
3. Fare clic su **Azioni**.
4. Selezionare **Sblocca**.
5. In alternativa, fare clic sul collegamento del nome del dispositivo per andare alla pagina Dettagli dispositivo e fare clic sull'icona **Sblocca** e su **OK**.

Sblocco di dispositivi Android

Quando viene ricevuto un comando di sblocco, l'app Android tenta di reimpostare il passcode. Nelle modalità Amministratore dispositivo e Proprietario dispositivo, il codice di sblocco viene reimpostato, mentre nelle modalità Proprietario profilo e Abilitato personale di proprietà dell'azienda, il codice di sblocco del profilo di lavoro viene reimpostato.

Il comando di sblocco consente all'amministratore di impostare il codice di sblocco con una combinazione di caratteri alfanumerici. L'opzione predefinita, che imposta il codice di sblocco su '0000', può essere eseguita su più dispositivi. Tuttavia, la nuova opzione, Codice di sblocco personalizzato per Android, può essere eseguita su un dispositivo alla volta. Il numero minimo di caratteri deve essere 6 e quello massimo 8. Questa opzione è disponibile nella scheda **Azioni** e nella pagina **Dettagli dispositivo**. Quando si seleziona l'opzione Sblocca dalla scheda **Azioni** o dalla pagina **Dettagli dispositivo**, vengono visualizzate le due opzioni seguenti.

- Predefinito
- (solo Android) Fornire un codice di sblocco - È possibile fornire un codice di sblocco da questa sezione e fare clic su **Sblocca**.
    - Salta la richiesta di reimpostazione del passcode sul dispositivo - Selezionare per saltare la reimpostazione del passcode se la configurazione del passcode viene inviata a un dispositivo.

Dopo aver impostato il codice di sblocco, l'amministratore può trovare il codice di sblocco nelle pagine **Audit Trail** e **Registri dispositivo**.

> Lo sblocco Directboot funziona solo con l'opzione di sblocco predefinita, il codice di sblocco '0000'. Il codice di sblocco personalizzato per l'avvio diretto non è supportato.

Sblocco di AppConnect per app Android

Per le app AppConnect, il comando **Sblocco di AppConnect** consente di sbloccare i contenitori che sono stati bloccati perché gli utenti hanno tentato di accedere diverse volte con passcode errati. Questa opzione non sblocca il dispositivo.

Sblocco di un dispositivo iOS

Ricevuto un comando di sblocco, l'app iOS rimuove il passcode dal dispositivo. Se la **configurazione del codice di accesso** specifica la necessità di un nuovo codice di accesso, verrà richiesto all'utente del dispositivo di impostare un nuovo codice di accesso conforme alle regole definite nella configurazione del codice di accesso. L'utente deve effettuare le modifiche entro 60 minuti oppure l'app forzerà l'utente a impostare il nuovo passcode.

Sblocco dispositivi ChromeOS

Quando si seleziona un dispositivo ChromeOS e si fa clic sull'opzione **Sblocca** viene visualizzata una finestra pop-up: "lo sblocco può cancellare un codice di accesso esistente per consentire all'utente di accedere al dispositivo. Lo sblocco varia a seconda della piattaforma". Fare clic su **Sblocca** e lo stato del dispositivo verrà aggiornato a "Sblocco inviato"; lo stato aggiornato sarà visibile dopo la sincronizzazione periodica del dispositivo.

7.5.36. Riavvio o arresto dei dispositivi

Argomenti della sezione:

- Riavvio di un dispositivo
- Arresto di un dispositivo

Applicabile a: Android 7.0+ (dispositivi gestiti), dispositivi iOS 10.3+ supervisionati, tvOS 10.3+ supervisionati, macOS 10.13+ e Windows 10+.

Gli amministratori possono riavviare o arrestare un singolo dispositivo supervisionato iOS dalla pagina dei dettagli del dispositivo oppure più dispositivi dalla pagina dell'elenco dei dispositivi.

Riavvio di un dispositivo

Procedura

1. Andare su **Dispositivi**.
2. Scorrere fino al dispositivo.
3. Fare clic sul collegamento nella colonna **Nome**.
4. Fare clic sul pulsante **Azioni**.
5. Fare clic su **Riavvia/Arresta dispositivo**.

> I dispositivi non supportati non possono essere riavviati.

6. Leggere l'avviso visualizzato.
7. (Facoltativo) Selezionare l'opzione per cancellare il passcode del dispositivo al riavvio. Se il passcode non viene cancellato, il dispositivo richiederà un passcode e non verrà connesso alla rete Wi-Fi dopo il riavvio.
8. Selezionare **Riavvia dispositivo**, se tale opzione non è già selezionata.
9. Se si desidera ancora riavviare il dispositivo, fare clic su **Invia a dispositivo**. In caso contrario, fare clic su **Annulla**.

> Per i dispositivi Android, gli amministratori possono visualizzare le informazioni relative al momento del riavvio del dispositivo nella sezione **Uptime** della pagina dei dettagli del dispositivo.

È possibile riavviare più dispositivi supportati dalla pagina dell'elenco dei **dispositivi**. A tale scopo, selezionare i dispositivi, fare clic su **Azioni > Riavvia/Arresta dispositivo** e seguire le istruzioni visualizzate.

Arresto di un dispositivo

Procedura

1. Andare su **Dispositivi**.
2. Scorrere fino al dispositivo.
3. Fare clic sul collegamento nella colonna **Nome**.
4. Fare clic sul pulsante **Azioni**.
5. Fare clic su **Riavvia/Arresta dispositivo**.

I dispositivi non supportati non possono essere riavviati.

6. Leggere l'avviso visualizzato.
7. Selezionare **Arresta dispositivo**.
8. Se si desidera ancora arrestare il dispositivo, fare clic su **Invia a dispositivo**. In caso contrario, fare clic su **Annulla**.

È possibile arrestare più dispositivi supportati dalla pagina dell'elenco dei **dispositivi**. A tale scopo, selezionare i dispositivi, fare clic su **Azioni > Riavvia/Arresta dispositivo** e seguire le istruzioni visualizzate.

7.5.37. Cancellazione della password restrizioni (solo iOS)

È possibile cancellare una password restrizioni impostata dagli utenti sui dispositivi supervisionati con iOS 8. Questa azione è disponibile soltanto per i dispositivi attivi.

Procedura

1. Andare in Dispositivi > Dispositivi.
2. Selezionare la voce relativa al dispositivo.
3. Selezionare Azioni > Cancella password restrizioni.
4. Confermare l'azione quando richiesto.

7.5.38. Eliminazione dell'associazione Sentry per un dispositivo

L'associazione Sentry viene effettuata nei dispositivi per il tunnelling delle app o per il sistema di e-mail abilitato per ActiveSync che controlla l'accesso e-mail ai dispositivi. Se necessario, qualunque dispositivo associato a Sentry può essere rimosso dall'associazione come segue:

Procedura

1. Andare in **Dispositivi**.
2. Nella colonna **Nome**, fare clic sul collegamento del dispositivo per cui si desidera eliminare l'associazione Sentry.
3. Fare clic sulla scheda **Sentry**.
4. Nella colonna **Azioni**, fare clic su **Elimina**.

7.5.39. Assegnazione di attributi personalizzati ai dispositivi

È possibile assegnare attributi personalizzati, come ID interno, a uno o più dispositivi. Ciascun attributo dispone di un valore che è possibile utilizzare per attività quali la creazione di configurazioni e gruppi di dispositivi. Dopo aver creato attributi personalizzati, è possibile assegnarli ai dispositivi. Per ulteriori informazioni sulla gestione degli attributi, vedere **Attributi**.

Procedura

1. Accedere al Portale amministrativo.
2. Andare su **Dispositivi**.
3. Selezionare uno o più dispositivi.
4. Fare clic su **Azioni**.
5. Selezionare **Assegna attributi personalizzati**.
6. Selezionare *una* delle seguenti opzioni:
    - Consente di forzare l'assegnazione (la sovrascrittura) di tutti gli attributi, anche in presenza di valori esistenti.
    - Consente di sovrascrivere solo se il valore è vuoto e di ignorare gli attributi con valori esistenti.

Selezionare gli attributi che si desidera assegnare e immettere i relativi valori (non sono consentiti campi vuoti).

8. Fare clic su **Assegna**.

> Gli **Attributi dispositivo personalizzato** con i loro valori possono essere esportati in formato CSV dalla pagina **Dettagli dispositivo**.

7.5.40. Rimozione di attributi personalizzati dai dispositivi

Si tenga presente che questa azione non può essere annullata. Per rimuovere attributi personalizzati da uno o più dispositivi, procedere come segue:

Procedura

1. Andare su **Dispositivi**.
2. Selezionare uno o più dispositivi.
3. Fare clic su **Azioni**.
4. Selezionare **Rimuovi attributi personalizzati**.
5. Selezionare gli attributi da rimuovere.
6. Fare clic su **Rimuovi**.

7.5.41. Sincronizzazione e recupero del feedback per un'app

È possibile inviare una richiesta a un'app installata nei dispositivi Android, per ottenere informazioni dettagliate sullo stato di configurazione dell'app. Quando l'utente invia una richiesta, riceve un report di feedback sulla configurazione dell'app per il dispositivo.

Procedura

1. Andare su **Dispositivi**.
2. Fare clic sul dispositivo per cui si desidera inviare la richiesta.
3. Fare clic su **Azioni**.
4. Selezionare **Sincronizza e recupera feedback app**. La richiesta di sincronizzazione e recupero del feedback per sulla configurazione dell'app viene inviata. Il campo Ultima sincronizzazione del feedback app accanto al campo Ultimo check-in del client viene aggiornato.
5. Nella scheda **App installate** fare clic sul collegamento **Visualizza dettagli** per l'app nella colonna **Feedback app**. Viene visualizzata la finestra **Feedback app**.
   Chiave - Fornisce informazioni dettagliate e il posizionamento delle impostazioni segnalate (nella configurazione dell'app gestita dell'app) in base al feedback ricevuto dalle app.
   Indicatore data e ora - Data e ora della chiave.
   Gravità -Indica il livello di gravità della chiave. Esempio: "Informazioni", "Errore".
   Messaggio - Tipo di messaggio ricevuto dal feedback sulla configurazione dell'app. Esempio: "Errore".
   Dati - Informazioni dettagliate sui dati ricevuti dal feedback sulla configurazione dell'app.

Visualizzazione del feedback sulla configurazione dell'app dall'App Catalog

Il report di feedback sulla configurazione di un'app specifica può essere visualizzato nell'App Catalog.

Procedura

1. Andare in **App > Catalogo app**.
2. Selezionare l'app per cui si desidera visualizzare i dettagli.
3. Fare clic sulla scheda **Feedback configurazione app**. Nella colonna **Conteggio dispositivi** viene visualizzato il numero di dispositivi (collegamento ipertestuale) per ciascuna chiave del report di feedback sulla configurazione dell'app.
4. Fare clic sul collegamento ipertestuale del numero dei dispositivi per visualizzare i dettagli relativi ai dispositivi. Se ad esempio si fa clic sul collegamento ipertestuale 5, vengono visualizzati i dettagli relativi a 5 dispositivi. Per la combinazione "Chiave" e "Gravità" visualizzata sopra la tabella vengono mostrati i dettagli seguenti:
   Indirizzo e-mail - Specifica il nome utente. Se si fa clic sul collegamento del nome utente, si accede alla scheda **App installate** in **Dispositivi> Dettagli dispositivo**.
   Tipo di dispositivo - Specifica il modello del dispositivo.
   Sistema operativo - Numero di versione del sistema operativo Android.
   Numero di serie - Numero di serie del dispositivo.
   Indicatore data e ora - Data e ora dell'ultimo aggiornamento.
   Messaggio - Tipo di messaggio ricevuto dal feedback sulla configurazione dell'app. Esempio: "Errore".
   Dati - Informazioni dettagliate sui dati ricevuti dal feedback sulla configurazione dell'app.

Per visualizzare notifiche di errori di feedback di configurazione delle app per il dispositivo Android, fare clic sull'icona della campana (in alto a destra) o nella pagina **Dashboard > Notifiche**. Facendo clic sul link della notifica viene aperta la scheda **Feedback configurazione app** e viene visualizzato il report di feedback dell'app.

> Se si cancellano i dati del dispositivo o se quest'ultimo viene dismesso, il report di feedback di configurazione dell'app viene rimosso e non più visualizzato. In background, viene eseguito un processo che elimina i dati più vecchi di 7 giorni ogni 24 ore.

7.5.42. Impostazione della password del firmware

Applicabile a: macOS 10.13 o versioni successive supportate.

L'amministratore può impostare o aggiornare la password del firmware (EFI) per un dispositivo macOS. Le password del firmware impediscono l'avvio del dispositivo macOS da qualsiasi dispositivo di archiviazione interna o esterna al di fuori del disco di avvio selezionato dall'utente del dispositivo. Di conseguenza, impedisce di utilizzare la maggior parte delle combinazioni di tasti per l'avvio.

Procedura:

1. Andare su **Dispositivi**.
2. Per impostare o modificare la password del firmware per un singolo dispositivo, procedere come segue:
    1. Fare clic sul nome utente al quale è associato il dispositivo per visualizzare la pagina dei dettagli del dispositivo.
    2. Nella sezione Generali, espandere **Password del firmware** e fare clic su **Imposta password** o su **Imposta/modifica password del firmware** dal menu Azioni del dispositivo.
    3. In questa sezione vengono visualizzate le seguenti informazioni:
        1. **Password:** la password o un elenco di password probabili.

            > Quando un amministratore imposta la password del firmware, il comando viene inviato al dispositivo. Se il dispositivo non risponde in tempo, la password viene memorizzata temporaneamente e mostrata in questo campo. La nuova password non verrà attivata fino a quando non viene inviato un riscontro dal dispositivo e quest'ultimo non viene riavviato. Fino a quel momento, vengono mostrate tutte le possibili password. Dopo il riavvio del dispositivo e il riscontro della modifica della password, tutte le password indesiderate vengono cancellate.

        2. **Modifica in attesa -** Indica se la modifica della password è in attesa.
        3. **Stato comando -** Indica se la modifica della password è riuscita o meno.
        4. **Consenti OptionROM:** indica se le optionROM devono essere attivate. Per impostazione predefinita, è impostato su No.

Per impostare o modificare la password del firmware per più di un dispositivo, procedere come segue:

1. Selezionare i dispositivi.
2. Dal menu Azioni, fare clic su **Imposta/modifica password del firmware**.

Immettere la password attuale e quella nuova.

Se si sta impostando la password per la prima volta, il campo della password attuale può essere lasciato vuoto.

Per reimpostare la password, lasciare il campo della nuova password vuoto.

5. Fare clic su **Salva**.

> Solo i dispositivi con versioni di macOS supportate verranno aggiornati con la nuova password. I dispositivi non supportati verranno ignorati.

7.5.43. Rilascio di una nuova chiave di ripristino personale

Applicabile a: dispositivi macOS con Mobile@Work per macOS 1.66 o versioni supportate successive.

Durante la migrazione da altre soluzioni MDM a Ivanti Neurons per MDM, gli amministratori possono richiedere al sistema operativo di rilasciare una nuova chiave di ripristino personale (PRK) al momento della registrazione, se era già stata rilasciata una PRK prima della registrazione. Ciò consente di archiviare la chiave in Ivanti Neurons per MDM.

È possibile visualizzare le voci dei registri di Audit trail per le attività PRK come segue:

1. Andare in **Dashboard > Audit trail**.
2. Nel filtro Tipo, selezionare **Chiave di ripristino personale**. Le voci PRK verranno visualizzate nella categoria Gestione dei dispositivi e verranno visualizzate attività quali "Visualizzata chiave di ripristino personale".

Prerequisito

Prima di eseguire la procedura, distribuire le seguenti configurazioni ai dispositivi:

- Configurazione di Mobile@Work per macOS.
- Configurazione della chiave di ripristino di FileVault.

Procedura

1. Contattare il supporto per richiedere allo script di generare una nuova PRK sul dispositivo.
2. Creare un attributo personalizzato del dispositivo con il nome "deviceprk" utilizzato nello script.
3. Caricare lo script nell'archivio in **Amministratore > Script e file > Tutti gli script**. Durante questa operazione, selezionare l'attributo personalizzato "deviceprk".
4. Creare un gruppo di dispositivi dinamico includendo i dispositivi per cui la chiave PRK non è stata recuperata dalla soluzione MDM precedente. Selezionare le regole del gruppo di dispositivi come segue: "**Piattaforma = macOS, Cifratura abilitata = Sì**, **Chiave di ripristino personale macOS depositata = No** e **Tipo di chiave di ripristino macOS = Personale**".
5. Creare una configurazione dello script di Mobile@Work per macOS in cui sia possibile selezionare lo script PRK nell'archivio. Distribuire la configurazione al nuovo gruppo di dispositivi.
6. Pianificare lo script affinché venga eseguito una volta al giorno o come desiderato. A ogni esecuzione, lo script chiederà di inserire la password utente. Per impostazione predefinita, il periodo di timeout per l'esecuzione dello script è 60 secondi. Si consiglia di estendere il periodo di timeout nella configurazione di Mobile@Work per macOS corrispondente impostando il campo **Tempo di esecuzione massimo** su 300 secondi.

- La chiave decrittata è disponibile nella pagina dei dettagli del dispositivo nella sezione Stato crittografia dispositivo. Fare clic su **Visualizza** accanto al campo Crittografia FileVault abilitata.
- Durante il recupero della chiave PRK, il dispositivo viene spostato fuori dal gruppo di dispositivi. Pertanto, la configurazione dello script non sarà più applicabile e verrà eliminata dal dispositivo.
- Dopo che MDM ha recuperato la chiave di ripristino di un dispositivo utilizzando lo script, quest'ultimo viene disinstallato dal dispositivo.

Argomenti correlati:

- **Attributi**
- **Tutti gli script**
- **Gruppi di dispositivi**
- **Mobile@Work per macOS**
- **Chiave di ripristino di FileVault**

7.5.44. Impostazione o modifica di un blocco di ripristino

Applicabile a: macOS 10.15 e versioni successive

L'amministratore può impostare o modificare il blocco di ripristino per il riavvio di un dispositivo macOS con processore Apple. Un blocco di ripristino impedisce l'avvio dei dispositivi macOS in modalità di ripristino, a meno che venga immesso il passcode.

Procedura:

1. Andare su **Dispositivi**.
2. Per impostare o modificare il blocco di ripristino per il riavvio:
    1. Fare clic sul nome utente visualizzato a cui è associato il dispositivo per visualizzare la pagina dei dettagli del dispositivo. Eseguire una delle operazioni seguenti:
    2. Nella sezione **Panoramica**, espandere **Blocco di ripristino** e fare clic su **Imposta password** o su **Modifica password**. Altrimenti, fare clic sul menu **Azioni** (puntini di sospensione), quindi su **Imposta/Modifica blocco di ripristino**.
    3. Nella finestra di dialogo **Imposta/Cambia blocco recupero** procedere come segue:
        1. **Password corrente**: immettere la password corrente qui. Mantenere il campo vuoto se la si sta impostando per la prima volta.
        2. **Password**: immettere la password che si desidera impostare.
        3. **Conferma password**: digitare nuovamente la password che si desidera impostare.

Fare clic su **Imposta/Modifica blocco di ripristino**.

> In Panoramica, l'opzione **Blocco di ripristino abilitato** mostra lo stato del passcode di blocco di ripristino.

> Gli amministratori possono cancellare il passcode rimuovendo il passcode esistente, quindi facendo clic su **Imposta/Modifica blocco di ripristino**.

7.5.45. Gestione accessi Apple

Prerequisiti:

- Verificare e bloccare il dominio su Apple Business Manager o Apple School Manager.
- Configurare almeno un server MDM delle organizzazioni Apple Business Manager o Apple School Manager, dove gli ID Apple gestiti sono presenti in Ivanti Neurons per MDM.

L'accesso all'ID Apple gestito consente alle organizzazioni di controllare quali servizi e funzioni Apple sono accessibili agli utenti.

In Apple Business Manager o Apple School Manager, **l'impostazione Consenti account Apple gestito su** controlla dove gli utenti possono accedere con i loro ID Apple gestiti. Gli amministratori possono configurare questa impostazione per limitare l'accesso ai dispositivi gestiti o supervisionati, oppure per consentirlo su qualsiasi dispositivo.

- **Qualsiasi dispositivo** (predefinito): gli utenti possono accedere con i loro ID Apple gestiti su qualsiasi dispositivo, indipendentemente dal fatto che sia gestito da una soluzione MDM.
- **Solo dispositivi gestiti**: gli utenti possono accedere solo ai dispositivi gestiti da una soluzione MDM che supporta l'endpoint Ottieni token.
- **Solo dispositivi supervisionati**: gli utenti possono accedere solo ai dispositivi supervisionati (e gestiti) da una soluzione MDM che supporta l'endpoint Ottieni token.

Queste impostazioni fanno parte della più ampia "Gestione degli accessi" per i servizi Apple all'interno di Apple Business Manager e Apple School Manager.

> Con una maggiore sicurezza, la limitazione dell'accesso ai dispositivi gestiti o supervisionati può migliorare la sicurezza dei dati, garantendo che i dati relativi al lavoro siano accessibili solo sui dispositivi controllati.

L'accesso all'account Apple gestito non riuscirà se nella scheda **Registrazione dispositivi** sono presenti zero o più organizzazioni di server MDM e l'amministratore regola l'impostazione **Consenti account Apple gestito su** presente in **Gestione accessi** > **Servizi Apple** su "Solo dispositivi supervisionati" o "Solo dispositivi gestiti" in Apple Business Manager o Apple School Manager.

> I dispositivi non riusciranno ad accedere se l'account **Apple gestito** non è presente nel server MDM Ivanti Neurons per MDM Registrazione dispositivi.

7.5.46. Registrazione criteri di gruppo

I dispositivi Windows 10/11 possono essere registrati in Ivanti Neurons per MDM utilizzando un criterio di gruppo. La creazione di un criterio di gruppo registrerà automaticamente tutti i dispositivi collegati in modo ibrido ad Azure AD.

ProcedurePer registrare i dispositivi con un criterio di gruppo

	1.	**Assicurarsi che i dispositivi siano collegati in modo ibrido ad Azure AD. Per maggiori informazioni, consultare la documentazione Microsoft: Dispositivi uniti Hybrid Azure AD.**
	2.	**Creare un oggetto Criteri di gruppo. Per maggiori informazioni, consultare la documentazione di Microsoft: Configurazione della registrazione automatica per un gruppo di dispositivi.**
	3.	**Creare un gruppo di sicurezza che includa i dispositivi da registrare. Per maggiori informazioni, consultare la documentazione di Microsoft: Gruppi di sicurezza di Active Directory.**
	4.	**Collegare l'oggetto Criteri di gruppo al gruppo di sicurezza. Per maggiori informazioni, consultare la documentazione di Microsoft: Collegare il GPO al dominio.**

Esperienza utente

Quando un utente accede al dispositivo utilizzando le credenziali di Azure AD, Microsoft trova la configurazione MDM basata su Azure AD che appartiene alla relativa organizzazione. Il dispositivo è registrato in Ivanti Neurons per MDM e può ricevere criteri e comandi.

8. App

Argomenti della sezione:

- Catalogo app
- Apps@Work
- Caratteristiche dell'AppStore iOS Apps@Work
- Visualizzazione dei dettagli delle app
- Configurazione dell'app
- Assegnazione di attributi personalizzati alle app
- Configurazioni gestite per Android
- Gestione delle app Google Play
- Rimozione di app dal Catalogo app
- Aggiornamento di app interne
- Ricerca del nome del pacchetto per le applicazioni Android
- Categorie
- Filtri di distribuzione
- Escludere o distribuire le app
- Recensioni
- Apple App e libri
- Impostazioni catalogo
- Distribuzione di dipendenze delle app
- Distribuzione di Divide Productivity con Android Enterprise
- Configurazione dell'app Provisioner
- Gestione delle applicazioni Windows
- Ivanti Bridge

8.1. Catalogo app

Argomenti della sezione:

- Licenze per le funzioni delle app
- Passaggio tra visualizzazione griglia e visualizzazione elenco
- Aggiunta di app Google Play Store per Android Enterprise
- Aggiunta di un'app da uno store pubblico
- Aggiunta di un'app interna
- Delega delle autorizzazioni del dispositivo per le app interne di Android Enterprise
- Visualizzazione dello stato del profilo di provisioning per le app interne iOS
- Aggiornamento del profilo di provisioning per le app iOS interne
- Distribuzione delle app interne in Google Play
- Aggiunta di un'app Web per dispositivi Android Enterprise
- Aggiunta di un'app Web per dispositivi iOS
- Utilizzo di Ricerca avanzata
- Esportazione delle app in un file CSV

Utilizzare la pagina Catalogo app per gestire il catalogo delle app. Nel Catalogo app vengono elencate le app mobili rese disponibili agli utenti. Queste includono le app che gli utenti possono scaricare dagli app store pubblici e le app che si intende distribuire usando Ivanti Neurons for MDM (app interne). Le app abilitate ad AppConnect, GoClient per iOS e M@W per macOS sono disponibili anche come app aziendali nella pagina Catalogo app, semplificando così il processo di importazione per la configurazione e la distribuzione. Sui dispositivi Solo MAM, all'apertura dell'App Catalog gli utenti iOS devono selezionare il certificato per autenticare l'accesso alle app.

I dispositivi Apple MacBook dotati di chipset M1 supportano le app VPP per iPhone e iPad. Solo l'amministratore può eseguire il push delle app VPP per iPhone e iPad supportate. Non è disponibile alcuna opzione equivalente che permetta agli utenti di eseguire l'installazione dall'App Catalog.

Per i tenant Ivanti Neurons for MDM con dispositivi Android, se Android Enterprise non sarà abilitato entro la fine di marzo 2021, gli amministratori non saranno in grado di cercare le app con i nomi. La comunicazione relativa a questo cambiamento viene mostrata con un messaggio banner quando si esegue l'accesso alla pagina App Catalog. Questo messaggio banner continua a essere visualizzato finché Android Enterprise non è abilitato su questi tenant e finché non viene selezionata l'opzione 'Non mostrare più questo messaggio'.

- il metodo di installazione dell'app invisibile all'utente non è disponibile per le app macOS pubbliche. Le app macOS possono essere distribuite anche mediante Apple Apps e Books tramite licenze basate su dispositivo e mediante il metodo di installazione app invisibile all'utente al momento delle registrazioni.
- Durante il caricamento dell'app Go sul server Ivanti Neurons for MDM, se risulta necessario selezionare l'opzione **Converti in app gestita**, l'utente deve abilitare anche l'opzione **Installa su dispositivo**.
- App Catalog e l'installazione di app non sono supportati per dispositivi Sonim XP5s.
- Android non consente la disinstallazione delle app con privilegi di amministratore attivi. Per disinstallare un'app di questo tipo, andare a **Impostazioni dispositivo > Sicurezza > Amministratori dispositivo** e disattivare i privilegi di amministratore dispositivo. Quindi, disinstallare l'app.

- Se un'app Android Enterprise viene installata manualmente utilizzando l'Android Enterprise Play Store sul dispositivo e se l'amministratore in seguito annulla la distribuzione dell'app, anche l'app deve essere disinstallata manualmente.
- Le app Android interne non possono essere caricate se l'app è compressa o offuscata.
- Le app pubbliche non sono supportate su **iPad condivisi**.
- A causa di una limitazione da parte di Apple, per le app iOS Business-to-Business (B2B) disponibili nel Catalogo app, le descrizioni e gli screenshot delle app non sono disponibili nella scheda **Dettagli**.
- Quando si cerca un'app nel Catalogo app o nel portale Amministratori, i risultati della ricerca saranno basati su **Nome app**, **Commento**, **Descrizione**, **Mostra versione** e **Novità**. Se i dati dell'app ricercata corrispondono a uno di questi campi, verranno visualizzati come risultati della ricerca.

Licenze per le funzioni delle app

Le funzioni del Catalogo app riportate di seguito richiedono licenze aggiuntive:

- Installazione/disinstallazione app invisibile all'utente: licenza Silver
- Configurazione per-app: licenza Gold
- Configurazione personalizzata di AppConnect: licenza Gold
- Configurazione personalizzata **Android Enterprise**: licenza Silver

Se un dispositivo Android è in modalità tutto schermo:

Quando il dispositivo è in modalità tutto schermo, è possibile installare soltanto le app in-house. È possibile installare app pubbliche, ma prima dell'installazione il dispositivo deve uscire dalla modalità tutto schermo. Inoltre, è possibile limitare le app disponibili per l'utilizzo sui dispositivi in modalità tutto schermo alle sole app approvate o consentite dall'azienda. Sui dispositivi che utilizzano Android 4.1, se un'app approvata ne avvia un'altra non inclusa dall'elenco delle app consentite, tale app viene avviata e immediatamente ridotta a icona. Sui dispositivi che utilizzano Android 5.0, le app non approvate che vengono avviate dalle app incluse nell'elenco delle app consentite rimangono disponibili.

Passaggio tra visualizzazione griglia e visualizzazione elenco

Fare clic sull'icona Elenco o sull'icona Griglia nella parte destra della schermata Catalogo applicazioni.

Aggiunta di app Google Play Store per Android Enterprise

- È possibile aggiungere un'app dal Google Play Store al Catalogo app e renderla disponibile agli utenti. Per aggiungere un'app da Google Play Store in Android Enterprise è necessario approvarne l'inclusione nell'App Catalog.
- Il layout di Google Play Store per dispositivi Android Enterprise include una home page per dispositivi migrati gestita in Core e un collegamento rapido a Ivanti Neurons for MDM che visualizza tutte le applicazioni gestite in Ivanti Neurons for MDM. Quando si migrano i dispositivi Android Enterprise da Core a Ivanti Neurons for MDM, solo le applicazioni comuni tra Core e Ivanti Neurons for MDM App Catalog sono elencate nel profilo di lavoro Google Play Store del dispositivo. È possibile fare clic sul pulsante Ivanti Neurons for MDM per visualizzare l'elenco di tutte le applicazioni disponibili nel Catalogo app di Ivanti Neurons for MDM.

Il layout di Google Play Store per dispositivi Android Enterprise include una home page per dispositivi migrati gestita in Core e un collegamento rapido a Ivanti Neurons for MDM che visualizza tutte le applicazioni gestite in Ivanti Neurons for MDM. Quando si migrano i dispositivi Android Enterprise da Core a Ivanti Neurons for MDM, solo le applicazioni comuni tra Core e Ivanti Neurons for MDM App Catalog sono elencate nel profilo di lavoro Google Play Store del dispositivo. È possibile fare clic sul pulsante Ivanti Neurons for MDM per visualizzare tutte le applicazioni disponibili nel Catalogo app di Ivanti Neurons for MDM.

Prerequisito

- Android Enterprise deve essere abilitato per accedere e aggiungere le applicazioni del Google Play Store all'App Catalog.

ProcedureProcedura

1. Andare in **App > Catalogo app**.
2. Fare clic su **Aggiungi** (in alto a sinistra).

> Selezionare Google Play dall'elenco a discesa per effettuare la ricerca di un'app in Google Play Store. L'iFrame di Google Play viene visualizzato quando Android Enterprise è registrato.

3. Cercare l'app nel campo di ricerca e fare clic sull'app.
4. Fare clic su **Fine**.

> L'approvazione di un'app può essere successivamente revocata facendo clic su **APPROVAZIONE REVOCATA**.

Opzione	Descrizione
Impostazioni di approvazione	
Mantenere l'approvazione quando l'app richiede nuove autorizzazioni	Consente agli utenti di installare un'app aggiornata
Revocare l'approvazione di app quando questa app richiede nuove autorizzazioni	**Rimuove l'app dallo store fino a quando non viene nuovamente approvata.**
Impostazioni di approvazione	
Aggiungi abbonato	Immettere l'indirizzo di posta elettronica per aggiungere abbonati alle notifiche di posta elettronica quando le app approvate richiedono nuove autorizzazioni.

Aggiunta di un'app da uno store pubblico

È possibile aggiungere un'app da uno store pubblico al Catalogo app e renderla disponibile agli utenti.

Procedura

1. Andare in **App > Catalogo app**.
2. Fare clic su **Aggiungi**.
3. Scegliere l'app desiderata:
4. Selezionare l'app store pubblico.
5. Immettere il nome dell'app.
6. Selezionare l'app dall'elenco.
7. Fare clic su **Avanti**.
8. Per descrivere l'app agli utenti:
9. Aggiungere o rimuovere le categorie.

10. Immettere una descrizione facoltativa.
11. Fare clic su **Avanti**.
12. Per definire la distribuzione dell'app:
13. Selezionare un'opzione di distribuzione.
14. Espandere la sezione **Opzioni avanzate e Configurazione app**.
15. Attenersi alle linee guida seguenti per completare le opzioni:

Impostazione	Operazione da eseguire
Installa su dispositivo	Selezionare questa opzione per avviare l'installazione subito dopo la registrazione. All'utente verrà richiesto di confermare l'installazione dell'app ad eccezione dei seguenti casi: • Il dispositivo è un dispositivo iOS supervisionato per le installazioni di nuove app e gli aggiornamenti delle app. • Il dispositivo è un dispositivo iOS non supervisionato per gli aggiornamenti delle app. • Per gli utenti che si sono registrati al programma App e libri. • Il dispositivo è un dispositivo Samsung Knox e la seguente opzione di installazione invisibile all'utente è stata selezionata. Per app iOS pubbliche installate sul dispositivo per la prima volta, in App Catalog viene visualizzato il pulsante "Reinstalla", che consente di reinstallare l'app. La reinstallazione viene eseguita se la versione dell'app sul dispositivo è diversa da quella nell'app Store iOS.
Non mostrare l'applicazione nell'App Catalog dell'utente finale	Selezionare questa opzione se non si desidera che l'utente visualizzi l'app nel Catalogo app del dispositivo.
Imposta priorità di installazione app	Per impostare la priorità di installazione delle app durante l'onboarding utente, selezionare Alta, Media o Bassa. Solo le app con priorità alta vengono installate durante l'onboarding utente.
Sospendi il repush dell'app dopo un numero definito di tentativi non riusciti (solo iOS)	Spostare l'interruttore su ON per sospendere il repush dell'app dopo un numero specificato di tentativi non riusciti, utilizzando le impostazioni seguenti: **Arresta repush dopo** - Specificare il numero di tentativi di repush non riusciti oltre il quale è necessario interrompere il repush. Immettere valori compresi fra **1** e **999** **tentativi non riusciti e riprova dopo**: specificare il numero di ore che devono trascorrere per consentire un nuovo repush dopo l'ultimo repush non riuscito. Immettere valori compresi fra **3** e **48** ore.
(Solo Android) Installazione invisibile sui dispositivi Samsung Knox	Questa opzione non si applica alle app pubbliche.
(Solo per iOS e macOS) Abilitare la VPN per app per questa app	Selezionare questa opzione per utilizzare una **configurazione VPN per-app** con l'app specifica. Selezionare la configurazione VPN per app che si desidera utilizzare dall'elenco a discesa. Per macOS, selezionare la configurazione VPN per-app di Tunnel.
(Solo iOS) Impedisci il backup su iCloud e iTunes	Selezionare questa opzione per impedire il backup dei dati relativi a questa app su iCloud e iTunes.
(Solo iOS) Rimuovi le app all'annullamento della registrazione	Selezionare questa opzione per rimuovere questa app quando il dispositivo non è più gestito da Ivanti Neurons for MDM.
(Solo iOS) Configurazione personalizzata AppConnect	Per le app con abilitazione AppConnect, immettere le chiavi e i valori che specificano le preferenze di configurazione personalizzate. Consultare la documentazione relativa

Impostazione	Operazione da eseguire
	all'app per visualizzare le chiavi disponibili.
Impostazioni delle app gestite di iOS 7 o versioni successive	Immettere le chiavi e i valori definiti per questa app su un'app gestita di iOS 7 o versioni successive. Consultare la documentazione relativa all'app per informazioni sulle chiavi supportate.

> Le app **Android Enterprise** avranno opzioni diverse.

Fare clic su **Avanti**

4. Selezionare un'opzione di promozione:
5. Fare clic su **+ Aggiungi descrizione** per immettere una breve descrizione della configurazione.

- Non in primo piano
- Elenco in primo piano
- Banner in evidenza
- Se si seleziona Banner in evidenza, specificare i seguenti dettagli:
    1. **Titolo** - Specificare il titolo dell'applicazione
    2. **Descrizione** - Specificare i dettagli dell'applicazione
    3. **Stile banner** - Selezionare un colore per il banner

6. Facoltativamente, modificare la distribuzione della configurazione.
7. Fare clic su **Fine** per salvare la configurazione dell'app.
8. Fare clic su **Fine**.

> Quando si cerca un'app di Windows nel Catalogo app, è possibile cercare l'app che corrisponde strettamente utilizzando l'opzione **Nome app** o **ID AppStore** dall'elenco a discesa:

- **Nome app** - Selezionare questa opzione e fornire il Nome app
- **ID AppStore** - Selezionare questa opzione e fornire l'ID AppStore

La ricerca di app nel Windows Store supporta le app dello store Win32.

Assicurarsi che lo strumento Winget sia disponibile sul dispositivo per gestire le app di Win32 Store.

Aggiunta di un'app interna

È possibile caricare un'app interna nel catalogo delle app con i seguenti formati di file. Il caricamento di un file di grandi dimensioni può richiedere alcuni minuti. Il numero di versioni di applicazioni interne è limitato a 100. Se questo numero viene superato, il sistema Ivanti Neurons for MDM elimina le versioni meno recenti dell'applicazione. Gli stati di caricamento ed eliminazione dell'applicazione vengono indicati e sono visibili nella pagina Audit trail.

Per alcune app, l'inventario delle app MIP restituito da Mobile@Work potrebbe non essere corretto. Mobile@Work potrebbe non riuscire a determinare lo stato di installazione delle app che non sono installate nel percorso predefinito. Al fine di determinare lo stato di installazione corretto per tali app è possibile utilizzare lo script di individuazione. Se il codice di uscita dello script di individuazione è

0, Mobile@Work determina che l'app è presente. Per tutti gli altri codici di uscita, determina che l'app non è installata. Mobile@Work prepara il report dell'inventario del dispositivo basandosi sulle app rilevate.

- IPA (iOS)
- MIP (app Packager macOS)
- PKG (macOS)
- APK (Android)
- APPX, APPXBUNDLE, EXE e MSI (Windows)

> Per applicazioni quali PKG con script o DMG che contengono PKG con script, Mobile@Work per macOS è in grado di rilevare solo una richiesta di installazione riuscita. Non indica se l'app è stata eliminata o se gli script installati sono stati rimossi. Il server Ivanti Neurons per MDM non sarà pertanto in grado di inviare nuovamente un comando di installazione. Se la connessione si interrompe durante il download delle app, ritentare l'installazione delle app eseguendo un check-in. Per le app MIP, anche se l'app viene rimossa dal dispositivo in seguito all'installazione tramite PKG o un DMG contenente un PKG con script, Mobile@Work non installa l'app MIP se la voce per il PKG esiste nella cartella di destinazione del dispositivo client.

Procedura

1. Andare in **App > Catalogo app**.
2. Fare clic su **Aggiungi** (in alto a sinistra).
3. In **Selezionare le piattaforme per caricare il file**, scegliere la propria categoria di piattaforma (ad es., **Apple Apps**) e selezionare il sistema operativo specifico (ad es., iOS o macOS dal menu a discesa di Apple Apps).

> Se un utente seleziona una piattaforma e tenta di caricare un tipo di file in conflitto (ad es., selezionando Apple ma caricando un .apk), il sistema attiverà un errore "Formato file non valido".

4. Trascinare il file dell'applicazione sulla casella tratteggiata, oppure fare clic su **Scegli file** per selezionarlo dal file system, quindi fare clic su **Conferma**.
5. Fare clic su **Avanti** (in basso a destra).
6. Immettere una descrizione dell'app per gli utenti e configurare le app necessarie come prerequisito:
7. Aggiungere le categorie.
8. Quando si aggiunge un pacchetto macOS, se il file del pacchetto contiene più di un'app (ad esempio i pacchetti Microsoft Office e Cisco AnyConnect), le app principali selezionate verranno utilizzare per identificare che il pacchetto è installato. Se configurata, VPN per-app verrà applicata a queste app.
9. Immettere una descrizione facoltativa.
10. **Codice prodotto MSI**: quando si caricano le app MSI, il codice del prodotto dell'app MSI viene inserito automaticamente in questo campo.

> È necessario selezionare l'opzione "Ho controllato il codice prodotto MSI" per assicurarsi che sia stato inserito il GUID corretto.

Sovrascrivi URL: immettere un'elevazione dei diritti facoltativa per l'URL di origine dell'app per consentire il download dell'app da un'altra origine o la ricezione di file di grandi dimensioni, come file di multimediali di installazione Microsoft Office da una rete locale (HTTP e HTTPS). Questa opzione richiede l'accesso a una rete interna sicura e la sincronizzazione manuale di un server alternativo su

cui sono archiviate le app. Non immettere valori a meno che non sia stata stabilita l'infrastruttura necessaria. È possibile modificare questo valore durante la modifica delle impostazioni delle app per l'app specifica.

- Per le app iOS, gli URL di sovrascrittura dell'app devono essere solo in formato HTTP o HTTPS.
- Per le app Android e macOS, gli URL di sovrascrittura dell'app devono essere esclusivamente in formato HTTPS.
- Per le applicazioni macOS, l'URL deve terminare con l'estensione .pkg.

6. **Riga di comando** (solo app MSI con Windows a 32 bit): immettere un'opzione della riga di comando facoltativa per specificare le informazioni aggiuntive che non appartengono al pacchetto durante la distribuzione dei file MSI. Ad esempio, per scrivere i registri di installazione in un file di output, è possibile immettere "/output registro.txt" in questo campo. Ciò consente di creare il file output.txt nella cartella C:\Windows\System32. Per impostazione predefinita, l'opzione della riga di comando /qn per l'installazione invisibile viene inserita automaticamente durante il caricamento dell'app MSI.

> Il nome del pacchetto dell'app MSI da caricare non deve essere aggiunto fra gli argomenti della riga di comando. Se aggiunto, il caricamento sarà limitato fino a quando il nome del pacchetto dell'app viene rimosso dagli argomenti della riga di comando. Un elenco di tutte le opzioni della riga di comando supportate è fornito sotto il link aggiuntivo. Questo link sarà visibile in modalità di visualizzazione e modifica dell'app.

App .EXE per Win32: vengono installate tramite Bridge utilizzando la modalità PowerShell amministratore. La funzionalità Bridge verrà utilizzata automaticamente, se disponibile.

- Aggiornare la versione per mantenere la coerenza tra la **Versione di visualizzazione** e la **Versione del bundle**
- Posizione del programma di installazione (.EXE)
- Parametri della riga di comando del programma di installazione: l'argomento per l'esecuzione silenziosa del file (ad esempio, /SILENT o /VERY SILENT) è obbligatorio
- Esecuzione del programma di installazione come utente: per installare utilizzando le credenziali dell'utente, selezionare l'opzione 'Esegui come utente'

Per le app Win32 store: vengono installate tramite Bridge utilizzando la modalità PowerShell amministratore.

9. Per le app macOS Packager, configurare le app necessarie come prerequisito (facoltativo). Per una panoramica della funzionalità delle app prerequisito, vedere Informazioni sulle app macOS interne Packager.
10. **URL di avvio**: immettere l'URL personalizzato per l'avvio dell'app in AppStation. Necessario solo quando si aggiungono app non abilitate per AppConnect per la distribuzione in un'implementazione solo MAM con AppStation e applicabile solo alle app iOS.
11. Configurare la **delega per l'app**.

> Dopo che un'app prerequisito è stata delegata e diventa un'app prerequisito per l'app dello spazio non predefinito, per annullare la delega di tale app è prima necessario rimuovere la relazione di prerequisito.

Fare clic su **Avanti**.

13. Fare clic su **Avanti**.
14. (Facoltativo) Aggiungere delle schermate relative all'app.
15. (Facoltativo) Aggiungere o sostituire le icone per l'app (app iOS, MacOS e Windows).
16. Fare clic su **Avanti**.
17. Per le app macOS Packager, definire o selezionare gli script di installazione da eseguire prima e/o dopo l'installazione dell'app. Selezionare uno o entrambi i seguenti script digitando nella casella di ricerca o facendo clic sul link per visualizzare l'elenco degli

script. Fare clic su **Avanti**.

18. È possibile creare gli script nella pagina **Amministratore > Script e file > Tutti gli script**. Se si aggiorna l'app, è possibile scegliere di copiare gli script dall'app precedente ed eseguire gli script per l'app aggiornata. Se si salta questa sezione, è possibile configurare gli script modificando l'app in seguito.

- **Script di pre-installazione** - Inserire il nome dello script per selezionare lo script da eseguire prima dell'installazione dell'app. Gli script di pre-installazione verranno eseguiti, se necessario con più tentativi, finché non si riceve dal client lo stato di esecuzione riuscita. Solo in seguito alla ricezione di questo stato viene inviato il comando di installazione dell'app. È possibile visualizzare lo stato di esecuzione degli script nella pagina dei dettagli del dispositivo nella scheda **Registri**.
- **Script di post-installazione** - Inserire il nome dello script per selezionare lo script da eseguire dopo l'installazione dell'app.
- **Script di disinstallazione** - Inserire il nome dello script che il server invia a un dispositivo quando rileva che un app non è più distribuita nel dispositivo.
- **Script di individuazione**: immettere il nome dello script inviato dal server a un dispositivo per rilevare un'app. Il risultato dello script di individuazione per l'app sostituisce il risultato dell'inventario predefinito per tale app nel dispositivo. Al dispositivo viene inviato lo script di individuazione relativo a tutte le app, allo scopo di determinare l'esistenza di tali app al suo interno anche se non sono state distribuite al dispositivo.
  Di seguito è riportato uno script di individuazione di esempio:

```
#!/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
```

Per definire la distribuzione dell'app:

12. Selezionare un'opzione di promozione:
13. Selezionare un'opzione di distribuzione.
14. Espandere la sezione **Opzioni avanzate e Configurazione app**.
15. Attenersi alle linee guida seguenti per completare le opzioni:
16. Fare clic su **Avanti**.

Impostazione	Operazione da eseguire
Installa su dispositivo	Selezionare questa opzione per avviare l'installazione subito dopo la registrazione. All'utente verrà richiesto di confermare l'installazione dell'app ad eccezione dei seguenti casi: • Il dispositivo è un dispositivo iOS supervisionato. • Il dispositivo è un dispositivo Samsung Knox e la seguente opzione di installazione invisibile all'utente è stata selezionata.
Non mostrare l'applicazione nell'App Catalog dell'utente finale	Selezionare questa opzione se non si desidera che l'utente visualizzi l'app nel Catalogo app del dispositivo.
Imposta priorità di installazione app	Per impostare la priorità di installazione delle app durante l'onboarding utente, selezionare Alta, Media o Bassa. Solo le app con priorità alta vengono installate durante l'onboarding utente.
Sospendi il repush dell'app dopo un numero definito di tentativi non riusciti (solo iOS)	Spostare l'interruttore su ON per sospendere il repush dell'app dopo un numero specificato di tentativi non riusciti, utilizzando le impostazioni seguenti: **Arresta repush dopo** - Specificare il numero di tentativi di repush non riusciti oltre il quale è necessario interrompere il repush. Immettere valori compresi fra **1** e **999** **tentativi non riusciti e riprova dopo**: specificare il numero di ore che devono trascorrere per consentire un nuovo repush dopo l'ultimo repush non riuscito. Immettere valori compresi fra **3** e **48** ore.
(Solo Android) Installazione invisibile sui dispositivi Samsung Knox	Selezionare questa opzione se non si desidera che all'utente venga richiesto di confermare l'installazione sui dispositivi Samsung Knox.
(Solo per iOS e macOS) Abilitare la VPN per app per questa app	Selezionare questa opzione per utilizzare una **configurazione VPN per-app** con l'app specifica. Selezionare la configurazione VPN per app che si desidera utilizzare dall'elenco a discesa. Per macOS, selezionare la configurazione VPN per-app di Tunnel.
(Solo iOS) Impedisci il backup su iCloud e iTunes	Selezionare questa opzione per impedire il backup dei dati relativi a questa app su iCloud e iTunes.
(Solo iOS) Rimuovi le app all'annullamento della registrazione	Selezionare questa opzione per rimuovere questa app quando il dispositivo non è più gestito da Ivanti Neurons for MDM.
(Solo iOS) Configurazione personalizzata AppConnect	Per le app con abilitazione AppConnect, immettere le chiavi e i valori che specificano le preferenze di configurazione personalizzate. Consultare la documentazione relativa all'app per visualizzare le chiavi disponibili.
Impostazioni delle app gestite di iOS 7 o versioni successive	Immettere le chiavi e i valori definiti per questa app su un'app gestita di iOS 7 o versioni successive. Consultare la documentazione relativa all'app per informazioni sulle chiavi supportate.

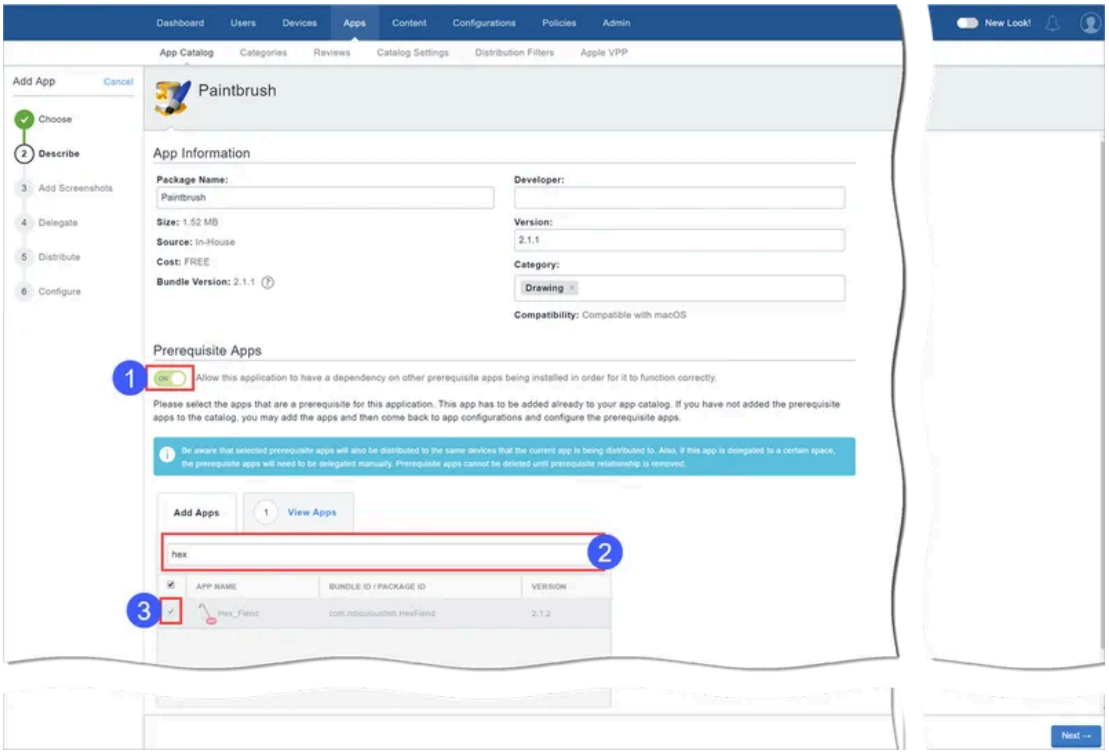
17. Fare clic su **Fine**.

- Non in primo piano

- Elenco in primo piano
- Banner

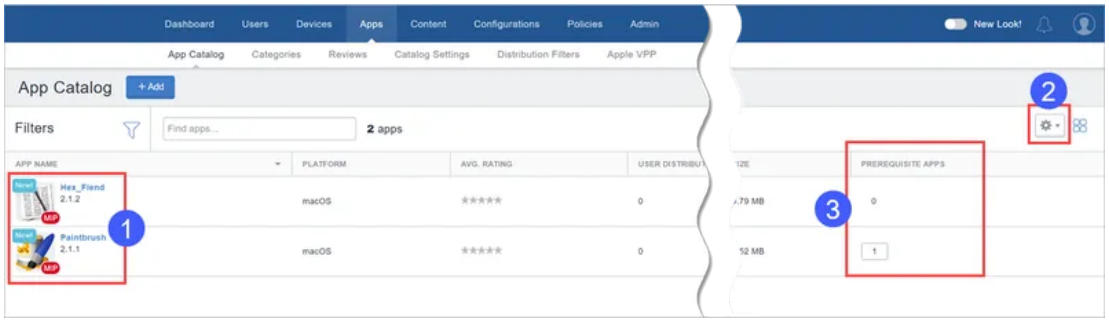
Informazioni sulle app macOS interne Packager

Durante l'importazione di app macOS Packager, l'amministratore può abilitare, 1, la funzionalità App prerequisito per cercare, 2, e selezionare, 3, le app prerequisito che devono essere installate sui client prima di installare l'app che l'amministratore sta importando.



Una volta importata, l'app macOS Packager viene visualizzata nell'App Catalog accompagnata dal badge MIP, 1, qui sotto. È quindi possibile utilizzare le impostazioni delle colonne, 2, per aggiungere la colonna APP PREREQUISITO, 3, per vedere a colpo d'occhio le app con dipendenze, ovvero, che dispongono di app prerequisito.

- È possibile cercare e selezionare app MIP, non MIP e pubbliche (app pubbliche App e libri e macOS App Store) come app prerequisito.
- Gli utenti devono accettare la licenza App e libri per l'installazione invisibile all'utente delle app prerequisito App e libri.
- Per le app prerequisito pubbliche non App e libri, gli amministratori devono distribuire in modo esplicito le app pubbliche e l'utente deve installarle. Le app pubbliche (App e libri e di altro tipo) devono essere importate nell'App Catalog per poter essere visualizzate nell'elenco di app prerequisito. La colonna Origine indica il tipo di app prerequisito.
- Per installare un'app non MIP interna a cui è associata un'app prerequisito non MIP, è necessario eseguire il check-in MDM.
- Gli utenti devono installare manualmente le app pubbliche prerequisito non App e libri.
- Se il token App e libri viene rimosso o se la licenza è scaduta, le app App e libri selezionate come app prerequisito, nonché l'app principale, non vengono installate. Se si verifica uno di questi casi per le app App e libri, l'amministratore deve seguire una procedura consigliata per informare gli utenti in anticipo.

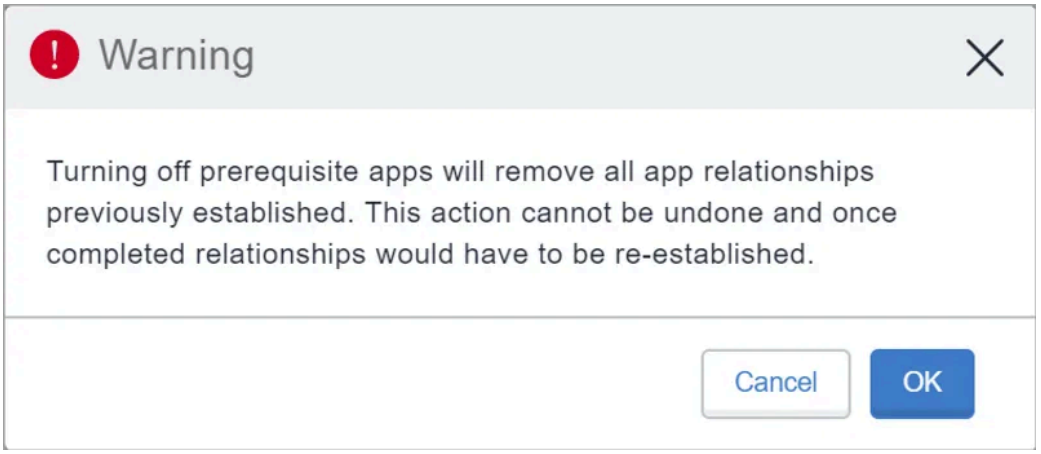


Le app prerequisito sono disponibili anche come app indipendenti per il download da parte dell'utente quando vengono distribuite in modo esplicito. Se l'utente tenta di disinstallare un'app prerequisito:

- Assicurarsi che l'app prerequisito venga installata nuovamente al successivo check-in del dispositivo.
- L'app prerequisito viene disinstallata se non esistono app principali dipendenti installate sullo stesso dispositivo.
- Se l'app prerequisito non è distribuita in modo esplicito, l'app prerequisito verrà disinstallata con l'app principale.
- Se l'app prerequisito è distribuita in modo esplicito, l'app prerequisito rimane sul dispositivo.
- Se l'app prerequisito è associata a un'app dipendente, l'app prerequisito rimane sul dispositivo.

Disattivazione della funzionalità App prerequisito

Quando si interagisce con app che presentano dipendenze e app prerequisito, ad esempio quando si aggiornano, si eliminano o si delegano tali app, vengono visualizzati messaggi di sistema che indicano all'utente il potenziale effetto dello stato della dipendenza o prerequisito dell'app sulle azioni che si sta cercando di eseguire. Ad esempio, quando si tenta di disattivare la funzionalità App prerequisito per un'app, viene visualizzato il messaggio seguente:



- Se si disattiva la funzionalità App prerequisito per un'app, i dettagli relativi alle app prerequisito vengono cancellati. Sono incluse la delega automatica e l'annullamento della delega delle app prerequisito dai sottospazi.
- In Apps@Work il pulsante Installa non viene visualizzato per le app dipendenti le cui app prerequisito non sono ancora installate nel client di destinazione.
- Sui dispositivi degli utenti, quando un utente tenta di installare un'app interna con dipendenze, le app prerequisito verranno installate per prime (se non sono già installate), seguite dall'app principale, un'operazione che può richiedere alcuni minuti. L'elenco delle app dipendenti diventa visibile per l'utente insieme allo stato delle installazioni.

Delega e annullamento della delega di app prerequisito dagli spazi

- Quando l'app principale viene delegata a un sottospazio, le app prerequisito associate a un'app (app principale) vengono delegate automaticamente.
- Se la delega dell'app principale da un sottospazio viene annullata, viene annullata anche la delega delle app prerequisito che non sono state distribuite esplicitamente. Non viene invece annullata la delega delle app prerequisito associate a più di un'app principale.
- Se le app prerequisito vengono delegate esplicitamente, la relativa la delega non viene annullata automaticamente.

Delega delle autorizzazioni del dispositivo per le app interne di Android Enterprise

Le autorizzazioni delegate possono essere assegnate alle app interne che possono essere applicate ai dispositivi gestiti da Android Enterprise e ai dispositivi AMA.

Procedura

1. Andare in **App > Catalogo app**.
2. In **App Catalog**, selezionare un'app per la quale si desidera delegare le autorizzazioni del dispositivo.
3. Fare clic sulla scheda **Configurazioni app**.
4. Nella sezione Autorizzazioni delegate (app Android Enterprise interna), selezionare le autorizzazioni richieste per le app:

> AMAPI viene utilizzata solo dall'implementazione COSU. Per ulteriori informazioni, vedere la sezione AMAPI.

   - **Configurare autorizzazioni di runtime di app di terze parti**
   - **Nascondere e sospendere app di terze parti**
   - **Gestire certificati**
   - **Gestire le configurazioni delle app**
   - **Gestire il blocco della disinstallazione delle app**
   - **Gestire l'abilitazione delle app di sistema**
   - **Gestire la selezione dei certificati** (non supportata in modalità AMAPI)
   - **Gestire la conservazione delle app disinstallate** (non supportata in modalità AMAPI)
   - **Gestisci raccolta registri di rete**(supportata solo da un'app alla volta)
   - **Gestisci raccolta registri di sicurezza**(supportata solo da un'app alla volta)
   - **Gestire l'installazione delle app esistenti** (non supportata in modalità AMAPI)
   - **Installare e rimuovere pacchetti** (non supportata in modalità AMAPI)

L'opzione di installazione e rimozione dei pacchetti è disponibile su tutti i dispositivi con la modalità Proprietario dispositivo Android supportati (7.0 o versione successiva). Altre autorizzazioni delegate sono applicabili solo per Android 8.0 o versione successiva. Configurare le opzioni di distribuzione, scegliendo tra **Tutti gli utenti con app**, **Nessuno** o **Personalizzata**.

6. Fare clic su **Salva**.

Visualizzazione dello stato del profilo di provisioning per le app interne iOS

Nella pagina App Catalog è possibile visualizzare lo stato del profilo di provisioning per le app iOS interne. La descrizione comando accanto al nome del profilo consente di visualizzare il numero di giorni alla scadenza del profilo. Questo stato può essere utile per controllare quando i profili di provisioning sono in scadenza per le app interne.

Lo stato è utile per la risoluzione dei problemi delle applicazioni che non si installano a causa del profilo scaduto. Le app possono installarsi ma non sarebbero in grado di aprirsi o avviarsi se non vi è nessun profilo di provisioning.

Procedura

1. Andare in **App > Catalogo app**.
2. Fare clic sull'icona a forma di ingranaggio in alto a destra per visualizzare le colonne.
3. Selezionare **Profilo di provisioning** per visualizzare la colonna dell'elenco di applicazioni disponibili nella pagina App Catalog.

I dettagli del profilo di provisioning sono anche disponibili nella pagina dei dettagli dell'app sotto la sezione Impostazioni del profilo di provisioning.

Aggiornamento del profilo di provisioning per le app iOS interne

Il profilo di provisioning viene applicato a un'app iOS interna specifica. I dettagli del profilo di provisioning di un'app sono disponibili nella pagina dei dettagli dell'app. Per lanciare un'app interna iOS su un dispositivo è necessario che questa disponga di un profilo di provisioning che non sia scaduto. Se è scaduto, è possibile aggiornare un profilo di provisioning caricando il profilo nella pagina dei dettagli dell'app.

Procedura

1. Andare in **App > Catalogo app**.
2. Fare clic sull'app per la quale è necessario l'aggiornamento del profilo di provisioning. Viene visualizzata la pagina dei dettagli dell'app.
3. Fare clic su **Modifica**.
4. Nella sezione **Profilo di provisioning**, fare clic su **Scegli file**.
5. Selezionare il file del profilo di provisioning (estensione del file .mobileprovision) che deve essere caricato e fare clic su **Salva**.

Distribuzione delle app interne in Google Play

Caricare le proprie app interne sul canale privato di Google Play e importarle in Ivanti Neurons for MDM per la distribuzione sui dispositivi Android Enterprise.

Procedura

1. Eseguire l'accesso alla console delle app private Google: **https://play.google.com/apps/publish**.
2. Fare clic su **Tutte le applicazioni** nel menu di sinistra.
3. Fare clic su **Crea nuova applicazione**, quindi immettere un nome per l'applicazione.
4. Fare clic su **Carica APK** per caricare il file .apk generato.
5. Fare clic su **Elenco store**:
    - Immettere una descrizione breve e una più dettagliata.
    - Caricare uno screenshot per tutte le schede.
    - Caricare un'icona ad alta risoluzione.
    - Caricare un'icona grafica della funzione (graphic.png)
    - Immettere le informazioni richieste per la categorizzazione, i recapiti e l'informativa sulla privacy.
    - Completare il questionario per una valutazione dell'app.

6. Fare clic su **Prezzi e distribuzione**.
   Se sono state immesse tutte le informazioni necessarie, nella parte superiore della pagina viene visualizzata la dicitura "Pronto per la pubblicazione".
7. Passare alla scheda App in Ivanti Neurons for MDM.
8. Fare clic su **Aggiorna cataloghi disponibili** per eseguire la sincronizzazione delle app private.

> È possibile che la pubblicazione dell'app richieda diverse ore.

Aggiunta di un'app Web per dispositivi Android Enterprise

Un'app Web è un link a un sito Web e viene installata sul dispositivo come collegamento. Le app Web hanno un comportamento simile a quello delle altre app e possono quindi essere distribuite con gli stessi criteri di un'app normale. Vengono mostrate nel Catalogo app e possono essere installate dagli utenti come qualsiasi altra app. Tuttavia, le app Web possono avere una sola versione e non supportano l'installazione invisibile all'utente. Le app Web utilizzano clip Web e vengono installate sul dispositivo come configurazioni, ma si comportano come app normali.

Configurare una clip Web come app nel Catalogo app per rendere disponibile l'app Web agli utenti. La clip Web può essere definita come configurazione, ma le configurazioni possono essere inviate esclusivamente dall'amministratore. Gli utenti possono scegliere di installare o meno l'app Web sui propri dispositivi, mentre non possono rifiutare la configurazione di una clip Web.

In Android Enterprise, un'app web è una forma incorporata di app web che viene eseguita su Google Chrome all'interno del profilo di lavoro. Può essere abbinato a una VPN o a soluzioni SSO in Android Enterprise. Una volta creata, l'app Web funziona come qualsiasi altra app Android ed è possibile distribuirla in base alle esigenze. Per eseguire le app Web, è necessario che Chrome sia installato sul Profilo di lavoro su dispositivo di proprietà dell'azienda.

> In caso di problemi durante l'utilizzo di questa funzionalità, gli amministratori possono contattare il **supporto**.

Procedura

1. Andare in **App > Catalogo app**.
2. Fare clic su **+ Aggiungi**.
3. Selezionare **Google Play** dall'elenco a discesa per effettuare la ricerca di un'app in Google Play Store. L'iFrame di Google Play viene visualizzato se Android Enterprise è registrato.
4. Fare clic su **Applicazione Web**.
5. Per descrivere l'app agli utenti:
   1. Titolo o nome dell'app.
   2. URL dell'app
   3. Tipo di visualizzazione dell'app Web.
   4. Caricare l'icona, che può essere un'immagine quadrata PNG o JPEG da 512 px.

Fare clic su **Crea**. Attendere la pubblicazione dell'app su iFrame. L'operazione può richiedere alcuni minuti. È possibile chiudere la pagina e ritornarvi in seguito.

7. Una volta pubblicata, importare l'app Web nell'App Catalog per la distribuzione. Fare clic sull'icona dell'app Web.
8. Scorrere verso il basso e fare clic su **Seleziona**.
9. Aggiungere le categorie e una descrizione (opzionale).

10. Fare clic su **Avanti**.
11. Selezionare una delle seguenti opzioni per Delega app:
    - Delega questa app a tutti gli spazi.
    - Non delegare questa app a tutti gli spazi.

Fare clic su **Avanti**.

13. Selezionare un'opzione di distribuzione per l'applicazione.
14. Fare clic su **Fine**.

Dopo l'aggiunta di un'app Web, è possibile modificarla ogni volta che è necessario. A tale scopo, procedere come segue:

1. Nella pagina **App Catalog**, fare clic sul nome dell'app Web esistente.
2. Fare clic su **Modifica** per modificare i campi dell'app Web.

Aggiunta di un'app Web per dispositivi iOS

Un'app Web è un link a un sito Web e viene installata sul dispositivo come collegamento. Le app Web hanno un comportamento simile a quello delle altre app e possono quindi essere distribuite con gli stessi criteri di un'app normale. Vengono mostrate nel Catalogo app e possono essere installate dagli utenti come qualsiasi altra app. Tuttavia, le app Web possono avere una sola versione e non supportano l'installazione invisibile all'utente. Le app Web utilizzano clip Web e vengono installate sul dispositivo come configurazioni, ma si comportano come app normali.

Configurare una clip Web come app nel Catalogo app per rendere disponibile l'app Web agli utenti. La clip Web può essere definita come configurazione, ma le configurazioni possono essere inviate esclusivamente dall'amministratore. Gli utenti possono scegliere di installare o meno l'app Web sui propri dispositivi, mentre non possono rifiutare la configurazione di una clip Web.

> In caso di problemi durante l'utilizzo di questa funzionalità, gli amministratori possono contattare il **supporto**.

Procedura

1. Andare in **App > Catalogo app**.
2. Fare clic su **+ Aggiungi** (in alto a sinistra).
3. Fare clic su **App Web**.
4. Per descrivere l'app agli utenti:
    1. Nome dell'app
    2. URL dell'app
    3. Tipo di piattaforma
    4. Icona dell'app
    5. Aggiungere o rimuovere le categorie.
    6. Schermo intero: selezionare questa opzione per visualizzare l'app Web come applicazione a schermo intero.
    7. Rimovibile: selezionare questa opzione per rendere l'app Web rimovibile.
    8. Fare clic su **Avanti**.

Selezionare una delle seguenti opzioni per Delega app:

- Delega questa app a tutti gli spazi.

- Non delegare questa app a tutti gli spazi.

Fare clic su **Avanti**.

7. Selezionare un'opzione di distribuzione per l'applicazione.
8. Fare clic su **Fine**.

Modifica di un'applicazione web

Dopo l'aggiunta di un'app Web, è possibile modificarla ogni volta che è necessario.

Procedura

1. Nella pagina **App Catalog**, fare clic sul nome dell'app Web esistente.
2. Fare clic su **Modifica** per modificare i campi dell'app Web.

Distribuzione rollout lento

L'impostazione **Distribuzione rollout lento** permette agli amministratori di distribuire automaticamente la nuova versione delle applicazioni ai dispositivi in modo graduale. L'opzione Usa il metodo di distribuzione con rollout lento è disponibile quando si esegue il rollout della versione successiva dell'applicazione. Il portale amministrativo Ivanti Neurons per MDM permette di modificare le applicazioni anche quando il roll out lento è in pausa.

Una volta che il roll out lento è impostato per una versione, è applicabile per le versioni successive con la stessa percentuale impostata l'ultima volta. È possibile interrompere la distribuzione di un'applicazione se risulta impostata su 100%. Tuttavia, se si imposta il target di distribuzione su 100%, è necessario impostare manualmente la percentuale del target di distribuzione per la versione successiva perché l'UI reimposta la percentuale su 0%.

Procedura

	1.	**Accedere ad App Catalog, App e selezionare una delle opzioni di modalità di distribuzione.**
	2.	**Selezionare l'opzione % personalizzata di dispositivi nel riepilogo selezioni (Rollout lento).**
	3.	**Dalle Impostazioni di rollout lento, trascinare il cursore in Specificare % del target di distribuzione.**
	4.	**Fare clic su Conferma, quindi su Fine. Viene visualizzato lo stato dell'ultima versione dell'app. La pagina Catalogo app indica lo stato ROLL OUT LENTO nella tabella.**

Se non è possibile eseguire le attività indicate nella pagina **App Catalog**, probabilmente non si dispone delle autorizzazioni necessarie. È richiesto il ruolo Gestione app e contenuti.

Utilizzo di Ricerca avanzata

È possibile utilizzare l'opzione Ricerca avanzata per cercare un'app in base a regole per identificare e visualizzare gli utenti con criteri specifici. Queste regole possono essere create utilizzando gli operatori applicabili, tra cui "è uguale a", "è inferiore a", "è maggiore di", "è uguale a" e "non è uguale a". Le opzioni delle regole possono essere nidificate insieme utilizzando le opzioni QUALSIASI (O) o TUTTO (E). Le app che soddisfano le regole vengono visualizzate sotto la sezione.

I valori degli attributi personalizzati utilizzati nella ricerca sono sensibili alle maiuscole e alle minuscole.

Procedura

1. Nella pagina Catalogo app, fare clic sul collegamento **Ricerca avanzata**. Si apre la procedura guidata Ricerca avanzata.
2. Fare clic su una delle seguenti opzioni:
    - **Qualsiasi**-se è necessario che le app soddisfino almeno una delle regole
    - **Tutte**-se è necessario che le app soddisfino tutte le regole

Per creare una regola che definisca i criteri di ricerca, selezionare una delle seguenti opzioni e scegliere l'azione associata appropriata:

- AppConnect abilitato
- Valutazione media
- ID pacchetto
- Categoria
- Costo
- Attributi personalizzati
- Data aggiunta al Catalogo app
- Data modificata
- Distribuzione dei dispositivi
- Distribuzione dei gruppi di dispositivi
- Tipo di dispositivo
- Distribuzione dei gruppi
- Versione minima sistema operativo
- Nome
- Piattaforma sistema operativo
- Profilo di provisioning
- Dimensione
- Origine
- Distribuzione utenti
- Nome gruppi di utenti
- Versione

4. (Opzionale) Fare clic su **+** per creare altre regole.
5. Fare clic su **Cerca**. L'elenco delle app che soddisfano i criteri di ricerca è visualizzato nella pagina.

Caricamento di query di ricerca

È possibile visualizzare l'elenco delle query di ricerca salvate.

Procedura

1. Fare clic su Ricerca avanzata e quindi fare clic sull'icona cartella. L'elenco delle query di ricerca create viene visualizzato nella sezione **Carica query** e vengono mostrati i seguenti dettagli.
    - **Nome query**: nome della query caricata.
    - **Contenuto query**: mostra il contenuto delle regole che definiscono la query di ricerca.
    - **Azioni**: selezionare l'azione da eseguire per la query.
2. Fare clic su **Carica query** nella colonna **Azioni** per visualizzare l'elenco delle app che soddisfano i criteri della query caricata.
3. Fare clic su **Elimina** per eliminare una query caricata.

Esportazione delle app in un file CSV

È possibile esportare le app utilizzando l'opzione Esporta in CSV dalla pagina App catalog.

Procedura

1. Andare in **App** > **Catalogo app**.
2. Fare clic su **Esporta in CSV** per esportare l'elenco delle app e i dettagli correlati in un file CSV.

> Vengono incluse solo le app elencate nello spazio selezionato e tutti i risultati impaginati vengono compilati in un unico file.

> Utilizzando i filtri o i risultati della ricerca, verranno esportate solo le app pertinenti.

3. Viene visualizzato un messaggio pop-up con i pulsanti **Continua** e **Annulla** che indica che il processo di esportazione è stato avviato e che un report sarà disponibile a breve.
4. Fare clic su **Continua** e attendere il completamento della richiesta prima di inviarne un'altra.
5. Viene visualizzato un messaggio che indica che il **report CSV di App catalog è terminato** con i pulsanti **Download** ed **Elimina**.
6. Fare clic su **Download** per scaricare il report.
7. (Opzionale) Fare clic su **Elimina** per eliminare il report.

> L'opzione **Esporta in CSV** sarà riattivata solo dopo aver selezionato l'opzione **Download** o **Elimina**.

> Se esistono più versioni di un'app, viene visualizzata una voce per ogni versione.

Argomenti correlati

- Ruoli utente
- Rimozione di app dal Catalogo app
- Distribuzione di dipendenze delle app

8.2. Gestione app Gestione dichiarativa dei dispositivi (DDM)

Panoramica

Gestione app Gestione dichiarativa dei dispositivi (DDM) introduce il supporto per il framework di gestione dichiarativa di Apple per la distribuzione delle applicazioni e la gestione del ciclo di vita su dispositivi iOS e iPadOS. Invece di fare affidamento sulla consegna continua dei comandi e sull'estrazione periodica, il DDM consente ai dispositivi di applicare le dichiarazioni localmente e segnalare proattivamente le modifiche allo stato.

Con DDM, il server invia una dichiarazione al dispositivo una sola volta. Il dispositivo applica quindi la configurazione, monitora il suo stato e riporta le modifiche di stato al server. Questo approccio basato sul dispositivo riduce la comunicazione con il server, migliora la scalabilità e fornisce aggiornamenti di stato più tempestivi per le distribuzioni delle applicazioni.

Gestione app DDM si concentra attualmente sulle funzionalità di gestione delle applicazioni principali per i dispositivi Apple supportati.

Flusso di lavoro Gestione app DDM

In un flusso di lavoro DDM, il server consegna lo stato desiderato al dispositivo e il dispositivo diventa responsabile del mantenimento e della segnalazione di tale stato.

Quando un'applicazione viene assegnata a un dispositivo abilitato DDM:

1. Il server invia una dichiarazione applicazione al dispositivo.
2. Il dispositivo elabora la dichiarazione localmente.
3. Il dispositivo installa, aggiorna o mantiene l'applicazione in base alla configurazione assegnata.
4. Il dispositivo monitora continuamente lo stato dell'applicazione.
5. Qualsiasi stato di installazione o cambiamento di stato viene immediatamente riportato al server.

Questo modello dichiarativo fornisce una visibilità quasi in tempo reale sull'avanzamento della distribuzione delle applicazioni senza richiedere l'estrazione periodica dello stato.

Abilita Gestione app DDM

Gestione app DDM è abilitato tramite Impostazioni utente ed è assegnato a gruppi di utenti specifici.

Per abilitare Gestione app DDM:

1. Andare in **Utenti** > **Impostazioni utenti**.
2. In **Impostazione DDM Apple**, fare clic sull'impostazione **+Aggiungi** per un gruppo di utenti specifico. Si apre la pagina **Impostazioni DDM Apple**.
3. Immettere un nome e attivare/disattivare il cursore **Abilita Gestione app DDM**.
4. Fare clic su **Avanti**. Si apre la pagina **Distribuzione impostazione utente**.
5. Selezionare il gruppo di utenti che utilizzerà Gestione app DDM.
6. Fare clic su **Fine**.

Dopo aver abilitato DDM per un gruppo di utenti, tutte le applicazioni supportate assegnate agli utenti in quel gruppo vengono elaborate tramite Gestione app DDM. La configurazione DDM è a livello di tenant ma viene applicata tramite assegnazioni di gruppi di

utenti, consentendo alle organizzazioni di distribuire gradualmente DDM a utenti o gruppi selezionati.

Metodi di registrazione supportati

Gestione app DDM supporta i dispositivi iOS / iPadOS registrati utilizzando:

- Client iReg/Ivanti Go gestito
- Profilo Registrazione dispositivi (DEP)
- Registrazione dispositivi guidata dall'account

Tipi di applicazione supportati

Gestione app DDM supporta i seguenti tipi di applicazione:

- Applicazioni pubbliche
- Applicazioni VPP (solo per la registrazione del dispositivo)
- Applicazioni interne

Il flusso di lavoro di assegnazione e distribuzione delle applicazioni rimane sostanzialmente invariato rispetto alle distribuzioni N-MDM tradizionali. I processi di distribuzione delle applicazioni esistenti continuano a funzionare beneficiando al contempo delle funzionalità avanzate di reporting dello stato di DDM.

8.2.1. Impostazioni Gestione app DDM

In generale, Gestione app include le seguenti impostazioni:

- Impedire il backup su iCloud
- Non installare l'app sui dispositivi appena registrati
- Dati mobili 5G
- Proxy DNS
- Configurazione app gestita
- App aziendali - Apps@Work, Email+, ecc.
- App per VPN
- Relè di rete
- Filtro contenuto Web
- Consenti aggiornamenti Appstore

Oltre alle impostazioni sopra elencate, Gestione app DDM introduce diverse funzionalità disponibili solo per i dispositivi gestiti da DDM.

Pinning versione app

Il pinning della versione dell'app consente all'amministratore di distribuire e gestire una versione specifica dell'applicazione su dispositivi gestiti da DDM.

Quando è abilitato il pinning della versione:

- I dispositivi installano la versione dell'applicazione specificata.
- Gli upgrade automatici alle versioni più recenti sono impediti.
- Le applicazioni rimangono sulla versione assegnata fino a quando una nuova versione non viene esplicitamente selezionata da un amministratore.

Questa funzionalità consente un controllo funzionalità più rigoroso sulla coerenza delle versioni delle applicazioni e sulle distribuzioni di upgrade in fasi.

Procedura

1. Andare in **App** > **Catalogo app**.
2. Fare clic su un'app dall'elenco visualizzato. Si apre la pagina **Dettagli app**.
3. Nella scheda **Configurazioni app**, fare clic su **Impostazioni app Apple**.
4. Fare clic su una delle impostazioni esistenti elencate.
5. Fare clic su **Modifica**.
6. Sotto la sezione **Blocca versione app di un dispositivo**, selezionare l'opzione **Blocca versione app**.
7. Dall'elenco **Seleziona versione app**, selezionare la versione richiesta dell'app.

> Se il dispositivo ha una versione esistente dell'app, non è possibile sostituirlo con una versione precedente.

8. Fare clic su **Aggiorna**.

Controlli automatici degli aggiornamenti dell'App Store (Aggiornamento automatico app)

Gli amministratori possono configurare il modo in cui vengono gestiti gli aggiornamenti dell'App Store per le applicazioni gestite. Questa funzionalità fornisce un maggiore controllo sul comportamento di aggiornamento delle applicazioni e aiuta le aziende ad allineare gli update con i processi interni di convalida e implementazione.

Consenti download tramite cellulare

DDM introduce un'impostazione dedicata per controllare i download e gli aggiornamenti delle applicazioni sulle reti cellulari.

Procedura

1. Andare in **App** > **Catalogo app**.
2. Fare clic su un'app dall'elenco visualizzato. Si apre la pagina **Dettagli app**.
3. Nella scheda **Configurazioni app**, fare clic su **Installa sul dispositivo**.
4. Fare clic su una delle impostazioni esistenti elencate.
5. Fare clic su **Modifica**.
6. Nella sezione **Download consentiti su dati mobili**, selezionare una delle seguenti opzioni:
   - **Memorizza impostazioni** - Opzione predefinita. Il dispositivo utilizza le impostazioni per lo store corrispondente durante il download delle app.
   - **Sempre acceso** - Il download delle app è autorizzato anche se il dispositivo non dispone di connettività Wi-Fi.
   - **Sempre spento** - Il download dell'app non è consentito se il dispositivo non dispone di connettività Wi-Fi.
7. Fare clic su **Aggiorna**.

Flusso di lavoro Installazione applicazione

Il processo di distribuzione delle applicazioni rimane simile a quello della tradizionale gestione app N-MDM.

Gli amministratori possono:

- Assegnare app
- Distribuire app
- Installare app

Tuttavia, il DDM cambia il modo in cui viene comunicato lo stato di distribuzione. Piuttosto che basarsi sull'estrazione del server, i dispositivi segnalano le modifiche allo stato dell'applicazione non appena viene completata un'azione. Ciò fornisce informazioni più accurate e tempestive sullo stato di avanzamento dell'installazione e sui risultati della distribuzione.

Segnalazione e monitoraggio dello stato

Uno dei principali vantaggi di Gestione app DDM è la creazione di report sullo stato proattivo.

Con DDM:

- I dispositivi monitorano lo stato dell'applicazione localmente.
- Gli eventi di installazione e aggiornamento vengono rilevati immediatamente.

- Le modifiche di stato vengono automaticamente segnalate al server.
- Le informazioni sulla distribuzione diventano disponibili senza attendere gli intervalli di polling pianificati.

Ciò fornisce agli amministratori una visibilità più rapida su:

- Progressi installazione applicazione
- Installazioni riuscite
- Completamento aggiornamento applicazione
- Modifiche allo stato dell'applicazione
- Errori di distribuzione

La creazione di report in tempo reale migliora la risoluzione dei problemi e fornisce un'esperienza di gestione delle applicazioni più reattiva.

Requisiti

Gestione app DDM è supportato solo su:

- iOS 26 o versioni successive
- iPadOS 26 o versioni successive
- Client gestito Ivanti Go 126 o versioni successive

Gli apparecchi che non soddisfano questi requisiti continuano a utilizzare la tradizionale Gestione app N-MDM.

> Una volta che un dispositivo viene elaborato tramite Gestione app DDM, la disattivazione o l'aggiornamento di questa distribuzione dei criteri non ripristina il dispositivo alla Gestione app MDM. Per riportare il dispositivo alla Gestione app MDM, eliminare l'assegnazione dei criteri e registrare nuovamente il dispositivo.

8.3. Apps@Work (iOS, Android, Windows e macOS)

Apps@Work è un app storefront aziendale che facilita la distribuzione sicura di software e app. Apps@work è disponibile per dispositivi iOS, Android, macOS e Windows. L'appstore aziendale Apps@Work è integrato nei client Ivanti Go app e Mobile@Work per iOS, Android e macOS. Per i dispositivi Windows è un'applicazione standalone nativa. Argomenti della sezione:

- **iOS Apps@Work**
- **Android Apps@Work**
- **macOS Apps@Work**
- **Windows Apps@Work**

iOS Apps@Work

L'appstore nativo Apps@work viene distribuito automaticamente con il client Go. Non è richiesta alcuna azione dall'amministratore. La scheda Apps@work viene visualizzata sulla barra delle applicazioni del client Go. L'utente finale può passare a questa scheda per visualizzare e installare le app approvate dalla propria azienda. Per ulteriori informazioni, vedere **Caratteristiche dell'AppStore iOS Apps@Work**.

Le notifiche per l'utente finale di iOS Apps@Work per gli aggiornamenti app sono abilitate per impostazione predefinita. Se si desidera cambiare le impostazioni, vedere l'argomento **Notifiche** in **Impostazioni catalogo**.

Clienti esistenti con iOS Apps@Work Webclip

I clienti che presentano la webclip legacy iOS Apps@Work distribuita, non otterranno il Catalogo app nativo integrato per impostazione predefinita. Se si desidera passare al catalogo iOS Apps@Work Native e rimuovere la webclip Apps@work dai dispositivi, completare i seguenti passi:

Push delle configurazioni

L'amministratore deve eseguire il push della configurazione di Catalogo app per client nativi ai dispositivi al fine di rendere Apps@Work disponibile in un'esperienza Native Appstore da un'applicazione client Go. Per maggiori informazioni, vedere **Utilizzo delle configurazioni**.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Andare su **Configurazioni** > Filtro e selezionare **Servizi client**. Sono elencate tutte le configurazioni del client.
3. Selezionare **Catalogo app per client nativo**. Si apre la pagina di configurazione di Catalogo app per client nativo.
4. Fare clic sull'icona **Modifica distribuzione**. Si apre la pagina Modifica distribuzione.
5. Selezionare una delle seguenti opzioni:
   - **Tutti i dispositivi**
   - **Nessun dispositivo** - se non si desidera distribuire ad alcun dispositivo
   - **Personalizzato** - permette di selezionare dispositivi, gruppi di dispositivi, utenti, gruppi di utenti
6. Dopo la distribuzione della configurazione, l'utente deve aggiornare la versione del client Go alla 83 o superiore. La scheda Apps@Work è ora visibile nel client Go app .

> La configurazione non può essere sottoposta a push per i dispositivi registrati usando iReg perché il client Go non è disponibile sul dispositivo. È necessario installare il client Go app per ottenere il catalogo app nativo. Per ulteriori informazioni, vedere **Registrazione del dispositivo (iOS, macOS e Android)**.

Rimuovere iOS Apps@Work Webclip

I clienti che presentano Apps@Work Webclip distribuito ai loro dispositivi e sono già migrati all'esperienza Apps@Work Native possono rimuovere la webclip iOS Apps@Work.

Procedura

1. Accedere a **Configurazioni**.
2. Filtrare la configurazione - **Catalogo app Apple**.
3. Fare clic su **Modifica**.
4. Da **Distribuzione** selezionare **Nessuna distribuzione ai dispositivi**.
5. Fare clic su **Salva**.

Android Apps@Work

L'appstore nativo Apps@work viene distribuito automaticamente con il client MI Go. Non è richiesta alcuna azione dall'amministratore. La scheda Apps@work viene visualizzata sulla barra delle applicazioni del client Mi Go. L'utente finale può passare a questa scheda per visualizzare e installare le app approvate dalla propria azienda. Per ulteriori informazioni, consultare **Amministratore - Android Enterprise**.

macOS Apps@Work

MacOs Apps@work è integrato nel client macOS Mobile@Work. Una volta che il dispositivo si è registrato in Ivanti Neurons per MDM il client passerà alla visualizzazione come Apps@Work. Per i tenant appena creati, la configurazione di Apple App Catalog Webclip non effettuerà il push ai dispositivi macOS. Se necessario, l'amministratore può distribuire la configurazione di Apps@work Webclip ai dispositivi macOS. Per ulteriori informazioni, vedere **Configurazione dei dispositivi macOS**.

Distribuzione di app macOS

- Ivanti supporta la distribuzione app macOS mediante il protocollo Apple MDM e l'utilizzo dell'app Mobile@Work. Gli amministratori possono scegliere di utilizzare uno o entrambi dei seguenti approcci:
  - Protocollo MDM di Apple - Gli amministratori possono caricare solo formati PKG specifici (formato di distribuzione), come le app interne, e può anche distribuire le app dal Mac App Store (il supporto per le licenze App e libri è incluso). Tuttavia, questo approccio non consente agli amministratori di distribuire DMG e altri formati PKG.
  - Mobile@Work per app macOS - Come metodo per distribuire le app agli utenti, gli amministratori possono utilizzare l'app MobileIron Packager (MIP) per convertire qualsiasi file PKG, DMG o .app in un file MIP. Carica il file MIP in Ivanti Neurons per MDM come app in-house

È possibile scaricare l'utilità dal **sito di download software**.

- Gli amministratori possono utilizzare Mobile@Work per distribuire le app interne nel formato DMG, PKG o .app. Per le app disponibili solo nel Mac App Store, gli amministratori possono continuare a utilizzare le funzionalità MDM native di Apple, che comprendono le licenze App e libri di Apple. Per ulteriori informazioni, vedere **Configurazione dei dispositivi macOS**.

Windows Apps@Work

Apps@Work è un'app nativa indipendente che può essere scaricata dal Microsoft Store o che può essere sottoposta a push direttamente da Ivanti Neurons per MDM. Permette l'uso di app pubbliche e interne di Windows su dispositivi Windows 10+ in Ivanti Neurons per MDM. L'installazione di Apps@Work sui dispositivi Windows 10+ supportati è invisibile all'utente.

Per ulteriori informazioni, consultare **Configurazione dell'app**.

Utilizzo di Windows Apps@Work

Apps@Work permette l'uso di app pubbliche e interne di Windows su dispositivi Windows 10 in Ivanti Neurons per MDM. L'installazione di Apps@Work sui dispositivi Windows 10 supportati è invisibile all'utente.

Autenticazione del certificato Apps@Work

Per utilizzare l'Autenticazione certificato con Windows Apps@Work:

1. Passare ad **Amministratore > Windows > Autenticazione certificato Apps@Work**.
2. Regolare l'impostazione su **ON**.

> Regolare l'impostazione su **OFF** per imporre l'uso di nome utente e password.

> SAML non è supportato per Apps@Work per Windows.

Per configurare un'app per Apps@Work:

1. Selezionare un'app di Windows.
2. Fare clic sulla scheda **Configurazioni delle app**.
3. Fare clic su **Installa su dispositivo**.
   È possibile impostare la configurazione delle app interne di Windows sull'installazione invisibile all'utente oppure installarle tramite Apps@Work. Non è possibile impostare l'installazione invisibile all'utente per le app pubbliche.
4. È possibile scegliere di visualizzare o nascondere le app nel catalogo di Apps@work.
   Questa opzione si applica solo alle app interne.
5. Fare clic sulla scheda **Promozione**.

> Apps@Work attualmente non supporta la promozione dei banner, quindi le opzioni disponibili sono **In evidenza** e **Non in evidenza**.
>
> Solo l'opzione **Promozione** viene visualizzata per le app pubbliche.

8.4. Caratteristiche dell'AppStore iOS Apps@Work

La scheda Apps@Work presenta le seguenti caratteristiche:

- Accedere alla scheda Apps@Work dall'applicazione Go
- Cerca
- Installazione di un'app - Stati pulsante
- Applicazioni e banner in evidenza
- Notifica aggiornamento applicazione
- Impostazioni-Dispositivi personali

Accedere alla scheda Apps@Work dall'applicazione Go

Procedura

1. Accedere a Go app dal proprio dispositivo iOS.
2. Toccare l'icona **Apps@Work**. Sono disponibili due schede predefinite: App e Categorie.

3. Toccare la scheda **Tutte le app**. La scheda Tutte le app elenca le app in ordine alfabetico.
4. Toccare la scheda **Categorie**. La scheda Categorie visualizza solo le categorie che contengono applicazioni nel modo seguente:
    - Ciascuna categoria visualizza il numero di applicazioni presenti al suo interno.
    - La riga MyApps sotto la scheda Categorie è un elemento elenco contenente tutte le applicazioni installate. La riga MyApps sarà sempre la prima categoria, mentre il resto delle categorie viene elenco alfabeticamente.
    - Quando non viene installata alcuna applicazione, l'elenco MyApps mostra Nessuno.
    - Quando si fa clic su una categoria, tutte le applicazioni specifiche per la categoria vengono elencate con l'opzione Installa. Fare clic su **Installa** per installare ogni applicazione individualmente oppure fare clic su **Installa tutto** per installare tutte le applicazioni della categoria. Verrà richiesta l'autorizzazione a installare ciascuna applicazione.

Cerca

Procedura

1. Accedere a Go app dal proprio dispositivo iOS.
2. Toccare l'icona **Apps@Work**.
3. Toccare l'icona di ricerca (lente) per ricercare quanto segue:
    - **Nuovi rilasci** - mostra un elenco delle app rilasciate di recente quando non viene digitato alcun testo nella barra di ricerca

    - Digitare qualsiasi testo e il campo ricerca predirà dinamicamente e visualizzerà le applicazioni corrispondenti.
    - Il conteggio risultato ricerca viene visualizzato come intestazione secondaria
    - È anche possibile toccare il pulsante **Installa** per installare un'applicazione senza passare alla pagina dei dettagli.


Installazione di un'app - Stati pulsante

Poiché l'installazione dell'app richiede che il server elabori la richiesta ed effettui il push dell'app sul dispositivo, il pulsante di installazione non mostrerà i progressi in tempo reale. Il pulsante di installazione cambia stato da Installa > Richiesto > Installato.

Procedura

1. Accedere a Go app dal proprio dispositivo iOS.
2. Toccare l'icona **Apps@Work**.
3. Toccare **Installa** e le notifiche di stato appariranno nel modo seguente:
   - Appare un messaggio di avviso, per la prima volta, a indicare che è richiesta un'installazione.
   - Toccare il pulsante Richiesto. Appare un messaggio di avviso.

     > Lo stato Installato non è un pulsante.



Applicazioni e banner in evidenza

La scheda Funzionalità è visibile in base alla configurazione con push dell'amministratore. La scheda In evidenza è la pagina di destinazione predefinita quando non sono disponibili aggiornamenti.



Procedura

1. Accedere a Go app dal proprio dispositivo iOS.
2. Toccare l'icona **Apps@Work**.
3. Toccare la scheda **In evidenza**.
   - Il Banner app in evidenza visualizza un'applicazione nel banner.
   - L'app in evidenza contiene un elenco di tutte le applicazioni in evidenza.



Notifica aggiornamento applicazione

L'utente finale riceve una notifica sul dispositivo quando sono disponibili aggiornamenti delle applicazioni. La notifica contiene il numero di applicazioni che hanno aggiornamenti disponibili. Quando l'utente fa clic sulla notifica, si apre Apps@Work.

Procedura

1. Accedere a Go app dal proprio dispositivo iOS. L'icona Apps@Work visualizza il conteggio delle applicazioni con aggiornamenti in sospeso.
2. Toccando la notifica di aggiornamento dell'applicazione, si verrà reindirizzati alla scheda Tutte le app di Apps@Work. Vengono visualizzate le seguenti indicazioni:
   - La sezione secondaria Aggiornamenti disponibili sotto la scheda Tutte le app visualizza il conteggio delle applicazioni disponibili per l'aggiornamento.
   - Un'icona con un punto rosso viene visualizzata per ogni applicazione che richiede un aggiornamento.



Impostazioni-Dispositivi personali

Procedura

1. Accedere a Go app dal proprio dispositivo iOS.
2. Toccare l'icona **Impostazioni**.
    - La scheda Dispositivi personali è disponibile sotto Impostazioni.
    - Dispositivi personali è ora elencato come un elemento di linea sotto Autentica.

8.5. Funzioni avanzate di iOS Go

Le coppie chiave-valore (KVP) sono semplici impostazioni dell'applicazione costituite da una chiave (il nome dell'impostazione) e un valore (la configurazione che si desidera applicare). In Ivanti Go per iOS, le organizzazioni utilizzano i KVP per abilitare o disabilitare le funzionalità e regolare il comportamento dell'app senza richiedere un aggiornamento.

Quando Ivanti Go viene eseguito su iPhone o iPad gestiti dall'organizzazione, legge queste impostazioni KVP all'avvio o durante un check-in. L'app applica immediatamente gli aggiornamenti, garantendo che le modifiche alla configurazione vengano consegnate rapidamente, in modo coerente e agli utenti corretti.

Utilizzo dei KVP nelle configurazioni dell'app Ivanti Go

I KVP per la personalizzazione dei messaggi di violazione sono supportati sull'app Ivanti Go. È possibile configurare i KVP all'interno delle impostazioni dell'app Ivanti Go per personalizzare l'applicazione.

Procedura

1. Aprire l'app **Ivanti Go** nel proprio AppCatalog.
2. Selezionare **Configurazioni**.
3. Fare clic su **Aggiungi** per creare una nuova **configurazione app Apple**.
4. Aggiungere manualmente i propri KVP:
    - Nella colonna **Chiave**, immettere la chiave di configurazione che si desidera personalizzare.
    - Nella colonna **Valore**, immettere il valore che si desidera applicare ai dispositivi.
5. (Facoltativo) Caricare un file *.plist* esistente contenente i KVP predefiniti che si desidera applicare.
6. **Salvare** la configurazione.
7. I KVP aggiornati verranno applicati ai dispositivi durante il prossimo check-in.

Aggiunta di un plist a una specifica app iOS (app per più coppie chiave-valore)

Gli amministratori possono impostare più coppie chiave-valore (KVP) per un'app iOS utilizzando i numeri di serie dell'app, gli identificatori del Bundle, i dettagli della versione o altri metadati. Ciò può avvenire in modo efficiente caricando un file .plist attraverso la console Ivanti Neurons for MDM.

Procedura

1. Andare ad **App**.
2. Aprire **App Catalog**.
3. Selezionare e aprire l'**app iOS specifica** che si desidera configurare.
4. Andare alla scheda Configurazioni app.
5. Selezionare **Configurazione app gestite Apple**.
6. Fare clic sul pulsante **Aggiungi**.
7. Immettere un **Nome** per la configurazione.
8. Fare clic su **Usa .plist**.
9. Selezionare **Scegli una di queste opzioni**.

10. Accedere al file plist, selezionarlo e fare clic su **Apri**. Il sistema compilerà automaticamente la tabella di configurazione con le coppie di valori chiave dal plist.
11. Scegliere il gruppo(i) di utenti o il gruppo di dispositivi (i) che dovrebbero ricevere la configurazione.
12. Fare clic su **Distribuisci questa configurazione app**.
13. Fare clic su **Salva** per completare la procedura.

> Il file caricato deve avere un'estensione .plist. Se è stato creato manualmente il file (esempio, in un editor di testo), assicurarsi che l'estensione sia cambiata da *.txt* a *.plist* prima di caricare.

Avvio di Ivanti Go app in modalità app singola durante la registrazione

Questa funzione consente all'amministratore di utilizzare coppie chiave-valore durante la registrazione del dispositivo per avviare automaticamente Ivanti Go for iOS in modalità app singola (SAM). Quando un dispositivo inizia la registrazione, le coppie chiave-valore configurate attivano l'apertura immediata di Ivanti Go. Durante questo processo, all'utente viene presentato un messaggio che indica:

Attendere mentre il dispositivo è in fase di configurazione.

Per attivare questo comportamento, è necessario installare la configurazione modalità app singola ed esplicitamente indirizzata a Ivanti Go per iOS prima o durante il flusso di lavoro di registrazione. Una volta completata con successo la registrazione, la modalità app singola viene app chiusa automaticamente. Il dispositivo viene quindi rilasciato all'utente finale per il normale funzionamento, garantendo una configurazione sicura senza limitare l'uso post-registrazione.

Questa funzionalità supporta l'ambiente Ivanti Mobile@Work, fornendo un flusso di registrazione protetto per i dispositivi iOS supervisionati.

Impostazione dell'attivazione Zero Touch

Per abilitare l'attivazione Zero Touch per Ivanti Go, completare i seguenti passaggi:

1. Impostare un gruppo che includa solo i dispositivi in cui *Client registrato = No*.
2. Creare una configurazione Modalità app singola (SAM) per l'applicazione Ivanti Go. Assegnare questa configurazione solo al gruppo di dispositivi creato nel *passaggio 1*.
3. Aggiungere la coppia di valori chiave (KVP) zero_touch_activation alla configurazione dell'app Ivanti Go. Destinare lo stesso gruppo di dispositivi utilizzato nei passaggi precedenti.

Configurazione KVP

Chiave	Valore	Tipo	Descrizione
zero_touch_activation	Vero	Booleano	Quando il valore è impostato su true, l'app Ivanti Go riconosce che è in esecuzione in Single App Mode (SAM) attraverso la configurazione SAM. La configurazione SAM avvia l'app Ivanti Go, mentre questo valore funge da impostazione aggiuntiva che consente all'app di funzionare correttamente in modalità SAM. Una volta completata la registrazione, il dispositivo esce dalla modalità SAM e diventa disponibile per l'utente finale per l'uso normale.

Abilitazione del pulsante Torna al servizio in Ivanti Go (iOS 18+)

La funzione **Ritorna al servizio** consente al dispositivo di registrarsi nuovamente in automatico una volta cancellati i dati, riducendo la necessità di registrare nuovamente in manuale il dispositivo dopo una cancellazione.

Gli amministratori possono abilitare o disabilitare il pulsante Torna al servizio utilizzando una coppia di valori chiave (KVP) configurabile. Quando il KVP viene distribuito a Ivanti Go come parte della configurazione dell'app:

- L'opzione Torna al servizio diventa visibile all'utente finale.
- L'utente può avviare il processo di ripristino direttamente da Ivanti Go.
- Il dispositivo esegue un ripristino del Ritorno al servizio gestito da Apple.
- I profili di gestione e le app richieste rimangono intatti.
- Il dispositivo completa il suo flusso di ri-provisioning e diventa pronto per il riutilizzo.

Questa funzione è supportata su Ivanti Go per iOS, iOS 18 e dispositivi successivi registrati in modalità DEP.

Configurazione KVP

Aggiungere il seguente KVP alla configurazione dell'app gestita da Ivanti Go in Ivanti Neurons for MDM:

Chiave	Valore	Descrizione
ReturnToServiceEnabled	vero	Abilita il pulsante **Torna al servizio** in Ivanti Go. Se impostata su Falso o Omesso, la funzione rimane nascosta.

Disattivazione della protezione screenshot nella schermata di autenticazione SAML

Ivanti Go per iOS include la protezione integrata degli screenshot per aumentare la protezione durante la registrazione del dispositivo. Per impostazione predefinita, la registrazione con le schermate di autenticazione SAML blocca:

- Schermate
- Registrazioni schermo
- Condivisione schermo

Questa protezione assicura che i dati di autenticazione riservati, come nomi utente, password e contenuto di accesso basato su SAML, non possano essere acquisiti o condivisi senza autorizzazione.

Gli amministratori possono disabilitare la protezione degli screenshot sui dispositivi gestiti utilizzando una configurazione KVP. Quando viene applicata questa configurazione, l'app Ivanti Go consentirà screenshot e registrazioni solo sulla schermata di autenticazione SAML, mantenendo tutti gli altri meccanismi di sicurezza in tutta l'app.

Configurazione KVP

Per disabilitare la protezione screenshot per la schermata di autenticazione SAML, applicare il seguente KVP alla configurazione dell'app Ivanti Go nel proprio MDM:

Chiave	Valore	Descrizione
SCREENSHOT_PROTECTION_DISABLED	Vero	Disabilita la protezione da screenshot, registrazione dello schermo e condivisione dello schermo nella schermata Autenticazione SAML. Se omessa o impostata su Falso, la protezione rimane abilitata per impostazione predefinita.

KVP per personalizzare i messaggi di violazione dei criteri

Questi KVP consentono agli amministratori di personalizzare i messaggi inviati agli utenti finali quando vengono rilevate Violazioni dei criteri.

Questi KVP per la personalizzazione descrivono i KVP e i tipi di violazione disponibili per gli amministratori per personalizzare il comportamento dell'app Ivanti Go per iOS. Questi KVP definiscono il comportamento delle app, come fornire notifiche dettagliate agli utilizzatori del dispositivo ed esportare i contatti da Ivanti Go per iOS.

I tipi di violazione non si escludono a vicenda. Se è presente una serie di violazioni, verrà visualizzato un elenco di messaggi in Ivanti Go per iOS.

Coppie di valori chiave (KVP)	Messaggi predefiniti
compliance.message.COMPROMISED	• Il proprio dispositivo è stato compromesso perché ha subito un jailbreak. Restituire correttamente il dispositivo a uno stato non jailbroken o contattare l'amministratore per ricevere assistenza nella risoluzione di questo problema.
compliance.message.DATA_PROTECTION_DISABLED	• L'accesso aziendale è stato disabilitato per la protezione dei dati. Contattare l'amministratore per ricevere assistenza nella risoluzione di questo problema.
compliance.message.OUT_OF_ CONTACT	• Il tuo dispositivo iOS non è contattabile. Contattare l'amministratore per ricevere assistenza nella risoluzione di questo problema.
compliance.message.APPS	• Il tuo dispositivo è privo di app richieste e/o presenta app non consentite. Aggiungere/rimuovere le app necessarie o contattare l'amministratore per ricevere assistenza nella risoluzione di questo problema.
compliance.message.MDM_DISABLED	• Il dispositivo non è conforme perché la funzionalità MDM è stata disattivata. Registrare nuovamente il dispositivo o contattare l'amministratore per ricevere assistenza nella risoluzione di questo problema.
compliance.message.ROAMING	
compliance.message.generic	• L'accesso aziendale è stato disabilitato per un motivo non specificato. Contattare l'amministratore per ricevere assistenza nella risoluzione di questo problema.
compliance.message.header	Il dispositivo non è conforme per i seguenti motivi: Quando il tipo di violazione è CUSTOM o CUSTOM_NOTIFY_ONLY, il sistema visualizza messaggi autonomi senza intestazione.
compliance.message.CUSTOM	Potrebbe essere richiesta un'azione sul dispositivo. Contattare l'amministratore se necessario.
compliance.message.CUSTOM_NOTIFY_ONLY	Il dispositivo non è conforme ed è stata inviata una notifica. Fare riferimento alla scheda Notifiche o alle e-mail per informazioni dettagliate.

Se l'elenco dei tipi di violazione non include alcuna violazione con un messaggio mappato, ma include almeno una violazione senza un messaggio mappato, visualizzare il messaggio predefinito:

- L'accesso aziendale è stato disabilitato per un motivo non specificato. Contattare l'amministratore per ricevere assistenza nella risoluzione di questo problema.

Se l'elenco dei messaggi contiene almeno un messaggio di violazione, visualizzare la seguente intestazione sopra l'elenco:
Il dispositivo non è conforme per i seguenti motivi:

> Se non si desidera modificare un messaggio predefinito, non includere una coppia chiave-valore (KVP). Definire solo i KVP per i messaggi che si intende modificare.

Configurare i client predefiniti del browser e delle e-mail utilizzando la Configurazione app gestita

Le coppie di valori chiave (KVP) consentono agli amministratori di impostare il browser e il client e-mail utilizzati da **Ivanti Go** per l'apertura di collegamenti Web e la composizione di e-mail tramite la configurazione dell'app gestita.

In qualità di amministratore, è possibile utilizzare i KVP Configurazione app gestita per controllare come vengono gestiti i collegamenti all'interno della scheda **Supporto**:

Chiave	Valori	Tipo	Descrizione
browser_predefinito	safari, edge, chrome, firefox, brave, opera, webatwork, duckduckgo	Stringa	Browser che Ivanti Go utilizza per aprire i collegamenti Web nella scheda Supporto. I collegamenti http/https vengono reindirizzati allo schema configurato dal browser. **Impostazione predefinita se non configurata**: browser predefinito di sistema.
Consenti_fallback_browser	vero, falso	Booleano	**Comportamento quando il browser predefinito non è installato**: **Vero**: ritorna al browser di sistema predefinito. **Falso**: link non aperto, l'utente vede l'avviso "<Browser> non installato". **Impostazione predefinita se non configurata**: Vero
limita_condivisione_log_a_e-mail	vero, falso	Booleano	Se la condivisione del registro/supporto è limitata solo alle e-mail (utilizzando l'e-mail_predefinita). L'associazione automatica dei registri funziona con e-mail+ e posta nativa Funziona con **consenti_fallback_email**. **Vero**: condivisione solo nelle e-mail. **Falso**: opzioni di condivisione standard disponibili. **Impostazione predefinita se non configurata**: falsa.
e-mail_predefinita	nativemail, Outlook, gmail, yahoo, citrixmail.emailplus, spark, protonmail	Stringa	Client e-mail che Ivanti Go utilizza per comporre le e-mail dai collegamenti mailto nella scheda Supporto. mailto viene trasformato nel'URL di composizione **predefinita del client se non configurato**: applicazione di posta predefinita. Doppio ruolo nella risoluzione dei collegamenti e nella condivisione dei registri quando il client_e-mail predefinito non è installato.
Consenti_fallback_e-mail	Vero, Falso	Booleano	**Comportamento quando le e-mail predefinite non sono installate**. **Vero**: la composizione delle e-mail ritorna all'applicazione di posta predefinita se il client e-mail configurato non è stato configurato e la condivisione dei registri può utilizzare un metodo di consegna alternativo. **Falso**: la composizione delle e-mail è bloccata e l'utente visualizza un avviso "**Non installato**" se il client e-mail configurato non è disponibile. Le restrizioni di condivisione registri vengono applicate senza opzione di fallback. **Impostazione predefinita se non configurata**: vero. (comportamento di fallback abilitato)

8.6. Visualizzazione dei dettagli delle app

È possibile eseguire il drill-down da App Catalog ai dettagli dell'applicazione di una qualunque delle applicazioni disponibili nel catalogo. Nella pagina dei dettagli dell'app vengono visualizzate informazioni quali Versione visualizzata (ad esempio 1.5.0), Versione in bundle (ad esempio 1.5.0.42) e Versione minima sistema operativo richiesta (ad esempio 5.0 per Android).

Le app che non soddisfano la versione specificata nel campo Versione minima sistema operativo richiesta non vengono visualizzati nel catalogo Apps@Work. Pertanto, tali app non sono disponibili per essere distribuite ai dispositivi. Il campo Versione minima sistema operativo richiesta viene visualizzato anche come parte di **Audit trail** delle app.

Procedura

1. Fare clic su **Applicazioni**.
2. Fare clic su **Catalogo app**.
3. Selezionare l'app.

Viene visualizzata la finestra Dettagli app.

> Per le app interne a iOS, è possibile controllare la **Data di scadenza profilo di provisioning** sulla pagina dettagli app.

> Informazioni sulle app include l'opzione **Consenti installazione app su dispositivi M1 al momento della distribuzione** per tutte le app VPP per iOS e iPadOS. L'amministratore deve abilitare l'opzione **Consenti installazione app su dispositivi M1 al momento della distribuzione** solo per le applicazioni VPP per iOS o iPad installabili in un dispositivo macOS M1. L'amministratore può vedere i dispositivi macOS M1 durante l'installazione delle applicazioni solo se ha abilitato questa opzione. La configurazione dell'app gestita è supportata per le applicazioni VPP iOS sui dispositivi Mac M1.

> Per le app dell'App Store di iOS e macOS, incluso il Business-to-Business, **Sincronizza nuova versione** controlla e sincronizza gli aggiornamenti delle app dall'App Store. La versione aggiornata dell'app viene visualizzata entro 12-24 ore in base al programma di sincronizzazione dell'app.

> In Dettagli dispositivo è stato aggiunto un pulsante di attivazione/disattivazione per **App prerequisito**. Gli amministratori possono selezionare questa opzione e aggiungere app come prerequisiti per un'app principale.

Una volta che un'app è stata distribuita a diversi dispositivi, lo stato di distribuzione dell'app può essere visualizzato nella scheda **Riepilogo dispositivi**. La scheda Riepilogo dispositivi contiene anche informazioni sul numero di dispositivi idonei, sul numero di dispositivi su cui l'app è stata installata, sul numero di dispositivi su cui l'installazione dell'app è in sospeso e sul numero di dispositivi su cui l'installazione dell'app non è riuscita. Il conteggio dei dispositivi in questi riquadri si basa sui dispositivi con installazione obbligatoria di app, in modo che gli amministratori possano tenere traccia della distribuzione iniziale delle app obbligatorie.

Per il conteggio generale delle applicazioni (comprese quelle installate dall'utente), utilizzare la ricerca Inventario app.

> Le app escluse dal dispositivo hanno lo stato di distribuzione In sospeso.

La seguente tabella elenca i motivi della mancata installazione delle app su iOS / OSX:

Motivo	Descrizione
AppAlreadyInstalled	"App già installata."
AppStoreDisabled	"L'app store è disattivato."
CouldNotVerifyAppID	"Impossibile verificare l'ID app."
Non riuscito	"L'installazione dell'app non è riuscita a causa di un errore sconosciuto".
ManagedButUninstalled	"L'app è gestita, ma è stata rimossa dall'utente. Quando l'app verrà installata di nuovo (anche dall'utente), verrà nuovamente gestita."
ManagementRejected	"L'utente ha rifiutato la conversione di un'app non gestita in un'app gestita".
NotAnApp	"Il comando InstallApplication è stato rifiutato a causa di un identificativo di applicazione non valido che si risolve in una risorsa diversa da un'app."
NotSupported	"L'app non è supportata".
Altro	"Motivo dei nuovi errori aggiunti".
PurchaseMethodNotSupported	"Per iOS 7 e successivi, l'app non può essere installata a causa di un metodo di acquisto non valido (applicabile solo alle app VPP)."
UserInstalledApp	"L'utente ha installato l'app prima che potesse avvenire l'installazione dell'app gestita".
UserRejected	"L'utente ha rifiutato l'offerta di installare l'app".
UpdateRejected	"L'utente ha rifiutato l'offerta di aggiornare l'app".

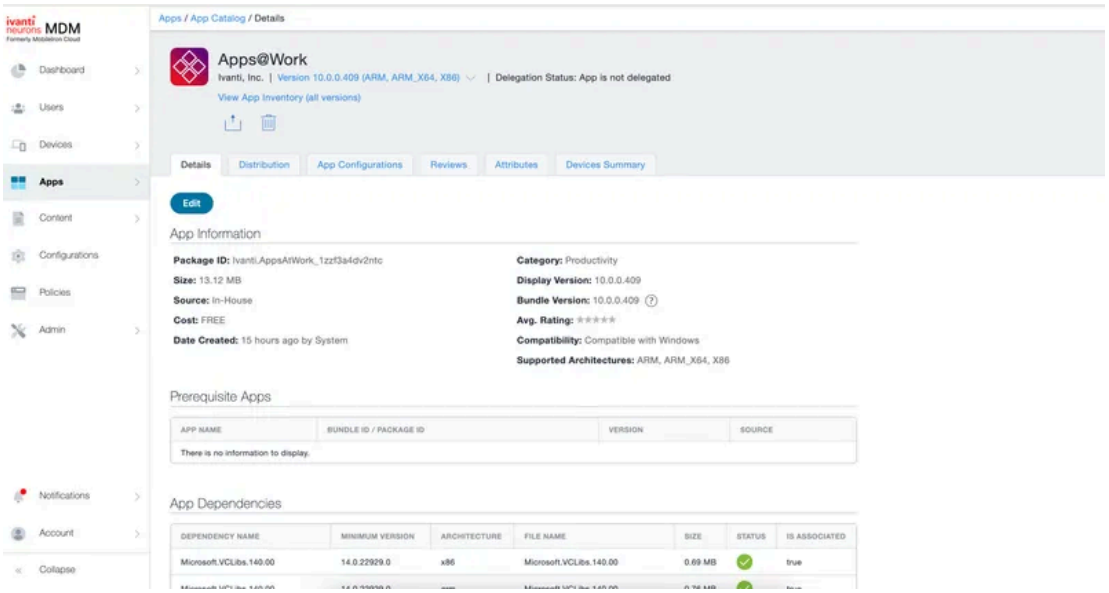
La seguente tabella elenca i motivi della mancata installazione delle app su Android:

Motivo	Descrizione
USER_INSTALLED	"Già installata sul dispositivo (al di fuori dell'MDM)."
NON SUPPORTATO	"Non supportata"
USER_REJECTED_INSTALL	"L'utente ha rifiutato l'installazione dell'applicazione."
ERROR_INSTALL	"Errore rilevato durante il tentativo di installazione; non riuscita."
UNRECOGNIZED	"L'elemento non è stato trovato o non è più tracciato (ad esempio, errore / disinstallazione dal dispositivo e rimozione dal tracciamento)."
UNSUPPORTED_INSTALL	"Aggiornato per il client Android 3.0/server 22.0.0: è necessario uno stato specifico per tenere traccia dell'installazione e della disinstallazione."
HIDDEN	"Durante la quarantena, verrà inviato lo stato HIDDEN/UNINSTALLED. L'opzione Rimuovi dalla quarantena dovrebbe ripristinare l'installazione".
OTHER	"Motivo dei nuovi errori aggiunti".

Per i dispositivi Windows, se l'app è impostata per l'installazione invisibile all'utente nelle Configurazioni app, il Riepilogo dispositivi visualizza il numero di dispositivi idonei, installati, in sospeso o non riusciti per l'app.

Visualizzazione delle informazioni sull'inventario app dalla pagina dettagli app

Per visualizzare le informazioni sull'inventario app, fare clic su **Visualizza inventario app (tutte le versioni)** per visualizzare in **Dispositivi > Inventario app** un elenco filtrato per ID bundle di tale app.



8.7. Configurazione dell'app

Argomenti della sezione:

- Licenze per le funzioni delle app
- Passaggi comuni per la configurazione di più app
- Nascondere e sospendere le app (solo per Android)
- Configurazione relay di rete
- Configurazione dello slicing 5G rete mobile
- Distribuzione dell'applicazione tramite la configurazione del Filtro contenuti web
- Distribuzione dell'applicazione tramite proxy DNS
- Cancellazione della cache delle app per dispositivi Android Enterprise

La configurazione dell'app consente di personalizzare l'installazione, la promozione e la distribuzione di ciascuna app implementata sui dispositivi degli utenti. Le app possono essere app interne, app provenienti da uno store pubblico o app Ivanti Neurons for MDM. È possibile distribuire le app a diversi utenti e gruppi con configurazioni e nomi univoci, specificamente personalizzati in base a ciascun destinatario. Il numero di versioni di applicazioni interne è limitato a 100. Se questo numero viene superato, il sistema Ivanti Neurons for MDM elimina le versioni meno recenti dell'applicazione. Gli stati di caricamento ed eliminazione dell'applicazione vengono indicati e sono visibili nella pagina Audit trail.

> Quando si modificano i valori per la configurazione di app presenti nel Catalogo app o nel profilo di configurazione delle app gestito, è necessario eseguire uno o due check-in del dispositivo, affinché il dispositivo riceva i nuovi valori di configurazione.

Licenze per le funzioni delle app

> Le funzioni riportate di seguito richiedono licenze aggiuntive:

- Installazione/disinstallazione app invisibile all'utente: licenza Silver
- Configurazione per-app: licenza Gold
- Configurazione personalizzata di AppConnect: licenza Gold

È necessaria una buona gestione dei gruppi per pacchetti di più applicazioni perché i nuovi tipi di dispositivo non potranno essere definiti dal sistema operativo di Windows. In questo è possibile installare la versione adeguata dell'app solo se l'amministratore usa il gruppo appropriato per l'applicazione appropriata.

Passaggi comuni per la configurazione di più app

Eseguire prima questi passaggi, quindi procedere con i passaggi per la configurazione di ciascuna app che si desidera distribuire. È possibile creare diverse configurazioni della stessa app e assegnare a ciascuna configurazione un nome univoco. Ciascuna configurazione può avere i propri livelli di distribuzione e promozione in base alla propria strategia di implementazione. Il numero di versioni di applicazioni interne è limitato a 100. Se questo numero viene superato, il sistema Ivanti Neurons for MDM elimina le versioni meno recenti dell'applicazione. Gli stati di caricamento ed eliminazione dell'applicazione vengono indicati e sono visibili nella pagina Audit trail. È possibile distribuire un'applicazione a un massimo di 100 utenti, gruppi di utenti, dispositivi o gruppi di dispositivi contemporaneamente. È possibile selezionare un'app da aggiungere al Catalogo app. Ivanti Neurons per MDM presenta una

procedura asincrona per il comando Invia richiesta di installazione/aggiornamento per le app iOS. Quando si usa il comando Invia richiesta di installazione/aggiornamento, il portale amministrativo di Ivanti Neurons per MDM visualizza un messaggio in cui:

- il processo continuerà a essere eseguito in background
- il processo è completo
- stato in cui il processo riesce o si verificano errori

Procedura

1. Andare a **App > Catalogo app** e fare clic su **+Aggiungi**.
2. Utilizzare il menu a discesa per selezionare l'App Store, Google Play oppure il proprio app store interno e scegliere un'app da aggiungere al catalogo.
   A seconda del contratto di licenza, potrebbero essere disponibili app da aggiungere al catalogo.
3. Facoltativamente, modificare la categoria dell'app.
4. Facoltativamente, aggiungere una breve descrizione dell'app nel campo **Descrizione**.
5. Fare clic su **Avanti**.
6. Scegliere un livello di distribuzione per questa configurazione dell'app:
   - **A tutti**: l'app viene aggiunta su tutti i dispositivi compatibili degli utenti.
   - **A nessuno**: l'app viene predisposta per essere distribuita in seguito.
   - **Distribuzione personalizzata** - Selezionare una delle opzioni seguenti:
     - **Utenti/Gruppi di utenti** - L'app viene distribuita solamente agli utenti o ai gruppi di utenti selezionati.
       Fare clic sulla scheda **Utenti** per selezionare gli utenti.
       Fare clic sulla scheda **Gruppi di utenti** per selezionare i gruppi di utenti.
     - **Dispositivi/Gruppi di dispositivi** - L'app viene distribuita solamente ai dispositivi o ai gruppi di dispositivi selezionati.
       Fare clic sulla scheda **Dispositivi** per selezionare i dispositivi.
       Fare clic sulla scheda **Gruppi di dispositivi** per selezionare i gruppi di dispositivi.
7. Fare clic su **Avanti**.

Configurazione delle opzioni di installazione

È possibile selezionare le opzioni di configurazione dell'installazione.

Procedura

1. Fare clic sulle **impostazioni di configurazione Installa applicazione** o fare clic sull'icona **+** per aggiungere un'altra configurazione e visualizzare la pagina **Impostazioni di configurazione**.
2. Immettere un nome per la configurazione nel campo **Nome**.
3. Facoltativamente, aggiungere una breve descrizione della configurazione dell'installazione nel campo **Descrizione**.
4. Selezionare l'opzione **Configurazioni installazione dispositivo**.
5. Selezionare una delle seguenti opzioni:
   - **Richiedi l'installazione sul dispositivo**
   - **Installa solo una volta alla registrazione del dispositivo**
6. Selezionare l'opzione **Non richiedere una versione specifica dell'app** per evitare il downgrade di un'app già installata a una versione inferiore. Questa opzione è disponibile solo per le app moderne.

7. Selezionare le opzioni seguenti:
    - **Installa in modo invisibile nell'area di lavoro Samsung Knox e sui dispositivi Zebra** (Solo Android)
    - **Non mostrare l'applicazione nel Catalogo app dell'utente finale**.
    - **Non installare l'app sui nuovi dispositivi registrati**: i dispositivi esistenti non subiranno alcun impatto e continueranno a visualizzare l'app nel catalogo app del dispositivo.
        - Per tutti i nuovi dispositivi registrati in questa distribuzione, l'app non sarà elencata e non ne verrà effettuato il push.
        - Se l'amministratore attiva un comando di invio di installazione/aggiornamento, il comando viene inviato al dispositivo.
    - **Rimanda aggiornamento app di**: è possibile utilizzare questa opzione per ritardare l'installazione della nuova versione dell'app. Questa impostazione ritarda l'installazione automatica di nuove versioni di app in base alla durata configurata.
    - **Modalità aggiornamento app** (supportata anche per i dispositivi AMAPI). (Solo Android)
      Usare questa opzione per aggiornare un'app all'ultima versione usando una delle tre modalità seguenti:
        - **Predefinita**: questa modalità viene selezionata quando si seleziona l'opzione Modalità aggiornamento app. In questa modalità, l'aggiornamento si verifica entro 24 ore dal momento in cui l'app diventa disponibile.
        - **Rinvia di 90 giorni**: se si seleziona questa modalità di aggiornamento, è possibile rinviare gli aggiornamenti dell'app di 90 giorni. Dopo 90 giorni, le app vengono aggiornate automaticamente sulla base delle altre impostazioni effettuate nella configurazione Google Play gestito.
        - **Priorità alta**: se si seleziona questa modalità di aggiornamento e il dispositivo dell'utente è online, l'app viene aggiornata immediatamente dopo che diventa disponibile sul Google Play Store.
    - **Imposta priorità di installazione app** - per maggiori dettagli, consultare l'argomento Configurazione della priorità delle app

> Sui dispositivi Android, gli aggiornamenti delle app sono consentiti utilizzando l'opzione Aggiornamento automatico anche senza selezionare l'opzione Installazione invisibile all'utente. L'amministratore può controllare gli aggiornamenti delle app non obbligatorie o di quelle autoinstallate dall'utente.

    - **Non aggiornare mentre l'app è in uso**: selezionare questa opzione per impedire l'aggiornamento di un'applicazione mentre l'utente la utilizza attivamente. Quando questa opzione è abilitata:
        - L'aggiornamento dell'applicazione viene differito mentre l'applicazione è in esecuzione in primo piano.
        - L'utente può continuare a utilizzare l'applicazione senza interruzioni.
        - L'aggiornamento in sospeso viene installato automaticamente quando l'applicazione viene chiusa o spostata in background.

Rimuovi applicazioni quando la distribuzione viene rimossa (Android)
Per le app Google Play gestite, Ivanti Neurons for MDM rimuove automaticamente le app dai dispositivi Android quando l'applicazione non è più assegnata al dispositivo.
Le applicazioni vengono rimosse nei seguenti scenari:

- La distribuzione dell'applicazione viene modificata in A nessuno.
- L'applicazione viene eliminata dall'App Catalog.
- Il dispositivo è escluso dalla distribuzione dell'applicazione.

È possibile imbattersi in opzioni di configurazione aggiuntive, a seconda dell'app selezionata. Tali opzioni possono includere la capacità di aggiungere più coppie di chiavi e valori. In questi casi fare clic su **+ Aggiungi** per immettere coppie di chiavi e valori. Per ulteriori informazioni, vedere **Aggiunta di un'app da uno store pubblico** in Catalogo app.

9. (macOS 11 e versioni successive) Selezionare le opzioni per installare e configurare le app come app gestite:
    - **Installa come app gestita**
    - **Converti in app gestita**

> In macOS 12.0 e versioni successive, il supporto per le app gestite è disponibile su dispositivi registrati dall'utente.

Nascondere e sospendere le app (solo per Android)

Per i dispositivi Android nelle seguenti modalità, **profilo di lavoro**, **dispositivo completamente gestito**, **dispositivo completamente gestito con profilo di lavoro** e **profilo di lavoro su dispositivo di proprietà dell'azienda**, è ora possibile nascondere o sospendere le app dopo l'installazione.

Procedura

	1. Installare una o più app sul dispositivo per il quale si desidera applicare l'azione Nascondi o Sospendi.
	2. Creare una configurazione di App Control e aggiungere le app gestite all'elenco Nascondi o Sospendi.
	3. Applicare le modifiche al dispositivo.

> Se un'app è presente in entrambi gli elenchi Nascondi e Sospendi, l'app verrà nascosta perché l'elenco Nascondi avrà la priorità.

Configurazione della priorità delle app

È possibile definire l'ordine di ricezione delle app sul dispositivo al momento della prima registrazione (nello specifico, entro i primi 20 minuti dalla data e ora di registrazione) e di invio delle app richieste per l'installazione. È possibile assegnare priorità di download ad app specifiche rispetto ad altre app. Ad esempio, assegnare la priorità al download delle app Tunnel e E-mail, prima di altre app non critiche. Questa funzionalità è applicabile alle app pubbliche e private. Le app prerequisito sono inviate prima delle app dipendenti.

Questa funzione è supportata su dispositivi iOS (tranne AppStation per iOS), Android (tranne Android for Enterprise), macOS (app PKG interne e app Apple Apps and Books) e Windows.

> Questa funzionalità è disponibile per dispositivi di nuova registrazione. Per impostazione predefinita, tutte le app sono impostate su priorità Media. Durante questo processo, l'utente può scegliere di installare manualmente qualsiasi app del catalogo, anche se questa competerà per le risorse da installare e potrebbe mettersi in coda prima delle app ad alta priorità.

> Nel caso delle app Windows, l'app Bridge ha la massima priorità rispetto alle altre app.

Vedere la sezione precedente, "Configurazione delle opzioni di installazione" per la procedura di impostazione della priorità delle app mediante l'opzione **Imposta Priorità installazione app**. È possibile impostare una priorità Alta, Media o Bassa per un'app. Le app con la stessa priorità verranno installate senza un ordine particolare. La priorità delle app non viene applicata durante gli aggiornamenti delle app, per le app già installate.

Selezione delle impostazioni Configurazione gestione applicazioni Apple

Queste impostazioni verranno applicate solo a quest'app e sovrascriveranno le impostazioni globali selezionate in **App > Impostazioni catalogo**. Per selezionare le impostazioni di **Gestione delle app Apple**.

Procedura

1. Fare clic sulle **impostazioni delle app Apple** o fare clic sull'icona **+** per aggiungere un'altra configurazione e visualizzare la pagina **Impostazioni di configurazione**.
2. Immettere un nome per la configurazione nel campo **Nome**.
3. Immettere una breve descrizione della configurazione nel campo **Descrizione**.
4. Selezionare o deselezionare una o più delle seguenti opzioni dalle **Impostazioni di gestione Apple**:
   - **Impedisci il backup su iCloud e iTunes**
   - **Rimuovi le app non registrate**
   - (iOS 14.0+) **Consenti la rimozione e l'offload di quest'app** - È possibile deselezionare questa opzione per evitare che un utente rimuova ed esegua l'offload di un'app gestita.
   - (Opzionale) Aggiungere una **Configurazione dell'app gestita Apple**
5. Fare clic su **Aggiorna**.

Selezione dei livelli di promozione dell'app

È possibile impostare il livello di promozione dell'app.

Procedura

1. Fare clic sulle **impostazioni di configurazione per la distribuzione delle promozioni** o fare clic sull'icona **+** per aggiungere un'altra configurazione e visualizzare la pagina di **configurazione della promozione**.
2. Fare clic su **Modifica**.
3. Immettere un nome per le impostazioni di configurazione per la distribuzione della promozione nel campo **Nome**.
4. Facoltativamente, aggiungere una breve descrizione della configurazione nel campo **Descrizione**.
5. Selezionare il livello di promozione desiderato per l'app: **Non in primo piano**, **Elenco in primo piano** oppure usare **Banner in primo piano**. Se si seleziona **Non in primo piano**, l'app non sarà elencata.
6. Se si seleziona Banner in evidenza, specificare i seguenti dettagli:
   1. **Titolo** - Specificare il titolo dell'applicazione
   2. **Descrizione** - Specificare i dettagli dell'applicazione
   3. **Stile banner** - Selezionare un colore per il banner
7. Fare clic su **+ Aggiungi descrizione** per immettere una breve descrizione della configurazione.
8. Facoltativamente, modificare la distribuzione della configurazione.
9. Fare clic su **Fine** per salvare la configurazione dell'app.

Configurazione delle regole di traffico di AppTunnel

Utilizzare la configurazione AppTunnel per definire le regole di traffico e consentire l'accesso ai servizi tramite Sentry:

Per informazioni sull'aggiunta di una configurazione AppTunnel, vedere "Adding an AppTunnel configuration" (Aggiunta di una configurazione AppTunnel) in *AppConnect Guide for Ivanti Neurons for MDM* (Guida di AppConnect per Ivanti Neurons for MDM).

Configurazione dell'app gestita

Procedura

1. Fare clic sull'icona **+** per aprire la pagina di configurazione.
2. Fare clic su **+ Aggiungi descrizione** per immettere una breve descrizione della configurazione.
3. Fare clic su **+ Aggiungi** per immettere una chiave e un valore.
4. Scegliere un livello di distribuzione.
5. Fare clic su **Avanti**.

Configurazione di una VPN per ciascuna app mediante VPN per-app

Procedura

1. Fare clic sull'icona **+** per aprire la pagina di configurazione.
2. Immettere un nome per la VPN di questa app nel campo **Nome**.
3. Fare clic su **+ Aggiungi descrizione** per immettere una breve descrizione della configurazione.
4. Fare clic sull'opzione **Abilita VPN per-app per questa app** e selezionare una configurazione disponibile di VPN per-app.
5. (Facoltativo) Per le app macOS, digitare la stringa **Requisito designato** nel formato, identificatore "\%s\". Ad esempio, l'identificatore "com.google.Chrome". Utilizzare questo campo per consentire a un'app macOS con più pacchetti di utilizzare una VPN per-app come Tunnel.
6. Scegliere la modalità di **distribuzione della configurazione app**.
7. Fare clic su **Avanti**.

Uso della configurazione dell'app gestita Apple

Utilizzando la configurazione dell'app gestita Apple, impostazioni specifiche possono essere configurate per l'app gestita installata. Un'applicazione potrebbe avere alcuni dei parametri di configurazione implementati o ristretti dallo sviluppatore. Per applicazioni con tali restrizioni le opzioni di configurazione disponibili potrebbero essere limitate. È possibile configurare le app gestite da Apple.

Procedura

1. Andare in **App > Catalogo app**.
2. Selezionare un'app.
3. Fare clic sulla scheda **Configurazioni app**.
4. Fare clic su **Configurazione app gestita Apple** oppure sul pulsante **+**.
   Nella configurazione dell'app gestita Apple esistono già impostazioni di configurazione predefinite.
5. Fare clic su **Aggiungi** per aggiungere un'altra configurazione, se necessario. In alternativa, fare clic sul nome della configurazione per modificare la configurazione.
6. In **Origine configurazione** selezionare una delle opzioni in **Tipo origine**

- **AppConfig Community** - Questa opzione è disponibile solo per le app che dispongono di una specifica di configurazione app nel community repository. Se questa opzione è disponibile, viene selezionata per impostazione predefinita.
- **Usa specifica .xml** - Selezionare questa opzione per caricare lo schema dell'app per inviare una particolare versione di configurazione dell'app. Fare clic su **Scegli file** per caricare il file .xml. Assicurarsi che il file .xml contenga l'ID bundle e la versione. Un messaggio di errore viene visualizzato se l'ID bundle nel file non corrisponde all'ID bundle dell'app.

- **Nessuno** - Selezionare questa opzione se non si desidera applicare uno schema per l'app. Questa opzione è selezionata per impostazione predefinita se l'opzione **AppConfig Community** non è disponibile.
  Il file .xml caricato viene visualizzato nella sezione **Origine configurazione**. Fare clic sull'icona Elimina per eliminare il file .xml caricato.

7. In **Impostazioni app gestite Apple**, è possibile impostare le opzioni di configurazione per inserire coppie chiave-valore.

- Fare clic su **Aggiungi** per aggiungere le seguenti coppie chiave-valore alla configurazione dell'app gestita per consentire al client Go di recuperare le informazioni sul nome della registrazione durante l'esecuzione di iReg o della procedura Apple per la registrazione dei dispositivi.
  È possibile selezionare i tipi di dati (stringa, intero, booleano, long float, doppio, data, array stringa, array intero, array doppio, array float, array long) per le coppie valore-chiave.

Aggiungere le seguenti coppie chiave-valore alla configurazione dell'app gestita per consentire al client Go di recuperare le informazioni sul nome della registrazione durante l'esecuzione di iReg o della procedura Apple per la registrazione dei dispositivi.

Chiave	Valore	Tipo
registration.username	$	STRINGA
registration.token	$	STRING
registration.token.expirationSeconds	$	STRINGA
registration.url	$	STRINGA

Aggiungere le seguenti coppie chiave-valore alla configurazione dell'app gestita per consentire al mac agent (Mobile@Work) di recuperare le informazioni sul nome della registrazione durante l'esecuzione di iReg o della procedura Apple per la registrazione dei dispositivi:

Chiave	Valore	Tipo
Url registrazione client	$	STRINGA
Token	$	STRINGA
Scadenza token	$	STRINGA

Se l'utente finale termina l'applicazione Ivanti Go, fare clic su **Modifica** per impostare l'applicazione in uno dei seguenti modi:

Chiave	Valore	Tipo
Per visualizzare la notifica predefinita, utilizzare i seguenti valori:		
abilita notifica terminazione app	Vero/Falso O 1/0	Booleano O stringa
Per visualizzare una notifica predefinita, utilizzare i seguenti valori:		
messaggio notifica terminazione app	Notifica personalizzata	Stringa
abilita notifica terminazione app	Vero/Falso O 1/0	Booleano O stringa

- **Usa .plist**: i file .plist contengono più coppie chiave-valore per il caricamento in blocco. Fare clic su **Scegli file** per caricare il file .plist. I dati plist convalidati verranno visualizzati nella tabella **Impostazioni app gestite Apple**.

> I file plist con dizionari nidificati non sono validi.

8. Fare clic su **Aggiorna** per salvare le proprie voci.

Configurazione relay di rete

Per rendere il traffico di rete della propria app più privato e sicuro senza connettersi alla VPN. Per ulteriori informazioni, consultare Configurazione relay di rete.

1. Fare clic sull'**icona Relay di rete +** per aprire la pagina di configurazione.
2. Immettere un nome per il **Relay di rete** per questa app nel campo Nome.
3. Fare clic su + **Aggiungi descrizione** per immettere una breve descrizione della configurazione.
4. Fare clic su **Abilita relay di rete** per questa opzione app e selezionare una **Configurazione relay di rete** disponibile.
5. Scegliere la modalità di **distribuzione** della configurazione app.
6. Fare clic su **Avanti**.

Configurazione dello slicing 5G rete mobile

Il supporto dello slicing 5G rete mobile consente di assegnare le singole app gestite (per tutte le app iOS) a una slice di rete che può fornire funzionalità e caratteristiche di rete specifiche per ottimizzare l'esperienza dell'app. L'assegnazione avviene utilizzando il nuovo attributo app **CellularSliceUUID** nel comando di installazione dell'app MDM o nella configurazione dichiarativa dell'app. Il valore della stringa della slice di rete da inserire nella chiave deve essere fornito dal gestore telefonico di supporto.

> Lo slicing 5G di rete non verrà utilizzato se l'app specifica o l'intero dispositivo è configurato per utilizzare una VPN.

ProcedureProcedura

1. Accedere ad **App > Catalogo app > Configurazioni app > Slicing 5G rete mobile** e fare clic su **Aggiungi**.
2. Sotto la sezione **Impostazioni configurazione**, aggiornare i campi seguenti:
   - Nome
   - Selezionare l'opzione **Abilita slicing 5G di rete**
   - Scegliere il **DNN** o la **Categoria app** (a seconda del provider di rete).

3. Scegliere un livello di distribuzione per questa configurazione dell'app:
4. Fare clic su **Salva**.

Distribuzione dell'applicazione tramite la configurazione del Filtro contenuti web

È possibile utilizzare la configurazione del Filtro contenuti Web per distribuire un'applicazione invece di un server proxy DNS. Dopo aver creato la configurazione del Filtro contenuti Web, è possibile aggiungere la configurazione a un'applicazione per la distribuzione. Per ulteriori informazioni sulla configurazione del Filtro contenuti web, vedere **Filtro contenuto Web**.

Procedura

1. Andare in **App** > **Catalogo app**.
2. Selezionare un'app.
3. Fare clic su **Avanti**.
4. Selezionare l'opzione di delega e fare clic su **Avanti**.
5. Selezionare le opzioni di distribuzione e fare clic su **Avanti**.
6. Selezionare **Configurazione del Filtro contenuti Web** e fare clic sull'icona **+**.
7. Specificare il **Nome**.
8. Selezionare la casella di controllo **Abilita Filtro contenuti web per questa app**.
9. Selezionare il Filtro contenuti Web dal menu a discesa.
10. Scegliere un livello di distribuzione per questa configurazione dell'app:
    1. **A tutti**: l'app viene aggiunta su tutti i dispositivi compatibili degli utenti.
    2. **A nessuno**: l'app viene predisposta per essere distribuita in seguito.
    3. **Distribuzione personalizzata** - Selezionare una delle opzioni seguenti:
        - **Utenti/Gruppi di utenti** - L'app viene distribuita solamente agli utenti o ai gruppi di utenti selezionati.
          Fare clic sulla scheda **Utenti** per selezionare gli utenti.
          Fare clic sulla scheda **Gruppi di utenti** per selezionare i gruppi di utenti.
        - **Dispositivi/Gruppi di dispositivi** - L'app viene distribuita solamente ai dispositivi o ai gruppi di dispositivi selezionati.
          Fare clic sulla scheda **Dispositivi** per selezionare i dispositivi.
          Fare clic sulla scheda **Gruppi di dispositivi** per selezionare i gruppi di dispositivi.
11. Fare clic su **Avanti**.
12. Fare clic su **Fine**. L'app selezionata viene distribuita agli utenti specifici attraverso la configurazione del Filtro contenuti Web.

Distribuzione dell'applicazione tramite proxy DNS

È possibile utilizzare la configurazione del Proxy DNS per distribuire un'applicazione. Dopo aver creato la configurazione del Proxy DNS, è possibile aggiungere la configurazione a un'applicazione per la distribuzione. Per ulteriori informazioni sulla configurazione del proxy DNS, vedere **Creazione della configurazione del proxy DNS**.

Procedura

1. Andare in **App** > **Catalogo app**.
2. Selezionare un'app.
3. Fare clic su **Avanti**.

4. Selezionare l'opzione di delega e fare clic su **Avanti**.
5. Selezionare le opzioni di distribuzione e fare clic su **Avanti**.
6. Selezionare **Configurazione proxy DNS** e fare clic sull'icona **+**.
7. Specificare il **Nome**.
8. Selezionare la casella di controllo **Abilita DNS Proxy per questa app**.
9. Selezionare il proxy DNS dal menu a discesa.
10. Scegliere un livello di distribuzione per questa configurazione dell'app:
    1. **A tutti**: l'app viene aggiunta su tutti i dispositivi compatibili degli utenti.
    2. **A nessuno**: l'app viene predisposta per essere distribuita in seguito.
    3. **Distribuzione personalizzata** - Selezionare una delle opzioni seguenti:
        - **Utenti/Gruppi di utenti** - L'app viene distribuita solamente agli utenti o ai gruppi di utenti selezionati.
          Fare clic sulla scheda **Utenti** per selezionare gli utenti.
          Fare clic sulla scheda **Gruppi di utenti** per selezionare i gruppi di utenti.
        - **Dispositivi/Gruppi di dispositivi** - L'app viene distribuita solamente ai dispositivi o ai gruppi di dispositivi selezionati.
          Fare clic sulla scheda **Dispositivi** per selezionare i dispositivi.
          Fare clic sulla scheda **Gruppi di dispositivi** per selezionare i gruppi di dispositivi.
11. Fare clic su **Avanti**.
12. Fare clic su **Fine**. L'app selezionata viene distribuita agli utenti specifici attraverso la configurazione DNS Proxy.

Clonazione impostazioni configurazione app

È possibile clonare le impostazioni di configurazione di un'app gestita, in modo che le stesse impostazioni possano essere applicate su altri dispositivi. È possibile anche rinominare e introdurre alcune modifiche alle impostazioni clonate.

Android

È possibile clonare le impostazioni di configurazione sui dispositivi Android.

Procedura

1. Andare in **App > Catalogo app**.
2. Selezionare un'app da cui si desiderano clonare le impostazioni di configurazione.
3. Fare clic su **Configurazioni app**.
4. Sotto la sezione **Riepilogo configurazioni app**, si troverà l'elenco delle configurazioni (**Configurazioni gestite per Android**, **Installa su dispositivo**, **Promozione**, **Autorizzazioni dispositivo delegate**, e **Versione Google Play**) disponibili per dispositivi Android.
5. Fare clic su una qualsiasi delle configurazioni disponibili.
6. Sotto **Azioni**, fare clic su **Clona** per avviare la procedura di clonazione.
7. Per impostazione predefinita, il nome della configurazione clonata sarà <Copy of the Cloned Configuration name>. Tuttavia, è possibile modificare il nome inserendo un nome a propria scelta nella casella **Nome**.
8. (Opzionale) Inserire del testo sull'impostazione clonata nella casella **Descrizione**.
9. Fare clic su **Continua**.

Appare una finestra di conferma a indicare che la clonazione delle impostazioni di configurazione dell'app sono complete. È possibile visualizzare la versione clonata sotto il riepilogo Configurazioni app e all'interno dell'app clonata.

iOS

È possibile clonare le Impostazioni configurazione app gestite sui dispositivi iOS.

Procedura

1. Andare in **App > Catalogo app**.
2. Selezionare un'app da cui si desiderano clonare le impostazioni di configurazione.
3. Fare clic su **Configurazioni app**.
4. Sotto la sezione **Riepilogo configurazioni app** si troverà l'elenco delle configurazioni (**Installa sul dispositivo**, **Impostazioni app Apple**, **Promozione**, **Configurazione personalizzata AppConnect**, **Tunnel app**, **Configurazione app gestite da Apple** e **Per App VPN**) disponibili per i dispositivi iOS.
5. Fare clic sulla configurazione richiesta che si desidera clonare.
6. Sotto **Azioni**, fare clic su **Clona** per avviare la procedura di clonazione.
7. Per impostazione predefinita, il nome della configurazione clonata sarà <Copy of the Cloned Configuration name>. Tuttavia, è possibile modificare il nome inserendo un nome a propria scelta nella casella **Nome**.
8. (Opzionale) Inserire del testo sull'impostazione clonata nella casella **Descrizione**.
9. Selezionare un'origine di configurazione dall'elenco **Tipo origine** .
10. Sotto la sezione **Impostazioni app gestite da Apple**, inserire **Chiave**, **Valore** e selezionare **Tipo** dall'elenco.
    Per informazioni su **Chiave**, **Valore** e **Tipo**, vedere **Utilizzo della configurazione delle app gestite da Apple**.
11. Fare clic su **Continua**.
    Appare una finestra di conferma a indicare che la clonazione delle impostazioni di configurazione dell'app è stata completata. È possibile visualizzare la versione clonata nella sezione **Configurazione app gestite da Apple**.

Windows

È possibile clonare le impostazioni di configurazione app sui dispositivi Windows.

Procedura

1. Andare in **App > Catalogo app**.
2. Selezionare un'app da cui si desiderano clonare le impostazioni di configurazione.
3. Fare clic su **Configurazioni app**.
4. Sotto la sezione **Riepilogo configurazioni app** si troveranno le configurazioni **Installa sul dispositivo** e **Promozione**.
5. Fare clic sulla configurazione richiesta che si desidera clonare.
6. Sotto **Azioni**, fare clic su **Clona** per avviare la procedura di clonazione.
7. Per impostazione predefinita, il nome della configurazione clonata sarà <Copy of the Cloned Configuration name>. Tuttavia, è possibile modificare il nome inserendo un nome a propria scelta nella casella **Nome**.
8. (Opzionale) Inserire del testo sull'impostazione clonata nella casella **Descrizione**.
9. Fare clic su **Continua**.

Appare una finestra di conferma a indicare che la clonazione delle impostazioni di configurazione dell'app sono complete. È possibile visualizzare la versione clonata sotto il riepilogo Configurazioni app e all'interno dell'app clonata.

Scelta delle app di Windows 10 per il catalogo interno

Scegliere le app da aggiungere al catalogo delle app interne. Le app interne, Microsoft Store e Microsoft for Business sono supportate per Windows 10. Windows 10 applica la conformità direttamente sul dispositivo in base all'app che si sceglie di consentire o non consentire.

> Per impostazione predefinita, l'intervallo di check-in di Windows 10 è una volta ogni 60 minuti. È possibile eseguire un check-in forzato del dispositivo per ottenere un aggiornamento dello stato del dispositivo e dell'app.

Sono supportate le seguenti azioni:

- Caricamento di nuove app
- Installazione invisibile all'utente
- Installazione manuale da Apps@Work
- Aggiunta di una nuova versione dell'app
- Eliminazione di un'app

Sono supportati i seguenti formati:

- APPX
- APPXBUNDLE
- MSI Win32 con wrapper, app di Win32 preinstallata
- MSIX (supportato su RS5 oltre che sui dispositivi Windows 10)
- .EXE (usando il ponte)

> L'app **Ivanti Neurons Agent** è disponibile sul **Catalogo app** per dispositivi **Windows**. L'amministratore può distribuire l'app **Ivanti Neurons Agent** come app interna e questa app può essere distribuita di conseguenza sui dispositivi Windows.

Configurare le app di Windows 10

Procedura

1. Fare clic su **Dispositivi** sulla barra di navigazione principale.
2. Selezionare un dispositivo Windows 10 registrato in Ivanti Neurons for MDM.
3. Fare clic su **App > Catalogo app**.
4. Selezionare un'app.
5. Utilizzare il menu a discesa **Azioni** per aggiungere l'app o eliminarla dal catalogo.
   Facoltativamente, aggiungere una nuova versione dell'app.
   - Fare clic sul menu a discesa **Azioni**.
   - Selezionare **Aggiungi nuova versione**.
   - Andare al catalogo e selezionare una nuova versione dell'app.
   - Fare clic su **Aggiorna e salva** per visualizzare la schermata Informazioni sulle app.
6. Utilizzare il menu a discesa **Versione** per scegliere la versione da utilizzare.
7. Fare clic su **Modifica** per iniziare ad apportare modifiche ai dettagli.

- Se necessario, modificare la **categoria**.
- Se necessario, immettere una **descrizione**.
- Aggiungere gli screenshot, se necessario.

8. Fare clic su **Salva**.
9. Fare clic sulla scheda **Distribuzione** e su **Modifica** per iniziare ad apportare modifiche al livello di distribuzione.
10. Fare clic su **Salva**.
11. Fare clic sulla scheda **Configurazioni app** per visualizzare un riepilogo della configurazione corrente.
12. Immettere una descrizione dell'app, se necessario.
13. Fare clic su **Installa sul dispositivo** nella pagina di riepilogo Configurazioni app.
    Installazione invisibile all'utente è l'impostazione predefinita e non è possibile modificarla.
14. Fare clic su **Promozione** nella finestra di navigazione sinistra, quindi fare clic sulle **impostazioni di configurazione per la distribuzione della promozione** per cambiare il livello di promozione.
    - Fare clic su **Modifica** per iniziare ad apportare modifiche alle impostazioni del livello di promozione.
    - Immettere un nome per la configurazione.
    - Immettere una descrizione per la configurazione.
    - Selezionare un livello di promozione.
    - Fare clic su **Aggiorna** per salvare le modifiche.
15. Fare clic sulla scheda **Recensioni** per visualizzare le informazioni sulle recensioni.
    Esportare i dati delle recensioni in un foglio di lavoro, se necessario.

Modifica delle impostazioni di configurazione delle app di Windows 10

Procedura

1. Fare clic su **Criteri > Configurazione**.
2. Fare clic su **+Aggiungi**.
3. Selezionare **Controllo dell'app di Windows** per visualizzare la schermata **Crea configurazione di controllo delle app di Windows**.
4. Immettere un **Nome** e una **Descrizione** per la configurazione.
5. Definire il tipo di app come:
    - Consentite (elenco delle app consentite): sono consentite solo le app incluse nell'elenco. Queste app vengono installate in modo invisibile, se non sono già presenti sul dispositivo.
    - Non consentite (elenco delle app non consentite): se queste app sono presenti nel dispositivo, in caso di avvio vengono bloccate.
6. Specificare le definizioni delle regole per il tipo di app e l'identificatore dell'app.
7. Fare clic su **App di ricerca** per visualizzare la schermata **Cerca app di Windows 10**.
8. Immettere il nome dell'app da cercare nel Windows Store.
9. Selezionare l'app dalle opzioni visualizzate per aggiungerla all'Identificatore app.
10. Facoltativamente, utilizzare il menu a discesa Tipo di app per impostare un percorso nell'Identificatore app per consentire o non consentire le app utilizzando il percorso specificato o bloccare tutte le app installate nel percorso specifico.
    Tipo app **Publisher/PFN Equals** si applica ai dispositivi Windows 10+ e supporta PFN. **EXE/Win32 Equals**.

11. Fare clic su **Avanti**.
12. Selezionare un livello di distribuzione.
    - **Tutti i dispositivi**.
    - **Nessun dispositivo**.
    - **Personalizzato** - immettere gli utenti o i gruppi che ricevono l'app.
13. Fare clic su **Fine**.
14. È possibile modificare le definizioni delle regole per selezionare un tipo di app e specificare un Identificatore app.
    - Fare clic sul menu a discesa **Azioni**.
    - Selezionare **Aggiungi nuova versione**.
    - Selezionare una nuova versione dell'app.
    - Fare clic su **Aggiorna e salva** per visualizzare la schermata **Informazioni sulle app**.

Configurazione dell'opzione Riavvia il dispositivo dopo l'installazione per Windows

È possibile configurare un dispositivo per il riavvio dopo un'installazione app usando l'opzione **Riavvia il dispositivo dopo l'installazione**.

Procedura

1. Andare in **App > Catalogo app**.
2. Selezionare qualsiasi app specifica di Windows dall'elenco.
3. Passare a **Configurazioni app > Installa sul dispositivo > Impostazioni di configurazione Installa applicazione**.
4. Fare clic su **Modifica** e impostare l'opzione su **Riavvia il dispositivo dopo l'installazione** su ON.
5. Selezionare una delle seguenti opzioni di pianificazione per il riavvio del dispositivo:

Impostazione	Operazione da eseguire
Subito dopo l'installazione	Selezionare questa opzione per riavviare il dispositivo subito dopo l'installazione dell'applicazione.
In un momento specifico della giornata	Selezionare questa opzione per riavviare il dispositivo in un orario specifico subito dopo l'installazione dell'applicazione.
Dopo pochi minuti	Selezionare questa opzione per riavviare il dispositivo dopo **15**, **30**, **60** o **120** minuti dall'installazione dell'applicazione.

6. Fare clic su **Aggiorna**.

Il dispositivo verrà riavviato all'orario pianificato.

> In caso di app pubbliche e app di Microsoft Store for Business (MSB), attivare l'impostazione **Installazione invisibile sui dispositivi Windows** dalla sezione **Configurazioni app**.

Installazione di app tramite Apps@Work

Per installare un'app tramite Apps@Work:

1. Fare clic sull'app **Apps@Work**.
   Nella casella di dialogo per l'accesso di Apps@Work, sono già inseriti l'indirizzo e-mail e l'URL del server dell'amministratore.
2. Immettere la password e fare clic su Accedi per visualizzare la pagina delle app.
3. Selezionare un'app da installare. Non è possibile installare app con dipendenze da app prerequisito, se queste ultime non sono già installate nel client.
   Nel caso di Apps@Work per dispositivi iOS, è facoltativamente possibile fare clic sul pulsante **Installa tutto** per installare tutte le app. Questa opzione è disponibile nelle schermate **Nuove versioni**, **App in primo piano** e **Categorie**.

> Le app App e libri non vengono installate se precedentemente non è stata accettata la licenza App e libri.

4. Fare clic su **Aggiorna e salva** per visualizzare la schermata **Informazioni sulle app**.

Installazione e aggiornamenti delle app per i dispositivi aziendali Android

Gli amministratori possono pubblicare un'app nel catalogo per l'accesso generale e contemporaneamente distribuirla su un dispositivo specifico per l'uso immediato. In questo modo gli utenti possono ricevere direttamente l'app, mentre questa rimane disponibile nel catalogo per essere installata da altri, se necessario.

Per installare app e aggiornamenti

1. Navigare in **App > App Catalog**.
2. Scegliere l'app desiderata.
3. Fare clic su **Azioni** nella schermata **Dettagli**. Viene visualizzato **Invia richiesta di installazione/aggiornamento**.
4. Fare clic su Invia richiesta di installazione/aggiornamento. Viene visualizzata la finestra di dialogo **Invia richiesta di installazione/aggiornamento**.
5. Eseguire quanto segue in **Invia notifiche di installazione e aggiornamento a dispositivi per questa applicazione**:
   - Selezionare la casella di controllo **Invia richiesta di nuova applicazione (si applica ai dispositivi che non hanno ancora installato l'applicazione)** per installare la nuova applicazione.
   - Selezionare la casella di controllo **Invia richiesta di aggiornamenti (si applica ai dispositivi che hanno installato l'app ma è disponibile un aggiornamento)** per aggiornare un'applicazione installata.
6. Eseguire quanto segue in **Selezionare gli utenti a cui inviare la richiesta**:
   - Fare clic su **Tutti** per distribuire la configurazione a tutti gli utenti compatibili. L'app viene visualizzata nel relativo App Catalog.
   - Fare clic su **Personalizzato** per definire il gruppo di utenti o l'utente che vede l'applicazione nell'App Catalog.

     > La distribuzione **Invia richiesta di installazione/aggiornamento** fa parte del processo di distribuzione app. Le impostazioni scelte nella schermata **Distribuzione** decidono quali dispositivi riceveranno l'app.

Viene visualizzata una finestra di conferma che indica che l'installazione dell'app è stata completata.

Le modifiche apportate da nuove installazioni o aggiornamenti sono mostrate in **Dashboard** > **Audit Trails**.

> Per le app pubbliche e private **Invia richiesta di aggiornamenti (si applica ai dispositivi che hanno installato l'app ma è disponibile un aggiornamento)** è disattivato. Sono consentite solo le richieste **Invia richiesta per nuova applicazione**.

Argomenti correlati:

Cancellazione della cache delle app per dispositivi Android Enterprise

La **richiesta Cancella cache app** consente all'amministratore di cancellare in remoto i dati memorizzati nella cache per un'applicazione selezionata installata su dispositivi Android Enterprise utilizzando Ivanti Neurons per MDM. Questa azione aiuta a risolvere i problemi comuni delle app, come prestazioni lente, errori imprevisti o dati temporanei obsoleti, senza disinstallare o reinstallare l'app. La richiesta cancella solo la cache dell'app e conserva i dati utente, le impostazioni delle app e le configurazioni. Gli amministratori utilizzano questa funzione per ripristinare rapidamente il normale comportamento delle app, riducendo al minimo le interruzioni per gli utenti finali.

Procedura

1. Navigare in **App** > **App Catalog**.
2. Selezionare e aprire l'app.
   Viene visualizzata la pagina **Dettagli** app.
3. Fare clic sul menu delle azioni (⋮) nella pagina **Dettagli** app.
4. Selezionare l'opzione **richiesta Cancella cache app**.
   Viene visualizzato il riquadro **richiesta Cancella cache app**.
5. Eseguire una delle seguenti azioni nella sezione **Seleziona utenti per invio richiesta** per la distribuzione della richiesta di cancellazione della cache delle app:
   - Selezionare **Tutti** per inviare la richiesta a tutti i dispositivi compatibili con l'app installata.
   - Selezionare **Personalizzato** per inviare la richiesta a utenti, gruppi di utenti, dispositivi o gruppi di dispositivi specifici.
6. (Facoltativo) Cercare un elenco di distribuzione esistente in **Altre opzioni filtro di distribuzione**.
7. (Facoltativo) Selezionare **+ Aggiungi filtro di distribuzione** per creare un filtro di distribuzione nel riquadro **Crea filtro di distribuzione**.

> Utilizzare questa opzione per inviare la **richiesta Cancella cache app** a un set specifico di dispositivi, come i dispositivi in modalità DO o EPO.

8. Fare clic su **Invia**.
9. Fare clic su **OK** nella finestra di dialogo **Cancella cache app**.
   Ivanti Neurons per MDM visualizza una notifica che elenca il numero di dispositivi che hanno ricevuto la **richiesta Cancella cache app**.

> Dopo aver completato la richiesta **Cancella cache app**, tutti i dettagli dell'app (versione, nome, platformAppId, displayVersion e bundleVersion) vengono registrati nella pagina **Audit Trail**.

8.8. Assegnazione di attributi personalizzati alle app

Dopo aver creato attributi personalizzati, è possibile assegnarli a una o più applicazioni. Ciascun attributo dispone di un valore che è possibile utilizzare per attività quali la creazione di gruppi di applicazioni. Per ulteriori informazioni sulla gestione degli attributi, vedere Attributi.

Creare e assegnare un attributo personalizzato per una singola applicazione

È possibile assegnare un attributo personalizzato a una singola applicazione.

Procedura

1. Accedere al Portale amministrativo.
2. Navigare in **App** > **Catalogo app**.
3. Selezionare un'applicazione e fare clic su **Attributi**.
4. Fare clic su **+Aggiungi nuovo** e selezionare un valore dal menu a discesa **Nome attributo**.
5. Specificare il valore attributo nel campo **Valore**.
6. Fare clic su **Salva**. L'attributo personalizzato viene aggiunto all'applicazione.

Assegnare un attributo personalizzato a più applicazioni

È possibile assegnare attributi personalizzati a una o più applicazioni. Quando si selezionano più applicazioni, l'attributo personalizzato viene applicato a tutte le versioni dell'applicazione. È possibile selezionare un'applicazione specifica, andare alla scheda Attributi e modificare i dettagli dell'attributo personalizzato per una versione specifica dell'applicazione.

Procedura

1. Accedere al Portale amministrativo.
2. Navigare in **App** > **Catalogo app**.
3. Selezionare le caselle di controllo per una o più applicazioni.
4. Fare clic su **Azioni**.
5. Selezionare **Assegna attributi personalizzati**. Appare la procedura guidata Assegna attributi personalizzati alle app.
6. Selezionare *una* delle seguenti opzioni:
   - Consente di forzare l'assegnazione (la sovrascrittura) di tutti gli attributi, anche in presenza di valori esistenti.
   - Consente di sovrascrivere solo se il valore è vuoto e di ignorare gli attributi con valori esistenti.
7. Selezionare le caselle di controllo per uno o più attributi.
8. Specificare il valore nei campi Valore (non sono ammessi valori vuoti).
9. Fare clic su **Assegna**. L'attributo personalizzato viene assegnato a tutte le versioni delle applicazioni selezionate.
10. (Facoltativo) Se si desidera modificare l'attributo personalizzato per una singola versione dell'applicazione, selezionare la versione dell'applicazione dal menu a discesa Versione e fare clic su Modifica.

> Gli **Attributi app personalizzati** con i loro valori possono essere utilizzati per creare report e per l'esportazione in formato CSV dalla pagina **Dettagli dispositivo**.

8.9. Configurazioni gestite per Android

Argomenti della sezione:

- Utilizzo delle configurazioni gestite di Android Enterprise
- Limitazioni e autorizzazioni app per app in-house
- Configurazione di Gmail con Android Enterprise

Se Ivanti Neurons per MDM è abilitato per Android Enterprise, allora la configurazione Android Enterprise è disponibile per l'uso per app.

Utilizzo delle configurazioni gestite di Android Enterprise

1. Fare clic su **Applicazioni**.
2. Fare clic su **Catalogo app**.
3. Selezionare un'app per cui impostare la configurazione di Android Enterprise.
4. Fare clic su **Configurazioni app**.
5. Fare clic su **Configurazioni gestite per Android**.
6. Fornire un nome per la configurazione.
7. È possibile aggiungere facoltativamente una descrizione.
8. Utilizzare i campi Configurazioni gestite per configurare i comportamenti delle configurazioni gestite:
9. Utilizzare le **Impostazioni di configurazione Tunnel** per integrare l'app Tunnel direttamente con l'app Ivanti Go per dispositivi Android. Selezionare l'opzione **Abilita configurazione Tunnel** per applicare questa impostazione. Grazie a questo miglioramento, gli amministratori possono attivare le funzionalità Tunnel tramite Ivanti Go e configurare la connettività sicura utilizzando le configurazioni Tunnel esistenti. La funzione è disponibile per i dispositivi Android appena registrati. Per garantire una transizione senza interruzioni, l'app Tunnel autonoma continua a essere supportata. Tuttavia, i dispositivi con l'app Tunnel autonoma installata non visualizzeranno l'esperienza Tunnel integrata in Ivanti Go. Dopo aver app rimosso l'app Tunnel autonoma, la funzionalità Tunnel integrata diventa disponibile all'interno dell'app Go. È possibile applicare una sola configurazione Tunnel a un dispositivo alla volta.

Impostazione	Descrizione
Impedisce la condivisione dei widget sui profili da parte delle app	Attivare l'opzione per bloccare le app e consentire la condivisione di widget tra i profili solo se l'app non viene installata in modo invisibile. Lasciare questa impostazione disattivata per consentire alle app attendibili distribuite nel profilo di Android Enterprise di mostrare i widget nella schermata principale in modo che gli utenti possano visualizzare le informazioni senza eseguire l'accesso.
Impedisce all'utente di disinstallare l'app	Consente di impedire all'utente di disinstallare l'app (pubblica, privata o in-house) dopo che Ivanti Neurons for MDM l'ha installata in modo invisibile.
Codice versione minima	Impostare un codice della versione minima richiesta perché l'app possa sovrascrivere il comportamento di aggiornamento predefinito. Se il codice della versione dell'app attualmente installata sul dispositivo è inferiore al codice della versione minima specificata, allora l'app viene aggiornata immediatamente alla versione più recente.
Avvio automatico all'installazione	Selezionare questa opzione se si desidera avviare un'app automaticamente dopo l'installazione. Questa funzionalità è disponibile solamente se l'app è appena stata installata nel dispositivo e non costituisce un aggiornamento a una nuova versione. In caso di dispositivi Profilo di lavoro e Profilo di lavoro di proprietà dell'azienda, l'app Go deve essere attiva e in primo piano. A causa delle limitazioni su Android 10+, se l'utente distribuisce più app a dispositivi Profilo di lavoro e Profilo di lavoro di proprietà dell'azienda, solo un'app viene avviata automaticamente.

10. L'amministratore può controllare i campi di configurazione dell'app che possono essere inviati ai dispositivi o che non devono essere inviati. In generale, i valori predefiniti vengono impostati quando si inviano le configurazioni a diversi dispositivi. Sotto la sezione Configurazioni gestite, all'interno dell'impostazione **Esegui il push al dispositivo**, selezionare **Esegui il push di tutte le impostazioni** o **Solo le impostazioni push con i valori definiti**.

Configurazioni gestite

Ogni configurazione dell'app Android Enterprise mostra il pulsante abilitato per il certificato per ciascun campo di testo e, quando si fa clic su di esso, il campo di testo viene sostituito da un elenco a discesa di certificati. Quando sono configurati, questi certificati vengono applicati in modo invisibile senza alcuna interazione da parte dell'utente.

Un campo abilitato per il certificato esistente può essere cambiato in abilitato per il testo facendo clic sullo stesso pulsante accanto al campo. Un campo abilitato per il testo modificato in campo abilitato per il certificato può essere cambiato nuovamente in campo abilitato per il testo facendo clic sullo stesso pulsante. (I campi a discesa predefiniti non può essere cambiati di nuovo in campi abilitati per il testo).

> Se nel tenant non sono configurati certificati ID, quando si passa dal testo all'elenco a discesa utilizzando il pulsante abilitato per il certificato, viene mostrata solo l'opzione "Nessuno" nell'elenco a discesa.

Fare clic su **Gestisci autorizzazioni** per selezionare e configurare le autorizzazioni di runtime per le applicazioni aventi come target le API 23 o versioni successive e Android 6.0 o versioni successive.

Solo le autorizzazioni pericolose valide per l'applicazione specifica sono elencate per la selezione. L'elenco completo di autorizzazioni pericolose (quali la lettura dei contatti, la ricerca degli account sul dispositivo, la scrittura nel registro delle chiamate, ecc.) è reperibile al seguente indirizzo **https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups.**

11. Tra i diritti da assegnare a ciascuna autorizzazione sono inclusi:
    - La autorizzazioni vengono applicate solo quando l'applicazione le richiede.
    - Le autorizzazioni non vengono applicate se gli utenti hanno in precedenza accettato o negato le autorizzazioni.
    - Concedi automaticamente
    - Nega automaticamente. Utilizzare questa impostazione con cautela.
    - Predefinite/Globali

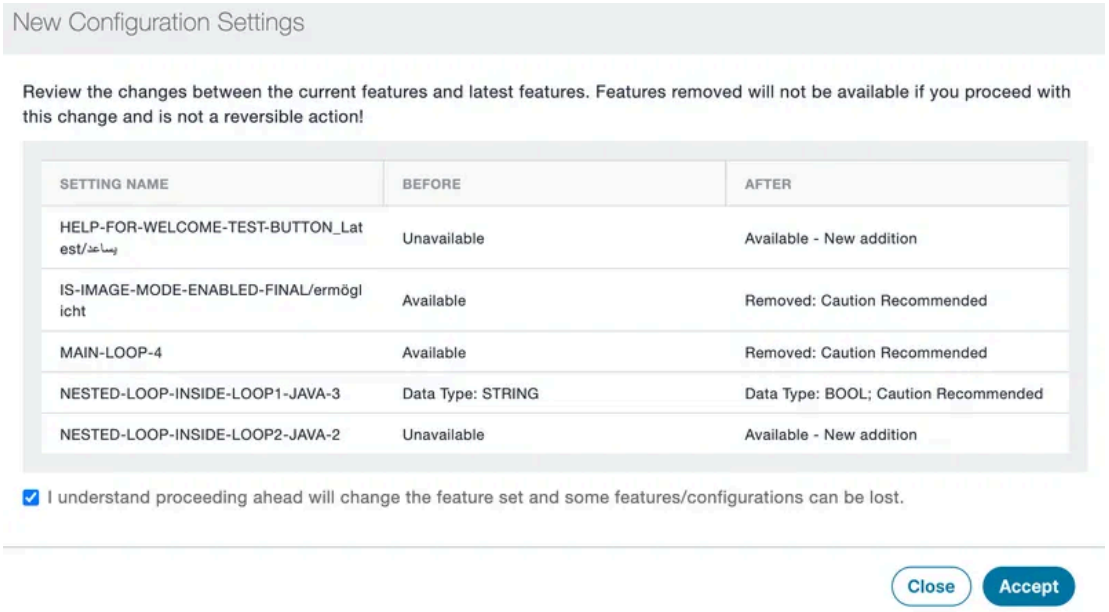
Configurare le opzioni di distribuzione, scegliendo tra **Tutti gli utenti con app**, **Nessuno** o **Personalizzata**.

12. Fare clic su **Salva**.

Nuove impostazioni di configurazione

Quando una versione dell'app viene aggiornata e se ci sono modifiche alle configurazioni esistenti, il pulsante **Aggiorna alle funzionalità più recenti** appare dopo la modifica della pagina Dettagli configurazione.

1. Fare clic su **Aggiorna a ultime funzionalità**.
   Sullo schermo appare un messaggio di avviso che indica che il passaggio alle funzioni più recenti impedirà agli utenti di accedere alle versioni precedenti dell'applicazione. Il messaggio di avviso consiglia di adottare le misure necessarie per integrare l'ultima versione dell'applicazione senza problemi.
2. Fare clic su **Avanti**.
3. A schermo appare la pagina **Nuove impostazioni di configurazione**.



La finestra **Nuove impostazioni di configurazione** elenca le diverse impostazioni esistenti nella configurazione e lo stato di ciascuna impostazione dopo l'aggiornamento. La finestra Nuove impostazioni di configurazione elenca tutte le restrizioni del database e lo schema di Google riporta il seguente stato:

- Aggiunto
- Rimosso
- Modificato

Selezionare la casella di controllo e fare clic su **Accetta** per procedere con l'aggiornamento.
Sullo schermo appare un messaggio di conferma che indica che la configurazione è stata aggiornata con le ultime caratteristiche. A questo punto è possibile distribuire e salvare le configurazioni per rendere effettive le modifiche.

Limitazioni e autorizzazioni app per app in-house

L'amministratore può impostare alcune restrizioni sulle app e limitare o concedere le autorizzazioni per le app interne. Questa funzionalità era disponibile solo per le app pubbliche. Ma questa funzionalità è stata ora estesa alle app interne.

> L'amministratore deve ricaricare le applicazioni In-house per avere le funzionalità **Limitazioni app** e **Autorizzazioni** disponibili sulle relative app. Si consiglia di eliminare l'app esistente prima di caricare una nuova versione.

Procedura

1. Andare in **App** > **Catalogo app**.
2. Selezionare un'app **In-house** dall'elenco.
3. Fare clic su **Configurazioni app**.
4. Fare clic su **Configurazioni gestite per Android**.
5. Fare clic su **Aggiungi**.
6. La sezione **Limitazioni app** appare a schermo.
   Immettere i valori richiesti per le restrizioni disponibili.
7. Selezionare **Gestisci autorizzazioni**.
8. La finestra **Seleziona autorizzazioni** appare a schermo.
   Selezionare le autorizzazioni richieste dall'elenco e quindi fare clic su **Seleziona**.
9. Sotto la sezione **Autorizzazioni di runtime**, impostare i valori per le autorizzazioni selezionate.
10. Sotto la sezione **Distribuisci configurazione di questa app**, selezionare una delle seguenti opzioni di **distribuzione app**:
    - **Tutti gli utenti con app**
    - **Nessuno**
    - **Personalizzato**
11. Fare clic su **Salva**.
    Le restrizioni e le autorizzazioni selezionate saranno applicate alle app interne.

Configurazione di Gmail con Android Enterprise

È possibile distribuire Gmail su dispositivi Android Enterprise solo se Ivanti Neurons for MDM è stato configurato per Android Enterprise. Per configurare Gmail con Android Enterprise

1. Andare in **App > Catalogo app**.
2. Selezionare l'app Gmail per cui impostare la configurazione di Android Enterprise. Viene visualizzata la sezione Impostazioni configurazione.
3. Fornire un nome per la configurazione.
4. È possibile aggiungere facoltativamente una descrizione.
5. Utilizzare i campi **Configurazioni gestite** per configurare i comportamenti delle configurazioni gestite:

Le opzioni **Espandi tutto** e **Comprimi tutto** sono disponibili solo per le limitazioni nidificate o gerarchiche.

Impostazione	Descrizione
Esegui push al dispositivo	Esegui push a tutte le impostazioni - Selezionare questa opzione per abilitare tutti i selettori, inclusi quelli senza alcun valore Eseguire solo il push delle impostazioni con valori definiti - Selezionare questa opzione per abilitare tutti i selettori con valori definiti e disabilitare i selettori per le impostazioni senza valori In molti casi, le impostazioni predefinite sono già disponibili. Tuttavia, l'amministratore può selezionare le impostazioni di configurazione dell'app necessarie o modificare le variabili che devono essere inviate ai dispositivi.
Indirizzo e-mail	Inserire variabili di sostituzione per definire l'indirizzo e-mail. In genere, si immette $emailaddress$. Le soluzioni UEM possono utilizzare questo campo per eseguire il pull delle credenziali dell'utente da Active Directory.
Nome host o host	Immettere il nome host per il server Active Sync, come ad esempio hostname.company.com:443/path.
Nome utente	Utilizzare la variabile per il nome utente Active Directory dell'utente, che può essere specificato come un nome utente diretto (paolorossi) o come valore basato su modello ($username$).
Tipi di autenticazione	Selezionare l'elenco di stringhe contenenti i tipi di autenticazione consentiti.
Richiesto SSL	Quando questa opzione è selezionata, permette e richiede il parametro SSL sui numeri di porta utilizzati con il nome host.
Considera attendibili tutti i certificati	Selezionare solo se si desidera che i certificati non attendibili vengano automaticamente accettati dall'app. Utilizzare questa opzione solo per attività di debug o sviluppo quando si lavora in un ambiente di test.
Alias certificato di accesso	Inserire l'alias del certificato di accesso utilizzato per l'autenticazione nei server ActiveSync.
Consenti gli account non gestiti	Selezionare questa opzione per consentire agli utenti di aggiungere o rimuovere qualsiasi account di Exchange diverso dall'account specificato in questa configurazione gestita.
Firma e-mail predefinita	Inserire la stringa che comprende la firma di posta elettronica predefinita da aggiungere in fondo al testo di tutti i messaggi di e-mail in uscita.
Finestra di sincronizzazione predefinita	Inserire un valore da 0 a 5 che rappresenta la finestra temporale per la sincronizzazione con EAS (Exchange Active Sync).

Fare clic su **Avanti**.

7. Configurare le opzioni di distribuzione, scegliendo tra **Tutti gli utenti con app**, **Nessuno** o **Personalizzata**.
8. Fare clic su **Salva**.

8.10. Gestione delle app Google Play

È possibile definire quale file binario dell'app Google Play deve essere distribuito a gruppi o utente specifici. Questo deployment è applicabile ai deployment di Android Enterprise. Lo sviluppatore di app deve anche consentire all'organizzazione di poter distribuire le app dei canali Alfa o Beta.

1. Fare clic su **Applicazioni**.
2. In **App Catalog** selezionare un'app per cui impostare la configurazione della versione di Google Play.
3. Fare clic sulla scheda **Configurazioni delle app**.
4. Fare clic su **Versione di Google Play**.

> La configurazione della versione di Google viene applicata solo per le app di Android Enterprise. Per impostazione predefinita viene applicata l'opzione Produzione se la configurazione della versione di Google non è selezionata per le app aggiunte di recente.

Fare clic su **Aggiungi**.

6. Fornire un nome per la configurazione.
7. È possibile aggiungere facoltativamente una descrizione.
8. Selezionare un'opzione dall'elenco a discesa per scegliere il file binario da rendere disponibile agli utenti e ai dispositivi che ricevono l'app. Sono disponibili le seguenti opzioni:
   - Produzione
   - Alpha
   - Beta

   > L'opzione Produzione viene applicata per impostazione predefinita per le app che sono già state inviate al dispositivo.
9. Configurare le opzioni di distribuzione, scegliendo tra **Tutti gli utenti con app**, **Nessuno** o **Personalizzata**.
10. L'opzione **Personalizzato** consente di distribuire l'app all'interno del gruppo di utenti con filtro di dispositivo.
    Fare clic su **Salva**.

Assegnazione di priorità per più configurazioni della versione

Se vengono aggiunte più configurazioni della versione di Google, è possibile stabilire l'ordine di priorità per l'applicazione delle configurazioni.

1. In **Configurazioni delle app**, fare clic su **Definisci priorità configurazioni**.

> Il pulsante viene mostrato solo se sono elencate più configurazioni

Dall'elenco di configurazioni, trascinare e rilasciare in cima all'elenco la configurazione da applicare con priorità.

3. Fare clic su **Aggiorna**.

Se viene cancellata la prima configurazione a cui era stata assegnata la priorità, la configurazione successiva nell'elenco diventa prioritaria.

8.11. Rimozione di app dal Catalogo app

È possibile eliminare app pubbliche e in-house dal Catalogo app. Non è possibile eliminare le app prerequisito. Prima di eliminare tali app è necessario modificare le app per rimuovere le relazioni relative al prerequisito. Se l'app è installata sui dispositivi, verrà rimossa al successivo check-in di tali dispositivi. L'installazione/disinstallazione invisibile delle app è supportata sui dispositivi Samsung e Zebra in modalità Amministratore dispositivo o su tutti i dispositivi in modalità Proprietario dispositivo.

Nel caso di applicazioni interne, a schermo appare una finestra di conferma. È necessario selezionare la conferma di voler proseguire con l'operazione Elimina e fare clic su **Elimina app**. Quando si tenta di eliminare più app e alcune non possono essere eliminate, sullo schermo appare una finestra contenente informazioni sulle app che non possono essere eliminate e il motivo.

Le seguenti condizioni si applicano quando si cerca di eliminare una o più app dal Catalogo app:

- Se non è possibile eliminare una versione dell'app interna, non è possibile eliminare alcuna versione.
- Se una versione dell'app interna è un'app prerequisito, l'app non può essere eliminata e nessuna delle versioni può essere eliminata.
- Quando si selezionano tutte o alcune delle app interne per eliminarle dal Catalogo app, tutte le versioni delle app interne selezionate vengono eliminate.
- Non è possibile eliminare un'app interna delegata da uno Spazio.

Procedura

1. Andare in **App > Catalogo app**.
2. Fare clic sul collegamento relativo all'app.
3. Selezionare **Azioni > Elimina dal catalogo**.
4. Leggere l'avviso in cui vengono illustrate le conseguenze dell'eliminazione di un'app.
5. Nell'avviso viene indicata l'ulteriore eliminazione delle licenze App e libri (iOS) e delle recensioni sulle app (tutti i sistemi operativi).
   Selezionare la casella di controllo "Sono consapevole delle conseguenze dell'eliminazione di un'app" per procedere con l'operazione di eliminazione.
6. Fare clic su **Elimina app**.

8.12. Aggiornamento di app interne

Utilizzare la seguente procedura per aggiornare un'app interna:

1. Andare in **App > Catalogo app**.
2. Selezionare l'app da aggiornare.
3. Selezionare **Azioni > Aggiungi nuova versione**.
4. Trascinare e rilasciare l'app nell'area **Carica App** oppure fare clic su **Scegli file** per selezionarlo dal proprio file system.
5. Selezionare una delle opzioni riportate di seguito, a seconda di cosa si desidera fare con la versione precedente dell'app:
   - **Mantieni inalterate la descrizione, le schermate, la distribuzione, i prerequisiti delle app e le configurazioni delle app:** sostituisce la versione precedente nell'App Catalog.
   - **Modifica la descrizione, le schermate, la distribuzione, i prerequisiti delle app o le configurazioni delle app**: include entrambe le versioni nell'App Catalog.
6. In **Novità**, immettere del testo per illustrare agli utenti le differenze con la nuova versione.
7. Questo testo verrà visualizzato sul dispositivo quando l'utente seleziona l'app per istallarla.
   Se si sceglie di modificare le opzioni relative a descrizione, schermate o distribuzione, completare tali modifiche.
8. Fare clic su **Fine**.

Se si sceglie di mantenere le versioni precedenti dell'app nel catalogo, in **App > Catalogo app** verrà visualizzata soltanto una voce. Nel riquadro sulla sinistra viene riportato il numero di app per ciascuna voce. Se si decide in un secondo momento di eliminare la versione più recente, quella precedente la sostituirà automaticamente sui dispositivi installati.

Visualizzazione di un elenco di versioni dell'app

Gli amministratori possono caricare app con lo stesso numero di versione e architetture diverse.

ProcedureProcedura

1. Fare clic sul collegamento relativo all'app in **App > App Catalog**.
2. Fare clic sulla scheda **Versione**.
   Se nel catalogo sono presenti più versioni dell'app, queste ultime verranno visualizzate in un menu a discesa. Se vengono caricate più app con lo stesso numero di versione e architetture diverse, il menu a discesa mostra informazioni dettagliate sulle architetture supportate. Le architetture supportate per le app sono visualizzate anche in **Informazioni app**.

8.13. Ricerca del nome del pacchetto per le applicazioni Android

Per le app pubbliche disponibili su Google Play Store, procedere come segue::

1. Utilizzare un browser web per individuare l'app nel Google Play Store.
2. Selezionare l'app.
3. Esaminare l'URL visualizzato nel browser.

Il nome del pacchetto è incluso nell'URL dopo id= come mostrato di seguito:

https://play.google.com/store/apps/details?id=<package name>

Per app in-house e altri tipi di app non disponibili nel Play Store, provare a scaricare **Package Name Viewer** o altre app simili da Google Play Store.

8.14. Categorie

Argomenti della sezione:

- Aggiunta di una categoria
- Rimozione di una categoria

Le Categorie descrivono i tipi di app e consentono di organizzare le app quando gli utenti visualizzano il catalogo app. È necessario assegnare almeno una categoria a ciascuna app. Quando si inizia a utilizzare Ivanti Neurons for MDM, è disponibile un elenco delle categorie di app più comuni. Utilizzare questa pagina per gestire le categorie delle app.

Aggiunta di una categoria

È possibile aggiungere nuove categorie direttamente da qui o quando si aggiunge un'app al Catalogo app.

1. Fare clic su **Aggiungi** (in basso a sinistra)
2. Digitare il nome della categoria.
3. Le categorie non effettuano la distinzione tra caratteri maiuscoli e minuscoli, pertanto la dicitura MINE equivale a Mine. Fare clic su **Salva**.

Rimozione di una categoria

- Fare clic sulla X accanto alla categoria.

Se non è possibile eseguire le attività indicate nella pagina **Categorie app**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei ruoli seguenti:

- Gestione app e contenuti

8.15. Filtri di distribuzione

Argomenti della sezione:

- Configurazione dei filtri di distribuzione
- Configurazione dei filtri di distribuzione per un amministratore delegato

Usare i filtri di distribuzione per limitare le app disponibili per l'installazione. I filtri di distribuzione consentono di visualizzare solo le app del Catalogo app idonee per il dispositivo.

Licenza: Silver

Tali filtri sono disponibili come impostazione predefinita:

- **App abilitate per Android enterprise** - limita la distribuzione delle app esclusivamente ai dispositivi abilitati per Android enterprise.
- **App solo per iPad** - limita la distribuzione delle app a dispositivi iPad.
- **App solo per iPhone** - limita la distribuzione delle app a dispositivi iPhone.

Configurazione dei filtri di distribuzione

1. Andare su **App > Filtri di distribuzione**.
   Qui vengono elencati i filtri delle app predefiniti e ogni altro filtro delle app creato.
2. Fare clic su **+Aggiungi** per accedere alla finestra di dialogo **Crea filtro di distribuzione**.
3. Immettere un nome e una descrizione per la configurazione nei campi appropriati.
4. Selezionare le definizioni delle regole. Queste regole possono essere create utilizzando gli operatori applicabili, tra cui "contiene", "è inferiore a", "è maggiore di", "è compreso nell'intervallo", "è uguale a", e "non è uguale a". Le regole possono essere nidificate insieme utilizzando le opzioni QUALSIASI (OR) o TUTTO (AND). I filtri di distribuzione delle app sono i seguenti:
   - Accesso bloccato
   - Supporto APNS
   - Dispositivo gestito Android con profilo di lavoro
   - Android for Work abilitato
   - Livello di patch di sicurezza di Android (dispositivi Android)
   - Dispositivi di lavoro gestiti Android (proprietario del dispositivo) abilitati
   - Profilo di lavoro Android su dispositivo di proprietà dell'azienda abilitato
   - Ultimo check-in del client
   - Client registrato
   - Conformità
   - Azione di conformità bloccata
   - Nome paese attuale
   - MCC attuale
   - MNC attuale
   - Attributo dispositivo personalizzato

- Attributo LDAP personalizzato
- Attributo utente personalizzato
- Attributo IDP personalizzato
- Tipo di dispositivo
- Nome paese principale
- MCC nazionale
- MNC nazionale
- IMEI
- IMEI2 (solo su dispositivi Android con doppia porta SIM e applicabile a dispositivi Android 8.0 o superiori)
- Modalità tutto schermo
- Produttore
- Versione SO
- Proprietà
- N. di telefono
- Roaming
- Stato Secure Apps
- Supervisionato
- Sentry bloccato
- Registrazione utente completata
- Registrato con Registrazione automatica dispositivo
- Automated Registrazione dispositivi abilitato

5. Fare clic su **Crea filtro di distribuzione**.
6. Se necessario, selezionare un filtro personalizzato da aggiornare.
    1. Fare clic su **Modifica** per visualizzare la pagina **Aggiorna filtro di distribuzione**.
    2. Immettere un nome e una descrizione per la configurazione nei campi appropriati.
    3. Utilizzare i menu a discesa per definire le regole per il filtro.
    4. Fare clic su **Aggiorna filtro di distribuzione**.
7. Selezionare un'app.
8. Nella pagina delle informazioni dell'app selezionare la scheda **Distribuzione**.
9. Fare clic su **Modifica**.
10. Scegliere un'opzione di distribuzione dell'app:
    - **Tutti**
    - **Nessuno**
    - **Personalizzato**

    > La sezione Filtro di distribuzione è visibile solo se è selezionata l'opzione di distribuzione **Tutti** o **Personalizzata**.

11. Scegliere un'opzione del filtro di distribuzione:

1. Inserire un nome di filtro nel campo **Cercare i filtri di distribuzione esistenti**... per individuare un filtro creato in precedenza.
2. Fare clic su **+Aggiungi filtro di distribuzione** per aggiungere un nuovo filtro.

I filtri di distribuzione possono essere creati o assegnati a un'app prima che sia aggiunta al catalogo. Le modifiche apportate ai filtri di distribuzione influenzano la distribuzione delle app che utilizzano quel filtro (in tutti gli spazi).

Se il filtro è impostato e l'opzione **Consenti installazione app su dispositivi M1 al momento della distribuzione** è abilitata, il risultato viene caricato nei dispositivi macOS M1. Se l'opzione **Consenti installazione app su dispositivi M1 al momento della distribuzione** è abilitata e il filtro di distribuzione è impostato su **Tutti** o **Personalizzato**, l'app VPP iOS sarà disponibile per tutti i dispositivi Mac. I filtri di distribuzione per gli attributi correlati a macOS non sono supportati per le app iOS.

Configurazione dei filtri di distribuzione per un amministratore delegato

Un amministratore delegato può gestire e modificare i filtri creati che sono stati aggiunti ad app singole durante il processo di distribuzione nello spazio delegato. Tuttavia, l'amministratore delegato non può utilizzare i filtri di distribuzione creati nello spazio predefinito in nessun altro spazio ma può utilizzarli per le app delegate.

Un amministratore delegato può creare, gestire e modificare i filtri di distribuzione in uno spazio specifico a cui hanno accesso. Il filtro di distribuzione è disponibile solo nello spazio in cui è stato creato. I filtri di distribuzione delle app non possono essere delegati.

Quando un amministratore delegato con ruolo di gestione di sistema e app aggiunge un'app utilizzando il filtro di distribuzione in uno spazio delegato, può visualizzare i dettagli per i dispositivi nel suo spazio e per i dispositivi in altri spazi.

Un utente con il ruolo di gestione del sistema o sistema di sola lettura non sarà in grado di creare, aggiornare o eliminare i filtri in alcun spazio.

L'amministratore delegato con ruolo di gestione di contenuti e app potrebbe non avere accesso al filtro di distribuzione. Per questo motivo, non è possibile:

- Creare app utilizzando i filtri di distribuzione. Ciò accade quando è stato effettuato l'accesso come amministratore delegato e si aggiunge un'app.
- L'amministratore delegato con ruolo di sola lettura del sistema o un ruolo superiore può aggiungere app con il filtro di distribuzione. Un amministratore delegato senza ruolo di gestione di sistema può aggiungere app senza il filtro di distribuzione.

L'amministratore delegato può filtrare lo stato della delega nel catalogo delle app selezionando le opzioni seguenti:

- Delegato
- Non delegato

8.16. Escludere o distribuire le app

Escludere o distribuire le app gestite da un dispositivo senza modificare la configurazione di distribuzione delle app per le app interne e pubbliche su dispositivi iOS, macOS e Windows. Per tutte le app gestite, queste opzioni sono presenti nella colonna **Azioni** della sezione **App disponibili** per tutti i dispositivi.

Autorizzazioni

Per escludere o distribuire un'applicazione a o da un dispositivo, è necessario disporre delle seguenti autorizzazioni:

- Dispositivo di accesso nello spazio (partizione)
- Accedere alle app disponibili per il dispositivo.

Escludi

L'opzione di esclusione per un'app selezionata disinstalla e rimuove i dati associati dal dispositivo. Seguire il flusso di lavoro per escludere un'app prerequisita. Un pop-up di conferma indica che si sta escludendo un'app prerequisito, con conseguente esclusione dell'app principale dal dispositivo.

Se si escludono le app interne con più versioni, vengono escluse dal dispositivo tutte le versioni app non distribuite. Se si esclude un'app dal dispositivo, questa viene eliminata da Apps@Work e Ivanti Go. Se si esclude ed elimina un'app dal Catalogo app e la si aggiunge nuovamente, l'app non rimarrà più esclusa per il dispositivo. Se si esclude un'app gestita dal dispositivo, questa deve essere visibile nell'elenco **Dispositivi** > **Dispositivi** > **App disponibili** affinché l'amministratore possa distribuire l'app dopo averla esclusa.

Distribuisci

Quando l'amministratore attiva il comando **Invia installazione** dall'app, l'app non verrà installata finché l'amministratore non deciderà di distribuirla dalle **app disponibili** del dispositivo. Viene visualizzato un nuovo messaggio di esclusione per i dispositivi che non ricevono l'app. Quando l'amministratore distribuisce un'applicazione disponibile, la sincronizzazione successiva installa l'applicazione distribuita sul dispositivo.

8.17. Recensioni

Argomenti della sezione:

- Visualizzazione di valutazioni e recensioni
- Disattivazione di valutazioni e recensioni
- Eliminazione di una recensione
- Esportazione delle recensioni in un file CSV

Le recensioni sono i commenti e le valutazioni (stelle) degli utenti sulle app presenti nel catalogo. Le recensioni informazioni preziose per gli utenti esistenti dell'app e per quelli che stanno valutando di installarla. Utilizzare la pagina **Recensioni** per visualizzare o eliminare le valutazioni e le recensioni. È possibile eliminare una recensione o una valutazione se è poco recente o inappropriata.

- Solo gli utenti dei dispositivi possono creare e modificare valutazioni e recensioni sulle app.
- Gli utenti dei dispositivi possono modificare ma non eliminare le loro valutazioni e recensioni.
- Solo gli amministratori possono eliminare le recensioni sulle app.
- Non è possibile eliminare le valutazioni. Le valutazioni (stelle) relative alle app vengono conservate sulla pagina **App > Catalogo app** anche qualora venisse disabilitata la funzione di recensioni e valutazioni per gli utenti.

Visualizzazione di valutazioni e recensioni

- Andare su **App > Recensioni** per leggere le recensioni complete dei commenti e per le valutazioni (stelle) degli utenti per le applicazioni distribuite.
- Andare ad **App > App Catalog** e visualizzare la colonna relativa alla **media delle valutazioni**, per ottenere una stima del numero totale di recensioni e la media delle valutazioni.
- Andare su **App > Catalogo app**, fare clic su **Nome dell'applicazione** e selezionare la scheda **Recensioni** per le recensioni e le valutazioni di un'applicazione specifica.

Disattivazione di valutazioni e recensioni

1. Andare su **App > Impostazioni del catalogo**.
2. Deselezionare **Abilita valutazioni e recensioni** nel catalogo app dell'utente finale.
3. Fare clic su **Salva**.

Eliminazione di una recensione

1. Andare su **App > Recensioni**.
2. Selezionare la recensione.
3. Fare clic sul pulsante **Azioni** in alto a destra della pagina.
4. Selezionare **Elimina**.
5. Fare clic su **Sì** nella finestra di dialogo di conferma **Elimina recensione**.

Se non è possibile eseguire le attività indicate nella pagina **Recensioni**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei ruoli seguenti:

- Gestione app e contenuti

Esportazione delle recensioni in un file CSV

È possibile esportare le recensioni delle app utilizzando l'opzione **Esporta in CSV** dalla pagina **Recensioni**.

Procedura

1. Andare su **App > Recensioni**.
2. Fare clic sull'opzione **Esporta in CSV** per esportare l'elenco delle recensioni e i dettagli correlati in un file CSV.
3. Viene visualizzato un messaggio pop-up con i pulsanti **Continua** e **Annulla** che indica che il processo di esportazione è stato avviato e che un report sarà disponibile a breve.
4. Fare clic su **Continua** e attendere il completamento della richiesta prima di inviarne un'altra.
5. Viene visualizzato un messaggio che indica che il **report Recensioni app in CSV è terminato** con i pulsanti **Download** ed **Elimina**.
6. Fare clic su **Download** per scaricare il report.
7. (Opzionale) Fare clic su **Elimina** per eliminare il report.

8.18. Apple App e libri

Argomenti della sezione:

- Distribuzione di licenze di app a più account Apple App e libri in uno spazio
- Distribuzione di licenze basate su dispositivo e basate sull'utente
- Utilizzo dell'opzione di licenza basata su dispositivo
- Utilizzo dell'opzione di licenza basata sull'utente
- Aggiunta di un'app App e libri al catalogo
- Aggiunta di account App e libri
- Aggiornamento di un token sicuro App e libri
- Aggiornamento della priorità di un account App e libri
- Eliminazione di un token sicuro App e libri
- Distribuzione di licenze per un'app App e libri nel catalogo
- Visualizzazione delle licenze delle app per utente
- Notifiche sull'utilizzo della licenza App e libri
- Visualizzazione dell'utilizzo della licenza App e libri
- Revoca della licenza App e libri per un'app
- Comportamento di App e libri per dispositivi macOS e iOS
- Diritti della licenza App e libri quando un dispositivo viene spostato in un altro spazio

Licenza: Silver

La schermata **Apple App e libri** è disponibile solo se Apple App e libri è stato configurato nelle **impostazioni dell'App Catalog**. La schermata mostra le licenze delle app acquistate per i dispositivi Apple tramite Apple App e libri e il numero di licenze utilizzate. Utilizzare questa schermata per:

- selezionare le app App e libri che verranno incluse nel catalogo
- distribuire licenze per app App e libri

Per ulteriori informazioni sulla distribuzione di applicazioni con App e libri, vedere l'articolo della Ivanti Community, **Ivanti Neurons for MDM: come distribuire le app con VPP**.

> Apple Books potrebbe non essere disponibile in tutti i Paesi o regioni. Per distribuire le licenze delle app tramite App e libri di Apple, è necessario inserire l'sToken fornito da Apple.

Distribuzione di licenze di app a più account Apple App e libri in uno spazio

- Se la stessa app è presente in più account App e libri, la licenza verrà distribuita dall'account secondo l'ordine di priorità degli account.
- Se la stessa app è presente in più account App e libri e la licenza dell'app nell'account App e libri con priorità più alta è scaduta, verrà distribuita una licenza per l'app dall'account con priorità successiva solo se l'utente o il dispositivo è presente nell'elenco di distribuzione delle licenze dell'account con priorità successiva.

- Se si modifica la priorità degli account App e libri, la licenza non sarà revocata né riassegnata. Verrà distribuita una licenza per l'app dal primo account. Se le licenze nel primo account sono scadute, verrà distribuita una licenza per l'app dall'account con priorità successiva e così via.
- L'utente può revocare tutte le licenze di un'app dalla pagina App Catalog. Questa azione revoca la licenza dell'app da tutti gli account App e libri disponibili.
- Le licenze riservate hanno la precedenza rispetto alla priorità degli account App e libri.

Distribuzione di licenze basate su dispositivo e basate sull'utente

Se la licenza di un'app è basata su dispositivo o basata sull'utente dipende dalla modalità di assegnazione. Quando si assegna la licenza di un'app a un dispositivo, diventa una licenza basata su dispositivo. Quando si assegna la licenza di un'app a un utente, diventa una licenza basata sull'utente.

Una licenza viene distribuita quando si installa un'app App e libri su un dispositivo, o quando viene rilasciato un token per quell'app. Se non sono disponibili licenze per l'app, l'utente può scegliere di installare e pagare l'app per conto proprio. Se è già stata assegnata una licenza basata sull'utente per l'app App e libri richiesta, quest'ultima viene installata utilizzando la licenza esistente basata sull'utente, anziché la licenza App e libri.

> In caso di **iPad condivisi**, App e libri viene installata sulla base delle licenze basate sul dispositivo indipendentemente dal fatto che le licenze basate sul dispositivo siano selezionate o meno.

Utilizzo dell'opzione di licenza basata su dispositivo

Con le licenze basate su dispositivo, gli utenti non devono effettuare la registrazione ad App e libri. Le app richieste verranno installate in modo automatico. I dispositivi supervisionati dall'azienda non necessitano di gestire un ID Apple di proprietà dell'IT.

Durante il check-in del dispositivo, quest'ultimo viene identificato dal numero di serie e, se esistono licenze disponibili, viene installata l'app richiesta. In assenza di licenze disponibili, l'app non viene installata. Se la licenza di un'app è riservata, l'assegnazione di una licenza basata su dispositivo non avviene durante l'installazione dell'app.

> Gli aggiornamenti delle app distribuite utilizzando licenze App e libri basate su dispositivo sono controllati dall'amministratore.

Per controllare in che modo un'app verrà aggiornata, in **App> App Catalog** scorrere fino alla scheda **Configurazioni delle app/Installa sul dispositivo**. Sarà possibile selezionare un aggiornamento immediato che verrà eseguito al successivo check-in del dispositivo, oppure è possibile scegliere di aggiornare l'app automaticamente quando nuove versioni diventano disponibili.

Importante: prima di assegnare una licenza basata su dispositivo a un'app business to business (B2B) o di produttività, verificare con lo sviluppatore che tale app sia idonea per una licenza basata su dispositivo.

Utilizzo dell'opzione di licenza basata sull'utente

Le licenze basate sull'utente rimangono valide per l'utente specifico se è necessario spostarle da un dispositivo a un altro in caso di perdita o smarrimento del dispositivo o se l'utente passa a un nuovo dispositivo. Con le licenze basate sull'utente, l'utente deve prima effettuare la registrazione ad Apple App e libri. La registrazione è un'operazione manuale che l'utente finale deve completare nell'App Catalog. Le app App e libri richieste non vengono installate sul dispositivo finché l'utente non effettua la registrazione ad App e libri.

Se l'app è un'app App e libri richiesta e la distribuzione della licenza è basata sull'utente:

- L'installazione dell'app non viene effettuata se l'utente non è registrato al programma App e libri.

- È possibile installare le app richieste se l'utente è registrato al programma App e libri ed è disponibile una licenza.
- Se l'utente è registrato al programma App e libri, ma non ci sono licenze disponibili, l'app non viene installata.

Aggiunta di un'app App e libri al catalogo

Procedura

1. Andare in **App > Catalogo app**.
2. Selezionare un'app e fare clic su **Aggiungi al catalogo**. Fare clic su **Avanti**.
3. È possibile aggiungere una descrizione dell'app. Fare clic su **Avanti**.
4. Selezionare un'opzione di distribuzione. Fare clic su **Avanti**.
5. Fare clic sulla scheda **Configurazioni delle app**.
6. Facoltativamente, selezionare **Installa sul dispositivo**. Questa opzione di configurazione installa l'app senza che ciò venga richiesto all'utente del dispositivo iOS supervisionato.
7. Se necessario, selezionare altre opzioni di configurazione.

Nella pagina delle informazioni del token sicuro App e libri, vengono visualizzati i seguenti dettagli del token:

- Data di creazione
- Posizione (se il token contiene queste informazioni)
- Data di scadenza

Aggiunta di account App e libri

Ivanti Neurons per MDM consente di aggiungere più account App e libri mediante l'aggiunta di più token sicuri App e libri in un singolo spazio.

Per aggiungere un token sicuro App e libri in uno spazio, procedere come segue:

1. Andare in **App > Apple App e libri**.
2. Fare clic su **+ Aggiungi sToken di App e libri**.
3. Immettere un nome e scegliere il file del token.
4. È possibile deselezionare l'opzione **Distribuisci automaticamente le app App e libri a tutti gli utenti**. Questa opzione è selezionata di default; in questo caso il gruppo Tutti gli utenti viene utilizzato per distribuire le licenze FCFS.
5. È possibile selezionare l'opzione **Cancella tutti i dati dalla licenza App e libri precedente** per rimuovere le licenze di tutte le app associate a questo token.
6. Fare clic su **Salva**.

Una volta aggiunto l'account, viene visualizzato un elenco di tutti gli account App e libri aggiunti.

Aggiornamento di un token sicuro App e libri

Procedura

1. Andare in **App > Apple App e libri**.
2. Fare clic sul nome dell'account App e libri.
3. Nella scheda Token, fare clic su **Aggiorna sToken** (file .stoken).

4. Immettere un nome per il token e scegliere il file del token.
5. È possibile deselezionare l'opzione **Distribuisci automaticamente le app App e libri a tutti gli utenti**. Questa opzione è selezionata di default; in questo caso il gruppo Tutti gli utenti viene utilizzato per distribuire le licenze FCFS.
6. È possibile selezionare l'opzione **Cancella tutti i dati dalla licenza App e libri precedente** per rimuovere le licenze di tutte le app associate a questo token.
7. Fare clic su **Aggiorna**.

Nella scheda Token, fare clic su **Risincronizza informazioni sull'utilizzo della licenza App e libri** per eseguire la sincronizzazione completa delle informazioni di tutte le app e le licenze dal servizio Apple App e libri. Questa azione è necessaria solo se le informazioni di allocazione della licenza in Ivanti Neurons per MDM non sono accurate. La mancanza di precisione potrebbe essere dovuta a incongruenze nelle API Apple App e libri.

Aggiornamento della priorità di un account App e libri

Gli amministratori possono assegnare una priorità a ciascun account App e libri in uno spazio, a seconda delle licenze da utilizzare. Le priorità degli account App e libri consentono di disporre di un sistema di distribuzione licenze prevedibile e risolvere i conflitti quando un utente o un dispositivo è idoneo a ricevere una licenza da più account App e libri per la stessa app.

Procedura

1. Andare in **App > Apple App e libri**.
2. Fare clic su **Modifica priorità** per il nome dell'account App e libri richiesto.
3. Nella finestra Modifica priorità, selezionare una nuova priorità.
4. Fare clic su **Salva**.

Eliminazione di un token sicuro App e libri

L'operazione di rimozione di un token sicuro App e libri è irreversibile e distruttiva. Quando un token viene rimosso:

- Verranno rimossi i token delle app che dispongono di token riservati
- Le app che sono state acquistate rimarranno nel catalogo e gli utenti potranno pagarle per conto proprio.
- Le app installate dagli utenti finali tramite l'account App e libri aziendale dovranno passare ad account personali, se gli utenti desiderano utilizzarle. A tale scopo, gli utenti avranno a disposizione un periodo di tolleranza di 30 giorni.

Procedura

1. Andare in **App > Apple App e libri**.
2. Fare clic sul nome dell'account App e libri.
3. Nella scheda Token, fare clic su **Elimina**.
4. Nella finestra Eliminazione token sicuro App e libri, selezionare l'opzione **Sì, elimina token sicuro App e libri** per confermare.
5. Fare clic su **Elimina**.

Distribuzione di licenze per un'app App e libri nel catalogo

1. Selezionare **App > Apple App e libri** nel menu principale.
2. Verrà visualizzato un elenco di account App e libri. In ciascun account viene visualizzato un elenco delle app acquistate tramite il programma App e libri.

Selezionare un'app e fare clic su **Distribuisci licenze**.

3. Nella sezione Licenze App e libri, selezionare un'opzione di distribuzione: **In base all'ordine cronologico**, **Riservata** o **Non consentita**.

Visualizzazione delle licenze delle app per utente

È possibile stabilire la preferenza per le licenze degli utenti dalla scheda Utilizzo licenze.

1. Fare clic sulla scheda **Utenti**.
2. Selezionare un utente
3. Fare clic sulla scheda **Utilizzo licenza**.
   Verrà visualizzato un elenco delle app con il relativo tipo di licenza App e libri e i relativi dettagli sull'assegnazione.

Per visualizzare l'utilizzo delle licenze per ogni app per utente:

1. Passare a **Utenti** nel menu principale di Ivanti Neurons for MDM.
2. Selezionare un utente
3. La scheda **Dispositivi** viene visualizzata per impostazione predefinita.
   Fare clic sulla scheda **Utilizzo licenza**.
   Verrà visualizzato un elenco delle app installate sul dispositivo dell'utente che include le informazioni sullo stato della licenza. Il numero di serie del dispositivo è riportato nella colonna Tipo di licenza App e libri per le licenze basate su dispositivo.
   - Nome app
   - Versione dell'app
   - Prezzo dell'app
   - Data di assegnazione dell'app
   - Tipo di licenza App e libri
   - Azioni (stato della licenza)
   - Informazioni sulla piattaforma per i dettagli della licenza.

È inoltre possibile visualizzare l'utilizzo della licenza App e libri per ciascuna app:

1. Passare a **App > Catalogo app** nel menu principale di Ivanti Neurons for MDM.
2. Selezionare un'app.
3. Fare clic sulla scheda **Licenze App e libri**, se presente.
4. Fare clic sul nome dell'account. Solo le app acquistate tramite il programma App e libri verranno visualizzate in questa scheda.

Viene visualizzata una scheda separata per ciascun tipo di licenza App e libri.

Tipo di licenza e registro	Descrizione
Ordine cronologico (FCFS, First Come First Served) - È possibile selezionare quale gruppo di utenti riceverà questo tipo di licenza.	• App richieste dall'utente - App che l'utente sceglie di installare. L'impostazione predefinita è la licenza basata sull'utente • App necessarie: App necessarie e installate dalla configurazione dell'amministratore tramite l'impostazione **Installa su dispositivo.** Queste app utilizzano licenze basate sul dispositivo per impostazione predefinita.
Riservate	Le licenze riservate hanno priorità sulle licenze assegnate in ordine cronologico. Qui è possibile selezionare gli utenti o i dispositivi che hanno una licenza riservata per l'app.
Non consentite	Immettere gli utenti a cui non è consentita una licenza per l'app. L'utente può ancora installare l'app, ma dovrà acquistarla.
Registro attività	Visualizza l'utente, il tipo di licenza App e libri assegnata, la data di assegnazione e l'ultima azione compiuta sulla licenza.

Per visualizzare l'utilizzo dettagliato delle licenze per ogni app per dispositivo:

1. Passare a **Dispositivi** nel menu principale di Ivanti Neurons for MDM.
2. Selezionare un dispositivo.
3. Fare clic sulla scheda **App installate**.
4. Verrà visualizzato un elenco delle app gestite installate sul dispositivo selezionato che include le informazioni sullo stato della licenza.
    - Nome app
    - Versione dell'app
    - Piattaforma supportata
    - Fonte dell'app
    - Dimensioni dell'app
    - Tipo di licenza App e libri
    - Data di segnalazione (installazione) dell'app per le app iOS

Ricercare le app installate per il dispositivo come indicato di seguito:

- Nome app
- ID bundle o pacchetto

Notifiche sull'utilizzo della licenza App e libri

Le notifiche di App e libri consentono di monitorare l'utilizzo della licenza App e libri. Le soglie delle notifiche vengono definite come:

- Viene emessa una notifica informazioni quando è stato utilizzato oltre il 50% delle licenze.
- Viene emessa una notifica di avviso quando sono state utilizzate dal 70 all'80% delle licenze.
- Viene emessa una notifica critica quando sono state utilizzate dal 90 al 100% delle licenze.
- Le notifiche vengono cancellate quando l'utilizzo scende al di sotto del 50%.

Per visualizzare le informazioni di licenza per ciascuna app:

1. Fare clic su **App > Apple App e libri**.
2. Vengono visualizzate le informazioni di licenza che includono:
    - Nome dell'app.
    - Costo della licenza.
    - Numero di licenze disponibili.
    - Numero di licenze riscattate.

Andare su **Dashboard > Notifiche** per visualizzare i dettagli di una notifica di licenza.

3. Viene visualizzata la pagina delle notifiche.
   Fare clic sul titolo della notifica per visualizzarne i dettagli. Consultare la pagina Dashboard per le notifiche disponibili.

Notifiche sull'utilizzo della licenza App e libri

Trigger	Gravità	Tipo di notifica	Tipo di componente
Riscattate al 50%	Informazioni	Utilizzo licenza	App e libri
Riscattate al 70%	Avviso	Utilizzo licenza	App e libri
Riscattate all'80%	Avviso	Utilizzo licenza	App e libri
Riscattate al 90%	Avviso	Utilizzo licenza	App e libri
Riscattate al 100%	Avviso	Utilizzo licenza	App e libri

Visualizzazione dell'utilizzo della licenza App e libri

I dettagli sull'utilizzo della licenza specifici per un utente sono visualizzati nella tabella sull'utilizzo della licenza nella colonna licenze.

1. Fare clic su un'app.
2. Fare clic sulla scheda **Utilizzo licenza**.
3. Immettere un nome utente nel campo di ricerca.

Revoca della licenza App e libri per un'app

Le licenze App e libri vengono revocate quando:

- Un dispositivo è inattivo (ritirato o cancellato).
- L'app App e libri viene eliminata.
- Viene revocata una licenza basata sul dispositivo in seguito al ritiro del dispositivo.
- Il token App e libri viene eliminato.

Per revocare la licenza App e libri di un'app:

1. Selezionare l'app in **App > Catalogo app**.
2. Fare clic sulla scheda **Licenze Apple App e libri**, se presente.

3. Eseguire una delle operazioni seguenti:
    1. Fare clic su **Revoca tutte le licenze** per revocare tutte le licenze di tutti gli utenti o dispositivi.
    2. Fare clic sulla scheda **Registro attività**. Usare la colonna **Azioni** per revocare singole licenze basate su utente o dispositivo.

- Per i dispositivi iOS, Apple consente un periodo di tolleranza di 30 giorni per app App e libri dopo la revoca della licenza App e libri. Pertanto, l'app App e libri rimane installabile.
- Per i dispositivi macOS, l'app rimane sul dispositivo in seguito alla revoca della licenza App e libri.

Per revocare la licenza App e libri per un utente:

1. Fare clic su un'app.
2. Fare clic sulla scheda **Utilizzo licenza**.
3. Fare clic sul collegamento **Revoca licenza** corrispondente all'utente per il quale si desidera revocare l'accesso alla licenza.

> Le licenze App e libri vengono revocate automaticamente se l'utente viene eliminato o rimuove il profilo MDM dal dispositivo.

Notifiche di errore di autenticazione di App e libri

Durante l'uso del servizio Apple App e libri, potrebbero verificarsi errori di autenticazione. Le notifiche degli errori di autenticazione di App e libri sono le seguenti:

Notifica di errore	Azione
Token di autenticazione non valido	Caricare un sToken App e libri valido
Token scaduto	Generare un nuovo token online utilizzando l'account aziendale
sToken revocato	Caricare un token App e libri valido
Accesso richiesto	Accedere al servizio App e libri

Comportamento di App e libri per dispositivi macOS e iOS

App e libri per iOS

Azione	Licenza basata su dispositivo	Licenze basata sull'utente
Rimuovere l'app App e libri dalla distribuzione per l'utente	L'app viene disinstallata sul dispositivo dell'utente	L'app viene disinstallata sul dispositivo dell'utente
Annullare la delega dell'app App e libri	L'app viene disinstallata da tutti i dispositivi in spazi non predefiniti	L'app viene disinstallata da tutti i dispositivi in spazi non predefiniti
Eliminare l'app App e libri dallo spazio predefinito o personalizzato	L'app viene disinstallata da tutti i dispositivi	L'app viene disinstallata da tutti i dispositivi

App e libri per macOS

Azione	Licenza basata su dispositivo	Licenze basata sull'utente
Rimuovere l'app App e libri dalla distribuzione per l'utente	L'app non viene disinstallata sul dispositivo dell'utente	ND
Annullare la delega dell'app App e libri	L'app non viene disinstallata da tutti i dispositivi in spazi non predefiniti	ND
Eliminare l'app App e libri dallo spazio predefinito o personalizzato	L'app non viene disinstallata da tutti i dispositivi	ND

Diritti della licenza App e libri quando un dispositivo viene spostato in un altro spazio

Se un dispositivo viene spostato in un nuovo spazio, la licenza App e libri assegnata al dispositivo o al proprietario del dispositivo viene revocata. Viene assegnata una nuova licenza App e libri a seconda della disponibilità nel nuovo spazio.

Di seguito sono indicati gli scenari dei diritti della licenza App e libri:

Scenario	Diritto
Una licenza App e libri è assegnata a un dispositivo o al proprietario di un dispositivo nello spazio di origine e una licenza App e libri per la stessa app è disponibile nello spazio di destinazione.	Assegnare una licenza dal token App e libri nello spazio di destinazione.
Una licenza App e libri è assegnata a un dispositivo o al proprietario di un dispositivo nello spazio di origine e non è disponibile alcuna licenza App e libri per la stessa app nello spazio di destinazione.	Revocare la licenza dal token App e libri nello spazio di origine.
Nessuna licenza App e libri è assegnata a un dispositivo o al proprietario di un dispositivo nello spazio di origine e una licenza App e libri per qualsiasi app App e libri installata è disponibile nello spazio di destinazione.	Assegnare una licenza dal token App e libri nello spazio di destinazione.

Se non è possibile eseguire le attività indicate nella pagina **Categorie app**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione app e contenuti

8.19. Impostazioni catalogo

Argomenti della sezione:

- Cambiamento delle impostazioni per la gestione delle app Apple
- Impostazione regione App Store predefinita
- Attivazione/disattivazione degli aggiornamenti delle app iOS
- Attivazione/disattivazione delle recensioni e delle valutazioni delle applicazioni
- Caricamento o aggiornamento di un sToken di App e libri iOS/macOS (licenza: Gold)
- Rimozione di un sToken di App e libri iOS/macOS dal servizio Ivanti Neurons for MDM

Nella pagina **App** > **Impostazioni di catalogo**, configurare le preferenze che si applicano a tutte le app del proprio catalogo. Sono disponibili le seguenti azioni:

- Includere gli aggiornamenti delle app durante il check-in del dispositivo
- Impedisci il backup su iCloud e iTunes (solo iOS)
- Impostare la regione App Store predefinita (Apple e Microsoft)
- Rimuovere le app iOS dopo l'annullamento della registrazione del dispositivo
- Abilita Ivanti Neurons for MDM "Valutazioni e Recensioni"
- Caricare i token per App e libri su iOS e macOS (richiede una licenza Gold)

Cambiamento delle impostazioni per la gestione delle app Apple

Queste impostazioni verranno applicate a tutte le app, a meno che non sia stata creata una configurazione di gestione per le singole app.

1. Selezionare o deselezionare una o più delle seguenti caselle di controllo:
   - **Aggiorna app durante il check-in del dispositivo** (selezionata per impostazione predefinita)
   - **Impedisci il backup su iCloud e iTunes**
   - **Rimuovi le app non registrate**

Fare clic su **Salva**.

Notifiche

1. Fare clic sull'elenco a discesa in corrispondenza di **Genera una notifica di sistema quando sono disponibili nuove versioni di app dall'App Store di Apple e dal Play Store di Google** e selezionare una delle seguenti opzioni:
   - **Una volta alla settimana**
   - **Una volta al giorno**

Fare clic sull'elenco a discesa sotto **Genera notifiche all'utente finale per gli aggiornamenti delle nuove app disponibili in Catalogo app** e selezionare una delle opzioni:

- **Una volta alla settimana**
- **Una volta al giorno**

Impostazione regione App Store predefinita

Nelle impostazioni di App Catalog, impostare la regione predefinita per App Store Apple e Microsoft.

1. Nella sezione Regione App Store predefinita:
    - Selezionare **Regione App Store Apple**.
    - Selezionare **Regione App Store Microsoft**.
2. Selezionare o deselezionare l'opzione per utilizzare l'ultima regione App Store selezionata come impostazione predefinita per ogni amministratore. Se l'opzione è selezionata, verrà impostata l'ultima regione App Store selezionata da ogni amministratore; l'impostazione sovrascriverà le impostazioni precedenti. Se l'amministratore utilizza questa funzionalità per la prima volta, verranno applicate le regioni App Store impostate per l'ultimo utilizzo precedente.
3. Fare clic su **Salva**.

Attivazione/disattivazione degli aggiornamenti delle app iOS

1. Selezionare o deselezionare **Aggiorna app durante il check-in del dispositivo.**
    - Questa opzione è selezionata per impostazione predefinita.
    - Se non è selezionata, nessun check-in dei dispositivi (inclusi i check-in forzati da parte dell'amministratore) include gli aggiornamenti dell'app.
    - Tuttavia l'utente può aggiornare manualmente le app facendo clic sull'azione di forzatura del check-in nel catalogo delle app del dispositivo.
    - Le installazioni di nuove app e tutte le altre configurazioni e impostazioni saranno aggiornate durante il check-in del dispositivo.

Fare clic su **Salva**.

Nel caso di un'app gestita, l'amministratore può fare clic sul pulsante **Aggiorna** nella pagina dei dettagli dell'app per aggiornare manualmente l'app all'ultima versione disponibile nell'App Store.

Per consentire il check-in del dispositivo e permettere che gli aggiornamenti delle app vengano eseguiti insieme agli altri aggiornamenti e configurazioni, l'utente può fare clic sul pulsante **Forza il check-in** nel menu dell'App Catalog sul proprio dispositivo.

Queste impostazioni consentono agli utenti finali di scegliere quando eseguire gli aggiornamenti delle app:

- Aspettare di essere connessi a una rete Wi-Fi per evitare addebiti per il traffico dati.
- Evitare di essere bloccati durante gli aggiornamenti delle app.

Attivazione/disattivazione delle recensioni e delle valutazioni delle applicazioni

In questo modo l'utente potrà valutare e recensire le applicazioni e gli altri utenti potranno leggere i suoi commenti.

1. Selezionare o deselezionare l'opzione **Abilita valutazioni e recensioni nell'App Catalog dell'utente finale**.
2. Fare clic su **Salva**.

> Il formato dell'sToken di App e libri è stato modificato. Anziché una stringa di caratteri come nelle versioni precedenti, ora viene memorizzata una stringa di caratteri in un file di testo nel formato di file vpptoken. Caricare direttamente il file nella console di amministrazione per l'elaborazione. La pagina dell'account App e libri è stata aggiornata per visualizzare le date di scadenza e il nome dell'organizzazione di App e libri.

Caricamento o aggiornamento di un sToken di App e libri iOS/macOS (licenza: Gold)

1. Selezionare **Aggiungi sToken App e libri**.
2. Immettere un nome per il file sToken nel campo **Nome alias**.
3. Trascinare il file sToken nell'area specificata o fare clic su **Scegli file** per passare al file sToken.
4. Fare clic su **Salva** oppure, se si intende aggiornare un file sToken, fare clic su **Aggiorna**.
5. Visitare la pagina **Apple App e libri** per visualizzare le app associate al token.

> Se i token di App e libri erano riservati a singoli utenti in una versione precedente di Ivanti Neurons per MDM, verificare che siano ancora riservati a tali utenti o riservarli nuovamente, se necessario.

Rimozione di un sToken di App e libri iOS/macOS dal servizio Ivanti Neurons for MDM

È possibile revocare un'app che non è più necessaria a un utente e riassegnarla in base alle necessità. Se l'app è stata distribuita come app gestita con MDM per iOS/macOS, è possibile rimuovere immediatamente l'app e tutti i dati.

1. Selezionare un'app da rimuovere.
2. Fare clic su **Elimina**.
   Appare un dialogo di avviso.
3. In alternativa, si può concedere all'utente un periodo di tolleranza di 30 giorni per
   - salvare i dati;
   - acquistare una copia personale dell'app;
   - trasferire le app installate dall'account App e libri agli account personali per continuare a utilizzarle.

Se non è possibile eseguire le attività indicate nella pagina **Impostazioni catalogo**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario il seguente **ruolo**:

- Gestione app e contenuti

8.20. Distribuzione di dipendenze delle app

Quando si carica un bundle di applicazioni interne, Ivanti Neurons for MDM esegue la scansione delle applicazioni per identificarne le dipendenze. Le eventuali dipendenze trovate vengono elencate nel terzo passaggio dell'aggiunta guidata dell'applicazione. Per ogni dipendenza di un'applicazione gli amministratori possono decidere se caricare o meno il file della dipendenza. Tuttavia, se non si caricano i file delle dipendenze, l'installazione di alcune applicazioni potrebbe non riuscire.

L'amministratore ha un'opzione per impostare la dipendenza delle app quando installa una particolare app. In questo caso, possono essere presenti una o più app etichettate con l'app principale. Quando un utente cerca di installare l'app principale, l'utente riceverà una notifica sulle app dipendenti che saranno installate con l'app principale.

> Questa funzione è supportata solo su dispositivi iOS, Android, Windows e macOS.

In relazione ai prerequisiti e alle dipendenze delle applicazioni, notare quanto segue:

- L'amministratore può installare le applicazioni prerequisito prima di installare l'applicazione dipendente nel dispositivo. Un'applicazione prerequisita può essere un'applicazione interna, pubblica, privata (Android) o VPP.
- Ora il numero delle applicazioni prerequisito viene visualizzato nella colonna App prerequisito della pagina App Catalog. Spostando il mouse sopra il numero, è possibile visualizzare l'elenco delle applicazioni prerequisito.
- Le applicazioni prerequisito vengono scaricate direttamente appena viene attivata l'installazione dell'applicazione principale.
- Se l'applicazione principale è delegata, le applicazioni prerequisito associate vengono delegate automaticamente.
- Le applicazioni prerequisito non possono essere eliminate dall'App Catalog finché la relazione di prerequisito non viene rimossa.
- Le diverse versioni di un'applicazione possono avere app prerequisito diverse.
- La pagina Audit trail registra l'aggiunta, la rimozione e la delega automatica delle applicazioni prerequisite per iOS, Android e macOS.
- Se l'amministratore o l'utente finale installa un'applicazione che ha applicazioni prerequisite, le applicazioni prerequisite sono installate prima dell'installazione dell'applicazione principale. Se il check-in di un dispositivo viene eseguito prima che siano state installate tutte le applicazioni prerequisito, le applicazioni prerequisito già installate vengono disinstallate.

> Anche se un'applicazione richiede un file di dipendenze, Ivanti Neurons for MDM non richiede il caricamento di alcun file per distribuire un'app.

> Per i dispositivi Samsung, l'amministratore dovrebbe aggiungere le app necessarie all'elenco App consentite in modalità tutto schermo. Le app prerequisite aggiunte all'elenco delle app consentite non vengono aggiunte all'elenco delle app nella lista nera.

> Per i dispositivi non-Samsung, se l'app principale viene aggiunta all'elenco App consentite in modalità tutto schermo, l'app prerequisita dovrebbe essere eseguita in modo invisibile in background. È possibile visualizzare l'app prerequisita in modalità tutto schermo solo se l'amministratore imposta questa app in tale modalità.

> **Dispositivi Windows** - Se l'app Bridge è un'app prerequisita che non viene distribuita e l'app principale è un .exe che viene distribuito in modo invisibile all'utente. Una volta rimossa la dipendenza, l'app Bridge viene disinstallata, ma il file .exe presenta un errore dopo questo passaggio. L'amministratore deve assicurarsi che l'app Bridge non venga resa non distribuibile per impostazione predefinita.

Dispositivi Windows - Quando l'app principale non viene distribuita in modo invisibile all'utente e l'app principale presenta un'app prerequisita senza distribuzione, l'app prerequisita viene installata per prima con successo. Tuttavia, nel caso in cui l'app principale non dovesse installarsi, l'app prerequisita verrà disinstallata immediatamente. Un nuovo tentativo sull'app principale non riuscita avviene solo quando l'utente attiva una richiesta di installazione.

Aggiunta di un'applicazione interna

1. Andare in **App > Catalogo app**.
2. Fare clic su **Aggiungi**.
3. Trascinare il file dell'applicazione sulla casella tratteggiata, oppure fare clic su **Scegli file** per selezionarlo dal file system, quindi fare clic su **Conferma**.
4. Fare clic su **Avanti** (in basso a destra). Ivanti Neurons for MDM analizza l'app alla ricerca di file di dipendenze e li elenca nella tabella **Dipendenze app**.
5. Rivedere le informazioni sull'app e verificare di aver selezionato l'app corretta.
6. Fare clic sull'icona Carica nella colonna **Azioni**. Viene visualizzata la finestra **Carica dipendenza**.
7. Fare clic su **Scegli file** per cercare e individuare una copia locale del file, quindi fare clic su **Carica**.
8. Ivanti Neurons for MDM ricerca i pacchetti opzionali per l'app e, se presenti, li indica nella tabella Pacchetti opzionali. Se indicati, fare clic sull'icona Carica nella colonna Azioni. Viene visualizzata la finestra Carica pacchetto opzionale.
9. Rivedere le informazioni sull'app e verificare di aver selezionato l'app corretta.
10. Fare clic su **Scegli file** per cercare e individuare una copia locale del file, quindi fare clic su Carica.
11. Fare clic su **Avanti**.
12. (Facoltativo) Aggiungere gli screenshot dell'app e fare clic su **Avanti**.
13. Se l'applicazione richiede altre applicazioni prerequisito:
    1. Selezionare l'opzione **On** nella sezione **App prerequisito**.
    2. Cercare l'applicazione prerequisito nella scheda **Aggiungi app**.
    3. Selezionare le applicazioni.
    4. Fare clic su **Salva**.
14. Definire la distribuzione dell'app e fare clic su **Avanti**.
15. Definire la sezione Configurazione app e fare clic su **Fine**. La prossima volta che i dispositivi si sincronizzano con Ivanti Neurons for MDM, l'app viene distribuita nel dispositivo insieme con i file delle dipendenze.

È possibile aggiungere ulteriori dipendenze facendo clic sul pulsante Aggiungi dipendenze. Una volta caricate, anche queste dipendenze aggiuntive vengono elencate nella tabella Dipendenze app. L'amministratore può inoltre aggiungere manualmente il pacchetto opzionale di tipo Solo contenuto. Questo tipo di pacchetto non dipende dalla versione.

Aggiunta di un'app prerequisito

È possibile aggiungere un'applicazione prerequisito a un'applicazione principale. È possibile aggiungere prerequisiti diversi alle diverse versioni di un'applicazione principale. Nella pagina App Catalog è possibile scegliere se mantenere le stesse impostazioni di descrizione, script, screenshot, distribuzione, app prerequisito e configurazioni dell'app della versione esistente dell'applicazione

oppure cambiare le applicazioni richieste associate. Non è possibile eliminare un'applicazione prerequisito senza rimuovere l'associazione all'applicazione principale.

Ora le applicazioni prerequisito supportate vengono visualizzate nei seguenti campi specifici della pagina Audit trail:

La sezione Applicazioni prerequisite per le applicazioni supportate iOS, Android e macOS nella pagina Audit trail visualizza i seguenti campi:

appVersionId

nome

platformAppId

Sono visualizzate le applicazioni prerequisito per cui viene concessa e annullata automaticamente la delega e che contengono i campi seguenti:

dmPartitionDistributionType

dmPartitionDistributionReason

Procedura

1. Selezionare un'applicazione da **App Catalog**.
2. Fare clic su **Modifica**.
3. Scorrere verso il basso fino a **Delega app** e selezionare l'opzione **Delega questa app a tutti gli spazi**.
4. Fare clic su **Salva**.

> Se si delegano più applicazioni e si sceglie di rimuovere la delega dall'applicazione principale, l'applicazione prerequisito non viene automaticamente rimossa dalla delega.

8.21. Distribuzione di Divide Productivity con Android Enterprise

Divide Productivity è un'app PIM distribuibile sui dispositivi Android Enterprise.

1. Andare in **App > Catalogo app**.
2. In **Applicazioni aziendali**, fare clic su **Separa produttività**.
3. Immettere categorie aggiuntive o una descrizione.
4. Fare clic su **Avanti**.
5. Accettare le autorizzazioni visualizzate.
6. Fare clic su **Avanti**.
7. Selezionare un'opzione di distribuzione.
8. Espandere **Opzioni avanzate e Configurazione app**.
9. Usare le linee guida seguenti per abilitare le opzioni:
10. Selezionare un'opzione di promozione.

Impostazione	Operazione da eseguire
Impedisce all'utente di disinstallare l'app	Selezionare questa opzione per evitare che l'utente finale disinstalli l'app quando è stata installata in modo invisibile.
Indirizzo di posta	Usare le variabili per definire l'indirizzo e-mail da associare all'app.
Password	Usare la variabile per definire la password per l'account e-mail. Se questo campo viene lasciato vuoto, all'utente verrà richiesta la password.
Host	Immettere il nome host del server di posta da utilizzare. Immettere il nome di dominio completo del server ActiveSync. Se si utilizza uno Standalone Sentry, immettere invece il nome di dominio completo (FQDN). Esempio: mySentry.mycompany.com
Tipo di server	Selezionare il tipo di server di posta.
Nome utente	Usare le variabili per definire il nome utente dell'account e-mail.
Richiesta crittografia SSL	Selezionare questa opzione se si desidera una comunicazione protetta utilizzando https con il server specificato nel campo Host.
Considera attendibili tutti i certificati	Selezionare questa opzione solo se si desidera che i certificati non attendibili vengano automaticamente accettati dall'app. Solitamente, si seleziona questa opzione solo quando si lavora in un ambiente di test.
Firma e-mail predefinita	Immettere la firma e-mail predefinita per tutte le e-mail. L'utente finale può modificarla in qualsiasi momento. Quando l'utente del dispositivo la modifica, le modifiche successive a questo campo non saranno effettive.
Dimensione massima allegati e-mail	Immettere la dimensione massima da consentire per i file allegati.
Abilita attività	Selezionare questa opzione per sincronizzare le attività.
Alias certificato di accesso	Immettere l'alias del certificato di accesso.
Certificato per la firma Smime	Attualmente non supportato.
Alias certificato di crittografia Smime	Attualmente non supportato.
Opzioni avanzate	
Installa su dispositivo	Selezionare questa opzione per richiedere all'utente di installare l'app.
Installa in modo invisibile sui dispositivi Samsung Knox	Selezionare questa opzione per installare automaticamente l'app sui dispositivi Samsung Knox.

Impostazione	Operazione da eseguire
Non mostrare l'applicazione nell'App Catalog dell'utente finale	Selezionare questa opzione se non si desidera visualizzare l'app nel catalogo di applicazioni sul dispositivo.

11. Fare clic su **Fine**.

8.22. Configurazione dell'app Provisioner

Argomenti della sezione:

- Requisiti per il provisioning
- Abilitare Android Beam per l'utilizzo del trasferimento dati tramite NFC
- Eseguire il provisioning di un dispositivo di proprietà dell'azienda
- Registrare il dispositivo
- Verificare lo stato di registrazione del dispositivo

Provisioner è un'app Ivanti Neurons per MDM utilizzata per il provisioning di dispositivi posseduti dall'azienda, in modo che possano essere registrati come dispositivi gestiti per il lavoro e posizionati in modalità Proprietario dispositivo.

Un dispositivo gestito dall'azienda dispone solo di un profilo aziendale e di nessun profilo personale. L'amministratore può impostare oltre venti blocchi sul dispositivo, che possono limitarne le funzioni come fotocamera, chiamate, SMS, social network e molto altro.

L'applicazione Provisioner è necessaria al dispositivo che avvierà la configurazione del dispositivo di destinazione Android Enterprise con un bump NFC. Per effettuare il provisioning dei dispositivi di proprietà dell'azienda, installare l'app Provisioner su un dispositivo principale e utilizzare il trasferimento dati tramite NFC (Near Field Communication) per effettuare il provisioning dei nuovi dispositivi. Il trasferimento dei contenuti mette in comunicazione i due dispositivi. È possibile effettuare il provisioning dei dispositivi in modo che utilizzino una delle seguenti app client:

- Go da usare con Ivanti Neurons for MDM
- At Work UEM, un'app client senza marchio, da utilizzare con Ivanti Neurons for MDM .

Requisiti per il provisioning

Per eseguire il provisioning di un dispositivo Android Enterprise posseduto dall'azienda, in modo che diventi un dispositivo gestito per il lavoro:

- I dispositivi nativi Android Enterprise di proprietà dell'azienda devono essere resettati ai valori di fabbrica prima del provisioning.
- La configurazione di Android Enterprise deve essere definita e applicata al gruppo di dispositivi Android.
- Un dispositivo Android con funzionalità NFC selezionato come dispositivo principale o come modello con l'app Provisioner installata.
- Dispositivi Android Enterprise da fornire.
- App Provisioner
  Scaricare l'app Provisioner per Android da Google Play.

Abilitare Android Beam per l'utilizzo del trasferimento dati tramite NFC

Procedura

1. Dal dispositivo, andare a **Impostazioni**
2. Andare su **Wireless e reti** e fare clic su **Altro**.
3. Selezionare la casella di controllo **NFC**.
4. Fare clic su **Android Beam** e scorrere l'interruttore su **On**.

I passaggi esatti possono variare leggermente a seconda del dispositivo in uso.

Eseguire il provisioning di un dispositivo di proprietà dell'azienda

Procedura

1. Installare l'app Provisioner sul dispositivo da utilizzare come dispositivo Android principale.
2. Avviare l'app Provisioner sul dispositivo principale.
3. Selezionare un'app dal menu a discesa.
4. Immettere le informazioni richieste dall'app Provisioner. Nel caso in cui sia presente un tipo di Wi-Fi supportato, è possibile che alcuni campi vengano compilati in modo automatico. Utilizzare queste linee guida:

Campo	Valore
Selezionare l'app per il provisioning	Go (selezionare per l'uso con Ivanti Neurons for MDM) At Work UEM (app client senza marchio; selezionare per l'utilizzo con marchio Ivanti Neurons for MDM).
SSID rete Wi-Fi	Immettere l'SSID Wi-Fi che verrà utilizzato dal dispositivo principale.
Tipo di protezione Wi-Fi	Immettere il tipo di protezione Wi-Fi
Password Wi-Fi	Immettere la password per il Wi-Fi
Fuso orario	Immettere il fuso orario locale
Impostazioni locali	Immettere le impostazioni locali

5. Fare clic su **Continua**.
   Viene visualizzata la schermata **Trasferimento dati dei dispositivi** sul dispositivo principale.
6. Con il dispositivo di destinazione attivo e la schermata di benvenuto di Android visualizzata, avvicinare il dispositivo principale al dispositivo di destinazione per avviare il trasferimento dati tramite NFC.
   Se il trasferimento NFC avviene correttamente, è possibile che il dispositivo di destinazione emetta un suono; procedere quindi con il download dell'app client prescelta. Se il dispositivo non è crittografato, prima di avviare il download, viene avviato il processo di crittografia.
7. Continuare a effettuare il provisioning di altri dispositivi mediante il trasferimento dati dei dispositivi. È necessario che il dispositivo di destinazione visualizzi la schermata di benvenuto e che il dispositivo principale visualizzi la schermata **Trasferimento dati dei dispositivi**.

Registrare il dispositivo

Una volta effettuato il provisioning del dispositivo di proprietà dell'azienda eseguendo il trasferimento dati tramite NFC, viene installata l'app client selezionata. Avviare l'app client e registrare il dispositivo.

Verificare lo stato di registrazione del dispositivo

Procedura

1. Andare in **Dispositivi > Dispositivi**.

2. Fare clic sul collegamento di un dispositivo per visualizzarne i dettagli.
3. Lo stato del dispositivo viene elencato nel riquadro a sinistra.

8.23. Gestione delle applicazioni Windows

Gli utenti possono gestire (importazione, configurazione, pianificazione, distribuzione, aggiornamento e rimozione) il ciclo di vita completo delle app per le applicazioni Windows. I processi di distribuzione e aggiornamento delle app sono supportati attraverso la console MDM. Per ulteriori dettagli sulla gestione delle app di Windows e di altre applicazioni, vedere **Configurazione dell'app**, **Approfondimenti app** e **Catalogo app**.

Tipi di app supportate

- In-house (verificare le opzioni in **Aggiunta di un'app in-house** dalla sezione **Catalogo app**)
- MSB (Microsoft Store for Business integration)
- La regione del Microsoft Store pubblico (tramite integrazione Microsoft Store nativa) può essere impostata in App > Impostazioni catalogo. Per ulteriori informazioni, vedere **Aggiunta di un'app da uno store pubblico** dalla sezione **Catalogo app**.

Estensioni app supportate

- MSI
- MSIX
- APPX
- Bundle APPX
- EXE (via **Ivanti Bridge**)

Controllo app

La configurazione di Controllo app controlla l'installazione delle app per ogni dispositivo. Per ulteriori informazioni, consultare **Configurazione del controllo delle app: controllo delle app installate per dispositivo**.

Pacchetti e dipendenze

Sono disponibili le seguenti funzioni:

1. Le app Windows possono essere impostate come prerequisiti per tutti i tipi di applicazioni. Per informazioni su come impostare i prerequisiti delle app, vedere **Distribuzione di dipendenze delle app**.
2. APPX e i bundle APPX Dipendenze delle applicazioni e dipendenze degli altri pacchetti. Nella pagina **Visualizzazione dei dettagli delle app**, esaminare la sezione **Dipendenze app e altri pacchetti**.
3. Le app Win32 supportano la selezione del codice prodotto corretto (MSI) e delle righe di comando e variabili. Un elenco delle opzioni per le righe di comando comuni è disponibile **qui**.

Script

Gli script sono supportati mediante Ivanti Bridge Client. Per informazioni sulla configurazione degli Script, vedere il **Ivanti Bridge**

Una volta installato Ivanti Bridge sui dispositivi, gli script possono essere distribuiti come segue:

- A livello di dispositivo con gli script e le azioni tramite l'azione Ivanti Bridge
- Tramite la configurazione di Ivanti Bridge (andare su **Configurazioni** > **Bridge**)

La casella di controllo **Controlla versione esistente sul dispositivo**, disponibile nella scheda **Script e file** per gli applicativi interni MSI e EXE, controlla il modo in cui l'app si installa sui dispositivi Windows. Quando si abilita questa opzione, il dispositivo esegue un check-in per verificare se l'app è già installata e per identificarne la versione. Ivanti Neurons per MDM installa o aggiorna l'app solo se non è presente o se la versione installata è precedente alla versione richiesta. Se esiste la stessa versione o una versione più recente, l'installazione viene saltata. Questa opzione richiede che l'app sia installata su almeno un dispositivo prima di abilitarla.

Script e file di pre-installazione e post-installazione

Per i file .exe e .MSI

È possibile configurare gli script di installazione pre e post-PowerShell, gli script di registro e i file eseguibili (.exe) di Windows e scaricare altri tipi di file per le app Windows al livello Dettagli app.

Quando si aggiunge un nuovo script o file di pre o post installazione, viene visualizzata la schermata Ivanti Bridge. È possibile allegare lo script o il file, aggiungere argomenti allo script e fornire una posizione di destinazione per i file. Lo script di preinstallazione deve essere eseguito correttamente sul dispositivo prima di inviare il comando di installazione dell'app al dispositivo. Gli script e i file di pre e post installazione verranno eseguiti/installati nello stesso ordine in cui sono stati caricati nella console. Se il download o l'installazione dello script di preinstallazione non riesce, l'installazione dell'app non può proseguire.

Se lo script post-installazione non riesce, è possibile visualizzare gli errori nella pagina dei dettagli del dispositivo nella sezione Registri del dispositivo. Inoltre, non è possibile ripristinare gli script pre-installazione / i file scaricati e i file .exe installati nel caso in cui le azioni post-installazione non riescano.

È possibile riordinare gli script e i file pre-installati o post-installati utilizzando l'opzione Prioritizza script e file. Questa opzione sarà disponibile solo se sono disponibili almeno due o più script o file. Con questa opzione, è possibile trascinare i file o gli script all'interno delle rispettive sezioni pre o post, e non da una sezione all'altra.

Comportamento e configurazioni dell'installazione

Le applicazioni Windows supportano le seguenti funzioni:

- Installazioni invisibili all'utente
- **Pianificazione delle app Windows**
- Opzioni di riavvio

Per maggiori dettagli sulle opzioni di comportamento dell'installazione, vedere **Configurazione dell'app**

> Le app MSI e le app EXE (installate tramite Bridge) supportano le installazioni con sessioni MDM senza utente.

Ad esempio, negli scenari seguenti

- Il dispositivo è stato riavviato e nessun utente ha ancora effettuato l'accesso
- L'utente si è disconnesso dalla sessione di Windows
- Il dispositivo è stato registrato in modalità Autopilot senza utente (Distribuzione automatica o Provisioning automatico)
- Le applicazioni sono installate a livello di dispositivo

Consente di installare le app MSI in modo più efficiente, ad esempio durante la registrazione pilota automatico o durante la notte, quando nessuno lavora sul dispositivo Windows. Quando si utilizza il semplice repacking per gli EXE in MSI, è possibile installarli, ma non aggiornarli o eliminarli. Il vero pacchetto MSI è collegato a CSP. Altri tipi di applicazione verranno installati dopo l'accesso dell'utente.

Tunnel per Windows (VPN per app)

Tunnel è un'applicazione nativa stand-alone di Windows. È attualmente disponibile nel Microsoft Store per la distribuzione ai dispositivi. Crea una configurazione VPN per-app. È necessaria l'implementazione di Sentry. Per configurare l'app Tunnel, andare in **Configurazioni** > **+Aggiungi** > Cerca Tunnel (scegliere le configurazioni che supportano i dispositivi Windows). Selezionare il profilo Sentry e configurare le impostazioni per avviare il tunneling dei dati dell'app tramite Sentry. Per configurare un Server Sentry, andare in **Amministratore** > **Infrastruttura** > **Sentry**.

Inventario delle applicazioni

L'inventario delle applicazioni e dei software installati nel parco dispositivi Windows può essere monitorato a due livelli:

- Per controllare le applicazioni installate sui dispositivi, andare su **Dispositivi** > **Inventario app**
- Per controllare l'inventario a livello di dispositivo, andare su Dispositivi > scegliere un dispositivo > fare clic su App installate

Gli amministratori possono impostare gli intervalli di raccolta dell'inventario delle applicazioni Windows. Andare in Amministratore > Windows > Intervalli inventario app Gli intervalli sono utilizzati quando la configurazione della privacy è impostata per la raccolta di tutte le app dal dispositivo. Per configurare la Configurazione privacy, andare su Configurazioni > +Aggiungi > cercare Privacy > Scegliere Raccogli inventario app Per tutte le app sul dispositivo. Selezionare i tipi di app da raccogliere.

Catalogo app aziendale (Apps@Work)

I clienti possono abilitare un catalogo aziendale sui dispositivi Windows utilizzando Apps@Work. Apps@Work è disponibile e distribuito tramite il Catalogo app di Neurons for UEM. Per ulteriori informazioni, vedere **Apps@Work (iOS, Android, Windows e macOS)**.

8.24. Ivanti Bridge

Argomenti della sezione:

- Tipi di file supportati da Bridge
- Configurazione di Bridge
- Registri Bridge
- Ultimo check-in bridge
- Recupero errore servizio Bridge

Ivanti Bridge unifica le operazioni mobili e desktop per Windows 10 utilizzando un'unica console e un unico canale di comunicazione. Permette di estendere le capacità UEM di gestione dei PC e permette alle organizzazioni di beneficiare di una riduzione significativa dei costi e di una maggiore efficienza, assicurando al tempo stesso una protezione omogenea su PC e dispositivi mobili. Utilizzando Ivanti Bridge, le aziende hanno la possibilità di utilizzare un unico protocollo per i dispositivi Windows 10 Desktop come fanno per i dispositivi mobili Windows supportati, per inviare informazioni alle applicazioni legacy sul sistema operativo.

Ivanti Bridge consente all'IT di aggiornare le attività di Windows sulle soluzioni UEM senza rinunciare alle funzionalità essenziali Il reparto IT è in grado di applicare le policy e gli script già esistenti senza richiedere un'immagine dei sistemi, l'aggiunta a un dominio, o più canali di comunicazione al dispositivo.

Con Ivanti Bridge, le organizzazioni possono ora:

- Avere il controllo completo sui PC con UEM
- Gestire i PC da remoto e over-the-air
- Ridurre la necessità di effettuare l'imaging dei desktop
- Sfruttare i comandi basati su GPO con gli script PowerShell distribuiti da UEM
- Modificare e gestire facilmente il registro
- Distribuisce senza problemi le app Win32 non-MSI e le app Win32 Store
- Ottenere visibilità sul file system

> Ivanti Bridge è supportato su dispositivi Windows 11+ e processori ARM. Ivanti Bridge non supporta i dispositivi desktop Windows 10 Home.

Tipi di file supportati da Bridge

Ivanti Bridge supporta i seguenti tipi di file:

- PowerShell
  Gli script PowerShell inviati ai dispositivi utilizzando Bridge supportano gli argomenti denominati.
  Gli script PowerShell a 64 bit sono supportati sui dispositivi desktop Windows 10 a 64 bit.

> Il timeout del Bridge sul lato server per attendere un risultato dopo l'invio di uno script PowerShell al dispositivo è di circa 20 minuti. Il timeout viene registrato come Operazione non riuscita. Tuttavia, lo script sul dispositivo continua a funzionare.

> Il timeout Bridge sul lato dispositivo per attendere la procedura di esecuzione di uno script PowerShell è di circa 60 minuti. Dopo 60 minuti, il processo viene terminato, nessun output dallo script viene salvato, e un nuovo messaggio di Operazione non riuscita viene inviato al server.

> I timeout lato server e lato dispositivo vengono registrati come Operazioni non riuscite. Se, una volta trascorso il secondo timeout, lo script genera qualche output, nessun output viene registrato sul lato server.

Registro

- Script VB
- .EXE per la distribuzione di applicazioni Win32
- Le applicazioni di Win32 Store utilizzano lo strumento WinGet per installare e disinstallare le app.

> Se gli amministratori devono inviare file Win32 (.EXE) a un dispositivo (ad esempio, un'app interna di Windows), viene automaticamente utilizzata la funzionalità Bridge, se disponibile. È necessario immettere un argomento per eseguire il file in modo invisibile (ad esempio, /SILENT o /VERYSILENT).
> Le app EXE vengono installate tramite Bridge utilizzando la modalità PowerShell amministratore. Per i dispositivi Windows, installare utilizzando le credenziali dell'utente e selezionare l'opzione "Esegui come utente".

> Gli amministratori devono selezionare la casella di controllo **Esecuzione programma di installazione come utente** in **Programma di installazione app - Impostazioni** per installare le app per un utente. Non selezionare la casella di controllo se si desidera che le app vengano installate a livello di sistema.

Utilizzando Ivanti Bridge, il dispositivo può essere potenziato nelle seguenti aree chiave.

- **Registro:** lettura, scrittura e aggiornamento dei valori del registro.
- **File:** verifica, lettura e aggiornamento dei contenuti di un file.
- **Distribuzione dell'applicazione:** aggiunta della possibilità di installare applicazioni basate su file .EXE sul dispositivo desktop. Queste applicazioni possono risiedere sui server Ivanti Neurons for MDM o su una Content Delivery Network (CDN) nel cloud.

Configurazione di Bridge

L'impostazione di Ivanti Bridge richiede che gli amministratori completino i seguenti passaggi nell'ordine seguente:

1. **Attivazione delle licenze Bridge**
2. **Installazione dell'applicazione Bridge**
3. **Caricamento degli script sui dispositivi** per l'utilizzo singolo o permanente per i dispositivi

Attivazione delle licenze Bridge

Ivanti Bridge fa parte del pacchetto Gold e dell'attuale pacchetto Secure UEM.

Installazione dell'applicazione Bridge

Dopo aver attivato le licenze Ivanti Bridge, l'applicazione mobile Bridge può essere installata come segue:

1. Andare in **App > Catalogo app**.

2. Fare clic su **+Aggiungi**.
3. Fare clic su **Ivanti Bridge** nella sezione App business.
4. Aggiungere i dettagli, personalizzare e distribuire l'applicazione mobile Bridge sui dispositivi richiesti, in base alle licenze ottenute.
   Se è stata attivata l'opzione **Installa in modo invisibile sui dispositivi Windows**, l'applicazione mobile Bridge viene installata in modo invisibile ed eseguita nei dispositivi.

> L'app Bridge viene aggiunta all'App Catalog e distribuita a tutti i dispositivi per impostazione predefinita.

> Dopo aver importato l'ultima versione di Ivanti Bridge nel catalogo del tenant, l'amministratore può visualizzare la nuova versione allineata dell'app.

Caricamento degli script sui dispositivi

Gli amministratori possono caricare script sui dispositivi per utilizzarli in modo permanente creando una nuova configurazione di Bridge:

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la **Configurazione di Ivanti Bridge for Windows Scripts and Actions**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Nella sezione Configura Ivanti Bridge, utilizzare una delle due seguenti opzioni per caricare gli Script:
   - Selezionare gli script dalla Libreria script - Selezionare uno degli script disponibili dall'elenco.
   - Oppure
     Carica script - Specificare le impostazioni come descritto nella tabella al punto 7.
     - Immettere le impostazioni della categoria **File di script** per specificare uno script di installazione da inviare o eseguire sui dispositivi.
     - (Facoltativo) Immettere le impostazioni della categoria **Annullafile di script** per specificare lo script di disinstallazione da inviare o eseguire sui dispositivi. Questa impostazione è utile per scenari quali la disattivazione di un dispositivo o l'eliminazione di una configurazione.
     - (Facoltativo) Selezionare l'opzione **Configura Outlook** per configurare Microsoft Outlook su un dispositivo Bridge.

       > Supportato solo su Outlook 2010 e 2013.

Fare clic su **Avanti**.

7. Selezionare una distribuzione per la configurazione.
   Per queste azioni del dispositivo verrà eseguita automaticamente la forzatura del check-in.

Categoria	Impostazione	Operazione da eseguire
	Nome	Immettere un nome identificativo della configurazione.
	Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
File di script	**Tutte le versioni (desktop Windows 10 e versioni successive)**	
	File di script	Consente di selezionare uno script valido o un file eseguibile (.ps1, .reg, .exe). • Il file di script o il file eseguibile (.ps1, .reg, .exe) verranno eseguiti automaticamente. • Gli altri tipi di file verranno esclusivamente copiati nella cartella di destinazione.
	Argomenti dello script	Specificare l'elenco di argomenti per il file di script. • Per i file Win32 (.exe), immettere un argomento per eseguire in modo invisibile il file (ad esempio /SILENT o /VERYSILENT). È un'azione obbligatoria.
	Cartella di destinazione	Specificare la cartella di destinazione per il file di script. • Se non viene specificata la cartella di destinazione, verrà utilizzato il valore della variabile d'ambiente di sistema %TEMP%.
Annulla file di script	**Tutte le versioni (desktop Windows 10 e versioni successive)**	
	File di script	Consente di selezionare uno script valido o un file eseguibile (.ps1, .reg, .exe). • Il file di script o il file eseguibile (.ps1, .reg, .exe) verranno eseguiti automaticamente. • Gli altri tipi di file verranno esclusivamente copiati nella cartella di destinazione.
	Argomenti dello script	Specificare l'elenco di argomenti per il file di script. • Per i file Win32 (.exe), immettere un argomento per eseguire in modo invisibile il file (ad esempio /SILENT o /VERYSILENT). È un'azione obbligatoria.
	Cartella di destinazione	Specificare la cartella di destinazione per il file di script. • Se non viene specificata la cartella di destinazione, verrà utilizzato per impostazione predefinita il valore della variabile d'ambiente di sistema %TEMP%.

Caricamento degli script sui dispositivi per un unico utilizzo

Gli amministratori possono caricare uno script sui dispositivi per utilizzarlo una sola volta (ad hoc).

1. Andare in **Dispositivi > Dispositivi**.

2. Fare clic sul nome del dispositivo per andare alla pagina dei dettagli del dispositivo. Questo è un dispositivo desktop Windows 10 su cui verrà inviato/eseguito lo script per l'utilizzo unico.
3. Fare clic sull'icona ⋮ e fare clic su **Script e azioni tramite Ivanti Bridge**.
4. Immettere un nome.
5. Nella sezione File di script, specificare uno script da inviare/eseguire sul dispositivo come descritto nella tabella precedente.
6. Fare clic su **Applica**.
   L'esecuzione dello script verrà messa in coda e il completamento dell'operazione potrebbe richiedere tempo. Andare alla scheda Registri per controllare e visualizzare lo stato (messaggi inviati o non riusciti). Per queste azioni del dispositivo verrà eseguita automaticamente la forzatura del check-in.

Registri Bridge

Questa funzione consente di estrarre i registri di Ivanti Bridge per i singoli dispositivi per la risoluzione dei problemi e la diagnosi delle applicazioni. I registri vengono inviati al successivo check-in del dispositivo. È possibile attendere la prossima sincronizzazione programmata o eseguire un check-in forzato del dispositivo per ottenere rapidamente i registri.

Per eseguire il pull dei registri da un dispositivo:

1. Andare in **Dispositivi > Dispositivi**.
2. Fare clic sul nome del dispositivo per andare alla pagina dei dettagli del dispositivo. Questo è un dispositivo desktop Windows 10 su cui verrà inviato/eseguito lo script per l'utilizzo unico.
3. Fare clic sull'icona ⋮ e fare clic su **Estrai registro Ivanti Bridge**. Viene visualizzata la finestra **Estrai registro Ivanti Bridge**.
4. Selezionare una delle seguenti opzioni:
   Registro singolo - Richiede a Ivanti Neurons for MDM di eseguire il pull dell'ultimo registro di Bridge presente sul dispositivo.
   Tutti i registri - Richiede a Ivanti Neurons for MDM di eseguire il pull di tutti i registri di Bridge (fino a un massimo di 30 giorni) presenti sul dispositivo.
5. Fare clic su **Esegui pull del registro**. Dopo che un dispositivo lo ha inviato a Ivanti Neurons for MDM, il registro di Bridge può essere visualizzato nella scheda Registri nella pagina dei dettagli del dispositivo.

> Solo i registri inviati tramite l'opzione **Tutti i registri** possono essere scaricati solo come file zip.

Ultimo check-in bridge

La colonna Ultimo check-in Bridge elenca la data e l'ora dell'ultimo check-in del servizio Bridge sulla pagina Dispositivi. La colonna può essere aggiunta alla pagina Dispositivi usando l'opzione Personalizza colonne e non è visibile per impostazione predefinita.

Per rendere visibile questa colonna, selezionare **Dispositivi** > **Personalizza colonne** > quindi selezionare **Check-in bridge**.

> I dati esportati avranno anche i dettagli dell'ultimo Check-in Bridge, ove applicabile.

Recupero errore servizio Bridge

Il Bridge Service Failure Recovery è stato introdotto nella versione Bridge 2.1.14. Per impostazione predefinita, questa versione viene importata nel Catalogo app per tutti gli utenti. In alcuni casi rari, il servizio Bridge potrebbe presentare un errore senza un motivo apparente. In questi casi, il supporto è disponibile in Bridge 2.1.14 e versioni successive.

9. Contenuti

Utilizzare la pagina dei contenuti per distribuire contenuti ospitati da una fonte esterna. I contenuti includono file che gli utenti possono scaricare, come presentazioni di vendita, immagini, fogli di calcolo e documenti.

Argomenti della sezione:

- **Gestione di contenuti**
- **Categorie**

9.1. Gestione di contenuti

Argomenti della sezione:

- Distribuzione di contenuti su host
- Eliminazione di contenuti

La funzione Contenuti su host supporta la distribuzione di contenuti scaricabili con URL esterni. L'URL esterno deve indirizzare esclusivamente a un file PDF, EPUB o IBOOK scaricabile e deve avere queste estensioni.

La distribuzione di licenze VPP Book non è supportata, pertanto la distribuzione di Apple Books basata su ID iTunes Store non è supportata.

Per accedere a contenuti pubblicati da Ivanti Neurons for MDM, utilizzare l'app Books o Pages sul dispositivo. È possibile accedervi nella sezione Libreria.

È possibile distribuire i contenuti **iBook ed EPUB** sui dispositivi iPad con iOS 8 e versioni successive (licenza Gold). Questi formati sono limitati ai dispositivi iPad poiché Apple ne supporta la distribuzione in-house solo su iPad. Questa restrizione non si applica ai dispositivi con iOS 9.

> Per questi formati non sono disponibili le anteprime dei contenuti.

Per i contenuti **PDF**, è disponibile l'opzione di invio dei documenti all'app iBook sui dispositivi con iOS 8 o versioni successive.

Distribuzione di contenuti su host

Anche se non è possibile caricare nuovi documenti su Ivanti Neurons per MDM, è possibile fornire un percorso (URL) in cui il contenuto viene ospitato e distribuirlo ai gruppi di dispositivi.

Procedura

1. Andare a **Contenuto > Contenuto su host**.
2. Fare clic su **+ Aggiungi**.
3. Immettere le informazioni seguenti:
    - Titolo
    - Autore
    - Categoria
    - (Facoltativo) Descrizione
4. Nel campo **Percorso contenuto su host**, inserire un URL per il file da caricare.
5. Fare clic su **Avanti**.
6. Apportare le modifiche necessarie alla distribuzione.
7. Fare clic su **Fine**.

Per modificare il contenuto su host, eliminare il contenuto precedente, quindi aggiungere e distribuire il nuovo contenuto su host.

Per modificare le altre impostazioni:

1. Andare a **Contenuto > Contenuto su host**.

2. Fare clic sul collegamento al documento nella colonna **Nome**.
3. Fare clic sull'icona Modifica.
4. Apportare le modifiche necessarie.
5. Fare clic su **Avanti**.
6. Apportare le modifiche necessarie alla distribuzione.
7. Fare clic su **Fine**.

Eliminazione di contenuti

1. Fare clic sul collegamento al documento nella colonna **Nome**.
2. Selezionare **Azioni > Elimina questo documento**.
3. Fare clic sulla casella di controllo per confermare.
4. Fare clic su **Elimina documento**.

Quando si elimina un documento:

- Viene rimosso dal sistema.
- Non sarà più disponibile nel catalogo dei contenuti.
- Viene rimosso dai dispositivi su cui è stato scaricato.

Se non è possibile eseguire le attività indicate nella pagina **Contenuto**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario il seguente **ruolo**:

- Gestione app e contenuti

9.2. Categorie

Argomenti della sezione:

- Aggiunta di una categoria
- Rimozione di una categoria

> Nell'ambito della fine del supporto per il contenuto annunciata il 15 aprile 2017, è stata disattivata la possibilità di aggiungere nuovo contenuto. Il contenuto attualmente caricato può ancora essere distribuito nell'app Apple iBooks e utilizzato.

Le categorie descrivono i tipi di contenuto nel {{catalogo dei contenuti}}. Tramite le categorie, è possibile organizzare i contenuti per facilitarne la ricerca da parte degli utenti. A ciascun elemento aggiunto al catalogo dei contenuti deve essere assegnata almeno una categoria.

Aggiunta di una categoria

Procedura

1. Fare clic su **Aggiungi** (in basso a sinistra)
2. Digitare il nome della categoria. Per le categorie non viene fatta distinzione tra maiuscole e minuscole.
3. Fare clic su **Salva**.

Rimozione di una categoria

È possibile fare clic sulla X accanto alla categoria per rimuoverla.

Se non è possibile eseguire le attività indicate nella pagina **Contenuto (Contenuto)**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario il seguente ruolo:

- Gestione app e contenuti

10. Configurazioni

Le configurazioni sono delle raccolte di impostazioni inviate ai dispositivi. Ad esempio, è possibile utilizzare le configurazioni per specificare automaticamente le impostazioni VPN e i requisiti del passcode sui dispositivi. Le configurazioni esistenti del sistema in uso sono elencate nella pagina Configurazioni.

Argomenti della sezione:

- Utilizzo delle configurazioni
- Creazione di una configurazione del Portale self-service utente
- Configurazione personalizzata
- Invio di SyncML su dispositivi con configurazioni personalizzate
- Configurazione layout schermata principale
- Configurazione del controllo delle app: controllo delle app installate per dispositivo
- Configurazione delle notifiche app
- Esportazione di configurazioni
- Assegnazione della priorità alle configurazioni
- Gestione delle configurazioni

10.1. Utilizzo delle configurazioni

Argomenti della sezione:

- Applicazione di filtri alla visualizzazione di configurazioni
- Aggiunta di una configurazione
- Distribuzione della configurazione
- Distribuzione rollout lento delle configurazioni
- Invio di configurazioni a più dispositivi
- Esclusione di configurazioni
- Invio di una configurazione esclusa
- Esportazione di configurazioni
- Importazione di una configurazione
- Modifica di una configurazione
- Eliminazione di configurazioni
- Pianificazione di aggiornamenti di applicazioni interne
- Configurazioni Windows che richiedono una sessione utente attiva

Le configurazioni sono delle raccolte di impostazioni che l'utente in quanto amministratore invia ai dispositivi. Ad esempio, è possibile utilizzare le configurazioni per specificare automaticamente le impostazioni VPN e i requisiti del passcode sui dispositivi. Le configurazioni esistenti del sistema in uso sono elencate nella pagina Configurazioni. È possibile selezionare più configurazioni nella pagina Configurazioni e inviarle a più dispositivi contemporaneamente. Tali configurazioni possono essere spinte ai dispositivi specifici degli spazi e i dispositivi negli altri spazi non ne sono influenzati. Le configurazioni possono essere inviate a un singolo spazio, a più spazi o a tutti gli spazi alla volta.

Sono presenti numerosi tipi di configurazioni disponibili. Tali tipi di configurazioni si suddividono nelle categorie di base seguenti:

- Protezione
- risorse utenti
- Accesso alla rete aziendale
- Rete cellulare
- Altro (altre configurazioni)

Per la maggior parte delle configurazioni è possibile eseguire le azioni seguenti:

- aggiungere
- modifica
- clonare
- elimina
- escludere una o più configurazioni da un dispositivi specifico
- inviare una o più configurazioni escluse a un dispositivo specifico

Determinate configurazioni dispongono di azioni con restrizioni:

- Non è possibile aggiungere o clonare alcune configurazioni. Blocco attivazione iOS è un esempio di questo tipo di configurazione. Pertanto, queste configurazioni non compaiono tra i riquadri elencati quando si aggiunge una configurazione. Queste configurazioni sono elencate solo nella pagina Configurazioni.
- È impossibile modificare o eliminare le configurazioni definite dal sistema. SCEP per la registrazione iOS è un esempio di questo tipo di configurazione.
- È possibile contrassegnare alcune configurazioni perché non possono essere eliminate o reinstallate in un dispositivo. Non è possibile escludere o inviare queste configurazioni al dispositivo.

Applicazione di filtri alla visualizzazione di configurazioni

Nella pagina **Configurazioni**, sono elencate tutte le configurazioni. Per restringere questo elenco a determinate configurazioni, utilizzare i filtri (riquadro di sinistra) sotto SO e Tipo di configurazione. Ad esempio, per restringere l'elenco e visualizzare solo le configurazioni macOS, selezionare **mac OS** nella sezione **SO**.

È possibile visualizzare le configurazioni nei dispositivi con tutti o alcuni degli spazi, selezionando più spazi dall'elenco a discesa. Quando si passa con il mouse sopra le configurazioni visualizzate, viene visualizzata una finestra pop-up con un elenco degli spazi. È possibile fare clic su uno spazio per visualizzare la pagina dei dettagli della configurazione.

Applicare il filtro **Supportato** sotto **Apple DDM** per identificare facilmente le configurazioni legate al DDM e consentire una migliore differenziazione tra i tipi di configurazione.

Per cercare una configurazione esistente in base al nome, immettere il relativo nome nel campo **Cerca**.

A partire dalla versione 81 di Ivanti Neurons per MDM, gli amministratori globali possono delegare gli amministratori di spazi per modificare il certificato di identità generato dinamicamente per tutti i dispositivi e per l'opzione di distribuzione personalizzata.

Aggiunta di una configurazione

Questa opzione è abilitata solo se un singolo spazio è selezionato nell'elenco a discesa.

> È possibile distribuire al massimo 100 file di configurazione contemporaneamente.

Procedura

1. Fare clic su **Aggiungi**.
2. Selezionare il tipo di configurazione che si desidera creare.
3. Fare clic su **Avanti**.
4. Se non si desidera che questa configurazione venga abilitata immediatamente, deselezionare **l'opzione Abilita questa configurazione**.
5. Scegliere un livello di distribuzione per la configurazione:
    - **Tutti i dispositivi**: distribuire la configurazione a tutti i dispositivi disponibili. Per delegare le configurazioni tra gli spazi, selezionare una delle seguenti opzioni:
        - **Non applicare ad altri spazi**.
        - Per delegare le configurazioni tra gli spazi, selezionare **Riepilogo distribuzione** > **Applica a dispositivi in altri spazi**.
            - Selezionare la casella di controllo **Consenti all'amministratore dello spazio di modificare la distribuzione** per consentire agli amministratori dello spazio delegati di modificare la distribuzione per lo spazio specifico.
    - **Nessun dispositivo**: selezionare questa configurazione per eseguire la distribuzione in un secondo momento.

- **Personalizzato** - Consente di definire un insieme di dispositivi specifico a cui inviare la configurazione. Per delegare le configurazioni tra gli spazi, selezionare una delle seguenti opzioni:
  - **Non applicare ad altri spazi**.
  - **Riepilogo distribuzione** > **Applica a dispositivi in altri spazi**.
    - Selezionare la casella di controllo **Consenti all'amministratore dello spazio di modificare la distribuzione** per consentire agli amministratori dello spazio delegati di modificare la distribuzione per lo spazio specifico.

> L'amministratore può utilizzare l'opzione Distribuzione personalizzata per distribuire la configurazione personalizzata a dispositivi, gruppi di dispositivi, utenti e gruppi di utenti. L'assegnazione o la distribuzione di configurazioni a utenti e gruppi di utenti non è disponibile per le configurazioni seguenti:

  - Android Enterprise: Profilo di lavoro (Android for Work)
  - Android Enterprise: dispositivo di lavoro gestito (Android for Work)
  - Android Enterprise: dispositivo gestito con Profilo di lavoro/Profilo di lavoro su dispositivo di proprietà dell'azienda
  - Dispositivi Android di lavoro gestiti (proprietario del dispositivo) per dispositivi di lavoro gestiti in modalità non GMS (AOSP)

6. Se il servizio dispone di spazi definiti, specificare se la configurazione deve essere applicata agli altri spazi e la priorità.
7. Fare clic su **Fine**.

> Per le configurazioni che eseguono un comando al dispositivo anziché installare un profilo sul dispositivo, nei dettagli di configurazione non verrà elencata la configurazione applicata ai dispositivi.

Distribuzione della configurazione

Gli amministratori globali possono delegare gli amministratori di spazi per modificare il certificato di identità generato dinamicamente per tutti i dispositivi e per l'opzione di distribuzione personalizzata. Per i certificati generati dinamicamente, è facoltativamente possibile selezionare l'opzione **Consenti che questa configurazione sia disponibile in tutti gli spazi**. Questa opzione rende disponibili in tutti gli spazi i certificati di identità generati dinamicamente e può essere utilizzata in Exchange, Wi-Fi, VPN e qualsiasi altra configurazione applicabile, incluse le configurazioni di app gestite. Questa opzione può essere utilizzata negli scenari in cui il certificato di identità generato dinamicamente deve essere distribuito ai dispositivi (in spazi non predefiniti) solo come parte di configurazioni associate e non come configurazione individuale.

Procedura

1. Specificare i campi di impostazione utilizzando le informazioni specificate nella tabella per la singola configurazione, a seconda dei casi.
2. Fare clic su **Avanti**.
3. Selezionare l'opzione **Abilita questa configurazione**.
4. (Facoltativo) Selezionare **Consenti che questa configurazione sia disponibile in tutti gli spazi**.
5. Selezionare una delle seguenti opzioni di distribuzione:
   - **Tutti i dispositivi**. Selezionare una delle seguenti opzioni:
     - **Non applicare ad altri spazi**.
     - **Applica a dispositivi in altri spazi**.

        - **Applicare a tutti i dispositivi in altri spazi dispositivi come massima priorità**. (Questo vale solo per la configurazione Wi-Fi.)
        - **Applicare a tutti i dispositivi in altri spazi dispositivi come minima priorità**. (Questo vale solo per la configurazione Wi-Fi.)
            - Selezionare la casella di controllo **Consenti all'amministratore dello spazio di modificare la distribuzione** per consentire agli amministratori dello spazio delegati di modificare la distribuzione per lo spazio specifico.
    - **Nessun dispositivo** (impostazione predefinita)
    - **Personalizza** Selezionare una delle seguenti opzioni:
        - **Non applicare ad altri spazi**.
        - **Applica a dispositivi in altri spazi**.
        - **Applicare a tutti i dispositivi in altri spazi dispositivi come massima priorità**. (Questo vale solo per la configurazione Wi-Fi.)
        - **Applicare a tutti i dispositivi in altri spazi dispositivi come minima priorità**. (Questo vale solo per la configurazione Wi-Fi.)
            - Selezionare la casella di controllo **Consenti all'amministratore dello spazio di modificare la distribuzione** per consentire agli amministratori dello spazio delegati di modificare la distribuzione per lo spazio specifico.

> Indipendentemente dagli spazi, il certificato di identità generato dinamicamente può essere configurato in tutti gli spazi, distribuito su tutti i dispositivi e applicato a tutti i dispositivi in altri spazi di dispositivi.

6. Fare clic su **Fine**.

Distribuzione rollout lento delle configurazioni

Quando si distribuiscono le configurazioni utilizzando l'opzione **Personalizzata**, è possibile distribuire le configurazioni utilizzando il processo di Rollout lento, in modo che le configurazioni vengano distribuite in modo tempestivo. È possibile pianificare la distribuzione a rollout lento in modo manuale o pianificato.

> La distribuzione a rollout lento è attualmente supportata solo per configurazioni VPN e Wi-Fi.

Procedura

1. Andare in **Configurazioni** > **Aggiungi**.
2. Cercare la configurazione richiesta.
3. Immettere i dettagli come **Nome**, **Descrizione**, ecc. a seconda della configurazione e fare clic su **Avanti**.
4. Selezionare **Personalizza** come opzione di distribuzione. La sezione **Distribuzione rollout lento** viene visualizzata sullo schermo.
5. Selezionare **Usa metodo di distribuzione a rollout lento**. Sullo schermo vengono visualizzate le opzioni **Rollout manuale** e **Rollout pianificato**.
    - **Rollout manuale** - Utilizzando questa opzione, è possibile impostare manualmente la percentuale di destinazione di distribuzione. Sarà eseguita solo la percentuale di distribuzione specificata. In alternativa, è possibile selezionare **Tutti i dispositivi nel riepilogo di selezione** per distribuire la configurazione a tutti i dispositivi.
    - **Rollout pianificato** - Utilizzare questa opzione per distribuire la distribuzione in quattro fasi. Per ogni fase, è possibile specificare la percentuale di rollout, assicurandosi che ogni fase successiva abbia una percentuale superiore a quella

precedente. La durata tra le fasi deve essere di almeno un giorno e non può superare i 30 giorni. La configurazione salvata più di recente viene precaricata automaticamente come modello modificabile per le configurazioni future.

6. Selezionare i gruppi desiderati a cui distribuire la configurazione.
7. Fare clic su **Fine**.

È possibile visualizzare i dettagli da **Configurazioni** > Configurazione appena creata > **Dettagli**. Dalla pagina Dettagli, è possibile mettere in pausa e riprendere il rollout.

> Quando si crea una nuova configurazione con Rollout pianificato, le percentuali fornite durante la creazione della configurazione esistente vengono trasferite a quella nuova. È possibile modificare i dettagli o continuare con le stesse percentuali.

Invio di configurazioni a un dispositivo

Se si desidera reinstallare alcune delle configurazioni escluse su un dispositivo, è possibile inviare tali configurazioni.

Procedura

1. Andare in **Dispositivi** > **Dispositivi**.
2. Fare clic sul nome di un dispositivo per visualizzare la pagina dei dettagli.
3. Accedere a **Configurazioni**.
4. Selezionare le caselle di controllo per selezionare le configurazioni specifiche da inviare al dispositivo.
5. Fare clic su **Invia profili**.
6. Per inviare una singola configurazione, fare clic su **Invia** nella colonna **Azioni**.

Invio di configurazioni a più dispositivi

È possibile selezionare più configurazioni nella pagina Configurazioni e inviarle a più dispositivi contemporaneamente.

Procedura

1. Accedere al portale amministratore di Ivanti Neurons per MDM.
2. Accedere a **Configurazioni**.
3. Selezionare le caselle di controllo per selezionare configurazioni specifiche.
4. Fare clic su **Azioni**, quindi selezionare **Invia configurazioni selezionate** a dispositivi. La procedura guidata Invia configurazioni viene aperta e vengono visualizzate tutte le configurazioni e i relativi stati di invio.
5. Fare clic su **Invia configurazioni valide**. Le configurazioni vengono inviate in blocco a tutti i dispositivi. Le configurazioni escluse per dispositivi specifici dalla scheda **Dispositivi** > **Configurazioni** non vengono inviate.

Esclusione di configurazioni

È possibile rimuovere manualmente da un dispositivo alcune configurazioni distribuite in precedenza escludendole.

Procedura

1. Andare in **Dispositivi** > **Dispositivi**.
2. Fare clic sul nome di un dispositivo per visualizzare la pagina dei dettagli.
3. Accedere a **Configurazioni**.

4. Selezionare le caselle di controllo per selezionare configurazioni specifiche.
5. Fare clic su **Escludi profili**.

> Per escludere una singola configurazione, fare clic su **Escludi** nella colonna **Azioni**. Le configurazioni selezionate ora vengono indicate nella scheda Configurazioni escluse.

Invio di una configurazione esclusa

Procedura

1. Andare in **Dispositivi** > **Dispositivi**.
2. Fare clic sul nome di un dispositivo per visualizzare la pagina dei dettagli.
3. Andare a **Configurazioni** > **Configurazioni escluse**.
4. Selezionare una o più configurazioni da inviare al dispositivo.
5. Fare clic su **Invia profili**.
6. Per inviare una singola configurazione, fare clic su **Invia** nella colonna **Azioni**.

Esportazione di configurazioni

È possibile esportare i dettagli delle configurazioni selezionate o tutte le configurazioni dagli spazi selezionati a singoli file.

Procedura

1. Accedere a **Configurazioni**.
2. Selezionare le caselle di controllo per selezionare configurazioni specifiche.
3. Fare clic su **Azioni** > **Esporta configurazioni selezionate con dettagli**. Se si desidera esportare tutte le configurazioni, selezionare **Esporta tutte le configurazioni con dettagli**.
   Viene incluso un set di file YAML in un file .ZIP. Il report include i dettagli di tutte le configurazioni esistenti negli spazi selezionati.

Esportazione di tutte le configurazioni

Esportare i file di configurazione da inviare al supporto per utilizzarli come ausilio diagnostico. È possibile esportare un solo file di configurazione in un file di formato Yaml o tutte le configurazioni in un file zip. È possibile esportare file da diverse aree della pagina Configurazione a seconda delle configurazioni che si desidera esportare.

Procedura

1. Accedere a **Configurazioni**.
2. Selezionare le caselle di controllo per selezionare configurazioni specifiche.
3. Fare clic su **Azioni** > **Esporta configurazioni selezionate con dettagli**. Se si desidera esportare tutte le configurazioni, selezionare **Esporta tutte le configurazioni con dettagli**.
   Viene incluso un set di file YAML in un file .ZIP. Il report include i dettagli di tutte le configurazioni esistenti negli spazi selezionati.

Esportazione di una configurazione personalizzata

Procedura

1. Accedere a **Configurazioni**.

2. Fare clic su **+Aggiungi** per selezionare una configurazione.
3. Seguire i passaggi per personalizzare la configurazione.
4. Fare clic su **Avanti**.
5. Scegliere un livello di distribuzione.
6. Fare clic su **Fine**.
7. Selezionare la configurazione appena creata dall'elenco presente nella pagina **Configurazione**.
8. Fare clic sul menu a discesa **Azioni**, quindi su **Esporta.**

Sul dispositivo verrà scaricato un file con il nome della configurazione e gli attributi data e ora _aaaammgg.yaml.

Esportazione di una configurazione esistente

Procedura

1. Accedere a **Configurazioni**.
2. Selezionare una configurazione esistente.
3. Fare clic sul menu a discesa **Azioni**, quindi su **Esporta**.
   Verrà scaricato un file con il nome della configurazione e gli attributi data e ora _aaaammgg.yaml.

Importazione di una configurazione

È possibile importare un file YAML contenente i dettagli della configurazione. Per modificare una configurazione è possibile modificare i dettagli nel file YAML, selezionare una configurazione e importare il file e i valori aggiornati appaiono nella configurazione. Se è selezionata più di una configurazione o spazio, il pulsante Importa viene disabilitato. Se viene selezionato un tipo di file errato, appare un messaggio di errore. Se si seleziona un file YAML che contiene dettagli diversi da quelli richiesti per una configurazione, appare un messaggio di errore.

Procedura

1. Accedere a **Configurazioni**.
2. Selezionare una configurazione, fare clic su **Importa**, fare clic su **Scegli file**, selezionare il file YAML e fare clic su **Importa**. Viene importato il file YAML con i dettagli di configurazione.

Configurazioni supportate in white list

- 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 (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

Creazione di una configurazione usando un file YAML

È possibile creare una configurazione da un file YAML. Le specifiche relative alla distribuzione non fanno parte del file YAML. La distribuzione è impostata per impostazione predefinita su Nessun dispositivo.

Procedura

1. Accedere a **Configurazioni**.
2. Fare clic su **Importa**, fare clic su **Scegli file**, selezionare il file YAML e fare clic su **Importa**. Viene importato il file YAML con i dettagli di configurazione. La pagina Crea configurazione si apre mostrando tutti i dettagli aggiunti nel file YAML.
3. Selezionare *uno* dei tipi di distribuzione:
    - **Tutti i dispositivi**

- **Nessun dispositivo**
- **Personalizzato**

4. Verificare i dettagli della configurazione e selezionare *una* delle seguenti opzioni di riepilogo della distribuzione:

> Il riepilogo distribuzioni non è disponibile per tutte le configurazioni.

- **Non applicare ad altri spazi**
- **Applica ai dispositivi negli altri spazi**

5. Se il nuovo nome della configurazione corrisponde al nome di una configurazione esistente, appare un messaggio di errore, fare clic su **OK**, fare clic su **Indietro** e modificare il nome della configurazione.
6. Fare clic su **Avanti**, quindi su **Fine**.

Modifica di una configurazione

È possibile aprire una configurazione e modificare direttamente i dettagli di una configurazione, o importare un file YAML con tutti i dettagli necessari. Se è selezionata più di una configurazione o spazio, il pulsante Importa viene disabilitato.

Procedura

1. Accedere a **Configurazioni**.
2. Selezionare e aprire una configurazione, fare clic sull'icona di modifica (matita) e modificare la configurazione.
3. In alternativa, dalla pagina di modifica della configurazione fare clic sull'icona **Importa**, selezionare il file YAML e fare clic su **Importa**. La pagina Modifica configurazione si apre mostrando tutti i dettagli aggiunti nel file YAML.
4. Verificare i dettagli della configurazione e selezionare una delle seguenti opzioni di riepilogo della distribuzione:

> Il riepilogo distribuzioni non è disponibile per tutte le configurazioni.

- **Non applicare ad altri spazi**.
- **Applica ai dispositivi negli altri spazi**

  > La distribuzione è impostata per impostazione predefinita su Nessun dispositivo.

5. Fare clic su **Fine**.

Eliminazione di configurazioni

È possibile eliminare le configurazioni selezionate.

Procedura

1. Selezionare le caselle di controllo per selezionare configurazioni specifiche.
2. Fare clic su **Azioni** > **Elimina**.

Pianificazione di aggiornamenti di applicazioni interne

Ivanti Neurons per MDM aggiorna automaticamente le applicazioni interne quando un dispositivo effettua il check-in. Gli amministratori possono ora programmare gli aggiornamenti delle applicazioni interne in base al fuso orario del server. Gli aggiornamenti delle

applicazioni vengono completati solo se il check-in del dispositivo viene eseguito entro l'orario pianificato. Per impostazione predefinita, la pianificazione degli aggiornamenti delle applicazioni è disabilitata.

> Questa configurazione è applicabile solo per gli aggiornamenti e non per una nuova installazione. È possibile utilizzare il comando Invia installazione/aggiornamento per sostituire la pianificazione degli aggiornamenti automatici delle applicazioni iOS. Se l'aggiornamento automatico è abilitato a livello di app o di catalogo, avrà la precedenza sulla Configurazione programmata dell'app e l'app verrà aggiornata immediatamente al momento del check-in.

La configurazione è applicabile solo ai seguenti tipi di applicazione:

- Applicazioni iOS interne.
- Applicazioni Android interne solo in modalità DO.
- Applicazioni macOS nei formati .pkg e .MIP.
- Applicazioni Windows.

Prerequisiti

Assicurarsi che i seguenti prerequisiti siano soddisfatti affinché la configurazione funzioni come previsto:

- Per iOS e Android, l'applicazione deve essere gestita. Per macOS, l'applicazione può essere gestita o non gestita.
- Assicurarsi che l'opzione Installa su dispositivo in Configurazione applicazione sia abilitata.
- Il dispositivo deve essere sottoposto a check-in nell'orario pianificato.

Procedura

1. Accedere al portale amministratore di Ivanti Neurons per MDM.
2. Accedere a **Configurazioni**.
3. Fare clic su **Aggiungi**. Viene aperta la pagina Aggiungi configurazione.
4. Cercare **Aggiornamento automatico app**. Viene aperta la pagina Crea configurazione aggiornamento automatico app.
5. Specificare un nome nel campo **Nome**.
6. Nella sezione **Impostazioni di configurazione**, selezionare **Fuso orario** nell'elenco a discesa.
7. Selezionare l'**Ora di inizio** nell'elenco a discesa, quindi selezionare la **Durata** nell'elenco a discesa.
8. Fare clic su **Avanti**.
9. Selezionare l'utente richiesto e il gruppo di dispositivi, quindi fare clic sulla casella di controllo **Abilita questa configurazione**.
10. Fare clic su **Fine**. La configurazione viene applicata e l'applicazione ora verrà aggiornata solo nell'orario pianificato specificato.

Se non è possibile visualizzare la pagina Configurazioni, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei ruoli seguenti:

- Gestione dispositivi
- Dispositivo di sola lettura

Argomenti correlati:

- Spazi
- Assegnare priorità alle configurazioni

Configurazioni Windows che richiedono una sessione utente attiva

Alcune configurazioni di Windows richiedono una sessione utente attiva (un utente ha effettuato l'accesso al dispositivo) prima di poter eseguire il provisioning. Se nessun utente ha effettuato l'accesso, questa configurazione viene applicata dopo che un utente MDM ha effettuato l'accesso al dispositivo.

Le seguenti configurazioni richiedono una sessione utente attiva:

- Passcode
- Certificato utente (certificato di identità con ambito utente)
- Windows Firewall
- configurazione
- VPN
- Licenza Windows
- Microsoft Defender for Endpoint
- Impostazioni Windows (ambito utente)
- Configurazioni Bridge dipendenti dal servizio
- Applicazioni moderne/UWP

Configurazioni Bridge dipendenti dal servizio

Le configurazioni che richiedono il servizio Ivanti Bridge vengono fornite solo quando è disponibile una sessione utente attiva. Gli esempi includono le restrizioni di Windows Desktop, le impostazioni del browser, il menu Start, il Kiosk, il BIOS, gli script di Windows, GPO e altre configurazioni dipendenti dal servizio Bridge.

Eccezione: i seguenti script Bridge predefiniti non richiedono una sessione utente attiva e vengono inviati al dispositivo indipendentemente dal fatto che un utente MDM abbia effettuato l'accesso:

- get-device-data.ps1
- get-bitlocker-status.ps1
- device-hardware.ps1

Applicazioni moderne/UWP

Le applicazioni moderne/UWP vengono fornite solo quando è disponibile una sessione utente attiva. Ciò include:

- Applicazioni interne realizzate come .appx o .appxbundle
- Applicazioni Microsoft Store/UWP

Le applicazioni MSI ed EXE tradizionali non sono soggette a questo requisito.

> Se una sessione utente richiesta non è disponibile quando una configurazione è pianificata per la distribuzione, la configurazione viene fornita automaticamente dopo che un utente MDM accede al dispositivo.

10.2. Creazione di una configurazione del Portale self-service utente

In qualità di utente aziendale, è possibile utilizzare il Portale self-service per gestire dispositivi e certificati. La scheda Dispositivi personali visualizza i dispositivi registrati dall'utente.

Nella scheda Dispositivi personali, è possibile eseguire le seguenti attività:

- Blocca
- Sblocca
- Ritira
- Reimposta passcode app protette

Nella scheda Certificati personali, è possibile eseguire le seguenti attività:

- Carica certificato

> È possibile distribuire al massimo 100 file di configurazione contemporaneamente.

Procedura

1. Accedere al portale amministratore di Ivanti Neurons for MDM.
2. Fare clic su **Aggiungi**.
3. Cercare **Crea configurazione portale self-service utente**.
4. Fare clic su **Avanti**.
5. Se non si desidera che questa configurazione venga abilitata immediatamente, deselezionare **l'opzione Abilita questa configurazione**.
6. Scegliere un livello di distribuzione per la configurazione:
    - **Tutti i dispositivi**: distribuire la configurazione a tutti i dispositivi disponibili. Per delegare le configurazioni tra gli spazi, selezionare una delle seguenti opzioni:
        - **Non applicare ad altri spazi**.
        - Per delegare le configurazioni tra gli spazi, selezionare **Riepilogo distribuzione** > **Applica a dispositivi in altri spazi**.
            - Selezionare la casella di controllo **Consenti all'amministratore dello spazio di modificare la distribuzione** per consentire agli amministratori dello spazio delegati di modificare la distribuzione per lo spazio specifico.
    - **Nessun dispositivo**: selezionare questa configurazione per eseguire la distribuzione in un secondo momento.
    - **Personalizzato** - Consente di definire un insieme di dispositivi specifico a cui inviare la configurazione. Per delegare le configurazioni tra gli spazi, selezionare una delle seguenti opzioni:
        - **Non applicare ad altri spazi**.
        - **Riepilogo distribuzione** > **Applica a dispositivi in altri spazi**.
            - Selezionare la casella di controllo **Consenti all'amministratore dello spazio di modificare la distribuzione** per consentire agli amministratori dello spazio delegati di modificare la distribuzione per lo spazio specifico.
7. Se il servizio dispone di spazi definiti, specificare se la configurazione deve essere applicata agli altri spazi e la priorità.
8. Fare clic su **Fine**.

Per le configurazioni che eseguono un comando al dispositivo anziché installare un profilo sul dispositivo, nei dettagli di configurazione non verrà elencata la configurazione applicata ai dispositivi.

10.3. Configurazione personalizzata

Argomenti della sezione:

- Definizione di una configurazione personalizzata
- Impostazioni della configurazione personalizzata

Licenza: Silver

Applicabile a: iOS, macOS, tvOS, Android e Windows

Descrizione

Consente di importare e distribuire un file di configurazione predefinito.

I formati validi per i file di configurazione sono i seguenti:

Sistema operativo	Formati file di configurazione validi
iOS e tvOS	• .plist • .mobileconfig • .xml
macOS	• .plist • .mobileconfig
Android	.xml. Attualmente, questa funzionalità supporta solo file di configurazione .xml per dispositivi Zebra.
Windows	SyncML.

Definizione di una configurazione personalizzata

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare "personalizzata" nel campo di ricerca, quindi fare clic sulla configurazione **Personalizzata**.
   Viene visualizzata la pagina dei dettagli relativa alla configurazione personalizzata.
4. Configurare le impostazioni su questa pagina. Fare riferimento alla tabella presente nella sezione delle impostazioni della configurazione personalizzata per istruzioni sui valori.
5. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
6. (Dispositivi macOS) Selezionare un'opzione aggiuntiva per l'impostazione **A chi viene applicata questa configurazione?** a seconda del comportamento desiderato per la configurazione:
   - A livello di dispositivo (più comune).
   - Specifica dell'utente (utente registrato corrente).

Fare clic su **Fine**.

Impostazioni della configurazione personalizzata

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Scegli sistema operativo	Fare clic sull'icona di un sistema operativo per aggiornare il file di configurazione corrispondente.
Scegli file	Questa opzione viene visualizzata dopo avere selezionato un sistema operativo. Trascinare un file di configurazione nella casella di trascinamento e rilascio, oppure fare clic sul pulsante **Scegli file** per selezionare un file di configurazione.

Configurazione CSP personalizzata (solo Windows)

È possibile creare una configurazione CSP personalizzata solo sui dispositivi Windows. Quando si seleziona il sistema operativo Windows dalla sezione Scegli il sistema operativo, si ottengono due opzioni:

Opzione 1 - File XML CSP - Selezionare questa opzione e seguire la stessa procedura indicata per l'impostazione **Scegli file**.

Opzione 2 - Nodo Schema CSP OMA-URI personalizzato

Procedura

1. Selezionare l'opzione Nodo schema CSP OMA-URI personalizzato dall'elenco. Sullo schermo appare la sezione Configurazione CSP personalizzata.
2. In **AZIONI**, fare clic sul pulsante + per avviare la creazione della configurazione con diversi campi OMA-URI.
3. Sullo schermo viene visualizzata la finestra pop-up **Aggiungi riga** con i seguenti campi:
    - Descrizione - Inserire qualsiasi informazione generale sull'impostazione
    - OMA-URI - Inserire l'OMA-URI che si desidera utilizzare come impostazione
    - Tipo di dati - Selezionare un tipo di dati da utilizzare per questa impostazione: DATE, FLOAT, BASE64, NODE, XML, BINARY, CHARACTER, TIME, BOOLEAN, INTEGER
    - Valore - Immettere un valore associato al tipo di dati selezionato
    - Tipo di accesso - Aggiungi, Elimina, Esegui, Sostituisci, Ottieni

Fare clic su **Salva e Chiudi** per chiudere la finestra con i dati forniti. Fare clic su **Salva e Aggiungi** altro per creare una nuova riga.

5. Fare clic su **Avanti**.
6. Selezionare la modalità di distribuzione e fare clic su **Fatto**.

Argomenti correlati

- Invio di SyncML su dispositivi con configurazione personalizzata
- Come creare una configurazione

10.4. Invio di SyncML su dispositivi con configurazioni personalizzate

È possibile creare i propri file di configurazione Synchronization Markup Language (SyncML) oppure ottenerli da terzi per implementare le funzionalità personalizzate aggiungendoli a una configurazione personalizzata.

Piattaforme supportate:

- Windows

Dispositivi supportati:

- Windows 10 e versioni successive
- Microsoft HoloLens 2

Procedura

1. Accedere a **Configurazioni**.
2. Fare clic su **+Aggiungi**.
3. Fare clic su **Configurazione personalizzata** per visualizzare la pagina **Crea configurazione personalizzata**.
4. Immettere un nome per la configurazione.
5. Fare clic sull'icona del sistema operativo Windows.
6. Trascinare il file SyncML nell'interfaccia oppure fare clic su **Scegli file** per cercare il file da caricare nel dispositivo.

> Ivanti Neurons for MDM non effettua verifiche di convalida sul codice nel file.

7. Fare clic su **Avanti**.

Registro SyncML personalizzato

I comandi SyncML inviati al dispositivo Windows e le risposte SyncML a tali comandi da parte del dispositivo possono essere visualizzati nella scheda Registri dispositivo. Queste informazioni di registro saranno disponibili dopo l'invio della configurazione **SyncML personalizzata di Windows**. Quando il sistema invia una configurazione SyncML personalizzata, lo stato "Installato" è sempre presente nella scheda "Configurazione" del dispositivo, indipendentemente dalle risposte SyncML.

10.5. Configurazione layout schermata principale

La configurazione del layout della schermata Home definisce un layout di app, cartelle e clip Web per la schermata Home.

Argomenti della sezione:

- Definizione di una configurazione Layout schermata principale
- Impostazioni di configurazione Layout schermata principale

Licenza: Silver

Dispositivi idonei:

- Solo iOS 9.3 o versione successiva supervisionati
- solo tvOS supervisionati

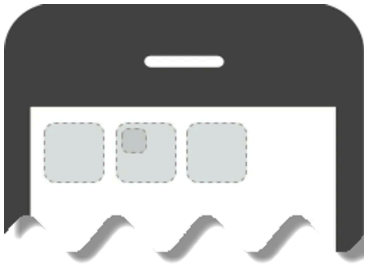
Definizione di una configurazione Layout schermata principale

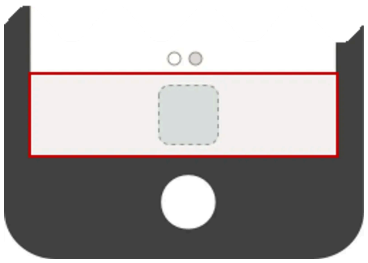
Procedura

1. Andare in **Configurazioni** > fare clic su **+ Aggiungi**.
2. Digitare "home" nel campo di ricerca, quindi fare clic sulla configurazione **Layout schermata home**. Si apre la pagina con i dettagli della Configurazione layout schermata principale.
3. Configurare le impostazioni su questa pagina. Fare riferimento alla tabella presente nella sezione Home_Screen_layout_Configuration_Settings per istruzioni sui valori.
4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione. Per i dispositivi iPad condivisi, selezionare il canale **Dispositivo** o il canale **Utente**. Per maggiori informazioni, vedere Utilizzo delle configurazioni.
5. Fare clic su **Fine**.

Impostazioni di configurazione Layout schermata principale

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Ancora	Fare clic sull'icona + per aggiungere un'app o un webclip al dock della schermata iniziale, come evidenziato qui, e seguire le indicazioni delle schermate successive: È possibile aggiungere manualmente app di sistema digitando l'ID bundle Apple (che inizia con 'com.apple'). Ad esempio, digitare "com.apple.DocumentsApp" per aggiungere l'app "File".
Pagina 1	Fare clic su ⊕ per aggiungere un'app o una clip Web all'area della pagina della schermata principale (qui evidenziata), quindi seguire le istruzioni nelle schermate successive: È possibile fare clic su Aggiungi pagina per aggiungere un'altra pagina al display del telefono.







10.6. Configurazione del controllo delle app: controllo delle app installate per dispositivo

La configurazione Controllo app consente di classificare le app come "consentite" o "non consentite" a livello di dispositivo. Le app già installate non saranno visibili e non potranno essere avviate. Le app saranno ancora visibili nell'App Store, ma non sarà possibile scaricarle o avviarle. Qualsiasi dispositivo a cui venga distribuita questa configurazione la utilizzerà e ignorerà le impostazioni della policy App consentite. Questa configurazione sostituirà le policy correlate alle app che si riferiscono alle stesse applicazioni sui dispositivi di destinazione.

Questa configurazione sostituirà le policy correlate alle app che si riferiscono alle stesse applicazioni sui dispositivi di destinazione. Per i dispositivi Windows 10, poiché le restrizioni si verificano a livello di dispositivo, la configurazione è l'unico modo per applicare le regole delle app.

La configurazione Controllo app permette di creare un:

- **Elenco app consentite**: consente solo le app aggiunte in modo esplicito all'elenco. Non sarà possibile installare altre app sui dispositivi.
- **Elenco app non consentite**: impedisce l'installazione di determinate app nei dispositivi.

Dispositivi supportati

È possibile utilizzare la configurazione Controllo app per inserire app diverse negli elenchi di app consentite o non consentite dei dispositivi seguenti:

- Profilo di lavoro Android su dispositivi di proprietà dell'azienda
- Solo iOS 9.3 o versione successiva supervisionati
- tvOS 11 e versioni successive
- Windows

Creazione della configurazione di Controllo app

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+Aggiungi**
3. Immettere **Controllo app** nel campo **Scegli configurazione** risultante, quindi selezionare la configurazione **Controllo app**.
4. Immettere un nome e una descrizione per la configurazione.
5. Selezionare un sistema operativo e passare alla sezione relativa al sistema operativo utilizzato.

Profilo di lavoro Android su dispositivi di proprietà dell'azienda

Gli utenti possono aggiungere fino a 50 ID applicazione agli elenchi delle app consentite o non consentite.

Procedura

1. Selezionare **Crea un elenco di app consentite per le app personali** o **Crea un elenco di app non consentite per le app personali**, al fine di aggiungere le applicazioni appropriate da inserire nell'elenco delle app consentite o non consentite.
2. Inserire l'ID applicazione (com.esempio.com) e fare clic su Aggiungi.

3. Fare clic su **Avanti** e scegliere un'opzione di distribuzione.
4. Fare clic su **Fine**.

Dispositivi iOS 9.3 supervisionati

Procedura

1. Scegliere se creare un elenco di app consentite o non consentite.
2. Fare clic su **Aggiungi app**.
3. Scegliere le app da consentire o non consentire, facendo clic su una o entrambe le schede seguenti:
   - Fare clic su **Aggiungi da ricerca** per cercare e scegliere le app dall'app Store o dall'App Catalog.
   - Fare clic su **Aggiungi manualmente** per scegliere le app immettendo l'ID pacchetto Apple (che inizia con "com.apple") solo per le app di sistema Apple.

Fare clic sulla scheda **Elenco app consentite** o **Elenco app non consentite** per esaminare l'elenco delle app selezionate come consentite o non consentite.

5. (Facoltativo) Selezionare l'opzione **Includi tutte le clip Web**.
6. Fare clic su **Avanti** e scegliere un'opzione di distribuzione.
7. Fare clic su **Fine**.

Dispositivi Windows

Procedura

1. Selezionare **Consentite** o **Non consentite** per aggiungere le applicazioni appropriate all'elenco delle app consentite o non consentite.
2. Nella sezione **Definizione regola**, selezionare il **Tipo di app** nell'elenco.
3. Immettere un nome identificatore nella casella **Identificatore app** per cercare un'app specifica. È inoltre possibile utilizzare il collegamento **Cerca app** per aprire una nuova finestra di dialogo e cercare identificatori di app specifiche di Windows.
4. (Opzionale) Immettere una descrizione dell'app nella casella **Descrizione app**.
5. Utilizzare il collegamento **+Aggiungi** per aggiungere ulteriori definizioni di regole con lo scopo di inserire le app nell'elenco delle app consentite o non consentite.
6. Fare clic su **Avanti** e scegliere un'opzione di distribuzione.
7. Fare clic su **Fine**.

10.7. Configurazione delle notifiche app

Consente di scegliere il modo in cui gli utenti ricevono le notifiche dalle app selezionate.

Valido per: dispositivi supervisionati con iOS 9.3 e versioni successive.

Creazione di una configurazione delle notifiche app

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare notifiche nel campo di ricerca, quindi fare clic sulla configurazione **Notifiche app**. Viene visualizzata la pagina Impostazione configurazione delle notifiche app.
4. Assegnare un nome e una descrizione alla configurazione.
5. Aggiungere app cercandole in App Store o manualmente immettendo l'ID bundle.
6. Scegliere un'app a cui associare le impostazioni relative alle notifiche app.
7. Configurare le impostazioni di notifica. Qui di seguito vengono riportate le notifiche che è possibile selezionare:
    - Consenti notifiche
        - Mostra in Centro notifiche
        - Suoni
        - Icona app Badge
        - Mostra su schermata di blocco
        - (Dispositivi supervisionati con IOS 12.0 e versioni successive) Mostra gli avvisi critici quando si utilizza CarPlay
        - (Dispositivi supervisionati con IOS 12.0 e versioni successive) Consenti agli avvisi critici di essere abilitati (ignorare "Non disturbare")
    - Sblocca stile avviso
        - Banner
        - Avviso modale
        - Nessuno
    - (Dispositivi supervisionati con IOS 12.0 e versioni successive) Tipo di raggruppamento
        - Automatico
        - Per app
        - Disattivato
    - (iOS 14.0 e versioni successive) Tipo di anteprima notifica - Consente di selezionare un tipo di anteprima per visualizzare l'anteprima dei messaggi di notifica nel dispositivo.
        - Controllato dall'utente - Mostra l'anteprima dei messaggi in base alle impostazioni dell'utente per le app sul dispositivo.
        - Sempre - Mostra l'anteprima dei messaggi.
        - Quando sbloccato - Mostra l'anteprima dei messaggi solo quando un dispositivo è sbloccato.
        - Mai - Impedisce che nelle app sia visualizzata l'anteprima dei messaggi in Notifiche.

8. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
9. Fare clic su **Fine**.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.8. Esportazione di configurazioni

Esportare i file di configurazione da inviare al supporto per utilizzarli come ausilio diagnostico. È possibile esportare un solo file di configurazione in un file di formato Yaml o tutte le configurazioni in un file zip.

Procedura

Esportazione delle configurazioni

È possibile esportare file da diverse aree della pagina Configurazione a seconda delle configurazioni che si desidera esportare.

Esportazione di tutte le configurazioni:

1. Accedere a **Configurazioni**.
2. Selezionare le caselle di controllo per selezionare configurazioni specifiche.
3. Fare clic su **Azioni** > **Esporta configurazioni selezionate con dettagli**. Se si desidera esportare tutte le configurazioni, selezionare **Esporta tutte le configurazioni con dettagli**.
   Viene incluso un set di file YAML in un file .ZIP. Il report include i dettagli di tutte le configurazioni esistenti negli spazi selezionati.

Esportazione di una configurazione personalizzata:

1. Accedere a **Configurazioni**.
2. Fare clic su **+Aggiungi** per selezionare una configurazione.
3. Seguire i passaggi per personalizzare la configurazione.
4. Fare clic su **Avanti**.
5. Scegliere un livello di distribuzione.
6. Fare clic su **Fine**.
7. Selezionare la configurazione appena creata dall'elenco presente nella pagina **Configurazione**.
8. Fare clic sul menu a discesa **Azioni**, quindi su **Esporta.**

Sul dispositivo verrà scaricato un file con il nome della configurazione e gli attributi data e ora _aaaammgg.yaml.

Esportazione di una configurazione esistente:

1. Accedere a **Configurazioni**.
2. Selezionare una configurazione esistente.
3. Fare clic sul menu a discesa **Azioni**, quindi su **Esporta**.
   Verrà scaricato un file con il nome della configurazione e gli attributi data e ora _aaaammgg.yaml.

10.9. Assegnazione della priorità alle configurazioni

Se si selezionano più gruppi di utenti per una configurazione, potrebbero venire assegnate più configurazioni dello stesso tipo a un dispositivo specifico. Se vengono applicate configurazioni dello stesso tipo allo stesso dispositivo, la priorità definita determina la configurazione applicata. La configurazione con la più alta priorità ha il numero minore. Per esempio, la configurazione con priorità 1001 ha una priorità più alta rispetto alla configurazione con priorità 1002. Il servizio assegna i numeri in modo automatico.

> La priorità Wi-Fi non può essere applicata al dispositivo ed è esente dalla priorità.

Questa opzione è disponibile solo se la pagina contiene due o più configurazioni dello stesso tipo e se un singolo spazio viene selezionato nel menu a discesa. È possibile modificare la priorità delle configurazioni.

Procedura

1. Accedere a **Configurazioni**.
2. Con nessuna configurazione selezionata, selezionare **Azioni > Definisci priorità configurazioni**.
   Se l'opzione **Azioni** non è visualizzata, significa che non sono disponibili più configurazioni di un tipo che necessita di priorità.
3. Utilizzare le frecce per spostare le configurazioni in modo tale che quella che deve avere la priorità più alta sia in cima.

> Un'icona a forma di lucchetto indica che non è possibile modificare la priorità della configurazione senza modificare l'impostazione di distribuzione Tutti i dispositivi all'interno della configurazione.

Fare clic su **Salva**.

> L'assegnazione della priorità può essere effettuata per un massimo di 400 configurazioni.

Se non è possibile visualizzare la pagina Configurazioni, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei ruoli seguenti:

- Gestione dispositivi
- Dispositivo di sola lettura

10.10. Gestione delle configurazioni

Argomenti della sezione:

- Configurazioni App Connect
- Configurazione di sicurezza
- Configurazioni delle risorse utenti
- Configurazione dell'accesso alla rete aziendale
- Cellulare
- Altra configurazione

10.10.1. Tipi di configurazione

Argomenti della sezione:

- Cerca una configurazione
- Protezione
- Risorse per gli utenti
- Accesso alla rete aziendale
- Rete dati
- Altre configurazioni
- Configurazione di sincronizzazione del dispositivo

Cerca una configurazione

Usare la funzionalità di ricerca e di filtro nella pagina **Scegli configurazioni** per trovare la configurazione da applicare.

Procedura

1. Scegliere **Configurazioni**.
2. Scegliere una delle configurazioni elencate o fare clic sul pulsante **+Aggiungi**.
3. Viene visualizzata la pagina **Scegli configurazione**
   Fare clic su una delle configurazioni elencate o :
   - Inserire il nome della configurazione nel campo di ricerca
   - Fare clic su un'icona filtro a destra del campo di ricerca per visualizzare i tipi di configurazione compatibili con la piattaforma.

Fare clic su un pulsante di configurazione per accedere alle opzioni di impostazione della configurazione.

Per maggiori informazioni, vedere Utilizzo delle configurazioni.

Protezione

Tipo	Funzioni	Per questi dispositivi	Licenza necessaria
Android Enterprise	Specifica le opzioni di Android Enterprise	Android Enterprise	Silver
Dispositivo AppConnect	Specifica le impostazioni di protezione sui dispositivi per le app con abilitazione AppConnect	• Android • iOS • macOS	Gold
Attestazione Apple PassKeys	Abilita l'attestazione enterprise WebAuthn per passkey specifici sui dispositivi Apple.		
Entra ID (Azure Tenant)	Collegando Ivanti Neurons for MDM a Entra ID, è possibile utilizzare lo stato di conformità dei dispositivi gestiti per l'accesso condizionato alle applicazioni di Microsoft 365.	• iOS • Android	• Per i nuovi clienti: Secure UEM Premium • Per i clienti esistenti: Platinum
Certificato	Stabilisce la fiducia con i server	• Android • iOS • macOS • watchOS • visionOS • tvOS	
Trasparenza certificato	Controlla l'applicazione della trasparenza certificato, che può apparire solo in un profilo dispositivo.	• iOS • macOS • tvOS • watchOS • visionOS	
Registrazione dispositivi	Recupera ulteriori registri, come quelli di rete e di sicurezza, dai dispositivi.	• Android Enterprise	
Configurazione gestione disco	Definisce i criteri di gestione dei dispositivi di archiviazione esterni e di rete.	• macOS 15.0+ supervisionato	
Cifratura Android	Chiede agli utenti di avviare la crittografia.	Android	
DNS cifrato	Permette di migliorare la sicurezza senza la necessità di configurare una VPN.	• iOS • macOS	Gold

Tipo	Funzioni	Per questi dispositivi	Licenza necessaria
		• visionOS	
Impostazioni Intelligence esterna	Consente integrazioni di intelligence esterna.	• iOS 26.4+ • macOS 26.4+ • VisionOS 26.4+	
Difesa dalle minacce per i dispositivi mobili	Protegge i dispositivi gestiti dalle minacce e vulnerabilità per dispositivi mobili che colpiscono dispositivi, reti e applicazioni.	• Android • iOS	
Azioni locali di Threat Defense	Creare e distribuire una configurazione dispositivo che definisce le azioni locali da eseguire sui dispositivi Android supportati quando il client abilitato per Threat Defense rileva una minaccia.	Android	
FileVault 2	Consente di eseguire la cifratura del disco XTS-AES 128 completa sui contenuti di un volume.	macOS	Gold
Chiave di ripristino di FileVault	Determina le impostazioni per il reindirizzamento delle chiavi di ripristino di FileVault in un server aziendale.	macOS	Gold
Certificato di identità	• Autentica il dispositivo sui server. • Autentica il dispositivo sulle risorse di rete.	• Android • iOS • macOS • watchOS • visionOS	
Blocco attivazione iOS	Abilita la funzionalità Blocco attivazione Apple sui dispositivi supervisionati.	iOS	Silver
Configurazione personalizzata iOS	Distribuisce un profilo di configurazione iOS creato da un'app diversa.	iOS	
Restrizioni iOS	• Blocca le funzionalità del dispositivo. • Abilita le funzionalità del dispositivo.	• iOS • watchOS • visionOS	
Impostazioni Intelligence	Consente le integrazioni di Apple Intelligence.	• iOS 26.4+ • macOS 26.4+	

Tipo	Funzioni	Per questi dispositivi	Licenza necessaria
		• VisionOS 26.4+	
Visualizzazione Sala conferenze	Attiva la modalità Visualizzazione Sala conferenze su Apple TV.	tvOS 10.2+	
Impostazioni tastiera	Consente di regolare come i dispositivi gestiscono il comportamento della tastiera, le opzioni di input e le relative impostazioni dell'esperienza utente.	• iOS 26.4+ • macOS 26.4+	
Blocco e tutto schermo: Android	• Blocca le funzionalità del dispositivo. • Riabilita le funzionalità del dispositivo. • Applica la funzionalità tutto schermo.	Android	
Blocco e tutto schermo: Android Enterprise	• Definisce quali funzionalità e app sono limitate sui dispositivi con Android enterprise. • Applica la funzionalità tutto schermo.	Android 5.0 +	
Blocco e tutto schermo: Samsung Knox Standard	• Definisce quali funzionalità e app sono limitate sui dispositivi Samsung Knox Standard. • Applica la funzionalità tutto schermo.	Samsung Knox	
Configurazione soluzione password amministratore locale	Consente agli amministratori di rigenerare automaticamente la password dell'amministratore locale sui dispositivi macOS gestiti a intervalli prestabiliti	macOS	
Firewall macOS	Gestisce le impostazioni del firewall applicazione, accessibili nel riquadro delle preferenze di sicurezza sui dispositivi macOS. L'amministratore può abilitare la modalità mascheramento specificando un dispositivo non rilevabile dal comando ping.	macOS 10.12+	Gold
Restrizioni di macOS	Determina quali restrizioni sono attivate sui dispositivi macOS.	macOS	Gold
Restrizioni dell'App Store di macOS	Consente di definire quali restrizioni sono abilitate nell'App Store di macOS.	macOS	Gold
Restrizioni della masterizzazione dischi in macOS	Consente di gestire le restrizioni della masterizzazione dischi in macOS.	macOS	Gold

Tipo	Funzioni	Per questi dispositivi	Licenza necessaria
Mobile@Work per macOS	Crea e distribuisce regole di esecuzione per Mobile@Work per macOS.	macOS	Gold
Script di Mobile@Work per macOS	Crea script da distribuire in Mobile@Work per macOS.	macOS	Gold
Preferenza identità	Consente di identificare una voce Preferenza identità nel portachiavi dell'utente che fa riferimento a un payload dell'identità incluso nello stesso profilo.	macOS	Gold
Preferenza certificato	Consente di identificare una voce Preferenza certificato nel portachiavi dell'utente che fa riferimento a un payload del certificato incluso nello stesso profilo.	• macOS	Gold
Controllo supporti multimediali consentito	Consente di configurare le opzioni di montaggio, smontaggio ed espulsione di supporti multimediali fisici.	macOS	Gold
Impostazioni Finder in macOS	Consente di gestire le impostazioni dell'app Finder in macOS.	macOS	Gold
Policy di estensione kernel di macOS	Controlla le restrizioni e le impostazioni per il caricamento delle estensioni del kernel approvate dagli utenti.	macOS	Gold
Active Directory (macOS)	Configurare le opzioni avanzate per associare i dispositivi macOS a un dominio Active Directory (AD) per accedere ai servizi software che si basano su AD per l'autenticazione e la sicurezza.	macOS	Gold
Creazione automatica dell'account Office 365 (macOS)	Configurare le informazioni utente e le opzioni per impostare la configurazione iniziale per tutte le applicazioni Microsoft Office 365.	macOS	Gold
Catalogo app Apple	Gestisce l'accesso al catalogo Apple App mediante una clip Web.	• iOS • macOS	
Domini gestiti	Specifica i domini e-mail e Web affidabili.	• iOS 8 e versioni successive	Silver

Tipo	Funzioni	Per questi dispositivi	Licenza necessaria
		• visionOS 1.1+	
Passcode	• Rende obbligatorio il passcode. • Specifica la lunghezza e il contenuto del passcode. • Modifica i requisiti del passcode.	• Android • iOS • macOS • watchOS	
Preferenze di privacy (macOS)	Configura le applicazioni che possono ottenere l'accesso ai servizi, ai file e alle risorse del sistema.	macOS	Gold
Autentica	Fornisce autenticazione senza password per i servizi cloud e/o gli accessi desktop.	• macOS • Windows	
Configurazione della privacy	Specifica quali dati di posizione vengono raccolti.	• iOS • Android • Windows	
Informazioni relative all'informativa sulla privacy del client	Mostra la politica sulla privacy all'utente nel client Go.	• Android • Android enterprise • iOS	
Impostazioni client Ivanti Go	Consente di eseguire la configurazione per raccogliere dati tramite Mixpanel, tra cui le informazioni sul dispositivo e l'utilizzo necessarie per risolvere i problemi e mantenere la migliore qualità dei servizi.	• iOS • macOS	
Configurazione impostazioni estensione Safari	Gestisce le estensioni del browser Safari da vari domini.	• iOS 18.0+ supervisionato • macOS 15.0+ supervisionato	
Impostazioni Siri	Consente di regolare come i dispositivi accedono e utilizzano le impostazioni Siri.	• iOS 26.4+ • macOS 26.4+ • watchOS 26.4+ • VisionOS 26.4+	

Tipo	Funzioni	Per questi dispositivi	Licenza necessaria
Configurazione servizi Configurazione file	Gli amministratori possono gestire e distribuire centralmente i file di configurazione per vari servizi di sistema.	macOS	
Aggiornamenti software	Crea e distribuisce ruoli per gli aggiornamenti del sistema operativo.	• iOS • macOS • Windows	
Configurazione impostazioni aggiornamento software	Crea e aggiorna le impostazioni di imposizione dell'aggiornamento software.	• iOS 18.0+ supervisionato • macOS 15.0+ supervisionato	
Server di riferimento orario	Consente ai dispositivi di connettersi ai server di riferimento orario personalizzati.	macOS	Gold
Filtro contenuto Web	Controlla i contenuti di Safari.	• Dispositivi con iOS 7 supervisionati • visionOS 1.1+	Silver
Windows_Firewall	La configurazione di Windows Firewall prevede diverse restrizioni del firewall. In base alle restrizioni del firewall applicate dall'amministratore, lo Stato del firewall risulterà in uno dei seguenti riportati nel riquadro Preferenze di sicurezza sui dispositivi Windows: • Il firewall è attivo e sta monitorando. • Il firewall è stato disabilitato. • Il firewall non sta monitorando tutte le reti o alcune regole sono state disattivate. • Il firewall non sta temporaneamente monitorando tutte le reti. • Non applicabile.	Windows 10 e versioni successive	
Protezione delle informazioni di Windows	Consente di definire le impostazioni di Protezione delle informazioni di Windows (WIP) per proteggere i dati aziendali.	Windows 10 e versioni successive	Gold

Tipo	Funzioni	Per questi dispositivi	Licenza necessaria
Restrizioni di Windows	Determina quali funzioni sono disponibili sui dispositivi Windows 10+.	Windows 10 e versioni successive	
Configurazione Gestione IA Windows	Consente di gestire le impostazioni e le configurazioni di IA di Windows.	Windows 10 e versioni successive	

Risorse per gli utenti

Tipo	Funzioni	Per questi dispositivi	Licenza necessaria
CalDAV	• Configura l'accesso al server CalDAV (come Google Calendar)	• iOS • visionOS	
CardDAV	• configura l'accesso a un server CardDAV (come Google Contacts)	• iOS • visionOS	
E-mail	• configura l'accesso per le e-mail POP/IMAP (ad esempio Gmail)	• iOS • visionOS	
configurazione	• configura l'accesso alle e-mail basate su ActiveSync (come Outlook) per i dispositivi mobili Android e iOS • configura le e-mail basate su Exchange Web Services (EWS) per i dispositivi macOS • definisce la quantità di dati da sincronizzare sul dispositivo • definisce la modalità di protezione delle e-mail	• Android • iOS • macOS • visionOS	• Exchange tramite Sentry non è supportato nei dispositivi macOS • Il contrassegno Sincronizza e-mail giorni passati non è applicabile ai dispositivi macOS
Google	• crea configurazioni dell'account Google per la connessione di dispositivi con sistema operativo iOS 9.3.2 e versioni successive ad account Google. • specifica quale app usare per effettuare chiamate ai contatti nel sistema Google.	• iOS • visionOS	
Carattere	• installa caratteri non standard necessari per la corretta visualizzazione dei documenti	• iOS	
Calendario sottoscritto	• configura una sottoscrizione a un calendario Internet	• iOS • visionOS	
Clip Web	• visualizza un collegamento (icona) a una pagina Web	• iOS • macOS	
Cache dei contenuti	• fornisce un servizio di creazione cache dei contenuti al fine di consentire copie locali del software App Store e • consente download di software e app più veloci per i client collegati.	• macOS	

Accesso alla rete aziendale

Tipo	Funzioni	Per questi dispositivi	Licenza necessaria
AirPlay	• configura l'accesso ai dispositivi alternativi per la visualizzazione dei contenuti multimediali	• iOS • macOS	Silver
AirPrint	• configura la stampa wireless	• iOS • macOS	Silver
VPN sempre attiva	• configura l'accesso al server VPN senza l'interazione dell'utente	• Android 7.0 e versioni successive • iOS 8 e versioni successive	• Gold per Android enterprise • Silver per iOS
Autorizzazioni di runtime delle app predefinite	• consente di impostare la configurazione delle autorizzazioni di runtime per le app distribuite sui dispositivi con Android enterprise.	• App che hanno come target le API Android 23 o versioni successive e che eseguono Android 6.0 o versioni successive su dispositivi con Android enterprise.	
Istruzione	• consente di configurare il payload di Apple Education e l'app Classroom per responsabili e membri	• supervised iOS 9.3+	Gold
Proxy globale	• configura i dispositivi per l'inoltro del traffico HTTP a un server proxy	• dispositivi con iOS 7 supervisionati • tvOS supervisionato	Silver
LDAP	• configura l'accesso a una directory aziendale	• iOS • visionOS	
Tunnel	• definisce una connessione VPN per app tra un client e Sentry utilizzando Tunnel	• iOS 7 e versioni successive • macOS 10.13+ • Windows 10 e versioni successive • Android	
Bridge	• consente all'IT di aggiornare le attività di Windows sulle soluzioni UEM senza rinunciare alle funzionalità essenziali	• Desktop Windows 10 e versioni successive	Licenza Bridge
Server macOS	• consente di definire l'account di un server macOS con tipi di account e impostazioni specifiche configurati. Consente all'utente di attivare Condivisione file sul server.	• iOS 10 e versioni successive	

Tipo	Funzioni	Per questi dispositivi	Licenza necessaria
VPN per-app	• configura le connessioni tra app specifiche e il server VPN	• iOS • watchOS • visionOS • tvOS	Silver
Configurazione relay di rete	• aggiunge la configurazione per definire le impostazioni dei relay di rete	• iOS • macOS • visionOS	
Single Sign-On	• configura l'accesso Single Sign-On per determinate app gestite	• iOS • macOS • visionOS	
Accesso sicuro multiutente	• imposta sicuro accesso multi-utente via web clip	• iOS	
VPN	• configura l'accesso al server VPN	• Android • Windows • iOS • macOS • visionOS • tvOS	
VPN on Demand	• configura l'accesso a un server VPN basato su domini, nomi host ecc.	• iOS	
Wi-Fi	• configura l'accesso a una rete wireless	• Android • Windows • iOS • macOS • watchOS • visionOS • tvOS	

Rete dati

Tipo	Funzioni	Per questi dispositivi	Licenza necessaria
APN	• configura il nome del punto di accesso cellulare del dispositivo	• iOS	
Cellulare	• configura l'accesso alla rete cellulare	• iOS • watchOS	
Configurazione della rete mobile privata	• imposta il payload per fornire informazioni sul dispositivo sulle distribuzioni di reti private	• iOS	
Configurazione delle impostazioni delle telecomunicazioni iOS	• imposta i valori predefiniti delle limitazioni roaming • imposta i valori predefiniti delle limitazioni dell'hotspot personale	• iOS	

Altre configurazioni

Tipo	Funzioni	Per questi dispositivi	Licenza necessaria
TV Apple	• definisce la lingua e le impostazioni locali per Apple TV	• dispositivi con iOS 7 supervisionati	Silver
Nome dispositivo predefinito	• definisce un nome dispositivo predefinito mediante le variabili	• dispositivi con iOS 8 supervisionati	Silver
Sfondo iOS	• installa una schermata principale e un blocco dello sfondo della schermata	• dispositivi con iOS 7 supervisionati	Silver
Sfondo macOS	• Installa una schermata principale e uno sfondo della schermata di blocco sui dispositivi. Gli sfondi distribuiti possono essere modificati dall'utente ma non possono essere rimossi da un dispositivo		Non richiesto
Impostazioni Assistente migrazione	Aiuta amministratori e utenti a trasferire dati, app e impostazioni durante la configurazione o la migrazione del dispositivo.	• macOS 26.4+	
Modalità App singola	• limita l'uso del dispositivo solo all'app specifica	• dispositivi con iOS 7 supervisionati • tvOS supervisionato	Silver
Configurazione dei domini associati	• La configurazione Domini associati è un dizionario che mappa le app ai loro domini associati. • I domini associati possono essere utilizzati con funzioni come Extensible AppSSO, collegamenti universali e Riempimento automatico password.	• macOS 10.15+	Gold
Configurazione delle impostazioni host per la Condivisione schermo	• Consente agli amministratori di esercitare un comando sicuro sulle funzionalità di condivisione dello schermo macOS su tutti i dispositivi gestiti.	• macOS 14+	

Configurazione di sincronizzazione del dispositivo

Le impostazioni di sincronizzazione del dispositivo forniscono un elenco di punti dati che è possibile monitorare sui dispositivi. Non è possibile modificare le configurazioni di sincronizzazione del dispositivo. È possibile visualizzare un elenco delle impostazioni controllate.

Procedura

1. Accedere a **Configurazioni**.
2. Fare clic su **Configurazione sincronizzazione dispositivi**. La scheda Dettagli della pagina **Configurazione sincronizzazione dispositivi** viene visualizzata con un elenco di voci selezionate.

Impostazioni	Tempo che intercorre tra le letture in minuti
Elenco dei certificati	
Informazioni sui dispositivi	60
Elenco di app installate	60
Elenco di app gestite	60
Elenco dei profili	60
Elenco dei profili di provisioning	60
Limitazioni	60
Informazioni di protezione	60
iOS9 e succ.	
Controlla aggiornamenti	1440

Argomenti correlati

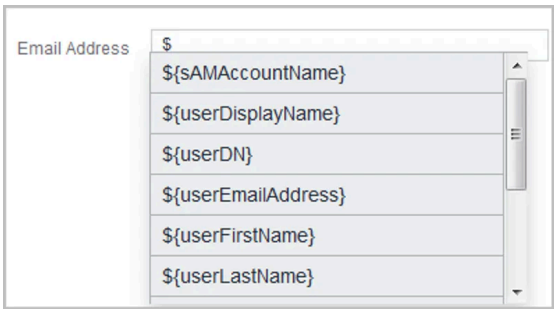
- Variabili
- Utilizzo delle configurazioni

10.10.2. Variabili

È possibile utilizzare le variabili in determinati campi di configurazione per la rappresentazione di valori specifici di un determinato utente. Se viene digitato il simbolo $ nei campi in grado di supportare le variabili, sarà possibile visualizzare un elenco delle variabili supportate. Argomenti della sezione:

Variabili account utente supportati

Variabili utente

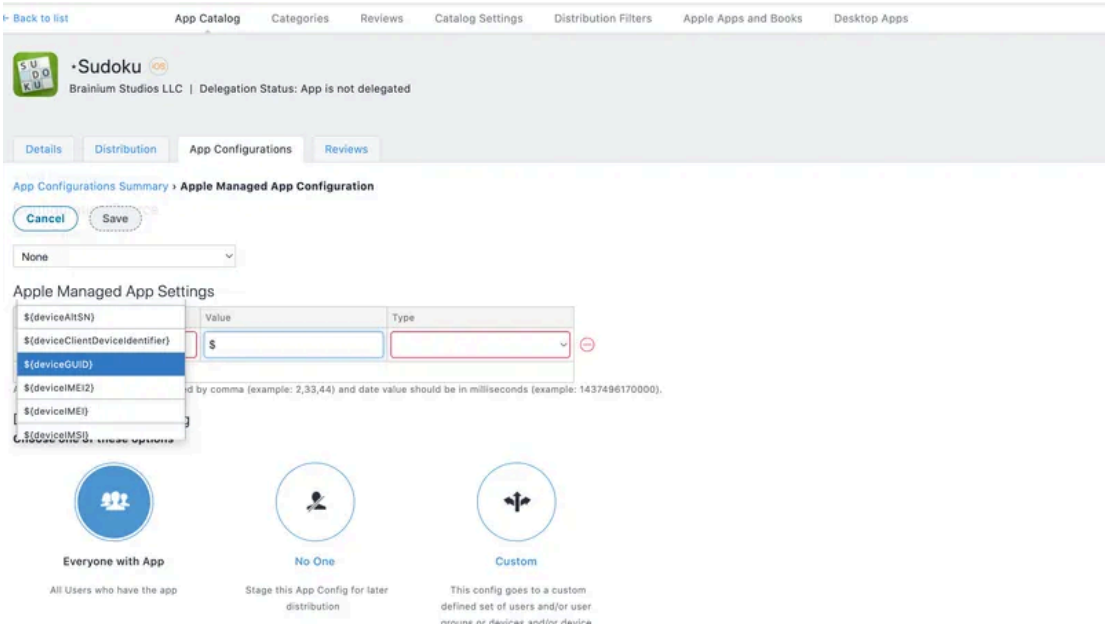


Chiave variabile	Descrizione valore
$	attributo reparto (richiede Entra ID)
$	Scambio elettronico di dati-Identificatore personale
$	ID Apple gestito dall'utente
$	Attributo sAMAccountName (richiede Active Directory)
$	Attributo Nome comune (CN) estratto dal nome distinto (richiede LDAP)
$	Nome visualizzato
$	Nome distinto (richiede LDAP)
$	La parte di dominio dell'indirizzo e-mail (la parte dopo '@')
$>	La parte locale dell'indirizzo e-mail (la parte prima di '@')
$	Indirizzo e-mail
$	Nome
$	Cognome
$	Impostazioni locali
$	Attributo Unità organizzativa (OU) estratto dal nome distinto (richiede LDAP)
$	Informazioni Kerberos Realm (richiede Active Directory)
$	La parte di dominio dell'ID login (la parte dopo '@')
$	La parte locale dell'ID login (la parte prima di '@')
$	ID login (formato indirizzo e-mail)
$	Attributo userPrincipalName (richiede Active Directory)

Variabili dispositivi supportati

Usare le variabili di dispositivo per specificare informazioni su un dispositivo mobile.

Variabili 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

Chiave variabile	Descrizione valore
$	Data ultimo check-in client (check-in più recente - MDM o Client)
$	Numero di serie alternativo
$	Identificatore utilizzato dall'applicazione client
$	Identificatore dispositivo globalmente univoco
$	ICCID
$	IMEI2
$	IMEI
$	IMSI
$	Data ultimo check-in dispositivo (check-in più recente - MDM o Client)
$	Identificatore dispositivo interno
$	Identificatore utilizzato per MDM
$	MEID
$	Modello
$	Nome dispositivo
$	Numero di telefono dispositivo
$	Identificatore dispositivo univoco cluster
$	Numero di serie
$	iOS UDID
$	Indirizzo MAC Wi-Fi

Variabili del modello di e-mail

Chiave variabile	Descrizione valore
$	Corpo e-mail
$	Oggetto e-mail

Variabili timestamp

Chiave variabile	Descrizione valore
$	Timestamp corrente (millisecondi dal periodo)

Variabili del modello di criteri

Chiave variabile	Descrizione valore
$	Nome criterio volato
$	Prossima azione conformità a livello (diversa da attendi e ritira) da intraprendere dopo l'invio del messaggio
$	Conteggio di giorni in cui il dispositivo è rimasto in uno stato di non conformità
$	Timestamp relativo alla prima attivazione della violazione del criterio (formato UTC GG-MM-AAAA)
$	Definizione regola (interroga la stringa nel modo in cui appare ora)

Argomenti correlati:

- Attributi

10.10.3. Configurazioni App Connect

Argomenti della sezione:

- Panoramica di AppConnect
- Passcode di AppConnect

10.10.3.1. Panoramica di AppConnect

AppConnect è una funzione di che consente di inserire le app in contenitori per proteggere i dati su dispositivi iOS e Android. Ogni app con abilitazione AppConnect diventa un contenitore sicuro con dati crittografati, protetti da accessi non autorizzati e rimovibili. Poiché ogni utente dispone di diverse app aziendali, ciascun contenitore di app è connesso anche ad altri contenitori sicuri di app. Questa connessione permette alle app con abilitazione AppConnect di condividere dati, come documenti. Ivanti Neurons for MDM utilizza le policy per gestire le app abilitate per AppConnect.

Per ulteriori informazioni su AppConnect e su come configurare e distribuire le app AppConnect, vedere la *Guida di AppConnect per Ivanti Neurons for MDM*.

Stato delle applicazioni protette

Dalla pagina **Dispositivi > Dispositivi** fare clic su un dispositivo per visualizzare la pagina **Panoramica**. Qui gli utenti possono controllare lo stato delle applicazioni protette con le seguenti informazioni:

- **Stato app sicure** - Indica se AppConnect è abilitato o disabilitato.
- **Stato cifratura app sicure** - Indica se il passcode di AppConnect è abilitato o disabilitato.
- **Modalità cifratura app sicure** - Indica la modalità di cifratura (ad esempio AES 256).

Inoltre, questi campi possono essere utilizzati nei seguenti modi:

- Come filtri (riquadro a sinistra) per restringere le voci relative ai dispositivi, visualizzate quando gli utenti tentano di trovare/applicare filtri ai dispositivi.
- Come regole durante la creazione di un gruppo di dispositivi gestiti dinamicamente.
- Come filtri di distribuzione che limitano ulteriormente i dispositivi su cui verranno distribuite le app in base a regole definite.

Per ogni app sicura, gli amministratori possono controllare lo stato della configurazione e dei criteri del contenitore (Installato, Applicato, Inviato o Installazione in sospeso) nella scheda **Configurazioni** della pagina relativa ai dettagli dei dispositivi.

10.10.3.2. Passcode di AppConnect

Argomenti della sezione:

- Modifica/reimpostazione del passcode
- Generazione di un PIN monouso per reimpostare un passcode delle app sicure per dispositivi iOS

È possibile richiedere un passcode di AppConnect, chiamato anche passcode delle app sicure. Effettuando un unico accesso con il passcode di AppConnect, l'utente del dispositivo può accedere a tutte le app protette. È possibile configurare le regole per il passcode di AppConnect sul portale Amministratori. Il passcode di AppConnect non è lo stesso passcode utilizzato per sbloccare il dispositivo.

Modifica/reimpostazione del passcode

Gli utenti possono modificare o reimpostare il passcode delle app sicure nell'app Secure Apps Manager per i dispositivi Android e nell'app Go per iOS, a condizione che sia stato consentito nella configurazione AppConnect. Per i dispositivi iOS:

Procedura

1. Aprire l'app Go per iOS.
2. Fare clic su **App sicure**.
3. Fare clic su **Autenticazione**.
4. Fare clic su **Modifica passcode delle app sicure** e seguire le istruzioni per modificare/reimpostare il passcode.

Per dispositivi Android:

1. Aprire l'app Secure Apps Manager.
2. Fare clic su **Modifica passcode** nel menu opzioni.
3. Fare clic su **Password dimenticata** per reimpostare il passcode.

Generazione di un PIN monouso per reimpostare un passcode delle app sicure per dispositivi iOS

Gli amministratori possono configurare Ivanti Neurons for MDM in modo da consentire agli utenti di dispositivi iOS di reimpostare il proprio passcode delle app sicure (AppConnect) nel caso l'abbiano dimenticato. Se questa opzione è configurata, gli utenti dei dispositivi registrati su Ivanti Neurons for MDM tramite un nome utente e una password possono immettere tali credenziali in Go 3.1.0 per iOS, o in una versione successiva supportata, per autenticarsi e reimpostare il proprio passcode delle app sicure. Tuttavia, gli utenti dei dispositivi che hanno dimenticato la password e il PIN devono autenticarsi seguendo un'altra procedura.

Procedura

1. In Ivanti Neurons for MDM, l'amministratore attiva l'opzione **Passcode delle app sicure** nella Configurazione predefinita AppConnect per iOS (o in qualsiasi altra configurazione AppConnect per iOS).
2. L'utente genera un PIN usa e getta per un dispositivo iOS specifico sul portale self-service degli utenti facendo clic sull'opzione **Reimposta passcode delle app sicure** e seguendo le istruzioni. Il PIN usa e getta è valido per 30 minuti.
3. In Go per iOS su un dispositivo, l'utente segue le istruzioni per reimpostare un passcode delle app sicure dimenticato.
4. Quando richiesto, l'utente immette il suo nome utente e il PIN usa e getta, invece del normale passcode.
5. L'utente reimposta il proprio passcode delle app protette.

10.10.4. Configurazione di sicurezza

Argomenti della sezione:

- Android Enterprise
- Modifica della configurazione predefinita di Android Enterprise
- Configurazione di Android Enterprise
- Richiesta di verifica di Android Work
- Configurazione dei certificati
- Trasparenza certificato
- Configurazione della verifica della revoca dei certificati
- Crea Configurazione modalità autonoma Single App
- Creazione della configurazione del proxy DNS
- Configurazione registrazione dispositivo
- Configurazione gestione disco
- Cifratura Android
- DNS cifrato
- Impostazioni Intelligence esterna
- Difesa dalle minacce
- FileVault 2
- Chiave di ripristino di FileVault
- Configurazione Opzioni FileVault
- Certificato di identità
- Configurazione blocco attivazione Apple
- Configurazione personalizzata iOS
- Impostazioni Intelligence
- Impostazioni tastiera
- Restrizioni iOS
- Visualizzazione Sala conferenze
- Blocco e tutto schermo: modalità di amministrazione del dispositivo Android
- Configurazione della modalità tutto schermo per Android
- Configurazione di tutto schermo per dispositivi Android condivisi
- Blocco e tutto schermo: Android Enterprise
- Blocco e tutto schermo: Samsung Knox Standard
- Firewall macOS
- Restrizioni di macOS
- Restrizioni dell'App Store di macOS
- Restrizioni della masterizzazione dischi in macOS

- Controllo supporti multimediali consentito (deprecato)
- Impostazioni Finder in macOS
- Policy di estensione kernel di macOS
- Mobile@Work per macOS
- Configurazione delle regole di aggiornamento del software macOS
- Preferenza certificato
- Active Directory (macOS)
- Preferenza identità
- Creazione automatica dell'account Office 365 (macOS)
- Autentica
- Catalogo app Apple
- Domini gestiti
- Impostazioni passcode
- Preferenze di privacy (macOS)
- Impostazioni client Ivanti Go
- Configurazione della privacy
- Informazioni relative all'informativa sulla privacy del client
- Configurazione impostazioni estensione Safari
- Aggiornamenti software
- Configurazione impostazioni aggiornamento software
- Configurazione delle preferenze di sicurezza
- Impostazioni Siri
- Server di riferimento orario
- Filtro contenuto Web
- Windows Firewall
- Protezione delle informazioni di Windows
- Restrizioni di Windows
- Restrizioni del desktop Windows
- Impostazioni desktop per Windows 10
- Configurazione di Windows Hello for Business
- Configurazione Gestione IA Windows
- Play Integrity (in precedenza SafetyNet Attestation)
- Passcode avanzato Android e schermata di blocco
- Microsoft Defender for Endpoint
- Autenticazione basata su certificati

10.10.4.1. Android Enterprise

Licenza: Silver

Una configurazione Android Enterprise definisce le opzioni **Android Enterprise** abilitate per i dispositivi supportati. È possibile creare configurazioni alternative per diversi gruppi di dispositivi o semplicemente modificare la configurazione predefinita. Per un elenco dei dispositivi che supportano Android Enterprise, consultare la pagina ufficiale di **Android**.

Impostazioni di Android Enterprise

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Disattiva Acquisizione schermo (Android 5.0 e versioni successive)	Selezionare questa opzione per impedire al dispositivo di utilizzare la funzionalità nativa di acquisizione schermo.
Disabilita controllo app (Android 5.0 +)	Selezionare questa opzione per impedire agli utenti di modificare le app nelle Impostazioni o nelle Utilità di avvio.
Non consentire Credenziali config (Android 5.0 +)	Selezionare questa opzione per impedire agli utenti di configurare le credenziali degli utenti.
Non consentire Copia/Incolla tra profili (Android 5.0 +)	Selezionare questa opzione per impedire ai dispositivi di effettuare copia e incolla su altri profili di lavoro di Android Enterprise.
Non consentire Modifica account (Android 5.0 +)	Selezionare questa opzione per impedire agli utenti di aggiungere e rimuovere gli account.
Non consentire Beam in uscita (Android 5.0 e versioni successive)	Selezionare questa opzione per impedire a un utente di utilizzare NFC per trasferire i dati delle app.
Non consentire Condividi la posizione (Android 5.0 +)	Selezionare questa opzione per impedire ai siti Web e alle app di richiedere all'utente del dispositivo di condividere la posizione.
Limita metodi di input (Android 5.0+)	Selezionare questa opzione per limitare i metodi di input, indicando un elenco di nomi di Pacchetti consentiti. In mancanza di pacchetti consentiti vengono autorizzati solo i metodi di input del sistema. I metodi di input non si limitano unicamente alle app aziendali, ma all'intero dispositivo.
Limita servizi di accessibilità (Android 5.0 e versioni successive)	Selezionare questa opzione per limitare i metodi di input, indicando un elenco di nomi di Pacchetti consentiti. In mancanza di pacchetti consentiti vengono autorizzati solo i servizi di accessibilità del sistema. I metodi di input non si limitano unicamente alle app aziendali, ma all'intero dispositivo.
Disabilita ID chiamante (Android 6.0 e versioni successive)	Consente di scegliere se visualizzare sul dispositivo le informazioni dell'ID chiamante del profilo di lavoro per le chiamate in entrata.

Argomenti correlati

- Configurazione di Android Enterprise

10.10.4.2. Attestazione Apple PassKeys

Utilizzare la configurazione Attestazione Passkey per configurare il dispositivo in modo da consentire l'attestazione enterprise WebAuthn per determinate passkey.

Quando l'utente utilizza una Passkey per l'autenticazione e la registrazione dei propri dispositivi, la configurazione Apple Passkey Attestation utilizza una Credenziale gestita a livello enterprise per attestare la Passkey con un certificato aziendale. Le credenziali supportate sono SCEP, ACME e Identity.

L'Attestazione Passkey supporta quanto segue:

- Versioni minime del sistema operativo supportate: macOS 14
- Metodi di registrazione supportati: Registrazione del dispositivo
- Gli account Apple gestiti sono necessari per controllare la sincronizzazione delle passkey.
- Può essere utilizzato in combinazione con la Gestione accessi di ABM.

> Il payload di Passkeys non funziona su Mac.

Quando si crea una configurazione Passkey, è necessario creare prima una configurazione di certificati di identità e collegarla alla configurazione Passkey. Inoltre, fornire i seguenti dettagli nella sezione Configurazione dell'attestazione Passkey sicurezza:

Campo	Descrizione
Nome	Nome della passkey.
Descrizione	Qualsiasi informazione sulla configurazione.
Riferimento asset identità attestazione • La chiave di attestazione dell'identità è estraibile	Fornire l'identità di riferimento dell'asset creata da collegare alla configurazione Passkey. Selezionare questa opzione per confermare se la chiave di identità è estraibile.
Parti fidate	Immettere i dettagli per i domini autenticati.

10.10.4.3. Impostazioni predefinite privacy app

Utilizzare le **Impostazioni predefinite privacy app** per definire i diritti di privacy predefiniti per le app sui dispositivi supervisionati. Gli amministratori possono identificare i componenti di privacy utilizzati da un'app, elencare l'app e i suoi componenti nella configurazione e impostare i valori predefiniti di privacy. Quando si avvia l'app, l'app controlla i valori predefiniti di privacy configurati e richiede all'utente di concedere le autorizzazioni, consentendogli al contempo di differire o gestire le autorizzazioni in un secondo momento nelle impostazioni del dispositivo.

Applicabile a:

- iOS 27.0+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.
- iPad 27.0+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.
- macOS 27.0+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Impostazioni predefinite privacy app**.
3. Nel campo **Nome**, immettere un nome che identifica questa configurazione.
4. Nel campo **Descrizione**, inserire una descrizione che chiarisca lo scopo di questa configurazione.
5. Nel riquadro **Impostazioni configurazione**, selezionare **Aggiungi per ricerca**.
6. Immettere il nome dell'app per la quale si desidera impostare i **valori predefiniti privacy app** selezionando una delle seguenti opzioni:

- iOS Store
- Catalogo app
- visionOS Store
- OS X Store (macOS)

> È possibile selezionare più app.

7. (Facoltativo) Selezionare **Aggiungi manualmente** per selezionare un'app.
8. (Facoltativo) Immettere il **Nome pacchetto** dell'app.
9. (Facoltativo) Fare clic su **Aggiungi app**.
10. Selezionare **Visualizza app**.

Il riquadro **Visualizza app** elenca tutte le app selezionate.

11. Fare clic su **Aggiungi impostazioni predefinite** su ciascuna applicazione per impostare individualmente le impostazioni predefinite sulla privacy dell'app.

Viene visualizzato il riquadro **Aggiungi impostazioni predefinite**.

12. Selezionare le **Impostazioni predefinite** e le **Restrizioni** in base alla tabella seguente:

Predefiniti	Imposta limitazioni
Fotocamera	Selezionare una delle seguenti opzioni: • Consenti • Nessuno
Bluetooth	Selezionare una delle seguenti opzioni: • Consenti • Nessuno
Accessibilità	Selezionare una delle seguenti opzioni: • Consenti • Nessuno
Dettatura	Selezionare una delle seguenti opzioni: • Consenti • Nessuno
Microfono	Selezionare una delle seguenti opzioni: • Consenti • Nessuno
Posizione	Selezionare una delle seguenti opzioni: • Durante l'utilizzo • Nessuno • Sempre
Accuratezza posizione	Selezionare una delle seguenti opzioni: • Approssimativo • Precisione • Nessuno
Rete locale	Selezionare una delle seguenti opzioni: • Consenti • Nessuno
Giustificazione organizzazione	Il prompt **Giustificazione organizzazione** può visualizzare il nome dell'organizzazione, il nome dell'app, la giustificazione fornita dall'amministratore e i dettagli per ciascun componente con un'impostazione predefinita di privacy consigliata. Se l'utente seleziona **Consenti**, il sistema si applica alle impostazioni predefinite sulla privacy consigliate. Se l'utente seleziona **Non ora**, i prompt di consenso vengono visualizzati quando l'app accede ai componenti specificati nel dispositivo dell'utente.

13. Fare clic su **Salva**.
14. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.

15. Selezionare una delle opzioni di distribuzione per impostare la configurazione **Impostazioni predefinite app privacy**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere **Utilizzo delle configurazioni**.
16. Fare clic su **Fine**.

10.10.4.4. Modifica della configurazione predefinita di Android Enterprise

Gli amministratori globali possono permettere agli amministratori dello spazio di modificare la distribuzione per una qualsiasi delle seguenti configurazioni predefinite di Android Enterprise nello spazio personalizzato.

- Android Enterprise: profilo di lavoro su un dispositivo di proprietà dell'azienda (Android for Work)
- Android Enterprise: dispositivo di lavoro gestito (Android for Work)
- Android Enterprise: dispositivo gestito con profilo di lavoro
- Android enterprise: AOSP

Modificare la distribuzione delle configurazioni sopra riportate

Procedura

1. Nella scheda Configurazioni, selezionare la configurazione da modificare.
2. Fare clic sull'icona Modifica.
3. Fare clic su **Avanti**
4. Selezionare uno dei seguenti livelli di distribuzione da modificare e configurare dalla pagina di distribuzione:
    - **Tutti i dispositivi**: selezionare una delle seguenti opzioni per distribuire la configurazione a tutti i dispositivi compatibili:
        1. Non applicare ad altri spazi
        2. Applica a dispositivi in altri spazi.
    - **Nessun dispositivo** (impostazione predefinita)
    - **Personalizzato**: selezionare una delle seguenti opzioni per distribuire la configurazione a tutti i dispositivi o utenti compatibili:
        1. **Utenti/Gruppi di utenti**: selezionare la casella di controllo accanto agli utenti o ai gruppi di utenti. In alternativa, è possibile digitare e cercare gli utenti o i gruppi di utenti.
        2. **Dispositivi/Gruppi di dispositivi**: selezionare la casella di controllo accanto ai dispositivi o ai gruppi di dispositivi. In alternativa, è possibile digitare e cercare i dispositivi o i gruppi di dispositivi.
           Nel **Riepilogo della distribuzione**, selezionare una delle seguenti opzioni per abilitare o disabilitare le configurazioni tra gli spazi:
            - Non applicare ad altri spazi.
            - Applica a dispositivi in altri spazi.

            > La casella di controllo **Consenti all'amministratore dello spazio di modificare la distribuzione** appare se si seleziona **Applica ai dispositivi in altri spazi** e consente agli amministratori dello spazio delegati di modificare la distribuzione per lo spazio specifico.

> Se si modifica l'opzione di distribuzione, è necessario selezionare la casella di controllo "**Sono consapevole che la modifica della distribuzione di Android Enterprise-Configurazione modalità dispositivo può causare il ritiro o la cancellazione dei dispositivi se la configurazione viene rimossa dai dispositivi esistenti**".

5. Fare clic su **Fine**.

Una volta applicata la configurazione agli spazi, gli amministratori degli spazi potranno modificare la distribuzione facendo clic sull'icona Distribuisci nello spazio personalizzato.

10.10.4.5. Configurazione di Android Enterprise

Argomento della sezione:

- Dispositivi supportati
- Connessione di Ivanti Neurons per MDM con Android Enterprise
- Come ottenere le credenziali di Android Enterprise
- Aggiunta del proprio token Android Enterprise MDM a Ivanti Neurons per MDM
- Sincronizzazione degli utenti tra Ivanti Neurons per MDM e Google
- Active Directory/Utenti LDAP
- Utenti locali
- Distribuzione di Android Enterprise ai dispositivi supportati
- Disattivazione dei dispositivi registrati
- Distribuzione al dispositivo
- Conferma della distribuzione
- Distribuzione di app Android Enterprise
- Configurazione di app aziendali

Licenza: Silver

Android Enterprise è un programma offerto da Google che permette agli amministratori di mobilità di:

- Separare i dati di lavoro e quelli personali
- Proteggere e gestire le app aziendali
- Controllare le app di sistema (come Fotocamera e Galleria)
- Eseguire il provisioning e configurare centralmente le applicazioni nel contenitore Android Enterprise
- Evitare la perdita di dati (acquisizione schermo)

È possibile configurare Ivanti Neurons per MDM come server UEM che gestisce Android Enterprise. Android Enterprise richiede almeno Android 3.0. Ci sono due configurazioni supportate di Android Enterprise, Proprietario dispositivo e Profilo gestito - Proprietà dipendente.

Dispositivi supportati

Ivanti Neurons per MDM attualmente supporta Android Enterprise solo sui dispositivi con in esecuzione Android 5.0 e che presentano Android Enterprise abilitato dal produttore. Android Enterprise è richiesto per la modalità tutto schermo sui dispositivi con Android 5.0.

Prerequisito

Se il dominio non è stato ancora registrato con Google, è necessario innanzitutto registrarsi al programma sul sito Web di Google:

https://admin.google.com.

Durante la procedura l'utente:

- Richiede un dominio (deve corrispondere al dominio degli indirizzi e-mail dell'utente)
- Riceve un token

- Scarica un ID client JSON

Entrambi gli elementi sono richiesti quando si configura Android Enterprise su Ivanti Neurons per MDM.

Al termine della procedura, l'utente riceverà un'e-mail con le istruzioni per verificare di possedere il dominio richiesto.

Se l'azienda ha già usato il suo nome di dominio per iscriversi a Google Apps for Work, vedere https://support.google.com/work/android/answer/6174062 per informazioni sull'abilitazione di Android Enterprise.

Connessione di Ivanti Neurons per MDM con Android Enterprise

Una volta effettua la registrazione per Android Enterprise, configurare Ivanti Neurons per MDM come UEM server.

Come ottenere le credenziali di Android Enterprise

Procedura

1. Andare in **Amministratore > Android Enterprise**.
2. Fare clic su **Console per gli sviluppatori Google**.
3. Fare clic sul primo collegamento visualizzato per andare alla console per gli sviluppatori di Google.
4. Selezionare **Crea un progetto** dal menu a discesa.
5. Immettere un nome per il progetto.
6. Accettare le condizioni per l'utilizzo del servizio.
7. Fare clic su **Crea**.
8. Fare clic su **API** .
9. Selezionare **API**.
10. Digitare **emm** nel campo di ricerca per trovare Google Play EMM.
11. Fare clic sul collegamento **API EMM di Google Play**.
12. Fare clic su **Abilita API**.
13. Fare clic su **Credenziali**.
14. Selezionare **Account di servizio**.
15. Fare clic su **Crea** per salvare il file JSON.

Aggiunta del proprio token Android Enterprise MDM a Ivanti Neurons per MDM

Procedura

1. Accedere a https://admin.google.com.
2. Fare clic su **Protezione**.
3. Se non si visualizza Impostazioni Android Enterprise, fare clic su **Mostra altro**.
4. Selezionare **Impostazioni Android Enterprise**.
5. Copiare il token MDM in **Gestisci il provider di gestione di enterprise mobility**.
6. Ritornare al portale Ivanti Neurons per MDM.
7. Fare clic su **Fine**.
8. Nella casella 2, incollare il token MDM appena copiato.

9. Nel campo **Dominio**, immettere il dominio richiesto a Google.
10. Fare clic su **Scegli file** e caricare il file JSON che è stato scaricato.
11. Fare clic su **Connetti**.
    Quando viene stabilita la connessione, verrà visualizzato il messaggio **Connesso a Google**.
12. Nella casella 3 fare clic su **Autorizza** per indicare che si desidera fornire a Ivanti Neurons per MDM accesso ai propri dati utente Google.
13. Fare clic su **Accetta**.
    Il messaggio **Connesso agli utenti** viene mostrato nel portale Ivanti Neurons per MDM.

Sincronizzazione degli utenti tra Ivanti Neurons per MDM e Google

Prima di distribuire Android Enterprise agli utenti Android gestiti da Ivanti Neurons per MDMIvanti Neurons for MDM, ogni utente deve avere un record corrispondente sul portale Amministratori Google. I passaggi richiesti per sincronizzare le informazioni utente tra Ivanti Neurons per MDM e il portale Amministratori Google dipendono dall'aver configurato un'integrazione con i servizi directory della propria organizzazione (AD/LDAP).

Active Directory/Utenti LDAP

Se si è configurato un'integrazione AD/LDAP con Ivanti Neurons per MDM, utilizzare Google Apps Directory Sync in modo da configurare un'integrazione AD/LDAP con il portale Amministratori Google. Per ulteriori informazioni, visitare il sito **https://support.google.com/a/answer/106368?hl=it**.

Utenti locali

Se si sono creati solo utenti locali in Ivanti Neurons per MDM e non si intende integrarli con un servizio directory, completare i seguenti passaggi per sincronizzare tali utenti con il portale Amministratori Google:

Procedura

1. Accedere al portale Amministratori Google, all'indirizzo **https://admin.google.com**.
2. Fare clic su **Utenti**.
3. Fare clic sull'icona **Aggiungi utente** o **Aggiungi utenti multipli** nell'angolo in basso a destra.
4. Per ciascun utente Ivanti Neurons per MDM che utilizzerà Android Enterprise, aggiungere un utente Google con lo stesso nome utente e indirizzo e-mail dell'utente Ivanti Neurons per MDM.
5. Nel portale Ivanti Neurons per MDM per ciascun utente Ivanti Neurons per MDM appena aggiunto al portale Amministratori Google:
   a. Fare clic sul collegamento del nome dell'utente nella scheda Utenti per visualizzare i dettagli dell'utente.
   b. Selezionare **Sincronizza l'utente con Directory utente di Google**.
   c. Fare clic su **Sincronizza con Directory utente di Google**.
   d. Confermare che lo Stato Google sia elencato come Abilitato.

Distribuzione di Android Enterprise ai dispositivi supportati

Sono necessarie due configurazioni per distribuire Android Enterprise:

- Android Enterprise: il profilo di lavoro su una configurazione dispositivo di proprietà dell'azienda consente Android Enterprise.
- Una configurazione Lockdown & tutto schermo definisce le restrizioni di Android Enterprise da applicare.

Disattivazione dei dispositivi registrati

Negli scenari BYOD, il passaggio da Amministratore dispositivo a Profilo di lavoro Android Enterprise su un dispositivo di proprietà dell'azienda non richiede un ritiro e una nuova registrazione dei dispositivi. La cancellazione o il ritiro del dispositivo è richiesto solo per passare dalla modalità Amministratore del dispositivo a Proprietario dispositivo.

Quando si seleziona un dispositivo registrato nelle modalità Proprietario dispositivo / Proprietario profilo migliorato / Proprietario azienda abilitato personalmente per l'azione Ritira, sullo schermo appare un pop-up che indica che il comando "Ritira non è supportato per i dispositivi di proprietà dell'organizzazione".

Distribuzione al dispositivo

Procedura

1. Nel portale Ivanti Neurons per MDM, passare a **Configurazioni**.
2. Fare clic su **Android Enterprise: Profilo di lavoro**.
3. Fare clic su **Modifica**.
4. Fare clic su **Avanti**.
5. Selezionare **Tutti i dispositivi** o **Personalizzazione**.
6. Se si seleziona **Personalizza**, cercare e selezionare i gruppi di dispositivi che devono ricevere le impostazioni di Android for Work.
7. Fare clic su **Fine**.
8. Fare clic su **Torna all'elenco** (nell'angolo in alto a sinistra).
9. Fare clic su **+Aggiungi**.
10. Fare clic su **Blocco e tutto schermo: Android Enterprise**.
11. Nel campo **Nome**, immettere il testo che identifica la configurazione.
12. In **Scegli tipo di blocco**, selezionare **Profilo di lavoro**.
13. Selezionare le impostazioni di blocco che si desidera applicare ai dispositivi di destinazione.
14. Fare clic su **Avanti**.
15. Selezionare **Tutti i dispositivi** o **Personalizzazione**.
16. Se si è selezionato Personalizza, cercare e selezionare i gruppi di dispositivi che devono ricevere le impostazioni di Android Enterprise.
17. Fare clic su **Fine**.

> Non è possibile apportare modifiche al profilo risultante dopo che è stato distribuito. Invece, è necessario creare una nuova configurazione Android Enterprise e distribuirla.

Conferma della distribuzione

È possibile confermare la distribuzione di Android Enterprise nei seguenti modi:

- In **Utenti > Utenti**, trovare la voce relativa a un utente e controllare che lo **stato di Google** sia **Abilitato**.
- Sotto **Dispositivi > Dispositivi,** fare clic sul collegamento di un dispositivo, quindi controllare che lo stato per **Android Enterprise** sia **Abilitato**.

Lo **Stato di Google** relativo a un utente deve essere riportato in elenco come **Abilitato**. Se non è Abilitato, l'utente non potrà registrare i dispositivi.

> Per le aziende prive di una sottoscrizione a GSuite, il metodo gestito Google Play Accounts consente agli utenti di registrarsi con Android Enterprise. Se Android Enterprise è stato configurato come Google Play Accounts gestito, l'utente non viene mostrato come **Stato Google: abilitato** fino a dopo la registrazione di un dispositivo Android Enterprise. Vedere **Account Google Play gestiti** per ulteriori informazioni sugli account Google Play gestiti.

Distribuzione di app Android Enterprise

Qualsiasi app sviluppata per Android Enterprise può includere opzioni configurabili mediante Ivanti Neurons per MDM.

Procedura

1. Nel portale Ivanti Neurons per MDM, passare a **App > Catalogo app**.
2. Trovare l'app su Google Play Store.
3. Fare clic sulla voce dell'app.
4. Accettare le autorizzazioni per conto degli utenti di Android Enterprise.
5. Fare clic su **Avanti**.
6. Selezionare un'opzione di distribuzione.
7. Espandere **Opzioni avanzate e Configurazione app**.
8. Attenersi alle linee guida seguenti per completare le opzioni:
9. Fare clic su **Avanti**.

Impostazione	Descrizione
Installa su dispositivo	Selezionare questa opzione per avviare l'installazione subito dopo la registrazione. All'utente verrà chiesto di confermare l'installazione dell'app, tranne quando il dispositivo è un dispositivo Samsung Knox ed è stata selezionata l'opzione di installazione invisibile indicata di seguito.
Non mostrare l'applicazione nell'App Catalog dell'utente finale	Selezionare questa opzione se non si desidera che l'utente visualizzi l'app nel Catalogo app del dispositivo.
Installa in modo invisibile sui dispositivi Samsung Knox	Selezionare questa opzione se non si desidera che all'utente venga richiesto di confermare l'installazione sui dispositivi Samsung Knox.
Imposta priorità di installazione app	Per le app Android Enterprise è possibile assegnare priorità di download ad app specifiche rispetto ad altre app. Ad esempio, è possibile assegnare la priorità al download delle app Tunnel ed E-mail, prima di altre app non critiche. Di seguito sono indicate le opzioni dei livelli di priorità disponibili: • **Alta** • Media (selezionata per impostazione predefinita) • **Bassa** Questa impostazione è applicabile alle app In-House, Pubbliche, Private e Web. Le app interne sono installate tramite il client mentre quelle pubbliche e private sono installate tramite Google. La priorità delle app viene applicata soltanto alle app installate sullo stesso canale.
Installa solo se disponibile una connessione Wi-Fi	Selezionare questa opzione per installare l'app solo quando il dispositivo è collegato alla rete Wi-Fi.
Installa solo durante la ricarica	Selezionare questa opzione per installare l'app solo quando è in corso la ricarica del dispositivo.
Installa solo se inattivo	Selezionare questa opzione per installare l'app solo quando il dispositivo è inattivo (non utilizzato attivamente dall'utente).
Avvio automatico all'installazione	Selezionare questa opzione per avviare un'app automaticamente dopo l'installazione. Questa funzionalità è disponibile solamente se l'app è appena stata installata nel dispositivo e non costituisce un aggiornamento a una nuova versione.

10. Selezionare un'opzione di promozione.
11. Fare clic su **Fine**.

Configurazione di app aziendali

Le app Android Enterprise sono disponibili nella sezione Business Apps del catalogo app, incluse le app seguenti:

- Divide Productivity
- E-mail+

- Tunnel
- Gmail

10.10.4.6. Android Enterprise: dispositivo di lavoro gestito in modalità non GMS (AOSP)

Ivanti Neurons for MDM supporta la registrazione del proprietario del dispositivo per i dispositivi di lavoro gestiti in modalità non GMS (AOSP) senza la necessità di Google Mobile Services (GMS). È una configurazione di sistema che non può essere aggiunta dagli amministratori. Gli amministratori possono eseguirne o annullarne la distribuzione.

Procedura

1. Accedere a Ivanti Neurons for MDM con le credenziali utente.
2. Ricerca configurazioni per Android Enterprise: dispositivo di lavoro gestito in modalità non GMS (AOSP).
3. Modificare la configurazione e distribuirla ai gruppi di dispositivi appropriati, ad esempio Dispositivi Android.
4. Fare clic su **Fine**.

10.10.4.7. Richiesta di verifica di Android Work

Argomento della sezione:

- Creazione della configurazione Richiesta di verifica del lavoro (Work Challenge) Android:
- Impostazioni di configurazione

Licenza: Silver

La configurazione Richiesta di verifica del lavoro (Work Challenge) Android permette di definire password sicure per gli utenti per l'accesso alle app e ai dati del Profilo di lavoro. Richiede il profilo di lavoro Android Enterprise.

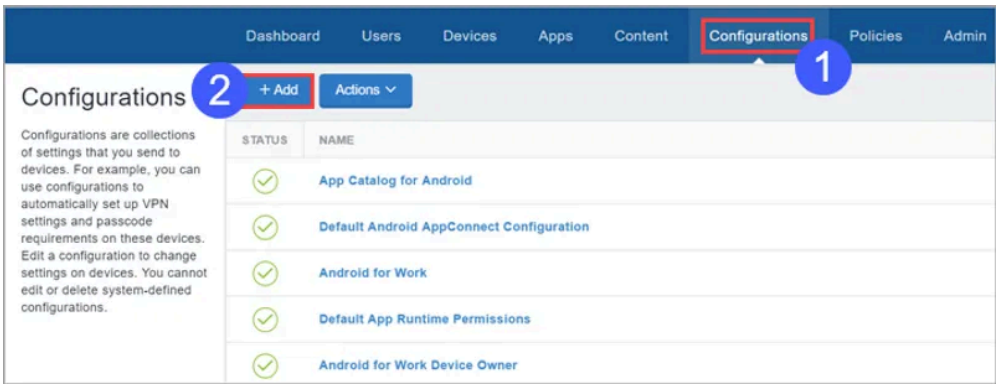
Note di implementazione:

- Gli amministratori possono applicare una policy per la password del dispositivo e una policy per la password del profilo di lavoro separatamente.
- Ivanti Neurons for MDM non invia questa configurazione ai client precedenti ad Android 7.0, in quanto tali dispositivi non supportano questa funzionalità.
  Ivanti Neurons for MDM invia questa configurazione solo ai dispositivi con un profilo di lavoro Android Enterprise.

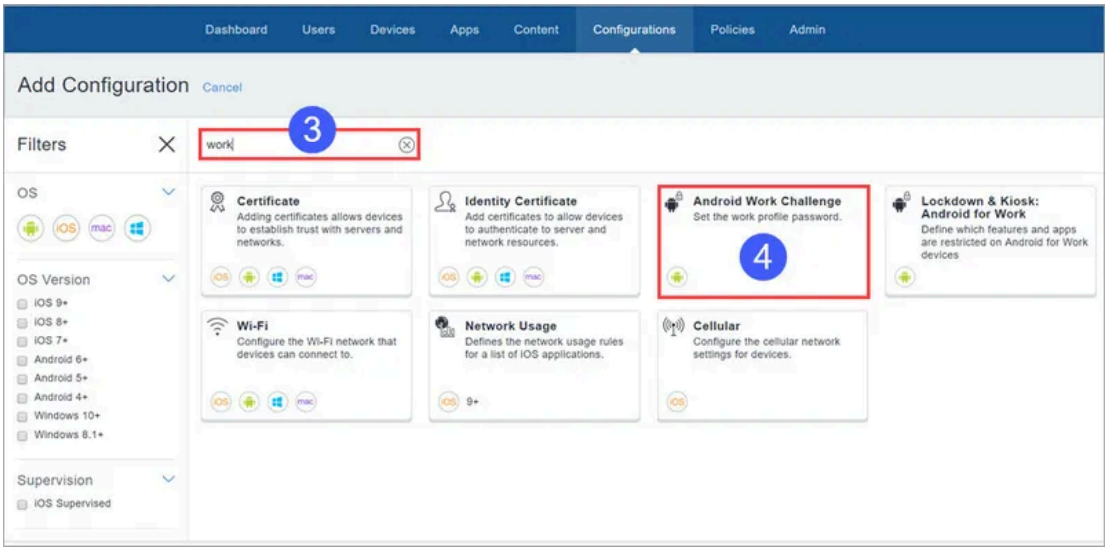
Creazione della configurazione Richiesta di verifica del lavoro (Work Challenge) Android:

Procedura

1. Fare clic su **Configurazioni**.

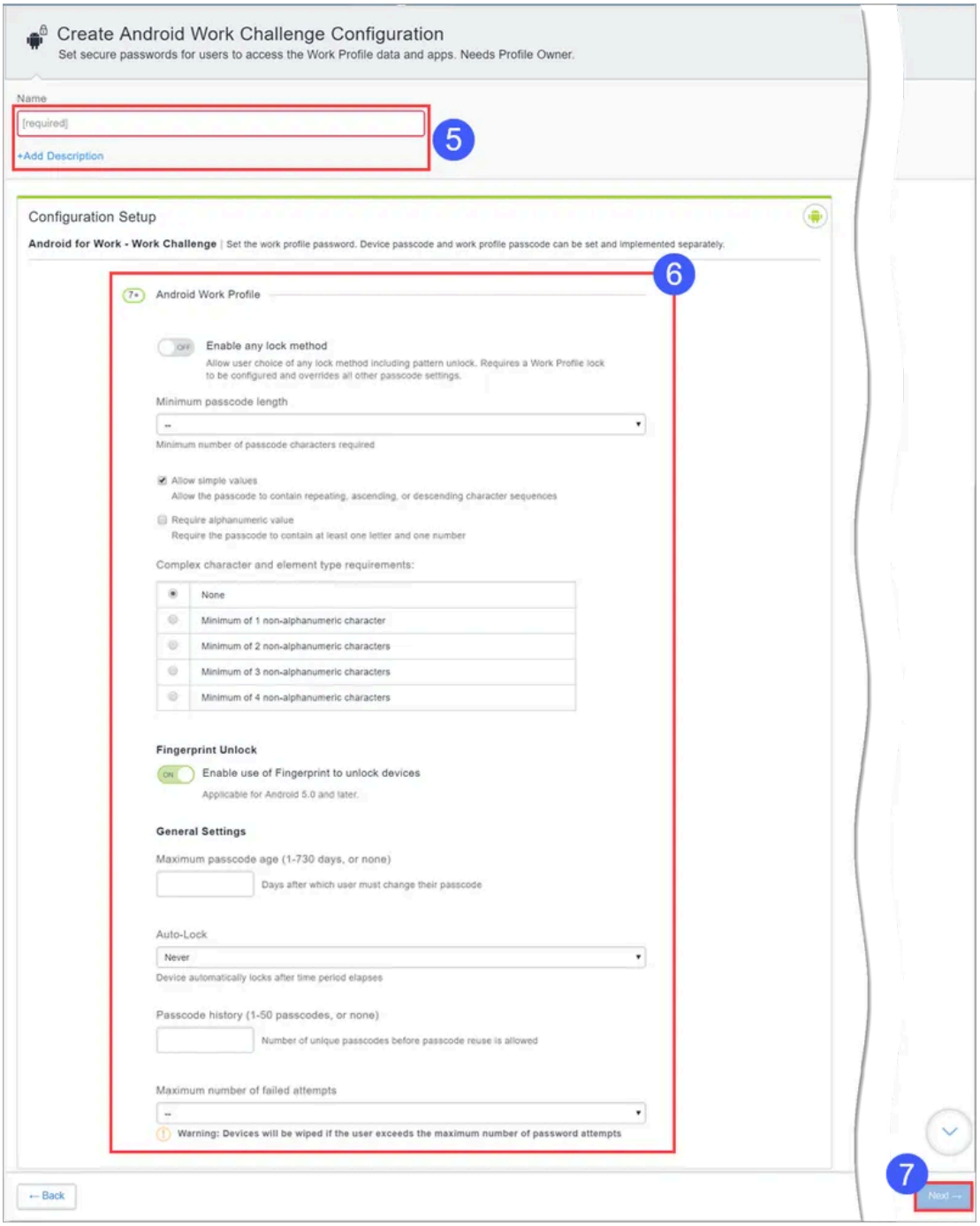


Fare clic su **+Aggiungi**.



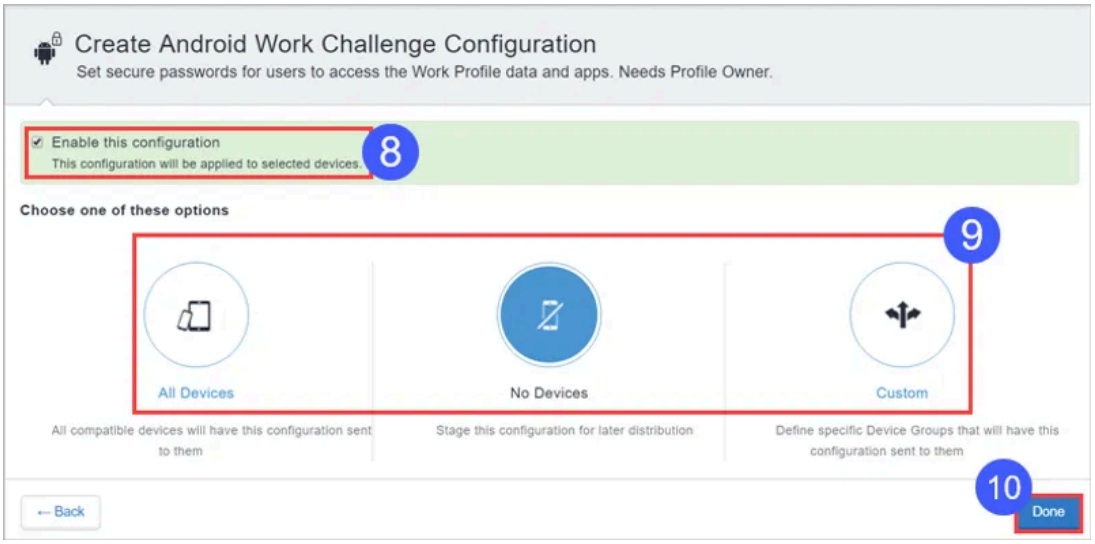
Digitare "lavoro" nel campo di ricerca.

4. Selezionare la configurazione **Richiesta di verifica del lavoro (Work Challenge) Android**.



Immettere un nome per la configurazione e, facoltativamente, una descrizione.

6. Utilizzare i campi Impostazioni configurazione per creare la configurazione. Fare riferimento a **Impostazioni di configurazione** per ulteriori dettagli.
7. Fare clic su **Avanti →**.



Abilitare la configurazione, se si desidera.

9. Configurare le impostazioni di distribuzione su tutti i dispositivi, nessun dispositivo o un insieme personalizzato di dispositivi.
10. Fare clic su **Fine**.

Impostazioni di configurazione

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Abilita qualsiasi metodo di blocco	Consentire all'utente di scegliere qualsiasi metodo di blocco, incluso lo sblocco dei criteri. Prevale su tutte le altre impostazioni del passcode.
Lunghezza minima del passcode	Selezionare una lunghezza minima per il passcode, da 4 a 16 caratteri.
Supporto dei valori semplici	Permette di includere nel passcode sequenze di caratteri ripetitive, crescenti o decrescenti.
Valore alfanumerico necessario	Impone di includere nel passcode almeno una lettera e un numero.
Requisiti dei caratteri complessi e dei tipi di elementi	Permette di configurare requisiti di caratteri complessi e di tipi di elementi, scegliendo tra: • Nessuno • Almeno 1 carattere non alfanumerico • Almeno 2 caratteri non alfanumerici • Almeno 3 caratteri non alfanumerici • Almeno 4 caratteri non alfanumerici
Sblocco tramite impronta digitale	Permette agli utenti di sbloccare i propri dispositivi mediante l'impronta digitale.
Validità passcode	Configurare la validità del passcode, da 0 a 730 giorni.
Blocco automatico	Selezionare un periodo di tempo dopo il quale attivare il blocco automatico sul dispositivo. Le opzioni variano da mai a 15 minuti.
Cronologia passcode	Specificare il numero di passcode univoci necessari prima che sia consentito riutilizzare il passcode, scegliendo un'opzione da 0 a 50 passcode.
Numero massimo di tentativi non riusciti	Selezionare il numero massimo di tentativi non riusciti. **ATTENZIONE: Ivanti Neurons for MDM cancella i dispositivi per i quali l'utente supera il numero massimo di tentativi di password!**

10.10.4.8. Configurazione dei certificati

La configurazione dei certificati consente di identificare il certificato da distribuire ai dispositivi. Tramite i certificati, i dispositivi sono in grado di stabilire una relazione di trust con il server e le risorse di rete. A partire dalla versione 76 supportiamo solo i certificati v3.

Ora l'amministratore può generare certificati Ivanti Neurons for MDM per l'accesso tramite smart card e ID oggetto (OID, Object ID) personalizzati. È possibile generare certificati per le seguenti opzioni di autenticazione:

- Autenticazione client - Abilitata per impostazione predefinita
- IPSEC - Facoltativo, può essere abilitato dall'amministratore
- Accesso smart card - Facoltativo, può essere abilitato dall'amministratore
- OID personalizzati - Facoltativi, possono essere abilitati dall'amministratore

> Questa funzionalità è applicabile solo per le seguenti autorità di certificazione (CA):

- Autorità di certificazione locale
- Autorità di certificazione intermedia
- Autorità di certificazione esterna - Configurare le policy di applicazione del modello CA nel server NDES per il supporto di IPSEC, Accesso smart card e OID personalizzati
- Autorità di certificazione SCEP locale

Distribuzione della configurazione

A partire dalla versione 91 di Ivanti Neurons for MDM, gli amministratori globali possono delegare gli amministratori di spazi per modificare l'opzione Configurazione certificati per tutti i dispostivi e per la distribuzione personalizzata. Per la configurazione dei certificati, è possibile selezionare l'opzione Consenti che questa configurazione sia disponibile in tutti gli spazi. Questa opzione rende la Configurazione certificati disponibile per tutti gli Spazi e può essere pertanto utilizzata in Exchange, WiFi, VPN, Per-App VPN e qualsiasi altra configurazione applicabile. Questa opzione può essere utilizzata negli scenari in cui la configurazione certificati è richiesta per essere distribuita ai dispositivi (in spazi non predefiniti) solo come parte di configurazioni associate e non come configurazione individuale.

Procedura

1. Inserire un nome nel campo Nome.
2. Caricare il file del certificato.
3. Fare clic su **Avanti**.
4. Selezionare l'opzione **Abilita questa configurazione**.
5. Selezionare una delle seguenti opzioni di distribuzione:
    - **Tutti i dispositivi**. Selezionare una delle seguenti opzioni:
        - **Non applicare ad altri spazi**.
        - **Applica a dispositivi in altri spazi**.
            - Selezionare la casella di controllo **Consenti all'amministratore dello spazio di modificare la distribuzione** per consentire agli amministratori dello spazio delegati di modificare la distribuzione per lo spazio specifico.
    - **Nessun dispositivo** (impostazione predefinita)

- **Personalizza** Selezionare una delle seguenti opzioni:
  - **Non applicare ad altri spazi**.
  - **Applica a dispositivi in altri spazi**.
    - Selezionare la casella di controllo **Consenti all'amministratore dello spazio di modificare la distribuzione** per consentire agli amministratori dello spazio delegati di modificare la distribuzione per lo spazio specifico.

> Indipendentemente dagli spazi, la configurazione certificati può essere configurata in tutti gli spazi, distribuita su tutti i dispositivi e applicata a tutti i dispositivi in altri spazi di dispositivi.

6. Fare clic su **Fine**.

Impostazioni dei certificati

In qualità di amministratore, è possibile configurare un'autorità di certificazione non SCEP locale.

Procedura

1. Accedere al portale amministratore di Ivanti Neurons for MDM.
2. Selezionare **Amministratore** > **Infrastruttura** > **Gestione certificati** > **Autorità di certificazione**.
3. Fare clic su **+Aggiungi**. Saranno visualizzate le seguenti opzioni:

- **Crea autorità di certificazione locale fornita da Ivanti Neurons for MDM**
- **Firma CA locale di Ivanti Neurons for MDM con la propria CA esistente**.
- **Connetti ad autorità di certificazione Cloud pubblicamente attendibile**.
- **Connetti autorità di certificazione SCEP locale**.
- **Connetti autorità di certificazione non SCEP in loco**.

4. Completare i seguenti campi, se pertinenti:
5. Fare clic su **Fine**.

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
URL	L'URL della CA OpenTrust che l'amministratore deve ottenere da OpenTrust.
Password	Immettere la password per il certificato di autenticazione.
Certificato di autenticazione	Accetta il formato file .p12 fornito da OpenTrust/IDnomic.
Catena di certificazione CA TLS	Accetta il formato file PEM fornito da OpenTrust/IDonomic.

Una volta configurata l'autorità di certificazione non SCEP locale, è necessario creare il certificato di identità. In base all'ID profilo, compilare tutti i campi obbligatori per completare la configurazione.

> Viene generata una notifica quando la generazione del certificato CA SCEP non riesce per i due motivi seguenti e viene raggiunto il timeout dello Stage 2:

1. Il connettore non è raggiungibile

2. Il server CA non è raggiungibile

10.10.4.9. Trasparenza certificato

Applicabile a: iOS 12.1.1, macOS 10.14.2, tvOS 12.1.1, watchOS 10.0+, visionOS 1.1+ e versioni più recenti supportate.

Controlla l'applicazione della trasparenza certificato, che può apparire solo in un profilo dispositivo. È possibile includere più certificati e disabilitare domini come necessario.

Creazione di una configurazione Trasparenza certificato

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **certificato** nel campo di ricerca, quindi fare clic sulla configurazione **Trasparenza certificato**.
4. Immettere un nome e una descrizione per la configurazione.
5. Specificare un valore per **Domini che verranno disabilitati**. Fare clic su **+ Aggiungi dominio** per aggiungere più di un dominio. Un periodo iniziale può essere usato per far corrispondere i sottodomini, tuttavia una regola di corrispondenza del dominio non deve corrispondere a tutti i domini all'interno di un dominio di primo livello. Ad esempio, ".example.com" e ".example.co.uk" sono consentiti, mentre ".com" e ".co.uk" no. Domini con caratteri jolly non supportati.
6. Selezionare un algoritmo (SHA 256) e specificare **Hash certificato**. Fare clic su **+ Aggiungi** per aggiungere più di un hash certificato.
7. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
8. Fare clic su **Fine**.

Per generare i dati specificati dalla chiave Hash nel dizionario subjectPublicKeyInfo, nel caso di un certificato con codifica PEM utilizzare il comando seguente:

```
openssl x509 -pubkey -in example_certificate.pem -inform pem | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

Se il certificato ha codifica DER, utilizzare il comando seguente:

```
openssl x509 -pubkey -in example_certificate.der -inform der | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.4.10. Configurazione della verifica della revoca dei certificati

Questa configurazione consente agli amministratori di verificare una serie di certificati su un dispositivo per determinare se sono stati revocati. Gli amministratori possono specificare un'autorità di certificazione (CA) che permette di configurazione la verifica della revoca per tutti i certificati collegati a tale CA.

Applicabile a: iOS 14.2+ e visionOS 1.1+.

Procedura

1. Andare in Configurazioni > +Aggiungi.
2. Digitare certificato nel campo di ricerca, quindi fare clic sulla configurazione Controllo revoca certificati.
3. Immettere un Nome e una Descrizione per la configurazione.
4. Selezionare l'algoritmo SHA 256 e immettere l'Hash del certificato radice.

> Nel campo Hash è necessario immettere un il valore hash SHA-256 con codifica Base64 (binaria) della chiave pubblica del certificato. Per informazioni sui certificati radice attendibili per i sistemi operativi Apple, vedere la **documentazione Apple**. In questa configurazione è possibile aggiungere più certificati radice.

5. Fare clic su Avanti.
6. Selezionare l'opzione Abilita questa configurazione.
7. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzata.
8. Fare clic su Fine.

10.10.4.11. Crea Configurazione modalità autonoma Single App

La configurazione modalità autonoma Single App consente di garantire che solo applicazioni specifiche vengano eseguite su un dispositivo. Anche se l'utente tenta di lanciare un'altra applicazione, la configurazione lancia solo l'applicazione specifica.

Procedura

1. Andare in **Configurazioni** > **Aggiungi** > **Modalità autonoma Single App**.
2. Utilizzare le linee guida seguenti per definire l'app e le impostazioni correlate.
3. Fare clic su **Avanti**.

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Impostazioni configurazione	**Identificatore bundle** - (obbligatorio) l'identificatore bundle univoco. Se due dizionari contengono lo stesso valore di BundleIdentifier ma un valore di TeamIdentifier diverso, questo sarà considerato un errore e il profilo non sarà installato.
	Identificatore team - (obbligatorio) L'identificatore del team dello sviluppatore, utilizzato al momento della firma dell'app.

4. Nella schermata **Distribuzione**, selezionare i gruppi che riceveranno questa configurazione.
5. Fare clic su **Fine**.

10.10.4.12. Creazione della configurazione del proxy DNS

In qualità di amministratore Ivanti Neurons per MDM, è possibile configurare le impostazioni del Proxy DNS utilizzando la Configurazione del Proxy DNS per gli utenti di dispositivi iPhone e iPad. È possibile utilizzare il payload DNS Proxy per specificare l'applicazione che fornisce l'estensione di rete del proxy DNS e altri valori specifici del fornitore.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Andare in **Configurazioni**
3. Digitare **DNS** nel campo di ricerca e fare clic su **DNSConfigurazione proxy**.
4. Immettere un nome e una descrizione per la configurazione.
5. Inserire le seguenti impostazioni di configurazione del proxy DNS:
    - Identificatore del bundle di app (obbligatorio).
    - Identificatore del bundle fornitori.
    - Configurazione del provider (valore-chiave).
6. Fare clic su **Avanti**.
7. Selezionare l'opzione **Abilita questa configurazione**.
8. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato

Fare clic su **Fine**.

10.10.4.13. Configurazione registrazione dispositivo

La configurazione della registrazione del dispositivo consente di abilitare i registri di rete e di sicurezza per i dispositivi Android.

Creazione di una configurazione della registrazione del dispositivo

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Nel campo di ricerca, digitare **Registrazione dispositivi** e selezionare la configurazione.
4. Immettere un nome e una descrizione per la configurazione.
5. Sotto la sezione **Impostazione configurazione**, selezionare una o entrambe le opzioni:
    - Abilita registrazione di rete
    - Abilita registrazione di sicurezza

> Per informazioni sulle versioni di Android supportate per la registrazione di sicurezza e di rete, consultare le tabelle in **Matrice di registrazione di sicurezza** di seguito.

Fare clic su **Avanti** per configurare le impostazioni di distribuzione.

7. Fare clic su **Fine**.

Matrice registrazione di sicurezza

Tipo di dispositivo	Versioni Android supportate
Dispositivi gestiti dal lavoro e dispositivi gestiti dal lavoro in modalità non GMS (AOSP)	7, 8, 9, 10, 11, 12, 13
Dispositivi gestiti con profilo di lavoro	8, 9, 10
Profilo di lavoro	ND
Profilo di lavoro su dispositivo di proprietà dell'azienda	11, 12, 13

Matrice registrazione di rete

Tipo di dispositivo	Versioni Android supportate
Dispositivi gestiti dal lavoro e dispositivi gestiti dal lavoro in modalità non GMS (AOSP)	8, 9, 10, 11, 12, 13
Dispositivi gestiti con profilo di lavoro	8, 9, 10
Profilo di lavoro	12, 13
Profilo di lavoro su dispositivo di proprietà dell'azienda	12, 13

Dopo aver installato la configurazione di registrazione del dispositivo sul dispositivo, l'utente riceve una notifica contenente informazioni sulla gestione del dispositivo e sulla registrazione di rete. Fare clic su **OK** per confermare la notifica.

Richiesta registri di debug

Procedura

1. Accedere a Ivanti Neurons per MDM.
2. Passare a **Dispositivi** > **Dettagli dispositivi**.
3. Dalla sezione **Panoramica**, fare clic sul pulsante con i tre punti verticali accanto al pulsante **Forza check-in**.
4. Selezionare **Richiedi registri di debug**.
5. Selezionare una delle due opzioni seguenti:
    - Escludi segnalazione bug - Quando si seleziona questa opzione e si fa clic su Avanti, viene visualizzata una finestra di conferma. Fare clic su **Richiedi registri di debug**. Gli utenti non devono fornire alcun consenso per questa opzione e questi registri escludono la segnalazione di bug per i dispositivi Android selezionati.
    - Includi segnalazione bug - Quando si seleziona questa opzione e si fa clic su Avanti, viene visualizzata una finestra di conferma. Fare clic su **Richiedi registri di debug**. Gli utenti devono fornire il consenso per la condivisione della segnalazione di bug. Nel caso dei dispositivi Android, agli utenti verrà richiesto di inviare i registri del dispositivo, compresa la segnalazione dei bug.

10.10.4.14. Configurazione gestione disco

Ivanti Neurons per MDM Le impostazioni di configurazione di Gestione disco definiscono i criteri per la gestione efficace dei dati nei dispositivi di archiviazione esterni e di rete.

Applicabile a: macOS 15.0 supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Gestione disco**.
3. Configurare le impostazioni **Gestione disco** come da tabella seguente:

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Gestione disco	
Archiviazione esterna	Selezionare uno dei valori seguenti dal menu a discesa: • **Consentito**: consente la lettura e la scrittura dell'archiviazione. • **Sola lettura**: consente la lettura dell'archiviazione. • **Non consentito**: non consente l'accesso all'archiviazione.
Archiviazione di rete	Selezionare uno dei valori seguenti dal menu a discesa: • **Consentito**: consente la lettura e la scrittura dell'archiviazione. • **Sola lettura**: consente la lettura dell'archiviazione. • **Non consentito**: non consente l'accesso all'archiviazione.

4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
5. Selezionare una delle opzioni di distribuzione per impostare la configurazione della **Gestione disco**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere Utilizzo delle configurazioni.
6. Fare clic su **Fine**.

10.10.4.15. Cifratura Android

La configurazione della crittografia definisce i requisiti di crittografia dei dispositivi Android in modalità Amministrazione del dispositivo. La crittografia del dispositivo rende più sicuri i dati aziendali sensibili impedendovi l'accesso da parte di autori di jailbreaking e di exploit che tentano di acquisire privilegi di root. La crittografia archivia i dati del dispositivo in un formato non leggibile in modo da impedirne l'accesso a eventuali utenti non autorizzati.

Quando viene abilitata la crittografia, viene richiesto all'utente di crittografare il dispositivo e di impostare un passcode. Il passcode esegue la decrittografia dei dati rendendoli leggibili. La cifratura del dispositivo viene automaticamente attivata in Android Enterprise (profilo di lavoro o dispositivi gestiti) o nei dispositivi iOS quando è impostato un passcode. Non è possibile utilizzare il dispositivo durante la procedura di crittografia. Una volta attivata, per disattivare la crittografia è necessario un ripristino delle impostazioni predefinite del dispositivo.

Impostazioni della crittografia

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Abilita crittografia dispositivo	Selezionare l'impostazione per attivare la crittografia su tutti i dispositivi Android con crittografia abilitata che ricevono questa configurazione.

> La configurazione della crittografia di Android è deprecata per i dispositivi Samsung in modalità Amministrazione dispositivo su Android 11. Questa crittografia è supportata per impostazione predefinita sui dispositivi Android Enterprise quando è impostato un codice di accesso al dispositivo.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.4.16. DNS cifrato

Licenza: Gold

Applicabile a:

- iOS 14.0 o versioni più recenti supportate.
- macOS 11.0 o versioni più recenti supportate.
- visionOS 1.1 o versioni più recenti supportate.

Configura DNS cifrato che permetterà di migliorare la sicurezza senza la necessità di configurare la VPN.

Argomenti della sezione:

- Configurazione DNS cifrato
- Impostazioni configurazione DNS cifrato

Configurazione DNS cifrato

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **DNS** nel campo di ricerca, quindi fare clic sulla configurazione **DNS cifrato**.
4. Immettere un nome e una descrizione per la configurazione.
5. Inserire le impostazioni di configurazione del DNS cifrato.
6. Fare clic su **Avanti**.
7. Selezionare l'opzione **Abilita questa configurazione**.
8. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato
9. Fare clic su **Fine**.

Impostazioni configurazione DNS cifrato

Utilizzare le impostazioni nella seguente tabella per configurare il DNS cifrato. Per ulteriori informazioni su queste impostazioni, vedere la documentazione di Apple.

Impostazione	Descrizione
Impostazioni DNS	Un dizionario che definisce una configurazione per un server DNS cifrato.
Protocollo DNS	Specificare il protocollo di trasporto cifrato utilizzato per comunicare con il server DNS. Selezionare uno dei seguenti protocolli: • HTTPS • TLS
URL del server	Il modello URI di un server DNS-over-HTTPS, come definito nello standard RFC 8484. Questo URL deve utilizzare lo schema https://, e il nome host o l'indirizzo nell'URL verranno utilizzati per convalidare il certificato del server. Se non viene fornito alcun indirizzo di server, il nome host o l'indirizzo nell'URL saranno utilizzati per determinare gli indirizzi del server. Questa chiave deve essere presente solo se il protocollo DNS è HTTPS.
Indirizzi server	Un elenco non ordinato di stringhe di indirizzo IP del server DNS. Questi indirizzi IP possono essere una combinazione di indirizzi IPv4 e IPv6. Fare clic su **Aggiungi** per aggiungere uno o più indirizzi del server.
Corrispondenza con i domini supplementare	Un elenco di stringhe di dominio utilizzato per determinare quali query DNS utilizzeranno il server DNS. Se questa matrice non viene fornita, tutti i domini utilizzeranno il server DNS. Fare clic su **Aggiungi** per aggiungere uno o più domini.
Impedisci agli utenti di disattivare le impostazioni DNS	Impedisce agli utenti di disattivare le impostazioni DNS. Questo tasto è disponibile solo sui dispositivi supervisionati.
Richiedi regole	Una matrice di regole che definiscono le impostazioni DNS. Se le regole non sono presenti, il sistema applica sempre le impostazioni DNS. Fare clic su **+ Aggiungi Richiedi regole** per aggiungere uno o più set di regole di richiesta.
Rete	L'azione da intraprendere se questo dizionario corrisponde alla rete attuale. Selezionare una delle seguenti azioni: • **Collega:** applica le impostazioni DNS quando il dizionario corrisponde. • **Disconnetti:** non applicare le impostazioni DNS quando il dizionario corrisponde. • **Valuta connessione:** applica le impostazioni DNS con eccezioni in base al dominio quando il dizionario corrisponde.
Valuta connessione	Questa opzione di rete ha le seguenti impostazioni: • **Azione di dominio** - Il comportamento delle impostazioni DNS per i domini specificati. Selezionare una delle seguenti azioni: ◦ **Non connettere in nessun caso** - Non utilizzare le impostazioni DNS per i domini specificati. ◦ **Connetti se necessario** - Consentire utilizzando le impostazioni DNS per i domini specificati.

Impostazione	Descrizione
	• **Domini** - I domini a cui si applica questa valutazione. Fare clic su **+ Aggiungi** per aggiungere uno o più domini.
Regole	Fare clic su **+ Aggiungi** per aggiungere una o più regole per abbinare i seguenti parametri con i corrispondenti valori specificati.
Corrispondenza dominio DNS	Una matrice di nomi di dominio. Questa regola viene soddisfatta se uno dei nomi di dominio nell'elenco specificato corrisponde a qualsiasi dominio nell'elenco dei domini di ricerca del dispositivo.
Corrispondenza indirizzo server DNS	Una matrice di indirizzi IP. Questa regola viene soddisfatta se uno dei server DNS specificati della rete corrisponde a una voce nella matrice.
Corrispondenza SSID	Una matrice di SSID da mettere in corrispondenza con la rete corrente. Se la rete non è una rete Wi-Fi o se l'SSID non appare in questa matrice, la corrispondenza non riesce. Omettere questa chiave e la matrice corrispondente per abbinare con qualsiasi SSID.
Corrispondenza tipo di interfaccia	Un tipo di interfaccia. Se specificata, questa regola è soddisfatta solo se l'hardware dell'interfaccia di rete principale corrisponde al tipo specificato. Selezionare uno dei seguenti tipi: • Ethernet • Wi-Fi • Cellulare
Probe stringa URL	Un URL per il probe. Se questo URL viene recuperato correttamente (con la restituzione di un codice di stato HTTP 200), senza reindirizzamento, questa regola è soddisfatta.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.4.17. Impostazioni Intelligence esterna

Utilizzare le **Impostazioni di intelligence esterna** per configurare le integrazioni di Intelligenza esterna sui dispositivi supervisionati. Questa configurazione aiuta gli amministratori ad applicare impostazioni coerenti basate su criteri che controllano il modo in cui i dispositivi si connettono e utilizzano i servizi di intelligence esterni supportati.

Applicabile a:

- iOS 26.4+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.
- macOS 26.4+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.
- visionOS 26.4+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Impostazioni Intelligence esterna**.
3. Configurare la configurazione delle **Impostazioni di Intelligence esterna** in base alla tabella seguente:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Consenti integrazioni di intelligence esterna	Selezionare la casella di controllo per abilitare le integrazioni di Intelligence esterna. Utilizzare il pulsante **Esegui push al dispositivo** per attivare le integrazioni di Intelligence esterna su dispositivi supervisionati.
Consenti accesso integrazioni di intelligence esterna	Selezionare la casella di controllo per abilitare l'accesso alle integrazioni di Intelligenza esterna. Utilizzare il pulsante **Esegui push al dispositivo** per attivare l'accesso alle integrazioni di Intelligence esterna sui dispositivi supervisionati.
ID consentiti dell'area di lavoro intelligence esterna	Immettere gli ID area di lavoro per abilitare l'Intelligenza esterna. Utilizzare il pulsante **Esegui push al dispositivo** per attivare l'Intelligenza esterna per l'ID area di lavoro immesso sui dispositivi supervisionati.

4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
5. Selezionare una delle opzioni di distribuzione per impostare la configurazione delle **Impostazioni di Intelligence esterna**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere Utilizzo delle configurazioni.
6. Fare clic su **Fine**.

10.10.4.18. Difesa dalle minacce

Applicabile a:

- Versione 3.2.0 del client Go per iOS o versioni successive supportate.
- Versione 52 del client Go per Android o versioni successive supportate.

Ivanti Neurons for MDM include la possibilità di distribuire token di attivazione per abilitare la tecnologia Threat Defense integrata in Go per i client Android e iOS. Threat Defense protegge i dispositivi gestiti dalle vulnerabilità e dalle minacce per i dispositivi mobili che colpiscono dispositivi, reti e applicazioni.

Se questa configurazione è abilitata in Ivanti Neurons for MDM e applicata ai dispositivi, le librerie di Threat Defense vengono abilitate nei client di Go. È possibile disattivare il servizio Threat Defense rimuovendo il token della licenza e reinviando la configurazione della licenza al client.

Il servizio Threat Defense monitora:

- A livello del dispositivo: parametri, configurazione, firmware, e librerie di sistema per individuare attività sospette o dannose.
- A livello della rete: traffico di rete e connessioni sospette verso e da dispositivi mobili.
- A livello dell'app: app non impermeabili (che possono mettere a repentaglio i dati aziendali) e app dannose, mediante la valutazione del rischio e l'analisi del codice.

Documentazione più recente

Per le istruzioni più recenti su Threat Defense, consultare la *Guida alla soluzione Ivanti Neurons for MDM Threat Defense* nel sito Documentazione sui prodotti all'indirizzo **Documentazione sul prodotto Ivanti Neurons for MDM**.

10.10.4.19. FileVault 2

Licenza: Gold

FileVault 2 consente di eseguire la crittografia XTS-AES 128 completa sui contenuti di un volume.

Quando si attiva FileVault 2, per la configurazione sono disponibili le seguenti impostazioni:

Categoria	Impostazioni
Impostazioni utente FileVault	• Abilitare FileVault in SetupAssist **Impostazione predefinita**: false • Se è vero e il payload viene installato dopo la registrazione con Ivanti Neurons for MDM in Assistente configurazione, richiede a quest'ultimo di abilitare FileVault al momento della configurazione. Inoltre, il sistema ignora tutte le altre chiavi di questo payload, tranne ShowRecoveryKey. **Prerequisito**:- Prima di abilitare il file vault nell'assistente di configurazione, assicurarsi che **Attendi configurazione dispositivo durante la Configurazione registrazione dispositivo** sia abilitato nel profilo di registrazione del dispositivo. • Rinvia abilitazione FileVault fino alla disconnessione dell'utente designato ◦ Richiedi sempre conferma per abilitare FileVault ◦ Numero massimo di volte in cui un utente può ignorare l'abilitazione di FileVault Non richiedere l'abilitazione di FileVault durante la disconnessione dell'utente
Percorso di output	Immettere il percorso alla posizione in cui verranno archiviate la chiave di ripristino e le informazioni sul computer.
Chiave di recupero personale	• Crea chiave di ripristino personale • Visualizza chiave di ripristino personale dopo l'abilitazione di FileVault Questa opzione è visibile solo quando la funzione **Crea chiave di ripristino personale** è abilitata. Per impostazione predefinita, l'opzione è disabilitata. • Abilita chiave di ripristino istituzionale - Utilizzo del portachiavi: se non viene fornita alcuna informazione sul certificato in questo payload, verrà utilizzato il portachiavi già creato in /Libreria/Portachiavi/FileVaultMaster.keychain. Selezionare una delle seguenti opzioni: ◦ Carica certificato ◦ Certificato ◦ Usa portachiavi nel sistema utenti
Ruota chiave FileVault dopo __ giorni	Gli amministratori possono configurare la rotazione periodica delle chiavi FileVault per i dispositivi macOS per ridurre il rischio di sicurezza dei dispositivi distribuiti. Gli amministratori possono impostare l'intervallo di rotazione in termini di giorni. Solo le chiavi di recupero personali vengono ruotate.

10.10.4.20. Chiave di ripristino di FileVault

Licenza: Gold

La configurazione Chiave di ripristino di FileVault determina il reindirizzamento e il deposito delle chiavi di ripristino di FileVault su un server aziendale.

> L'opzione Exclude and Re-push of File Vault Recovery Key (Escludi e invia nuovamente la configurazione Chiave di ripristino di FileVault) è disabilitata, perché i dispositivi macOS smettono di inviare la chiave di ripristino al reinvio della configurazione.

È possibile impostare le seguenti opzioni:

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	(Facoltativo) Immettere una descrizione esplicativa dello scopo della configurazione.
Impostazioni di configurazione per macOS 10.13 o versioni precedenti	
Archivia la chiave di recupero per il tenant Ivanti Neurons for MDM	Selezionare questa opzione per abilitare l'archiviazione delle chiavi sul tenant da parte di Ivanti Neurons for MDM. All'occorrenza, è possibile decriptare la chiave nella pagina Dettagli dispositivo.
Reindirizza URL al server	Immettere le seguenti impostazioni: • Immettere l'**URL di reindirizzamento** (non Apple) a cui inviare le chiavi di ripristino FDE. L'URL deve iniziare con https://. • Selezionare un certificato dall'elenco a discesa. È supportato solo il certificato in formato PKCS1.
Impostazioni di configurazione per macOS 10.13 o versioni successive	
Posizione	(Obbligatorio) Immettere una breve descrizione della posizione in cui verrà depositata la chiave di ripristino. Questo testo verrà inserito nel messaggio visualizzato dall'utente all'attivazione di FileVault.
Chiave dispositivo	(Facoltativo) Immettere una stringa da includere nel testo di aiuto se l'utente sembra avere dimenticato la password.

10.10.4.21. Configurazione Opzioni FileVault

Questa configurazione permette all'amministratore di abilitare o disabilitare FileVault, distruggendo la chiave di FileVault quando il sistema passa alla modalità di standby.

Applicabile a: macOS 10.7 e versioni successive

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Digitare FileVault nel campo di ricerca, quindi fare clic sulla configurazione Opzioni FileVault.
3. Immettere un Nome e una Descrizione per la configurazione.
4. In Impostazioni configurazione, configurare le opzioni necessarie:
    - Elimina definitivamente la chiave FileVault quando il sistema passa in modalità standby
    - Non consentire la disattivazione della crittografia completa
    - Non consentire l'attivazione della crittografia completa
5. Fare clic su Avanti.
6. Selezionare l'opzione Abilita questa configurazione.
7. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzata.
8. Fare clic su Fine.

10.10.4.22. Certificato di identità

Argomenti della sezione:

- Impostazioni del certificato di identità
- Distribuzione della configurazione

Una configurazione del certificato di identità definisce un meccanismo di autenticazione del certificato per i dispositivi mobili. I certificati di identità sono certificati X.509 (.p12 o .pfx). Inoltre, i certificati di identità possono essere generati dinamicamente utilizzando l'autorità di certificazione come origine. Prima di avviare la procedura, è necessario conoscere le modalità di distribuzione dei certificati ai dispositivi mobili. Bisogna inoltre aver configurato ogni autorità di certificazione necessaria.

> A partire dalla release 91, il certificato Identità dispositivo per i dispositivi Apple viene rinnovato automaticamente entro 30 giorni dalla scadenza. I dispositivi iOS ricevono i certificati MDM rinnovati da Ivanti Neurons for MDM come parte del regolare flusso di check-in dei dispositivi. Tuttavia, i dispositivi iOS devono essere nuovamente registrati con Ivanti Neurons for MDM quando sono offline per un periodo di tempo sufficiente a far scadere il certificato MDM prima di un check-in che rinnoverebbe il certificato prima della scadenza.

- I certificati SHA-1 perdono l'approvazione quando si creano i certificati d'identità. È possibile scegliere altri algoritmi. Mentre si aggiornano i certificati, se quelli più datati utilizzano SHA-1, può essere utilizzato lo stesso algoritmo SHA-1. Se i certificati più datati utilizzano un algoritmo superiore a SHA-1, il passaggio a SHA-1 non è consentito.
- Dopo aver configurato un certificato di identità, è possibile fare clic su **Prova configurazione e continua** per emettere il certificato di prova e verificarne la validità. Se si esegue questo test per una configurazione nuova o esistente con certificato di identità generato dinamicamente, e il nome del soggetto coincide con quello dell'autorità di certificazione locale è possibile che venga visualizzato un errore. Se viene visualizzato questo messaggio di errore, è necessario modificare il nome del soggetto del certificato di identità, in modo che sia diverso da quello specificato per l'autorità di certificazione locale. Per le configurazioni esistenti del certificato di identità, se si modifica il nome del soggetto il certificato viene riemesso e viene ripetuto il push della configurazione.
  Se è stata configurata l'opzione che consente di creare una configurazione senza emettere il certificato di prova per la distribuzione del certificato **Generato dinamicamente**, fare clic su **Continua**.
- I certificati verranno riemessi implicitamente.
- Quando i certificati di identità sono assegnati alle app Android, l'app dell'utente ottiene i certificati di identità senza richiedere agli utenti di concedere l'autorizzazione (invece dell'app) per utilizzare il certificato. Sono incluse tutte le app come E-mail+, Gmail ecc.
- L'app Email+ può essere configurata con un certificato di identità fornito dall'utente, quindi è possibile eseguirne il push e assegnarla come configurazione app ai dispositivi con Android Enterprise. È applicabile solo alle modalità Profilo di lavoro su dispositivo di proprietà dell'azienda e Proprietario del dispositivo.

Impostazioni del certificato di identità

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Distribuzione dei certificati	Selezionare il tipo di distribuzione di certificato da impostare: • **File singolo**: caricare un certificato esistente per la distribuzione ai dispositivi. • **Generato dinamicamente**: creare certificati su richiesta tramite autorità di certificazione locale o esterna. • **Fornito dall'utente**: creare etichette per il tipo di certificati che verranno caricati dall'utente. Dopo aver creato le etichette, l'utente sarà in grado di visualizzare le etichette create (opzioni) nel portale self-service e di caricare i certificati corrispondenti a tali etichette. • **Credenziali derivate:** specificare uno dei seguenti utilizzi per le credenziali derivate: ◦ Autenticazione ◦ Crittografia ◦ Firma ◦ Decifratura • **Configurazione SCEP**: specificare come richiedere un certificato a un server SCEP. Selezionare una delle seguenti configurazioni: ◦ Configurazione Apple ◦ Configurazione Windows La selezione determina quali opzioni visualizzare nella parte restante del modulo.
Consenti a tutte le app di accedere alla chiave privata (macOS 10.10 e versioni successive) File singolo	**Applicabile a:** file singolo, generato dinamicamente, fornito dall'utente e certificati di identità SCEP Apple Config. (Facoltativo) Per i certificati PKCS#12, abilitare l'opzione **Consenti a tutte le app di accedere alla chiave privata** per consentire a tutte le app di accedere alla chiave privata. Ad esempio, questa chiave può essere utilizzata nei casi in cui l'utente deve immettere una password per consentire l'accesso a un certificato utilizzato per la VPN.
Dati del certificato di identità	Trascinare il file del certificato sulla casella tratteggiata oppure fare clic su **Scegli file** per selezionarlo dal proprio file system.
Password	Immettere la password di protezione del file del certificato PKCS#12. Tale password viene utilizzata per l'installazione senza richiesta di conferma.
Generato dinamicamente	
Origine	Selezionare l'autorità di certificazione locale dal menu a discesa. È necessario avere già creato questa autorità di certificazione in **Amministratore >** Gestione certificazione.
Crea configurazione senza emettere certificato di prova	Selezionare la casella di controllo per creare una configurazione senza emettere il certificato di prova.

Impostazione	Operazione da eseguire
Solo Windows - Archivio certificati di destinazione	Ora gli amministratori possono selezionare l'opzione Archivio certificati di destinazione sui dispositivi Windows.
Fornito dall'utente	
Nome visualizzato certificato	Immettere il nome del certificato. Il nome del certificato è univoco per un tenant e l'utente sarà in grado di visualizzare il nome nel portale self-service durante il caricamento del certificato.
Elimina la chiave privata	Selezionare questa opzione per eliminare la chiave privata del certificato dopo *n* (1-30) giorni. È possibile utilizzare anche le API fornite da Ivanti Neurons for MDM per queste operazioni. Fare riferimento alla Ivanti Neurons per MDM*Guida delle API* per ulteriori informazioni sulle API. Se si tenta di utilizzare questo certificato in qualsiasi configurazione (per esempio per autenticare un'applicazione o per inviare una configurazione di rete Wi-Fi o VPN) dopo che la relativa chiave privata è stata eliminata, l'attività non riesce. Assicurarsi che l'attività venga eseguita prima dell'eliminazione della chiave privata.
Elimina la chiave privata dopo giorni	Selezionare il numero di giorni (1-30) dopo i quali le chiavi private del certificato vengono cancellate. Il valore predefinito è di 2 giorni.
Credenziali derivate	
Utilizzo delle credenziali derivate	Selezionare una delle seguenti opzioni: • **Autenticazione** - Per specificare che le credenziali derivate vengono utilizzate a scopo di autenticazione. • **Cifratura** - Per specificare che le credenziali derivate vengono utilizzate per la cifratura. • **Firma** - Per specificare che le credenziali derivate vengono utilizzate per la firma. • **Decifratura** - Per specificare che le credenziali derivate vengono utilizzate per la decifratura.
Marchio	Specificare il provider di credenziali derivate in uso, selezionando una delle opzioni seguenti: • **Affida** • **Intercede** • **Purebred** Per aggiungere i provider di credenziali derivate personalizzati in uso, vedere **Provider di credenziali derivate**.
Configurazione ACME - Applicabile solo a iOS/iPadOS16+ /macOS14+	
Identificatore client	Una stringa unica che identifica un dispositivo specifico
URL directory	(Obbligatorio) L'URL della directory del server ACME. L'URL deve utilizzare lo schema https.
Uso esteso della chiave	Il valore è un array di stringhe. Ogni stringa è un OID in notazione punteggiata. Ad esempio, [”1.3.6.1.5.5.7.3.2”, “1.3.6.1.5.5.7.3.4”] indica l'autenticazione del cliente e la protezione della posta elettronica.

Impostazione	Operazione da eseguire
	Il dispositivo richiede questo campo per il certificato rilasciato dal server ACME. Il server ACME può sovrascrivere o ignorare questo campo nel certificato che emette.
Dimensione chiave	(Richiesto) I valori validi per KeySize dipendono dai valori di KeyType e HardwareBound. Per i requisiti specifici, consultare le chiavi.
Tipo di chiave	(Obbligatorio) Il tipo di coppia di chiavi da generare.
Oggetto	(Richiesto) Immettere un nome X.500 rappresentato come una matrice di OID e valori separati da virgola. Solitamente, l'oggetto è impostato sul nome di dominio completo dell'utente. Ad esempio, C=US,DC=com,DC=MobileIron,OU=InfoTech o CN=www.mobileiron.com. È inoltre possibile personalizzare l'oggetto aggiungendo una variabile all'OID. Ad esempio, CN=www.mobileiron.com-${{deviceGUID}}. Per semplificare la configurazione, è possibile anche utilizzare la variabile $ per popolare il campo Oggetto con il FQDN dell'utente. Non utilizzare il carattere barra rovesciata () nel nome dell'oggetto.
Nome alternativo oggetto	Il Nome alternativo oggetto che il dispositivo richiede per il certificato emesso dal server ACME. Il server ACME può sovrascrivere o ignorare questo campo nel certificato che emette.
Utilizzo chiave	Questo valore è un campo di bit. Il bit 0x01 indica la firma digitale. Il bit 0x10 indica l'accordo sulla chiave. Il dispositivo richiede questa chiave per il certificato rilasciato dal server ACME. Il server ACME può sovrascrivere o ignorare questo campo nel certificato che emette.
Vincolo hardware	Se l'opzione Vincolo hardware è impostata su true, la chiave privata è vincolata al dispositivo e solo allora il Tipo di chiave deve essere ECSECPrimeRandom e la Dimensione della chiave deve essere 256 o 384.
Attesta	Se vero, il dispositivo fornisce attestati che descrivono il dispositivo e la chiave generata al server ACME. Se Attesta è vero, anche Vincolo hardware deve essere vero.
SCEP Config - Configurazione Apple	
Certificato di identità (SCEP)	Selezionare questa opzione per specificare un server SCEP.
Autorità di certificazione locale	Selezionare questa opzione per specificare un'autorità di certificazione locale creata in precedenza tramite **Amministratore >** Gestione certificati. Selezionare l'autorità di certificazione locale dal menu a discesa che compare selezionando questa opzione.
URL	Immettere l'URL del server SCEP.
Identificatore CA	Immettere l'identificatore fornito dall'autorità di certificazione.
Oggetto	Immettere un nome X.500 rappresentato come una matrice di OID e valori separati da virgola. Solitamente, l'oggetto è impostato sul nome di dominio completo dell'utente. Ad esempio,

Impostazione	Operazione da eseguire
	C=US,DC=com,DC=MobileIron,OU=InfoTech o CN=www.mobileiron.com. È inoltre possibile personalizzare l'oggetto aggiungendo una variabile all'OID. Ad esempio, CN=www.mobileiron.com-$DEVICE_CLIENT_ID$. Per semplificare la configurazione, è possibile anche utilizzare la variabile $USER_DN$ per popolare il campo Oggetto con il FQDN dell'utente. Non utilizzare il carattere barra rovesciata (\) nel nome del soggetto.
Tipo di nome alternativo soggetto	Selezionare Nome RFC 822, Nome DNS, Uniform Resource Identifier o Nessuno, in base agli attributi del modello di certificato.
Valore del nome alternativo soggetto	Immettere il valore per il tipo corrispondente. Se si digita "$" come primo carattere, viene visualizzato un elenco a discesa con possibili attributi LDAP ed Entra ID personalizzati. Selezionare l'attributo personalizzato appropriato dall'elenco. Se il valore utilizzato è Entra ID, viene supportato solo 'onPremisesImmutableId'. Immettere fn:base64tohex($)
Nome principale NT	Immettere un nome soggetto alternativo per l'ambiente Microsoft. In genere questo viene configurato per includere il nome UPN (nome principale dell'utente) dell'utente.
Richiesta di verifica	(Facoltativo) Utilizzato come segreto già condiviso per l'iscrizione automatica
Tentativi	Selezionare un valore dall'elenco per impostare il numero di volte per cui verrà tentata l'autenticazione dopo la prima restituzione dello stato "In sospeso".
Intervallo tra tentativi	Selezionare un valore dall'elenco per impostare il numero di secondi da attendere prima di riprovare.
Dimensione chiave	Selezionare 1024, 2048 o 4096 bit.
Usa come firma digitale	Selezionare questa opzione se il certificato può essere utilizzato per la firma.
Usa come crittografia chiave	Selezionare questa opzione se il certificato può essere utilizzato per la cifratura.
Impronta digitale CA	Se l'autorità di certificazione utilizza HTTP, immettere la stringa esadecimale da utilizzare come impronta digitale del certificato di CA. Sono supportate le impronte digitali MD5. Se si preferisce, è possibile creare un'impronta digitale dal certificato. È sufficiente trascinare il certificato all'interno dell'area designata o fare clic su **Crea da certificato** per selezionare il certificato dal proprio file system.
Configurazione SCEP - Configurazione per Windows	
CA (autorità di certificazione)	Selezionare questa opzione per specificare un'autorità di certificazione creata in precedenza tramite **Amministratore >** Gestione certificati. Selezionare l'autorità di certificazione dall'elenco a discesa che viene visualizzato quando si seleziona questa opzione.

Impostazione	Operazione da eseguire
Oggetto	Immettere un nome X.500 rappresentato come una matrice di OID e valori separati da virgola. Solitamente, l'oggetto è impostato sul nome di dominio completo dell'utente. Ad esempio, C=US,DC=com,DC=MobileIron,OU=InfoTech o CN=www.mobileiron.com. È inoltre possibile personalizzare l'oggetto aggiungendo una variabile all'OID. Ad esempio, CN=www.mobileiron.com-$DEVICE_CLIENT_ID$. Per semplificare la configurazione, è possibile anche utilizzare la variabile $USER_DN$ per popolare il campo Oggetto con il FQDN dell'utente. Non utilizzare il carattere barra rovesciata (\) nel nome del soggetto.
Tipo di nome alternativo soggetto	Fare clic su **+ Aggiungi** per selezionare Nome RFC 822, Nome DNS, Uniform Resource Identifier o Nessuno, in base agli attributi del modello di certificato.
Tentativi	Selezionare un valore dall'elenco per impostare il numero di volte per cui verrà tentata l'autenticazione dopo la prima restituzione dello stato "In sospeso".
Intervallo tra tentativi	Selezionare un valore dall'elenco per impostare il numero di secondi da attendere prima di riprovare.
Lunghezza della chiave	Specificare la dimensione della chiave, selezionando 1024, 2048 o 4096 bit.
Selezione dell'utilizzo	Selezionare almeno una delle opzioni seguenti: • Usa come firma digitale - Selezionare questa opzione se il certificato può essere utilizzato per la firma. • Usa come cifratura chiave - Selezionare questa opzione se il certificato può essere utilizzato per la cifratura.
Validità	Selezionare il periodo di validità in giorni, mesi o anni.
Identificazione personale CA	Se l'autorità di certificazione utilizza HTTP, immettere la stringa esadecimale da utilizzare come impronta digitale del certificato di CA. Sono supportate le impronte digitali MD5. Se si preferisce, è possibile creare un'impronta digitale dal certificato. È sufficiente trascinare il certificato all'interno dell'area designata o fare clic su **Crea da certificato** per selezionare il certificato dal proprio file system.
Famiglia di algoritmi hash	Selezionare gli algoritmi SHA-2 o SHA-3.

Quando si applica un certificato di identità a un profilo di lavoro su un dispositivo senza impostare un passcode per la richiesta di verifica del lavoro, il dispositivo richiede un passcode del dispositivo invece di un passcode per la richiesta di verifica del lavoro.

Per maggiori informazioni, vedere **Utilizzo delle configurazioni**.

10.10.4.23. Configurazione blocco attivazione Apple

Licenza: Silver

Argomenti della sezione:

- Attivazione del Blocco attivazione iOS
- Attivare la funzione Blocco attivazione iOS nei dispositivi supervisionati
- Attivazione del Blocco attivazione macOS
- Attivare la funzione Blocco attivazione macOS nei dispositivi supervisionati
- Utilizzo del codice bypass di Blocco attivazione iOS
- Cancellazione del codice bypass di Blocco attivazione iOS

Blocco attivazione è una funzione di Apple progettata per impedire a chiunque di utilizzare un dispositivo smarrito o rubato. Dopo l'abilitazione la funzionalità Dov'è, viene salvata una mappatura tra l'account iCloud e un identificatore hardware del dispositivo nei server di attivazione di Apple. Da quel momento, nessun utente può disabilitare l'opzione Trova il mio dispositivo, cancellare i dati del dispositivo o riattivarlo senza immettere l'ID e la password Apple esistenti. Se una persona diversa dall'utente cancella i dati del dispositivo e cerca successivamente di riattivarlo e utilizzarlo, nell'Assistente configurazione verranno richiesti l'ID e la password Apple.

La disattivazione di Blocco attivazione non disabiliterà questa funzione sui dispositivi supervisionati se l'utente finale ha abilitato Trova il mio dispositivo. L'Assistente configurazione chiede all'utente di intervenire se il dispositivo viene reimpostato o cancellato da remoto.

Blocco attivazione fornisce un maggior numero di opzioni agli amministratori per impedire il furto dei dispositivi supervisionati. Tuttavia, è probabile che la maggior parte degli amministratori aziendali lasci disabilitata Blocco attivazione, poiché si tratta principalmente di una funzionalità lato utente. La tabella sottostante mostra un riepilogo delle opzioni per le distribuzioni soggette all'azienda:

Tipo di dispositivo	Risultato
Soggetto all'azienda e supervisionato	• Per impostazione predefinita, Blocco attivazione è disabilitata per i dispositivi supervisionati. • Gli utenti dei dispositivi non possono attivare Blocco attivazione.
Soggetto all'azienda e non supervisionato	• La funzione Blocco attivazione viene abilitata non appena l'utente finale effettua l'accesso a iCloud utilizzando l'ID Apple personale e attiva l'opzione Trova il mio dispositivo. • I server MDM, incluso Ivanti Neurons for MDM, non possono controllare la funzione Blocco attivazione sui dispositivi non supervisionati. Gli utenti dei dispositivi possono bloccare l'attivazione utilizzando le proprie credenziali personali, creando problemi nel caso in cui decidano di lasciare l'azienda.

Attivazione del Blocco attivazione iOS

Valido per: dispositivi supervisionati con iOS 7 e versioni successive

Questa configurazione viene applicata ai dispositivi supervisionati (iOS 7 e versioni successive) in cui la funzionalità **Trova il mio dispositivo** è abilitata. Se un amministratore o un altro utente prova a cancellare, attivare o a disattivare la funzionalità Trova

dispositivo personale nel dispositivo, viene visualizzata la schermata Blocco di attivazione Apple. Per continuare, è necessario immettere le credenziali iTunes o un codice bypass.

Il codice bypass per i dispositivi supervisionati viene memorizzato al momento dell'attivazione ed è possibile visualizzarlo nei dettagli del dispositivo. È possibile inviare da remoto il codice bypass utilizzando il comando "Cancella blocco attivazione" per i dispositivi supervisionati. Tuttavia, è necessario immettere manualmente il codice quando si riattiva un dispositivo o quando si disattiva la funzionalità Trova dispositivo personale.

> È possibile creare una sola Configurazione blocco attivazione per tutti gli spazi.

Attivare la funzione Blocco attivazione iOS nei dispositivi supervisionati

Procedura

1. Abilitare la funzionalità **Trova il mio dispositivo**.
2. Accedere a **Configurazioni**.
3. Selezionare la configurazione **Blocco attivazione Apple** nell'elenco di configurazioni esistenti.
4. Fare clic su **Modifica**.
5. Nella sezione Dispositivi supervisionati con iOS 7 e versioni successive, fare clic su **Abilita blocco attivazione**.
6. Fare clic su **Fine**.
7. Registrare il dispositivo.

Attivazione del Blocco attivazione macOS

Valido per: dispositivi supervisionati con iOS 10.15 e versioni successive

Questa configurazione sarà applicata ai dispositivi supervisionati macOS 10.15 e versioni successive. Il Blocco di attivazione su macOS si applica solo ai dispositivi Mac dotati del chip di protezione Apple T2. Il Blocco di attivazione è disattivato per impostazione predefinita sui dispositivi supervisionati, aggiornati o installati di recente, e sui dispositivi registrati aggiornati di recente. L'abilitazione di Trova il mio dispositivo non abilita automaticamente il Blocco di attivazione su questi dispositivi

Se un amministratore o un altro utente tenta di cancellare, attivare o disabilitare la funzionalità Trova il mio dispositivo, viene visualizzata la schermata Blocco attivazione Apple. Per continuare, è necessario immettere le credenziali iTunes o un codice bypass. Il codice bypass per i dispositivi supervisionati viene memorizzato al momento dell'attivazione ed è possibile visualizzarlo nei dettagli del dispositivo. È possibile inviare da remoto il codice bypass utilizzando il comando "Cancella blocco attivazione" per i dispositivi supervisionati. Tuttavia, è necessario immettere il codice manualmente quando si riattiva un dispositivo o quando si disattiva la funzionalità Trova il mio dispositivo.

> È possibile creare una sola Configurazione blocco attivazione per tutti gli spazi.

Attivare la funzione Blocco attivazione macOS nei dispositivi supervisionati

Procedura

1. Abilitare la funzionalità Trova il mio dispositivo.
2. Accedere a **Configurazioni**.
3. Selezionare la configurazione **Blocco attivazione Apple** nell'elenco di configurazioni esistenti.

4. Fare clic su **Modifica**.
5. Nella sezione Dispositivi supervisionati con macOS 10.15 e versioni successive, fare clic su **Abilita blocco attivazione**.
6. Fare clic su **Fine**.
7. Registrare il dispositivo.

Utilizzo del codice bypass di Blocco attivazione iOS

Quando vengono cancellati i dati del dispositivo mentre è attivata la funzione Blocco attivazione iOS, il codice bypass viene memorizzato sul server di attivazione di Apple e nell'interfaccia di amministrazione di Ivanti Neurons for MDM.

Procedura

1. Andare su **Dispositivi**.
2. Selezionare il dispositivo.
3. Fare clic su **Azioni > Cancella**. Il riavvio del dispositivo potrebbe richiedere alcuni minuti.
4. Quando il dispositivo richiede di immettere l'ID Apple e la password, lasciare vuoto il campo **ID Apple**.
5. Immettere il codice bypass nel campo **password**.
6. Fare clic su **Avanti**.
7. Procedere con la configurazione.

Cancellazione del codice bypass di Blocco attivazione iOS

Se si deseleziona Blocco attivazione iOS nell'interfaccia di amministrazione di Ivanti Neurons for MDM, il codice di bypass viene rimosso dal server di attivazione Apple, ma continua a essere indicato nei dettagli del dispositivo nell'interfaccia di amministrazione di Ivanti Neurons for MDM.

Procedura

1. Andare in **Dispositivi**.
2. Selezionare il dispositivo.
3. Selezionare **Configurazioni**.
4. Selezionare **Blocco attivazione Apple**.
5. Fare clic su **Modifica**.
6. Nella sezione Dispositivi supervisionati con iOS 7 e versioni successive, disabilitare **Abilita blocco attivazione**.
7. Fare clic su **Fine**.
8. Andare in **Dispositivi**.
9. Selezionare il dispositivo.
10. Fare clic su **Azioni > Cancella**. Il riavvio del dispositivo potrebbe richiedere alcuni minuti. Il dispositivo può ora essere impostato con l'AppleID e la password del nuovo utente.
11. Procedere con la configurazione.

Nell'interfaccia, lo stato del comando Cancella blocco attivazione iOS viene visualizzato come segue:

Stato	Risultato
In sospeso	• Il server sta inviando il codice del comando Cancella blocco attivazione a Apple.
Inviato	• Apple riconosce la ricezione del codice del comando Cancella blocco attivazione.
Non riuscito	• Il server non è riuscito a inviare il codice a Apple. • Apple ha segnalato un errore.

10.10.4.24. Configurazione personalizzata iOS

Una configurazione personalizzata di iOS consente di caricare e distribuire un profilo di configurazione di iOS creato da un'applicazione diversa, come iPhone Configuration Utility di Apple.

Impostazioni personalizzata di iOS

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Dati file	Trascinare e rilasciare il file di configurazione oppure fare clic su **Scegli file** per selezionarlo dal proprio file system.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.4.25. Impostazioni Intelligence

Utilizzare le impostazioni di Intelligence per configurare le impostazioni di Apple Intelligence sui dispositivi supervisionati. Questa dichiarazione aiuta gli amministratori ad applicare controlli coerenti basati su criteri che gestiscono il modo in cui i dispositivi accedono e utilizzano le funzionalità di Apple Intelligence.

Applicabile a:

- iOS 26.4+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.
- macOS 26.4+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.
- visionOS 26.4+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Impostazioni Intelligence**.
3. Configurare le **Impostazioni Intelligence** come da tabella seguente:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Consenti report Intelligence Apple	Selezionare la casella di controllo per abilitare il report Apple Intelligence. Utilizzare il pulsante **Esegui push al dispositivo** per attivare Apple Intelligence Report sui dispositivi supervisionati.
Consenti Genmoji	Selezionare la casella di controllo per abilitare Genmoji. Utilizzare il pulsante **Esegui push al dispositivo** per attivare Genmoji su dispositivi supervisionati.
Consenti Image Playground	Selezionare la casella di controllo per abilitare Playground immagine. Utilizzare il pulsante **Esegui push al dispositivo** per attivare Playground immagine sui dispositivi supervisionati.
Consenti Image Wand	Selezionare la casella di controllo per abilitare la bacchetta Immagine. Utilizzare il pulsante **Esegui push al dispositivo** per abilitare la bacchetta Immagine sui dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi macOS.
Consenti bacchetta risultati di scrittura personalizzata	Selezionare la casella di controllo per abilitare la bacchetta Risultati scrittura manuale personalizzata. Utilizzare il pulsante **Esegui push al dispositivo** per attivare la bacchetta Risultati scrittura manuale personalizzata sui dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi macOS e visionOS.
Consenti riepilogo Visual Intelligence	Selezionare la casella di controllo per abilitare Riepilogo Visual Intelligence. Utilizzare il pulsante **Esegui push al dispositivo** per attivare il Riepilogo Visual Intelligence sui dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi macOS e visionOS.
Consenti Writing Tools	Selezionare la casella di controllo per abilitare Strumenti di scrittura. Utilizzare il pulsante **Esegui push al dispositivo** per attivare gli Strumenti di scrittura sui dispositivi supervisionati.
Imponi dettatura dispositivo solo su dispositivo	Selezionare la casella di spunta per attivare la dettatura solo su dispositivo. Utilizzare il pulsante **Esegui push al dispositivo** per attivare la dettatura solo su dispositivo sui dispositivi supervisionati.
Imponi Traduzione solo su dispositivo	Selezionare la casella di spunta per attivare Traduzione solo su dispositivo. Utilizzare il pulsante **Esegui push al dispositivo** per attivare Traduzione solo su dispositivo sui dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi macOS e visionOS.
App	
Calendario	

Impostazione	Operazione da eseguire
Consenti modifica in linguaggio naturale	Selezionare la casella di controllo per abilitare la modifica in linguaggio naturale in Calendario e Promemoria. Attivare il pulsante **Esegui push al dispositivo** per attivare la modifica in linguaggio naturale nel Calendario e nei Promemoria sui dispositivi supervisionati.
E-mail	
Consenti Risposte smart	Selezionare la casella di controllo per abilitare le Risposte smart. Utilizzare il pulsante **Esegui push al dispositivo** per attivare le Risposte smart sui dispositivi supervisionati.
Consenti riepilogo	Selezionare la casella di controllo per abilitare Riepilogo. Utilizzare il pulsante **Esegui push al dispositivo** per attivare Riepilogo sui dispositivi supervisionati.
Note	
Consenti trascrizione	Selezionare la casella di controllo per abilitare la Trascrizione. Utilizzare il pulsante **Esegui push al dispositivo** per attivare la trascrizione su dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi VisionOS.
Consenti Riepilogo trascrizione	Selezionare la casella di controllo per abilitare Riepilogo trascrizione. Utilizzare il pulsante **Esegui push al dispositivo** per attivare Riepilogo trascrizione sui dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi visionOS.
Safari	
Consenti riepilogo	Selezionare la casella di controllo per abilitare Riepilogo. Utilizzare il pulsante **Esegui push al dispositivo** per attivare Riepilogo sui dispositivi supervisionati.

4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
5. Selezionare una delle opzioni di distribuzione per impostare la configurazione di **Impostazioni Intelligence**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere Utilizzo delle configurazioni.
6. Fare clic su **Fine**.

10.10.4.26. Restrizioni iOS

Le restrizioni di iOS sono impostazioni che aiutano l'utente principale del dispositivo a controllare ciò che gli altri utenti possono fare con i dispositivi iOS, watchOS e visionOS. Queste impostazioni sono definite da Apple e gestite da Ivanti Neurons for MDM.

Durante la distribuzione di questa configurazione agli **iPad condivisi**, è possibile selezionare il canale dispositivi o il canale utenti. Questo è utile per distribuire configurazioni separate e applicare restrizioni che sono applicabili solo al canale dispositivi o al canale utenti.

Gli amministratori globali possono delegare gli amministratori di spazi per modificare la configurazione per **Tutti i dispositivi e per l'opzione di distribuzione personalizzata**. Per la configurazione Limitazione iOS, è possibile selezionare l'opzione **Consenti che questa configurazione sia disponibile in tutti gli spazi**.

> Le modifiche alla distribuzione sono applicabili solo allo spazio specifico. Tutti gli altri spazi continuano a ereditare le impostazioni di distribuzione predefinite.

Impostazioni delle restrizioni per iOS

Categoria	Impostazione	Operazione da eseguire
Funzionalità dispositivo	Nome Descrizione **Tutte le versioni di iOS**	Immettere un nome identificativo della configurazione. Immettere una descrizione esplicativa dello scopo della configurazione. **Permette di utilizzare le funzionalità del dispositivo.**
	Consenti screenshot e registrazioni schermo	Selezionare questa opzione per consentire all'utente del dispositivo di acquisire le schermate tramite la funzione di acquisizione schermo iOS integrata.
	Consenti osservazione schermo remoto (iOS 9.3 e versioni successive)	Selezionare per consentire all'utente di osservare lo schermo remoto.
	Consenti osservazione schermo classe gestito non richiesta (solo supervisione - iOS 10.3+)	(Valido solo per iPad) Selezionare questa opzione per mostrare messaggi non richiesti sullo schermo quando un iPad supervisionato viene configurato con classi gestite.
	Consenti la sincronizzazione automatica durante il roaming	Selezionare questa opzione per consentire la sincronizzazione degli account di posta quando il dispositivo si trova al di fuori del Paese di residenza.
	Consenti Siri	Selezionare questa opzione per consentire l'app dell'assistente personale sui dispositivi supportati.
	Consenti Siri quando il dispositivo è bloccato Abilita il filtro contro le volgarità di Siri (solo Supervisione)	Selezionare questa opzione per consentire all'app dell'assistente personale di eseguire delle attività anche quando il dispositivo è bloccato. Selezionare per abilitare il Filtro contro le volgarità di Siri.
	Consenti la composizione	Selezionare questa opzione per consentire agli utenti di chiamare un contatto o un numero parlando con il dispositivo.

Categoria	Impostazione	Operazione da eseguire
	vocale	
	Consenti l'acquisto di In-App	Selezionare questa opzione per consentire agli utenti di effettuare acquisti tramite le app in esecuzione sul dispositivo.
	Consenti Passbook quando il dispositivo è bloccato	Selezionare questa opzione per consentire la visualizzazione delle notifiche Passbook quando il dispositivo è bloccato.
	Consenti schermata di blocco Centro di controllo	Selezionare questa opzione per consentire l'accesso al Centro di controllo dalla schermata di blocco.
	Consenti schermata di blocco visualizzazione Notifiche	Selezionare questa opzione per consentire la visualizzazione delle notifiche sulla schermata di blocco.
	Consenti schermata di blocco visualizzazione Oggi	Selezionare questa opzione per consentire l'accesso alla visualizzazione Oggi dalla schermata di blocco.
	Consenti Apri in da app gestite a non gestite	**È necessaria la licenza Gold**. Selezionare questa opzione per consentire l'apertura in app e account gestiti di documenti relativi ad app e account non gestiti. Se questa opzione viene disabilitata, non sarà possibile effettuare lo scambio di documenti da app e account gestiti verso app e account non gestiti. Ad esempio, si consiglia di impedire l'apertura dei documenti aziendali mediante le app personali. È possibile utilizzare questa opzione (disattivazione) anche con una configurazione dei domini gestiti per garantire che i dati scaricati dai domini gestiti possano essere aperti soltanto nell'app gestita.
	Consenti Apri in da app gestite a non gestite	**È necessaria la licenza Gold**. Selezionare questa opzione per consentire l'apertura in app e account gestiti di documenti relativi ad app e account non gestiti. Se questa opzione viene disabilitata, non sarà possibile effettuare lo scambio di documenti da app e account non gestiti verso app e account gestiti. Ad esempio, si consiglia di impedire agli utenti l'invio di documenti personali tramite l'indirizzo e-mail aziendale. È possibile inoltre utilizzare questa opzione (disattivazione) anche con una configurazione dei domini gestiti per garantire che i dati scaricati dai domini non gestiti non possano essere aperti nelle app gestite.
	Richiedi passcode al primo abbinamento AirPlay	Selezionare questa opzione per richiedere alla Apple TV di visualizzare un passcode che l'utente deve inserire nel dispositivo iOS per autorizzare l'abbinamento iniziale dei dispositivi.
	Forza la password sulle richieste	Selezionare per richiedere all'utente di immettere la password per tutte le richieste in arrivo di AirPlay.

Categoria	Impostazione	Operazione da eseguire
	AirPlay in entrata (tvOS fino a 10.1) **iOS 26+** App esenti dalle restrizioni di classificazione (applicabile per iOS 26.1+)	Impostazione predefinita: deselezionato Inserire l'elenco delle app che si desidera esentare dalle restrizioni di classificazione in base all'età solo se i loro ID bundle sono inclusi nell'intersezione di tutti gli elenchi di esenzioni provenienti da più payload e app di controllo parentale come ScreenTime. Predefinito: selezione
	Dispositivi supervisionati con tutte le versioni di iOS	
	Consenti libri Apple	Selezionare questa opzione per consentire l'accesso all'app libri Apple.
	Consenti contenuti sessualmente espliciti in iBooks Store (iOS e tvOS 11.3 e versioni successive) Consenti modifica account Consenti modifica rete dati app Consenti modifica di Trova i miei amici	Selezionare questa opzione per consentire agli utenti di scaricare da iBooks Store del materiale contrassegnato come erotico. Selezionare questa opzione per consentire agli utenti dei dispositivi iOS 7 supervisionati di aggiungere account e-mail e di apportare delle modifiche agli account e-mail già configurati. Selezionare questa opzione per consentire agli utenti di apportare modifiche alle impostazioni della rete dati per le app. Selezionare questa opzione per consentire agli utenti di effettuare delle modifiche alle impostazioni dell'app Trova i miei amici.
	Consenti il pairing con host non basati su configuratore	Selezionare questa opzione per consentire l'abbinamento host per la sincronizzazione iTunes. L'attivazione di questa opzione consente ai dispositivi supervisionati di effettuare la sincronizzazione con iTunes su un Mac diverso dall'host di supervisione. Se questa opzione viene disabilitata, verranno disattivati tutti gli abbinamenti host tranne che quello dell'host di supervisione. Se non è stato configurato nessun certificato host di supervisione, vengono disattivati tutti gli abbinamenti.
	Consenti AirDrop	Selezionare questa opzione per consentire l'utilizzo di AirDrop sul dispositivo. AirDrop è il sistema Wi-Fi specifico di Apple che consente la condivisione di file con gli utenti che si trovano nelle vicinanze. Limitando questa funzione, i documenti personali non verranno inviati a dispositivi non autorizzati o non protetti.

Categoria	Impostazione	Operazione da eseguire
	Consenti ID tocco/ID faccia per sbloccare il dispositivo	Selezionare questa opzione per consentire ID tocco o ID faccia per sbloccare i dispositivi.
	Consenti alla ricerca di Spotlight di tornare ai risultati ricerche in Internet	Selezionare questa opzione per consentire alla ricerca di Spotlight di restituire i risultati delle ricerche in Internet.
	Consenti app in modalità app singola	Immettere un elenco separato da virgole di ID bundle per le app che possono attivare in autonomia la modalità Single-App sui dispositivi supervisionati con iOS. Ad esempio, è possibile specificare app per esami personalizzate per gli studenti. Quando lo studente avvia l'app, quest'ultima attiva la modalità Single-App per assicurare che lo studente non possa utilizzare altre risorse durante lo svolgimento dell'esame. Questa funzione si applica alle app sviluppate per l'attivazione della modalità autonoma Single App. La supervisione viene stabilita tramite Apple Configurator.
	iOS 8 e versioni successive	
	Consenti copia dei libri dell'azienda	Selezionare questa opzione per consentire il backup personale dei documenti iBooks, ePub e PDF inviati al dispositivo tramite MDM.
	Consenti sincronizzazione delle note e dei punti salienti dei libri dell'azienda	Selezionare questa opzione per consentire la sincronizzazione delle note e dei punti salienti aggiunti ai libri dell'azienda su iTunes.
	Forza rilevamento polsi Apple Watch	Selezionare questa opzione per nascondere le notifiche su schermo, a meno che qualcuno non indossi l'Apple Watch.
	Dispositivi supervisionati con iOS 8 o versioni successive	
	Consenti tastiera predittiva	Selezionare questa opzione per consentire agli utenti di abilitare la predizione iOS della parola digitata, in modo che gli utenti tocchino una delle tre predizioni per completare la parola.
	Consenti correzione automatica tastiera	Selezionare questa opzione per consentire l'utilizzo della correzione automatica con tastiere Bluetooth.
	Consenti controllo ortografia tastiera	Selezionare questa opzione per consentire il controllo ortografia con tastiere Bluetooth.

Categoria	Impostazione	Operazione da eseguire
	Consenti ricerca definizioni tastiera	Selezionare questa opzione per consentire la ricerca delle definizioni con tastiere Bluetooth.
	Consenti modifica delle impronte digitali Touch ID/facce Face ID **iOS 9 e succ. supervisionato**	Selezionare questa opzione per consentire la modifica delle impostazioni di ID tocco o ID faccia.
	Consenti scelte rapide da tastiera su dispositivi iPad	Seleziona per consentire l'uso dei tasti a scelta rapida sull'iPad.
	Consenti modifica dello sfondo	Seleziona per consentire agli utenti di cambiare le immagini dello sfondo.
	Consenti l'abbinamento con l'Apple Watch	Selezionare questa opzione per consentire l'abbinamento dell'iPhone con l'Apple Watch.
	Consenti modifica del nome dispositivo	Selezionare questa opzione per consentire all'utente di cambiare il nome del dispositivo.
	Consenti modifica impostazione di attendibilità app aziendali	Selezionare questa opzione per consentire all'utente di cambiare le impostazioni di trust delle app aziendali.
	Dispositivi supervisionati con iOS 9.3 e versioni successive Consenti la modifica delle impostazioni di notifica	Selezionare questa opzione per consentire agli utenti di cambiare le impostazioni delle notifiche.
	Dispositivi supervisionati con iOS 9.3.2 e versioni successive Consenti modifica invio diagnostica	Selezionare questa opzione per consentire agli utenti di modificare le impostazioni relative all'invio di dati diagnostici ad Apple.

Categoria	Impostazione	Operazione da eseguire
	iOS 10 e succ. supervisionato	
	Consenti modifica Bluetooth **Dispositivi supervisionati con iOS 10.3 o versioni successive**	Selezionare questa opzione per consentire all'utente di modificare l'impostazione Bluetooth sui dispositivi supervisionati. Utile in casi come iPad condivisi utilizzati per l'app Classroom for Education, in cui per eseguire l'app è necessario il Bluetooth.
	Consenti dettatura	Selezionare questa opzione per consentire all'utente di usare i comandi vocali su iPhone o iPad, invece della digitazione.
	Dispositivi supervisionati con iOS 11 e versioni successive	
	Consenti AirPrint	Selezionare questa opzione per consentire la funzionalità AirPrint per la stampa wireless.
	Consenti archiviazione credenziali AirPrint Consenti identificazione iBeacon di AirPrint	Selezionare questa opzione per consentire l'archiviazione portachiavi del nome utente e della password per AirPrint. Selezionare questa opzione per consentire all'utente di impostare l'identificazione iBeacon delle stampanti AirPrint.
	Consenti aggiunta di configurazioni VPN	Selezionare questa opzione per consentire all'utente di creare una configurazione VPN.
	Imponi requisito TLS attendibile di Airprint Consenti rimozione app di sistema	Selezionare questa opzione per consentire certificati attendibili per la comunicazione di stampa TLS. Impostazione predefinita: deselezionato Selezionare questa opzione per consentire la rimozione dell'app di sistema.
	Consenti modifica impostazioni piano cellulare	Selezionare questa opzione per consentire agli utenti di modificare le impostazioni del piano cellulare.

Categoria	Impostazione	Operazione da eseguire
	Consenti configurazione nuovi dispositivi vicini	Selezionare questa opzione per consentire agli utenti di configurare i nuovi dispositivi vicini.
	Partecipa automaticamente ai corsi di Classroom senza chiedere	Selezionare questa opzione per consentire agli utenti di partecipare automaticamente ai corsi di Classroom senza chiedere. Impostazione predefinita: deselezionato
	Consenti a Classroom di bloccare un'app e bloccare il dispositivo senza chiedere	Selezionare questa opzione per consentire a Classroom di bloccare un'app e bloccare il dispositivo senza chiedere all'utente. Impostazione predefinita: deselezionato
	Imporre all'utente di autenticarsi prima di poter inserire in automatico i dati di password o carte di credito in Safari e nelle app	Il proprietario del dispositivo deve autenticarsi prima che le password o le informazioni della carta di credito possano essere compilate automaticamente nel browser Safari e nelle applicazioni. Impostazione predefinita: false
	iOS 11.3 e versioni successive	
	Consenti abbinamento con app remota (tvOS 11.3 e versioni successive)	Selezionare questa opzione per consentire l'abbinamento del dispositivo con l'app remota.
	Consenti richieste AirPlay in entrata (tvOS 11.3 e versioni successive)	Selezionare per consentire le richieste di AirPlay in entrata.
	iOS 11.3 e succ. supervisionato	
	Consenti modalità limitata USB	Selezionare questa opzione per consentire all'utente di accedere alla modalità limitata USB.
	Rimanda aggiornamenti	Selezionare questa opzione per immettere il numero di giorni per cui si desidera rimandare gli aggiornamenti software. L'impostazione predefinita è 30 giorni e il valore massimo è 90 giorni.

Categoria	Impostazione	Operazione da eseguire
	software di 30 giorni (per iOS 11.3, tvOS 12.2 e versioni successive, solo per i dispositivi supervisionati)	Impostazione predefinita: deselezionato
	Richiedi autorizzazione insegnante per abbandonare corsi non gestiti da Classroom Dispositivi supervisionati con iOS 12 e versioni successive	Selezionare questa opzione per consentire all'utente di ottenere l'autorizzazione da parte dell'insegnante necessaria per abbandonare i corsi non gestiti da Classroom.
	Forza data e ora automatiche (iOS 12.0 e tvOS 12.2 e versioni successive)	Selezionare per attivare la funzionalità “Imposta automaticamente” di data e ora. Essa non può essere disattivata dall'utente. Impostazione predefinita: false
	Consenti modifica impostazioni di eSIM (iPhone XS, iPhone XS Max e iPhone XR - iOS 12.1 e versioni successive)	Selezionare questa opzione per consentire all'utente di modificare la configurazioni eSim sui dispositivi supervisionati. Questa opzione impedisce inoltre agli utenti di aggiungere o rimuovere un piano cellulare nelle impostazioni dei dispositivi. Impostazione predefinita: true
	Dispositivi supervisionati con iOS 12.2 o versioni successive Consenti modifica impostazioni dell'hotspot personale	Selezionare questa opzione per consentire all'utente di modificare le impostazioni di Hotspot personale. Impostazione predefinita: true
	iOS 13.0 e versioni successive	

Categoria	Impostazione	Operazione da eseguire
	Consenti Accesso unità di rete File	Selezionare questa opzione per consentire all'utente di connettersi alle unità di rete nell'app File. Impostazione predefinita: true
	Consenti Accesso unità USB file **Dispositivi supervisionati con iOS 13.0 o versioni successive**	Selezionare questa opzione per consentire all'utente di connettersi a qualsiasi dispositivo USB connesso nell'app File. Impostazione predefinita: true
	Consenti tastiera Continuous Path Consenti Sospensione dispositivo	Selezionare per abilitare la tastiera percorso continuo (scorrimento o trace typing) Impostazione predefinita: true Selezionare per abilitare la sospensione dispositivo. Impostazione predefinita: true
	Consenti Trova dispositivo	Selezionare per abilitare Trova il mio dispositivo in Trova la mia app. Impostazione predefinita: true
	Consenti Trova il mio amico Forza attivazione Wi-Fi **iOS 13.4 e versioni successive**	Selezionare per abilitare Trova i miei amici in Trova la mia app. Impostazione predefinita: true Selezionare per abilitare la potenza Wi-Fi in modo che sia nello stato attivo. Impostazione predefinita: false
	Consenti sessione guest per iPad condivisi **iOS 14.0 e versioni successive**	Se ha valore false, le sessioni temporanee non sono disponibili per gli iPad condivisi. Impostazione predefinita: true
	Consenti pubblicità personalizzata di Apple **Dispositivi supervisionati con**	Se ha valore false, limita la pubblicità personalizzata di Apple. Questa restrizione impedirà ad Apple di utilizzare le informazioni dell'utente per proporre annunci pubblicitari mirati. Questo potrebbe non ridurre il numero di annunci ricevuti, ma gli annunci saranno meno rilevanti per l'utente. Impostazione predefinita: true

Categoria	Impostazione	Operazione da eseguire
	iOS 14.0 e versioni successive Consenti App Clips	Se ha valore false, impedisce all'utente di aggiungere App Clips e di rimuovere App Clips esistenti sul dispositivo. Impostazione predefinita: true
	Dispositivi supervisionati con iOS 14.2 o versioni successive Consenti NFC	Se false, disabilita NFC. Richiede un dispositivo supervisionato. Disponibile su iOS 14.2 e versioni successive. Impostazione predefinita: true
	iOS 14.5+	
	Consenti sblocco automatico	Gli amministratori possono utilizzare la restrizione allowAutoUnlock esistente per gestire questa funzionalità. Se ha valore false, non consente lo sblocco automatico. Disponibile in macOS 10.12 e versioni successive e in iOS 14.5 e versioni successive. Impostazione predefinita: true
	Forza dettatura solo su dispositivo	Se ha valore true, disabilita le connessioni ai server Siri ai fini della dettatura. Impostazione predefinita: false
	Dispositivi supervisionati con iOS 14.5 o versioni successive Consenti avvio esterno non corrispondente per il recupero	Se ha valore true, consente l'avvio dei dispositivi in modalità di ripristino da parte di un dispositivo non abbinato. Impostazione predefinita: false
	Forza Wi-Fi solo su reti consentite	Se ha valore true, il dispositivo può connettersi esclusivamente alle reti Wi-Fi impostate tramite il profilo di configurazione. Impostazione predefinita: false Se la limitazione **Forza Wi-Fi solo su reti consentite** è attiva e la configurazione del Wi-Fi non è distribuita nel dispositivo, la connessione Wi-Fi viene persa.
	iOS 15 e versioni successive	

Categoria	Impostazione	Operazione da eseguire
	Forza traduzione solo su dispositivo	Se ha valore True, il dispositivo non si connette ai server Siri ai fini della traduzione. Impostazione predefinita: false
	Richiedi area di montaggio gestita **iOS 15.2+** Consenti protezione privacy e-mail	Se ha valore True, la funzionalità di Copia e Incolla rispetta le limitazioni allowOpenFromManagedToUnmanaged e allowOpenFromUnmanagedToManaged. Impostazione predefinita: false Se falso, disabilita la protezione privacy e-mail sul dispositivo. Disponibile su iOS 15.2 e versioni successive. Quando la configurazione Consenti protezione della privacy della posta è installata e attivata dal portale amministrativo Ivanti Neurons per MDM, il selettore Proteggi attività di posta è attivato sul dispositivo e sono visibili le seguenti opzioni: • **Nascondi indirizzo IP** - Il mittente dell'e-mail non può collegare l'e-mail alla propria attività online o determinare la propria posizione. • **Blocca tutto il contenuto remoto** - Impedisce al mittente di vedere le proprie attività e-mail Impostazione predefinita: vero
	iOS 15.4+	
	Consenti screen saver automatico di Apple TV (tvOS 15.4 e successivi) **Da iOS 16.0 fino a 26.0**	Se falso, disabilita lo screen saver automatico di Apple TV. Disponibile su tvOS 15.4 e versioni successive. Impostazione predefinita: vero
	Consenti installazione dei Miglioramenti alla sicurezza in background	Per disabilitare le risposte. L'utente non può installare miglioramenti della sicurezza in background.
	Consenti rimozione miglioramenti di sicurezza in background **Dispositivi supervisionati con iOS 17.0 e versioni successive**	Per impedire all'utente di annullare le risposte. L'utente non può rimuovere i miglioramenti della sicurezza in background.

Categoria	Impostazione	Operazione da eseguire
	Consenti widget dell'iPhone sui dispositivi Mac	Selezionare per consentire la visualizzazione dei widget dell'iPhone sui dispositivi Mac che utilizzano lo stesso AppleID dell'iPhone per iCloud su entrambi i dispositivi.
	Dispositivi iOS 17.2+ supervisionati Consenti posta vocale live	Selezionare per abilitare la posta vocale live sul dispositivo.
	Imponi conservazione ESIM durante la cancellazione	Selezionare per preservare la eSIM quando il sistema cancella il dispositivo a causa di un numero eccessivo di tentativi di password non riusciti o dell'opzione Cancella tutto il contenuto e le impostazioni in **Impostazioni** >**Generale** > **Reimposta**. Il sistema non preserva la eSIM se **Trova personale** inizia a cancellare il dispositivo.
	Dispositivi iOS 17.4+ supervisionati Consenti installazione app del Marketplace	Selezionare per consentire agli utenti di scaricare app da marketplace alternativi. Questa restrizione, se impostata su false, impedirà agli utenti di installare nuove app di marketplace alternativi e app installate da tali marketplace.
	Consenti oscuramento automatico **Dispositivi iOS 17.5+ supervisionati** Consenti installazione di app di distribuzione web	Selezionare per consentire l'opzione di oscuramento automatico sugli iPad con display OLED. Questa restrizione **allowWebdistributionAppInstallation**, se impostata su false, impedirà agli utenti di installare app direttamente da nuovi siti web alternativi. Si applica solo ai dispositivi supervisionati.
	Dispositivi iOS 18.0+ supervisionati Consenti trasferimenti eSIM in uscita Consenti Genmoji	Selezionare per consentire il trasferimento di una eSIM a un dispositivo diverso da quello su cui è installata la restrizione. Selezionare per consentire la creazione di Genmoji.
	Consenti Image Playground	Selezionare per consentire l'uso della generazione di immagini.
	Consenti Image Wand	Selezionare per consentire l'uso della bacchetta per le immagini.

Categoria	Impostazione	Operazione da eseguire
	Consenti iPhone Mirroring	Selezionare per consentire il mirroring dell'iPhone in un dispositivo macOS.
	Consenti risultati di scrittura personalizzati	Selezionare per consentire al sistema di generare testo utilizzando la scrittura dell'utente.
	Consenti Writing Tools	Selezionare per abilitare gli strumenti di scrittura di Apple Intelligence.
	Consenti di nascondere le app	Seleziona per consentire di nascondere le app.
	Consenti blocco app	Seleziona per consentire il blocco delle app.
	iOS 18.1+ supervisionati	
	Consenti registrazione chiamate	Seleziona per consentire la registrazione delle chiamate. Impostazione predefinita: true
	Consenti riepilogo posta	Seleziona per consentire la creazione manuale di riepiloghi dei messaggi e-mail. Impostazione predefinita: true
	Consenti messaggistica RCS **iOS 18.2+ supervisionati**	Seleziona per consentire la messaggistica RCS. Impostazione predefinita: true Sui dispositivi iOS 26 e sui modelli di iPad cellulari con iPadOS 26, l'utilizzo di RCS Messaging può essere limitato sui dispositivi il cui piano cellulare è associato all'ICCID.
	Consenti integrazioni di intelligence esterna	Seleziona per abilitare l'uso di servizi di intelligence esterni basati sul cloud con Siri.
	Consenti accesso integrazioni di intelligence esterna	Seleziona per consentire ai provider di intelligence esterni di entrare in modalità anonima. Se un utente ha già effettuato l'accesso a un provider di intelligence esterno, l'applicazione di questa restrizione ne causerà la disconnessione.
	Consenti modifica browser predefinito	Seleziona per abilitare la modifica delle preferenze del browser predefinito. Le impostazioni di Ivanti Neurons per MDM consentono di impostare il browser Web predefinito.
Applicazioni	**Tutte le versioni di iOS**	Abilita l'accesso alle applicazioni presenti nei dispositivi.

Categoria	Impostazione	Operazione da eseguire
	Consenti l'installazione delle applicazioni	Selezionare questa opzione per abilitare l'utente all'installazione di applicazioni dall'App Store di Apple. Deselezionare questa opzione per disabilitare l'App Store e rimuovere la relativa icona dalla schermata Home.
	Consenti uso della fotocamera	Selezionare questa opzione per consentire all'utente di utilizzare la fotocamera. Deselezionare questa opzione per disabilitare la fotocamera e rimuovere la relativa icona dalla schermata Home. Nei dispositivi iOS 26+, se le app vengono aggiunte all'elenco delle eccezioni, la restrizione Consenti fotocamera non verrà applicata.
	Consenti l'uso di Safari Abilita il riempimento automatico Forza avviso antifrode	Selezionare questa opzione per consentire l'uso del browser Web Safari. Deselezionare questa opzione per disabilitare il browser Web Safari, rimuovere la relativa icona dalla schermata Home e impedire agli utenti di aprire le clip Web. Selezionare questa opzione per attivare la funzione di riempimento automatico per i campi visualizzati in Safari. Selezionare questa opzione per richiedere a Safari di tentare di impedire agli utenti di visitare i siti Web identificati come fraudolenti o compromessi.
	Abilita JavaScript	Selezionare questa opzione per attivare il supporto Javascript per Safari.
	Blocca i pop-up	Selezionare questa opzione per bloccare i pop-up per Safari.
Safari	**Solo con supervisione - Versione 26+** Consenti cancellazione della cronologia Safari	Selezionare per consentire agli utenti di cancellare la cronologia di navigazione.
	Consenti navigazione privata in Safari **Dispositivi supervisionati con tutte le versioni di iOS**	Selezionare per consentire l'uso della navigazione privata.
	Consenti rimozione delle app	Selezionare questa opzione per consentire agli utenti di rimuovere le app dal dispositivo.
	Consenti uso di Game Center	Selezionare questa opzione per consentire l'accesso a Game Center.

Categoria	Impostazione	Operazione da eseguire
	Consenti l'aggiunta di amici Game Center	Selezionare questa opzione per consentire agli utenti l'aggiunta di amici a Game Center.
	Consenti la modalità di gioco multiplayer	Selezionare questa opzione per consentire agli utenti di giocare a dei giochi multigiocatore.
	Consenti iMessage	Selezionare questa opzione per consentire l'uso di iMessage. Sui dispositivi iOS 26 e sui modelli di iPad cellulare con iPadOS 26, l'utilizzo di iMessage può essere limitato se il dispositivo viene aggiunto all'elenco dei dispositivi negati.
	Accetta i cookie	Selezionare Mai, Sempre o Da siti visitati.
	Consenti FaceTime **iOS 8 e versioni successive**	Selezionare questa opzione per consentire all'utente di eseguire FaceTime se la fotocamera è attiva. Sui dispositivi iOS 26 e sui modelli di iPad cellulare con iPadOS 26, l'utilizzo di Face Time può essere limitato se il dispositivo viene aggiunto all'elenco dei dispositivi negati.
	Consenti alle applicazioni gestite di utilizzare la sincronizzazione cloud	Selezionare questa opzione per consentire alle app gestite di utilizzare la sincronizzazione cloud.
	Consenti continuazione dell'attività	Selezionare questa opzione per consentire la continuazione dell'attività nelle app che supportano le funzioni di handoff.
	Dispositivi supervisionati con iOS 8 o versioni successive	
	Consenti l'uso di podcast	Selezionare questa opzione per consentire l'uso di podcast.
	iOS9 e succ.	
	Consenti trusting di nuovi autori di app aziendali	Seleziona per consentire all'utente di accedere alle nuove app enterprise.

Categoria	Impostazione	Operazione da eseguire
	iOS 9 e succ. supervisionato	
	Consenti App Store	Seleziona per consentire all'utente l'accesso all'App store di Apple.
	Consenti download automatico delle app	Seleziona per consentire all'app di scaricare file, dati, aggiornamenti inviando un prompt all'utente.
	Consenti app Notizie	Seleziona per consentire l'uso dell'app News.
	Dispositivi supervisionati con iOS 9.3 e versioni successive	
	Consenti iTunes Radio	Selezionare questa opzione per utilizzare la radio di iTunes.
	Consenti Apple Music	Selezionare questa opzione per consentire l'uso di Apple Music.
	Consenti ID aggregati app elencate	Selezionare questa opzione per limitare la visualizzazione o l'utilizzo ai soli ID aggregati elencati nella matrice. Il valore com.apple.webapp è incluso per consentire tutte le clip Web.
	ID aggregati app bloccati	Selezionare questa opzione per impedire la visualizzazione o l'utilizzo degli ID aggregati elencati nella matrice. Il valore com.apple.webapp è incluso per bloccare tutte le clip Web.
	Dispositivi supervisionati con iOS 13.0 o versioni successive	
	Consenti l'uso di iTunes Store	Selezionare questa opzione per consentire l'uso di iTunes Music Store. Deselezionare questa opzione per disabilitare iTunes Music Store e rimuovere la relativa icona dalla schermata Home.

Categoria	Impostazione	Operazione da eseguire
iCloud	Tutte le versioni di iOS	Abilita l'accesso ai servizi iCloud.
	Consenti il backup	Selezionare questa opzione per consentire al dispositivo di eseguire il backup dei dati tramite il servizio iCloud di Apple.
	Consenti la sincronizzazione dei documenti	Selezionare questa opzione per consentire la sincronizzazione dei documenti tramite il servizio iCloud di Apple.
	Consenti streaming foto	Selezionare questa opzione per consentire la sincronizzazione delle foto sugli altri dispositivi iOS in uso tramite il servizio iCloud di Apple.
	Streaming foto condiviso consentito (non consentire potrebbe causare la perdita di dati)	Selezionare questa opzione per consentire la sincronizzazione delle foto condivise. Deselezionando questa opzione è possibile perdere alcune foto.
	Consenti sincronizzazione portachiavi **iOS9 e succ.**	Selezionare questa opzione per consentire la sincronizzazione del portachiavi.
	Consenti catalogo fotografico di iCloud **iOS 15 e versioni successive (supervisionato)**	Seleziona per consentire l'accesso al catalogo fotografico di iCloud.
	Consenti inoltro privato iCloud	Se ha valore False, disabilita l'inoltro privato a iCloud. Impostazione predefinita: true

Categoria	Impostazione	Operazione da eseguire
Protezione e privacy	**Tutte le versioni di iOS**	Abilitare le policy di protezione e privacy.
	Consenti aggiornamento dei certificati over-the-air	Selezionare questa opzione per consentire gli aggiornamenti dei certificati principali over-the-air.
	Forza Limita Ad Tracking	Selezionare questa opzione per richiedere l'uso della funzione Limita Ad Tracking.
	Dispositivi supervisionati con tutte le versioni di iOS	
	Consenti installazione profilo di configurazione	Selezionare questa opzione per consentire agli utenti di installare in modo interattivo i profili di configurazione e i certificati.
	Accetta contenuto generato dall'utente assistente	Selezionare questa opzione per consentire a Siri di consultare il contenuto generato dall'utente dal Web.
	Dispositivi supervisionati con iOS 8 o versioni successive	
	Consenti all'utente di eliminare tutti i contenuti e le impostazioni in Reimposta UI	Selezionare questa opzione per abilitare l'opzione "Cancella tutti i contenuti e le impostazioni" in Reimposta UI di iOS sul dispositivo.
	Consenti Tempo allo schermo	Selezionare questa opzione per consentire l'uso di Tempo allo schermo (Impostazioni > Tempo allo schermo).
	Consenti l'invio dei dati di diagnostica a Apple	Selezionare questa opzione per consentire l'invio automatico dei dati di diagnostica a Apple.
	Consenti all'utente di accettare i certificati TLS considerati non attendibili	Selezionare questa opzione per consentire agli utenti di accettare i certificati HTTPS considerati non attendibili. Se questa opzione non è selezionata, il dispositivo rifiuterà automaticamente i certificati HTTPS considerati non attendibili senza chiederlo all'utente.
	Forza i backup crittografati	Selezionare questa opzione per richiedere i backup crittografati tramite iTunes. L'opzione è automaticamente selezionata a causa dei requisiti SCEP.
	Forza utente a inserire la password iTunes Store per tutte le transazioni	Selezionare questa opzione per forzare gli utenti a immettere la password iTunes per ciascuna transazione nell'App Store. Se questa opzione non è selezionata, l'utente può effettuare più transazioni su una singola autenticazione.
	iOS9 e succ.	
	Elabora AirDrop come	Selezionare questa opzione per consentire all'utente di accedere alla condivisione file di AirDrop.

Categoria	Impostazione	Operazione da eseguire
	destinazione non gestita	Impostazione predefinita: false
	iOS 9 e succ. supervisionato	
	Consenti modifica del passcode dispositivo	Seleziona per consentire all'utente di cambiare il codice di accesso al dispositivo.
	iOS 12+	
	Consenti alle app gestite di scrivere i contatti negli account dei contatti non gestiti	Selezionare questa opzione per consentire alle app gestite di scrivere i contatti negli account dei contatti non gestiti. Impostazione predefinita: false
	Dispositivi supervisionati con iOS 12 e versioni successive	
	Consenti riempimento automatico password	Selezionare questa opzione per consentire agli utenti di utilizzare la funzionalità di riempimento automatico delle password funzione su iOS e perché sia richiesto di utilizzare una password salvata in Safari o nelle app.
	Consenti ai dispositivi situati nelle vicinanze di condividere le richieste di password	Selezionare questa opzione per consentire al dispositivo dell'utente di richiedere le password dai dispositivi nelle vicinanze.
	Consenti la condivisione di password	Selezionare questa opzione per consentire agli utenti di condividere le proprie password con la funzionalità delle password AirDrop.
	Consenti alle app non gestite di leggere i contatti dagli account dei contatti gestiti	Selezionare questa opzione per consentire alle app non gestite di leggere i contatti dagli account dei contatti gestiti. Impostazione predefinita: false
	iOS 18.3	
	Consenti ID dell'area di lavoro intelligence esterna	Immettere ID dell'area di lavoro Intelligence esterna consentita.
	Consenti Note Sintesi trascrizione	Selezionare per abilitare la creazione di riepiloghi dalle trascrizioni. Impostazione predefinita: true
	Consenti riepilogo Visual Intelligence	Selezionare per abilitare la creazione di riepiloghi da Visual Intelligence di Apple utilizzando immagini o contenuti visivi. Impostazione predefinita: true

Categoria	Impostazione	Operazione da eseguire
Valutazioni dei contenuti		Controllare l'accesso ad applicazioni e contenuti multimediali.
	Consenti la riproduzione di musica, podcast e media iTunes U espliciti (iOS 13+ solo supervisionati e tvOS 11.3 e versioni successive)	Il contenuto esplicito è contrassegnato come tale dai fornitori dei contenuti, come ad esempio le etichette di registrazione, quando tale contenuto viene venduto tramite l'iTunes Store.
	Regione valutazioni	Selezionare una regione dall'elenco a discesa per modificare la regione associata alle selezioni di valutazione per applicazioni, programmi TV e film.
	Film	Selezionare un limite di valutazione per i film memorizzati sul dispositivo: • Non consentire film • G • PG • PG-13 • R • NC-17 • Consenti tutti i film
	Programmi TV	Selezionare un limite di valutazione per i programmi TV memorizzati sul dispositivo: • Non consentire programmi TV • TV-Y • TV-Y7 • TV-G • TV-PG • TV-14 • TV-MA • Consenti tutti i programmi TV
	App	Selezionare un limite di valutazione per le applicazioni memorizzate sul dispositivo: • Non consentire app • 4+ • 9+ • 12+

Categoria	Impostazione	Operazione da eseguire
		• 17+ • Consenti tutte le app

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.4.27. Visualizzazione Sala conferenze

Applicabile a: tvOS 10.2 e versioni successive supportate.

Questa configurazione attiverà la modalità Visualizzazione Sala conferenze su Apple TV. L'app Apple TV viene bloccata nella modalità Visualizzazione Sala conferenze per impedire altri tipi di utilizzo.

A partire dalla versione tvOS 10.2, è possibile impostare dispositivi Apple TV supervisionati in modalità Visualizzazione Sala conferenze. La modalità Visualizzazione Sala conferenze blocca i dispositivi Apple TV con ambito su una schermata con sfondo nero e scarica uno screen saver predefinito, a meno che l'immagine di sfondo e lo screen saver non vengano definiti manualmente nelle impostazioni del dispositivo Apple TV. Inoltre, questa modalità può visualizzare un messaggio, come configurato in Visualizzazione Sala conferenze.

È possibile distribuire automaticamente la configurazione Visualizzazione Sala conferenze e le app possono eseguire l'installazione quando i dispositivi sono in questa modalità. Se un dispositivo impostato in modalità Visualizzazione Sala conferenze viene riavviato, il blocco dello schermo viene ripristinato automaticamente senza prima visualizzare la schermata principale.

> Se un dispositivo Apple TV è in esecuzione in modalità App singola o se la modalità App singola viene distribuita con la modalità Visualizzazione Sala conferenze, quest'ultima sostituirà la modalità App singola. Inoltre, se un dispositivo Apple TV è connesso a una rete tramite Ethernet, la modalità Visualizzazione Sala conferenze non visualizzerà automaticamente una rete Wi-Fi a cui connettersi per la condivisione AirPlay. È possibile visualizzare questa istruzione sullo schermo utilizzando il campo Messaggio personalizzato della configurazione Visualizzazione Sala conferenze.

Creazione di una configurazione Visualizzazione Sala conferenze

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **conferenza** nel campo di ricerca, quindi fare clic sulla configurazione **Visualizzazione Sala conferenze**.
4. Immettere un nome e una descrizione per la configurazione.
5. Specificare il **messaggio personalizzato**. Sarà il messaggio personalizzato visualizzato sullo schermo in modalità Visualizzazione Sala conferenze.
6. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
7. Fare clic su **Fine**.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.4.28. Impostazioni tastiera

Utilizzare le **Impostazioni tastiera** per configurare le impostazioni della tastiera sui dispositivi supervisionati. Questa dichiarazione aiuta gli amministratori ad applicare controlli coerenti basati su criteri che gestiscono il comportamento della tastiera, le opzioni di input e le relative impostazioni dell'esperienza utente.

Applicabile a:

- iOS 26.4+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.
- macOS 26.4+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Impostazioni tastiera**.
3. Configurare le **Impostazioni tastiera** come da tabella seguente:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Consenti correzione automatica	Selezionare la casella di controllo per abilitare la Correzione automatica. Utilizzare il pulsante **Esegui push al dispositivo** per attivare la Correzione automatica sui dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi macOS.
Consenti la ricerca delle definizioni	Selezionare la casella di controllo per abilitare Ricerca definizione. Utilizzare il pulsante **Esegui push al dispositivo** per attivare la Ricerca definizione sui dispositivi supervisionati.
Consenti dettatura	Selezionare la casella di controllo per abilitare Dettatura. Utilizzare il pulsante **Esegui push al dispositivo** per attivare la Dettatura sui dispositivi supervisionati.
Consenti suggerimenti tastiera matematica	Selezionare la casella di controllo per abilitare Suggerimenti tastiera matematica. Utilizzare il pulsante **Esegui push al dispositivo** per attivare i suggerimenti della tastiera matematica sui dispositivi supervisionati.
Consenti testo predittivo	Selezionare la casella di controllo per abilitare il Testo predittivo. Utilizzare il pulsante **Esegui push al dispositivo** per attivare il Testo predittivo sui dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi macOS.
Consenti Slide to Type	Selezionare la casella di controllo per abilitare Slide to Type. Utilizzare il pulsante **Esegui push al dispositivo** per attivare Slide to Type sui dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi macOS.
Consenti controllo ortografico	Selezionare la casella di controllo per abilitare il Controllo ortografico. Utilizzare il pulsante **Esegui push al dispositivo** per attivare il Controllo ortografico su dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi macOS.
Consenti sostituzione testo	Selezionare la casella di controllo per abilitare la sostituzione del testo. Utilizzare il pulsante **Esegui push al dispositivo** per consentire la Sostituzione del testo sui dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi macOS.

4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
5. Selezionare una delle opzioni di distribuzione per impostare la configurazione di **Impostazioni tastiera**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere **Utilizzo delle configurazioni**.
6. Fare clic su **Fine**.

10.10.4.29. Blocco e tutto schermo: modalità di amministrazione del dispositivo Android

La configurazione della modalità amministrativa del dispositivo Android Lockdown & Kiosk disabilita alcune funzioni dei dispositivi Android e crea un elenco di app disponibili per gli utenti in modalità a tutto schermo.

> La configurazione della modalità amministrativa del dispositivo Android è deprecata e non è supportata per i dispositivi con Android 8 e versioni successive. Si consiglia di utilizzare Android Enterprise Lockdowns per Kiosk Lockdowns su Android 8 e versioni successive.

È possibile restringere l'opzione per la modifica di impostazioni o app quando un dispositivo Android è in modalità tutto schermo.

- Aggiungere le app e selezionare le impostazioni nella pagina di configurazione Crea blocco e tutto schermo: modalità di amministrazione del dispositivo Android.
- L'opzione di modifica delle impostazioni mediante l'icona Impostazioni è disponibile in modalità tutto schermo.
- Selezionando le app senza scegliere opzioni per la configurazione delle impostazioni, l'icona delle impostazioni non verrà visualizzata in modalità tutto schermo.
- Se si sceglie di non inserire app nella configurazione, l'icona delle impostazioni verrà visualizzata.

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Impostazioni di blocco: consente di disabilitare funzioni di tutti i dispositivi Android.	
Disattiva Wi-Fi	Selezionare quest'opzione per disattivare l'accesso alle LAN wireless.
Disattiva fotocamera	Selezionare quest'opzione per disattivare l'accesso alla fotocamera.
Disattiva Bluetooth	Selezionare quest'opzione per disattivare le funzioni Bluetooth. Prestare attenzione quando si utilizza questa opzione. Ivanti sconsiglia di disattivare l'audio, perché viene disabilitato l'accesso al Bluetooth vivavoce. I requisiti legali relativi all'uso in vivavoce dei dispositivi durante la guida stanno diventando sempre più diffusi.
Impostazioni modalità tutto schermo: consente di utilizzare il dispositivo come tutto schermo, limitando le operazioni a poche app specifiche. Le impostazioni della modalità tutto schermo non verranno applicate a dispositivi con Android 8.0 e versioni successive. Per tali dispositivi, lo stato tutto schermo viene segnalato nella pagina dei dettagli del dispositivo come UNSUPORTED_ON_DEVICE.	
Attiva modalità tutto schermo	Selezionare questa opzione per configurare la **modalità tutto schermo** sui dispositivi Android.
Disabilita impostazioni rapide	Selezionare questa opzione per disattivare le impostazioni rapide nella modalità tutto schermo.
Consenti all'utente di accedere alle impostazioni Wi-Fi	Selezionare questa opzione per consentire a un utente di modificare le impostazioni Wi-Fi e accedere alle reti wireless preferite.
Consenti all'utente di accedere alle impostazioni Bluetooth	Selezionare questa opzione per consentire a un utente di modificare le impostazioni Bluetooth e associare dispositivi Bluetooth aggiuntivi.
Consenti all'utente di accedere a Impostazioni posizione	Selezionare questa opzione per consentire all'utente di accedere alle impostazioni della posizione.

Impostazione	Operazione da eseguire
Consenti all'utente di ritardare gli aggiornamenti delle applicazioni	Selezionare questa opzione per consentire all'utente di ritardare gli aggiornamenti delle applicazioni.
PIN di uscita dalla modalità tutto schermo	Immettere il codice di quattro cifre che l'utente finale deve digitare per uscire dalla modalità tutto schermo.
Creazione di un elenco di app consentite: le app aggiunte all'elenco delle app consentite saranno disponibili agli utenti in modalità tutto schermo. Trascinare per disporre le app nell'ordine in cui devono essere visualizzate nell'utilità di avvio della modalità tutto schermo. L'aggiunta di un'applicazione all'elenco delle app consentite non ne determina l'installazione sul dispositivo. Assicurarsi di distribuire ciascuna app agli utenti e ai gruppi di utenti appropriati nell'App Catalog.	
App incorporate	Fare clic su +Aggiungi per includere le applicazioni native elencate nel gruppo di applicazioni consentite nella modalità tutto schermo. Se il dialer e la fotocamera sono stati disattivati nelle impostazioni di blocco sopracitate, non possono essere aggiunti all'elenco delle app consentite.
Catalogo app	Fare clic su +Aggiungi per includere le applicazioni elencate nel Catalogo app nel gruppo di applicazioni consentite nella modalità tutto schermo.
Altre app	Fare clic su +Aggiungi per includere il **nome del pacchetto** di un'app non disponibile in Google Play Store.
App consentite in modalità tutto schermo	Fare clic su X per rimuovere un'app dal gruppo di app consentite nella modalità tutto schermo. Trascinare e rilasciare per modificare l'ordine in cui le app vengono visualizzate sui dispositivi tutto schermo.

> Per i dispositivi Samsung con Knox Standard 4.0 o versione superiore, la funzionalità multiutente viene automaticamente bloccata in modalità tutto schermo.

Per i dispositivi non Samsung, la modalità tutto schermo non è supportata su dispositivi Android 8.0 o versioni successive. Per la modalità tutto schermo in Android 8.0 o versioni successive, Ivanti raccomanda l'utilizzo dei blocchi di Android Enterprise.

Argomenti correlati:

- **Configurazione della modalità tutto schermo per Android**
- **Come creare una configurazione**

10.10.4.30. Configurazione della modalità tutto schermo per Android

Argomenti della sezione:

- Avvio della modalità tutto schermo in remoto
- Uscita dalla modalità tutto schermo

Licenza: Silver

La modalità tutto schermo per i dispositivi Android consente di limitare l'uso di un dispositivo ad app specifiche. È possibile utilizzare la modalità tutto schermo per configurare i dispositivi per i dipendenti che utilizzeranno solo app specifiche per le attività lavorative.

Durante la preparazione dei dispositivi Android per la modalità tutto schermo o Proprietario del dispositivo con modalità tutto schermo, è necessario **creare un elenco di app consentite** che si desidera mettere a disposizione degli utenti in modalità tutto schermo. Per i dispositivi che utilizzano Proprietario del dispositivo, è possibile aggiungere app all'elenco delle app consentite mediante trascinamento per disporre le app nell'ordine in cui devono essere visualizzate nell'utilità di avvio della modalità tutto schermo. Per ulteriori informazioni, consultare la sezione **Configurazione Blocco e tutto schermo**.

Prerequisiti

Prima di configurare la modalità tutto schermo per i dispositivi Android, assicurarsi di aver eseguito le attività seguenti:

- Aver installato Go sui dispositivi.
- Aver configurato il Catalogo app con le app necessarie per la configurazione tutto schermo.
- Aver distribuito il Catalogo app ai dispositivi che verranno eseguiti nella modalità tutto schermo.

> I dispositivi SonimXP5S non supportano la modalità tutto schermo.

- Aver installato le app necessarie per la configurazione tutto schermo.
- (Facoltativo) Configurazione della **personalizzazione della modalità tutto schermo per Android**.

> La modalità tutto schermo è supportata su Android 5.1 e 6.0. Non- Samsung Knox deve essere impostato in modalità proprietario del dispositivo per impedire l'uso di applicazioni indesiderate.

Importante: le funzionalità di alcuni dispositivi possono causare la copertura dello schermo o la disattivazione della modalità tutto schermo. La funzione People Edge del dispositivo Samsung Galaxy S6 Edge è un esempio di questa funzionalità. Si consiglia la disattivazione di questi tipi di funzioni da parte di un amministratore prima di distribuire il dispositivo.

Procedura

1. Accedere a **Configurazioni**.
2. Fare clic su **+Aggiungi**.
3. Fare clic su **Blocco e tutto schermo: modalità di amministrazione del dispositivo Android**.
4. Nella schermata **Crea impostazioni**, completare almeno la sezione **Impostazioni modalità tutto schermo**.
5. Nella schermata **Distribuzione**, selezionare i gruppi di dispositivi che riceveranno questa configurazione.
6. Fare clic su **Fine**.

7. Per i dispositivi non Samsung, continuare con i passaggi seguenti:
    1. Andare in **Dispositivi** > **Dispositivi**.
    2. Selezionare i dispositivi su cui si desidera attivare la modalità tutto schermo.
    3. Selezionare **AzioniImponi il check-in**.
    4. Sui dispositivi, toccare il pulsante **Modalità tutto schermo**.
    5. Premere il pulsante **Home** sul dispositivo.
    6. Se viene visualizzata la finestra di dialogo **Seleziona utilità di avvio**, toccare **Utilità di avvio tutto schermo Go** e selezionare **Sempre**. Questo passaggio è necessario per assicurarsi che verrà utilizzata l'utilità di avvio appropriata per la funzione. Altrimenti, all'utente verrà richiesto di selezionare un'utilità di avvio.

Avvio della modalità tutto schermo in remoto

Procedura

1. Andare in **Dispositivi > Dispositivi**.
2. Aggiungere la colonna Modalità tutto schermo alla visualizzazione.
3. Selezionare i dispositivi in cui è abilitata la modalità tutto schermo, ma che non sono attualmente in modalità tutto schermo.
4. Selezionare **Azioni > Passa in modalità tutto schermo**.

Uscita dalla modalità tutto schermo

Se si imposta un codice PIN nella configurazione, è possibile uscire dalla modalità tutto schermo sul dispositivo.

Procedura

1. Toccare l'icona **Impostazioni**.
2. Selezionare **Esci dalla modalità tutto schermo**.
3. Toccare il campo **Codice PIN a tutto schermo** quando richiesto.
4. Immettere il codice PIN tutto schermo.

È possibile uscire dalla modalità tutto schermo da dispositivi specifici tramite il portale:

Procedura

1. Andare in **Dispositivi > Dispositivi**.
2. Visualizzare i dettagli del dispositivo.
3. Selezionare **Azioni > Esci dalla modalità tutto schermo**.

È possibile anche utilizzare i metodi seguenti per uscire dalla modalità tutto schermo:

- Eliminare la configurazione.
- Disattivare la configurazione
- Rimuovere il gruppo di dispositivi dalla configurazione

10.10.4.31. Configurazione di tutto schermo per dispositivi Android condivisi

Per le distribuzioni a task worker le aziende possono offrire dispositivi Android dedicati personalizzati in base a specifici ruoli dell'utente. Sui dispositivi possono essere installate diverse app e configurazioni, in base al profilo dell'utente. Ad esempio, un utente con mansioni tecniche utilizzerà un gruppo specifico di app, mentre un altro utente, addetto alla manutenzione, avrà accesso ad app differenti.

La modalità a tutto schermo per dispositivi condivisi Android funge da filtro per le app per diversi gruppi di utenti che condividono dispositivi. Un utente che ha eseguito l'accesso a tutto schermo per dispositivi condivisi potrà visualizzare solo le app specifiche per il proprio ruolo. Uno dei vantaggi principali di tutto schermo per dispositivi condivisi è la possibilità di consentire a gruppi di utenti diversi di accedere ad app differenti sullo stesso dispositivo. Quando un utente esce dalla modalità a tutto schermo di un dispositivo condiviso Android, le sue app e i suoi dati utente, compresa la cronologia, vengono cancellati dal display dell'utente successivo che accede al dispositivo (se l'app è contrassegnata per essere reinstallata). tutto schermo per dispositivi condivisi è disponibile solo per le distribuzioni di Android enterprise con account Google Play gestiti.

Tutto schermo per dispositivi condivisi richiede due tipi di utente, un utente temporaneo e un utente a tutto schermo condiviso, e almeno due criteri corrispondenti a tali utenti. L'utente temporaneo può richiedere la visualizzazione della schermata di accesso su un dispositivo condiviso. Inoltre, è un tipo speciale di utente amministratore, che consente ad altri utenti di eseguire l'accesso al dispositivo tutto schermo in uso. Dopo avere effettuato l'accesso a tutto schermo per dispositivi condivisi, la policy temporanea viene sostituita da una policy per modalità tutto schermo condivisa. L'utente tutto schermo ha accesso alle app installate sul dispositivo in base alla policy assegnata. Sebbene sia possibile creare più policy per modalità tutto schermo condivisa, sul dispositivo tutto schermo viene attivata solo una policy tutto schermo per volta. Quando l'utente si disconnette dal tutto schermo condiviso, sul dispositivo vengono riattivati l'utente temporaneo e la rispettiva policy.

Solo l'utente temporaneo può visualizzare la pagina di accesso. Pertanto, è necessario creare policy temporanee dedicate. Al contrario, gli utenti di tutto schermo per dispositivi condivisi possono accedere al gruppo di app definito nella relativa policy (Naturalmente, è anche necessario installare le app consentite sui dispositivi a tutto schermo del dispositivo condiviso). Il criterio a tutto schermo del dispositivo condiviso permette di creare un filtro di app consentite da tutte le app installate in precedenza. Non è possibile caricare direttamente app in una policy tutto schermo per dispositivi Android condivisi. A seconda dell'organizzazione, spesso è necessario dedicare una policy per tutto schermo condiviso a un tipo di utenti o gruppo di utenti tutto schermo. Ad esempio, un'azienda potrebbe avere dipendenti che lavorano su turni diurni e notturni, con ruoli diversi, e che hanno necessità di accedere a gruppi di app differenti. In questo caso, è necessario creare un criterio per i turni diurni e un criterio per i turni notturni.

Per ulteriori informazioni sull'abilitazione di un dispositivo tutto schermo condiviso, vedere **Blocco e tutto schermo: Android Enterprise**

10.10.4.32. Blocco e tutto schermo: Android Enterprise

Blocco e tutto schermo: la configurazione Android Enterprise disattiva alcune funzionalità dei dispositivi Android e crea un elenco di app consentite disponibili agli utenti in modalità tutto schermo.

Argomenti della sezione:

- Impostazioni di blocco
- Profilo di lavoro
- Dispositivi di lavoro gestito (impostazioni Proprietario del dispositivo e modalità tutto schermo)
- Impostazioni di blocco per dispositivo gestito con Profilo di lavoro/Profilo di lavoro su dispositivo di proprietà dell'azienda

Impostazioni di blocco

Impostazione	Descrizione
Nome Descrizione	Immettere un nome identificativo della configurazione. Immettere una descrizione esplicativa dello scopo della configurazione.
Scegli tipo di blocco	Selezionare il tipo di impostazioni di blocco che si desidera configurare: • Profilo di lavoro • Dispositivi di lavoro gestito (impostazioni Proprietario del dispositivo e modalità tutto schermo) • Impostazioni di blocco per dispositivo gestito con Profilo di lavoro/Profilo di lavoro su dispositivo di proprietà dell'azienda Le impostazioni di blocco per dispositivo gestito con Profilo di lavoro su dispositivo di proprietà dell'azienda sono applicabili solo ai dispositivi Android 11 e versioni successive. È consentito un solo tipo per configurazione. Le opzioni visualizzate dipendono dal tipo selezionato. Se una configurazione Dispositivo di lavoro gestito (proprietario del dispositivo) e Dispositivo gestito con Profilo di lavoro su dispositivo di proprietà dell'azienda vengono distribuite sullo stesso dispositivo, prevale Dispositivo gestito con Profilo di lavoro.

Profilo di lavoro

Consente di disabilitare alcune funzioni su dispositivi Android Enterprise.

Impostazione	Operazione da eseguire	Per i dispositivi
Disattiva Acquisizione schermo	Selezionare quest'opzione per disattivare la possibilità di utilizzare la funzione di acquisizione schermo integrata nel dispositivo.	• Android 5.0 e versioni successive
Non consentire Controllo app	Selezionare questa opzione per impedire a un utente di modificare le applicazioni nelle Impostazioni o nelle utilità di avvio.	• Android 5.0 e versioni successive
Non consentire Credenziali config	Selezionare questa opzione per impedire a un utente di configurare le credenziali degli utenti.	• Android 5.0 e versioni successive
Non consentire Copia/Incolla tra profili	Selezionare questa opzione per impedire di copiare/incollare le informazioni tra i profili.	• Android 5.0 e versioni successive
Non consentire Modifica account	Selezionare questa opzione per impedire a un utente di aggiungere o rimuovere gli account.	• Android 5.0 e versioni successive
Non consentire Beam in uscita	Selezionare questa opzione per impedire a un utente di utilizzare NFC per trasferire i dati delle app.	• Android 5.1 e versioni successive
Non consentire Condividi la posizione	Selezionare questa opzione per impedire a un utente di rivelare la posizione del dispositivo alle applicazioni.	• Android 5.0 e versioni successive
Non consentire Funzioni di debug	Selezionare per disabilitare le funzioni di debug sui dispositivi. Per impostazione predefinita, questa opzione è attivata.	• Android 5.0 e versioni

Impostazione	Operazione da eseguire	Per i dispositivi
		successive
Assicura Verifica app	Selezionare per consentire le funzionalità di verifica applicazioni sui dispositivi. Per impostazione predefinita, questa opzione è attivata. Quando questa opzione è disabilitata, nel dispositivo viene ripristinato il comportamento predefinito che può variare a seconda del dispositivo.	• Android 5.0 e versioni successive
Disabilita le origini sconosciute sul dispositivo	Selezionare questa opzione per impedire l'installazione di app da origini sconosciute sul dispositivo. Affinché questa impostazione venga applicata sul dispositivo, è necessario un aggiornamento previsto di Google Play.	• Android 5.0 e versioni successive
Limita metodi di input	Selezionare questa opzione per limitare i nomi dei pacchetti IME consentiti, specificando i nomi dei pacchetti consentiti mediante il campo **Nome del pacchetto**. Sui dispositivi sarà possibile utilizzare sia i metodi di input dei pacchetti consentiti, sia quelli predefiniti del sistema. L'utente può passare dai metodi di input predefiniti del sistema a quelli dei pacchetti consentiti e viceversa. Per Android versione 10 e successive, l'elenco degli elementi consentiti è applicabile solo alle app IME sul lato Profilo di lavoro. Per le versioni precedenti di Android, l'elenco degli elementi consentiti è applicabile a tutte le app IME del dispositivo (sia all'interno che all'esterno del Profilo di lavoro).	• Android 5.0 e versioni successive
Limita servizi di accessibilità	Selezionare questa opzione per limitare i servizi di accessibilità delle app di lavoro specificando i nomi dei pacchetti consentiti mediante il campo **Nome del pacchetto**. In mancanza di pacchetti consentiti vengono autorizzati solo i servizi di accessibilità del sistema.	• Android 5.0 e versioni successive
Disabilita origini sconosciute all'interno del profilo di lavoro	Selezionare per non consentire il download da origini sconosciute all'interno del profilo di lavoro.	• Android 5.0 e versioni successive
Abilita/Disattiva app di sistema	Selezionare questa opzione per abilitare e disabilitare le applicazioni di sistema da distribuire designando due elenchi di nomi di pacchetti tramite i campi **Nome pacchetto app di sistema**. Utilizzare questa funzionalità per gestire l'accesso alle applicazioni di sistema che non sono pubblicate in Google Play. Non è supportata l'aggiunta di app al Catalogo app e a un elenco di app di sistema.	• Android 5.0 e versioni successive

Impostazione	Operazione da eseguire	Per i dispositivi
Disabilita ID chiamante	Consente di scegliere se visualizzare sul dispositivo le informazioni dell'ID chiamante del profilo di lavoro per le chiamate in entrata.	• Android 6.0 e versioni successive
Disattiva Condivisione contatti tramite Bluetooth	Selezionare questa opzione per impedire che il dispositivo condivida i contatti con altri dispositivi tramite Bluetooth.	• Android 6.0 e versioni successive
Disattiva Condivisione contatti tramite Ricerca	Selezionare questa opzione per impedire che gli utenti cerchino i contatti di lavoro nella connessione telefonica personale.	• Android 7.0 e versioni successive
Non consentire riempimento automatico	Selezionare per non consentire il riempimento automatico	• Android 8.0 e versioni successive
Non consentire notifiche app di lavoro nel profilo personale	Selezionare questa opzione per impedire le notifiche nel Profilo di lavoro.	• Android 8.0 e versioni successive
Non consentire stampa	Selezionare questa opzione per impedire la stampa da tutte le app.	• Android 9.0 e versioni successive
Non consentire condivisione nel profilo	Selezionare questa opzione per impedire agli utenti di condividere dati personali in un profilo di lavoro sul dispositivo.	• Android 9.0 e versioni successive
Consenti accesso ai calendari del profilo di lavoro	Selezionare una delle seguenti opzioni per consentire tutte le app, oppure selezionare un insieme di app nel profilo personale per accedere alle informazioni del calendario presenti nel Profilo di lavoro:	• Android 10.0 e versioni

Impostazione	Operazione da eseguire	Per i dispositivi
	• **Tutte le app nel profilo personale**: consente a tutte le app di accedere alle informazioni del calendario presenti nel Profilo di lavoro • **Solo le seguenti app nel profilo personale**: immettere gli ID bundle delle app nel campo di testo sottostante, separandoli con virgole. Solo le app selezionate nel profilo personale potranno accedere alle informazioni del calendario presenti nel Profilo di lavoro. L'app nel profilo personale deve implementare specifiche API per essere in grado di accedere al calendario condiviso.	successive
Abilita elenchi di app consentite tra profili	Selezionare la casella di controllo per permettere agli utenti di condividere informazioni da app specifiche, dal profilo di lavoro al lato utente del dispositivo. Nel campo **App consentite** digitare gli ID pacchetto delle app da consentire, separandoli con virgole. Per impostazione predefinita, questa opzione è abilitata.	• Android 11.0 e versioni successive
Abilitare il sezionamento della rete 5G	Selezionare per fornire un'opzione di sezionamento rete 5G sul profilo di lavoro dei dispositivi di proprietà dell'azienda. Per impostazione predefinita, questa opzione è abilitata.	• Android 12.0+
Non consentire più condivisione Wi-Fi configurata dall'amministratore	Selezionare per impedire agli utenti di condividere le configurazioni Wi-Fi impostate dall'amministratore.	• Android 13.0+
Disabilita AI Assist	Selezionare per impedire agli utenti di utilizzare le funzioni di AI Assist. Per impostazione predefinita, questa opzione è abilitata.	• Android 15.0+

Dispositivi di lavoro gestito (impostazioni Proprietario del dispositivo e modalità tutto schermo)

Disabilitare alcune funzioni nei dispositivi di lavoro gestito (Proprietario del dispositivo) per Android 5.0 e versioni successive.

Impostazione	Descrizione
Disattiva Wi-Fi	Selezionare quest'opzione per disattivare l'accesso alle LAN wireless.
Disattiva impostazioni Wi-Fi	Selezionare questa opzione per disattivare l'accesso alle impostazioni wireless.
Disattiva fotocamera	Selezionare quest'opzione per disattivare l'accesso alla fotocamera.
Disattiva Bluetooth (Android 8.0 e versioni successive)	Selezionare quest'opzione per disattivare le funzioni Bluetooth. Prestare attenzione quando si utilizza questa opzione. Ivanti sconsiglia di disattivare l'audio, perché viene disabilitato l'accesso al Bluetooth vivavoce. I requisiti legali relativi all'uso in vivavoce dei dispositivi durante la guida stanno diventando sempre più diffusi.
Non consentire impostazioni Bluetooth (Android 8.0 e versioni successive)	Selezionare questa opzione per disattivare l'accesso alle impostazioni Bluetooth.
Disattiva Acquisizione schermo	Selezionare quest'opzione per disattivare la possibilità di utilizzare la funzione di acquisizione schermo integrata nel dispositivo.
Disabilita ripristino rete	Selezionare per prevenire il ripristino della rete. (Si applica ai dispositivi Android 7.0+ e non è supportato in modalità Profilo di lavoro su dispositivo di proprietà dell'azienda).
Disattiva volume master	Selezionare questa opzione per disattivare il volume master.
Non consentire Controllo app	Selezionare questa opzione per impedire a un utente di modificare le applicazioni nelle Impostazioni o nelle utilità di avvio.
Non consentire credenziali	Selezionare questa opzione per impedire a un utente di configurare le credenziali degli utenti.
Non consentire broadcast di emergenza	Selezionare per impedire broadcast di emergenza.
Non consentire reti mobili	Selezionare questa opzione per disattivare l'accesso alle reti mobili. Questa opzione non può essere disattivata se il Wi-Fi è disattivato.
Non consentire tethering	Selezionare questa opzione per disattivare il tethering come opzione per l'utilizzo della connessione Internet di un dispositivo allo scopo di fornire accesso a Internet a un altro dispositivo.
Non consentire VPN	Selezionare questa opzione per disattivare le connessioni alla VPN.
Non consentire ripristino delle impostazioni predefinite	Selezionare quest'opzione per impedire agli utenti di ripristinare il dispositivo ai valori predefiniti di fabbrica.
Abilita protezione anti ripristino factory	Selezionare quest'opzione per consentire agli utenti di ripristinare il dispositivo ai valori predefiniti di fabbrica. È possibile specificare facoltativamente un elenco di ID di account Google autorizzati (un valore intero) che possono eseguire il provisioning del dispositivo dopo la reimpostazione delle impostazioni di fabbrica o posizionare il cursore del

Impostazione	Descrizione
	mouse sopra l'icona della Guida in linea per visualizzare le istruzioni per il recupero degli ID di account autorizzati.
Non consentire Modifica account	Selezionare questa opzione per impedire a un utente di aggiungere o rimuovere gli account.
Non consentire NFC (raggio in uscita)	Selezionare questa opzione per impedire a un utente di utilizzare NFC per trasferire i dati delle applicazioni.
Non consentire chiamate in uscita	Selezionare questa opzione per impedire a un utente di effettuare chiamate in uscita.
Non consentire modalità provvisoria (Android 6.0 e versioni successive)	Selezionare questa opzione per impedire a un utente di riavviare un dispositivo in modalità provvisoria.
Non consentire Condividi la posizione	Selezionare questa opzione per impedire a un utente di rivelare la posizione del dispositivo alle applicazioni.
Non consentire Funzioni di debug	Selezionare per disabilitare le funzioni di debug sui dispositivi. Per impostazione predefinita, questa opzione è attivata.
Assicura Verifica app	Selezionare per consentire le funzionalità di verifica applicazioni sui dispositivi. Per impostazione predefinita, questa opzione è attivata. Quando questa opzione è disabilitata, nel dispositivo viene ripristinato il comportamento predefinito che può variare a seconda del dispositivo.
Non consentire SMS	Selezionare questa opzione per impedire a un utente di inviare e ricevere SMS.
Non consentire Riattiva microfono	Selezionare questa opzione per impedire a un utente di riattivare il microfono del dispositivo.
Non consentire ora automatica	Selezionare questa opzione per impedire a un utente di abilitare le modifiche automatiche dell'ora.
Non consentire fuso orario automatico	Selezionare questa opzione per impedire all'utente di abilitare la modifica automatica dell'ora del dispositivo in base al fuso orario.
Sincronizza ora con il server (Android 9.0+)	Selezionare questa opzione per consentire ai dispositivi di sincronizzare l'ora con i server Ivanti Neurons for MDM, la prima volta al momento della registrazione e successivamente ogni 24 ore dopo ciascun check-in. Questa opzione è disponibile solo se l'opzione **Disattiva ora automatica** è selezionata.
Imposta fuso orario (Android 9.0+)	Specificare la stringa del fuso orario nel formato ID fuso orario Olson (ad esempio, Pacifico/Midway).
Disattiva roaming dati	Selezionare quest'opzione per disattivare lo scambio di dati quando il dispositivo è in roaming.
Disattiva sospensione Wi-Fi	Selezionare questa opzione per mantenere attivo il Wi-Fi mentre il dispositivo si trova in modalità di sospensione.

Impostazione	Descrizione
Limita metodi di input	Selezionare questa opzione per limitare i nomi dei pacchetti IME consentiti, specificando i nomi dei pacchetti consentiti mediante il campo **Nome del pacchetto**. Sui dispositivi sarà possibile utilizzare sia i metodi di input dei pacchetti consentiti, sia quelli predefiniti del sistema. L'utente può passare dai metodi di input predefiniti del sistema a quelli dei pacchetti consentiti e viceversa. Per Android versione 10 e successive, l'elenco degli elementi consentiti è applicabile solo alle app IME lato dispositivo. Per le versioni precedenti di Android, l'elenco degli elementi consentiti è applicabile a tutte le app IME del dispositivo.
Limita servizi di accessibilità	Selezionare questa opzione per limitare i servizi di accessibilità delle app di lavoro specificando i nomi dei pacchetti consentiti mediante il campo **Nome del pacchetto**. In mancanza di pacchetti consentiti vengono autorizzati solo i servizi di accessibilità del sistema.
Disattiva trasferimento file tramite USB	Selezionare questa opzione per disattivare il trasferimento di file tramite USB.
Disattiva supporti esterni	Selezionare questa opzione per disattivare i supporti esterni.
Disattiva keyguard (non sarà effettivo se è impostato il PIN/passcode)	Selezionare questa opzione per disattivare la funzione keyguard. Questa opzione non ha effetto se una password, un PIN o un modello sono attualmente impostati. Se una password, un PIN o un modello sono impostati dopo la disattivazione della funzione keyguard, questa smette di essere disattivata.
Mantieni lo schermo attivo quando il dispositivo è collegato all'alimentazione.	Selezionare questa opzione per mantenere lo schermo attivo quando si è collegati alla presa di alimentazione. Lo schermo può oscurarsi ma non si spegne mentre il dispositivo è collegato a una fonte di alimentazione. Questa impostazione avrà effetto solo se il blocco automatico o il timeout di inattività nella configurazione passcode non è utilizzato per impostare un valore di timeout.
Non consentire la creazione di finestre	Selezionare questa opzione per impedire alle app di visualizzare alcuni tipi di finestre sovrapposte, quali avvisi e finestre popup.
Salta suggerimenti primo utilizzo	Selezionare questa opzione per abilitare il consiglio del sistema che propone di saltare l'esercitazione utente e altri suggerimenti introduttivi al primo avvio di un'app.
Non consentire origini sconosciute sul dispositivo	Selezionare questa opzione per non consentire all'utente l'installazione di app da origini sconosciute.
Impostare il messaggio schermata di blocco (Android 7.0+)	Selezionare la visualizzazione del messaggio schermata di blocco sul dispositivo. Digitare il messaggio schermata di blocco (massimo 256 caratteri) nel campo di testo. Abilitando questa opzione, l'utente non potrà impostare il messaggio in Impostazioni; viene visualizzato il messaggio impostato dall'amministratore. Se l'amministratore non inserisce alcun messaggio schermata di blocco dopo avere abilitato l'opzione "Imposta messaggio schermata di blocco", l'utente non potrà impostare il messaggio in Impostazioni, ma non verrà visualizzato alcun messaggio.
Imposta luminosità schermo	Selezionare per impostare la luminosità dello schermo del dispositivo.

Impostazione	Descrizione
	• Manuale - Selezionare per inserire manualmente un numero (da 0 a 255) • Adattiva - Selezionare per consentire al dispositivo di impostare la luminosità Si consiglia di attivare l'opzione "Disabilita luminosità configurazione" prima di impostare la luminosità dello schermo del dispositivo.
Imposta timeout schermo	Selezionare per impostare la durata del timeout dello schermo (in secondi). Si consiglia di attivare l'opzione "Disabilita timeout schermata di configurazione" prima di impostare la luminosità dello schermo del dispositivo.
Imposta orientamento schermo	Selezionare per impostare l'orientamento dello schermo. È possibile impostare l'orientamento dello schermo su 0, 90, 180 o 270 gradi dall'elenco a discesa. Questa opzione non è selezionata per impostazione predefinita. Per Go app 89 e versioni successive, è necessario selezionare questa opzione e impostare il valore su 0 per mantenere il dispositivo in modalità Verticale a tutto schermo.
Abilita/Disattiva app di sistema	Selezionare questa opzione per abilitare e disabilitare le applicazioni di sistema da distribuire designando due elenchi di nomi di pacchetti tramite i campi **Nome pacchetto app di sistema**. Utilizzare questa funzionalità per gestire l'accesso alle applicazioni di sistema che non sono pubblicate in Google Play. Non è supportata l'aggiunta di app al Catalogo app e a un elenco di app di sistema.
Android 8.0 e versioni successive	
Non consentire riempimento automatico	Selezionare per non consentire all'utente di utilizzare i servizi di riempimento automatico.
Non consentire condivisione Bluetooth	Selezionare questa opzione per non consentire all'utente di condividere Bluetooth in uscita sul dispositivo.
Disabilita servizio di backup	Selezionare per disattivare il servizio di backup.
Android 9.0 e versioni successive	
Non consentire stampa	Selezionare questa opzione per impedire all'utente di stampare.
Non consentire modalità aereo	Selezionare per disattivare la modalità aereo su tutto il dispositivo.
Non consentire visualizzazione in base a luce ambiente	Selezionare per non consentire la visualizzazione in base a luce ambiente.
Non consentire config. luminosità	Selezionare per non consentire all'utente di configurare la luminosità. Si consiglia di definire la modalità "Imposta modalità luminosità schermo" prima di selezionare questa opzione.
Non consentire config. data e ora	Selezionare per non consentire la configurazione di data, ora e fuso orario.
Non consentire config. posizione	Selezionare per non consentire all'utente di disattivare i provider di posizione.
Non consentire config. timeout schermo	Selezionare per non consentire all'utente la modifica del timeout schermo. Si consiglia di definire il valore "Imposta timeout schermo" prima di selezionare

Impostazione	Descrizione
	questa opzione.
Android 12.0+	
Abilitare USB solo per la ricarica	Selezionare per abilitare la porta USB solo per la carica.
Android 13.0+	
Imposta sicurezza Wi-Fi minima richiesta	Utilizzare questa opzione per impostare la sicurezza Wi-Fi minima richiesta: • Nessuna sicurezza minima richiesta - Selezionare questa opzione se non è richiesta alcuna sicurezza minima • Sicurezza basata su rete personale - Selezionare questa opzione per bloccare le reti Wi-Fi personali come WEP, WPA/WPA2/WPA3, ecc. • Sicurezza basata su rete aziendale EAP - Selezionare questa opzione per bloccare le reti Wi-Fi basate sul protocollo EAP. • Sicurezza basata su rete aziendale 192 - Selezionare questa opzione per bloccare le reti Wi-Fi aziendali EAP. Tutti i dispositivi esistenti che non soddisfano i criteri minimi saranno scollegati. I dettagli del dispositivo mostreranno il livello di sicurezza Wi-Fi minimo richiesto (se disponibile) in **Generale > Livello di sicurezza Wi-Fi**.
Non consentire più condivisione Wi-Fi configurata dall'amministratore	Selezionare per impedire agli utenti di condividere le configurazioni Wi-Fi impostate dall'amministratore.
Android 15.0+	
Disabilita AI Assist **Impostazioni modalità tutto schermo:** la modalità tutto schermo consente di applicare restrizioni aggiuntive ai dispositivi, tra cui l'accesso limitato alle app tramite un'utilità di avvio personalizzata.	Selezionare per impedire agli utenti di utilizzare le funzioni di AI Assist. Per impostazione predefinita, questa opzione è abilitata.
Attiva modalità tutto schermo	Selezionare questa opzione per configurare la **modalità tutto schermo** sui dispositivi Android. • Se un utente si connette in modalità tutto schermo condivisa e quindi si disconnette, il nome utente rimane disponibile nei client Go per gli accessi successivi. Nella modalità tutto schermo condivisa, il client Go conserva gli ultimi sette nomi utente utilizzati. • Ora la modalità tutto schermo condivisa supporta l'autenticazione IdP. Pertanto, se Ivanti Neurons for MDM è configurato con IDP, è possibile utilizzare la modalità tutto schermo condivisa con l'autenticazione IDP.

Impostazione	Descrizione
Abilita la modalità di blocco delle attività	Selezionare questa opzione per abilitare la modalità di blocco delle attività sui dispositivi Android. Quando è abilitata, i dispositivi possono visualizzare la funzione keyguard, la barra di stato e la modalità provvisoria. Questa opzione è disabilitata per impostazione predefinita. Di seguito sono riportate la impostazioni aggiuntive che vengono visualizzate quando è abilitata la modalità di blocco delle attività per Android 9 o le versioni più recenti supportate: **Icona Impostazioni**: consente alle app di avere accesso a funzioni di sistema dipendenti dall'app Impostazioni dispositivo. Se si consente l'uso di Impostazioni dispositivo, è possibile evitare le violazioni della modalità di blocco delle attività in scenari come l'associazione Bluetooth da un'app. Si consiglia di mantenere questa impostazione abilitata per app specifiche. **Informazioni sistema**: visualizza informazioni su data/ora, connettività, batteria e modalità di vibrazione nella barra di stato. Questa opzione è disabilitata per impostazione predefinita. **Keyguard** (abilitata per impostazione predefinita): consente di abilitare la funzione keyguard quando il dispositivo è in modalità di blocco delle attività. **Azioni globali** (abilitata per impostazione predefinita): consente di abilitare il menu visualizzato quando l'utente preme a lungo il pulsante di accensione. Se questa opzione è disabilitata, potrebbe non essere possibile spegnere il dispositivo. **Pulsante Home**: consente di abilitare il pulsante Home. Questa opzione è disabilitata per impostazione predefinita. Se abilitata, vengono visualizzate le seguenti opzioni secondarie: • **Pulsante Panoramica** (disabilitato per impostazione predefinita): consente di abilitare il pulsante e la schermata Panoramica quando il dispositivo è in modalità di blocco delle attività. • **Notifiche** (disabilitata per impostazione predefinita): consente di abilitare le notifiche quando il dispositivo è in modalità di blocco delle attività. Ciò include icone di notifica sulla barra di stato, notifiche di avvisi e l'ombreggiatura della notifica espandibile. Se l'opzione Pulsante Home non è abilitata, non è possibile utilizzare la funzione Finestra multipla.
Passa a tutto schermo automaticamente (solo durante la configurazione iniziale)	Selezionare questa opzione per consentire automaticamente la modalità tutto schermo quando la configurazione viene applicata.
Mantenere la modalità Kiosk dopo gli aggiornamenti dei criteri	Selezionare per riportare il dispositivo in modalità Kiosk in automatico dopo l'applicazione di un aggiornamento dei criteri di blocco. Questa impostazione aiuta a mantenere il funzionamento ininterrotto del Kiosk e riduce la necessità di un intervento manuale in seguito a modifiche ai criteri. In precedenza, l'aggiornamento di un criterio di blocco poteva causare l'uscita del dispositivo dalla modalità Kiosk. Se abilitato, il dispositivo torna in modalità Kiosk in automatico dopo l'elaborazione del criterio aggiornato.

Impostazione	Descrizione
Disabilita impostazioni rapide per i dispositivi Android 5	Selezionare questa opzione per disabilitare le impostazioni rapide in modalità tutto schermo per i dispositivi in esecuzione su Android 5.
Disabilita impostazioni rapide per i dispositivi Android 6 e versioni successive e Samsung	Selezionare questa opzione per disabilitare le impostazioni rapide in modalità tutto schermo per dispositivi Android Enterprise dalla versione 6 alla versione più recente e per tutti i dispositivi Samsung. La disattivazione di questa impostazione non comporta il blocco delle icone di notifica e dei suoni sul dispositivo.
Consenti all'utente di accedere alle impostazioni Wi-Fi	Selezionare questa opzione per consentire a un utente di modificare le impostazioni Wi-Fi e accedere alle reti wireless preferite.
Consenti all'utente di accedere alle impostazioni Bluetooth	Selezionare questa opzione per consentire a un utente di modificare le impostazioni Bluetooth e associare dispositivi Bluetooth aggiuntivi.
Consenti all'utente di accedere a Impostazioni posizione	Selezionare questa opzione per consentire all'utente di accedere alle impostazioni della posizione.
Consenti all'utente di ritardare gli aggiornamenti delle applicazioni	Selezionare questa opzione per consentire all'utente di ritardare gli aggiornamenti delle applicazioni.
Consenti all'utente di accedere alle impostazioni di ora e data	Selezionare questa opzione per consentire all'utente di accedere alle impostazioni di ora e data.
Consenti all'utente di accedere alle impostazioni della rete mobile	Selezionare questa opzione per consentire all'utente di accedere alle impostazioni della rete mobile.
Consenti la selezione della lingua da parte dell'utente	Selezionare questa opzione per consentire all'utente di accedere alle impostazioni della lingua.
Abilita dispositivo condiviso	In modalità tutto schermo per dispositivo condiviso, il dispositivo viene condiviso tra più utenti finali. Questa opzione consente di condividere un dispositivo in modalità tutto schermo. • **Abilita accesso**: questa opzione è riservata ad utenti amministratore tutto schermo. Quando un dispositivo è configurato con questa opzione, viene visualizzata la schermata di accesso dell'utente, che consente agli utenti finali di accedere alla modalità tutto schermo per dispositivo condiviso. L'opzione Abilita accesso sarà visualizzata solo se l'utente è stato creato come Account dispositivi Android Enterprise (utente temporaneo). Selezionare Usa la sostituzione del dominio e inserire il dominio in modo corretto. Questa opzione controlla il nome utente alla ricerca del suffisso di dominio. Se il suffisso di dominio non è presente, il sistema aggiungerà automaticamente il suffisso di dominio al nome utente. • **Abilita disconnessione**: se l'utente finale esegue l'accesso a un dispositivo configurato con questa opzione, può accedere alle app consentite. L'utente può visualizzare l'opzione per disconnettersi ma non può uscire dalla modalità tutto

Impostazione	Descrizione
	schermo. Quando un utente si disconnette dalla modalità tutto schermo del dispositivo condiviso, un altro utente può accedervi e visualizzare le app, in base alla configurazione dell'amministratore. • Le app appaiono con un'icona Ricicla, che viene utilizzata per imporre la reinstallazione di un'app ad ogni login. Questa opzione può essere utilizzata per le app che hanno dati nella cache locale. L'utente può uscire dalla modalità tutto schermo se l'amministratore fornisce il relativo PIN di uscita. • **Timeout**: specifica la durata del timeout in ore. Ad esempio, se la durata del timeout è configurata su 2 ore e l'utente finale non si disconnette dalla modalità tutto schermo del dispositivo condiviso, dopo 2 ore l'azione di disconnessione verrà eseguita automaticamente sul dispositivo. Il campo **Timeout** è opzionale e viene visualizzato solo quando l'opzione **Abilita disconnessione** è selezionata. È inoltre possibile disconnettere gli utenti finali dalla modalità tutto schermo condivisa facendo clic sull'opzione **Disconnetti da tutto schermo Android enterprise** nella pagina dei dettagli del dispositivo.
Consenti autenticazione FIDO (richiede l'app Google Chrome sul dispositivo)	Selezionare questa opzione per utilizzare l'autenticazione FIDO per gli utenti quando utilizzano lo schermo condiviso. Consentire agli utenti di utilizzare le chiavi FIDO per accedere al dispositivo. Google Chrome è l'unico browser supportato e deve essere disponibile sul dispositivo affinché l'autenticazione FIDO sia disponibile nello schermo condiviso.
Consenti all'utente di configurare luminosità e rotazione automatica	Selezionare per consentire all'utente di configurare luminosità e rotazione automatica.
Abilita finestra multipla	Selezionare questa opzione per consentire la visualizzazione di più app contemporaneamente con dispositivi Samsung (modalità Proprietario del dispositivo e tutto schermo). Per utilizzare la funzione Finestra multipla in modalità di blocco delle attività, è necessario abilitare anche le seguenti opzioni della modalità di blocco delle attività: • **Pulsante Home** • **Pulsante Panoramica**
Abilita protezione inattività	Selezionare per attivare la protezione dall'inattività in modalità Chiosco. Se selezionato, il valore predefinito è di 30 secondi, fino al quale la schermata del Chiosco rimarrà attiva. È possibile impostare qualsiasi valore compreso tra 30 e 3600.
Personalizzazione tutto schermo	Selezionare le opzioni di personalizzazione predefinite o personalizzate dall'elenco a discesa.
PIN di uscita dalla modalità tutto schermo	Immettere il PIN di 6 cifre che l'utente deve digitare per uscire dalla modalità tutto schermo. Il PIN deve contenere da un minimo di 6 cifre a un massimo di 10. Tale PIN viene applicato a tutti i dispositivi in modalità tutto schermo.

Impostazione	Descrizione
	Nelle versioni precedenti, il PIN per la modalità tutto schermo ha una lunghezza di 4 cifre. L'utente può continuare a utilizzare il PIN di 4 cifre anche dopo l'aggiornamento a Ivanti Neurons for MDM 82 da una versione precedente. Tuttavia, in caso di modifica della configurazione, è necessario impostare un PIN di lunghezza conforme ai nuovi requisiti, ovvero da un minimo di 6 cifre a un massimo di 10. L'app Go protegge il dispositivo dagli attacchi di forza bruta. Per ulteriori informazioni, vedere la documentazione di Go per Android.
Abilitare il Chiosco per il lancio di una singola app	Selezionare l'uso della modalità Chiosco per mantenere un'app in primo piano sui dispositivi GMS e non GMS. È necessario selezionare un'app dal Catalogo app o inserire un ID pacchetto.
Consenti accesso utente alle impostazioni dell'agente Ivanti	Selezionare per accedere alle **Impostazioni agente Ivanti** mentre il dispositivo rimane in modalità **Kiosk app singola**. In precedenza, l'amministratore doveva uscire dalla modalità kiosk per accedere alle impostazioni dell'agente. Dopo aver abilitato e distribuito l'impostazione ai dispositivi, gli utenti possono aprire la pagina Impostazioni agente Ivanti premendo e tenendo premuti contemporaneamente i pulsanti Volume su e Volume giù. La funzione è supportata solo sui dispositivi Android registrati in modalità Dispositivo gestito dal lavoro.
Abilita sicurezza conducente	Selezionare per abilitare l'icona Sicurezza conducente per tutte le app nella sezione App consentite della modalità Chiosco. Fare clic sull'icona Sicurezza conducente per disattivare l'app se la velocità supera il limite.
Creazione di un elenco di app consentite: le app aggiunte all'elenco delle app consentite saranno disponibili agli utenti in modalità tutto schermo. Trascinare per disporre le app nell'ordine in cui devono essere visualizzate nell'utilità di avvio della modalità tutto schermo. L'aggiunta di un'applicazione all'elenco delle app consentite non ne determina l'installazione sul dispositivo. Assicurarsi di distribuire ciascuna app agli utenti e ai gruppi di utenti appropriati nell'App Catalog.	
App incorporate	Fare clic su +Aggiungi per includere le applicazioni native elencate nel gruppo di applicazioni consentite nella modalità tutto schermo. Nelle impostazioni per le app consentite in modalità tutto schermo, sono disponibili le opzioni seguenti: • **Cancellare i dati utente delle app**: attivando questa opzione, tutti i dati delle applicazioni vengono cancellati automaticamente senza alcuna richiesta

Impostazione	Descrizione
	quando l'utente esce dal tutto schermo. Selezionare Abilita dispositivo condiviso nelle impostazioni della modalità tutto schermo per rendere questa opzione disponibile con le applicazioni. ◦ I dati delle app non vengono eliminati per Google Chrome e il pacchetto WebView, anche se sono stati aggiunti alla lista delle app consentite attivando l'opzione per l'eliminazione dei dati dell'utente. Questo avviene perché, se i dati dell'app vengono eliminati per questi 2 pacchetti, la modalità tutto schermo potrebbe subire un arresto anomalo. ◦ I dati dell'app non vengono cancellati per le app Sistema per cui l'utilità di avvio dell' app non è disponibile (sia all'interno che all'esterno di tutto schermo). • **Rendi nascoste**: attivando questa opzione, l'applicazione diventa accessibile da altre app ma non è disponibile nell'utilità di avvio di tutto schermo. Se il dialer e la fotocamera sono stati disattivati nelle impostazioni di blocco sopracitate, non possono essere aggiunti all'elenco delle app consentite.
Catalogo app	Fare clic su +Aggiungi per includere le applicazioni elencate nel Catalogo app nel gruppo di applicazioni consentite nella modalità tutto schermo.
Altre app	Fare clic su +Aggiungi per includere il **nome del pacchetto** di un'app non disponibile in Google Play Store. Per i dispositivi Samsung, gli amministratori dovrebbero inserire nell'elenco degli elementi consentiti i seguenti pacchetti dialer o di sistema, al fine di renderli operativi nella modalità tutto schermo e consentire la funzionalità dialer in tale modalità. • Call - com.samsung.android.incallui • Phone - com.samsung.android.dialer (deve essere consentito e l'amministratore deve selezionare l'opzione Nascondi per questo pacchetto, al fine di evitare problemi dovuti alla presenza di due opzioni dialer per l'utente) • Call - com.sec.phone • Call Setting - com.samsung.android.app.telephonyui • Assisted Dialing - com.sec.providers.assisteddialing • Call Log Backup / Restore - com.android.calllogbackup • Dialer Storage - com.android.providers.telephony • Phone - com.android.server.telecom • Phone - com.android.phone • Smart Call - com.samsung.android.smartcallprovider • WiFi Calling - com.sec.unifiedwfc
App consentite in modalità tutto schermo	Fare clic su X per rimuovere un'app dal gruppo di app consentite nella modalità tutto schermo. Trascinare e rilasciare per modificare l'ordine in cui le app vengono visualizzate sui dispositivi tutto schermo. **Aggiungi cartella** - È possibile utilizzare questa opzione per creare una cartella in questa sezione e spostare una o più app in questa cartella. È possibile creare

Impostazione	Descrizione
	cartelle fino a due livelli. Le app copiate in una cartella non possono essere copiate in un'altra. All'interno di una cartella sono supportate solo 25 app.
Creazione di un elenco di app consentite: le app aggiunte all'elenco delle app consentite saranno disponibili agli utenti in modalità tutto schermo. Trascinare per disporre le app nell'ordine in cui devono essere visualizzate nell'utilità di avvio della modalità tutto schermo. L'aggiunta di un'applicazione all'elenco delle app consentite non ne determina l'installazione sul dispositivo. Assicurarsi di distribuire ciascuna app agli utenti e ai gruppi di utenti appropriati nell'App Catalog.	
App incorporate	Fare clic su +Aggiungi per includere le applicazioni native elencate nel gruppo di applicazioni consentite nella modalità tutto schermo. Nelle impostazioni per le app consentite in modalità tutto schermo, sono disponibili le opzioni seguenti: • **Cancellare i dati utente delle app**: attivando questa opzione, tutti i dati delle applicazioni vengono cancellati automaticamente senza alcuna richiesta quando l'utente esce dal tutto schermo. Selezionare Abilita dispositivo condiviso nelle impostazioni della modalità tutto schermo per rendere questa opzione disponibile con le applicazioni. ◦ I dati delle app non vengono eliminati per Google Chrome e il pacchetto WebView, anche se sono stati aggiunti alla lista delle app consentite attivando l'opzione per l'eliminazione dei dati dell'utente. Questo avviene perché, se i dati dell'app vengono eliminati per questi 2 pacchetti, la modalità tutto schermo potrebbe subire un arresto anomalo. ◦ I dati dell'app non vengono cancellati per le app Sistema per cui l'utilità di avvio dell' app non è disponibile (sia all'interno che all'esterno di tutto schermo). • **Rendi nascoste**: attivando questa opzione, l'applicazione diventa accessibile da altre app ma non è disponibile nell'utilità di avvio di tutto schermo. Se il dialer e la fotocamera sono stati disattivati nelle impostazioni di blocco sopracitate, non possono essere aggiunti all'elenco delle app consentite.
Catalogo app	Fare clic su +Aggiungi per includere le applicazioni elencate nel Catalogo app nel gruppo di applicazioni consentite nella modalità tutto schermo.
Altre app	Fare clic su +Aggiungi per includere il **nome del pacchetto** di un'app non disponibile in Google Play Store.

Impostazione	Descrizione
	Per i dispositivi Samsung, gli amministratori dovrebbero inserire nell'elenco degli elementi consentiti i seguenti pacchetti dialer o di sistema, al fine di renderli operativi nella modalità tutto schermo e consentire la funzionalità dialer in tale modalità. • Call - com.samsung.android.incallui • Phone - com.samsung.android.dialer (deve essere consentito e l'amministratore deve selezionare l'opzione Nascondi per questo pacchetto, al fine di evitare problemi dovuti alla presenza di due opzioni dialer per l'utente) • Call - com.sec.phone • Call Setting - com.samsung.android.app.telephonyui • Assisted Dialing - com.sec.providers.assisteddialing • Call Log Backup / Restore - com.android.calllogbackup • Dialer Storage - com.android.providers.telephony • Phone - com.android.server.telecom • Phone - com.android.phone • Smart Call - com.samsung.android.smartcallprovider • WiFi Calling - com.sec.unifiedwfc
App consentite in modalità tutto schermo	Fare clic su X per rimuovere un'app dal gruppo di app consentite nella modalità tutto schermo. Trascinare e rilasciare per modificare l'ordine in cui le app vengono visualizzate sui dispositivi tutto schermo. **Aggiungi cartella** - È possibile utilizzare questa opzione per creare una cartella in questa sezione e spostare una o più app in questa cartella. È possibile creare cartelle fino a due livelli. Le app copiate in una cartella non possono essere copiate in un'altra. All'interno di una cartella sono supportate solo 25 app.
Abilitare il Chiosco per il lancio di una singola app	Selezionare l'uso della modalità Chiosco per mantenere un'app in primo piano sui dispositivi GMS e non GMS. È necessario selezionare un'app dal Catalogo app o inserire un ID pacchetto.
Creazione di un elenco di app consentite: le app aggiunte all'elenco delle app consentite saranno disponibili agli utenti in modalità tutto schermo. Trascinare per disporre le app nell'ordine in cui devono essere visualizzate nell'utilità di avvio della modalità tutto schermo. L'aggiunta di un'applicazione all'elenco delle app consentite non ne determina l'installazione sul dispositivo. Assicurarsi di distribuire ciascuna app agli utenti e ai gruppi di utenti appropriati nell'App Catalog.	

Impostazione	Descrizione
App incorporate	Fare clic su +Aggiungi per includere le applicazioni native elencate nel gruppo di applicazioni consentite nella modalità tutto schermo. Nelle impostazioni per le app consentite in modalità tutto schermo, sono disponibili le opzioni seguenti: • **Cancellare i dati utente delle app**: attivando questa opzione, tutti i dati delle applicazioni vengono cancellati automaticamente senza alcuna richiesta quando l'utente esce dal tutto schermo. Selezionare Abilita dispositivo condiviso nelle impostazioni della modalità tutto schermo per rendere questa opzione disponibile con le applicazioni. ◦ I dati delle app non vengono eliminati per Google Chrome e il pacchetto WebView, anche se sono stati aggiunti alla lista delle app consentite attivando l'opzione per l'eliminazione dei dati dell'utente. Questo avviene perché, se i dati dell'app vengono eliminati per questi 2 pacchetti, la modalità tutto schermo potrebbe subire un arresto anomalo. ◦ I dati dell'app non vengono cancellati per le app Sistema per cui l'utilità di avvio dell' app non è disponibile (sia all'interno che all'esterno di tutto schermo). • **Rendi nascoste**: attivando questa opzione, l'applicazione diventa accessibile da altre app ma non è disponibile nell'utilità di avvio di tutto schermo. Se il dialer e la fotocamera sono stati disattivati nelle impostazioni di blocco sopracitate, non possono essere aggiunti all'elenco delle app consentite.
Catalogo app	Fare clic su +Aggiungi per includere le applicazioni elencate nel Catalogo app nel gruppo di applicazioni consentite nella modalità tutto schermo.
Altre app	Fare clic su +Aggiungi per includere il **nome del pacchetto** di un'app non disponibile in Google Play Store. Per i dispositivi Samsung, gli amministratori dovrebbero inserire nell'elenco degli elementi consentiti i seguenti pacchetti dialer o di sistema, al fine di renderli operativi nella modalità tutto schermo e consentire la funzionalità dialer in tale modalità. • Call - com.samsung.android.incallui • Phone - com.samsung.android.dialer (deve essere consentito e l'amministratore deve selezionare l'opzione Nascondi per questo pacchetto, al fine di evitare problemi dovuti alla presenza di due opzioni dialer per l'utente) • Call - com.sec.phone • Call Setting - com.samsung.android.app.telephonyui • Assisted Dialing - com.sec.providers.assisteddialing • Call Log Backup / Restore - com.android.calllogbackup • Dialer Storage - com.android.providers.telephony • Phone - com.android.server.telecom • Phone - com.android.phone • Smart Call - com.samsung.android.smartcallprovider

Impostazione	Descrizione
	• WiFi Calling - com.sec.unifiedwfc
App consentite in modalità tutto schermo	Fare clic su X per rimuovere un'app dal gruppo di app consentite nella modalità tutto schermo. Trascinare e rilasciare per modificare l'ordine in cui le app vengono visualizzate sui dispositivi tutto schermo. **Aggiungi cartella** - È possibile utilizzare questa opzione per creare una cartella in questa sezione e spostare una o più app in questa cartella. È possibile creare cartelle fino a due livelli. Le app copiate in una cartella non possono essere copiate in un'altra. All'interno di una cartella sono supportate solo 25 app.
Abilitare il Chiosco per il lancio di una singola app **Creazione di un elenco di app consentite**: le app aggiunte all'elenco delle app consentite saranno disponibili agli utenti in modalità tutto schermo. Trascinare per disporre le app nell'ordine in cui devono essere visualizzate nell'utilità di avvio della modalità tutto schermo. L'aggiunta di un'applicazione all'elenco delle app consentite non ne determina l'installazione sul dispositivo. Assicurarsi di distribuire ciascuna app agli utenti e ai gruppi di utenti appropriati nell'App Catalog.	Selezionare l'uso della modalità Chiosco per mantenere un'app in primo piano sui dispositivi GMS e non GMS. È necessario selezionare un'app dal Catalogo app o inserire un ID pacchetto.
App incorporate	Fare clic su +Aggiungi per includere le applicazioni native elencate nel gruppo di applicazioni consentite nella modalità tutto schermo. Nelle impostazioni per le app consentite in modalità tutto schermo, sono disponibili le opzioni seguenti: • **Cancellare i dati utente delle app**: attivando questa opzione, tutti i dati delle applicazioni vengono cancellati automaticamente senza alcuna richiesta quando l'utente esce dal tutto schermo. Selezionare Abilita dispositivo condiviso nelle impostazioni della modalità tutto schermo per rendere questa opzione disponibile con le applicazioni. ◦ I dati delle app non vengono eliminati per Google Chrome e il pacchetto WebView, anche se sono stati aggiunti alla lista delle app consentite attivando l'opzione per l'eliminazione dei dati dell'utente. Questo avviene perché, se i dati dell'app vengono eliminati per questi 2 pacchetti, la modalità tutto schermo potrebbe subire un arresto anomalo. ◦ I dati dell'app non vengono cancellati per le app Sistema per cui l'utilità di avvio dell' app non è disponibile (sia all'interno che all'esterno di tutto

Impostazione	Descrizione
	schermo). • **Rendi nascoste**: attivando questa opzione, l'applicazione diventa accessibile da altre app ma non è disponibile nell'utilità di avvio di tutto schermo. Se il dialer e la fotocamera sono stati disattivati nelle impostazioni di blocco sopracitate, non possono essere aggiunti all'elenco delle app consentite.
Catalogo app	Fare clic su +Aggiungi per includere le applicazioni elencate nel Catalogo app nel gruppo di applicazioni consentite nella modalità tutto schermo.
Altre app	Fare clic su +Aggiungi per includere il **nome del pacchetto** di un'app non disponibile in Google Play Store. Per i dispositivi Samsung, gli amministratori dovrebbero inserire nell'elenco degli elementi consentiti i seguenti pacchetti dialer o di sistema, al fine di renderli operativi nella modalità tutto schermo e consentire la funzionalità dialer in tale modalità. • Call - com.samsung.android.incallui • Phone - com.samsung.android.dialer (deve essere consentito e l'amministratore deve selezionare l'opzione Nascondi per questo pacchetto, al fine di evitare problemi dovuti alla presenza di due opzioni dialer per l'utente) • Call - com.sec.phone • Call Setting - com.samsung.android.app.telephonyui • Assisted Dialing - com.sec.providers.assisteddialing • Call Log Backup / Restore - com.android.calllogbackup • Dialer Storage - com.android.providers.telephony • Phone - com.android.server.telecom • Phone - com.android.phone • Smart Call - com.samsung.android.smartcallprovider • WiFi Calling - com.sec.unifiedwfc
App consentite in modalità tutto schermo	Fare clic su X per rimuovere un'app dal gruppo di app consentite nella modalità tutto schermo. Trascinare e rilasciare per modificare l'ordine in cui le app vengono visualizzate sui dispositivi tutto schermo. **Aggiungi cartella** - È possibile utilizzare questa opzione per creare una cartella in questa sezione e spostare una o più app in questa cartella. È possibile creare cartelle fino a due livelli. Le app copiate in una cartella non possono essere copiate in un'altra. All'interno di una cartella sono supportate solo 25 app.

Per i dispositivi Samsung con Knox Standard 4.0 o versione superiore, la funzionalità multiutente viene automaticamente bloccata in modalità tutto schermo.

Dispositivi gestiti con profilo di lavoro

Disabilita determinate funzionalità sul dispositivo gestito con profilo di lavoro per Android 8.0 e versioni successive.

Determinate funzioni possono essere disabilitate per il profilo di lavoro sui dispositivi di proprietà dell'azienda (applicabile ai dispositivi Android 11 e versioni successive).

Impostazione	Descrizione
Impostazioni di blocco del dispositivo gestito	
Disattiva Wi-Fi	Selezionare per disattivare l'accesso alle LAN wireless.(Non applicabile ai dispositivi Android 11+)
Disattiva impostazioni Wi-Fi	Selezionare questa opzione per disattivare l'accesso alle impostazioni wireless.
Disattiva fotocamera	Selezionare quest'opzione per disattivare l'accesso alla fotocamera.
Disattiva Bluetooth	Selezionare quest'opzione per disattivare le funzioni Bluetooth. Prestare attenzione quando si utilizza questa opzione. Ivanti sconsiglia di disattivare l'audio, perché viene disabilitato l'accesso al Bluetooth vivavoce. I requisiti legali relativi all'uso in vivavoce dei dispositivi durante la guida stanno diventando sempre più diffusi.
Non consentire impostazioni Bluetooth	Selezionare questa opzione per disattivare l'accesso alle impostazioni Bluetooth.
Disabilita ripristino rete	Selezionare per impedire il ripristino della rete (applicabile ai dispositivi con Android 7.0 e versioni successive).
Disattiva volume master	Selezionare questa opzione per disabilitare il volume master. (Non applicabile ai dispositivi Android 11 e versioni successive)
Non consentire broadcast di emergenza	Selezionare per impedire broadcast di emergenza.
Non consentire reti mobili	Selezionare questa opzione per disattivare l'accesso alle reti mobili. Questa opzione non può essere disattivata se il Wi-Fi è disattivato.
Non consentire tethering	Selezionare questa opzione per disattivare il tethering come opzione per l'utilizzo della connessione Internet di un dispositivo allo scopo di fornire accesso a Internet a un altro dispositivo.
Non consentire VPN	Selezionare questa opzione per disabilitare le connessioni alla VPN. (Non applicabile ai dispositivi Android 11 e versioni successive)
Disattiva Ripristino impostazioni predefinite	Selezionare questa opzione per impedire agli utenti di ripristinare i valori predefiniti di fabbrica del dispositivo. (Non applicabile ai dispositivi Android 11 e versioni successive)
Abilita protezione anti ripristino factory	Selezionare questa opzione per consentire agli utenti di ripristinare il dispositivo ai valori predefiniti di fabbrica. È possibile specificare facoltativamente un elenco di ID di account Google autorizzati (un valore intero) che possono eseguire il provisioning del dispositivo dopo la reimpostazione delle impostazioni di fabbrica o posizionare il cursore del mouse sopra l'icona della Guida in linea per visualizzare le istruzioni per il recupero degli ID di account autorizzati.
Non consentire chiamate in uscita	Selezionare questa opzione per impedire a un utente di effettuare chiamate in uscita.

Impostazione	Descrizione
Non consentire modalità provvisoria (Android 6.0 e versioni successive)	Selezionare questa opzione per impedire a un utente di riavviare un dispositivo in modalità provvisoria.
Non consentire Funzioni di debug	Selezionare per disabilitare le funzioni di debug sui dispositivi. Per impostazione predefinita, questa opzione è attivata.
Assicura Verifica app	Selezionare per consentire le funzionalità di verifica applicazioni sui dispositivi. Per impostazione predefinita, questa opzione è attivata. Quando questa opzione è disabilitata, nel dispositivo viene ripristinato il comportamento predefinito che può variare a seconda del dispositivo.
Non consentire SMS	Selezionare questa opzione per impedire a un utente di inviare e ricevere SMS.
Non consentire Riattiva microfono	Selezionare questa opzione per impedire a un utente di riattivare il microfono del dispositivo.
Non consentire ora automatica	Selezionare questa opzione per impedire a un utente di abilitare le modifiche automatiche dell'ora.
Non consentire fuso orario automatico	Selezionare questa opzione per impedire a un utente di abilitare la modifica automatica dell'ora del dispositivo in base al fuso orario.
Disattiva roaming dati	Selezionare quest'opzione per disattivare lo scambio di dati quando il dispositivo è in roaming.
Sincronizza ora con il server (Android 9.0+)	Selezionare questa opzione per consentire ai dispositivi di sincronizzare l'ora con i server Ivanti Neurons for MDM, la prima volta al momento della registrazione e successivamente ogni 24 ore dopo ciascun check-in. Questa opzione è disponibile solo se l'opzione **Disattiva ora automatica** è selezionata.
Imposta fuso orario (Android 9.0+)	Specificare la stringa del fuso orario nel formato ID fuso orario Olson (ad esempio, Pacifico/Midway).
Disattiva sospensione Wi-Fi	Selezionare questa opzione per mantenere attivo il Wi-Fi mentre il dispositivo si trova in modalità di sospensione. (Non applicabile ai dispositivi Android 11 e versioni successive)
Limita metodi di input	Selezionare per limitare i metodi di input per le app di lavoro designando un elenco di nomi di pacchetti Allowlisted tramite il campo **Nome pacchetto** (non applicabile ai dispositivi Android 11+). Sui dispositivi sarà possibile utilizzare sia i metodi di input dei pacchetti consentiti, sia quelli predefiniti del sistema. L'utente può passare dai metodi di input predefiniti del sistema a quelli dei pacchetti consentiti e viceversa. In Android 10+, i metodi di input sono applicabili solo sul lato dispositivo, mentre negli altri casi sono limitati all'intero dispositivo.
Limita servizi di accessibilità	Selezionare questa opzione per limitare i servizi di accessibilità delle app di lavoro specificando i nomi dei pacchetti consentiti mediante il campo **Nome del pacchetto**. In mancanza di pacchetti consentiti vengono autorizzati solo i servizi di accessibilità del sistema.

Impostazione	Descrizione
	In Android 10+, i metodi di input sono limitati alle sole app aziendali, mentre negli altri casi sono limitati all'intero dispositivo.
Disattiva trasferimento file tramite USB	Selezionare questa opzione per disattivare il trasferimento di file tramite USB.
Disattiva supporti esterni	Selezionare questa opzione per disattivare i supporti esterni.
Non consentire origini sconosciute sul dispositivo	Selezionare questa opzione per impedire l'installazione di app da origini sconosciute sul dispositivo. Affinché questa impostazione venga applicata sul dispositivo, è necessario un aggiornamento previsto di Google Play.
Impostare il messaggio schermata di blocco (Android 7.0+)	Selezionare la visualizzazione del messaggio schermata di blocco sul dispositivo. Digitare il messaggio schermata di blocco (massimo 256 caratteri) nel campo di testo. Abilitando questa opzione, l'utente non potrà impostare il messaggio in Impostazioni; viene visualizzato il messaggio impostato dall'amministratore. Se l'amministratore non inserisce alcun messaggio schermata di blocco dopo avere abilitato l'opzione "Imposta messaggio schermata di blocco", l'utente non potrà impostare il messaggio in Impostazioni, ma non verrà visualizzato alcun messaggio.
Imposta luminosità schermo	Selezionare per impostare la luminosità dello schermo del dispositivo. • Manuale - Selezionare per inserire manualmente un numero (da 0 a 255) • Adattiva - Selezionare per consentire al dispositivo di impostare la luminosità Si consiglia di attivare l'opzione "Disabilita luminosità configurazione" prima di impostare la luminosità dello schermo del dispositivo. Se l'utente è autorizzato ad apportare modifiche, al prossimo check-in queste impostazioni verranno ripristinate a quelle definite dall'amministratore. Questa impostazione non è supportata sui dispositivi con Android 11 e versioni successive per la modalità Profilo di lavoro su dispositivo aziendale.
Imposta timeout schermo	Selezionare per impostare la durata del timeout dello schermo (in secondi). Si consiglia di attivare l'opzione "Disabilita timeout schermata di configurazione" prima di impostare la luminosità dello schermo del dispositivo. Se l'utente è autorizzato ad apportare modifiche, al prossimo check-in queste impostazioni verranno ripristinate a quelle definite dall'amministratore. Questa impostazione non è supportata sui dispositivi con Android 11 e versioni successive per la modalità Profilo di lavoro su dispositivo aziendale.
Imposta orientamento schermo	Selezionare per impostare l'orientamento dello schermo. È possibile impostare l'orientamento dello schermo su 0, 90, 180 o 270 gradi dall'elenco a discesa. Questa impostazione non è supportata sui dispositivi con Android 11 e versioni successive per la modalità Profilo di lavoro su dispositivo aziendale.
Non consentire riempimento automatico (Android 8.0+)	Selezionare questa opzione per non consentire il riempimento automatico. (Non applicabile ai dispositivi Android 11 e versioni successive)

Impostazione	Descrizione
Non consentire condivisione Bluetooth (Android 8.0 e versioni successive)	Selezionare questa opzione per non consentire all'utente di condividere Bluetooth in uscita sul dispositivo.
Disabilita servizio di backup (Android 8.0 e versioni successive)	Selezionare questa opzione per disabilitare il servizio di backup. (Non applicabile ai dispositivi Android 11 e versioni successive)
Non consentire stampa (Android 9.0+)	Selezionare per limitare la stampa da tutte le app.(Non applicabile ai dispositivi Android 11+)
Non consentire modalità aereo (Android 9.0 e versioni successive)	Selezionare per disattivare la modalità aereo su tutto il dispositivo.
Non consentire visualizzazione in base a luce ambiente (Android 9.0 e versioni successive)	Selezionare questa opzione per non consentire la visualizzazione in base a luce ambiente. (Non applicabile ai dispositivi Android 11 e versioni successive)
Non consentire config. luminosità (Android 9.0 e versioni successive)	Selezionare per non consentire all'utente di configurare la luminosità (non applicabile ai dispositivi Android 11+). Si consiglia di definire la modalità "Imposta luminosità schermo" prima di selezionare questa opzione.
Non consentire config. data e ora (Android 9.0 e versioni successive)	Selezionare per non consentire la configurazione di data, ora e fuso orario.
Non consentire config. posizione (Android 9.0 e versioni successive)	Selezionare per non consentire all'utente di disattivare i provider di posizione.
Non consentire config. timeout schermo (Android 9.0 e versioni successive)	Selezionare per non consentire all'utente la modifica del timeout schermo. (Non applicabile ai dispositivi Android 11 e versioni successive) Si consiglia di impostare i valori "Imposta timeout schermo" prima di selezionare questa opzione.
Non consentire finestre di dialogo per errori di sistema (Android 9.0 e versioni successive)	Selezionare per disabilitare le finestre di dialogo degli errori di sistema.(Non applicabile ai dispositivi Android 11+)
Disattiva acquisizione schermo (Android 11.0 e versioni successive)	Selezionare quest'opzione per disattivare la possibilità di utilizzare la funzione di acquisizione schermo integrata nel dispositivo. Una volta selezionata questa opzione, l'acquisizione dello schermo viene disattivata sul lato personale del dispositivo.
Android 12.0+	

Impostazione	Descrizione
Abilitare USB solo per la ricarica **Android 13.0+**	Selezionare per abilitare la porta USB solo per la carica.
Imposta sicurezza Wi-Fi minima richiesta	Utilizzare questa opzione per impostare la sicurezza Wi-Fi minima richiesta: • Nessuna sicurezza minima richiesta - Selezionare questa opzione se non è richiesta alcuna sicurezza minima • Sicurezza basata su rete personale - Selezionare questa opzione per bloccare le reti Wi-Fi personali come WEP, WPA/WPA2/WPA3, ecc. • Sicurezza basata su rete aziendale EAP - Selezionare questa opzione per bloccare le reti Wi-Fi basate sul protocollo EAP. • Sicurezza basata su rete aziendale 192 - Selezionare questa opzione per bloccare le reti Wi-Fi aziendali EAP. Tutti i dispositivi esistenti che non soddisfano i criteri minimi saranno scollegati. I dettagli del dispositivo mostreranno il livello di sicurezza Wi-Fi minimo richiesto (se disponibile) in **Generale > Livello di sicurezza Wi-Fi**.
Non consentire più condivisione Wi-Fi configurata dall'amministratore	Selezionare per impedire agli utenti di condividere le configurazioni Wi-Fi impostate dall'amministratore.
Impostazioni di blocco profilo di lavoro	
Disattiva Acquisizione schermo	Selezionare quest'opzione per disattivare la possibilità di utilizzare la funzione di acquisizione schermo integrata nel dispositivo.
Non consentire Controllo app	Selezionare questa opzione per impedire a un utente di modificare le applicazioni nelle Impostazioni o nelle utilità di avvio.
Non consentire Credenziali config	Selezionare questa opzione per impedire a un utente di configurare le credenziali degli utenti.
Non consentire Copia/Incolla tra profili	Selezionare questa opzione per impedire di copiare/incollare le informazioni tra i profili.
Non consentire Modifica account	Selezionare questa opzione per impedire a un utente di aggiungere o rimuovere gli account.
Non consentire NFC (raggio in uscita) (Android 5.1 e versioni successive)	Selezionare questa opzione per impedire a un utente di utilizzare NFC per trasferire i dati delle applicazioni.
Non consentire Condividi la posizione	Selezionare questa opzione per impedire ai siti Web e alle app di richiedere all'utente del dispositivo di condividere la posizione.

Impostazione	Descrizione
Non consentire Funzioni di debug	Selezionare per disabilitare le funzioni di debug sui dispositivi. Per impostazione predefinita, questa opzione è attivata.
Assicura Verifica app	Selezionare per consentire le funzionalità di verifica applicazioni sui dispositivi. Per impostazione predefinita, questa opzione è attivata. Quando questa opzione è disabilitata, nel dispositivo viene ripristinato il comportamento predefinito che può variare a seconda del dispositivo.
Disabilita origini sconosciute all'interno del profilo di lavoro	Selezionare per non consentire il download da origini sconosciute all'interno del profilo di lavoro.
Abilita/Disattiva app di sistema	Selezionare questa opzione per abilitare e disabilitare le applicazioni di sistema da distribuire designando due elenchi di nomi di pacchetti tramite i campi **Nome pacchetto app di sistema**. Utilizzare questa funzionalità per gestire l'accesso alle applicazioni di sistema che non sono pubblicate in Google Play. Non è supportata l'aggiunta di app al Catalogo app e a un elenco di app di sistema.
Disabilita ID chiamante (Android 6.0+)	Consente di scegliere se visualizzare sul dispositivo le informazioni dell'ID chiamante del profilo di lavoro per le chiamate in entrata.
Disattiva Condivisione contatti tramite Bluetooth (Android 6.0+)	Selezionare questa opzione per impedire che il dispositivo condivida i contatti con altri dispositivi tramite Bluetooth.
Disattiva Condivisione contatti tramite Cerca (Android 7.0+)	Selezionare questa opzione per impedire che gli utenti cerchino i contatti di lavoro nella connessione telefonica personale.
Non consentire riempimento automatico (Android 8.0+)	Selezionare questa opzione per non consentire il riempimento automatico. (Non applicabile ai dispositivi Android 11 e versioni successive)
Non consentire notifiche app di lavoro nel profilo personale (Android 8.0+)	Selezionare questa opzione per impedire le notifiche nel Profilo di lavoro.
Non consentire stampa (Android 9.0+)	Selezionare questa opzione per limitare la stampa da tutte le app. (Non applicabile ai dispositivi Android 11 e versioni successive)
Non consentire condivisione nel profilo (Android 9.0+)	Selezionare questa opzione per impedire agli utenti di condividere dati personali in un profilo di lavoro sul dispositivo.
Limita metodi di input (Android 10.0 e versioni successive)	Selezionare questa opzione per limitare i nomi dei pacchetti IME consentiti, specificando i nomi dei pacchetti consentiti mediante il campo **Nome del pacchetto** (non applicabile ai dispositivi Android 11 e versioni successive). Sui dispositivi sarà possibile utilizzare sia i metodi di input dei pacchetti consentiti, sia quelli

Impostazione	Descrizione
	predefiniti del sistema. L'utente può passare dai metodi di input predefiniti del sistema a quelli dei pacchetti consentiti e viceversa. I metodi di input si applicano alle app IME installate sul lato profilo di lavoro. Anche se questo blocco consente di utilizzare le app installate sul lato dispositivo, tali app non saranno disponibili per l'utilizzo sul lato Profilo di lavoro.
Consenti accesso ai calendari del profilo di lavoro (Android 10.0 e versioni successive)	Selezionare una delle opzioni seguenti per consentire tutte le app o selezionare un insieme di app nel profilo personale per accedere alle informazioni del calendario presenti nel Profilo di lavoro: • **Tutte le app nel profilo personale**: consente a tutte le app di accedere alle informazioni del calendario presenti nel Profilo di lavoro • **Solo le seguenti app nel profilo personale**: immettere gli ID bundle delle app nel campo di testo sottostante, separandoli con virgole. Solo le app selezionate nel Profilo personale potranno accedere alle informazioni del calendario presenti nel Profilo di lavoro. L'app nel profilo personale deve implementare specifiche API per essere in grado di accedere al calendario condiviso.
Abilita elenco app consentite tra profili (Android versione 11.0 e successive)	Selezionare la casella di controllo per permettere agli utenti di condividere informazioni da app specifiche, dal profilo di lavoro al lato utente del dispositivo. Nel campo **App consentite** digitare gli ID pacchetto delle app da consentire, separandoli con virgole. Per impostazione predefinita, questa opzione è abilitata.
Abilita timeout profilo massimo (Android 11.0 e versioni successive)	Selezionare questa opzione per impostare una finestra di tempo massimo in cui il profilo lavorativo può essere disattivato prima che Ivanti Neurons for MDM sospenda le app personali sul dispositivo. È possibile impostare un tempo compreso tra 72 e 8760 ore. 8760 ore corrisponde a un anno di tempo. Il valore predefinito è impostato su 72 ore se l'opzione è selezionata. L'utente del dispositivo vede un messaggio che richiede di attivare il profilo di lavoro per abilitare le app sospese. Disponibile su dispositivi Android 11 e versioni successive con Profilo di lavoro su dispositivo di proprietà dell'azienda. Se il profilo viene disattivato per lunghi periodi, le app personali vengono sospese sul dispositivo.
Abilita Sezionamento rete Android 5G (Android 12.0+)	Selezionare per fornire un'opzione di sezionamento rete 5G sul profilo di lavoro dei dispositivi di proprietà dell'azienda. Per impostazione predefinita, questa opzione è abilitata.
Disabilita AI Assist (Android 15.0+)	Selezionare per impedire agli utenti di utilizzare le funzioni di AI Assist. Per impostazione predefinita, questa opzione è abilitata.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.4.33. Blocco e tutto schermo: Samsung Knox Standard

La configurazione Blocco e tutto schermo: Samsung Knox Standard consente di disattivare alcune funzionalità dei dispositivi Samsung Knox Standard e creare un elenco di app consentite disponibili agli utenti in modalità tutto schermo.

> La configurazione standard Samsung KNOX è deprecata e non è supportata sui dispositivi con Android 9 e versioni successive.

Impostazioni di blocco

Impostazione

Operazione da eseguire

Nome

Immettere un nome identificativo della configurazione.

Descrizione

Immettere una descrizione esplicativa dello scopo della configurazione.

Impostazioni di blocco Samsung Knox: consente di disattivare alcune funzionalità solo sui dispositivi Samsung Knox.

Disattiva Wi-Fi

Selezionare quest'opzione per disattivare l'accesso alle LAN wireless.

Disattiva fotocamera

Selezionare quest'opzione per disattivare l'accesso alla fotocamera.

Disattiva Bluetooth

Selezionare quest'opzione per disattivare le funzioni Bluetooth.

Consenti solo audio Bluetooth

Selezionare questa opzione per attivare soltanto le funzioni audio Bluetooth.

Disattiva dati cellulare

Selezionare quest'opzione per interrompere lo scambio di dati quando due dispositivi si toccano.

Questa opzione non può essere disattivata se il Wi-Fi è disattivato.

Disattiva GPS

Selezionare quest'opzione per disabilitare il GPS.

Disattiva connessione telefonica

Selezionare quest'opzione per disabilitare l'applicazione del telefono.

Disattiva scheda SD

Selezionare questa opzione per disabilitare l'accesso alla scheda SD.

Disattiva backup Google

Selezionare quest'opzione per disattivare i backup sui server Google.

Disattiva Copia/Incolla

Selezionare quest'opzione per disattivare l'accesso alle funzioni di copia/incolla.

Disattiva NFC

Selezionare quest'opzione per disattivare lo scambio di dati NFC (Near-field Communication) quando il dispositivo tocca un altro dispositivo.

Disattiva microfono

Selezionare quest'opzione per disattivare l'accesso delle app al microfono del dispositivo.

Disattiva Acquisizione schermo

Selezionare quest'opzione per disattivare la possibilità di utilizzare la funzione di acquisizione schermo integrata nel dispositivo. L'attivazione di questa opzione non consente le acquisizioni dello schermo di Go. Tali acquisizioni dello schermo non sono consentite.

Disattiva tethering Bluetooth

Selezionare quest'opzione per disattivare il tethering Bluetooth come opzione per l'utilizzo della connessione Internet di un dispositivo per fornire accesso a Internet a un altro dispositivo.

Disattiva debug USB

Selezionare quest'opzione per disattivare la funzione di debug USB.

Disattiva tethering USB

Selezionare quest'opzione per disattivare il tethering USB come opzione per l'utilizzo della connessione Internet di un dispositivo per fornire accesso a Internet a un altro dispositivo.

Disattiva tethering Wi-Fi

Selezionare quest'opzione per disattivare il tethering Wi-Fi come opzione per l'utilizzo della connessione Internet di un dispositivo per fornire accesso a Internet a un altro dispositivo.

Disattiva browser nativo

Selezionare quest'opzione per impedire agli utenti di accedere al browser Android.

Disattiva YouTube

Selezionare quest'opzione per impedire agli utenti di accedere a YouTube.

Disattiva Ripristino impostazioni predefinite

Selezionare quest'opzione per impedire agli utenti di ripristinare il dispositivo ai valori predefiniti di fabbrica.

Disattiva aggiornamento OTA

Selezionare quest'opzione per disattivare gli aggiornamenti OTA del firmware del dispositivo.

Avviso: non disabilitare l'opzione **Disattiva modifiche impostazioni** se l'opzione **Aggiornamento OTA** è attivata. **La disattivazione delle modifiche alle impostazioni** quando l'opzione **Aggiornamento OTA** è attivata può causare il malfunzionamento del dispositivo poiché le modifiche alle impostazioni sono necessarie per gli aggiornamenti.

Disattiva chiamate in roaming

Selezionare quest'opzione per disattivare l'accesso alle chiamate vocali quando il dispositivo è in roaming.

Disattiva USB Media Player

Selezionare quest'opzione per disattivare il media player USB.

Disattiva Google Play

Selezionare quest'opzione per disattivare l'accesso a Google Play.

Disattiva roaming dati

Selezionare quest'opzione per disattivare lo scambio di dati quando il dispositivo è in roaming.

Disabilita origini sconosciute

Selezionare questa opzione per disattivare l'installazione di app da qualsiasi posizione tranne Google Play Store, ad eccezione dell'app Go.

Disabilita rimozione privilegi amministratore dispositivo

Selezionare questa opzione per impedire agli utenti di disattivare i privilegi di amministratore dispositivo da Go.

Disattiva modifiche impostazioni

Selezionare questa opzione per disattivare l'accesso alle applicazioni delle Impostazioni del dispositivo.

Avviso: non disabilitare l'opzione **Disattiva modifiche impostazioni** se l'opzione **Aggiornamento OTA** è attivata. **La disattivazione delle modifiche alle impostazioni** quando l'opzione **Aggiornamento OTA** è attivata può causare il malfunzionamento del dispositivo poiché le modifiche alle impostazioni sono necessarie per gli aggiornamenti.

Impostazioni modalità tutto schermo: la modalità tutto schermo consente di applicare restrizioni aggiuntive ai dispositivi, tra cui l'accesso limitato alle app tramite un'utilità di avvio personalizzata.

Applicabile alle versioni di Android fino alla 8.1. Per le versioni 9.0 di Android, utilizzare la configurazione Android Enterprise Managed Device tutto schermo.

Attiva modalità tutto schermo

Selezionare questa opzione per configurare la **modalità tutto schermo** sui dispositivi Android.

Consenti all'utente di accedere alle impostazioni Wi-Fi

Selezionare questa opzione per consentire a un utente di modificare le impostazioni Wi-Fi e accedere alle reti wireless preferite.

Consenti all'utente di accedere alle impostazioni Bluetooth

Selezionare questa opzione per consentire a un utente di modificare le impostazioni Bluetooth e associare dispositivi Bluetooth aggiuntivi.

Consenti all'utente di ritardare gli aggiornamenti delle applicazioni

Selezionare questa opzione per consentire all'utente di ritardare gli aggiornamenti delle applicazioni.

Impostazioni posizione GPS

Selezionare una delle seguenti impostazioni di posizione GPS:

- Disabilita posizione
- Abilita posizione
- Consenti la selezione da parte dell'utente

PIN di uscita dalla modalità tutto schermo

Immettere il codice di quattro cifre che l'utente finale deve digitare per uscire dalla modalità tutto schermo.

Creazione di un elenco di app consentite: le app aggiunte all'elenco delle app consentite saranno disponibili agli utenti in modalità tutto schermo. Trascinare per disporre le app nell'ordine in cui devono essere visualizzate nell'utilità di avvio della modalità tutto schermo.

L'aggiunta di un'applicazione all'elenco delle app consentite non ne determina l'installazione sul dispositivo. Assicurarsi di distribuire ciascuna app agli utenti e ai gruppi di utenti appropriati nell'App Catalog.

App incorporate

Fare clic su +Aggiungi per includere le applicazioni native elencate nel gruppo di applicazioni consentite nella modalità tutto schermo.

Se il dialer e la fotocamera sono stati disattivati nelle impostazioni di blocco sopracitate, non possono essere aggiunti all'elenco delle app consentite.

Catalogo app

Fare clic su +Aggiungi per includere le applicazioni elencate nel Catalogo app nel gruppo di applicazioni consentite nella modalità tutto schermo.

Altre app

Fare clic su +Aggiungi per includere il **nome del pacchetto** di un'app non disponibile in Google Play Store.

App consentite in modalità tutto schermo

Fare clic su X per rimuovere un'app dal gruppo di app consentite nella modalità tutto schermo. Trascinare e rilasciare per modificare l'ordine in cui le app vengono visualizzate sui dispositivi tutto schermo.

> Se si utilizza la modalità tutto schermo con Android 4.4 o una versione supportata più recente, i dispositivi Samsung che supportano più utenti bloccano automaticamente la funzionalità multiutente quando è attiva la modalità tutto schermo.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.4.34. Configurazione soluzione password amministratore locale

Le impostazioni di configurazione **Local Administrator Password Solution (LAPS)** consentono agli amministratori Ivanti Neurons per MDM di rigenerare automaticamente la password dell'amministratore locale sui dispositivi macOS gestiti a intervalli prestabiliti. Per maggiori informazioni sulle soluzioni LAPS, vedere Local Admin Password Solution (LAPS).

Applicabile a: dispositivi macOS registrati e gestiti tramite la Registrazione automatica dei dispositivi.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Local Administrator Password Solution (LAPS)**.
3. Configurare le impostazioni **LAPS** in base alla tabella seguente:

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Piattaforma	Selezionare macOS dall'elenco a discesa.
Intervallo di rotazione	Selezionare una delle seguenti opzioni dall'elenco a discesa per definire la rotazione automatica delle password: • Nessuna rotazione (**valore predefinito**) • 15 giorni • 30 giorni • 60 giorni • 90 giorni • 120 giorni • 180 giorni
Rotazione dopo l'intervallo di visualizzazione	Selezionare una delle seguenti opzioni dall'elenco a discesa per ruotare automaticamente le password dopo averle visualizzate dalla pagina **Dettagli dispositivo**: • Da 1 a 24 ore • 36 ore • 48 ore Il valore predefinito è impostato su **2 ore**.

4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
5. Selezionare una delle opzioni di distribuzione per impostare la configurazione **Local Administrator Password Solution (LAPS)**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere Utilizzo delle configurazioni.
6. Fare clic su **Fine**.

10.10.4.35. Firewall macOS

Licenza: Gold

Il firewall di macOS gestisce le impostazioni del firewall applicazione, accessibili nel riquadro delle preferenze di protezione sui dispositivi macOS

Applicabile a: macOS 12.3+

- **Consenti ai software integrati di ricevere le connessioni in arrivo** - Se vero, permette al software integrato di ricevere le connessioni in entrata.
- **Consenti ai software firmati scaricati di ricevere le connessioni in arrivo** - Se vero, permette al software firmato scaricato di ricevere le connessioni in entrata.

Applicabile a: macOS 12.0+

- **Abilita registrazione** - Se vero, abilita la registrazione
- **Specificare il tipo di registrazione**
  - **Limita**
  - **Brief**
  - **Dettagli**

Applicabile a: macOS 10.12 e versioni successive

Quando si fa clic su **Abilita firewall**, è possibile selezionare una o più delle seguenti opzioni:

- **Blocca tutte le connessioni in entrata** - Seleziona per impedire a tutti i servizi di condivisione di ricevere connessioni in entrata sui dispositivi macOS, come la condivisione dello schermo o la condivisione dei file. I seguenti servizi di sistema potrebbero ancora ricevere connessioni in arrivo:
  - configd, che implementa DHCP e altri servizi di configurazione di rete
  - mDNSResponder, che implementa Bonjour
  - racoon, che implementa IPSec
- **Abilita modalità mascheramento** - Selezionare per impedire ai dispositivi macOS di rispondere alle richieste di sondaggio. I dispositivi macOS gestiti continuano a rispondere alle richieste in arrivo per le app autorizzate, ignorando le richieste inaspettate, come ICMP (ping).
- **Applicazioni** - L'elenco delle applicazioni con connessioni controllate dal firewall. Selezionare le app specifiche per cui si desidera ricevere connessioni in entrata sui dispositivi macOS.

Selezionare **Aggiungi** per aggiungere una riga all'elenco delle app. Seleziona la cella sotto **ID bundle** per selezionare l'app di cui si desidera consentire esplicitamente le connessioni in entrata. Selezionare la casella di controllo nella cella **Consenti connessioni** per consentire le connessioni in arrivo dall'app selezionata.

> Deve esistere un profilo con ambito sistema. Se più di un profilo contiene questa configurazione, verrà utilizzata l'unione di impostazioni più restrittiva.

> Le opzioni **Consenti automaticamente software scaricato firmato** e **Consenti automaticamente software incorporato** non sono supportate, tuttavia vengono entrambe attivate in modo forzato quando è disponibile questa configurazione.

L'amministratore può abilitare la modalità mascheramento specificando un dispositivo non rilevabile dal comando ping.

10.10.4.36. Restrizioni di macOS

Licenza: Gold

Le restrizioni di macOS determinano quali restrizioni sono attivate sui dispositivi macOS.

Sui dispositivi macOS è possibile attivare o disattivare le seguenti funzionalità:

Versione macOS	Funzionalità
macOS 10.11+	• Consenti Fotocamera • Consenti sincronizzazione documenti iCloud **Solo supervisionati:** • Consenti risultati Internet Spotlight
macOS 10.11.2+	• Consenti la ricerca delle definizioni
macOS 10.12+	• Consenti sincronizzazione portachiavi iCloud • Consenti Torna al mio Mac • Consenti Trova il mio Mac • Consenti condivisione con Note, Promemoria o LinkedIn • Consenti sincronizzazione segnalibri • Consenti servizio iCloud per macOS Mail • Consenti servizio Calendario iCloud per macOS • Consenti servizio Rubrica iCloud per macOS • Consenti servizio Promemoria iCloud • Consenti sblocco automatico **Solo supervisionati:** • Consenti Apple Music
macOS 10.12.4+	• Consenti l'impronta del dito per sbloccare
macOS 10.13+	• Consenti Condivisione file di iTunes • Consenti memorizzazione del contenuto nella cache • Consenti modifica dello sfondo **Solo supervisionati:** • Consenti AirPrint • Consenti identificazione iBeacon di AirPrint • Imponi requisito TLS attendibile di AirPrint • Consenti AirDrop • Consenti Game Center

Versione macOS	Funzionalità
macOS 10.13.4 e versioni successive	
macOS 10.14+	**Solo supervisionati:** Rimanda gli aggiornamenti software per un intervallo di giorni (da 30 a 90 giorni) Valore predefinito: 30 giorni.
macOS 10.14.4+	**Solo supervisionati:** Consenti ai dispositivi situati nelle vicinanze di condividere le richieste di password
	• Consenti screenshot • Consenti osservazione schermata remota **Solo supervisionati:** • Consenti di partecipare automaticamente ai corsi Classroom • Consenti a Classroom di richiedere l'autorizzazione per abbandonare i corsi • Consenti a Classroom di bloccare un'app e bloccare il dispositivo senza chiedere • Consenti forzatura osservazione schermata Classroom gestita non richiesta
macOS 11.0+	
macOS 11.3+	**Solo supervisionati:** Consenti imposizione ritardo aggiornamenti software app
macOS 11.3+	Timeout impronta digitale imposto Predefinito: 48 ore Prerequisito: ID touch deve essere configurato sul dispositivo
macOS 11.3+	**Solo supervisionati:** • Applicato ritardo installazione ritardata aggiornamenti principali software OS • Applicato ritardo installazione ritardata aggiornamenti secondari software OS • Applicato ritardo installazione ritardata aggiornamenti secondari software non OS • Forza installazione ritardata aggiornamenti principali software
macOS 12+	

Versione macOS	Funzionalità
	• allowCloudPrivateRelay: se si imposta il relay privato su ON in un dispositivo macOS, il traffico di rete viene criptato in modo che l'attività internet sia privata e sicura. Questa limitazione richiede un dispositivo supervisionato. • Consenti catalogo fotografico di iCloud **Solo supervisionati**: • Consenti cancellazione di tutti i contenuti e le impostazioni
Da macOS 13.0 a 26.0	• Consenti installazione miglioramenti di sicurezza in background: per disabilitare le risposte. L'utente non può installare miglioramenti della sicurezza in background. • Consenti rimozione miglioramenti di sicurezza in background: per impedire all'utente di annullare le risposte. L'utente non può rimuovere i miglioramenti della sicurezza in background. • Consenti controllo universale: ◦ Se è **vero**, la configurazione consente di utilizzare i dispositivi di input del dispositivo primario per controllare il dispositivo di visualizzazione secondario. ◦ Se è **falso**, sarà possibile aggiungere un dispositivo di visualizzazione secondario, ma non sarà possibile controllarlo con i dispositivi di input primari. **Solo supervisionati**: • Consenti installazione profilo di configurazione IU: se Falso, la configurazione non consente l'installazione di profili, configurazioni o certificati sul dispositivo macOS. • Consenti modalità limitata USB: se è vero, la configurazione blocca il dispositivo dall'uso di dispositivi di input collegati in remoto. Le opzioni Consenti accessori per la connessione sono disattivate sul dispositivo.
macOS 14.0+	
	• Consenti la modifica della gestione remota ARD ◦ Se è falso, impedisce di modificare l'impostazione Condivisione gestione remota in Impostazioni di sistema. ◦ Impostazione predefinita: true • Consenti modifica condivisione Bluetooth ◦ Se è falso, impedisce di modificare l'impostazione Bluetooth in Impostazioni di sistema. ◦ Impostazione predefinita: true • Consenti Cloud Freeform ◦ Se è falso, disattiva i servizi iCloud Freeform. ◦ Impostazione predefinita: true • Consenti modifica condivisione file ◦ Se è falso, impedisce di modificare l'impostazione Condivisione file in Impostazioni di sistema.

Versione macOS	Funzionalità
	◦ Impostazione predefinita: true • Consenti modifica condivisione Internet ◦ Se è falso, impedisce di modificare l'impostazione Condivisione Internet in Impostazioni di sistema. ◦ Impostazione predefinita: true • Consenti la creazione di utenti locali ◦ Se è falso, impedisce la creazione di nuovi utenti nelle Impostazioni di sistema. ◦ Impostazione predefinita: true • Consenti modifica condivisione stampante ◦ Se è falso, impedisce di modificare l'impostazione Condivisione stampante in Impostazioni di sistema. ◦ Impostazione predefinita: true • Consenti la modifica degli eventi Apple da remoto ◦ Se è falso, impedisce di modificare l'impostazione Condivisione eventi Apple da remoto in Impostazioni di sistema. ◦ Impostazione predefinita: true • Consenti Siri ◦ Impostazione predefinita: true • Consenti la modifica del disco di avvio ◦ Se falso, impedisce la modifica dell'impostazione del disco di avvio in Impostazioni di sistema. ◦ Impostazione predefinita: true • Consenti il backup con Time Machine ◦ Se falso, impedisce la modifica delle impostazioni di Time Machine in Impostazioni di sistema. ◦ Impostazione predefinita: true **Solo supervisionati**: • Consenti modifica account ◦ Se falso, impedisce la modifica dell'account. ◦ Impostazione predefinita: true • Consenti modifica nome dispositivo ◦ Se falso, impedisce la modifica del nome del dispositivo. ◦ Impostazione predefinita: true • Consenti modifica di impronte digitali Touch ID ◦ Se falso, impedisce la modifica delle impronte digitali di Touch ID. ◦ Impostazione predefinita: true
macOS 15.0+	**Solo supervisionati**:

Versione macOS	Funzionalità

	• Consenti Genmoji
	  ◦ Selezionare per consentire la creazione di Genmoji.
	  ◦ Impostazione predefinita: true
	• Consenti Image Playground
	  ◦ Selezionare per consentire l'uso della generazione di immagini.
	  ◦ Impostazione predefinita: true
	• Consenti iPhone Mirroring
	  ◦ Selezionare per consentire il mirroring dell'iPhone in un dispositivo macOS.
	  ◦ Impostazione predefinita: true
	• Consenti Writing Tools
	  ◦ Selezionare per abilitare gli strumenti di scrittura di Apple Intelligence.
	  ◦ Impostazione predefinita: true

macOS 15.1+
 	
macOS 15.2+
	Solo supervisionati:
	• Consenti riepilogo posta
	  ◦ Seleziona per consentire la creazione manuale di riepiloghi dei messaggi e-mail.
	  ◦ Impostazione predefinita: true
	• Consenti modifica condivisione elementi multimediali
	  ◦ Seleziona per consentire la modifica delle impostazioni di condivisione elementi multimediali.
	  ◦ Impostazione predefinita: true
	
	Solo supervisionati:
	• Consenti integrazioni di intelligence esterna
	  ◦ Seleziona per abilitare l'uso di servizi di intelligence esterni basati sul cloud con Siri.
	  ◦ Impostazione predefinita: true
	• Consenti accesso integrazioni di intelligence esterna
	  ◦ Seleziona per abilitare la modifica delle preferenze del browser predefinito. Il comando Impostazioni Ivanti Neurons per MDM per impostare le preferenze del browser predefinito continuerà a funzionare anche quando questa opzione viene applicata.
	  ◦ Impostazione predefinita: true

macOS 15.3	**Protezione e privacy**: • Consenti ID dell'area di lavoro intelligence esterna ◦ Immettere ID dell'area di lavoro Intelligence esterna consentita

Versione macOS	Funzionalità

	• Consenti Note Sintesi trascrizione
	  ◦ Selezionare per abilitare la creazione di riepiloghi dalle trascrizioni.
	  ◦ Impostazione predefinita: true

10.10.4.37. Restrizioni dell'App Store di macOS

Licenza: Gold

Le restrizioni dell'App Store di macOS consentono di definire quali restrizioni sono abilitate nell'App Store di macOS.

È possibile impostare le seguenti opzioni:

Impostazione	**Operazione da eseguire**
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Impostazioni configurazione	
Versione macOS	**Funzionalità**
10.9 e versioni successive	Limitare le installazioni di app agli utenti amministratori.
10.10 e versioni successive	• Limita le installazioni di app ai soli aggiornamenti software. • Disabilita l'adozione di app da parte degli utenti. • Disabilita le notifiche di aggiornamenti software.
10.11 e versioni successive	Limita l'installazione di app agli aggiornamenti software e alle app installate su MDM.

Distribuzione della configurazione

Procedura

1. Impostare le opzioni utilizzando la tabella precedente.
2. Fare clic su **Avanti**.
3. Selezionare l'opzione **Abilita questa configurazione**.
4. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato

Fare clic su **Fine**.

10.10.4.38. Restrizioni della masterizzazione dischi in macOS

Licenza: Gold

Le restrizioni della masterizzazione dischi in macOS consentono di gestire le restrizioni della masterizzazione dischi in macOS. È possibile configurare le **Impostazioni Finder in macOS** per abilitare o disabilitare le opzioni di masterizzazione dischi dall'app Finder in macOS.

È possibile impostare le seguenti opzioni:

Impostazione	**Operazione da eseguire**
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Impostazioni configurazione	
Impostazione	**Operazione da eseguire**
Consenti masterizzazione dischi	• Attivato • Disattivato • Richiedi autenticazione

Distribuzione della configurazione

Procedura

1. Impostare le opzioni utilizzando la tabella precedente.
2. Fare clic su **Avanti**.
3. Selezionare l'opzione **Abilita questa configurazione**.
4. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato

Fare clic su **Fine**.

10.10.4.39. Controllo supporti multimediali consentito (deprecato)

Licenza: Gold

La configurazione Controllo supporti multimediali consentitogestisce le opzioni di montaggio, smontaggio ed espulsione di supporti multimediali fisici in macOS.

È possibile impostare le seguenti opzioni:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione **Impostazioni configurazione** **Controllo montaggio per tipi di supporti multimediali** Attivare il controllo montaggio per ciascun tipo di supporto multimediale e configurare le impostazioni di montaggio. Se si disattiva il controllo montaggio, verrà applicata l'impostazione predefinita del sistema operativo.	Immettere una descrizione esplicativa dello scopo della configurazione.
Tipo di supporto multimediale	**Impostazioni di montaggio**
• CD • DVD • BD	• Sola lettura con autenticazione • Nega montaggio • Espelli supporto multimediale
• CD vuoto • DVD vuoto • BD vuoto • DVD-RAM • Immagine disco • Hard disk interno • Hard disk esterno • Disco di rete	• Sola lettura • Nega montaggio • Espelli supporto multimediale • Autentica
• l'hard disk esterno include HDD USB, unità flash USB e schede SD. • I supporti multimediali di sola lettura, come CD, DVD e BD, vengono montati come supporti di sola lettura per impostazione predefinita.	
Controllo smontaggio per tipi di supporti multimediali	
Attivare il controllo smontaggio per ciascun tipo di supporto multimediale e configurare le impostazioni di smontaggio. Se si disattiva il controllo smontaggio, verrà applicata l'impostazione predefinita del sistema operativo. Prestare attenzione quando si seleziona l'impostazione Nega smontaggio per i tipi di supporti multimediali.	

Impostazione	Operazione da eseguire
Tipo di supporto multimediale • CD • DVD • BD • CD vuoto • DVD vuoto • BD vuoto • DVD-RAM • Immagine disco • Hard disk interno • Hard disk esterno • Disco di rete **Impostazioni Espelli alla disconnessione** I tipi di supporti multimediali da espellere automaticamente quando l'utente si disconnette. **Tipo di supporto multimediale** • CD • DVD • BD • CD vuoto • DVD vuoto • BD vuoto • DVD-RAM • Immagine disco • Hard disk esterno • Disco di rete	**Impostazioni di montaggio** • Nega smontaggio • Autentica

Distribuzione della configurazione

Procedura

1. Impostare le opzioni utilizzando la tabella precedente.
2. Fare clic su **Avanti**.
3. Selezionare l'opzione **Abilita questa configurazione**.
4. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi

- Nessun dispositivo (impostazione predefinita)
- Personalizzato

Fare clic su **Fine**.

10.10.4.40. Impostazioni Finder in macOS

Licenza: Gold

Le Impostazioni Finder in macOS consentono di gestire le impostazioni dell'app Finder in macOS.

È possibile impostare le seguenti opzioni:

Impostazione	**Operazione da eseguire**
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Impostazioni configurazione	
Impostazione	**Operazione da eseguire**
Disabilita supporto per la masterizzazione dischi in Finder	• ON • OFF

Distribuzione della configurazione

Procedura

1. Impostare le opzioni utilizzando la tabella precedente.
2. Fare clic su **Avanti**.
3. Selezionare l'opzione **Abilita questa configurazione**.
4. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato

Fare clic su **Fine**.

10.10.4.41. Policy di estensione kernel di macOS

Applicabile a: macOS 10.13.2 o versioni successive supportate.

Controlla le restrizioni e le impostazioni per il caricamento delle estensioni del kernel approvate dagli utenti.

Creazione della configurazione di una policy di estensione kernel di macOS

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **kernel** nel campo di ricerca, quindi fare clic sulla configurazione **Policy di estensione kernel di macOS**.
4. Assegnare un nome e una descrizione alla configurazione.
5. Selezionare l'opzione **Consenti le sostituzioni da parte dell'utente** per consentire agli utenti di approvare ulteriori estensioni del kernel non esplicitamente consentite dalla seguente configurazione.
6. Nella sezione Identificatori del team ed estensioni del kernel consentiti, fare clic su **+ Aggiungi** per aggiungere gli identificatori del team e le estensioni del kernel consentiti. Un'estensione del kernel è l'identificatore bundle di un pacchetto. Per ciascun identificatore del team, è possibile aggiungere diversi nomi di estensioni del kernel con firma valida nella finestra pop-up.
7. Fare clic su **Aggiungi**.
8. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
9. Fare clic su **Fine**.

Per ulteriori informazioni, vedere Come creare una configurazione

10.10.4.42. Mobile@Work per macOS

Argomenti della sezione:

- Configurazione di Mobile@Work per macOS e flusso di lavoro di esecuzione degli script
- Creazione di una configurazione Mobile@Work per macOS
- Attivazione dell'onboarding utenti per i dispositivi macOS
- Creazione di una configurazione dello script di Mobile@Work per macOS
- Eseguire una disinstallazione completa di Mobile@Work per macOS
- Applicazione di script tramite macOS Mobile@Work

Ivanti Neurons per MDM consente di creare i propri script della shell macOS, che è quindi possibile caricare in Ivanti Neurons per MDM ed eseguire sui dispositivi macOS gestiti. Per informazioni sulle attività di creazione, caricamento e gestione del repository di script, vedere Tutti gli script.

Un utente di dispositivo macOS può avviare il ritiro del dispositivo utilizzando Mobile@Work per macOS 1.1 o versioni successive. L'opzione di dismissione è disponibile quando si fa clic su **Disinstalla** nella schermata Informazioni su Mobile@Work. In Ivanti Neurons per MDM, è possibile verificare lo stato del dispositivo nella pagina **Dispositivi** e nella pagina dei dettagli del dispositivo.

Mobile@Work per macOS 1.5 o versioni successive apre Apps@Work immediatamente dopo la registrazione e non è necessario attendere il completamento della registrazione MDM.

In Mobile@Work per macOS, fare clic sul riquadro di un'applicazione per visualizzare la pagina Dettagli app per tale applicazione, che include la descrizione, le schermate, le valutazioni e le recensioni dell'app.

Mobile@Work per macOS notifica al server Ivanti Neurons per MDM se le app macOS interne Packager sono installate o meno nel report dell'inventario.

Prerequisiti

Nell'App Catalog, il client Mobile@Work per macOS è disponibile come app aziendale. Prima di poter eseguire gli script della shell sui dispositivi macOS, richiedere agli utenti di registrare i loro dispositivi con Ivanti Neurons per MDM usando Mobile@Work per macOS.

Procedura

1. Scaricare l'applicazione Mobile@Work per macOS. È disponibile come file PKG all'indirizzo https://support.mobileiron.com/support/CDL.html. Vedere questo articolo del forum dei clienti Ivanti per informazioni su come ottenere le credenziali per il sito di download.
2. Caricare il file PKG per Mobile@Work per macOS su un server sicuro. Il server deve essere accessibile da parte degli utenti del dispositivo.
3. Condividere l'URL del file di installazione per Mobile@Work per macOS con gli utenti del dispositivo tramite un messaggio di posta elettronica o altro tipo di messaggio.
4. Richiedere agli utenti di:
    1. Scaricare e installare Mobile@Work per macOS sul proprio dispositivo.
    2. Registrare i dispositivi con Ivanti Neurons per MDM utilizzando Mobile@Work per macOS.

Configurazione di Mobile@Work per macOS e flusso di lavoro di esecuzione degli script

Procedura

1. Configurare e distribuire una configurazione Mobile@Work per macOS.
2. Configurare e distribuire una configurazione Mobile@Work per macOS per caricare lo script in Ivanti Neurons per MDM. Gli script sono crittografati e firmati utilizzando un certificato firmato che è unico per ciascun tenant. La chiave per decrittografare lo script viene inviata al dispositivo insieme all'URL di download dello script, che viene crittografato e firmato.
3. Ivanti Neurons per MDM esegue gli script sui dispositivi macOS utilizzando Mobile@Work per macOS. Mobile@Work per macOS esegue periodicamente il polling di Ivanti Neurons per MDM per verificare se ci sono script in attesa di esecuzione. Se ci sono script nella coda, Mobile@Work scarica ed esegue gli script sui dispositivi macOS in base alle impostazioni definite in Ivanti Neurons per MDM.
4. Mobile@Work restituisce i risultati di esecuzione dello script a Ivanti Neurons per MDM, che vengono visualizzati nei registri del dispositivo. È possibile verificare i registri del dispositivo nella pagina dei dettagli del dispositivo macOS, nella scheda **Registri** .

Creazione di una configurazione Mobile@Work per macOS

Per la configurazione di Mobile@Work per macOS è disponibile una configurazione di sistema predefinita. Tuttavia, essa non viene distribuita a tutti i dispositivi per impostazione predefinita.

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **work** nel campo di ricerca e fare clic sulla configurazione **Mobile@Work per macOS**.
4. Assegnare un nome e una descrizione alla configurazione.
5. Immettere il valore **Tempo di esecuzione massimo** in secondi per specificare per quanto tempo lo script può essere eseguito. Il valore predefinito è 60 secondi.
6. Immettere il valore **Dimensioni risposta massime** in kilobyte (KB) per specificare il limite massimo delle dimensioni della risposta dell'output dello script che viene restituito a Ivanti Neurons per MDM. Si tratta dei dati stdout o stderr che vengono restituiti quando viene eseguito lo script. Il valore predefinito è 1 KB.
7. Immettere il valore **Frequenza check-in** in minuti per specificare la frequenza con cui l'app Mobile@Work per macOS deve effettuare il check-in con Ivanti Neurons per MDM. Il valore predefinito è di 15 minuti.
8. (Opzionale) È possibile attivare l'onboarding utenti per dispositivi macOS nella sezione **Attivazione dell'onboarding utenti per i dispositivi macOS**.
9. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
    1. Scegliere un livello di distribuzione:
    2. **A tutti**: l'app viene aggiunta su tutti i dispositivi compatibili degli utenti.
    3. **A nessuno**: l'app viene predisposta per essere distribuita in seguito.
    4. **Distribuzione personalizzata** - Selezionare una delle opzioni seguenti:
        - **Utenti/Gruppi di utenti** - L'app viene distribuita solamente agli utenti o ai gruppi di utenti selezionati.
          Fare clic sulla scheda **Utenti** per selezionare gli utenti.
          Fare clic sulla scheda **Gruppi di utenti** per selezionare i gruppi di utenti.

- **Dispositivi/Gruppi di dispositivi** - L'app viene distribuita solamente ai dispositivi o ai gruppi di dispositivi selezionati.
  Fare clic sulla scheda **Dispositivi** per selezionare i dispositivi.
  Fare clic sulla scheda **Gruppi di dispositivi** per selezionare i gruppi di dispositivi.

10. Fare clic su **Fine**.

Attivazione dell'onboarding utenti per i dispositivi macOS

Se di desidera attivare l'onboarding degli utenti per i dispositivi macOS durante il processo Registrazione dispositivi automatizzato, procedere come segue:

- Al termine del processo Registrazione dispositivi, Mobile@Work per macOS (necessaria versione 1.68 o successiva) viene inviato al dispositivo insieme ai profili, alle configurazioni e alle app.
- Il client Mobile@Work per macOS e altre app sono inviati ai dispositivi solo se:
  - Le app sono sia app PKG in-house o app pubbliche Apple App e libri.
  - L'impostazione di installazione invisibile per le app è impostata su Vero. L'impostazione è disponibile nella pagina **App** > Dettagli app > **Configurazione app** > **Installa su dispositivo**.
  - La priorità per le app è impostata su Alta. Per impostazione predefinita, la priorità dell'app client Mobile@Work per macOS è impostata su alta (e non può essere modificata), **senza la quale il processo di onboarding degli utenti potrebbe non riuscire**.
  - Le app sono configurate per essere distribuite ai dispositivi, gruppi di utenti o gruppi di dispositivi.
- Dopo avere installato e registrato Mobile@Work per macOS, il dispositivo macOS entra in modalità tutto schermo (l'utente non ha controllo sul dispositivo) finché i profili, le configurazioni e le app rimanenti non vengono configurati e installati. L'avanzamento viene visualizzato in passaggi.

Per Mobile@Work per macOS 1.73 o versioni successive, fino alla versione più recente supportata da Ivanti Neurons per MDM, sono supportate le seguenti funzioni aggiuntive:

- Il processo di onboarding degli utenti viene completato subito dopo aver completato l'operazione Registrazione dispositivi per un dispositivo. Il processo di onboarding degli utenti non inizia dopo la scadenza della finestra di tempo per avviare l'onboarding degli utenti (in genere 20 minuti dopo la registrazione del dispositivo), anche se un amministratore consente l'onboarding degli utenti nella configurazione di Mobile@Work. Ciò impedisce a un dispositivo di entrare nella modalità tutto schermo di onboarding degli utenti quando il dispositivo viene utilizzato normalmente.
- Il processo di onboarding degli utenti viene visualizzato in passaggi nel client Mobile@Work per macOS. Le configurazioni verranno installate come parte del primo passaggio.
- All'inizio vengono installate le app ad alta priorità. Ogni app ad alta priorità viene considerata come un passaggio. Le app di Packager non vengono conteggiate fra i passaggi.
- Le app rimanenti continueranno a essere installate in background anche dopo che l'onboarding degli utenti è stato completato. Le app sono contrassegnate come installate una volta inizializzata l'installazione su un dispositivo o dopo che l'app è stata effettivamente installata.
- Dopo l'onboarding degli utenti, è possibile andare alla pagina dei dettagli del dispositivo per verificare le configurazioni e le app inviate a ciascun dispositivo. Ulteriori informazioni sono disponibili nei registri.

Procedura

1. Creare una configurazione Mobile@Work per macOS utilizzando **Creazione di una configurazione Mobile@Work per macOS**.
2. Selezionare l'opzione **Attiva onboarding utenti**.

3. Immettere i seguenti dettagli:
    - **Valore timeout onboarding utente** - Specificare il tempo approssimativamente impiegato dal dispositivo per installare l'app e le configurazioni durante la configurazione iniziale del dispositivo. Per impostazione predefinita, il processo di onboarding degli utenti su un dispositivo macOS termina dopo 120 secondi, un valore che può essere modificato i base alle esigenze.
    - **URL pagina di destinazione utente** - Specificare l'URL della pagina di destinazione dell'utente visualizzata al termine dell'onboarding.
4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
5. Fare clic su **Fine**.

Creazione di una configurazione dello script di Mobile@Work per macOS

È possibile creare e distribuire più configurazioni dello script di Mobile@Work per macOS ai dispositivi. Tramite questa configurazione è possibile selezionare dal repository uno script (**Amministratore > Script e file > Tutti gli script**) da distribuire a Mobile@Work per macOS.

Con Mobile@Work per macOS 1.66 o versioni successive, è possibile pianificare l'esecuzione degli script nei dispositivi. Se si pianifica l'esecuzione di uno script per l'esecuzione nei dispositivi con versioni client di Mobile@Work per macOS anteriori alla 1.66, lo script viene eseguito una volta sola. Se il client Mobile@Work per macOS viene aggiornato dalla versione 1.4 alla versione 1.66, tutte le configurazioni client macOS verranno redistribuite ai dispositivi.

Prerequisiti

- Accedere ad **Amministratore > Script e file > Tutti gli script** per caricare e gestire gli script utilizzabili in questa configurazione e distribuiti ai dispositivi.
- Impostare la configurazione Mobile@Work per macOS e distribuirla ai dispositivi. In caso contrario, la configurazione dello script di Mobile@Work per macOS sarà in stato di errore.

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **work** nel campo di ricerca e fare clic sulla configurazione **Script di Mobile@Work per macOS**.
4. Assegnare un nome e una descrizione alla configurazione.
5. Nel campo **Seleziona script** immettere il nome dello script da cercare e selezionare lo script dall'elenco a discesa.
6. Nella sezione Input script, vengono visualizzate le etichette di input script e le variabili degli script associate con lo script. Se è necessario sovrascriverle, inserire le variabili di script alternativi (ad esempio, {$userWorkEmailAddress}) e i loro valori predefiniti alternativi (ad esempio, mario.rossi@azienda.com).
7. Nella sezione Esecuzione script selezionare una delle seguenti opzioni di pianificazione:
    - Esegui una volta arrivato al deployment
    - Esecuzione ricorrente
8. Se si sceglie Esecuzione ricorrente, specificare i dettagli seguenti:
    - Fuso orario da usare - Selezionare l'ora UTC o l'ora locale del dispositivo. Lo script verrà eseguito all'ora selezionata in questo campo.
    - L'esecuzione inizia il - Selezionare la data di inizio.
    - L'esecuzione termina il - Selezionare la data di fine, che deve essere maggiore o uguale a quella di inizio.

- Esegui script - Selezionare Quotidianamente o Settimanalmente e immettere le ore (nel formato a 24 ore), i minuti e i giorni, come applicabile.

9. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
10. Fare clic su **Fine**.

Eseguire una disinstallazione completa di Mobile@Work per macOS

Se è stata attivata l'opzione **Rimuovi le app non registrate (applicabile solo ad app gestite)** durante l'installazione di Mobile@Work per macOS e si avvia il dispositivo da dismettere nel portale amministratore di Ivanti Neurons for MDM, l'applicazione Mobile@Work per macOS e lo script di disinstallazione vengono eliminati dal dispositivo. Per evitare che processi e script vengano eseguiti nel back-end, assicurarsi di deselezionare l'opzione riportata di seguito dal portale amministratore di Ivanti Neurons for MDM durante la registrazione del dispositivo di nuovi utenti o la dismissione di utenti esistenti, al fine di garantire che lo script di disinstallazione venga eseguito ed elimini i processi e gli script associati dal back-end.

Procedura

1. Accedere al portale amministratore di Ivanti Neurons for MDM.
2. Selezionare **App** > **Mobile@Work** > **Configurazioni app** > **Elenco Riepilogo configurazioni app** > **Impostazioni app Apple** >**Impostazioni di configurazione per la gestione delle applicazioni Apple**.
3. Nella pagina **Impostazioni di configurazione**, deselezionare la seguente opzione:
   - **Rimuovi le app non registrate (applicabile solo ad app gestite)**.

Applicazione di script tramite macOS Mobile@Work

Gli script tramite macOS Mobile@Work consentono agli amministratori di distribuire ed eseguire script di shell in remoto su dispositivi macOS gestiti. Ciò aiuta ad automatizzare le attività, applicare correzioni, applicare criteri e semplificare la configurazione senza richiedere l'intervento dell'utente, garantendo una gestione del dispositivo uniforme ed efficace su larga scala.

Prerequisiti:

- I dispositivi devono eseguire macOS.
- Mobile@Work per macOS deve essere già installato sui dispositivi.
- Assicurarsi che la configurazione Mobile@Work per macOS sia correttamente creata, distribuita e assegnata. Per ulteriori dettagli, vedere Creazione di un Mobile@Work per la configurazione macOS.

> Non è possibile applicare script tramite macOS Mobile@Work se il dispositivo non dispone del client Mobile@Work, o se la piattaforma del dispositivo non supporta l'esecuzione degli script. Assicurarsi che il client macOS sia attivo e che si selezionino solo i dispositivi macOS supportati.

Procedura

1. Accedere al portale amministratore di Ivanti Neurons for MDM.
2. Andare su **Dispositivi** e selezionare l'elenco di dispositivi macOS per i quali si desidera eseguire lo script.
3. Nella pagina **Dispositivi**, passare ad **Azioni** > **macOS** > **Script tramite macOS Mobile@Work**.
   Viene visualizzato il riquadro **Script tramite macOS Mobile@Work**.
4. Per applicare gli script, nel campo **Seleziona script** immettere e selezionare il nome dello script.
   Per maggiori informazioni sulla creazione di uno script, vedere Tutti gli script.

5. Selezionare **OK** per eseguire lo script sui dispositivi.

Argomenti correlati:

- **Amministratore > Script e file > Tutti gli script**
- **Come creare una configurazione**

10.10.4.43. Configurazione delle regole di aggiornamento del software macOS

Gli amministratori possono configurare le policy di aggiornamento del software di un dispositivo definendo le **Regole dei aggiornamento del software macOS**.

Applicabile a: da macOS 10.7 a 26.0.

1. Andare in Configurazioni > +Aggiungi.
2. Digitare macOS nel campo di ricerca, quindi fare clic sulla configurazione Impostazioni aggiornamento software per macOS.
3. Immettere un Nome e una Descrizione per la configurazione.
4. Selezionare le configurazioni necessarie in **Regole dei aggiornamento del software macOS**.
5. Fare clic su Avanti.
6. Selezionare l'opzione Abilita questa configurazione.
7. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzata.
8. Fare clic su Fine.

Regole dei aggiornamento del software macOS

Gli amministratori possono selezionare le regole dall'elenco seguente:

> Quando queste regole sono applicare nel dispositivo, gli utenti non possono modificare queste impostazioni.

- Autorizzazione dell'installazione di versioni preliminari del software.
- Automaticamente:
    - Controlla aggiornamenti
    - Scarica nuovi aggiornamenti quando disponibili
    - Installa aggiornamenti di macOS
    - Installa aggiornamenti delle app dall'App Store
    - Installa aggiornamenti dei file di dati di sistema e della sicurezza
- Limitare le installazioni di app agli utenti amministratori.
- Opzione per l'aggiunta dell'URL del catalogo di aggiornamento del software (non supportata in macOS 11 e versioni successive).

10.10.4.44. Preferenza certificato

Applicabile a:

- macOS 10.12 fino alla versione più recente supportata da Ivanti Neurons for MDM.

Consente di identificare una voce Preferenza certificato nel portachiavi dell'utente che fa riferimento a un payload del certificato incluso nello stesso profilo.

Questa configurazione viene utilizzata per associare un certificato a un indirizzo e-mail o a un URL. Dopo che un certificato è stato associato a un indirizzo e-mail, l'app Mail lo utilizza per tale account e-mail. Se un certificato SSL di un sito Web non è attendibile, l'aggiunta di una Preferenza certificato assicura che il browser non mostri un messaggio di avviso quando l'utente prova ad accedere al sito Web.

> Gli amministratori devono essere in possesso di un certificato. Per ulteriori informazioni sull'aggiunta e la distribuzione di un certificato, vedere **Configurazione dei certificati**.

Creazione di una configurazione Preferenza certificato

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **preferenza** nel campo di ricerca, quindi fare clic sulla configurazione **Preferenza certificato**.
4. Assegnare un nome e una descrizione alla configurazione.
5. Nel campo **Nome** della sezione Impostazioni configurazione, immettere un ID e-mail o un nome per cui viene richiesto un certificato preferenziale.
6. Nel campo **UUID certificato** selezionare un certificato.
7. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
8. Fare clic su **Fine**.

Argomenti correlati:

- **Preferenza identità**
- **Configurazione dei certificati**
- **Come creare una configurazione**

10.10.4.45. Active Directory (macOS)

Applicabile a: macOS 10.9 o versioni successive supportate.

Configurare le opzioni avanzate per associare i dispositivi macOS a un dominio Active Directory (AD) per accedere ai servizi software che si basano su AD per l'autenticazione e la sicurezza.

Argomenti della sezione:

- Creazione di una configurazione di Active Directory
- Impostazioni di Active Directory

Creazione di una configurazione di Active Directory

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **privacy** nel campo di ricerca, quindi fare clic sulla configurazione **Active Directory**.
4. Assegnare un nome e una descrizione alla configurazione.
5. Immettere le impostazioni come descritto nella seguente tabella delle impostazioni di Active Directory.
6. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
7. Fare clic su **Fine**.

Impostazioni di Active Directory

Impostazione	Operazione da eseguire
Impostazioni di Active Directory di base	
Nome host	(Obbligatorio) Immettere il nome host, ovvero il dominio di Active Directory da aggiungere.
Nome utente	Immettere il nome utente dell'account usato per aggiungere il dominio.
Password	Immettere la password dell'account usato per aggiungere il dominio.
Unità organizzativa AD	Immettere l'unità organizzativa (UO) a cui l'oggetto computer di unione viene aggiunto.
Stile di montaggio di AD	Selezionare una delle opzioni seguenti per indicare il protocollo della home directory della rete da usare: • AFP • SMB
Impostazioni di Active Directory avanzate	
Abilita la chiave ADCreateMobileAccountAtLogin	Abilitare o disabilitare la chiave ADCreateMobileAccountAtLogin. Opzione aggiuntiva: creare un account per dispositivi mobili all'accesso.
Abilita la chiave ADWarnUserBeforeCreatingMA	Abilitare o disabilitare la chiave ADWarnUserBeforeCreatingMA. Opzione aggiuntiva: avvisare l'utente prima di creare un account per dispositivi mobili.
Abilita la chiave ADForceHomeLocal	Abilitare o disabilitare la chiave ADForceHomeLocal. Opzione aggiuntiva: forzare la home directory locale.
Abilita la chiave ADUseWindowsUNCPath	Abilitare o disabilitare la chiave ADUseWindowsUNCPath. Opzione aggiuntiva: usare il percorso UNC da AD per ricavare la posizione della home directory della rete.
Abilita la chiave ADAllowMultiDomainAuth	Abilita o disabilita la chiave ADAllowMultiDomainAuth. Opzione aggiuntiva: consentire l'autenticazione da qualsiasi dominio nella foresta.
Shell dell'utente predefinita	Immettere la shell dell'utente predefinita, ad esempio /bin/bash.
Mappa l'UID dell'utente per l'attributo	Selezionare questa opzione per mappare l'UID dell'utente per l'attributo specificato.
Mappa il GID dell'utente per l'attributo	Selezionare questa opzione per mappare il GID dell'utente per l'attributo specificato.
Mappa il GID del gruppo per l'attributo	Selezionare questa opzione per mappare il GID del gruppo per l'attributo specificato.
Server di dominio preferito	Impostare questo server di dominio come Preferito.
Convenzione spazio dei nomi	Selezionare una delle seguenti convenzioni di denominazione dell'account utente: • Dominio (opzione predefinita) • Foresta

Impostazione	Operazione da eseguire
Firma del pacchetto	Selezionare una delle seguenti opzioni di firma del pacchetto: • Consenti (opzione predefinita) • Disattiva • Richiedi
Cifratura del pacchetto	Selezionare una delle seguenti opzioni di cifratura del pacchetto: • Consenti (opzione predefinita) • Disattiva • Richiedi • SSL
Consenti l'amministrazione da gruppi di Active Directory specifici	Selezionare questa opzione per consentire l'amministrazione da gruppi di Active Directory specifici. Fare clic su **Aggiungi** per aggiungere uno o più gruppi.
Limita DNS dinamico	Selezionare questa opzione per limitare gli aggiornamenti DNS per interfacce specifiche (ad esempio en0, en1 e così via). Fare clic su **Aggiungi** per aggiungere uno o più nomi dell'interfaccia.
Modifica intervallo di password	Specificare la frequenza (in giorni) con cui è necessario modificare la password dell'account del computer trust. Il valore zero è disabilitato.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.4.46. Preferenza identità

Applicabile a: macOS 10.12 o versioni successive supportate.

Consente di identificare una voce Preferenza identità nel portachiavi dell'utente che fa riferimento a un payload dell'identità incluso nello stesso profilo.

Nei dispositivi MacOS, una Preferenza identità consente di scegliere l'identità (coppia di chiavi) che si desidera utilizzare con un sito Web. Dopo aver eseguito il push di una Preferenza identità (composta dall'URL e dall'identità) al dispositivo, questa voce comparirà in **Accesso portachiavi → Tutte le voci** (il "Tipo" sarà "Preferenza identità"). La prossima volta che si prova ad accedere all'URL specifico da Safari, il dispositivo mostrerà il certificato configurato.

Ivanti Neurons per MDM crea una configurazione Preferenza identità di sistema predefinita con un payload per l'URL AppStore e il certificato da utilizzare.

Durante l'accesso all'App Catalog macOS tramite Safari su macOS 10.12 e versioni successive, all'utente viene richiesto di immettere una password di sistema per memorizzare il certificato di identità nella cache. La prima volta è necessario selezionare "Consenti sempre" per evitare richieste successive durante l'accesso all'App Catalog macOS.

Safari con versioni di macOS anteriori alla 10.12 e gli altri browser richiedono il certificato e la password di sistema durante l'accesso all'App Catalog macOS nelle nuove sessioni del browser dai dispositivi macOS.

Creazione di una configurazione Preferenza identità

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **preferenza** nel campo di ricerca, quindi fare clic sulla configurazione **Preferenza identità**.
4. Assegnare un nome e una descrizione alla configurazione.
5. Nel campo **Nome** della sezione Impostazioni configurazione, immettere un ID e-mail, un nome host DNS o un nome che identifica il servizio in modo univoco.
6. Nel campo **UUID certificato** selezionare un certificato.
7. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
8. Fare clic su **Fine**.

Argomenti correlati:

- Preferenza certificato
- Come creare una configurazione

10.10.4.47. Creazione automatica dell'account Office 365 (macOS)

Applicabile a:

- Dispositivi macOS supportati.
- Le versioni app di Microsoft Office 365 consigliate sono 16.13.x o successive.

Configurare le informazioni utente e le opzioni per impostare la configurazione iniziale per tutte le applicazioni Microsoft Office 365.

Argomenti della sezione:

- Creazione di una configurazione automatica dell'account Office 365
- Impostazioni di creazione automatica dell'account Office 365

Creazione di una configurazione automatica dell'account Office 365

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **Office** nel campo di ricerca e fare clic sulla configurazione **Creazione automatica dell'account Office 365**.
4. Assegnare un nome e una descrizione alla configurazione.
5. Immettere le impostazioni come descritto nella seguente tabella delle impostazioni di creazione automatica dell'account Office 365.
6. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
7. Fare clic su **Fine**.

Impostazioni di creazione automatica dell'account Office 365

Impostazione	Operazione da eseguire
Indirizzo e-mail di attivazione di Office	Immettere l'indirizzo e-mail dell'utente.
Accesso automatico a Office	Selezionare questa opzione non mostrare e finestra della prima esecuzione. Richiede all'utente solo informazioni obbligatorie come le informazioni di autenticazione di O365.
Impostazione predefinita su Apri e Salva locale	Selezionare questa opzione per forzare il pannello Apri/Salva su "Sul mio Mac" invece che su "Posizioni online".
Mostra le novità all'avvio	Selezionare questa opzione per visualizzare le informazioni sulle nuove funzionalità all'avvio.
Stato di esecuzione macro di Visual Basic	Selezionare una delle seguenti opzioni: • Disabilitato con avvisi • Disabilitato senza avvisi • Abilitato con avvisi
Disabilita file esterni con estensione DYLIB di Visual Basic	Selezionare questa opzione per disabilitare le dipendenze esterne di Visual Basic.
Consenti a Visual Basic di associare il sistema	Selezionare questa opzione per consentire alle macro di usare un'istruzione DECLARE per eseguire l'associazione all'API del sistema operativo. Questa API consente alle macro di eseguire processi esterni arbitrari e di passare loro dati arbitrari sulla riga di comando.
Disabilita Visual Basic per associarlo alla funzione popen	Selezionare questa opzione per consentire alle macro di usare un'istruzione DECLARE per eseguire l'associazione all'API del sistema operativo della funzione popen. Questa API consente alle macro di eseguire processi esterni arbitrari e di passare loro dati arbitrari sulla riga di comando.
Disabilita lo script Mac di Visual Basic	Selezionare questa opzione per consentire alle macro di richiamare l'API di Visual Basic dello script Apple.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.4.48. Autentica

Applicabile a:

- macOS 10.13 e versioni successive supportate.
- Windows 10 e versioni successive supportate.

Utilizzare la configurazione Autenticazione per fornire autenticazione senza password per i servizi cloud e/o gli accessi desktop. Ogni dispositivo avrà una sola configurazione Autenticazione.

Prerequisiti

- È necessaria la licenza Zero Sign-On.
- Ivanti Neurons per MDM deve essere registrato con Access (il profilo Access deve essere configurato).
- Dopo aver impostato la configurazione Autenticazione, non è possibile annullare la registrazione al profilo Access in quanto si farà riferimento a questo profilo dalla configurazione Autenticazione.
- Se il profilo Access viene modificato, distribuire di nuovo la configurazione Autenticazione nei dispositivi macOS. Per i dispositivi Windows, copiare e utilizzare i nuovi valori CLI nelle nuove app.

Creazione di una configurazione Autenticazione

Procedure

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **auth** nel campo di ricerca, quindi fare clic sulla configurazione **Autenticazione**.
4. Assegnare un nome e una descrizione alla configurazione.
5. Selezionare un **Certificato di identità desktop** dall'elenco a discesa.
6. Selezionare una o entrambe le opzioni di sistema operativo seguenti:
    - macOS
    - Windows
7. Per macOS:
    1. Nell'area Dati personalizzati, fare clic su **+Aggiungi** per aggiungere le chiavi e i valori di stringa in modo da inviare i dati personalizzati ai dispositivi.
    2. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
    3. Fare clic su **Fine**.
8. Per i dispositivi Windows 10, questa configurazione aiuta a generare gli argomenti della riga di comando per l'app Authenticator MSI per Windows come segue:
    1. Fare clic su **Fine** per completare la configurazione di Autenticazione.
    2. Nella pagina **Configurazioni**, visualizzare la configurazione Autenticazione per copiare il testo della riga di comando visualizzato. Questo testo è necessario quando si distribuisce l'app Autenticazione per i dispositivi Windows.

> Quando la configurazione di Autenticazione viene applicata a dispositivi Windows, la configurazione rimane nello stato Installazione in sospeso. È possibile ignorare questo passaggio in quanto non ci sarà alcun impatto sulla funzionalità.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.4.49. Catalogo app Apple

Applicabile a: iOS e macOS

La configurazione del Catalogo app Apple gestisce l'accesso al catalogo mediante una clip Web. A partire dalla versione 83 di Ivanti Neurons for MDM, è possibile eseguire la transizione all'esperienza nativa Apps@Work dall'applicazione Go. Per i tenant creati di recente, la configurazione Apps@work Webclip non viene distribuita per impostazione predefinita per i dispositivi iOS installati mediante iReg o client. L'amministratore deve distribuire manualmente la configurazione della webclip ai dispositivi registrati mediante iReg o client.

> Il risultato della ricerca sul webclip di Apps@Work visualizza solo 10 applicazioni sui dispositivi iOS e iPad, anche se la richiesta di ricerca ha come parametro righe superiori a 10.

Procedura

Gli amministratori possono modificare la distribuzione di questa configurazione definita dal sistema come segue:

1. Accedere a **Configurazioni**.
2. Fare clic su **App Catalog Apple**.
3. Fare clic su **Modifica distribuzione**.
4. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi: la configurazione viene inviata a tutti i dispositivi compatibili.
    - Nessun dispositivo: consente di disattivare l'accesso a App Catalog Apple oppure di memorizzare la configurazione per distribuirla in seguito.
    - Personalizzato: consente di definire gruppi di dispositivi specifici a cui inviare la configurazione.

Fare clic su **Salva**.

10.10.4.50. Domini gestiti

Licenza: Silver

Una configurazione di dominio gestito consente di specificare quali domini sono attendibili per Mail e Safari sui dispositivi iOS 8+ e visionOS 1.1+. Dopo aver applicato la configurazione al dispositivo, i domini non specificati nella configurazione verranno evidenziati (non attendibili) nelle applicazioni Mail e Safari sul dispositivo. Utilizzare questa configurazione insieme alla **configurazione delle limitazioni** per controllare i download dei dati consentiti in Safari.

Impostazioni domini gestiti

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Domini e-mail gestiti	Fare clic su **+Aggiungi** per inserire un dominio, come ad esempio in lamiaazienda.com.
Domini Web gestiti	Fare clic su **+Aggiungi** per inserire un dominio, come ad esempio in lamiaazienda.com.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.4.51. Impostazioni passcode

Una delle prime azioni da svolgere in Ivanti Neurons per MDM durante la procedura di installazione guidata, è la configurazione di un passcode. Tale configurazione consente di definire le impostazioni relative alla funzione di blocco schermo sui dispositivi.

Impostazioni passcode

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Supporto dei valori semplici	Limita l'inclusione di determinati caratteri o cifre nel PIN o nella password. **Per iOS, macOS, watchOS, e Android:** selezionare per consentire pin o passcode meno sicuri perché contengono sequenze di caratteri ripetute, ascendenti o discendenti. Esempi: 1111, 1234, abcd. Deselezionando questa opzione per i dispositivi Android vengono applicati passcode con PIN complessi. Ad esempio, gli utenti non possono configurare sequenze di caratteri ripetute, crescenti, o decrescenti. **Per Windows 10+**: selezionare per consentire passcode meno sicuri perché contengono sequenze numeriche ripetute o ascendenti. Esempi: 1111, 1234.
Valore alfanumerico necessario	Impone al passcode di contenere almeno una lettera e un numero. **Per iOS e Android**: selezionare questa opzione per assicurarsi che i passcode contengano lettere e numeri. **Per Windows 10+**: selezionare per garantire una password robusta basata sullo standard Microsoft.
Lunghezza minima del passcode	Selezionare un numero dall'elenco per impostare una lunghezza minima per il passcode. **Per Windows 10 Desktop**: per gli account locali si applicano passcode con almeno 6 caratteri.
Numero minimo di caratteri complessi	**Per iOS e Android**: selezionare un numero dall'elenco per impostare un numero minimo di caratteri diversi da numeri o lettere. **Per Windows 10+**: gli account locali imporranno 3 caratteri complessi.
Validità passcode	Immettere un numero nel campo del numero di giorni dopo cui l'utente del dispositivo deve reimpostare il passcode. Se non si desidera impostare una validità del passcode, lasciare vuoto questo campo.
Blocco automatico	Selezionare un intervallo dall'elenco per definire la durata di inattività del dispositivo prima che venga attivato il blocco dello schermo.
Qualsiasi metodo di blocco	**Solo Android**. Consente all'utente di scegliere qualsiasi metodo di blocco, incluso lo sblocco dei criteri. Le impostazioni del passcode sopra citate non vengono applicate a questo dispositivo.
Cronologia passcode	Immettere un numero per impostare il numero di passcode univoci che un utente deve immettere prima di riutilizzare un passcode. Ad esempio, se questo campo viene impostato su 4, l'utente deve impostare 4 passcode prima di poter riutilizzare il primo passcode.
Periodo di tolleranza per il blocco del dispositivo	Selezionare un intervallo dall'elenco per impostare l'intervallo di tempo tra la visualizzazione della schermata di blocco e il momento in cui l'utente del dispositivo deve immettere un passcode per sbloccare il dispositivo.

Impostazione	Operazione da eseguire
Numero massimo di tentativi non riusciti	Selezionare un numero dall'elenco per impostare il numero di volte consecutive in cui un utente può immettere un passcode errato prima che il dispositivo venga reimpostato e ne vengano cancellati i dati. **Avviso**: i dispositivi verranno cancellati se l'utente supera il numero massimo di tentativi per la password. Utilizzare questa opzione con cautela.
(Solo macOS) Abilita espressione regolare del passcode (macOS 14+) (Solo macOS) Lingua	Specificare la stringa di espressione che corrisponde alla password per determinare se corrisponde al criterio. Specificare la lingua della descrizione.
(Solo macOS) Descrizione	Descrivere la complessità della password. Ad esempio, numeri, caratteri speciali, stringhe e così via.
(Solo macOS) Applica la regola del passcode al prossimo accesso	Selezionare per consentire a macOS di chiedere all'utente di modificare la password per renderla conforme alla policy delle password la prossima volta che l'utente esegue l'accesso. Questa opzione non è selezionata per impostazione predefinita. Applicabile per macOS 10.13 e versioni successive.
(Solo macOS) Minuti al mancato reset di accesso SmartLock	Specificare i minuti prima che il login venga ripristinato dopo il raggiungimento del numero massimo di tentativi di accesso non riusciti. Assicurarsi che il numero Massimo di tentativi non riusciti sia impostato per abilitare questo campo. Disponibile in macOS 10.10 e versione successiva. **Per dispositivi Android 5.0 ad eccezione dei profili di lavoro Android enterprise:** **Per Android 6.0 o versione successiva:** consente o non consente a un utente di scegliere la funzionalità SmartLock per sbloccare un dispositivo. La funzionalità SmartLock consente di sbloccare automaticamente un dispositivo in determinate circostanze, tra cui la vicinanza dell'utente al dispositivo, il dispositivo in una posizione, o quando il dispositivo viene associato a un dispositivo attendibile.
Sblocco tramite impronta digitale	**Per dispositivi Android 5.0 ad eccezione dei profili di lavoro Android enterprise:** **Per Android 6.0 o versione successiva:** Consente o non consente all'utente di scegliere Impronta digitale per sbloccare un dispositivo.
Notifiche della schermata di blocco (solo per Android enterprise)	**Attiva le notifiche per i dispositivi di lavoro gestiti (per il proprietario del dispositivo)** Consente o impedisce la visualizzazione delle notifiche sulla schermata di blocco sui dispositivi di lavoro gestiti **Attiva le notifiche non revisionate per il profilo di lavoro** **Per Android 6.0 o versione successiva:** Consente o impedisce la visualizzazione di notifiche non revisionate sulla schermata di blocco sui dispositivi con profilo di lavoro. Dopo aver attivato questa impostazione, si riceverà la notifica ma il contenuto verrà mostrato come

Impostazione	Operazione da eseguire
	"nascosto dalla policy". È possibile visualizzare il contenuto (notifica push/e-mail) esclusivamente dall'app.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.4.52. Preferenze di privacy (macOS)

Applicabile a: macOS 10.14 o versioni successive supportate.

Configurare le applicazioni che possono ottenere l'accesso ai servizi, ai file e alle risorse del sistema. Questa configurazione controlla le impostazioni su un dispositivo macOS in Preferenze di sistema > Sicurezza e privacy > Privacy.

Creazione di una configurazione di Preferenze di privacy

Procedure

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **privacy** nel campo di ricerca, quindi fare clic sulla configurazione **Preferenze di privacy**.
4. Assegnare un nome e una descrizione alla configurazione.
5. Passare a una delle applicazioni elencate nella pagina. Per informazioni correlate, consultare la **documentazione Apple**.
    1. Per macOS 10.14 e versioni successive, le applicazioni e le impostazioni disponibili per la configurazione includono:
        - Accessibilità: consente di specificare le policy dell'app tramite il sottosistema Accessibilità.
        - Rubrica: consente di specificare le policy per le informazioni di contatto gestite dall'app Contatti.
        - Eventi Apple: consente di specificare le policy dell'app per l'invio di eventi Apple limitati a un altro processo.
        - Calendario: consente di specificare le policy per informazioni del calendario gestite dall'app Calendario.
        - Fotocamera: la fotocamera del sistema. L'accesso alla fotocamera non può essere fornito in un profilo, può solo essere negato.
        - Microfono: il microfono del sistema. L'accesso al microfono non può essere fornito in un profilo, può solo essere negato.
        - Foto: le immagini gestite dall'app Foto in ~/Pictures/.photoslibrary.
        - Pubblica evento: consente di specificare le policy dell'applicazione per l'uso di API CoreGraphics allo scopo di inviare eventi CG al flusso di eventi del sistema.
        - Promemoria: consente di specificare le policy per informazioni di promemoria gestite dall'app Calendario.
        - Policy sistema (tutti i file): consente all'applicazione di accedere a tutti i file protetti, inclusi i file di amministrazione del sistema.
        - Policy sistema (file di amministrazione): consente all'applicazione di accedere ad alcuni file utilizzati per l'amministrazione del sistema.
    2. Per macOS 10.15 e versioni successive, le applicazioni e le impostazioni disponibili per la configurazione includono:
        - Utilizzo file: consente di sapere quando l'utente sta utilizzando file gestiti da un'applicazione Provider di file.
        - Ascolta eventi da tutti i processi: consente all'applicazione di utilizzare API CoreGraphics e HID per ascoltare (ricevere) eventi CG e HID da tutti i processi. L'accesso a questi eventi non può essere fornito in un profilo, può solo essere negato. Deselezionare l'opzione Consentito.
        - Accedi a libreria multimediale: consente all'applicazione di accedere ad Apple Music, ad attività di musica e video e alla libreria multimediale.
        - Acquisizione dello schermo di sistema: consente all'applicazione di acquisire (leggere) i contenuti di visualizzazione del sistema. L'accesso ai contenuti non può essere fornito in un profilo, può solo essere negato. Deselezionare l'opzione Consentito.

- Riconosci dati riconoscimento vocale e inviali ad Apple: consente all'applicazione di utilizzare la funzione di riconoscimento vocale del sistema e di inviare i dati vocali ad Apple.
- Accedi ai file nella cartella Desktop dell'utente: consente all'applicazione di accedere ai file nella cartella Desktop dell'utente.
- Accedi ai file nella cartella Documenti dell'utente: consente all'applicazione di accedere ai file nella cartella Documenti dell'utente.
- Accedi ai file nella cartella Download dell'utente: consente all'applicazione di accedere ai file nella cartella Download dell'utente.
- Accedi ai file nei volumi di rete: consente all'applicazione di accedere ai file nei volumi di rete.
- Accedi ai file nei volumi rimovibili: consente all'applicazione di accedere ai file nei volumi rimovibili.

6. Per ogni applicazione che si desidera configurare, fare clic su **Azioni > Aggiungi**.
7. Immettere i valori per le chiavi del dizionario di identità seguenti:
   - Identificatore - Nome delle impostazioni. Ad esempio: "us.zoom.ZoomPresence".
   - Tipo di identificatore: selezionare l'ID bundle o il percorso. Ad esempio: "ID bundle".
   - Requisito codice: specificare il valore per l'ID bundle o il percorso. Ad esempio: "identificatore us.zoom.ZoomPresence e ancoraggio Apple generico".
   - Codice statico (vero o falso)
   - Consentito (vero o falso)
   - Commento
8. Fare clic su **Salva**.
9. (Facoltativo) In un'applicazione, fare clic su **Azioni > Elimina** per rimuovere le impostazioni di preferenza della privacy esistenti.
10. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
11. Fare clic su **Fine**.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.4.53. Configurazione della privacy

Una configurazione della privacy definisce se:

- i dati di localizzazione sono raccolti sul dispositivo e inviati al sistema di gestione del dispositivo
- Se gli amministratori sono autorizzati a cancellare il dispositivo
- Se l'inventario delle app viene raccolto per tutte le applicazioni o solo per quelle contenute nel Catalogo app

Impostazioni sulla privacy

> La cancellazione dei dati del dispositivo e la raccolta dei dati per l'inventario di tutte le app sul dispositivo non è applicabile ai dispositivi registrati in User Enrolled.

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Raccogli dati sulla posizione	Selezionare questa opzione per abilitare la raccolta dei dati sulla posizione. Visualizzare la posizione del dispositivo nella pagina **Dispositivi**. • Per i dispositivi iOS, la posizione visualizzata per un dispositivo è basata esclusivamente sulla posizione di rete. • P er i dispositivi Android, la posizione è basata sia sulla posizione di rete sia su quella del GPS (se disponibile). • Per i dispositivi Windows, la posizione si basa sui valori di latitudine e longitudine ottenuti durante un check-in del dispositivo. Quando la raccolta di dati sulla posizione è abilitata su un dispositivo, la posizione attuale viene aggiornata ogni 4 ore. I dati sulla posizione vengono rimossi dal sistema di gestione dei dispositivi quando questo non viene più utilizzato o quando la configurazione della privacy viene disabilitata o rimossa. Gli utenti dei dispositivi possono **disattivare la raccolta di dati sulla posizione sul dispositivo**.
Disabilita operazione di cancellazione dispositivo	Selezionare questa opzione per impedire agli amministratori di cancellare il dispositivo. Valutare la possibilità di selezionare questa opzione per i dispositivi di proprietà dell'utente (ovvero del dipendente).
Richiedi all'utente di attivare i servizi di localizzazione	Selezionare per consentire agli utenti di abilitare o meno l'uso dei servizi di localizzazione, compresa la localizzazione dei dispositivi, del Wi-Fi e dell'MTD, come necessario. Nel caso di dispositivi completamente gestiti, questo può essere concesso automaticamente se l'amministratore sceglie di disabilitare l'opzione.
Raccogli inventario app	Selezionare **Raccogli inventario app** per raccogliere informazioni su tutte le app installate sul dispositivo, indipendentemente dal fatto che un'app sia presente nel catalogo delle app. Selezionare **Per app sul dispositivo che fanno parte del catalogo app** per raccogliere informazioni sulle app installate sul dispositivo solo se presenti nel catalogo app. Selezionare **Per tutte le app sul dispositivo** per raccogliere informazioni su tutte le app sul dispositivo. Questa opzione è applicabile ai dispositivi Windows 10 e versioni successive. Gli inventari di tipo origine app seguenti sono visualizzati e selezionati per impostazione predefinita. • **Abilita inventario non App Store** - per app interne (app universali) inviate tramite MDM o installate dall'utente finale direttamente sul dispositivo aprendo manualmente l'app e installandola localmente. • **Abilita inventario App Store** - per le app installate da Microsoft Store manualmente o tramite Apps@Work. • **Abilita inventario sistema** - per le app riportate come pre-installate insieme al sistema operativo Windows 10 da Microsoft. • **Abilita inventario Win32** - per le app basate sul sistema 32, come le app MSI, EXE, Win32 Store e così via, che vengono installate tramite MDM o installate direttamente

Impostazione	Operazione da eseguire
	sul dispositivo dall'utente finale. È possibile selezionare in maniera facoltativa solo quegli inventari di tipo origine delle app per raccogliere informazioni su app selettive. Le app installate da MDM appaiono nell'Inventario app, anche se non si seleziona l'Inventario app non App Store o Win32. L'inventario.EXEs viene raccolto anche quando la configurazione della privacy utilizza la configurazione predefinita per raccogliere l'Inventario app solo per Catalogo app. L'inventario deve essere raccolto in modo coerente per tutte le app quando si raccoglie solo per le app del Catalogo app. L'inventario delle app Modern, MSI ed EXE disponibili nel Catalogo app viene estratto solo quando viene distribuita almeno un'app appartenente a ciascuna di queste varianti.
Impostazioni per dispositivi Android Enterprise (7.0+) Configurare le impostazioni riportate di seguito per impostare le norme sulla privacy sui dispositivi Android Enterprise.	
Nome organizzazione	Immettere il nome dell'organizzazione che gestisce il dispositivo.
Colore organizzazione	Selezionare il colore dell'organizzazione, che deve essere visualizzato sullo sfondo dello schermo dell'utente.
Messaggio breve	Inserire un breve messaggio da visualizzare quando l'utente tenta di utilizzare una funzione bloccata dall'amministratore.
Messaggio lungo	Immettere il messaggio lungo da visualizzare quando l'utente fa clic sul messaggio breve. Questo messaggio fornisce ulteriori informazioni sulle restrizioni applicate all'utente.
Tenere nascoste le schermate dell'app Go	Selezionare Vero o Falso dall'elenco. • **Vero** - Durante la condivisione remota, le schermate dell'app Ivanti Go non saranno visibili. • **Falso** - Durante la condivisione remota, le schermate dell'app Ivanti Go saranno visibili per l'assistenza alla risoluzione dei problemi e per la consultazione della documentazione.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.4.54. Informazioni relative all'informativa sulla privacy del client

Applicabile a: dispositivi Android, Android Enterprise e iOS o versioni più recenti supportate.

Configurazione per la distribuzione delle informazioni relative alla policy sulla privacy agli utenti dei client Go. Questa è una configurazione definita dal sistema, che può essere modificata solo per configurare le impostazioni di distribuzione.

Le informazioni mostrate all'utente includono i dettagli configurati nell'ambito delle configurazioni seguenti:

- Privacy
  - Raccolta dati sulla posizione
  - Raccolta inventario app
  - Android 7.0 e versioni successive:
    - Nome organizzazione
    - Colore organizzazione
    - Messaggio breve
    - Messaggio lungo
- Privacy client
  - SLC - Riattivazione periodica del dispositivo in caso di modifica significativa della posizione
  - Intervallo minimo di riattivazioni in base alla posizione
  - Abilita lo stato Mixpanel
- Mobile Device Management - Diritti di accesso MDM (non applicabile ai dispositivi registrati dall'utente)
  - Blocco dispositivo e rimozione passcode
  - Cancellazione dispositivo
  - Informazioni rete (numeri di telefono/SIM, indirizzi MAC)

10.10.4.55. Impostazioni client Ivanti Go

Configurare la raccolta di dati anonimi dell'utente finale, comprese le informazioni sul dispositivo e sull'utilizzo, per aiutare a identificare i problemi del prodotto e garantire un'elevata qualità del servizio. Questa impostazione abilita anche le opzioni di configurazione dei contatti di assistenza.

Creazione di una configurazione Impostazioni client Ivanti Go

Applicabile a:

- Mobile@Work per macOS 1.67 o versioni successive supportate.
- Go per iOS 3.5.0 o versioni successive supportate.
- Mobile@Work per Android 12.9.0.0 o versioni più recenti supportate.
- Scegliere Android 124 o versioni più recenti supportate.

Procedura

1. Accedere a **Configurazioni** > **Aggiungi configurazione** > **Impostazioni client Ivanti Go**. Viene visualizzata la pagina **Crea configurazione impostazioni client Ivanti Go**.
2. Immettere un nome per la configurazione nella casella **Nome**.
3. Immettere una **Descrizione** per la configurazione.
4. In **Riattivazioni in base alla posizione**, selezionare l'opzione **Abilita SLC**. Il servizio di posizione con modifica significativa offre un'alternativa che richiede meno alimentazione per fornire aggiornamenti sulla posizione a Go per l'app iOS solo quando la posizione dell'utente cambia in modo significativo, dopo un periodo minimo di 15 minuti (intervallo predefinito). Se questo servizio è attivato, al momento del cambiamento di posizione l'app Go si riattiva in background ed effettua il check-in.
5. In **Raccolta dati tramite Analisi per i clienti**, selezionare l'opzione **Abilita Analisi** se è stata disattivata. Di default questa opzione è abilitata.
6. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
7. Fare clic su **Fine**.

Configura impostazione per la scheda Supporto

Applicabile a:

- Mobile@Work per macOS 1.67 o versioni successive supportate.
- Go per iOS 3.5.0 o versioni successive supportate.
- Mobile@Work per Android 12.9.0.0 o versioni più recenti supportate.
- Scegliere Android 124 o versioni più recenti supportate.

Procedura

1. Accedere a **Configurazioni** > **Aggiungi configurazione** > **Impostazioni client Ivanti Go**. Viene visualizzata la pagina **Crea configurazione impostazioni client Ivanti Go**.
2. Immettere un nome per la configurazione nella casella **Nome**.
3. Immettere una **Descrizione** per la configurazione.
4. Sotto l'opzione **Piattaforma**, selezionare la piattaforma corrispondente.

5. Nella sezione **Configura impostazione per la scheda supporto**, fare clic su **Abilita scheda supporto**.

> Il campo **Abilita scheda Assistenza** è applicabile solo per i dispositivi iOS.

> È possibile abilitare la scheda **Supporto** da Go per iOS versione 118.0.0 o superiore e da Go per Android versione 124 o superiore. I dispositivi con versioni precedenti non visualizzano né supportano questa funzione.

Nella sezione **Configurazione contatto di supporto**, fornire i seguenti dettagli:

- **Nome scheda** - Inserire il nome della scheda visualizzata nella navigazione dell'app Ivanti. Il valore predefinito è 'Supporto'. (Lunghezza massima: 10 caratteri)
- **Istruzioni per l'utente finale** - Inserire le istruzioni per l'utilizzo dei contatti di supporto. (Lunghezza massima: 40 caratteri)
- **Aggiungi contatti** - Fare clic su **+Aggiungi** per aggiungere i contatti. (Contatti max: 5)
  - **Nome** - Inserire il nome del contatto. (Lunghezza massima: 20 caratteri)
  - **Numero di telefono** - Inserire un numero di telefono valido. (Con prefisso internazionale)
- **Aggiungi URL** - Fare clic su **+Aggiungi** per aggiungere gli URL. (URL max: 5)
  - **Nome URL** - Inserire il nome URL. (Lunghezza massima: 20 caratteri)
  - **URL** - Inserire un URL valido.
- **Informazioni aggiuntive** - Inserire qui eventuali messaggi aggiuntivi relativi al supporto che si desidera visualizzare. (Lunghezza massima: 120 caratteri)
- **Indirizzo e-mail** - Immettere l'e-mail a cui inviare le e-mail di supporto. (Lunghezza massima: 40 caratteri)

  > È necessario inserire un indirizzo e-mail valido nel formato alias@nomedominio.com.

- **URL del sistema di ticketing di supporto** - Aggiungere un pulsante "**Genera un ticket di supporto**" alla scheda **Supporto** nell'app **Ivanti Go per iOS** e nell'app **Ivanti Go for Android**. Abilitare il selettore per visualizzare il pulsante nella scheda Supporto e immettere l'URL appropriato nel campo fornito per reindirizzare gli utenti al sistema di supporto.

  > Questo URL viene utilizzato nella scheda **Supporto** Ivanti Go per reindirizzare gli utenti al sistema di supporto designato. Per una maggiore protezione, si consiglia di utilizzare URL che inizino con *https://* anziché *http://*.

Fare clic su **Avanti** per configurare le impostazioni di distribuzione.

8. Fare clic su **Fine**.

Per ulteriori informazioni, consultare **Configurazioni**.

10.10.4.56. Impostazioni Siri

Utilizzare le **Impostazioni Siri** per configurare le impostazioni Siri sui dispositivi supervisionati. Questa configurazione aiuta gli amministratori ad applicare controlli coerenti basati su criteri che gestiscono il modo in cui i dispositivi accedono e utilizzano le funzionalità Siri.

Applicabile a:

- iOS 26.4+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.
- macOS 26.4+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.
- watchOS 26.4+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.
- visionOS 26.4+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.
- tvOS 27+ supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Impostazioni Siri**.
3. Configurare le **Impostazioni Siri** come da tabella seguente:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Attivato	Selezionare la casella di controllo per abilitare Siri. Utilizzare il pulsante **Esegui push al dispositivo** per attivare Siri su dispositivi supervisionati.
Consenti Siri IA	Seleziona la casella di controllo per abilitare le funzionalità specifiche di **Siri IA**. Attiva/disattiva il pulsante **Esegui push al dispositivo** per abilitare le funzionalità specifiche di **Siri IA** sui dispositivi supervisionati.
Consenti contenuto generato dall'utente	Selezionare la casella di controllo per abilitare il contenuto generato dall'utente. Utilizzare il pulsante **Esegui push al dispositivo** per attivare il contenuto generato dall'utente sui dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi macOS e visionOS.
Consenti durante il blocco	Selezionare la casella di controllo per abilitare Mentre bloccato. Utilizzare il pulsante **Esegui push al dispositivo** per attivare Mentre bloccato sui dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi macOS e visionOS.
Imponi filtro profanità	Selezionare la casella di controllo per abilitare Imponi filtro profanità. Utilizzare il pulsante **Esegui push al dispositivo** per attivare Imponi filtro profanità sui dispositivi supervisionati. Questa impostazione non è applicabile ai dispositivi visionOS.
Imponi la riduzione dei contenuti sensibili	Selezionare la casella di controllo per forzare Siri a ridurre i contenuti sensibili. Attivare il pulsante **Esegui push al dispositivo** per forzare Siri a ridurre il contenuto sensibile sui dispositivi supervisionati.

4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
5. Selezionare una delle opzioni di distribuzione per impostare la configurazione di **Impostazioni Siri**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere Utilizzo delle configurazioni.
6. Fare clic su **Fine**.

10.10.4.57. Configurazione servizi Configurazione file

Gli amministratori della configurazione **File di configurazione servizi** per gestire e distribuire centralmente i file di configurazione per vari servizi di sistema sui dispositivi registrati. Inoltre, gli amministratori possono garantire che le impostazioni dei servizi rimangano coerenti e resistenti a modifiche non autorizzate, consegnando i file a directory sicure e specifiche per il servizio in un ambiente a prova di manomissione.

Applicabile a: dispositivi macOS

Prima di iniziare:

- È possibile caricare varie configurazioni in un formato file *ZIP*. Per maggiori informazioni sull'aggiunta di un file, vedere **File**.
- Tutti i file nell'archivio espanso sono impostati alle autorizzazioni file *-r–r–r– unix*. Qualsiasi collegamento presente nell'archivio sarà limitato ai file di riferimento all'interno della posizione specifica del servizio.
- I file nell'archivio zip devono rispecchiare la struttura delle cartelle e i file di configurazione che il servizio si aspetta di trovare nella directory principale del file system. Il servizio utilizza solo i file forniti dalla dichiarazione e ignora quelli presenti nelle directory predefinite.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **File configurazione servizio**.
3. Configurare le impostazioni **File configurazione servizio** in base alla tabella seguente:

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Seleziona file	Inserire il nome del file.
Scegli tipo di servizio	Selezionare uno dei **tipi di servizio** dall'elenco a discesa: • SSHD • SUDO • PAM • CUPS • HTTP_D • BASH • ZSH

4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
5. Selezionare una delle opzioni di distribuzione per impostare la configurazione **File configurazione servizio**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere **Utilizzo delle configurazioni**.
6. Fare clic su **Fine**.

10.10.4.58. Aggiornamenti software

Applicabile a:

- Dispositivi supervisionati iOS 10.3 fino a 26.0 e tvOS 12.0 fino a 26.0
- dispositivi macOS
- Dispositivi Windows 10 e versioni successive

Creare e distribuire le regole per gli aggiornamenti del sistema operativo.

Argomenti della sezione:

- **Configurazione di aggiornamenti software per dispositivi iOS/tvOS**
- **Configurazione di aggiornamenti software per dispositivi macOS Non-DEP e DEP**
- **Configurazione di aggiornamenti software per dispositivi Windows**
- **Imposizione degli aggiornamenti software tramite la gestione dichiarativa dei dispositivi**

Configurazione di aggiornamenti software per dispositivi iOS/tvOS

Procedura

Per consentire l'invio degli aggiornamenti del sistema operativo ai dispositivi iOS/tvOS se sono in modalità di supervisione, procedere come segue:

1. Accedere a **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Fare clic su **Aggiornamenti software**.
4. Fare clic su **iOS/tvOS** per visualizzare la sezione Impostazioni configurazione.
5. Selezionare l'opzione **Consente di installare automaticamente gli aggiornamenti del sistema operativo nei dispositivi supervisionati**.
6. Selezionare una delle seguenti opzioni:
    - Aggiorna all'ultima versione
    - Aggiorna a una versione specifica - Ad esempio, immettere iOS versione numero 11.3.0.
7. Selezionare una delle seguenti azioni di installazione:
    - Predefinito
    - Solo download
    - Installa il prima possibile
8. Selezionare le seguenti opzioni di orario per l'esecuzione degli aggiornamenti:
    - Ora di inizio
    - Ora di fine
    - Fuso orario
9. Fare clic su **Avanti**.
10. Selezionare l'opzione **Abilita questa configurazione**.

11. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato
12. Fare clic su **Fine**.

- Quando si installa una versione specifica di aggiornamento del sistema operativo per i dispositivi iOS, è necessario selezionare una versione disponibile per il dispositivo. Se si seleziona una versione non valida o non disponibile, l'aggiornamento del software del dispositivo verrà ignorato.
- Se il dispositivo ha un passcode, dopo che MDM avrà inviato l'aggiornamento al dispositivo, quest'ultimo mette in coda l'aggiornamento e all'utente viene richiesto di inserire il passcode per avviare l'installazione.
- Abilitare `enforcedSoftwareUpdateDelay` in **Restrizioni iOS** per assicurarsi che la scansione manuale sui dispositivi per gli aggiornamenti software non elimini le versioni specifiche scaricate da questa configurazione.

Configurazione di aggiornamenti software per dispositivi macOS Non-DEP e DEP

Il profilo Registrazione dispositivi, parte di Apple Business Manager, consente ai clienti di acquistare dispositivi in blocco e di registrare automaticamente tali dispositivi in MDM durante l'attivazione. Per ulteriori informazioni, vedere **Registrazione dispositivo**.

La seguente procedura aiuta a inviare gli aggiornamenti del sistema operativo ai dispositivi macOS Non-DEP e DEP.

Procedura

1. Accedere a **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Fare clic su **Aggiornamenti software**.
4. Fare clic su **macOS** per visualizzare la sezione Impostazioni configurazione.
5. Selezionare l'opzione **Abilita aggiornamenti software macOS**.
6. Selezionare il tipo di aggiornamenti per il dispositivo. Per ogni tipo è possibile anche selezionare gli aggiornamenti che non richiedono il riavvio.
    - Aggiornamenti del sistema operativo
    - Aggiornamenti critici
    - Aggiornamenti dati di configurazione
    - Aggiornamento del Firmware
    - Aggiornamenti non critici

    > L'amministratore può gestire (installazione/programmazione) gli aggiornamenti macOS non critici, attivando l'opzione **Attiva aggiornamenti non critici**. Questa opzione è disattivata per impostazione predefinita per i tenant esistenti e deve essere attivata da un amministratore in modo esplicito dopo l'aggiornamento, se necessario.

    > In **Aggiornamenti del sistema operativo**, gli amministratori possono aggiornare il dispositivo a una versione specifica di macOS.

> È possibile configurare tutti gli aggiornamenti macOS con azioni come segue:

- Predefinito
- Solo notifica
- Installa in seguito
- Installa con riavvio forzato
- Solo download
- Installa il prima possibile

Valori possibili - Basso, Alto

Predefinita - Bassa

Priorità

- N. massimo differimenti dell'utente
  Valore possibile - Numero intero
  È supportato solo quando è selezionata l'opzione Installa più tardi.

7. Selezionare le seguenti opzioni di orario per l'esecuzione degli aggiornamenti:
   - Ora di inizio
   - Ora di fine
   - Fuso orario
8. Fare clic su **Avanti**.
9. Selezionare l'opzione **Abilita questa configurazione**.
10. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato
11. Fare clic su **Fine**.

Configurazione di aggiornamenti software per dispositivi Windows

Procedura

Per configurare la pianificazione degli aggiornamenti dell'installazione di Windows:

1. Accedere a **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Fare clic su **Aggiornamenti software**.
4. Fare clic su **Windows** per visualizzare la sezione Impostazioni configurazione.
5. Immettere le seguenti opzioni a seconda della versione dei dispositivi Windows posseduti.
6. Fare clic su **Avanti**.
7. Selezionare l'opzione **Abilita questa configurazione**.

8. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato

Fare clic su **Fine**.

Aggiornamenti software per dispositivi Windows 10 e versioni successive

- Origini aggiornamenti: selezionare una delle seguenti origini:
    - WSUS aziendale
    - Microsoft Update e/o WSUS aziendale

Origine aggiornamento driver

- Origine aggiornamento funzionalità
- Altra origine aggiornamento
- Origine aggiornamento qualità
- URL al server WSUS aziendale
- Server di aggiornamento Microsoft intranet alternativo
- Consenti aggiornamenti da "Autori attendibili": consente di limitare le origini degli aggiornamenti solo agli autori attendibili.
- Strategia di aggiornamento automatico: selezionare una delle opzioni dal menu a discesa.
- Giorno di installazione pianificato: impostare la frequenza degli aggiornamenti.
- Ora di installazione pianificata: selezionare un'ora di installazione per gli aggiornamenti.
- Consenti di scaricare gli aggiornamenti in automatico su connessioni a consumo: attivare o disattivare l'opzione.
- Non consentire alle policy di differimento degli aggiornamenti di avviare scansioni di Windows Update: attivare o disattivare l'opzione.
- Scadenza di riavvio in caso di Occupato: selezionare il numero di giorni alla scadenza di riavvio.
- Posponi scadenza di riavvio in caso di Occupato: selezionare il numero di giorni per posporre la scadenza di riavvio in caso di Occupato.
- Pianificazione di transizione di riavvio in caso di Occupato: selezionare il numero di giorni per la pianificazione della transizione di riavvio.
- Aggiorna/Riempi URL senza contenuto.
- Limite di download MO per app: selezionare una delle seguenti opzioni:
    - Non ignorare il limite di download MO per le app e i relativi aggiornamenti
    - Ignora limite di download MO (consenti download illimitato) per le app e i relativi aggiornamenti
- Limite di download MO per aggiornamenti: selezionare una delle seguenti opzioni:
    - Non ignorare il limite di download MO per gli aggiornamenti del sistema operativo
    - Ignora limite di download MO (consenti download illimitato) per gli aggiornamenti del sistema operativo
- Gestisci build di anteprima: selezionare una delle seguenti opzioni:
    - Disattiva build di anteprima

    - Disattiva build di anteprima quando viene resa pubblica la versione successiva
    - Attiva build di anteprima
- Pianificazione delle notifiche di avviso di riavvio automatico per gli aggiornamenti: selezionare i minuti per la notifica di avvertimento di riavvio automatico.
- Promemoria avviso di riavvio: selezionare le ore per impostare il promemoria avviso di riavvio.
- Pianificazione di aggiornamento automatico: selezionare la frequenza degli aggiornamenti automatici.
- Notifica di riavvio automatico per gli aggiornamenti: attivare la notifica di riavvio automatico per gli aggiornamenti.
- Versione prodotto - Immettere la versione del prodotto come elencata nella pagina della versione di Windows Update (URL: aka.ms/WindowsTargetVersioninfo). Ad esempio, "Windows 11" o "11" o "Windows 10".
- Versione release destinazione - Immettere la versione della release di destinazione nella pagina della versione di Windows Update.
- Avvio nelle ore attive - Se si attiva questa opzione, un PC non si riavvia automaticamente dopo gli aggiornamenti durante le ore attive. Al di fuori delle ore attive, il PC tenterà di riavviarsi.
- Fine nelle ore attive - Se si attiva questa opzione, il PC non si riavvia automaticamente dopo gli aggiornamenti durante le ore attive. Al di fuori delle ore attive, un PC tenterà di riavviarsi.
- Intervallo massimo ore attive - Attivare questa opzione per indicare il numero massimo di ore dall'ora di inizio in cui gli utenti possono impostare le loro ore attive.
- Nessuna notifica di aggiornamento durante le ore attive - Le opzioni di notifica degli aggiornamenti sono riportate di seguito.
    - Notifiche predefinite di Windows Update
    - Disattiva tutte le notifiche eccetto gli avvisi di riavvio
    - Disattiva tutte le notifiche inclusi gli avvisi di riavvio
- Disabilita aggiornamenti per i driver - Attivare questa opzione per escludere i driver con aggiornamenti di qualità di Windows. Se si disattiva o non si configura questa opzione, Windows Update includerà gli aggiornamenti con una classificazione dei driver.
- Scadenza aggiornamenti di qualità - Il numero di giorni prima dell'installazione automatica degli aggiornamenti di qualità sui dispositivi è indipendente dalle ore di attività.
- Periodo di tolleranza scadenza aggiornamenti di qualità - Il numero minimo di giorni dall'installazione dell'aggiornamento fino al riavvio automatico degli aggiornamenti di qualità.
- Periodo di tolleranza scadenza aggiornamenti delle funzioni - Il numero di giorni prima della distribuzione automatica degli aggiornamenti delle funzioni sui dispositivi, indipendentemente dalle ore di attività.
- Periodo di tolleranza scadenza aggiornamenti delle funzioni - Il numero minimo di giorni prima della distribuzione automatica degli aggiornamenti delle funzioni sui dispositivi, indipendentemente dalle ore di attività.
- Non riavviare automaticamente fino alla fine del periodo di tolleranza - Se abilitato, i dispositivi non si riavvieranno automaticamente al di fuori delle ore di attività finché non saranno trascorsi la scadenza e il periodo di tolleranza, anche se un aggiornamento è pronto per il riavvio. Quando è disattivato, è possibile tentare un riavvio automatico al di fuori dell'orario attivo se l'aggiornamento è disponibile per il riavvio prima della scadenza.

Aggiornamenti software per dispositivi precedenti a Windows 10.0.14393

Nei dispositivi in cui la funzione di restrizione della telemetria è disattivata, le impostazioni seguenti non funzionano:

- Sospendi aggiornamento/aggiornamenti: attivare per ritardare le modifiche a una data successiva
- Rimanda aggiornamenti per: scegliere di ritardare fino a 4 settimane

- Rimanda aggiornamenti: attivare per rimandare gli aggiornamenti
- Rimanda aggiornamenti per: scegliere di ritardare fino a 8 mesi

Aggiornamenti software per dispositivi Windows 10.0.14393 e versioni successive

- Ramo da cui installare gli aggiornamenti - Consente all'amministratore IT di impostare il ramo da cui un dispositivo riceve gli aggiornamenti. Il ramo per installare gli aggiornamenti dal campo contiene le seguenti opzioni:
  - Windows Insider build - Veloce
  - Windows Insider build - Lenta
  - Rilascia Windows Insider build
  - Canale semestrale (mirato)
  - Canale semestrale
  - Rilascia anteprima dei soli aggiornamenti di qualità
  - Canary Channel

Aggiornamenti delle funzionalità (upgrade) - Supportati solo in Windows Professional, Windows Enterprise e Windows Education.

  - Sospendi aggiornamenti
  - Rimanda di: scegliere di ritardare fino a 180 giorni.

Aggiornamenti di qualità (aggiornamenti) - Supportati solo in Windows Professional, Windows Enterprise e Windows Education.

  - Sospendi aggiornamenti
  - Rimanda di: scegliere di ritardare fino a 30 giorni.

Aggiornamenti software per dispositivi Windows 10.0.17083 e versioni successive

- Aggiornamenti delle funzionalità:
  - Periodo di disinstallazione degli aggiornamenti delle funzionalità: selezionare il numero di giorni per la disinstallazione di un aggiornamento della funzione.

Aggiornamenti software per dispositivi Windows 10.0.17763 e versioni successive

- Disattiva l'accesso a "Sospendi aggiornamenti" per gli utenti
- Disattiva l'accesso UXWU degli utenti (analisi, download e installazione di Windows Update)
- Livello di notifica degli aggiornamenti: selezionare una delle seguenti opzioni:
  - Usa le notifiche predefinite di Windows Update
  - Disattiva tutte le notifiche eccetto gli avvisi di riavvio
  - Disattiva tutte le notifiche inclusi gli avvisi di riavvio
- Aggiornamenti delle funzionalità:
  - Scadenza prima del riavvio automatico per l'installazione dell'aggiornamento: selezionare il numero di giorni per la scadenza prima del riavvio automatico per l'installazione dell'aggiornamento.
  - Scadenza di riavvio in caso di Occupato: selezionare il numero di giorni per la scadenza di riavvio in caso di Occupato.
  - Posponi scadenza di riavvio in caso di Occupato: selezionare il numero di giorni per posporre la scadenza di riavvio in caso di Occupato.

- Pianificazione di transizione di riavvio in caso di Occupato: selezionare il numero di giorni per la pianificazione della transizione di riavvio.

Imposizione aggiornamenti software tramite DDM

L'amministratore può imporre l'installazione degli aggiornamenti software sui dispositivi iOS, macOS e iPadOS utilizzando la DDM.

Supportato su:

- iOS 17+
- iPadOS 17+
- macOS 14+

Procedura

1. Creare una configurazione **Imposizione aggiornamento software** dalla sezione Configurazioni.
2. Eseguire Imponi check-in per assicurarsi che la configurazione Imposizione aggiornamento software sia installata sul dispositivo.

Quando si apre il dispositivo, dovrebbe apparire una notifica relativa agli aggiornamenti software richiesti con dettagli quali il numero di versione, la data di richiesta, ecc.

> Se non si desidera imporre l'aggiornamento software, è necessario impostare l'opzione di distribuzione della configurazione su **Nessuna**.

Distribuzione dei predicati per una configurazione di applicazione dell'aggiornamento software

1. Creare la configurazione dell'imposizione dell'aggiornamento software.
2. Impostare l'interruttore "Attivazione con predicati" su ON e utilizzare i pulsanti + per includere i predicati (se necessario).



Per modificare o eliminare un predicato, andare in **Amministratore** > **Apple** > **Predicati**. L'elenco dei predicati disponibili è riportato in questa pagina. Fare clic su **Modifica** per apportare le modifiche al predicato esistente e salvarlo. Allo stesso modo, per eliminare un predicato esistente, selezionare il predicato e fare clic su **Elimina**.

> Non è possibile eliminare un predicato se è associato a una configurazione.

10.10.4.59. Configurazione impostazioni aggiornamento software

consente la creazione di impostazioni di imposizione dell'aggiornamento software e definisce il comportamento degli aggiornamenti per l'utente finale per quanto riguarda la cadenza e i rinvii.

Applicabile a:

- iOS 18.0 supervisionato fino alla versione rilasciata più recente supportata da .
- macOS 15.0 supervisionato fino alla versione rilasciata più recente supportata da .

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Impostazioni aggiornamento software**.
3. Configurare le **Impostazioni di aggiornamento software** come da tabella seguente:

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
iOS 18+ supervisionato e **macOS15+** Registrazione alla beta	
Registrazione al programma (facoltativa)	Selezionare una delle seguenti opzioni: • **Consentito**: l'utente può registrarsi a tutti i programmi beta applicabili associati al proprio account Apple. • **Sempre attivo**: vengono utilizzati i programmi beta specificati dall'organizzazione e l'utente non è in grado di registrarsi a un programma beta utilizzando il proprio account Apple. **Offri programma** - Con Offri programma è possibile far rispettare un programma obbligatorio. Durante l'applicazione, è possibile impostare le versioni richieste per i dispositivi iOS e macOS. **Richiedi programma** - Il dispositivo si registra automaticamente a questo programma beta. • **Sempre spento**: il dispositivo non può registrarsi a nessun programma beta. Il sistema rimuove il dispositivo da qualsiasi programma beta, se già registrato.
iOS 18+ Supervisionato e **macOS15+ Supervisionato**	
Notifiche	Selezionare le caselle di controllo **Notifiche** e **Mostra tutte le notifiche di imposizione degli aggiornamenti software** per visualizzare tutte le notifiche di imposizione degli aggiornamenti software nel dispositivo dell'utente. Se si seleziona solo la casella di controllo **Notifiche**, il dispositivo visualizzerà una singola notifica di imposizione un'ora prima del termine di imposizione. Se non si seleziona nessuna delle caselle di controllo, il dispositivo visualizza le notifiche attivate per visualizzare tutte le notifiche di imposizione degli aggiornamenti software nel dispositivo dell'utente.
Azioni automatiche	
Scarica	Selezionare una delle seguenti opzioni: • **Consentito**: l'utente può attivare o disattivare il download automatico. • **Sempre attivo**: i download automatici sono sempre attivi per l'utente. • **Sempre disattivo**: i download automatici sono sempre disattivi per l'utente.
Installa aggiornamenti OS	Selezionare una delle seguenti opzioni: • **Consentito**: l'utente può attivare o disattivare l'installazione automatica degli aggiornamenti del sistema operativo. • **Sempre attivo**: l'installazione automatica degli aggiornamenti del sistema operativo è sempre attiva per l'utente.

Impostazione	Descrizione
	• **Sempre disattivo**: l'installazione automatica degli aggiornamenti del sistema operativo è sempre disattivata per l'utente.
Miglioramenti della sicurezza in background	
Miglioramenti della sicurezza in background	**Abilita rollback:**se selezionata, offre all'utente il rollback dei **Miglioramenti alla sicurezza in background**. Selezionare la casella di controllo **Miglioramenti della sicurezza in background** per controllare l'installazione e il rollback degli aggiornamenti. Selezionare le opzioni seguenti: • **Abilita**: se selezionata, offre l'installazione dei **Miglioramenti alla sicurezza in background all'utente.**
iOS 18+ supervisionato	
Cadenza consigliata	Selezionare una delle seguenti opzioni per mostrare all'utente gli aggiornamenti del software quando sono disponibili più aggiornamenti: • **Tutte**: mostra tutte le versioni di aggiornamento del software. • **Più datata**: mostra solo la versione di aggiornamento software più datata (numero più basso). • **Più recente**: mostra solo la versione di aggiornamento software più recente (numero più alto).
Rinvii	È possibile scegliere di rinviare gli aggiornamenti software per tutti i dispositivi supervisionati. Non è possibile posticipare i **Miglioramenti alla sicurezza in background**.
Periodo combinato in giorni	Impostare i giorni per rinviare un aggiornamento di sistema principale o secondario sul dispositivo. Una volta configurati, gli aggiornamento software principali o secondari verranno visualizzati dopo un determinato numero di giorni dal loro rilascio. È possibile impostare qualsiasi valore compreso tra 1 e 90 giorni.
macOS 15+ supervisionato	
Consenti aggiornamenti del sistema operativo agli utenti standard	Selezionare la casella di controllo **Consenti aggiornamenti del sistema operativo agli utenti standard** per consentire a un utente di eseguire gli aggiornamenti del sistema operativo. Selezionare la casella di controllo **Consenti all'utente standard di eseguire aggiornamenti software principali e secondari** per consentire a un utente standard di eseguire aggiornamenti software principali e secondari. Se non si seleziona la casella di controllo, solo gli amministratori possono eseguire gli aggiornamenti software principali e secondari.
Rinvii	
Periodo di aggiornamento principale in giorni	Impostare i giorni per rinviare un aggiornamento software del sistema operativo principale sul dispositivo. Una volta configurato, l'aggiornamento software principale verrà visualizzato dopo un determinato numero di giorni dal suo rilascio. È possibile impostare qualsiasi valore compreso tra 1 e 90 giorni.

Impostazione	Descrizione
Periodo di aggiornamento secondario in giorni	Impostare i giorni per rinviare un aggiornamento software del sistema operativo secondario sul dispositivo. Una volta configurato, l'aggiornamento software principale verrà visualizzato dopo un determinato numero di giorni dal suo rilascio. È possibile impostare qualsiasi valore compreso tra 1 e 90 giorni.
Periodo di aggiornamento sistema in giorni	Impostare i giorni per rinviare un aggiornamento OS di sistema sul dispositivo. Una volta configurato, l'aggiornamento software principale verrà visualizzato dopo un determinato numero di giorni dal suo rilascio. È possibile impostare qualsiasi valore compreso tra 1 e 90 giorni.
Azioni automatiche	
Installa aggiornamento sulla sicurezza	Selezionare una delle seguenti opzioni: • **Consentito**: l'utente può attivare o disattivare l'installazione degli aggiornamenti di sicurezza. • **Sempre attivo**: l'installazione degli aggiornamenti di sicurezza è sempre attiva per l'utente. • **Sempre disattivo**: l'installazione degli aggiornamenti di sicurezza è sempre disattivata per l'utente.

4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
5. Selezionare una delle opzioni di distribuzione per impostare la configurazione di **Impostazioni aggiornamento software**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere Utilizzo delle configurazioni.
6. Fare clic su **Fine**.

10.10.4.60. Configurazione delle preferenze di sicurezza

La configurazione delle preferenze di sicurezza permette agli amministratori di controllare e gestire le modifiche apportate dagli utenti alle impostazioni del firewall, bloccare i messaggi e modificare le password nel dispositivo.

Applicabile a: macOS 10.10 e versioni successive

Procedure

1. Andare in Configurazioni > +Aggiungi.
2. Digitare Sicurezza nel campo di ricerca, quindi fare clic sulla configurazione Preferenze di sicurezza.
3. Immettere un Nome e una Descrizione per la configurazione.
4. Selezionare le configurazioni necessarie:
    - Disabilita modifiche a impostazioni firewall
    - Disabilita modifiche al messaggio di blocco
    - Disabilita modifiche alla password
5. Fare clic su Avanti.
6. Selezionare l'opzione Abilita questa configurazione.
7. Selezionare una delle opzioni di canale seguenti per applicare la configurazione:
    - Canale del dispositivo (più comune)
    - Canale dell'utente (utente registrato corrente)
8. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzata.
9. Fare clic su Fine.

10.10.4.61. Server di riferimento orario

Applicabile a: macOS 10.12.4 o versioni successive supportate.

Permette di creare una configurazione server di riferimento orario per consentire ai dispositivi di connettersi ai server di riferimento orario personalizzati.

Creazione di una configurazione server di riferimento orario

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **orario** nel campo di ricerca, quindi fare clic sulla configurazione **Server di riferimento orario**.
4. Immettere un nome e una descrizione per la configurazione.
5. Specificare **Server NTP**.
6. Specificare la stringa **Fuso orario** nel formato ID fuso orario Olson (ad esempio / Pacifico/Midway). Per visualizzare il formato del fuso orario Olson, eseguire il comando `"/usr/sbin/systemsetup -listtimezones` " dal dispositivo macOS dell'amministratore.
7. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
8. Fare clic su **Fine**.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.4.62. Filtro contenuto Web

Licenza: Silver

La configurazione del filtro dei contenuti web limita l'accesso al web per i dispositivi iOS 7+, macOS 10.15+ e visionOS 1.1+.

Impostazioni del filtro contenuti Web

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Siti Web consentiti	**Limita contenuti per adulti:** selezionare questa opzione se si desidera bloccare l'accesso ai siti Web in base ai filtri iOS automatici. Questi filtri tentano, con un alto livello di precisione, di bloccare i siti Web con contenuti inappropriati. **Solo siti Web specifici:** selezionare questa opzione se si desidera elencare manualmente i siti Web accessibili. **Plug-in (solo iOS8 supervisionato e macOS 10.15+):** selezionare questa opzione per utilizzare un plug-in di terze parti.
URL consentiti	Questa opzione è disponibile solo se è stata selezionata l'opzione Limita contenuto per adulti. Immettere gli URL consentiti. Ciascun URL deve iniziare con: • http:// o con • https:// Se si desidera consentire gli URL http:// e https:// per lo stesso sito, includere due URL separati. Tutti gli URL con i caratteri iniziali corrispondenti a quelli degli URL consentiti saranno accessibili. Esempio: http://www.sitoAzienda.com consente l'accesso agli indirizzi seguenti: • http://www.sitoAzienda.com • http://www.sitoAzienda.com/offerte di lavoro Tali URL sono accessibili anche se bloccati dai filtri iOS automatici.
Usa elenco URL da rifiutare	Questa opzione è disponibile solo se è stata selezionata l'opzione Limita contenuto per adulti. Immettere gli URL da includere nell'elenco degli elementi non consentiti. Ciascun URL deve iniziare con: • http:// o con • https:// Se si desidera bloccare gli URL http:// e https:// per lo stesso sito, includere una riga per ciascun URL. Tutti gli URL con caratteri iniziali corrispondenti a un URL non consentito vengono bloccati. Esempio: http://www.sitoAzienda.com blocca l'accesso agli indirizzi seguenti: • http://www.sitoAzienda.com • http://www.sitoAzienda.com/offerte di lavoro Tali URL sono bloccati anche se consentiti dai filtri iOS automatici.
Segnalibri consentiti	Questa opzione è disponibile soltanto se è stata selezionata l'opzione Solo siti Web specifici. Facoltativamente, è possibile inserire la cartella in cui aggiungere i segnalibri in Safari. Esempio: /Vendite/Prodotti/ Se non presente, il segnalibro viene aggiunto alla directory dei segnalibri predefinita.
Nome filtro	Questa opzione è disponibile solo se è stata selezionata l'opzione Plugin. Inserire del testo che verrà visualizzato per identificare il filtro.
Identificatore	Questa opzione è disponibile solo se è stata selezionata l'opzione Plugin. Inserire l'ID del pacchetto del plugin che fornisce il servizio filtri.

Impostazione	Operazione da eseguire
Indirizzo del servizio	Questa opzione è disponibile solo se è stata selezionata l'opzione Plugin. Facoltativo: inserire l'eventuale indirizzo del server necessario per l'utilizzo da parte del plugin. Consultare la documentazione del plugin per stabilire se tale valore è necessario.
Organizzazione	Questa opzione è disponibile solo se è stata selezionata l'opzione Plugin. Facoltativo: inserire l'eventuale stringa dell'organizzazione richiesta dal plugin. Consultare la documentazione del plugin per stabilire se tale valore è necessario.
Nome utente	Questa opzione è disponibile solo se è stata selezionata l'opzione Plugin. Facoltativo: inserire l'eventuale nome utente richiesto dal servizio del plugin. Consultare la documentazione del plugin per stabilire se tale valore è necessario.
Password	Questa opzione è disponibile solo se è stata selezionata l'opzione Plugin. Facoltativo: inserire l'eventuale password richiesta dal servizio del plugin. Consultare la documentazione del plugin per stabilire se tale valore è necessario.
Certificato	Questa opzione è disponibile solo se è stata selezionata l'opzione Plugin. Facoltativo: inserire l'eventuale certificato richiesto dal servizio del plugin per l'autenticazione dell'utente. Consultare la documentazione del plugin per stabilire se tale valore è necessario.
Filtro traffico webkit	Questa opzione è disponibile solo se è stata selezionata l'opzione Plugin. Selezionare quest'opzione per includere il traffico webkit nel filtro.
Filtro traffico socket	Questa opzione è disponibile solo se è stata selezionata l'opzione Plugin. Selezionare quest'opzione per includere il traffico socket nel filtro.
Dati personalizzati	Questa opzione è disponibile solo se è stata selezionata l'opzione Plugin. Facoltativo: aggiungere eventuali coppie chiave/valore richieste dal servizio del plugin. Consultare la documentazione del plugin per stabilire se tale valore è necessario.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.4.63. Windows Firewall

La configurazione di Windows Firewall consente di configurare impostazioni del profilo del firewall di Windows nonché il set desiderato di regole personalizzate da eseguire sul dispositivo. Questa configurazione può essere utilizzata per gestire dispositivi non di dominio e ridurre il rischio delle minacce alla sicurezza della rete in tutti i sistemi che si collegano alla rete aziendale.

Configurazione di Windows Firewall

Procedura

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Firewall**.
3. Fare clic sull'icona di **Windows**.
4. Immettere un nome per la configurazione.
5. Immettere una descrizione per la configurazione firewall.
6. Nella sezione Impostazioni configurazione, specificare le impostazioni rimanenti come descritto nella tabella seguente.

Impostazione	Operazione da eseguire
Profili	
Attiva	Far scorrere l'interruttore su ON per abilitare il profilo.
Tipo	Viene visualizzato il tipo di profilo. Esempio: Dominio.
Azione predefinita traffico in entrata	Selezionare un'opzione per l'azione predefinita che deve essere eseguita sul traffico in entrata. **Consenti**: per consentire il traffico. **Blocca**: per bloccare il traffico.
Azione predefinita traffico in uscita	Selezionare l'azione predefinita che deve essere eseguita sul traffico in entrata. **Consenti**: per consentire il traffico. **Blocca**: per bloccare il traffico.

7. Per aggiungere Regole, fare clic su **+Aggiungi** e configurare le seguenti impostazioni:

Impostazione	Operazione da eseguire
Regole	
Attivato	Far scorrere l'interruttore per abilitare il profilo.
Nome regola	Immettere un nome identificativo della regola.
Descrizione	Immettere una descrizione esplicativa dello scopo della regola.
Direzione	Selezionare la direzione del traffico a cui la regola deve essere applicata: • **In**: per il traffico in ingresso • **Out**: per il traffico in uscita • **Entrambi**: entrambe le direzioni.
Azione	Selezionare l'azione da eseguire • **Consenti**: per consentire il traffico. • **Blocca**: per bloccare il traffico.
Profilo	Selezionare i profili a cui la regola deve essere applicata: • **Tutti** • **Dominio** • **Privato** • **Pubblica**
App	Digitare il nome comune pacchetto (PFN, Package Family Name) o il percorso completo al file eseguibile dell'app.
Protocollo	Selezionare uno qualsiasi dei seguenti protocolli a cui la regola deve essere applicata: • **TCP** • **UDP** • **ICMP**
Intervalli di indirizzi locali	Digitare gli intervalli di indirizzi IPv4/IPv6 locali o subnet mask.
Intervalli di porte locali	Digitare l'elenco separato da virgole di porte locali o intervalli di porta. Esempio: 20,50,100-120.
Intervalli di indirizzi remoti	Digitare gli intervalli di indirizzi IPv4/IPv6 remoti o subnet mask.
Intervalli di porte remote	Digitare l'elenco separato da virgole di porte locali o intervalli di porta. Esempio: 20,50,100-120.
Tipi di interfacce	Selezionare una delle seguenti opzioni di tipi di interfaccia: • **Tutti** • **Accesso remoto** • **Wireless**

Impostazione	Operazione da eseguire
	• **LAN** • **Mobile a banda larga** L'opzione predefinita **Tutte** viene applicata se non viene selezionata nessuna opzione per il tipo di interfaccia.

8. Fare clic su **Avanti**.
9. Selezionare una delle seguenti opzioni di distribuzione:
   - Tutti i dispositivi
   - Nessun dispositivo (impostazione predefinita)
   - Personalizzato
10. Fare clic su **Fine**.

10.10.4.64. Protezione delle informazioni di Windows

Licenza: Gold

Applicabile a: Windows 10+

La configurazione di Protezione delle informazioni di Windows definisce le impostazioni per proteggere i dati aziendali. Questa configurazione può essere applicata ai dispositivi registrati nell'ambito della gestione. È inoltre possibile visualizzare i dettagli di Protezione delle informazioni di Windows per un dispositivo configurato nella pagina della panoramica di tale dispositivo.

Configurazione della Protezione delle informazioni di Windows

Procedura

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione di **Protezione delle informazioni di Windows**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Nella sezione Impostazioni configurazione, specificare le impostazioni rimanenti come descritto nella tabella seguente.
6. Fare clic su **Avanti**.
7. Selezionare una distribuzione per la configurazione.

Categoria	Impostazione	Operazione da eseguire
	Nome	Immettere un nome identificativo della configurazione.
	Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Informazioni sull'azienda	**Tutte le versioni (Windows 10+)**	
	Nomi dei domini protetti	Specificare l'elenco di identità per il quale sono state configurate le policy per la protezione dei dati. Le e-mail e gli altri dati associati a queste identità saranno considerati aziendali e protetti. • Si tratta di un elenco di domini delimitato da "|" in cui il primo dominio dell'elenco è considerato l'identità principale per gli scopi dell'interfaccia utente Windows. • Ad esempio: "domain1.com|domain2.co.uk"
	Nomi dei domini di rete	Specificare l'elenco di domini che includono i confini dell'azienda. I dati provenienti da uno di questi domini e inviati a un dispositivo saranno considerati dati aziendali e protetti. • Queste posizioni saranno considerate destinazioni sicure con cui condividere i dati aziendali. • Si tratta di un elenco di domini delimitato da virgole. • Ad esempio: "mail.domain3.com, domain4.com"
	Risorse cloud	Include un elenco di domini di risorse aziendali ospitati nel cloud che devono essere protetti. Le connessioni a queste risorse sono considerate dati aziendali. Specificare uno o più nomi di dominio con indirizzi proxy opzionali tra parentesi. • Ad esempio: "domainname1.com, domainname2 (10.0.0.1)". • Se un proxy è abbinato a una risorsa cloud, il traffico verso tale risorsa verrà indirizzato attraverso la rete aziendale mediante il server proxy specificato (sulla porta 80). • Tutti gli indirizzi proxy specificati in questo campo devono anche essere immessi nel campo Server proxy interni seguente.
	Intervallo IP	Consente di impostare gli intervalli di IP aziendali che definiscono i computer all'interno della rete aziendale. I dati provenienti da questi computer saranno considerati aziendali e protetti. Queste posizioni saranno considerate destinazioni sicure con cui condividere i dati

Categoria	Impostazione	Operazione da eseguire
		aziendali. Si tratta di un elenco di intervalli di IPv4 e IPv6 delimitati da virgole. • Si tratta di un elenco di intervalli di IPv4 e IPv6 delimitati da virgole. • Selezionare l'opzione **Gli intervalli IP sono autorevoli** se il client deve accettare l'elenco configurato e non utilizzare dati euristici per trovare altre sottoreti.
	Risorse neutre	Consente di specificare l'elenco di nomi di domini che è possibile utilizzare per risorse personali o lavorative.
	Server proxy	Consente di specificare l'elenco di server proxy delimitati da virgole. Qualsiasi server in questo elenco è considerato come non aziendale. • Ad esempio: "157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59". • Selezionare l'opzione **I server proxy sono autorevoli** se il client deve accettare l'elenco configurato di proxy e non tentare di rilevare altri proxy di lavoro.
	Server proxy interni	Consente di specificare l'elenco di server proxy interni separati da virgole. • Ad esempio: "157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59". • Questi proxy sono stati configurati dall'amministratore per connettersi a risorse specifiche su Internet. Sono considerati posizioni di rete aziendali. Questi proxy vengono sfruttati solo per la configurazione della policy EnterpriseCloudResources per forzare il traffico verso le risorse cloud corrispondenti attraverso tali proxy.
Protezione dati	**Tutte le versioni (Windows 10+)**	
	Livello di imposizione	Scegliere uno dei seguenti livelli di imposizione: • Off - nessuna protezione (i dati crittografati in precedenza verranno decrittografati). • Invisibile all'utente - viene eseguita la crittografia dei dati e delle attività di controllo sul dispositivo dopo avere protetto i dati. All'utente non viene chiesta nessuna informazione negativa sull'app o i dati. • Sostituisci - simile alla modalità Invisibile all'utente. Inoltre, se un'app o i dati non vengono utilizzati correttamente, all'utente

Categoria	Impostazione	Operazione da eseguire
		viene chiesto se procedere o annullare l'operazione attualmente in esecuzione. • Blocca - simile alla modalità Invisibile all'utente. Inoltre, se un'app o i dati non vengono utilizzati correttamente, l'operazione attualmente in esecuzione da parte dell'utente viene bloccata e all'utente viene mostrato un avviso con il motivo del blocco. Ad eccezione della modalità Off, qualsiasi dato o app per cui non è previsto l'utilizzo di dati o risorse aziendali verrà collegato al dispositivo. È possibile rimuovere i dati dal dispositivo utilizzando un altro fornitore di servizi di configurazione.
	Certificato di recupero dati	Specificare un certificato di recupero utilizzabile per il recupero dei dati dei file crittografati. • Funziona allo stesso modo del certificato dell'agente di recupero dei dati per Encrypting File System (EFS). Tuttavia, questo certificato viene rilasciato mediante MDM anziché mediante la policy di gruppo. È possibile selezionare una o più delle seguenti opzioni: • Consenti decrittografia utente • Revoca all'annullamento della registrazione • Mostra icone EDP • Richiedi protezione durante il blocco (solo Windows 10 Mobile)
RMS	**Tutte le versioni (Windows 10+)**	
	Consenti Azure RMS	Consente di specificare se permettere la crittografia di Azure Rights Management (Azure RMS) per Protezione delle informazioni di Windows.
	ID modello RMS	Consente di specificare il GUID TemplateID da utilizzare per la crittografia di RMS. Il modello RMS permette agli amministratori di configurare i dettagli relativi a coloro che hanno accesso al file protetto da RMS e al periodo di tempo per cui è consentito l'accesso.
Controllo app	**Tutte le versioni (Windows 10+)**	
	Consente di specificare una raccolta di app create nella pagina **App > Catalogo app** con un valore di Protezione delle informazioni di Windows. Consente di specificare le	

Categoria	Impostazione	Operazione da eseguire
	definizioni delle regole per le app utilizzando il seguente insieme di parametri:	
	Tipo di app	Selezionare uno dei seguenti tipi di app: • Publisher/PFN Equals - si applica a Windows 10+ con supporto PFN. • EXE/Win32 Equals - si applica solo a Windows Desktop.
	Identificatore app	Selezionare l'app dalle opzioni visualizzate per aggiungerla all'Identificatore app. È anche possibile fare clic su **Cerca app**.
	Descrizione app	Immettere una descrizione per l'app.

10.10.4.65. Restrizioni di Windows

Le restrizioni di Windows determinano quali funzioni sono abilitate sui dispositivi Windows 10+.

Impostazioni delle restrizioni per Windows

Categoria	Impostazione	Operazione da eseguire
	Nome	Immettere un nome identificativo della configurazione.
Funzionalità del dispositivo **Tutte le versioni (Windows 10+)**	Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
	Disabilita offloading Wi-Fi	Selezionare questa opzione per impedire che il dispositivo acceda a reti compatibili per utilizzare i dati previsti per le reti wireless autorizzate.
	Disattiva condivisione Internet	Selezionare questa opzione per impedire al dispositivo di accedere a Internet mediante un altro dispositivo wireless.
	Disabilita posizione	Selezionare questa opzione per disattivare i servizi di posizione.
	Disattiva roaming rete dati	Selezionare questa opzione per disattivare il roaming dati quando il dispositivo è in modalità cellulare.
	Disattiva Bluetooth	Selezionare questa opzione per impedire che il dispositivo stabilisca connessioni Bluetooth.
	Disattiva VPN durante il roaming o su una rete cellulare	Selezionare questa opzione per impedire al dispositivo di stabilire connessioni VPN quando non è attiva la modalità WiFi.
Telemetria - Consentire al dispositivo di inviare dati di telemetria diagnostica e di utilizzo. **Solo Windows 10**	Disabilita la configurazione manuale del Wi-Fi	Selezionare per impedire all'utente di configurare manualmente le impostazioni Wi-Fi del dispositivo.
	Disattiva Wi-Fi	Selezionare per consentire o negare la connessione WiFi.
	Livello di telemetria	Selezionare uno dei seguenti livelli di telemetria per la segnalazione dei dati: • **Sicurezza**: per inviare informazioni su esperienze utente connesse, impostazioni del componente Telemetria, strumento di rimozione malware e Windows Defender. • **Base**: per inviare informazioni di base sul dispositivo, tra cui dati relativi alla qualità, compatibilità delle app, dati sull'uso delle app e dati del livello Sicurezza. • **Avanzato**: per inviare ulteriori informazioni che includono utilizzo e prestazioni di Windows, Windows Server, System

Categoria	Impostazione	Operazione da eseguire
		Center e app. Tali informazioni includono anche i dati avanzati sull'affidabilità, nonché i dati dei livelli Base e Sicurezza. • **Completa (predefinito)**: per inviare tutti i dati per l'identificazione e la correzione dei problemi, più i dati dei livelli Sicurezza, Base e Avanzato.
Prevenzione della perdita dei dati (DLP)	**Tutte le versioni (Windows 10+)**	
	Disattiva fotocamera	Selezionare questa opzione per impedire all'utente finale di utilizzare l'app fotocamera.
	Disattiva accesso a scheda di memoria SD	Selezionare questa opzione per impedire l'accesso del dispositivo a una scheda di memoria.
	Disabilita l'acquisizione dello schermo (solo per il desktop)	Selezionare per impedire l'acquisizione dello schermo tramite le app specifiche presenti all'interno del dispositivo.
	Disabilita l'archiviazione di massa USB (solo HoloLens)	Selezionare per impedire a HoloLens di accedere ai dispositivi di archiviazione di massa.
Utilizzo dei dati	**Windows 10 e versioni successive**	
	Costo di connessioni 3G	Selezionare una delle seguenti opzioni: • **Illimitata**: la connessione non è limitata da costi di utilizzo e da vincoli di capacità. • **Fissa**: la connessione è limitata da costi di utilizzo e vincoli di capacità dopo il superamento di un determinato limite di dati. • **Variabile**: la connessione ha un costo calcolato in base ai byte.
	Costo di connessioni 4G	
Defender	**Windows 10 e versioni successive**	
DeviceGuard	Disabilita funzionalità monitoraggio in tempo reale di Defender **Windows 10 e versioni successive**	Selezionare per disabilitare la funzionalità monitoraggio in tempo reale di Defender
	Disabilita sicurezza basata su virtualizzazione (VBS)	Selezionare per impedire che la sicurezza basata su virtualizzazione fornisca assistenza per servizi di protezione.
	Credential Guard con sicurezza basata su virtualizzazione	Selezionare una delle seguenti opzioni: • **Disabilitato**: consente di disattivare Credential Guard con sicurezza basata su virtualizzazione.

Categoria	Impostazione	Operazione da eseguire
		• **Abilitato con blocco UEFI**: consente di attivare Credential Guard con sicurezza basata su virtualizzazione con blocco Unified Extensible Firmware Interface (UEFI). • **Abilitato senza blocco**: consente di attivare Credential Guard con sicurezza basata su virtualizzazione senza blocco UEFI.
	Livello Protezione piattaforma (richiede funzionalità di protezione piattaforma)	Selezionare una delle seguenti opzioni: • **VBS con avvio sicuro**: selezionare questa opzione per abilitare la sicurezza basata su virtualizzazione con avvio sicuro. • **VBS con avvio sicuro e Direct memory Access**: selezionare questa opzione per abilitare la sicurezza basata su virtualizzazione con avvio sicuro e accesso diretto alla memoria (DMA, Direct Memory Access).
Privacy	**Windows 10 e versioni successive**	
	Disabilita ID annunci	Selezionare per disabilitare ID annunci.
	Disabilita pubblicazione feed attività per App/OS	Selezionare per impedire ad app/OS di pubblicare feed sull'attività.
Windows e applicazione	**Tutte le versioni (Windows 10+)**	
	Disattiva account Microsoft per servizi diversi dall'e-mail	Selezionare questa opzione per impedire all'utente finale di utilizzare gli account Microsoft per l'autenticazione ai servizi non e-mail.
	Disattiva account non Microsoft	Selezionare questa opzione per impedire all'utente finale di configurare l'e-mail utilizzando account non Microsoft.
	Disattiva assistente personale Cortana	Selezionare questa opzione per impedire all'utente finale di accedere all'assistente personale di Microsoft.
	Disattiva ricerca in base alla posizione	Selezionare questa opzione per impedire alle ricerche di utilizzare la posizione del dispositivo.
	Disattiva sblocco dallo sviluppatore	Selezionare questa opzione per impedire all'utente finale di abilitare il trasferimento locale di app. La modalità predefinita quando un dispositivo è registrato in MDM è SideLoad abilitato.
	Solo le edizioni 11+ supportate	
	Configurazione dell'icona della chat di Teams nella barra delle applicazioni	Selezionare una delle seguenti opzioni: • **Mostra:** l'icona Chat viene visualizzata nella barra delle applicazioni per impostazione predefinita. Gli utenti possono visualizzarla o nasconderla in Impostazioni.

Categoria	Impostazione	Operazione da eseguire
		• **Nascondi:** l'icona Chat viene nascosta per impostazione predefinita. Gli utenti possono visualizzarla o nasconderla in Impostazioni. • **Disabilitata:** l'icona Chat non viene visualizzata e gli utenti non possono visualizzarla o nasconderla in Impostazioni. • **Non configurata:** il comportamento dell'icona Chat dipende dalle impostazioni predefinite dell'edizione di Windows in uso. Le modifiche non vengono applicate fino al riavvio del dispositivo Windows.
	Solo le versioni supportate di Windows 10+ Disabilita aggiornamento automatico delle app da Microsoft Store	 Selezionare per impedire l'aggiornamento automatico di app da Microsoft Store.
	Disabilita l'avvio di tutte le app da Microsoft Store che sono state fornite pre-installate o scaricate	Selezionare per impedire all'utente finale di avviare tutte le app pre-installate o scaricate da Microsoft Store. Supporta solo le edizioni Windows Enterprise ed Education.
	Consenti l'esecuzione delle app in background	Selezionare una delle seguenti opzioni: • **Controllo utente**: consente all'utente di controllare l'esecuzione delle app in background. • **Forza consenso**: consente di eseguire app in background. • **Forza negazione**: impedisce di eseguire app in background.
Altre restrizioni	**Tutte le versioni (Windows 10+)** Disabilitare la possibilità di annullare la registrazione da UEM ed eliminare l'account aziendale.	 Selezionare questa opzione per impedire che l'utente finale annulli la registrazione da UEM ed elimini l'immagine dell'account aziendale.
	Disabilita l'impostazione da parte dell'utente del periodo di tolleranza del blocco del dispositivo (solo HoloLens). **Solo le versioni supportate di Windows 10+**	Selezionare per impedire all'utente di impostare il periodo di tolleranza blocco dispositivo.
	Disabilita l'utente a ripristinare il dispositivo tramite il pannello di	Selezionare questa opzione per impedire all'utente finale di impostare il periodo di tolleranza blocco dispositivo.

Categoria	Impostazione	Operazione da eseguire
	controllo e la combinazione di tasti hardware	
	Richiedere agli utenti di connettersi alla rete durante la configurazione del dispositivo (è richiesto il profilo Autopilot)	Selezionare questa opzione per abilitare TenantLockdown al blocco di tutti i dispositivi Windows registrati con la funzione Autopilot.
	Solo le versioni supportate di Windows 11+	
	Impedisci all'utente dall'apportare modifiche all'eSIM attraverso l'interfaccia utente.	Selezionare questa opzione per impedire all'utente di apportare modifiche ai profili eSIM.

10.10.4.66. Restrizioni del desktop Windows

Applicabile a: desktop Windows 10

Argomenti della sezione:

- Configurazione di restrizioni di Windows Desktop
- Creazione di un elenco di dispositivi di archiviazione rimovibili consentiti

Gli amministratori possono controllare le informazioni sul sistema operativo nei dispositivi desktop Windows 10 gestiti limitando l'accesso degli utenti alle aree seguenti di un dispositivo:

- Pannello di controllo
- Gestione attività
- Esplora file
- Editor del registro

Le funzioni di cui sopra consentono a un utente di fare diverse modifiche al proprio dispositivo. Tramite questa funzionalità, gli amministratori hanno la possibilità di limitare l'accesso a questi controlli dei livelli del sistema e assicurare in tal modo l'accesso.

Questa funzione richiede Bridge. Per ulteriori dettagli, vedere **Ivanti Bridge**.

Configurazione di restrizioni di Windows Desktop

Procedura

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Restrizioni di Windows Desktop**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Nella sezione Impostazioni configurazione, specificare le impostazioni rimanenti come descritto nella tabella seguente.

Impostazione	Operazione da eseguire
Gestione attività **Pannello di controllo** **Editor del registro** **Esplora file**	Selezionare la casella di controllo **Nega accesso** per l'impostazione per cui l'accesso deve essere negato. Selezionare la casella di controllo **Limita funzionalità** per limitare le funzionalità di Esplora file. Esempio: rimozione di "Connetti unità di rete". Fare clic sul link fornito per visualizzare l'elenco delle funzionalità limitate.
Archivi rimovibili	
Modalità di accesso per Archivi rimovibili	• **Limita accesso in lettura**: questo impedisce qualsiasi accesso ed è la configurazione più restrittiva. • **Limita accesso in scrittura**: questo consente un accesso limitato, ma impedisce la rimozione non autorizzata di dati o la possibilità di aggiungere virus, ecc. al dispositivo.

6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni di distribuzione:
   - Tutti i dispositivi
   - Nessun dispositivo (impostazione predefinita)
   - Personalizzato
8. Fare clic su **Fine**.

Perché questa configurazione diventi effettiva, il dispositivo deve essere riavviato dopo averla applicata.

Creazione di un elenco di dispositivi di archiviazione rimovibili consentiti

Se si desidera creare un elenco di dispositivi di archiviazione consentiti, portare prima a termine la procedura seguente:

- Collegare i dispositivi di archiviazione USB che si desidera consentire a un PC.
- Aprire Gestione dispositivi e fare clic sul controller USB.
- Esaminare le impostazioni di ciascun controller per informazioni sul dispositivo.
- Memorizzare le informazioni sul dispositivo da utilizzare durante la creazione dell'elenco dei dispositivi consentiti.

Per creare un elenco di dispositivi di archiviazione rimovibili consentiti:

Procedura

1. Nella pagina di configurazione **Restrizioni di Windows Desktop**, fare clic su **+Aggiungi** nella sezione **Dispositivi di archiviazione rimovibili consentiti**.
2. Nella finestra **Aggiungi ID hardware**, immettere l'ID hardware di uno o più dispositivi che si desidera rimuovere dall'elenco Consenti e bloccare come dispositivi di archiviazione.

3. Fare clic su **Aggiungi ID hardware**. L'elenco degli ID hardware dei dispositivi consentiti viene visualizzato nella sezione **Dispositivi di archiviazione rimovibili consentiti**.

Per modificare o eliminare un ID hardware dall'elenco, selezionare l'opzione Modifica o Elimina sotto la colonna **Azioni**.

Perché questa configurazione diventi effettiva, il dispositivo deve essere riavviato dopo averla applicata.

10.10.4.67. Impostazioni desktop per Windows 10

Le configurazione delle impostazioni del desktop di Windows 10 consente di personalizzare le impostazioni del desktop e di inviarle ai dispositivi con Windows 10. Tramite questa configurazione, è possibile configurare le seguenti impostazioni del desktop:

- Immagine di sfondo del desktop
- Immagine schermata di blocco
- Carica uno screen saver personalizzato
- Collegamenti rapidi desktop

> Questa funzione richiede Bridge. Per ulteriori dettagli, vedere **Ivanti Bridge**.

Procedura

1. Sotto **Configurazione**, fare clic su **+Aggiungi**.
2. Selezionare la configurazione **Impostazioni del desktop per Windows 10**. Viene visualizzata la pagina **Impostazioni desktop per Windows 10**.
3. Nel campo **Nome**, digitare un nome appropriato per le impostazioni.
4. (Facoltativo) Fare clic sul collegamento +**Aggiungi descrizione** per aggiungere una descrizione per la configurazione.
5. Nella sezione **Impostazioni configurazione**, configurare le impostazioni seguenti:

Impostazione	Descrizione
Recapito file	Seleziona una delle seguenti opzioni di fornitura dei file per Impostazioni desktop: • **Carica file** - Carica le impostazioni in Ivanti Neurons for MDM. • **Sovrascrivi URL** - Fornire URL di sovrascrittura con i file delle impostazioni da scaricare.
Impostazioni sfondo desktop	Fare clic su **Scegli file** per individuare e caricare un'immagine di sfondo: i formati di file supportati sono BMP, JPG, JPEG, PNG.
Impostazioni wallpaper schermata di blocco (L'impostazione del wallpaper della schermata di blocco **NON** è supportata sui dispositivi Windows 10 Pro)	Fare clic su **Scegli file** per individuare e caricare un'immagine di sfondo. I formati file supportati sono BMP, JPG, JPEG e PNG.
Impostazioni screen saver	Fare clic su **Scegli file** per individuare e caricare un file di screen saver. Caricare solo file .SCR compatibili con Windows. Selezionare **Protezione password per screen saver** se si desidera impostare la password per sbloccare la modalità Screen saver. Selezionare un periodo **Timeout screen saver** (in minuti).
Collegamenti rapidi desktop	Fare clic su **Aggiungi scelta rapida** per impostare collegamenti sul desktop da aggiungere ai desktop del dispositivo. Viene visualizzata la finestra **Aggiungi collegamento rapido**. Compilare la tabella utilizzando le seguenti opzioni: • **Posizione** - Digitare la posizione in cui il collegamento viene visualizzato sul dispositivo Windows. • **Percorso di destinazione** - Digitare il percorso locale, o il percorso UNC o la lettera di unità a cui porta il collegamento. Il percorso di destinazione può anche essere un URL. • **Argomenti** - Digitare qualsiasi argomento da utilizzare quando si apre il file di destinazione. • **Directory di lavoro** - Digitare il percorso della cartella che contiene i file richiesti dalla destinazione. • **File icona** - Caricare file .ico Windows validi. Dopo aver configurato le opzioni, fare clic su **Aggiungi scelta rapida**.

6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni di distribuzione:
   - Tutti i dispositivi
   - Nessun dispositivo (impostazione predefinita)
   - Personalizzato
8. Fare clic su **Fine**.

10.10.4.68. Configurazione di Windows Hello for Business

Questa configurazione consente agli amministratori di impostare Windows Hello nei dispositivi. Per configurare Windows Hello è necessario impostare un PIN per l'accesso al dispositivo.

Applicabile a: Windows 10

ProcedureProcedura

1. Andare in Configurazioni > +Aggiungi.
2. Digitare windows nel campo di ricerca e fare clic sulla configurazione Windows Hello for Business.
3. Immettere un Nome e una Descrizione per la configurazione.
4. Impostare Abilita/Disabilita Windows Hello for Business per dispositivi Windows 10 su On.

> Questo interruttore è in posizione On per impostazione predefinita. Se si disabilita Windows Hello for Business, i PIN non vengono rimossi dai dispositivi.

5. Impostare Complessità PIN.
6. Selezionare le configurazioni necessarie:
    - Richiede un TPM (Trusted Platform Module) per Windows Hello for Business
    - Usa certificati Windows Hello for Business come certificati smart card
    - Usa dati biometrici, come viso e impronte digitali, come alternativa al PIN per Windows Hello for Business
    - Richiede l'anti-spoofing avanzato per la funzione di riconoscimento facciale utilizzata per l'autenticazione con riconoscimento del viso tramite Windows Hello
    - Blocco dinamico
    - Consente agli utenti di effettuare l'accesso con un codice di sicurezza FIDO2.
7. Fare clic su Avanti.
8. Selezionare l'opzione Abilita questa configurazione.
9. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzata.
10. Fare clic su Fine.

10.10.4.69. Configurazione Gestione IA Windows

Ivanti Neurons per MDM consente agli amministratori di gestire le impostazioni e le configurazioni dell'IA Windows. Gestione Windows IA migliora la creatività e la produttività con l'aiuto di un potente assistente IA. Utilizzare la configurazione **Gestione Windows IA** per gestire le funzionalità di Windows IA sui dispositivi Windows registrati. Questa configurazione consente agli amministratori di controllare le funzionalità Microsoft Copilot, Windows Recall e Microsoft Paint IA tramite i provider Configuration Service Provider (CSP) di Windows IA.

Gli amministratori possono disabilitare le funzionalità IA selezionate, rimuovere l'accesso alle funzionalità Copilot, controllare il comportamento di richiamo di Windows e gestire le funzionalità di generazione di immagini basate sull'IA in Microsoft Paint.

Applicabile a: Windows 10+

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Gestione IA Windows**.
3. Immettere un **Nome** e una **Descrizione** per la configurazione.
4. Nella **Sezione Configurazione**, selezionare tra le seguenti opzioni: ### Impostazioni Copilot

Impostazione	Descrizione
Disabilita Copilot Windows	Impedisce agli utenti di accedere a Windows Copilot.
Disabilita chiave hardware Copilot	Disabilita la chiave hardware Copilot dedicata sui dispositivi supportati.
Rimuovi app Microsoft Copilot	Rimuove l'applicazione Microsoft Copilot dal dispositivo.

Impostazioni Richiamo

Impostazione	Descrizione
Disabilita analisi dati IA	Disabilita l'analisi dei dati basata sull'IA utilizzata da Windows Recall.
Imposta l'archiviazione massima per le istantanee di richiamo (GB)	Specifica la quantità massima di spazio di archiviazione che Windows Recall può utilizzare per archiviare le snapshot.

Impostazioni Paint IA

Impostazione	Descrizione
Disabilita Image Creator	Disabilita la funzione Image Creator in Microsoft Paint.
Disabilita Cocreator	Disabilita la funzione Cocreator in Microsoft Paint.
Disabilita Riempimento generativo	Disabilita la funzione Riempimento generativo in Microsoft Paint.

Microsoft ha deprecato il criterio **TurnOffWindowsCopilot** utilizzato da questa configurazione. Di conseguenza, questa configurazione non influisce più sull'app Copilot che risiede sui dispositivi.

Se non si seleziona la casella di controllo **Disabilita Windows Copilot**, la configurazione sovrascriverà la precedente selezione della configurazione sul dispositivo per abilitare la Gestione IA Windows.

5. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
6. Selezionare una delle opzioni di distribuzione per impostare la configurazione della **Gestione IA Windows**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere **Utilizzo delle configurazioni**.
7. Fare clic su **Fine**.

10.10.4.70. Play Integrity (in precedenza SafetyNet Attestation)

Play Integrity (precedentemente SafetyNet) aiuta a valutare la sicurezza e la compatibilità dei dispositivi Android utilizzando le API Play Integrity di Google. Se configurato, consente di analizzare i dispositivi dopo un intervallo di tempo regolare per determinare se il dispositivo è stato manomesso o meno.

> Play Integrity è ora supportato su tutte le versioni di Android.

Procedura

1. Nella scheda **Configurazione**, fare clic su **+Aggiungi**.
2. Selezionare la configurazione **Play Integrity**. Viene visualizzata la pagina **Configurazione Play Integrity**
3. Nel campo **Nome**, digitare un nome appropriato per la configurazione Play Integrity.
4. Fare clic sul collegamento **+Aggiungi descrizione** per aggiungere una descrizione per la configurazione. Questo campo è facoltativo.
5. Nella sezione **Impostazione Configurazione**, digitare l'intervallo di tempo minimo (in ore) da applicare per la valutazione del controllo di sicurezza e compatibilità dei dispositivi. Il valore deve essere compreso tra 1 e 24.
6. Fare clic su **Avanti** e selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato

Fare clic su **Fine**.

> Quando i nonce di Play Integrity e SafetyNet saranno inviati al dispositivo, il nonce di Play Integrity avrà la priorità sul nonce di SafetyNet.

10.10.4.71. Passcode avanzato Android e schermata di blocco

Couldn't convert your doc.

10.10.4.72. Microsoft Defender for Endpoint

La configurazione di Microsoft Defender for Endpoint (MDE), precedentemente nota come Windows Advanced Threat Protection, consente ai clienti di inserire e disinserire i dispositivi nel servizio MDE.

Procedura

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Microsoft Defender for Endpoint**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Nella sezione Impostazioni configurazione, specificare le impostazioni rimanenti come descritto nella tabella seguente.

Impostazione	Descrizione
Blob di onboarding o offboarding	Incollare il blob di onboarding o offboarding dal sito di Microsoft Defender for Endpoint Security Center.

6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni di distribuzione:

- Tutti i dispositivi
- Nessun dispositivo (impostazione predefinita)
- Personalizzato

8. Fare clic su **Fine**.

10.10.4.73. Autenticazione basata su certificati

Ivanti Neurons per MDMsupporta l'autenticazione basata su certificati che consente agli amministratori di effettuare l'accesso utilizzando certificati digitali e un nome host (vanity) specificato del tenant. Quando questa funzionalità è abilitata e configurata, gli amministratori possono accedere utilizzando i certificati digitali al posto dell'autenticazione di base (nome utente e password).

> Questa funzionalità è disabilitata per impostazione predefinita. Per attivare questa funzionalità sui tenant, gli amministratori devono contattare il supporto. Questa funzionalità è disponibile solo su ambienti cluster NA3, e solo se abilitata dal supporto. Assicurarsi di aver testato e di avere a disposizione il nome utente e la password di super-amministratore, perché una volta che l'autenticazione basata su certificati è abilitata, queste credenziali saranno le uniche che sarà possibile utilizzare per l'accesso fino a quando non viene configurato il dominio personalizzato.

Procedura

1. Nella scheda **Amministratore**, selezionare **Configurazione vanity host**.
2. Nella pagina Configurazione vanity host, configurare le seguenti opzioni:
3. Fare clic su **Salva**.
   Potrebbero essere necessari alcuni minuti prima che l'host vanity sia accessibile.

Impostazione	Operazione da eseguire
Crea dominio personalizzato	Digitare il nome del dominio vanity. Questo è il nome di dominio che può allinearsi più strettamente alla propria identità aziendale e a cui è possibile accedere utilizzando certificati digitali.
Carica certificati CA emessi in modo affidabile	Fare clic su **Scegli file** per selezionare e caricare il certificato CA che rilascia certificati agli amministratori. Per abilitare il controllo della revoca del certificato, selezionare **Abilita impostazioni di convalida stato per questo certificato** (facoltativo). Questa opzione è attivata per impostazione predefinita. Deselezionare l'opzione per disattivare la revoca dei certificati. Fare clic su **Aggiungi altro** per aggiungere altri certificati. Assicurarsi che il formato del certificato sia .p7b, .pem, .der, .crt o .cer.
Mapping attributi certificato	Il mapping degli attributi certificato configura il mapping tra gli elementi dell'identità del certificato e gli attributi dell'account dell'amministratore. Nel campo **Da certificato**, selezionare uno dei seguenti elementi del certificato: • **Nome principale NT** • **Nome RFC 822** Nel campo **A variabile**, selezionare uno dei seguenti attributi dell'account dell'amministratore: • **UPN utente** • **$UserEmailAddress** • **$EDIPI**

10.10.5. Configurazioni delle risorse utenti

Argomenti della sezione:

- Configurazione CalDAV
- CardDAV
- Configurazione di Google
- Configurazione delle e-mail
- Configurazione di Exchange
- Configurazione del tipo di carattere
- Configurazione del calendario sottoscritto
- Creare una configurazione clip Web
- Installazione di Office 365
- Impostazioni GPO Windows
- Configurazione della crittografia BitLocker

10.10.5.1. Configurazione CalDAV

La configurazione CalDAV consente di definire l'accesso a un calendario Web mediante lo standard Internet CalDAV.

Impostazioni di CalDAV

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Nome host e porta	Immettere il nome host e la porta del server calendario.
URL principale	Immettere l'URL per l'accesso ai servizi calendario.
Utente	Immettere il nome utente da utilizzare per l'accesso.
Password	Immettere la password da utilizzare per l'accesso.
Utilizza SSL	Selezionare quest'opzione per utilizzare soltanto il Secure Socket Layer per le comunicazioni tra il dispositivo e il server.
VPN per-app	**Prerequisito**: configurare Tunnel o la configurazione VPN per-app prima di configurare la VPN per-app nella configurazione CalDAV. Nel menu a discesa, selezionare la configurazione VPN per-app preconfigurata. **Applicabile a**: iOS 14+

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.5.2. CardDAV

La configurazione CardDAV consente di definire l'accesso a una rubrica Web mediante lo standard Internet CardDAV.

Impostazioni di CardDAV

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Nome host e porta	Immettere il nome host e la porta del server della rubrica.
URL principale	Immettere l'URL per l'accesso ai servizi della rubrica.
Nome utente	Immettere il nome utente da utilizzare per l'accesso.
Password	Immettere la password da utilizzare per l'accesso.
Utilizza SSL	Selezionare quest'opzione per utilizzare soltanto il Secure Socket Layer per le comunicazioni tra il dispositivo e il server.
VPN per-app	**Prerequisito**: configurare Tunnel o la configurazione VPN per-app prima di configurare la VPN per-app nella configurazione CardDAV. Nel menu a discesa, selezionare la configurazione VPN per-app preconfigurata. **Applicabile a**: iOS 14+
iOS 10 e versioni successive	
Regole servizi di comunicazione	Scegliere un'app predefinita da utilizzare per effettuare chiamate audio ai contatti all'interno del sistema CardDAV.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.5.3. Configurazione di Google

La configurazione dell'account Google collega i dispositivi iOS 9.3.2 e visionOS 1.1 o Android 6.0+, o versioni più recenti supportate, agli account Google. Per gli account di Google è necessario Android enterprise. La configurazione può prevedere più indirizzi e-mail Google e qualsiasi altro servizio Google attivato dall'utente dopo l'autenticazione.

Procedura

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Account Google**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Nella sezione Impostazioni configurazione, specificare le impostazioni rimanenti come descritto nella tabella seguente:

Impostazione	Operazione da eseguire
iOS 9.3.2+ , Android 6.0+	
Nome	Immettere un nome identificativo della configurazione.
Descrizione account	Immettere il nome visualizzato dell'account.
Nome account	Immettere nome e cognome dell'utente dell'account.
Indirizzo e-mail	Immettere l'indirizzo e-mail Google dell'account.
VPN per-app	**Prerequisito**: configurare Tunnel o la configurazione VPN per-app prima di configurare la VPN per-app nella configurazione dell'account Google. Nel menu a discesa, selezionare la configurazione VPN per-app preconfigurata. **Applicabile a**: iOS 14+
iOS 10 e versioni successive	
Regole servizi di comunicazione	Scegliere l'app predefinita da usare per chiamare i contatti nel sistema Google selezionando una delle seguenti opzioni: • **Da catalogo app e app di sistema**: cercare le app digitando le prime lettere del nome dell'app. • **Immetti ID bundle (solo per app di sistemi Apple)**: digitare l'ID bundle dell'app del sistema. L'ID bundle deve iniziare con "com.apple".

6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni di distribuzione:

- Tutti i dispositivi
- Nessun dispositivo (impostazione predefinita)
- Personalizzato

8. Fare clic su **Fine**.

Quando si applica una configurazione Account Google al dispositivo, il client Go richiede all'utente di accedere a Google.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.5.4. Configurazione delle e-mail

La configurazione delle e-mail consente di impostare le e-mail POP e IMAP sui dispositivi.

Impostazioni delle e-mail

Impostazione	Operazione da eseguire
Nome Descrizione	Immettere un nome identificativo della configurazione. Immettere una descrizione esplicativa dello scopo della configurazione.
Descrizione account Tipo di account	Immettere il testo che si desidera utilizzare per identificare l'account e-mail. Selezionare IMAP o POP. Se si seleziona IMAP, è possibile immettere anche il prefisso del percorso. Il provider di servizi Internet (ISP, Internet Service Provider) è in grado di fornire le informazioni sui tipi di account disponibili. Generalmente, è necessario un prefisso se tutte le cartelle IMAP sono elencate nella casella della posta in arrivo. Gli ISP che richiedono dei prefissi solitamente forniscono delle informazioni sul prefisso specifico della configurazione.
Nome utente visualizzato	Immettere il testo che si desidera utilizzare per identificare l'account e-mail dell'utente. Tenere presente che l'utente può impostare questo valore anche sul dispositivo.
Indirizzo e-mail	Immettere una variabile per specificare l'indirizzo e-mail dell'account.
Consenti spostamento	Selezionare quest'opzione se non si desidera impedire che le e-mail vengano spostate da questo account.
Abilita S/MIME	Selezionare questa opzione per attivare il supporto della crittografia S/MIME. È possibile quindi selezionare i certificati di crittografia e firma. Richiede la memorizzazione del certificato nella cache. Assicurarsi che la memorizzazione nella cache sia abilitata nell'autorità di certificazione utilizzata dalla configurazione del certificato di identità. **iOS 10.3 e versioni successive:** Selezionare una delle seguenti opzioni per i campi **Firma S/MIME** e **Crittografia S/MIME**: • Disattivato • Attivato • Selezione utente **iOS 12.0 e versioni successive:** • Consentire all'utente di ignorare le impostazioni di firma S/MIME • Consentire all'utente di selezionare l'identità di firma S/MIME • Consentire all'utente di ignorare le impostazioni di cifratura S/MIME • Consentire all'utente di selezionare l'identità di cifratura S/MIME **Abilitare la firma e la crittografia S/MIME per messaggio**, se richiesto.

Impostazione	Operazione da eseguire
Consenti Mail Drop	Seleziona per permettere Mail Drop per questo account. Mail Drop mette l'utente in grado di inviare e-mail con allegati di grandi dimensioni memorizzando l'allegato in iCloud e mettendo un link all'allegato nell'e-mail. Per altre informazioni su Mail Drop andare a: **https://support.apple.com/**
VPN per-app	Apple supporta la possibilità di associare diversi profili VPN a livello di app in Domini e-mail. Ora la VPN a livello di app supporta le configurazioni e-mail IMAP e POP3. **Prerequisito**: configurare Tunnel o la configurazione VPN per-app prima di configurare la VPN per-app nella configurazione e-mail. Scegliere **Seleziona config. VPN per-app** dal menu a discesa.

Posta in arrivo

Impostazione	Operazione da eseguire
Porta e server di posta	Il provider di servizi Internet (ISP) è in grado di fornire questo indirizzo.
Nome utente	Immettere il nome utente per l'accesso al server della posta in arrivo. Solitamente il nome utente coincide con l'indirizzo e-mail. L'ISP fornisce il formato del nome utente.
Tipo di autenticazione	Selezionare il tipo di autenticazione definito dall'ISP.
Password	Immettere la password per l'accesso al server della posta in arrivo.
Utilizza SSL	Selezionare quest'opzione per utilizzare soltanto il Secure Socket Layer per le comunicazioni tra il dispositivo e il server.

Posta in uscita

Impostazione	Operazione da eseguire
Porta e server di posta	Il provider di servizi Internet (ISP) è in grado di fornire questo indirizzo.
Nome utente	Immettere il nome utente per l'accesso al server della posta in uscita. Solitamente il nome utente coincide con l'indirizzo e-mail. L'ISP fornisce il formato del nome utente.
Tipo di autenticazione	Selezionare il tipo di autenticazione definito dall'ISP.
Password	Immettere la password per l'accesso al server della posta in uscita.
La password della posta in uscita corrisponde a quella della posta in arrivo	Selezionare quest'opzione se l'autenticazione SMTP utilizza la stessa password di POP/IMAP.
Utilizza solo la Posta	Selezionare se si desidera che questa configurazione sia utilizzata solo dal client e-mail. Altre applicazioni per l'invio di e-mail, incluse le applicazioni per l'invio di contenuti tramite il client e-mail nativo, non sono in grado di utilizzare questa configurazione.
Utilizza SSL	Selezionare quest'opzione per utilizzare soltanto il Secure Socket Layer per le comunicazioni tra il dispositivo e il server.

10.10.5.5. Configurazione di Exchange

Una configurazione di Exchange imposta la posta elettronica basata su ActiveSync sui dispositivi Android, iOS e visionOS e la posta elettronica basata su Exchange Web Services (EWS) per i dispositivi macOS.

> La configurazione di Exchange è stata deprecata da Samsung in Android 9. Per i dispositivi Samsung con Android 9 e versioni successive, la configurazione di Exchange non è supportata in modalità Amministrazione dispositivo.

Impostazioni di Exchange

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Host Exchange Consenti spostamento	Se si sta utilizzando **Sentry** per controllare l'accesso e-mail, immettere il nome host del server Sentry. In alternativa, immettere l'indirizzo del server ActiveSync.* **Per iOS e Android:** selezionare questa opzione se non si desidera impedire che le e-mail vengano spostate da questo account. **Per Windows 10:** non applicabile.
Abilita S/MIME	Selezionare questa opzione per attivare il supporto della crittografia S/MIME. È possibile quindi selezionare i certificati di crittografia e firma. Richiede la memorizzazione del certificato nella cache. Assicurarsi che la memorizzazione nella cache sia abilitata nell'autorità di certificazione utilizzata dalla configurazione del certificato di identità. **iOS 10.3 e versioni successive:** Selezionare una delle seguenti opzioni per i campi **Firma S/MIME** e **Crittografia S/MIME**: • Disattivato • Attivato • Selezione utente **iOS 12.0 e versioni successive:** • Consentire all'utente di ignorare le impostazioni di firma S/MIME • Consentire all'utente di selezionare l'identità di firma S/MIME • Consentire all'utente di ignorare le impostazioni di cifratura S/MIME • Consentire all'utente di selezionare l'identità di cifratura S/MIME **Abilitare la firma e la crittografia S/MIME per messaggio**, se richiesto.
Sincronizza indirizzi e-mail recenti	Selezionare questa opzione per sincronizzare tra il dispositivo e il server gli indirizzi e-mail contattati di recente.
Utilizza solo la Posta Utilizza SSL	Selezionare questa opzione se si desidera che questa configurazione venga utilizzata solo dal client e-mail. Altre applicazioni per l'invio di e-mail, incluse le applicazioni per l'invio di contenuti tramite il client e-mail nativo, non sono in grado di utilizzare questa configurazione. Selezionare quest'opzione per utilizzare soltanto il Secure Socket Layer per le comunicazioni tra il dispositivo e il server.
Attiva OAuth per il payload Exchange Dominio	iOS 12.0 e versioni successive e macOS 10.14 e versioni successive: Selezionare questa opzione per abilitare l'autenticazione tramite OAuth. Se questa opzione è abilitata, per le app e-mail che supportano l'autenticazione tramite OAuth sono disponibili le seguenti opzioni aggiuntive: • URL accesso OAuth • URL richiesta token OAuth Immettere il dominio per questo account e-mail, a meno che non si desideri che venga richiesto all'utente.

Impostazione	Operazione da eseguire
Utente	Inserire una variabile che rappresenta l'indirizzo e-mail per questo account.*
Password dell'account	Immettere la password per questo account, a meno che non si desideri che venga richiesto all'utente.
Indirizzo e-mail	Inserire una variabile che rappresenta l'indirizzo e-mail per questo account.*
Giorni passati di posta da sincronizzare	Selezionare il numero di giorni di e-mail da sincronizzare tra il dispositivo e il server.
VPN per-app **Android e Windows**	**Prerequisito**: configurare Tunnel o la configurazione VPN per-app prima di configurare la VPN per-app nella configurazione Exchange Active Sync. Nel menu a discesa, selezionare la configurazione VPN per-app preconfigurata. **Applicabile a**: iOS 14+
Sincronizza calendario	**Per Android e Windows 10:** selezionare per sincronizzare gli elementi del calendario tra il dispositivo e il server. **Per i dispositivi Samsung:** questa impostazione non è utilizzata (è attiva per impostazione predefinita). **Per l'app E-mail+ Android:** questa impostazione viene utilizzata.
Sincronizza contatti	**Per Android e Windows 10:** selezionare per sincronizzare i contatti tra il dispositivo e il server. **Per i dispositivi Samsung:** questa impostazione non è utilizzata (è attiva per impostazione predefinita). **Per l'app E-mail+ Android:** questa impostazione viene utilizzata.
Sincronizza e-mail	**Per Android e Windows 10:** selezionare per sincronizzare le e-mail tra il dispositivo e il server. **Per i dispositivi Samsung:** questa impostazione non è utilizzata (è attiva per impostazione predefinita). **Per l'app E-mail+ Android:** questa impostazione non è utilizzata (è attiva per impostazione predefinita).
Sincronizza attività **iOS 13.0 e versioni successive**	**Per Android e Windows 10:** selezionare per sincronizzare le attività tra il dispositivo e il server. **Per i dispositivi Samsung:** questa impostazione non è utilizzata (è attiva per impostazione predefinita). **Per l'app Android Email+:** non applicabile.
• Sincronizza calendario • Sincronizza contatti • Sincronizza posta • Sincronizza note • Sincronizza promemoria	Specificare la sincronizzazione di singoli elementi di Outlook in Exchange, quali Posta, Calendario, Contatti, Note e Promemoria. Per ciascuno di questi elementi, selezionare o deselezionare le opzioni **Abilita** e **Consenti le sostituzioni da parte dell'utente**. La sincronizzazione deve essere abilitata per almeno uno di questi elementi. Se la sincronizzazione risulta disabilitata per una delle opzioni, ma tale impostazione può essere sostituita dall'utente, quest'ultimo può abilitare la sincronizzazione.

Impostazione	Operazione da eseguire
Certificato di identità **Android**	Selezionare un certificato di identità dall'elenco se si desidera che il dispositivo venga autenticato sul server tramite un certificato. I certificati vengono visualizzati in questo elenco soltanto se sono già stati configurati tramite la configurazione del certificato di identità.
Utilizza solo autenticazione basata su certificato	Utilizzare il certificato di identità selezionato come unico metodo di autenticazione sul server Exchange.
Accetta tutti i certificati SSL	Selezionare questa opzione per consentire agli utenti del dispositivo di impostare i dispositivi Android per l'accettazione di tutti i certificati SSL. Questa impostazione è valida per E-mail+ di Android e E-mail di Samsung Knox. • prestare attenzione durante l'abilitazione di questa impostazione, poiché gli utenti potrebbero esporre inconsapevolmente il dispositivo a vari attacchi. • È necessario attivare questa opzione se il certificato Sentry è un certificato autofirmato o sconosciuto.
Priorità applicazione Exchange **iOS 10 e versioni successive**	Selezionare il client e-mail da configurare per impostazione predefinita sui dispositivi Android, ad esempio Android Email+ o Samsung Email. L'app Email+ viene inclusa nell'App Catalog per tutti i tenant con priorità applicazione Exchange abilitata.
Regole servizi di comunicazione	Scegliere un'app predefinita da utilizzare per effettuare chiamate audio ai contatti all'interno del sistema CardDAV.
Solo Windows 10+	
Configura Outlook	Selezionare questa opzione per configurare Microsoft Outlook in un dispositivo. Questa opzione è supportata solo se Bridge è abilitato.

*Digitare $ per visualizzare una lista delle **variabili** supportate, se disponibili, per questo campo.

10.10.5.6. Configurazione del tipo di carattere

La configurazione del tipo di carattere consente di fornire ulteriori file carattere nei formati TrueType o OpenType ai dispositivi con iOS 7. Nella seguente tabella sono descritte le impostazioni del tipo di carattere:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Carica caratteri	Trascinare il file del tipo di carattere sulla casella tratteggiata oppure fare clic su **Scegli file** per selezionarlo dal proprio file system. I file del tipo di carattere devono essere nei formati .otf o .ttf.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.5.7. Configurazione del calendario sottoscritto

La configurazione del calendario sottoscritto consente di definire l'accesso a un calendario Web pubblico.

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
URL	Inserire l'URL per accedere al calendario.*
Utente	Immettere il nome utente da utilizzare per l'accesso.*
Password	Immettere la password da utilizzare per l'accesso.
Utilizza SSL	Selezionare quest'opzione per utilizzare soltanto il Secure Socket Layer per le comunicazioni tra il dispositivo e il server.

Digitare $ per visualizzare un elenco delle **variabili** supportate eventualmente disponibili per questo campo.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.5.8. Creare una configurazione clip Web

Una clip Web è un collegamento a un sito o a una pagina Web a cui è possibile accedere dai dispositivi iOS. Utilizzare la configurazione delle clip Web per creare delle clip Web standard sui dispositivi. È possibile aggiungere al dispositivo iOS l'icona di un clip web che avvierà un sito web specifico. Le clip web aiutano a trovare e utilizzare rapidamente i segnalibri nelle schermate iniziali dei dispositivi. È inoltre possibile controllare alcuni parametri dell'esperienza di visualizzazione di Mobile Safari per il sito.

> Per questa configurazione è disponibile l'opzione di delega con distribuzione personalizzata. Per ulteriori informazioni, vedere l'argomento *Distribuzione della configurazione* in **Utilizzo delle configurazioni**.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Fare clic su **Configurazioni**.
3. Fare clic su +**Aggiungi**.
4. Cercare e selezionare la configurazione della clip web.
5. Configurare le impostazioni su questa pagina. Fare riferimento alla tabella presente nella sezione **Impostazioni configurazione clip web** per istruzioni sui valori.
6. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
7. Selezionare **Personalizzato** quindi selezionare **Dispositivi/ Gruppi di dispositivi**.
8. Fare clic su **Fine**.

Impostazioni configurazione clip web

Nella seguente tabella sono elencate le impostazioni di configurazione clip web:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Etichetta **URL** **Rimovibile** **Icona**	Inserire il testo che si desidera visualizzare sotto il collegamento rapido sullo schermo del dispositivo.* Inserire l'URL a cui il web clip accederà.* Selezionare la casella di controllo per consentire all'utente del dispositivo di eliminare la clip web. Trascinare il file del tipo di carattere sulla casella tratteggiata oppure fare clic su **Scegli file** per selezionarlo dal proprio file system.
Icona precomposta	Selezionare quest'opzione per eliminare gli effetti speciali aggiunti dalle versioni più recenti di Safari.
Schermo intero	Selezionare quest'opzione per visualizzare la clip Web in modalità schermo intero invece che come contenuto all'interno di un browser.
Ignora ambito manifesto **Identificatore bundle applicazione destinazione**	Selezionare per consentire la navigazione verso un sito web esterno senza visualizzare il browser Safari. Questa opzione non ha effetto quando non è selezionato Schermo intero. L'identificatore del bundle dell'applicazione che specifica l'applicazione che apre l'URL. **Esempio**: com.google.chrome.ios

Digitare $ per visualizzare un elenco delle **variabili** supportate eventualmente disponibili per questo campo.

Argomenti correlati:

- **Accesso sicuro multiutente per iOS**
- **Come creare una configurazione**

10.10.5.9. Installazione di Office 365

Licenza: Silver

Applicabile a: Windows 10+

Configurazione dell'installazione di Office 365

L'installazione di Office 365 è un'impostazione di configurazione che può essere applicata a dispositivi selezionati per l'installazione o la disinstallazione di Office 365. È possibile definire le impostazioni di configurazione in formato xml utilizzando lo strumento di distribuzione di Office e quindi caricando il file. Dopo aver caricato i file, è possibile inviare le opzioni di configurazione ai dispositivi selezionati.

Procedura

1. Nella scheda **Configurazione**, fare clic su **+Aggiungi**.
2. Selezionare **Installazione di Office 365**. La pagina **Installazione di Office 365** viene visualizzata.
3. Nel campo **Nome**, digitare un nome appropriato per la configurazione.
4. Fare clic sul collegamento +**Aggiungi descrizione** per aggiungere una descrizione della configurazione. Questo campo è facoltativo.
5. Nella sezione **Impostazioni configurazione**, aggiornare i campi seguenti:

Nome del campo	Descrizione
File di configurazione per l'installazione di Office 365	Fare clic sul pulsante **Scegli file** per sfogliare e selezionare il file di configurazione in formato XML che include le impostazioni definite per l'installazione di Office 365. Esempio: <Configuration> <Add OfficeClientEdition="64" Channel="Current"> <Product ID="O365ProPlusRetail"> <Language ID="en-us"/> </Product> </Add> </Configuration> Assicurarsi che il file di configurazione sia in formato xml e che sia visualizzato un segno di spunta di colore verde una volta che il file delle impostazioni di configurazione è stato aggiunto.
File di configurazione per la disinstallazione di Office 365	Fare clic sul pulsante **Scegli file** per sfogliare e selezionare il file di configurazione in formato XML che include le impostazioni definite per la disinstallazione di Office 365. Esempio: <Configuration> <Remove All="TRUE"/><Display Level="None" AcceptEULA="TRUE" /> </Configuration> Assicurarsi che il file di configurazione sia in formato xml e che sia visualizzato un segno di spunta di colore verde una volta che il file delle impostazioni di configurazione è stato aggiunto.

6. Fare clic su **Avanti**.
7. Selezionare una qualsiasi delle opzioni seguenti per distribuire le impostazioni nei dispositivi.

Opzione	Descrizione
Abilita questa configurazione	Selezionando la casella di controllo è possibile abilitare questa configurazione nei dispositivi selezionati. Deselezionando la casella di controllo si rimuove la configurazione, se questa è già stata applicata ai dispositivi.
Tutti i dispositivi	Consente di distribuire le impostazioni in tutti i dispositivi.
Nessun dispositivo	Consente di trattenere le impostazioni da distribuire ai dispositivi.
Personalizzato	Consente di distribuire l'impostazione per un gruppo di dispositivi definito. Selezionare la casella di controllo accanto al tipo di dispositivo per il quale si desidera distribuire le impostazioni. In alternativa è possibile cercare gruppi di dispositivi digitando il nome del gruppo nel campo di ricerca **Cerca gruppi di dispositivi**. Per creare un nuovo gruppo di dispositivi, fare clic sul collegamento **Crea nuovo gruppo di dispositivi** in fondo alla pagina. Vedere **Gruppi di dispositivi** per ulteriori informazioni. Se e quando si seleziona la categoria del dispositivo, è possibile visualizzare i dettagli (**NOME**, **N. TELEFONO** e **TIPO DI DISPOSITIVO**) dell'elenco di utenti del dispositivo per la categoria di dispositivo selezionata sotto la sezione **Riepilogo distribuzione**.

8. Fare clic su **Fine** per inviare l'impostazione ai dispositivi selezionati.

10.10.5.10. Impostazioni GPO Windows

Licenza: Bridge

Applicabile a: Windows Desktop

Configurazione delle impostazioni GPO Windows GPO

Group Policy Object (GPO) è un insieme di impostazioni che definiscono le autorizzazioni consentite o non consentite ai dispositivi. Per gestire le impostazioni GPO, è necessario disporre di un'installazione di Bridge. Vedere Ivanti Bridge per ulteriori dettagli.

Contattare l'amministratore del sito se i metadati GPO non sono stati caricati nel database. La configurazione GPO viene distribuita ai dispositivi tramite script PowerShell che utilizzano Bridge. Con le impostazioni GPO è possibile configurare e inviare determinate impostazioni ai dispositivi.

Procedura

1. Nella scheda **Configurazione**, fare clic su **+Aggiungi**.
2. Selezionare la configurazione **Impostazioni GPO Windows**. Viene visualizzata la pagina **Impostazioni GPO Windows**.
3. Nel campo **Nome**, digitare un nome appropriato per le Impostazioni GPO Windows.
4. Fare clic sul collegamento +**Aggiungi descrizione** per aggiungere una descrizione per la configurazione. Questo campo è facoltativo.
5. Nella sezione **Impostazioni configurazione**, fare clic su +**Aggiungi**. Viene visualizzata la finestra **Aggiungi Group Policy Object (GPO) Windows**.
6. Cercare e selezionare un GPO facendo clic sul componente pertinente dalla struttura gerarchica GPO nel riquadro sinistro. La struttura gerarchica GPO rappresenta il percorso delle impostazioni dei criteri. In alternativa, è possibile cercare un'impostazione GPO specifica facendo clic sul nome delle impostazioni GPO nel campo di ricerca.
   Una volta selezionata un'impostazione GPO, è possibile visualizzare l'impostazione GPO selezionata nel riquadro sinistro.
7. Nel campo **Stato delle impostazioni**, sono disponibili le seguenti opzioni:

Opzione	Descrizione
Non configurata	Rimuove le impostazioni GPO esistenti.
Attivato	Attiva le impostazioni GPO.
Disattivata	Disattiva le impostazioni GPO.

8. Nel campo **Valore impostazioni**, digitare un nome appropriato da assegnare al GPO.
   Per aggiungere ulteriori valori di impostazione, fare clic sull'icona **+**. È possibile che alcune impostazioni GPO non richiedano valori delle impostazioni aggiuntivi. Alcuni possono richiedere dati aggiuntivi da specificare alla voce Valore impostazioni nel modulo del valore di testo. In tali impostazioni, selezionare qualsiasi valore dai valori disponibili nell'elenco a discesa.

> Questo campo è modificabile solo se è selezionata l'opzione **Attivata** in **Stato delle impostazioni**.

9. Fare clic su **Salva e chiudi** per salvare il GPO e chiudere la finestra. Per aggiungere un altro GPO, fare clic su **Salva e aggiungi un altro** per salvare e mantenere aperta la finestra GPO.
   L'impostazione GPO aggiunta viene visualizzata nella sezione **Impostazioni configurazione**.

È possibile modificare o eliminare un'impostazione GPO facendo clic sulle icone pertinenti nella colonna **Azioni**.

OpzioneDescrizioneAbilita questa configurazione Selezionando la casella di controllo è possibile abilitare questa configurazione nei dispositivi selezionati. Deselezionando la casella di controllo si rimuove la configurazione, se questa è già stata applicata ai dispositivi.**Tutti i dispositivi**Consente di distribuire le impostazioni in tutti i dispositivi.**Nessun dispositivo**Consente di trattenere le impostazioni da distribuire ai dispositivi.**Personalizzato**Consente di distribuire l'impostazione per un gruppo di dispositivi definito. Selezionare la casella di controllo accanto al tipo di dispositivo per il quale si desidera distribuire le impostazioni. In alternativa è possibile cercare gruppi di dispositivi digitando il nome del gruppo nel campo di ricerca **Cerca gruppi di dispositivi**. Per creare un nuovo gruppo di dispositivi, fare clic sul collegamento **Crea nuovo gruppo di dispositivi** in fondo alla pagina. Vedere **Gruppi di dispositivi** per ulteriori informazioni.

Se e quando si seleziona la categoria del dispositivo, è possibile visualizzare i dettagli (**nome**, **n. telefono** e **tipo di dispositivo**) dell'elenco di utenti del dispositivo per la categoria di dispositivo selezionata sotto la sezione **Riepilogo distribuzione**.

10. Fare clic su **Fine** per inviare l'impostazione GPO ai dispositivi selezionati.

10.10.5.11. Configurazione della crittografia BitLocker

Licenza: Bridge

Applicabile a: Windows Desktop

Argomenti della sezione:

- Configurazione della crittografia BitLocker
- Visualizzazione delle impostazioni di BitLocker

Configurazione della crittografia BitLocker

La crittografia BitLocker è una funzionalità che applica la crittografia sui dischi rigidi e rimovibili dei dispositivi per proteggere i dati. Per gestire la crittografia BitLocker è necessario disporre di un'installazione di Bridge. Per ulteriori dettagli, vedere **Bridge**. La configurazione della crittografia BitLocker aiuta a configurare le impostazioni di crittografia sui dispositivi.

Procedura

1. Nella scheda **Configurazione**, fare clic su **+Aggiungi**.
2. Selezionare la configurazione **Crittografia BitLocker**. Viene visualizzata la pagina **Crittografia BitLocker**.
3. Nel campo **Nome** digitare un nome appropriato per la Crittografia BitLocker.
4. Fare clic sul collegamento **+Aggiungi descrizione** per aggiungere una descrizione per la configurazione. Questo campo è facoltativo.
5. Nella sezione Impostazioni configurazione, configurare le impostazioni seguenti:

Impostazione	Descrizione
Metodo e tipo di crittografia	Selezionare il tipo di algoritmo di crittografia in base alle dimensioni della chiave per la crittografia. Sono disponibili le seguenti opzioni: • **AES-CBL a 128 bit** • **AES-CBL a 256 bit**
Crittografa tutte le unità hardware	Fare clic sull'interruttore per **ATTIVARE** o **DISATTIVARE** l'impostazione per crittografare tutte le unità hardware. Se un'unità hardware è già stata crittografata su un dispositivo, la modifica di questa configurazione non verrà applicata perché il processo di crittografia è irreversibile tramite la modifica.
Seleziona le unità	Selezionare le unità da crittografare. Esempio: **C:** Fare clic su **+ Aggiungi** per aggiungere più unità. Questo campo non viene visualizzato se è stata attivata l'impostazione **Crittografa tutte le unità hardware**.
Crittografia basata su hardware per tipi di unità	Il modulo TPM (Trusted Platform Module) è un chip della scheda madre del computer, che consente di eseguire una crittografia a prova di manomissione. Se si utilizza la crittografia BitLocker o la crittografia del dispositivo su un computer con TPM, parte della chiave viene memorizzata sul TPM. È possibile scegliere le seguenti opzioni di crittografia basata su hardware dall'elenco a discesa: • **Richiedi TPM all'avvio** • **Richiedi PIN di avvio con TPM** • **Non utilizzare TPM** L'opzione TPM è valida solo per le unità del sistema operativo e per la versione TPM 1.2 o successiva. Se si applica un'impostazione di crittografia basata sull'hardware a un dispositivo, non è più possibile modificare tale impostazione per il dispositivo. Se su un dispositivo è già stata impostata una configurazione BitLocker, non è possibile inviare un'altra configurazione BitLocker con un'altra opzione TPM.
Selezionare le seguenti opzioni di configurazione (facoltative): • **Nega accesso di scrittura per le unità fisse non protette da BitLocker** • **Nega accesso di scrittura per le unità rimovibili non protette da BitLocker**	

Impostazione	Descrizione
Azione dispositivi con cifratura preliminare	Selezionare una delle seguenti opzioni per definire come si desidera gestire l'unità non completamente decifrata o già dotata di una protezione con chiave. • Interrompi crittografia - Interrompe la crittografia se una qualsiasi delle unità selezionate è già stata crittografata. • Decriptare l'unità selezionata che non presenta una password di recupero memorizzata in Ivanti Neurons for MDM - Selezionare questa opzione per applicare solo alle unità che non hanno una password di recupero in Ivanti Neurons per MDM.
Opzioni di ripristino	L'opzione di ripristino viene utilizzata se un utente dimentica la password. È possibile recuperarla dalla pagina dei dettagli del dispositivo. È possibile impostare le opzioni seguenti: • **Disattiva ripristino** • **Utilizza password e memorizza in AD** • **Utilizza password e memorizza in AD e MobileIron**
Intervallo di riavvio	Dopo aver inviato la configurazione al dispositivo, è necessario riavviarlo. La crittografia viene attivata con il riavvio. Per configurare l'intervallo di riavvio, selezionare dall'elenco a discesa l'intervallo di tempo dopo il quale è necessario riavviare il dispositivo. L'intervallo minimo di riavvio è di 1 minuto, mentre l'intervallo massimo è di 120 minuti (2 ore).
Messaggio di riavvio	Digitare il messaggio di riavvio da mostrare sul dispositivo. Ove applicabile, vengono mostrati all'utente anche il PIN o la password di avvio. L'utente può annotare tali credenziali per digitarle quando richiesto dopo il riavvio.

6. Fare clic su **Avanti**.
7. Selezionare una qualsiasi delle opzioni seguenti per distribuire le impostazioni nei dispositivi.

Impostazione	Descrizione
Abilita questa configurazione	Selezionando la casella di controllo è possibile abilitare questa configurazione nei dispositivi selezionati. Deselezionando la casella di controllo si rimuove la configurazione, se questa è già stata applicata ai dispositivi.
Tutti i dispositivi	Consente di distribuire le impostazioni in tutti i dispositivi.
Nessun dispositivo	Consente di trattenere le impostazioni da distribuire ai dispositivi.
Personalizzato	Consente di distribuire l'impostazione per un gruppo di dispositivi definito. Selezionare la casella di controllo accanto al tipo di dispositivo per il quale si desidera distribuire le impostazioni. In alternativa è possibile cercare gruppi di dispositivi digitando il nome del gruppo nel campo di ricerca **Cerca gruppi di dispositivi**. Per creare un nuovo gruppo di dispositivi, fare clic sul collegamento **Crea nuovo gruppo di dispositivi** in fondo alla pagina. Vedere Gruppi di dispositivi per ulteriori informazioni. Se e quando si seleziona la categoria del dispositivo, è possibile visualizzare i dettagli (**NOME**, **N. TELEFONO** e **TIPO DI DISPOSITIVO**) dell'elenco di utenti del dispositivo per la categoria di dispositivo selezionata sotto la sezione **Riepilogo distribuzione**.

8. Fare clic su **Fine** per inviare l'impostazione ai dispositivi selezionati.

Visualizzazione delle impostazioni di BitLocker

È possibile visualizzare le impostazioni di BitLocker configurate per un dispositivo nella pagina Dettagli dispositivo (**Dispositivi>Dispositivi>[Nome dispositivo]**) nella sezione **Impostazioni BitLocker**. Per impostazione predefinita, i dettagli sono nascosti.

È possibile visualizzare i seguenti dettagli facendo clic sull'icona di visualizzazione (a forma di occhio) accanto a ciascun campo:

Impostazione	Descrizione
Password di ripristino	Se questa opzione è selezionata, la password di ripristino viene generata da Windows e restituita a Ivanti Neurons for MDM dopo l'invio della configurazione BitLocker. Se il dispositivo entra in modalità di ripristino, all'utente viene chiesto di digitare tale password. Se vengono crittografate più unità, è necessario utilizzare la stessa password di ripristino. La password di ripristino verrà pubblicata solo se è selezionata l'opzione **Utilizza password e memorizza in AD e MobileIron**.
PIN	Mostra il PIN di avvio a 6 cifre. Il PIN viene mostrato solo se è stata selezionata l'opzione **Richiedi PIN di avvio con TPM** nelle impostazioni di configurazione di BitLocker.
Password di avvio	La password di avvio impostata per il dispositivo. La password viene mostrata solo se è stata selezionata l'opzione **Non usare TPM** nelle impostazioni di configurazione di BitLocker.
Versione TPM	Mostra la versione TPM configurata.

In base alle impostazioni della configurazione di BitLocker, in alcuni campi potrebbe essere mostrato **N/D**.

- Lo stato della crittografia è mostrato sotto Stato di crittografia del dispositivo nella pagina Dettagli dispositivo.
- Verranno utilizzati lo stesso PIN o la stessa password di avvio per tutte le unità di un dispositivo per cui verrà applicata la crittografia BitLocker.
- Se si crea una configurazione per criptare una seconda unità di un dispositivo che ha già un'unità criptata e una password di ripristino salvata, la password meno recente verrà sovrascritta. Di conseguenza, si consiglia di utilizzare l'opzione Password di ripristino solo per un'unità in un dispositivo.

10.10.6. Configurazione dell'accesso alla rete aziendale

Argomenti della sezione:

- Configurazione di AirPlay
- Configurazione di AirPrint
- Configurazione VPN Always-on
- Autorizzazioni di runtime delle app predefinite
- Istruzione
- Configurazione proxy globale
- Configurazione LDAP
- Configurazione server macOS
- Configurazione relay di rete
- Tunnel
- Configurazione di AppTunnel
- Configurazione VPN per-app
- Configurazione Single Sign-On
- Accesso sicuro multiutente per iOS
- Configurazione delle impostazioni di APN Android
- Configurazione VPN
- VPN on Demand
- Configurazione Wi-Fi

10.10.6.1. Configurazione di AirPlay

Licenza: Silver

La configurazione di AirPlay consente di impostare l'accesso ai dispositivi alternativi per la visualizzazione di contenuti multimediali. Nella seguente tabella sono elencate le impostazioni di Airplay:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Lista elementi consentiti	Immettere l'ID del dispositivo di ciascuna destinazione AirPlay consentita. Se non viene fornito alcun ID, alle destinazioni AirPlay non verranno applicate delle limitazioni. **Applicabile a**: iOS 7.0+ e macOS 10.10+ (supervisionati).
Impostazioni dispositivo	Immettere l'ID dispositivo (macOS) o il nome dispositivo (iOS) e la password per ciascuna destinazione AirPlay nota.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.6.2. Configurazione di AirPrint

Licenza: Silver

La configurazione di AirPrint consente di impostare la stampa wireless. Nella seguente tabella sono elencate le impostazioni di AirPrint:

Impostazioni	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Impostazioni di AirPrint	**Indirizzo IP:** immettere l'indirizzo IP della stampante AirPrint. **Percorso risorse:** immettere il percorso risorse associato alla stampante AirPrint. Tale percorso corrisponde al parametro rp del record _ipps.tcp di Bonjour. Esempi: • printers/Canon_MG5300_series • printers/Xerox_Phaser_7600 • ipp/print • Epson_IPP_Printer. Il percorso delle risorse rileva la distinzione tra maiuscole e minuscole. **Porta:** immettere la porta in ascolto della destinazione AirPrint. Se non viene specificata, AirPrint utilizza la porta predefinita. Per dettagli sulle porte standard Apple, visitare https://support.apple.com/it-it/HT202944 **Forza TLS:** consente di abilitare la connessione protetta tramite Transport Layer Security (TLS). Per impostazione predefinita, questa opzione è disabilitata.

Dopo l'installazione della configurazione di **AirPrint** su macOS, i dettagli della stampante sono trasmessi dalla configurazione di **AirPrint** al dispositivo. Gli utenti possono visualizzare i dettagli della stampante inseriti automaticamente cliccando su Preferenze di sistema > Stampanti e scanner > +. Nella schermata **Aggiungi**, l'utente deve selezionare **Impostazione predefinita**, quindi selezionare il profilo di stampa richiesto. In questo modo la stampante richiesta viene aggiunta a **Stampanti e scanner**.

Per ulteriori informazioni, vedere Come creare una configurazione

10.10.6.3. Configurazione VPN Always-on

Licenza:

- **Gold per Android Enterprise**
- **Silver per iOS**

La configurazione VPN Always-on assicura che gli utenti si connettano automaticamente alla VPN (quando disponibile) senza dover compiere alcuna azione. Questa funzionalità richiede le versioni successive di Android 7.0 oppure le versioni successive di iOS 8, oltre a un provider VPN in grado di supportare il protocollo IKEv2.

Impostazioni VPN Always-on per Android

La configurazione VPN Always-on viene inviata ai dispositivi Android Enterprise con Android 7.0 +. Sui dispositivi gestiti con Profilo di lavoro (Android 8.0 e versioni successive), la configurazione VPN viene applicata al Profilo di lavoro.

> Quando un dispositivo viene distribuito in modalità **COSU** con **AMA** come tipo di Registrazione dispositivo, e se si esegue il push di un'app con la configurazione **Always-on** al dispositivo, verrà eseguito il push al dispositivo anche della configurazione **Always-on**.

Per abilitare questa configurazione, selezionare un'app dal Catalogo app oppure immettere il nome di un pacchetto.

Impostazioni VPN Always-on per iOS

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Usa la stessa configurazione del tunnel per cellulare e Wi-Fi	Selezionare questa opzione per definire una coppia identificatore-server per le connessioni VPN, indipendentemente dal fatto che la connessione venga stabilita su una rete cellulare o Wi-Fi.
Server	Immettere il nome host o l'indirizzo IP del server VPN.
Identificatore locale	Identificatore del client IKEv2 in uno dei formati seguenti: • FQDN • UserFQDN • Indirizzo • ASN1DN
Identificatore remoto	Identificatore remoto in uno dei formati seguenti: • FQDN • UserFQDN • Indirizzo • ASN1DN
Abilita EAP	Selezionare questa opzione per abilitare l'autenticazione estesa.
Autenticazione computer	Disponibile soltanto se l'opzione Abilita EAP non è selezionata. Selezionare una delle opzioni seguenti: • Certificato • Segreto condiviso
Autenticazione EAP	Disponibile soltanto se l'opzione Abilita EAP è selezionata. Selezionare una delle opzioni seguenti: • Certificato • Nome utente/Password
Segreto condiviso	Disponibile solo se è stata selezionata l'opzione Segreto condiviso per l'Autenticazione computer. Inserire il segreto condiviso per la connessione.
Credenziale	Disponibile solo se è stata selezionata l'opzione Certificato per l'Autenticazione computer. Selezionare il certificato da utilizzare. Questo certificato verrà inviato per l'autenticazione del client IKE. Se viene utilizzata l'autenticazione estesa, è possibile utilizzare questo certificato per EAP-TLS.
Account	Disponibile soltanto se l'opzione Nome utente/Password è stata selezionata per l'autenticazione EAP. Immettere l'ID account del server VPN.
Password	Disponibile soltanto se l'opzione Nome utente/Password è stata selezionata per l'autenticazione EAP. Immettere la password del server VPN.

Impostazione	Operazione da eseguire
Intervallo Dead Peer Detection	Selezionare una delle opzioni seguenti: • Nessuno (disattivato) • Basso (keepalive inviato ogni ora) • Medio (keepalive inviato ogni 30 minuti) • Alto (keepalive inviato ogni 10 minuti)
Algoritmo di crittografia	Selezionare una delle opzioni seguenti: • DES • 3DES • AES-128 • AES-256 • AES-128-GCM • AES-256-GCM • ChaCha20-Poly1305
Algoritmo di integrità	Selezionare una delle opzioni seguenti: • SHA1-96 • SHA1-160 • SHA2-256 • SHA2-384 • SHA2-512
Gruppo Diffie-Hellman	Selezionare il gruppo di Exchange della chiave D-H.
Durata in minuti	Inserire la durata SA (intervallo di reimpostazione della chiave) espressa in minuti. I valori validi sono compresi tra 10 e 1440.
Casella vocale	Selezionare Consenti traffico via tunnel per rendere la posta vocale esente per la VPN Always-on. Selezionare Interrompi traffico per applicare l'opzione.
Airprint	Selezionare Consenti traffico via tunnel per rendere il traffico Airprint esente per la VPN Always-on. Selezionare Interrompi traffico per applicare l'opzione.
Servizi di telefonia mobile	Selezionare Consenti traffico via tunnel per rendere il traffico dei servizi da cellulare esente per la VPN Always-on. Selezionare Interrompi traffico per applicare l'opzione.
Consenti traffico da foglio web bloccato all'esterno del tunnel VPN	Selezionare questa opzione per consentire il traffico dai fogli web bloccati all'esterno del tunnel VPN.
Consenti traffico da tutte le app di rete bloccate all'esterno del tunnel VPN	Selezionare questa opzione per consentire il traffico da tutte le app di rete bloccate all'esterno del tunnel VPN per gestire la rete bloccata.

Impostazione	Operazione da eseguire
Identificatori bundle di app di rete bloccate	Elencare gli ID dei pacchetti delle app di rete bloccate il cui traffico sarà consentito all'esterno del tunnel VPN per gestire la rete bloccata. Le app di rete bloccate potrebbero richiedere diritti aggiuntivi per funzionare in un ambiente bloccato.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.6.4. Autorizzazioni di runtime delle app predefinite

Valido per: app che hanno come target le API Android 23 o versioni successive e che eseguono Android 6.0 o versioni successive su dispositivi con Android Enterprise.

Gli amministratori possono impostare la configurazione delle autorizzazioni di runtime per le app distribuite sui dispositivi con Android enterprise. Le app che hanno come target le API 23 (o versioni successive) e che eseguono Android 6.0 o versioni successive sono in grado di chiedere le autorizzazioni agli utenti durante il runtime. La configurazione Autorizzazioni di runtime predefinite delle app permette di impostare il valore predefinito per le autorizzazioni di runtime delle app. Ivanti Neurons for MDM crea questa configurazione per impostazione predefinita. È possibile modificare questa configurazione di sistema predefinita o creare una nuova configurazione in base ai propri requisiti.

Le autorizzazioni specifiche per le app hanno la precedenza sulla configurazione delle autorizzazioni generiche delle app. Le app interne sono soggette alle autorizzazioni globali. Non è consentito impostare autorizzazioni per app per le app interne.

Impostazione delle autorizzazioni globali di runtime

Gli amministratori possono modificare le autorizzazioni di runtime predefinite delle app e la distribuzione di questa configurazione come segue:

ProcedureProcedura

1. Accedere a **Configurazioni**.
2. Eseguire una delle operazioni seguenti:
    - Per modificare la configurazione predefinita del sistema, fare clic su **Autorizzazioni di runtime delle app predefinite** e fare clic su **Modifica**.
    - Per aggiungere una nuova configurazione, fare clic su **Aggiungi > Autorizzazioni di runtime predefinite**.

Immettere un nome per la configurazione.

4. Immettere una descrizione.
5. Nella sezione Impostazioni configurazione, impostare una delle seguenti autorizzazioni di runtime predefinite:
    - Richiesta utente (opzione predefinita)
    - Concedi automaticamente
    - Nega automaticamente (da usare con cautela)

Fare clic su **Avanti**.

7. Selezionare l'opzione **Abilita questa configurazione**.

> Se si deseleziona questa opzione, la configurazione non verrà applicata ad alcun dispositivo. Sarà rimossa da tutti i dispositivi ai quali era stata applicata.

8. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)

- Personalizzato

Fare clic su **Fine**.

Impostazione delle autorizzazioni di runtime specifiche per l'app

Gli amministratori possono impostare le autorizzazioni di runtime predefinite per una singola applicazione come segue:

Procedura

1. Andare ad **App**.
2. Fare clic sul nome dell'app.
3. Fare clic su **Configurazioni delle app > Android Enterprise**.
4. Fare clic su **Aggiungi** o sul nome della configurazione per modificare una configurazione esistente.
5. Impostare le opzioni di configurazione come il nome, la descrizione e le restrizioni.
6. Nella sezione Autorizzazioni di runtime, fare clic su **Gestisci autorizzazioni**.
7. Selezionare le autorizzazioni dalla finestra visualizzata e fare clic su **Seleziona**.
   Solo le autorizzazioni pericolose valide per l'applicazione specifica sono elencate per la selezione. L'elenco completo di autorizzazioni pericolose (quali la lettura dei contatti, la ricerca degli account sul dispositivo, la scrittura nel registro delle chiamate, ecc.) è reperibile al seguente indirizzo https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups.
   - La autorizzazioni vengono applicate solo quando l'applicazione le richiede.
   - Le autorizzazioni non vengono applicate se gli utenti hanno in precedenza accettato o negato le autorizzazioni.

Nella sezione Autorizzazioni di runtime, selezionare una delle seguenti autorizzazioni di runtime predefinite:

- Predefinite/Globali (opzione predefinita)
- Concedi automaticamente
- Nega automaticamente (da usare con cautela)

Nella sezione Distribuisci configurazione di questa app, selezionare una delle seguenti opzioni di distribuzione:

- Tutti gli utenti con app
- Nessuno
- Personalizzato

Fare clic su **Salva**.

10.10.6.5. Istruzione

Licenza: Gold

Valido per: dispositivi supervisionati iOS 9.3 e versioni successive

Consente di configurare il payload di Apple Education e l'app Classroom per responsabili e membri. Nella seguente tabella sono elencate le impostazioni di Education:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Tipo di configurazione	Selezionare uno dei seguenti tipi: • Responsabile • Membro
Abilita questa configurazione	• Selezionare questa opzione per applicare la configurazione ai dispositivi selezionati. • Deselezionare questa opzione per rimuovere la configurazione da tutti i dispositivi su cui era stata applicata in precedenza.
Distribuisci	Selezionare una delle seguenti opzioni di distribuzione: • Tutti i dispositivi • Nessun dispositivo • Personalizzato

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.6.6. Configurazione proxy globale

Licenza: Silver

La configurazione proxy globale consente di impostare i dispositivi per l'inoltro di traffico HTTP a un server proxy. Nella seguente tabella sono elencate le impostazioni del proxy globale:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Tipo	Selezionare **Manuale** o **Automatico**. Se si seleziona **Manuale**, è necessario disporre del nome host e della porta del server proxy e facoltativamente di un nome utente e di una password per accedere al server proxy. Se si seleziona **Automatico**, sarà possibile immettere un URL di configurazione automatica dei proxy (PAC).
Nome host e porta	Se è stato selezionato **Manuale**, immettere il nome host e il numero di porta del server proxy.
Utente	(Facoltativo) Nome utente per l'accesso al server proxy.*
Password	(Facoltativo) Password per l'accesso al server proxy.
URL PAC	(Facoltativo) Se è stato selezionato **Automatico**, è possibile immettere l'URL del file PAC che definisce la configurazione proxy. Se quest'impostazione viene lasciata vuota, per il rilevamento dei proxy il dispositivo utilizza il protocollo WPAD (Web Proxy AutoDiscovery).
Consenti la connessione diretta se PAC non è raggiungibile	(iOS 7 e versioni successive) Selezionare quest'opzione per consentire una connessione diretta se il dispositivo non dovesse essere in grado di accedere al file PAC.
Consenti di oltrepassare il proxy per accedere a reti bloccate	(iOS 7 e versioni successive) Selezionare quest'opzione per consentire di oltrepassare il proxy per visualizzare la pagina di accesso di una rete bloccata.

Digitare $ per visualizzare un elenco delle **variabili** supportate eventualmente disponibili per questo campo.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.6.7. Configurazione proxy globale (Android)

> Applicabile solo ai dispositivi Android in modalità Proprietario dispositivo e AOSP.

La configurazione proxy globale consente di impostare i dispositivi per l'inoltro di traffico HTTP a un server proxy.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Fare clic su **Configurazioni**.
3. Fare clic su +**Aggiungi**.
4. Digitare **Globale** nel campo di ricerca, quindi fare clic su **Proxy globale**:
   Viene visualizzata la pagina Dettagli configurazione proxy globale.
5. Nella casella **Nome**, immettere un nome per la configurazione.
6. Facoltativamente, è possibile aggiungere una descrizione sulla configurazione.
7. Dall'elenco **Piattaforma**, selezionare **Android**. Viene visualizzata la sezione **Impostazioni configurazione**.
8. In Tipo, selezionare **Manuale** o **Automatico**.
   - **Manuale**
     - Immettere il **Nome host** (nome dominio/indirizzo IP) e i dettagli **Porta**.
     - In **Aggiungi esclusioni**, è possibile aggiungere più nomi host (nomi dominio/schede con caratteri jolly) che devono trovarsi nell'elenco di esclusione.
   - **Automatico**
     - Inserire l'URL PAC.
9. Fare clic su **Avanti** per configurare le impostazioni di distribuzione, quindi fare clic su **Fine**.

10.10.6.8. Configurazione LDAP

La configurazione LDAP consente di impostare l'accesso a una directory aziendale. Nella seguente tabella sono elencate le impostazioni LDAP:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Nome host	Inserire il nome dell'host del server LDAP.*
Utente	Inserire il nome utente per l'accesso all'account LDAP.*
Password	Immettere la password per l'accesso all'account LDAP.
Utilizza SSL	Selezionare quest'opzione se si desidera utilizzare SSL per la connessione al server LDAP.
Impostazioni di ricerca	Immettere almeno una voce per l'account. Ogni voce rappresenta un nodo nell'albero LDAP da cui si desidera iniziare la ricerca. Fare clic sul pulsante + per aggiungere una nuova voce, quindi modificarla. Una voce è formata dai valori seguenti: Descrizione: illustra lo scopo dell'impostazione di ricerca. Ambito: **selezionare Base, Sottoalbero** o **Un livello** per indicare l'ambito della ricerca. **Base** indica soltanto il livello del nodo, **Sottoalbero** indica il nodo e tutti i figli, **Un livello** indica il nodo e un livello di figli. Base di ricerca: il percorso concettuale alla nota specificata (ad es. ou=people, o=mycorp).
VPN per-app	**Prerequisito**: configurare Tunnel o la configurazione VPN per-app prima di configurare la VPN per-app nella configurazione LDAP. Nel menu a discesa, selezionare la configurazione VPN per-app preconfigurata. **Applicabile a**: iOS 14+
iOS 10 e versioni successive	
Regole servizi di comunicazione	Scegliere un'app predefinita da utilizzare per effettuare chiamate audio ai contatti all'interno del sistema LDAP.

Digitare $ per visualizzare un elenco delle **variabili** supportate eventualmente disponibili per questo campo.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.6.9. Configurazione server macOS

La configurazione di un server macOS determina un account del server macOS con impostazioni e tipi di account configurati. Consente all'utente di attivare Condivisione file sul server.

Applicabile a: iOS 10 e versioni successive

Configurazione del server macOS

Procedura

1. Andare in **Configurazioni > +Aggiungi**.
2. Selezionare la configurazione **Server macOS** per visualizzare la pagina per la **creazione della configurazione del server macOS**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Immettere il **Nome host** per indicare l'indirizzo del server.
6. Immettere il **Nome utente** per indicare il nome di accesso dell'utente.
7. (Facoltativo) Immettere la **Password** per l'utente.
8. (Facoltativo) Immettere la **Descrizione** per l'account.
9. (Facoltativo) In Account configurati, immettere il numero della **Porta** da utilizzare per contattare il server per l'account del dizionario Documenti. Se non si specifica il numero della porta, viene utilizzato quello predefinito.
10. Fare clic su **Avanti**.
11. Selezionare una distribuzione per la configurazione.

10.10.6.10. Tunnel

Ivanti Tunnel abilita la funzionalità VPN su dispositivi iOS, Android e Windows. Ivanti Tunnel interagisce con la piattaforma Unified Endpoint Management (UEM), Standalone Sentry e Access per proteggere l'accesso alle risorse aziendali dall'esterno della rete aziendale. La risorsa aziendale può essere in loco o nel cloud. Le piattaforme UEM sono: Ivanti EPMM e Ivanti Neurons per MDM.

> La Configurazione per app è deprecata per i dispositivi Android Enterprise. È necessario utilizzare la configurazione gestita per Ivanti Tunnel dal Catalogo app.

Informazioni sulla configurazione di Ivanti Tunnel

Le configurazioni per Ivanti Tunnel vengono create in una piattaforma UEM (Unified Endpoint Management). Ivanti Tunnel riceve la configurazione dal client UEM. Il client per Ivanti EPMM è Mobile@Work, mentre il client per Ivanti Neurons for MDM è Go.

Documentazione più recente

Per le istruzioni più recenti su Tunnel, visitare la documentazione del prodotto:

- Tunnel per Android, vedere **Guida a Ivanti Tunnel for Android**
- Tunnel for iOS, vedere **Guida a Ivanti Tunnel for iOS**
- Tunnel for macOS, vedere **Guida a Ivanti Tunnel for macOS**
- Windows Tunnel, vedere **Guida a Ivanti Tunnel per Windows**

> Ivanti Tunnel per Windows è deprecato e ora non è più supportato da Ivanti Neurons per MDM.

10.10.6.11. Configurazione di AppTunnel

AppTunnel consente di proteggere i dati delle app fornendo una sessione di protezione app per app tra il container delle singole app e la rete aziendale.

Argomenti della sezione:

- Configurazione di Sentry per l'utilizzo di AppTunnel con certificati
- Caricamento di certificati Sentry
- Configurazione di app per utilizzare AppTunnel
- Informazioni sul nome del servizio AppTunnel

Configurazione di Sentry per l'utilizzo di AppTunnel con certificati

> Alla prima installazione di Standalone Sentry, viene installato anche un certificato autofirmato. Ivanti consiglia vivamente di sostituire il certificato predefinito con un certificato di terze parti pubblicamente attendibile.

Prerequisiti

- AppTunnel dipende dalla versione più recente supportata di Sentry. Completare l'installazione di Sentry prima di iniziare le attività di configurazione di AppTunnel.
- Se si intende utilizzare un'identità SCEP:
  - Aggiungere un'autorità di certificazione locale o esterna. È richiesta l'installazione di un Connettore.
  - Aggiungere una Configurazione certificato di identità app. È la distribuzione dinamica utilizzata per configurare AppTunnel.

È possibile configurare ActiveSync e/o AppTunnel utilizzando certificati X.509 per l'autenticazione per utilizzare i server Sentry assegnati a un profilo.

Procedura

1. Andare su **Admin > Sentry**.
2. Fare clic su **+ Aggiungi profilo Sentry**.
3. Fare clic su **ActiveSync e/o AppTunnel con certificati**.
4. Fare clic su **Avanti**.
5. Usare le linee guida contenute nella seguente tabella per completare la pagina **Impostazioni globali**.

Tabella: Impostazioni globali per Amministratore > Sentry	
Impostazione	**Operazione da eseguire**
Nome	Immettere un nome con cui identificare questo profilo.
Descrizione	Immettere una descrizione con cui spiegare lo scopo di questo profilo.
Nome host e porta esterni	Immettere il nome host e la porta del Sentry.
Modalità di autenticazione dispositivo	
Usa certificato singolo per l'autenticazione a 2 fattori	Selezionare questa opzione per usare un certificato singolo per l'autenticazione. Se non si è già caricato un certificato, è possibile eseguire questa operazione nell'area visualizzata sotto l'opzione selezionata.
Seleziona certificato	Per caricare il certificato di un gruppo richiesto per l'autenticazione dei dispositivi: 1. Fare clic su **Aggiungi**. Viene visualizzata la finestra **Aggiungi certificato**. 2. Immettere il nome del certificato nel campo **Nome certificato**. 3. Immettere la password di protezione del file PKCS12. 4. Fare clic su **Scegli file** per caricare il certificato di gruppo. Assicurarsi che il formato file sia .p7b, .p12, .pfx, .pem, .der, .crt o .cer.
Abilita elenco di revoche di certificati (CRL)	Selezionare questa opzione per convalidare i certificati presentati dal dispositivo in base all'elenco di revoche di certificati (CRL, Certificate Revocation List) pubblicato dall'Autorità di certificazione.
Comportamento predefinito dei dispositivi non gestiti	
Consenti ai dispositivi non gestiti di ricevere e-mail e dati	Selezionare se non si desidera bloccare l'accesso ai dati per i dispositivi non gestiti da Ivanti Neurons per MDM.

6. Fare clic su **Avanti**.
7. Nella pagina **Configurazione server Sentry**, configurare i seguenti campi:
8. Fare clic su **Avanti**.

Tabella: Configurazione server Sentry per Amministratore > Sentry	
Impostazione	Operazione da eseguire
Protocollo Listener	Selezionare una delle seguenti opzioni di protocollo: • **Solo HTTPS** • **Solo HTTP** • **HTTPS e HTTP**
Porta Https	Immettere il numero di porta Https. Questo campo non viene visualizzato se il protocollo Listener è impostato su Solo HTTP.
Porta Http	Immettere il numero di porta Http. Questo campo non viene visualizzato se il protocollo Listener è impostato su Solo HTTPS.
Certificato/chiave server TLS di Sentry	
Usa il certificato autofirmato di Sentry	Selezionare questa opzione per utilizzare il certificato autofirmato creato dal servizio Ivanti Neurons for MDM e inviato a Sentry come parte del profilo. Questo certificato viene utilizzato per la comunicazione tra Sentry e i dispositivi mobili.
Aggiungi	Per caricare un certificato personale richiesto per l'autenticazione: 1. Fare clic su **Aggiungi**. Viene visualizzata la finestra **Aggiungi certificato**. È possibile visualizzare questa opzione solo se si deseleziona l'opzione **Usa il certificato autofirmato** di Sentry. 2. Immettere il nome del certificato nel campo **Nome certificato**. 3. Immettere la password di protezione del file PKCS12. 4. Fare clic su **Scegli file** per caricare il certificato. Assicurarsi che il formato del file sia .p12. 5. Fare clic su **Aggiungi**. Tutti i certificati server TLS caricati (inclusi quelli caricati dalla pagina principale di Sentry e da altri profili) vengono visualizzati nella sezione Certificato/chiave server TLS di Sentry. Per selezionare il certificato TLS richiesto per l'autenticazione, fare clic sul pulsante di opzione accanto al certificato.
Aggiungi secondo certificato	Selezionare per abilitare il secondo certificato. Quando il certificato primario scade, Sentry passa automaticamente al certificato di riserva senza l'intervento dell'amministratore. Tunnel memorizza già entrambi i certificati ed è in grado di abbinarli, garantendo una connettività ininterrotta.
Protocolli	Selezionare i protocolli in entrata e in uscita richiesti.
Pacchetti di crittografia	La crittografia viene utilizzata nella comunicazione crittografata con SSL con il server Sentry. In genere, è preferibile l'utilizzo della crittografia avanzata. La crittografia debole può essere richiesta per i dispositivi

Tabella: Configurazione server Sentry per Amministratore > Sentry	
	meno recenti. La crittografia forte è selezionata per impostazione predefinita. Selezionare la crittografia aggiuntiva da utilizzare. È necessario selezionare almeno una crittografia.

9. Aggiungere almeno uno dei servizi visualizzati.
10. Fare clic su **Salva**.

Dopo aver registrato un server Sentry, quest'ultimo viene visualizzato nella pagina Sentry della sezione Server Sentry non configurati. Per assegnare un profilo al server Sentry, fare clic su **Assegna** nella colonna **Azioni**.

Caricamento di certificati Sentry

Ivanti Neurons per MDM carica i certificati del server TLS e i certificati di gruppo quando si crea un profilo Sentry. È inoltre possibile caricare questi certificati dalla pagina **Sentry** nella sezione **Certificati Sentry**.

Ivanti Neurons convalida i certificati Sentry al momento del caricamento, restituendo i seguenti tipi di informazioni a seconda delle condizioni trovate nei certificati:

Condizione	Tipo di informazioni
Il certificato leaf non contiene una catena verso un'autorità di certificazione o non esiste alcuna autorità di certificazione nel file caricato.	Errore
Non è disponibile un'autorità di certificazione root.	Avviso
L'autorità di certificazione root non ha firmato l'autorità di certificazione intermedia per il certificato leaf.	Avviso

Ivanti Neurons per MDM viene convalidato anche rispetto alle regole in **questo articolo**.

Procedura

1. Nella sezione **Certificati server TLS**, fare clic su **Aggiungi**. Viene visualizzata la finestra **Aggiungi certificato**.
2. Immettere il nome del certificato nel campo **Nome certificato**.
3. Immettere la password di protezione del file PKCS12.
4. Fare clic su **Scegli file** per caricare il certificato di gruppo. Assicurarsi che il formato file sia .p7b, .p12, .pfx, .pem, .der, .crt o .cer.
5. Fare clic su **Aggiungi**. Il certificato caricato viene visualizzato nella tabella.
6. Per eliminare il certificato server TLS, fare clic sull'icona Elimina nella colonna **Azioni**.

> Se il certificato del server TLS è utilizzato in un profilo Sentry, non sarà possibile eliminare il certificato. Se l'azione di eliminazione viene eseguita, viene visualizzato un messaggio di errore.

Aggiungere certificati di gruppo

Procedura

1. Nella sezione **Certificati di gruppo**, fare clic su **Aggiungi**. Viene visualizzata la finestra **Aggiungi certificato**.
2. Immettere il nome del certificato nel campo **Nome certificato**.
3. Immettere la password di protezione del file PKCS12.
4. Fare clic su **Scegli file** per caricare il certificato di gruppo. Assicurarsi che il formato file sia .p7b, .p12, .pfx, .pem, .der, .crt o .cer.
5. Fare clic su **Aggiungi**.

Per eliminare il certificato di gruppo caricato, fare clic sull'icona Elimina nella colonna **Azioni**.

Modifica del certificato radice Sentry

L'amministratore ha la possibilità di modificare la distribuzione della configurazione del certificato radice di Sentry. È anche possibile fornire l'autorizzazione di modifica all'amministratore dello spazio personalizzato, delegando la configurazione ad altri spazi.

1. Accedere a **Configurazioni**.
2. Cercare il **Certificato Root di Sentry**.
3. Fare clic sull'icona Modifica.
4. Selezionare le caselle di controllo corrispondenti ai dispositivi o ai gruppi di dispositivi a cui distribuire il certificato. In alternativa, deselezionare le caselle di controllo corrispondenti ai dispositivi o ai gruppi di dispositivi.
5. Selezionare una delle seguenti opzioni dalla sezione Riepilogo distribuzione, a seconda dei casi:
   - **Non applicare ad altri spazi**
   - **Applica ai dispositivi negli altri spazi**
6. (Facoltativo) Fare clic sulla casella di controllo **Consenti all'amministratore dello spazio di modificare la distribuzione**.
7. Fare clic su **Salva**.
8. Viene visualizzato un messaggio di avviso. Fare clic su **Sì** per confermare.

Configurazione di app per utilizzare AppTunnel

Per le istruzioni più recenti per Sentry, visitare la pagina della **documentazione dei prodotti** e fare clic su Sentry. Selezionare il documento appropriato per la versione di Sentry desiderata.

Informazioni sul nome del servizio AppTunnel

Un servizio AppTunnel definisce il servizio di backend verso cui un'app AppConnect esegue il tunneling.

Per le istruzioni più aggiornate, visitare la pagina della **Documentazione dei prodotti** e selezionare i documenti appropriati per le versioni di **Sentry** e **AppConnect** in uso.

10.10.6.12. Configurazione VPN per-app

Licenza: Silver

Applicabile a: dispositivi iOS, watchOS, visionOS e tvOS

La configurazione VPN per-app consente di definire le impostazioni dell'accesso VPN per le seguenti app specifiche:

- Impostazioni VPN per-app
- Psec (Cisco)
- Cisco AnyConnect
- Juniper SSL
- VPN NetMotion
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- SSL personalizzato
- Palo Alto Networks GlobalProtect

> La configurazione VPN per-app dipende dalla configurazione dell'app. La configurazione VPN per-app viene creata durante l'impostazione della configurazione dell'app. Se si elimina o si annulla la distribuzione della configurazione VPN per-app, la configurazione dell'app smette di funzionare correttamente e disconnette l'app dalla rete.

Distribuzione della configurazione

A partire dalla versione 91 di Ivanti Neurons for MDM, gli amministratori globali possono delegare gli amministratori di spazi per modificare l'opzione Configurazione VPN per app per tutti i dispostivi e per la distribuzione personalizzata. Per la Configurazione VPN per app, è possibile selezionare l'opzione Consenti che questa configurazione sia disponibile in tutti gli spazi.

> Le modifiche alla distribuzione sono applicabili solo allo spazio specifico. Tutti gli altri spazi continuano a ereditare le impostazioni di distribuzione predefinite.

Specificare le impostazioni di configurazione nei campi utilizzando le informazioni delle tabelle seguenti, a seconda dei casi, e quindi distribuire la configurazione:

Per ulteriori informazioni, vedere l'argomento *Distribuzione della configurazione* in Utilizzo delle configurazioni.

Impostazioni VPN per-app

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Tipo connessione Abilità VPN on demand	Selezionare il tipo di VPN da configurare. Le impostazioni rimanenti dipendono da questa selezione. Selezionare quest'opzione per utilizzare questa configurazione per i domini e i nomi host che stabiliscono una connessione VPN on demand.
Abilita regole iOS (applicabile se viene selezionato Abilità VPN on demand)	Per iOS e macOS, è possibile configurare: • Le regole di rete che permettono o vietano le connessioni e permettono o ignorano le reti considerate vere. • Le regole di connessione che permettono se necessario o non permettono mai le connessioni alle reti considerate vere. Per le regole di rete, è possibile specificare i seguenti tipi di parametri: • Corrispondenza dominio DNS • Corrispondenza indirizzo server DNS • Corrispondenza SSID • Probe stringa URL • Corrispondenza tipo di interfaccia Per le regole di connessione, è possibile specificare i seguenti tipi di parametri: • Corrispondenza dominio DNS • Corrispondenza indirizzo server DNS • Corrispondenza SSID • Probe stringa URL • Corrispondenza tipo di interfaccia • Domini • Server DNS • Probe URL
App corrispondente on demand attivata Abilitare il sezionamento della rete 5G	Selezionare questa opzione per abilitare la VPN on demand per-app. Selezionare **DNN** (Data Network Name fornito dal provider di rete) per eseguire il tunnel, mirando alla specifica sezione della rete mobile VPN. Selezionare **Categoria app** (fornito dal provider di rete), per identificare il tipo di sezione della rete mobile da collegare al tunnel.
Domini	

Impostazione	Operazione da eseguire
Domini Safari (iOS) **iOS 14.0 e versioni successive e macOS 11.0 e versioni successive**	Una matrice in cui ciascuna delle voci deve specificare un dominio che attiva la connessione VPN in Safari. Il formato dei domini immessi deve corrispondere a www.apple.com.
Domini associati	Specificare uno o più domini associati. Le connessioni ai server all'interno di uno di questi domini sono associate con la VPN per-app.
Domini esclusi **iOS 13 e versioni successive e macOS 10.15 e versioni successive**	Specificare uno o più domini esclusi. Le connessioni ai server all'interno di uno di questi domini sono escluse dalla VPN per-app.
Domini e-mail	Fare clic su **+ Aggiungi** per immettere uno o più domini che attiveranno la connessione VPN in E-mail. Il formato dei domini immessi deve corrispondere a www.apple.com.
Domini contatti Domini calendario **iOS 9 e versioni successive**	Fare clic su **+ Aggiungi** per immettere uno o più domini che attiveranno la connessione VPN in Contatti. Il formato dei domini immessi deve corrispondere a www.apple.com. Fare clic su **+ Aggiungi** per immettere uno o più domini che attiveranno la connessione VPN in Calendario. Il formato dei domini immessi deve corrispondere a www.apple.com.
Tipo di provider (iOS 9 e versioni successive)	Selezionare uno dei seguenti provider per il tunneling: • app-proxy: effettua il tunneling del traffico a livello di app. Per una panoramica del provider proxy delle app, consultare la **documentazione Apple**. • packet-tunnel: effettua il tunneling del traffico a livello di IP. Per una panoramica del provider per il tunneling dei pacchetti, consultare la **documentazione Apple**.

IPsec (Cisco)

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione computer	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Includi PIN utente	Selezionare quest'opzione per richiedere all'utente di immettere un codice PIN.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. **Se si seleziona Manuale,** saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. **Se si seleziona Automatico,** saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

Cisco AnyConnect

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Gruppo	Immettere il gruppo da utilizzare per autenticare la connessione.
Autenticazione dell'utente	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

Juniper SSL

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Area di autenticazione	Immettere l'area di autenticazione da utilizzare per l'autenticazione della connessione.
Ruolo	Immettere il ruolo di autenticazione da utilizzare per l'autenticazione della connessione.
Autenticazione dell'utente	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

VPN NetMotion

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione dell'utente	**Certificato** è il metodo di autenticazione dell'utente da utilizzare. È disponibile il campo seguente: **Credenziale**: selezionare il certificato di identità da utilizzare. I certificati forniti dall'utente sono supportati solo per i dispositivi iOS.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy. Selezionare le opzioni seguenti: • Abilita VPN on demand - Aggiungere domini e nomi host che stabiliscono una connessione VPN on demand. • Abilita regole iOS. • App corrispondente on demand attivata.
Domini Safari	Fare clic su **+ Aggiungi** per aggiungere domini Safari.
Tipo di provider (iOS 9.0 e versioni successive)	Come tipo di provider predefinito per il tunneling è selezionata l'opzione **Tunneling pacchetti**. Per una panoramica del provider per il tunneling dei pacchetti, consultare la documentazione Apple.

F5 SSL

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione dell'utente	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

SonicWALL Mobile Connect

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Gruppo o dominio di accesso	Immettere il gruppo o il dominio di accesso da utilizzare per l'autenticazione della connessione.
Autenticazione dell'utente	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

Aruba VIA

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione dell'utente	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

SSL personalizzato

Impostazione	Operazione da eseguire
Identificatore	Immettere l'identificatore per questo SSL VPN personalizzato in formato DNS inverso (ad esempio com.lamiaazienda.ilmioserver).
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Dati personalizzati	Immettere le coppie chiave-valore che definiscono i dati personalizzati per questo VPN.
Autenticazione dell'utente	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.
(iOS 9.0+) Includere ProviderType nel dizionario VPN principale e secondario	Scegliere di includere il tipo di provider durante la generazione di un plist (file di configurazione predefinito).
Fornisci identificativo bundle	Inserire l'identificativo del bundle del provider VPN. È possibile mantenere più Config app per la stessa app con diversi identificativi bundle del provider.

Palo Alto Networks GlobalProtect

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.
Dati personalizzati	Immettere le coppie chiave-valore che definiscono i dati personalizzati per questo VPN.
Autenticazione dell'utente	Il certificato è il metodo di autenticazione dell'utente. Selezionare un certificato di identità da utilizzare nel campo **Credenziale**.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

Digitare $ per visualizzare un elenco delle **variabili** supportate eventualmente disponibili per questo campo.

Argomenti correlati:

Come creare una configurazione

10.10.6.13. Configurazione Single Sign-On

Ivanti Neurons per MDM consente la funzionalità Single Sign-On (SSO) estendibile con le configurazioni SSO estendibile e SSO estendibile Kerberos. L'implementazione richiede un'estensione dell'app, come ad esempio Microsoft Authenticator, dal provider di identità. Con l'implementazione di SSO estendibile, gli utenti devono autenticarsi una sola volta quando accedono alle risorse aziendali. Agli utenti non viene richiesto di autenticarsi per gli accessi successivi. Per informazioni sulle informazioni di configurazione del provider di identità previsto, vedere **Configurare il provider di identità**.

Argomenti della sezione:

- **Impostazioni dell'account Single Sign-On**
- **Impostazioni dell'account Single Sign-On estendibile**
- **Impostazioni dell'account Kerberos di Single Sign-On estendibile**

Impostazioni dell'account Single Sign-On

Applicabile a:

- iOS 7.0 fino alla versione più recente supportata da Ivanti Neurons per MDM.
- visionOS 1.1 fino alla versione più recente supportata da Ivanti Neurons per MDM.

Utilizzare le seguenti impostazioni per configurare l'SSO aziendale basato su Kerberos per qualsiasi app gestita e il browser Apple Safari su dispositivi iOS.

> Questa configurazione richiede Tunnel e Sentry. Per ulteriori informazioni, vedere "Configurazione del single sign-on con Kerberos" nella *Guida a Tunnel for iOS*.

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Nome utente	Inserire il nome principale Kerberos.
Nome area di identificazione Kerberos	Inserire il nome area di identificazione Kerberos.
Certificato	**Per dispositivi iOS 8 con licenza Gold**: selezionare il certificato da utilizzare per rinnovare le credenziali Kerberos.
Prefissi corrispondenti URL	Elenco dei prefissi URL per cui deve esistere una corrispondenza per consentire l'utilizzo di questo account per l'autenticazione Kerberos su HTTP.
Elenco delle applicazioni consentite per l'SSO	Aggiungere le app desiderate dall'App Catalog all'elenco delle applicazioni consentite per l'SSO. Ad esempio, inserire "Safari" per aggiungere Apple Safari. Quando si utilizza una configurazione di questo tipo, se l'elenco delle applicazioni consentite per l'SSO non contiene alcuna app, tutte le app che supportano l'SSO in iOS possono utilizzare l'SSO, incluse le app iOS integrate.

Impostazioni dell'account Single Sign-On estendibile

Applicabile a:

- iOS 13.0 fino alla versione più recente supportata da Ivanti Neurons per MDM.
- macOS 10.15 fino alla versione più recente supportata da Ivanti Neurons per MDM.
- visionOS 1.1 fino alla versione più recente supportata da Ivanti Neurons per MDM.

Utilizzare le seguenti impostazioni per configurare il profilo dell'estensione SSO con il tipo di estensione generica per abilitare SSO per le app e i siti Web nativi con vari metodi di autenticazione.

> L'SSO estendibile non funziona quando la configurazione viene inviata nel canale utente per i dispositivi macOS 10.15.x.

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Scegli il tipo di SSO	Selezionare uno dei seguenti tipi di SSO: • **Credenziali** ◦ Inserire uno o più nomi **Host** o nomi di dominio che possono essere autenticati tramite l'estensione dell'app. I nomi host o di dominio sono abbinati senza la distinzione tra maiuscole e minuscole, e tutti i nomi di host/dominio di tutti i payload di SSO estendibile installati devono essere univoci. Gli host che iniziano con un "." sono suffissi jolly e corrisponderanno a tutti i sottodomini, altrimenti l'host deve essere una corrispondenza esatta. ◦ Inserire il nome dell'**area di autenticazione**. Questo valore deve essere adeguatamente in maiuscolo. • **Reindirizza** ◦ Inserire uno o più prefissi **URL** di provider di identità per cui l'estensione dell'app esegue l'SSO. Gli URL devono iniziare con http:// o https://, lo schema e il nome host sono abbinati senza distinzione tra maiuscole e minuscole, i parametri di query e i frammenti di URL non sono consentiti, e gli URL di tutti i payload di SSO estendibile installati devono essere univoci.
Identificatore dell'estensione	Inserire l'identificativo del bundle dell'estensione dell'app che esegue SSO per gli URL specificati.
Identificatore del team	L'identificatore del team dell'estensione dell'app. Questa chiave è richiesta su macOS e ignorata altrove.
Dati personalizzati	Inserire uno o più dati personalizzati come coppie chiave-valore.
Metodo di autenticazione (Applicabile solo a macOS 13+)	• Password • Chiave enclave sicura utente
Token di registrazione	Inserire il token. Questo campo è abilitato quando si seleziona uno dei Metodi di autenticazione.

Impostazione	Descrizione
Comportamento schermo bloccato (applicabile a iOS 15.0+ e macOS 12.0+)	Selezionare una delle seguenti opzioni: • **Annulla**: il sistema annulla le richieste di autenticazione quando lo schermo è bloccato. • **Non gestire**: la richiesta di autenticazione continua senza SSO quando lo schermo è bloccato.
Identificatori bundle negati (applicabile a iOS 15.0+ e macOS 12.0+)	Consente di aggiungere più identificatori di bundle di app che non utilizzano l'SSO fornito da questa estensione. Ad esempio, *com.company.appname.www*.

Applicabile a: macOS 14.0 fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.

Impostazione	Descrizione
Nome visualizzato account	Inserire un nome per l'account che verrà visualizzato nelle notifiche e nelle richieste di autenticazione.
Gruppi aggiuntivi	Inserire il nome dei gruppi che non avranno accesso amministratore.
Gruppi amministratore	Inserire il nome del gruppo che avrà accesso amministratore.
Metodo di autenticazione	Selezionare uno dei metodi di autenticazione dall'elenco a discesa: • Password • Chiave enclave sicura utente • Smart Card
Gruppi di autorizzazione	Inserire il diritto di autorizzazione per un nome di gruppo.
Abilita autorizzazione	Selezionare la casella di controllo per abilitare le richieste di autorizzazione per i gruppi di amministratori, i gruppi di autorizzazione o i gruppi aggiuntivi.
Abilita creazione utente all'accesso	Selezionare la casella di controllo per abilitare la creazione di nuovi utenti durante il login utilizzando una password o una smart card come metodo di autenticazione.
Frequenza di accesso	La durata, in secondi, fino a quando il sistema richiede un login completo invece di un aggiornamento. Il valore predefinito è 64.800 (18 ore). Il valore minimo è 3.600 (1 ora).
Modalità di autorizzazione nuovo utente	Selezionare uno dei metodi di autenticazione per un nuovo utente dall'elenco a discesa: • Standard: l'account è per un utente standard. • Amministratore: il sistema aggiunge l'account al gruppo dell'amministratore locale. • Gruppi: il sistema raggruppa automaticamente il nuovo utente nel gruppo amministratore, nel gruppo di autorizzazione o nel gruppo aggiuntivo.
Mappatura da token a utente	Inserire il nome dell'account e il nome completo dei nuovi utenti per mapparli ai fini dell'autorizzazione.
Modalità autorizzazione utente	Selezionare uno dei metodi di autenticazione per un utente dall'elenco a discesa: • Standard: l'account è per un utente standard. • Amministratore: il sistema aggiunge l'account al gruppo dell'amministratore locale. • Gruppi: il sistema raggruppa automaticamente il nuovo utente nel gruppo amministratore, nel gruppo di autorizzazione o nel gruppo aggiuntivo.
Utilizza chiavi dispositivo condivise	Selezionare la casella di controllo per abilitare lo stesso login e le stesse chiavi di crittografia per tutti gli utenti.

Applicabile a: macOS 15.4 fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.

Impostazione	Descrizione
Consenti attestazione identificatore dispositivo	Selezionare la casella di controllo per includere l'UDID e il numero di serie del dispositivo negli attestati SSO della piattaforma, consentendo il tracciamento dei dispositivi registrati nel backend.

Applicabile a: macOS 14.0 fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.

Per visualizzare le impostazioni dell'account Extensible single sign-on, selezionare l'opzione a discesa come **Password** nel campo **Metodo di autenticazione**.

Impostazione	Descrizione
Criterio FileVault	Abilitare il criterio per visualizzare le seguenti impostazioni: • Tentativo di autenticazione • Richiedi autenticazione Selezionare la casella di controllo **Richiedi autenticazione** per attivare ulteriori impostazioni di configurazione. • Consenti periodo di tolleranza offline • Consenti Periodo di tolleranza di autenticazione
Criterio di login	Abilitare il criterio per visualizzare le seguenti impostazioni: • Tentativo di autenticazione • Richiedi autenticazione Selezionare la casella di controllo **Richiedi autenticazione** per attivare ulteriori impostazioni di configurazione. • Consenti periodo di tolleranza offline • Consenti Periodo di tolleranza di autenticazione
Sblocca criterio	Abilitare il criterio per visualizzare le seguenti impostazioni: • Tentativo di autenticazione • Richiedi autenticazione Selezionare la casella di controllo **Richiedi autenticazione** per attivare ulteriori impostazioni di configurazione. • Consenti periodo di tolleranza offline • Consenti Periodo di tolleranza di autenticazione • Consenti TouchID o Watch per lo sblocco
Periodo di tolleranza di autenticazione	Immettere l'intervallo di tempo dopo la selezione di uno dei criteri per l'utilizzo di account locali non registrati. Se si seleziona la casella di controllo **Consenti periodo di tolleranza autenticazione** in uno dei criteri, questo diventa un campo obbligatorio.
Periodo di tolleranza offline	Inserire l'intervallo di tempo dopo la selezione di uno dei criteri per l'utilizzo di una password dell'account locale offline dopo un accesso riuscito a Platform SSO. Se si seleziona la casella di controllo **Consenti periodo di tolleranza offline** in uno dei criteri, questo diventa un campo obbligatorio.
Account SSO non di piattaforma	Selezionare **+ Aggiungi** per inserire l'elenco dei nomi utente non soggetti ai criteri FileVault, Accesso o Sblocco.

Impostazioni dell'account Kerberos di Single Sign-On estendibile

Applicabile a:

- iOS 13.0 fino alla versione più recente supportata da Ivanti Neurons per MDM.
- macOS 10.15 fino alla versione più recente supportata da Ivanti Neurons per MDM.

- visionOS 1.1 fino alla versione più recente supportata da Ivanti Neurons per MDM.

Utilizzare le seguenti impostazioni per configurare un'estensione dell'app che esegue SSO con l'estensione Kerberos.

> Kerberos SSO estendibile non funziona quando la configurazione viene inviata nel canale utente per i dispositivi macOS 10.15.x.

Impostazione	Descrizione
Impostazioni di base	
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Nome utente	Inserire il nome principale Kerberos.
Area di autenticazione	Inserire il nome area di identificazione Kerberos.
Certificato	Selezionare il certificato da utilizzare per rinnovare le credenziali Kerberos.
Prefissi URL	Elenco dei prefissi URL per cui deve esistere una corrispondenza per consentire l'utilizzo di questo account per l'autenticazione Kerberos su HTTP.
Impostazioni avanzate	
Consenti accesso automatico	Se ha valore false, le password non possono essere salvate nel portachiavi. Di default questa opzione è abilitata.
Ritarda configurazione utente	Se ha valore true, non richiede all'utente di configurare l'estensione Kerberos finché l'amministratore non la abilita con lo strumento app-sso o non si riceve una sfida Kerberos. Questa opzione è applicabile a macOS 11 fino all'ultima versione supportata da Ivanti Neurons per MDM.
Richiede la presenza dell'utente	Se ha valore true, richiede all'utente di fornire Touch ID, Face ID o il proprio passcode per accedere al portachiavi.
Monitora cache credenziali	Se ha valore false, la credenziale è richiesta in occasione della successiva sfida Kerberos corrispondente o della modifica dello stato della rete. Se la credenziale è scaduta o mancante, ne verrà creata una nuova. Questa opzione è applicabile a macOS 11 fino all'ultima versione supportata da Ivanti Neurons per MDM. Di default questa opzione è abilitata.
Nome della cache	Immettere il nome GSS (Generic Security Service) della cache Kerberos da utilizzare. Questa opzione è attualmente deprecata.
Mappatura area di autenticazione dominio	Immettere il nome dell'area di autenticazione come chiave. Il valore è una matrice di suffissi DNS che mappano all'area di autenticazione. Fare clic su **+ Aggiungi** per aggiungere una o più coppie chiave-valore.
Area di autenticazione predefinita	Questa proprietà specifica che si tratta dell'area di autenticazione predefinita se è presente più di una configurazione dell'estensione Kerberos.

Impostazione	Descrizione
Usa la scoperta automatica del sito	Se ha valore false, l'estensione Kerberos non usa automaticamente LDAP e DNS per determinare il nome del sito AD. Di default questa opzione è abilitata.
Codice del sito	Immettere il nome del sito Active Directory che l'estensione Kerberos deve usare.
Tempo di replica	Inserire il tempo, in secondi, richiesto per replicare le modifiche nel dominio Active Directory. L'estensione Kerberos lo userà al momento di verificare l'età della password dopo una modifica. Questa opzione è applicabile a macOS 11 fino all'ultima versione supportata da Ivanti Neurons per MDM. Questa opzione è attualmente deprecata.
ACL ID bundle credenziali	Fare clic su **+ Aggiungi** per aggiungere un elenco di ID bundle consentiti per accedere al Ticket Granting Ticket (TGT) per l'autenticazione.
Includi le app gestite nell'ACL ID bundle	Se ha valore true, l'estensione Kerberos consentirà solo alle app gestite di accedere e usare la credenziale. Questo è in aggiunta all'ACL ID bundle credenziali, se specificato. Questa opzione è applicabile a iOS 14 o alle versioni più recenti supportate di Ivanti Neurons per MDM.
Includi app Kerberos in ACL ID bundle	Se vero, l'estensione Kerberos consente alle utility Kerberos standard, tra cui Ticket Viewer e klist, di accedere all'utilizzo della credenziale. Disponibile su macOS 12 e versioni successive.
Etichetta nome utente personalizzata	Inserire l'etichetta del nome utente personalizzato utilizzato nell'estensione Kerberos al posto di "Nome utente". Ad esempio, "ID azienda". Questa opzione è applicabile a macOS 11 fino all'ultima versione supportata da Ivanti Neurons per MDM.
Testo guida	Inserire il testo da mostrare all'utente nella parte inferiore della finestra di accesso di Kerberos. Può essere usato per mostrare informazioni di assistenza o il disclaimer. Questa opzione è applicabile a iOS 14 e macOS 11 fino all'ultima versione supportata da Ivanti Neurons per MDM.
Modalità di utilizzo delle credenziali	Questa impostazione influisce su come la credenziale dell'estensione Kerberos viene utilizzata da altri processi. Utilizzare una delle seguenti opzioni: • Sempre (default) - La credenziale dell'estensione sarà sempre utilizzata se il nome principale del servizio (SPN) corrisponde alla matrice degli host dell'estensione Kerberos. La credenziale non sarà utilizzata se l'app chiamante non è in credentialBundleIDACL. • Quando non specificato - La credenziale sarà utilizzata solo quando un'altra credenziale non è stata specificata dal chiamante e l'SPN corrisponde alla matrice degli host dell'estensione Kerberos. La credenziale non sarà utilizzata se l'app chiamante non è in credentialBundleIDACL. • Kerberos predefinito - Viene utilizzato il processo Kerberos predefinito per la selezione delle credenziali, che normalmente utilizza la credenziale Kerberos predefinita. Ciò equivale a disattivare questa funzionalità. (Facoltativo) Selezionare **Richiedi TLS per LDAP**.
Centri di distribuzione chiavi preferiti	Aggiungere i propri centri di distribuzione chiavi preferiti. Per aggiungere un centro di distribuzione chiavi preferito, fare clic su **+Aggiungi**.

Impostazione	Descrizione
	Consenti fallback dell'autorizzazione della piattaforma SSO - Se True e se Usa TGT piattaforma SSO è true, consente all'utente di accedere manualmente. Disponibile su macOS 13 e versioni successive **Esegui solo Kerberos** - Se True, l'estensione Kerberos gestisce solo le richieste Kerberos. Disponibile su macOS 13 e versioni successive. **Usa TGT piattaforma SSO** - Se True, questa configurazione utilizza un TGT dalla piattaforma SSO invece di richiederne uno nuovo. Disponibile su macOS 13 e versioni successive.
Configura Passa alla modalità password	Se vero, consente all'utente di passare alla modalità Password dell'interfaccia utente. Disponibile su macOS 15 e versioni successive.
Configura Passa alla modalità Smart Card	Se vero, consente all'utente di passare alla modalità Smart Card dell'interfaccia utente. Disponibile su macOS 15 e versioni successive.
Configura Inizia in modalità Smart Card	Se vero, l'interfaccia utente si avvia in modalità Smart Card. Disponibile su macOS 15 e versioni successive.
Filtro selezione automatica emittente di identità	Filtra l'elenco delle Smart Card disponibili. Disponibile su macOS 15 e versioni successive.
Impostazioni password	
Consenti modifica della password	Se ha valore false, disattiva le modifiche della password. Questa opzione è applicabile a macOS 10.15 fino all'ultima versione supportata da Ivanti Neurons per MDM. Di default questa opzione è abilitata.
URL modifica password	Inserire l'URL da lanciare nel browser Web predefinito dell'utente quando questo avvia una modifica della password. Questa opzione è applicabile a macOS 10.15 fino all'ultima versione supportata da Ivanti Neurons per MDM.
Consenti complessità della password	Se è vero, le password devono soddisfare la definizione di "complesso" di Active Directory. Questa opzione è applicabile a macOS 10.15 fino all'ultima versione supportata da Ivanti Neurons per MDM.
Lunghezza minima della password	Inserire la lunghezza minima (in caratteri) delle password nel dominio. Questa opzione è applicabile a macOS 10.15 fino all'ultima versione supportata da Ivanti Neurons per MDM.

Impostazione	Descrizione
Notifica scadenza password	Inserire il numero di giorni prima della scadenza della password in cui una notifica di scadenza della password sarà inviata all'utente. Questa opzione è applicabile a macOS 10.15 fino all'ultima versione supportata da Ivanti Neurons per MDM. Il valore predefinito è di 15 giorni.
Sostituzione scadenza password	Inserire il numero di giorni in cui le password possono essere usate in questo dominio. Per la maggior parte dei domini, può essere calcolato automaticamente. Questa opzione è applicabile a macOS 10.15 fino all'ultima versione supportata da Ivanti Neurons per MDM. (Questa opzione è attualmente deprecata)
Testo richiesto per la password	Inserire la versione del testo dei requisiti della password del dominio. Utilizzabile solo se pwReqComplexity o pwReqLength non sono specificati. Questa opzione è applicabile a macOS 10.15 fino all'ultima versione supportata da Ivanti Neurons per MDM.
Conteggio cronologia password	Inserire il numero di password precedenti che non possono essere usate in questo dominio. Questa opzione è applicabile a macOS 10.15 fino all'ultima versione supportata da Ivanti Neurons per MDM.
Età minima della password	Inserire l'età minima delle password (in giorni) prima che possano essere modificate in questo dominio. Questa opzione è applicabile a macOS 10.15 fino all'ultima versione supportata da Ivanti Neurons per MDM.
Consenti sincronizzazione della password locale	Se ha valore false, disattiva la sincronizzazione della password. Questo non funziona se l'utente è connesso con un account mobile. Questa opzione è applicabile a macOS 10.15 fino all'ultima versione supportata da Ivanti Neurons per MDM.
Dati RTF requisito password	Versione in formato file RTF dei requisiti di password del dominio. Disponibile su macOS 15 e versioni successive. Utilizzabile solo se pwReqComplexity o pwReqLength non sono specificati.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.6.14. Configurazione relay di rete

Ivanti Neurons per MDM abilita la configurazione Relay di rete per il payload che si usa per configurare le impostazioni relay per un dispositivo o un'applicazione senza la necessità di VPN o tunnel per accedere a risorse private.

Applicabile a

- iOS 17.0 fino alla versione più recente supportata da Ivanti Neurons per MDM.
- macOS 14 fino alla versione più recente supportata da Ivanti Neurons per MDM.
- visionOS 1.1 fino alla versione più recente supportata da Ivanti Neurons per MDM.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Relay di rete**.
3. Configurare le impostazioni **Relay di rete** come da tabella seguente:

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
URL relay HTTP/3	Specificare un valore URL da usare come valore del campo HTTP per questa configurazione. Includere l'URL del relay HTTP/2 o l'URL del relay HTTP/3, oppure entrambi.
URL relay HTTP/2	Specificare un valore URL da usare come valore del campo HTTP per questa configurazione. Includere l'URL del relay HTTP/2 o l'URL del relay HTTP/3, oppure entrambi.
Campi aggiuntivi dell'intestazione HTTP	Specificare il valore del campo header HTTP per il nome del campo header corrispondente.
Certificato	Selezionare uno dei certificati di identità creati dall'utente dall'elenco a discesa.
Chiave pubblica non elaborata	Specificare le chiavi pubbliche non elaborate per autenticare il server durante una connessione di rete.
+ Aggiungi	Selezionare **+ Aggiungi** per aggiungere la configurazione di più relay di rete.
Corrispondenza domini	Specificare l'elenco dei domini per determinare quale connessione instradare attraverso i server nei relay.
Escludi domini	Specificare l'elenco dei domini per determinare quale connessione evitare attraverso i server nei relay.
Corrispondenza di FQDN(supportato su dispositivi iOS 18.4+ e macOS 15.4+)	Specificare l'elenco dei nomi di dominio pienamente qualificati (FQDN), noti anche come nomi di host, che devono essere instradati attraverso i server contenuti nei relè. Qualsiasi connessione che corrisponda a questo esatto FQDN o hostname utilizzerà i relè. Se non sono elencati né FQDN né "MatchDomains", il traffico verso tutti i domini, tranne quelli che corrispondono a un dominio escluso o a un FQDN escluso, sarà instradato verso i server di relè.
Escludi FQDN (supportato su dispositivi iOS 18.4+ e macOS 15.4+)	Specificare l'elenco dei nomi di dominio pienamente qualificati (FQDN), noti anche come nomi di host, che **NON** devono essere instradati attraverso i server contenuti nei relè. Qualsiasi connessione che corrisponda esattamente all'FQDN non utilizzerà il server di relè. Quando sono specificati anche i "MatchDomains", qualsiasi FQDN elencato in "ExcludedFQDNs" deve essere un sottodominio di almeno un MatchDomain. In caso contrario, non avrà alcun effetto.

4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
5. Selezionare una delle opzioni di distribuzione per impostare la configurazione del **Relay di rete**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere Utilizzo delle configurazioni.
6. Fare clic su **Fine**.

10.10.6.15. Accesso sicuro multiutente per iOS

La clip Web multiutente consente agli utenti di accedere e disconnettersi dai dispositivi iOS che sono registrati in Ivanti Neurons for MDM. Quando un utente accede per la prima volta, i profili, le app e le configurazioni associate a tale utente vengono inviate al dispositivo. Quando l'utente ha terminato il lavoro, può aprire la clip Web e selezionare la funzione di disconnessione, che assegna il dispositivo all'utente "Nessuno" e rimuove i profili, le app e le configurazioni associate all'utente che aveva originariamente effettuato l'accesso, a condizione che le configurazioni e le app non vengano distribuite all'utente Nessuno. Dopo una disconnessione, la clip Web viene reimpostata in modo che l'utente successivo possa accedere e ricevere le configurazioni, app e policy personalizzate. La supervisione del dispositivo non è necessaria per utilizzare la funzionalità di accesso sicuro multiutente. Vedere l'articolo della knowledge base **Ivanti Neurons for MDM: Accesso sicuro multiutente per iOS**, per informazioni più approfondite sulla funzionalità di accesso multiutente.

Applicabile a: dispositivi iOS (non applicabile ai dispositivi con Registrazione utente)

Argomenti della sezione:

- **Credenziali supportate**
- **Informazioni sull'utente Nessuno**
- **Accesso a un dispositivo**
- **Disconnessione da un dispositivo**

Credenziali supportate

È necessario utilizzare nome utente e password per accedere alla clip Web sicura multiutente. La registrazione basata su PIN non è supportata con la clip Web sicura multiutente.

Procedura

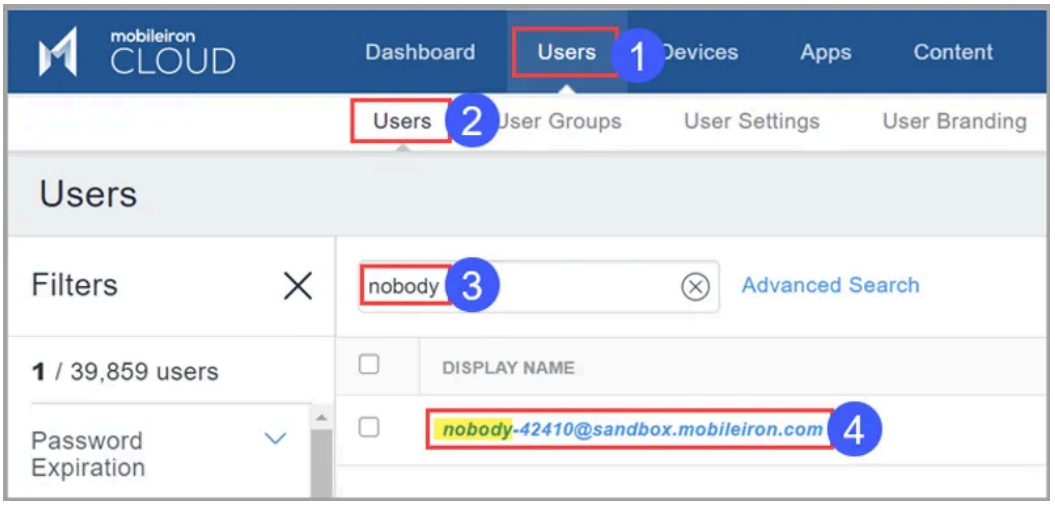
1. Accedere a **Configurazioni**.
2. Fare clic su **Accesso sicuro multiutente per iOS**. Potrebbe essere necessario utilizzare la funzionalità di ricerca per scoprire se ci sono più pagine di configurazioni. Questa configurazione non è accessibile selezionando **+ Aggiungi**.
3. Fare clic su **Modifica distribuzione**, o sull'icona associata, per distribuire la clip Web al gruppo di dispositivi appropriato.
   
   Se si vuole distribuirla a un gruppo di utenti, è possibile creare un gruppo di dispositivi dinamico legato a un gruppo di utenti.
4. Selezionare una delle seguenti opzioni di distribuzione, ricordando che si deve sempre distribuire la clip Web all'utente Nessuno, o al gruppo di dispositivi a cui l'utente Nessuno è associato. Poiché questo non avviene per impostazione predefinita, assicurarsi di effettuare la distribuzione all'utente Nessuno.
   - Tutti i dispositivi
   - Nessun dispositivo (impostazione predefinita)
   - Personalizzato

Fare clic su **Salva**.

Informazioni sull'utente *Nessuno*

Quando un dispositivo è stato disconnesso mediante una clip Web, rimane registrato con Ivanti Neurons per MDM a un utente speciale chiamato Utente nessuno. Se si desidera rimuovere le app e le configurazioni dal dispositivo quando un utente si disconnette, è

necessario assicurarsi che queste app e configurazioni non siano distribuite all'utente Nessuno. Se si desidera che alcune configurazioni, come quella Wi-Fi, rimangano sul dispositivo quando un utente si disconnette dalla clip Web di accesso sicuro, è necessario assicurarsi che tali configurazioni siano distribuite anche all'utente Nessuno.



Questo significa che si deve prestare attenzione ai gruppi di utenti e ai gruppi di dispositivi a cui si distribuiscono app e configurazioni. Se si distribuisce un'app a Tutti, e si desidera che venga rimossa quando un utente si disconnette dal dispositivo, la prassi migliore è quella di creare un gruppo di utenti che non include l'utente Nessuno. Gli attributi personalizzati rendono molto più facile creare un gruppo di utenti che sono "multiutenti" e un altro gruppo di utenti composto esclusivamente dall'utente Nessuno. È possibile creare un attributo utente da Amministratore > Sistema > Attributi chiamato "Proprietario multiutente", quindi assegnare il valore "Sì" o "True" all'utente Nessuno. È quindi possibile creare gruppi di utenti e gruppi di dispositivi in base al valore dell'attributo.

Accesso a un dispositivo

L'utente può accedere a un dispositivo iOS e assegnarsi il dispositivo. Dopo aver eseguito l'accesso, tutti i certificati, le applicazioni, le policy e le configurazioni pertinenti vengono inviati al dispositivo.

> Per motivi di sicurezza, l'utente di iDP deve effettuare nuovamente l'autenticazione a ogni accesso, anche se ha già effettuato l'accesso al dispositivo.

Disconnessione da un dispositivo

L'utente può disconnettersi dal proprio dispositivo iOS dopo l'utilizzo. Dopo avere eseguito la disconnessione, tutti i certificati, le applicazioni, le policy e le configurazioni vengono rimossi dal dispositivo, lasciando quest'ultimo nello stato in cui si trovava prima dell'accesso dell'utente. Il dispositivo è quindi disponibile per l'accesso da parte di un altro utente.

> Disconnettersi da tutte le applicazioni Microsoft prima di disconnettersi da Clip Web multiutente.

Per ulteriori informazioni, vedere **Personalizzazione dell'accesso multiutente**

10.10.6.16. Configurazione delle impostazioni di APN Android

La configurazione delle impostazioni di APN Android consente di impostare l'Access Point Name (APN) richiesto sui dispositivi di una rete pubblica. Questa configurazione è applicabile ai dispositivi di lavoro Android Enterprise gestiti e ai dispositivi gestiti con Profilo di lavoro su un dispositivo di proprietà dell'azienda (su Android versione 9.0 o versioni successive supportate).

Procedura

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Impostazioni APN Android**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Nella sezione Impostazioni configurazione, configurare le opzioni seguenti:
6. Fare clic su **Avanti**.

Impostazione	Descrizione
Nome voce	Digitare il nome delle impostazioni del punto di accesso.
Nome del punto di accesso	Digitare il nome del punto di accesso.
Tipo di punto di accesso	Selezionare il tipo di punto di accesso, scegliendo fra le opzioni seguenti: • **Predefinito** • **DUN** • **IMS** • **Emergenza** • MMS • **HIPRI** • **CBS** • **MCX** • **SUPL** • **FOTA** • **IA**
Tipo MVNO	Selezionare il tipo di operatore virtuale di rete mobile tra le seguenti opzioni: • **Nessuno** • **SPN** • **IMSI** • **GID** • **ICCID**
Bearer	Selezionare il tipo di servizio portante utilizzato per la trasmissione dei dati tra le seguenti opzioni: • **1xRTT** • **CDMA** • **EDGE** • **EHRPO** • **EVDO** • **EVDO A** • **EVDO B** • **GPRS** • **GSM** • **HSDPA** • **HASP** • **HSPAP** • **HSUPA** • **IDEN**

Impostazione	Descrizione
	• **IWLAN** • **LTE** • **NR** • **TD_SCDMA** • **UMTS**
Protocollo APN	Selezionare il protocollo APN richiesto per l'APN. Di seguito sono indicate le opzioni disponibili: • **Nessuno** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP** (Point-to-Point Protocol) • **NON STRUTTURATO**
Protocollo di roaming APN	Selezionare il protocollo di roaming APN richiesto per l'APN. Di seguito sono indicate le opzioni disponibili: • **Nessuno** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP** (Point-to-Point Protocol) • **NON STRUTTURATO**
Attiva/Disattiva APN	Attivare la configurazione APN.
ID vettore	Inserire il valore numerico dell'ID vettore.
Tipo di autenticazione	Selezionare il tipo di protocollo di autenticazione, scegliendo fra le opzioni seguenti: • **Nessuno** • **PAP** (Password Authentication Protocol) • **CHAP** (Challenge-Handshake Authentication Protocol) • **PAP o CHAP**
Nome utente	Inserire il nome utente di accesso.
Password	Immettere la password di accesso.
Conferma password	Immettere nuovamente la password per conferma.
Numero porta	Inserire il numero della porta (valore numerico compreso tra 1 e 65535).

Impostazione	Descrizione
Indirizzo proxy	Digitare l'indirizzo proxy.
Mobile Country Code (MCC)	Inserire il Mobile Country Code.
Mobile Network Code (MNC)	Inserire il Mobile Network Code.
Indirizzo proxy MMS	Digitare l'indirizzo proxy MMS.
Numero porta MMS	Inserire il numero della porta MMS (valore numerico compreso tra 1 e 65535).
Indirizzo server MMS (mmsc)	Digitare l'indirizzo server MMS.

7. Selezionare una delle seguenti opzioni di distribuzione:
8. Fare clic su **Fine**.

- **Tutti i dispositivi**
- Nessun dispositivo (impostazione predefinita)
- **Personalizzato**

> Non è possibile aggiungere un'altra configurazione APN con gli stessi valori per i seguenti campi se esiste una configurazione APN con questi valori per il dispositivo:

- Mobile Country Code (MCC)
- Mobile Network Code (MNC)
- Nome del punto di accesso
- Indirizzo proxy
- Numero porta
- Indirizzo proxy MMS
- Numero porta MMS
- Indirizzo server MMS
- Attiva/Disattiva APN
- Tipo MVNO
- Protocollo APN
- Protocollo di roaming APN

La configurazione delle impostazioni di APN Android ha priorità sulle altre impostazioni APN, eventualmente già configurate nel dispositivo manualmente o dall'operatore di rete.

10.10.6.17. Configurazione VPN

Applicabile a:

- Android (deprecato per i dispositivi Android Enterprise. È necessario utilizzare la Configurazione gestita per VPN specifiche dal Catalogo app).
- Windows
- iOS
- macOS
- tvOS
- visionOS

La configurazione VPN consente di definire le impostazioni relative all'accesso alle reti private virtuali.

> Per questa configurazione è disponibile l'opzione di delega con distribuzione personalizzata. Per ulteriori informazioni, vedere l'argomento *Distribuzione della configurazione* in **Utilizzo delle configurazioni**.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Selezionare la configurazione **VPN**.
3. Immettere un **Nome** per la configurazione.
4. Immettere una descrizione.
5. Configurare le impostazioni VPN in base alle descrizioni seguenti.
6. (Solo iOS 9.0+) Nella sezione Corrispondenza con i domini, fare clic su **+ Aggiungi** per inserire uno o più domini corrispondenti (esempio: company.com). La connessione proxy viene utilizzata quando il dominio è uno dei domini specificati.
7. Fare clic su **Avanti**.
8. (solo macOS) Nella pagina Distribuisci, selezionare una delle seguenti opzioni di distribuzione:
   - Canale dispositivi: la configurazione è attiva per tutti gli utenti di un dispositivo (opzione tipica).
   - Canale utenti: la configurazione è attiva solo per l'utente attualmente registrato sul dispositivo.
9. Selezionare le opzioni di distribuzione rimanenti per questa configurazione.
10. Fare clic su **Fine**.

Impostazioni VPN

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Tipo connessione	Selezionare il tipo di VPN da configurare. Le impostazioni rimanenti dipendono da questa selezione.

Protocolli e relative impostazioni:

- **L2TP** (non supportato su Ivanti Go)
- **PPTP** (non supportato su Ivanti Go)
- **IPsec (Cisco)** (non supportato su Ivanti Go)
- **Cisco AnyConnect** (supportato su Ivanti Go)
- **Juniper SSL** (non supportato su Ivanti Go)
- **NetMotion VPN** (non supportato su Ivanti Go)
- Pulse Secure (supportato su Ivanti Go)
- **F5 SSL** (non supportato su Ivanti Go)
- **SonicWALL Mobile Connect** (non supportato su Ivanti Go)
- **Aruba VIA** (non supportato su Ivanti Go)
- **SSL personalizzato** (non supportato su Ivanti Go)
- **Palo Alto Networks GlobalProtect** (supportato su Ivanti Go)
- **KEv2 (solo Windows)** (non supportato su Ivanti Go)
- **IKEv2** (non supportato su Ivanti Go)

L2TP

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione dell'utente	Selezionare il metodo di autenticazione da utilizzare: **Password** o **RSA SecurID**.
Segreto condiviso	Immettere il passcode del segreto condiviso, se richiesto, per l'inizializzazione della connessione.
Invia tutto il traffico	Selezionare quest'opzione per utilizzare questa connessione per tutto il traffico di rete. Questa opzione consente di proteggere i dati impedendone la compromissione, in particolare sulle reti pubbliche.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

PPTP

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione dell'utente	Selezionare il metodo di autenticazione da utilizzare: **Password** o **RSA SecurID**.
Livello di crittografia	Selezionare un livello di crittografia dei dati per la connessione: **Nessuno, Automatico** o **Massimo** (128 bit).
Invia tutto il traffico	Selezionare quest'opzione per utilizzare questa connessione per tutto il traffico di rete. Questa opzione consente di proteggere i dati impedendone la compromissione, in particolare sulle reti pubbliche.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

IPsec (Cisco)

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione computer	Selezionare il metodo di autenticazione da utilizzare: **Segreto condiviso/Nome del gruppo** o **Certificato**.
Nome del gruppo	Autenticazione tramite Segreto condiviso/Nome del gruppo. Specificare il nome del gruppo da utilizzare. Se viene utilizzata un'autenticazione ibrida, la stringa deve terminare con la dicitura "[hybrid]".
Segreto condiviso	Autenticazione tramite Segreto condiviso/Nome del gruppo. Immettere il passcode del segreto condiviso.
Utilizza l'autenticazione ibrida	Autenticazione tramite Segreto condiviso/Nome del gruppo. Selezionare per specificare l'autenticazione ibrida, ad es., il server fornisce un certificato e il client una chiave pre-condivisa.
Richiedi password	Autenticazione tramite Segreto condiviso/Nome del gruppo. Specificare se richiedere all'utente di immettere una password durante la connessione.
Credenziale	*Autenticazione tramite Certificato* Selezionare il certificato di identità da utilizzare.
Includi PIN utente	*Autenticazione tramite Certificato* Selezionare quest'opzione per richiedere all'utente di immettere un codice PIN.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

Cisco AnyConnect

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Gruppo	Immettere il gruppo da utilizzare per autenticare la connessione.
Autenticazione dell'utente	Selezionare il metodo di autenticazione dell'utente da utilizzare: **Password** o **Certificato**. Se si seleziona **Certificato**, sarà disponibile il campo seguente: **Credenziale**: selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

Juniper SSL

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Area di autenticazione	Immettere l'area di autenticazione da utilizzare per l'autenticazione della connessione.
Ruolo	Immettere il ruolo di autenticazione da utilizzare per l'autenticazione della connessione.
Autenticazione dell'utente	Selezionare il metodo di autenticazione dell'utente da utilizzare: **Password** o **Certificato**. Se si seleziona **Certificato**, sarà disponibile il campo seguente: **Credenziale**: selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

VPN NetMotion

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione dell'utente	Selezionare il metodo di autenticazione dell'utente da utilizzare: **Password** o **Certificato**. Se si seleziona **Certificato**, sarà disponibile il campo seguente: **Credenziale**: selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

F5 SSL

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.
Autenticazione dell'utente	Selezionare il metodo di autenticazione dell'utente da utilizzare: **Password** o **Certificato**. Se si seleziona **Certificato**, sarà disponibile il campo seguente: **Credenziale**: selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare Manuale o Automatico per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

SonicWALL Mobile Connect

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Gruppo o dominio di accesso	Immettere il gruppo o il dominio di accesso da utilizzare per l'autenticazione della connessione.
Autenticazione dell'utente	Selezionare il metodo di autenticazione dell'utente da utilizzare: **Password** o **Certificato**. Se si seleziona Certificato, sarà disponibile il campo seguente: **Credenziale**: selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

Aruba VIA

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione dell'utente	Selezionare il metodo di autenticazione dell'utente da utilizzare: **Password** o **Certificato**. Se si seleziona **Certificato**, sarà disponibile il campo seguente: **Credenziale**: selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare Manuale o Automatico per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

SSL personalizzato

Impostazione	Operazione da eseguire
Identificatore	Immettere l'identificatore per questo SSL VPN personalizzato in formato DNS inverso (ad esempio com.lamiaazienda.ilmioserver).
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Dati personalizzati	Immettere le coppie chiave-valore che definiscono i dati personalizzati per questo VPN.
Autenticazione dell'utente	Selezionare il metodo di autenticazione dell'utente da utilizzare: **Password** o **Certificato**. Se si seleziona Certificato, sarà disponibile il campo seguente: **Credenziale**: selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

Palo Alto Networks GlobalProtect

> Non applicabile ai dispositivi Android.

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.
Dati personalizzati	Immettere le coppie chiave-valore che definiscono i dati personalizzati per questo VPN.
Autenticazione dell'utente	Selezionare il metodo di autenticazione dell'utente da utilizzare: **Password** o **Certificato**. Se si seleziona Certificato, sarà disponibile il campo seguente: **Credenziale**: selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

IKEv2 (solo Windows)

Impostazione	Operazione da eseguire
Server	Immettere il nome host o l'indirizzo IP del server VPN.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

IKEv2

Impostazione	Operazione da eseguire
Server	Immettere il nome host o l'indirizzo IP del server VPN.
Identificatore locale	Identificatore del client IKEv2 in uno dei formati seguenti: • FQDN • UserFQDN • Indirizzo • ASN1DN
Identificatore remoto	Identificatore remoto in uno dei formati seguenti: • FQDN • UserFQDN • Indirizzo • ASN1DN
Autenticazione computer	Disponibile soltanto se l'opzione **Abilita EAP** non è selezionata. Selezionare una delle opzioni seguenti: • Certificato • Segreto condiviso
Autenticazione EAP	Disponibile soltanto se l'opzione **Abilita EAP** è selezionata. Selezionare una delle opzioni seguenti: • Certificato • Nome utente/Password
Segreto condiviso	Disponibile solo se è stata selezionata l'opzione Segreto condiviso per l'Autenticazione computer. Inserire il segreto condiviso per la connessione.
Credenziale	Disponibile solo se è stata selezionata l'opzione Certificato per l'Autenticazione computer. Selezionare il certificato da utilizzare. Questo certificato verrà inviato per l'autenticazione del client IKE. Se viene utilizzata l'autenticazione estesa, è possibile utilizzare questo certificato per EAP-TLS.
Abilita EAP	Selezionare questa opzione per abilitare l'autenticazione estesa.
Account	Disponibile soltanto se l'opzione Nome utente/Password è stata selezionata per l'autenticazione EAP. Immettere l'ID account del server VPN.
Password	Disponibile soltanto se l'opzione Nome utente/Password è stata selezionata per l'autenticazione EAP. Immettere la password del server VPN.
Intervallo Dead Peer Detection	Selezionare una delle seguenti opzioni: • Nessuno (disattivato) • Basso (keepalive inviato ogni ora) • Medio (keepalive inviato ogni 30 minuti) • Alto (keepalive inviato ogni 10 minuti)

Impostazione	Operazione da eseguire
Nome comune autorità di certificazione server	(Facoltativo) - Nome comune dell'autorità di certificazione del server, fa sì che il server IKE invii al server una richiesta di certificato basata sull'autorità di certificazione.
Nome comune certificato server	(Facoltativo) - Nome comune di un certificato del server usato per convalidare il certificato inviato dal server IKEv2.
Usa attributi sottoreti IP4 e IP6	(Facoltativo) Selezionare per utilizzare gli attributi delle sottoreti IP4 e IP6.
Abilita protocollo mobilità e multihoming (MOBIKE) di IKEv2	(Facoltativo) L'impostazione predefinita è 0. MOBIKE (capacità di supportare dispositivi mobili con multihoming connessi sia a una rete Wi-Fi sia a collegamenti cellulari con più indirizzi IP) è abilitato. Abilitato per impostazione predefinita. Impostare su 1 per disabilitare MOBIKE.
Abilita PFS (Perfect Forward Secrecy)	(Facoltativo) Se impostato su 1, abilita il PFS per le connessioni IKEv2. L'impostazione predefinita è 0.
Abilita reindirizzamento IKEv2	(Facoltativo) L'impostazione predefinita è 0. La connessione IKEv2 viene reindirizzata se il server invia una richiesta di reindirizzamento. Abilitato per impostazione predefinita. Impostare su 1 per disabilitare il reindirizzamento IKEv2.
Abilita NAT keep-alive	Abilita il keepalive Network Address Translation che impedisce l'eliminazione delle voci NAT in assenza di traffico con NAT fra i peer IKE.
Intervallo NAT keep-alive	Se il NAT keepalive è abilitato, questo è il tempo in secondi in cui verranno inviati i pacchetti keepalive per il dispositivo.
PPK	Immettere la chiave precondivisa post-quantum (PPK) con i server VPN che supportano RFC 8784. Se questa chiave è presente, deve essere presente anche l'identificatore PPK.
Identificatore PPK	Inserire l'identificativo PPK.
PPK obbligatorio	Selezionare una delle seguenti opzioni a discesa: • **Obbligatorio**: la connessione VPN verrà stabilita con successo se il server supporta RFC 8784 o se accetta l'identificatore PPK specificato nell'identificatore PPK. • **Non obbligatorio**: la connessione VPN non verrà stabilita se il server non supporta RFC 8784 o non accetta l'identificatore PPK specificato nell'identificatore PPK.
Algoritmo di crittografia	Selezionare una delle seguenti opzioni: • **DES** • **3DES** • **AES-128** • **AES-256** (predefinito) • **AES-128 GCM** • **AES-256 GCM**

Impostazione	Operazione da eseguire
Algoritmo di integrità	Selezionare una delle seguenti opzioni: • **SHA2-256** (predefinito) • **SHA2-384** • **SHA2-512**
Gruppo Diffie-Hellman	Selezionare una delle seguenti opzioni: • **1** • **2** (Predefinito) • **5** • **14** • **15** • **16** • **17** • **18**
Durata in minuti	Inserire la durata SA (intervallo di reimpostazione della chiave) espressa in minuti. I valori validi sono compresi tra 10 e 1440.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

*Digitare $ per visualizzare una lista delle **variabili** supportate, se disponibili, per questo campo.

Per ulteriori informazioni, vedere **Come creare una configurazione**

10.10.6.18. VPN on Demand

Applicabile a: dispositivi iOS

La configurazione di VPN on demand consente di impostare l'accesso a un server VPN basato su domini, nomi host ecc.

Impostazioni di VPN on demand

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Tipo connessione Abilità VPN on demand	Selezionare il tipo di VPN da configurare. Le impostazioni rimanenti dipendono da questa selezione. Selezionare quest'opzione per utilizzare questa configurazione per i domini e i nomi host che stabiliscono una connessione VPN on demand.
Abilita regole iOS (applicabile se viene selezionato Abilità VPN on demand)	Per iOS e macOS, è possibile configurare: • Le regole di rete che permettono o vietano le connessioni e permettono o ignorano le reti considerate vere. • Le regole di connessione che permettono se necessario o non permettono mai le connessioni alle reti considerate vere. Per le regole di rete, è possibile specificare i seguenti tipi di parametri: • Corrispondenza dominio DNS • Corrispondenza indirizzo server DNS • Corrispondenza SSID • Probe stringa URL • Corrispondenza tipo di interfaccia Per le regole di connessione, è possibile specificare i seguenti tipi di parametri: • Corrispondenza dominio DNS • Corrispondenza indirizzo server DNS • Corrispondenza SSID • Probe stringa URL • Corrispondenza tipo di interfaccia • Nome dominio • Server DNS • Probe URL
Tipo di provider (iOS 9 e versioni successive)	Selezionare uno dei seguenti provider per il tunneling: • app-proxy: effettua il tunneling del traffico a livello di app. Per una panoramica del provider proxy delle app, consultare la **documentazione Apple**. • packet-tunnel: effettua il tunneling del traffico a livello di IP. Per una panoramica del provider per il tunneling dei pacchetti, consultare la **documentazione Apple**.
Imponi percorsi	Quando è abilitato, i percorsi non predefiniti della VPN sovrascrivono qualsiasi percorso definito localmente. • Se Includi tutte le reti è abilitato, il sistema non tiene conto dell'impostazione Imponi percorsi • Disponibile su iOS 14.2 e versioni successive.

Impostazione	Operazione da eseguire
Escludi reti locali	Se abilitato insieme a Includi tutte le reti, tutto il traffico della rete locale viene instradato all'esterno della VPN.
Includi tutte le reti	Se abilitato, instrada tutto il traffico attraverso la VPN.

Protocolli e relative impostazioni:

- **IPsec (Cisco)**
- **Cisco AnyConnect**
- **Juniper SSL**
- **VPN NetMotion**
- **F5 SSL**
- **SonicWALL Mobile Connect**
- **Aruba VIA**
- **SSL personalizzato**
- **Palo Alto Networks GlobalProtect**

IPsec (Cisco)

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione computer	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Includi PIN utente	Selezionare quest'opzione per richiedere all'utente di immettere un codice PIN.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. **Se si seleziona Manuale,** saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. **Se si seleziona Automatico,** saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

Cisco AnyConnect

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Gruppo	Immettere il gruppo da utilizzare per autenticare la connessione.
Autenticazione dell'utente	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. **Se si seleziona Manuale,** saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. **Se si seleziona Automatico,** saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

Juniper SSL

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Area di autenticazione	Immettere l'area di autenticazione da utilizzare per l'autenticazione della connessione.
Ruolo	Immettere il ruolo di autenticazione da utilizzare per l'autenticazione della connessione.
Autenticazione dell'utente	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. **Se si seleziona Manuale,** saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. **Se si seleziona Automatico,** saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

VPN NetMotion

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione dell'utente	Il certificato è il metodo di autenticazione dell'utente. **Credenziale**: selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: **URL server proxy**: immettere l'URL completo del proxy.

F5 SSL

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione dell'utente	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. **Se si seleziona Manuale,** saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. **Se si seleziona Automatico,** saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

SonicWALL Mobile Connect

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Gruppo o dominio di accesso	Immettere il gruppo o il dominio di accesso da utilizzare per l'autenticazione della connessione.
Autenticazione dell'utente	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. **Se si seleziona Manuale,** saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. **Se si seleziona Automatico,** saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

Aruba VIA

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Autenticazione dell'utente	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. **Se si seleziona Manuale,** saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. **Se si seleziona Automatico,** saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

SSL personalizzato

Impostazione	Operazione da eseguire
Identificatore	Immettere l'identificatore per questo SSL VPN personalizzato in formato DNS inverso (ad esempio com.lamiaazienda.ilmioserver).
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.*
Dati personalizzati	Immettere le coppie chiave-valore che definiscono i dati personalizzati per questo VPN.
Autenticazione dell'utente	È supportata soltanto l'autenticazione tramite certificato.
Credenziale	Selezionare il certificato di identità da utilizzare.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. **Se si seleziona Manuale,** saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. **Se si seleziona Automatico,** saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

Palo Alto Networks GlobalProtect

Impostazione	Operazione da eseguire
Server	Immettere l'indirizzo IP o il nome host del server VPN.
Account	Immettere l'account utente da utilizzare per l'autenticazione della connessione.
Dati personalizzati	Immettere le coppie chiave-valore che definiscono i dati personalizzati per questo VPN.
Autenticazione dell'utente	Il certificato è il metodo di autenticazione dell'utente. Selezionare un certificato di identità da utilizzare nel campo **Credenziale**.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. **Se si seleziona Manuale,** saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. **Se si seleziona Automatico,** saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.

Digitare $ per visualizzare un elenco delle variabili supportate eventualmente disponibili per questo campo.

Per ulteriori informazioni, vedere Come creare una configurazione

10.10.6.19. Configurazione Wi-Fi

Applicabile a:

- Android
- Windows
- iOS
- macOS
- watchOS
- visionOS
- tvOS

Argomenti della sezione:

[Impostazioni Wi-Fi]

- [WEP, WPA/WPA2/WPA3, qualsiasi impostazione (personale)]
- [WEP Enterprise, WPA/WPA2/WPA3 Enterprise, qualsiasi impostazione (Enterprise)]
- [iOS, macOS e visionOS]

Impostazioni Wi-Fi

La configurazione Wi-Fi consente di impostare l'accesso alle reti wireless.

> Un utente può modificare alcune delle impostazioni Wi-Fi del dispositivo. Tuttavia, il server MDM potrebbe ricevere o meno informazioni sulle modifiche, in base al sistema operativo del dispositivo. Di conseguenza, le configurazioni non verranno inviate di nuovo automaticamente al dispositivo per sostituire la configurazione sul dispositivo con la configurazione sul server.

> Per questa configurazione è disponibile l'opzione di delega con distribuzione personalizzata. Per ulteriori informazioni, vedere l'argomento *Distribuzione della configurazione* in **Utilizzo delle configurazioni**.

> Alcune versioni specifiche di dispositivi Android possono richiedere agli amministratori di inserire il dominio e ulteriori informazioni per connettersi a un sistema TLS, TTLS, PEAP, ecc. Reti (WPA2). Si consiglia di assicurarsi che le modifiche alla configurazione Wi-Fi siano state apportate su dispositivi selezionati prima di effettuare tali modifiche su un gruppo più ampio di dispositivi.

> I dispositivi Android 14.x registrati su qualsiasi versione di Ivanti Neurons for MDM precedente alla 94 avranno lo stato di configurazione "Installazione in sospeso". Quando si aggiorna Ivanti Neurons per MDM alla versione 94 senza modificare la configurazione Wi-Fi, lo stato della configurazione rimane "Installazione in sospeso". È necessario abilitare il campo Dominio per EAP_PEAP e aggiornare il Dominio e i Certificati nella configurazione per aggiornare lo stato a "Installato".

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Selezionare la configurazione **Wi-Fi**.

3. Immettere un **Nome** per la configurazione.
4. Immettere una descrizione.
5. Configurare le impostazioni Wi-Fi in base alle descrizioni seguenti.
6. Fare clic su **Avanti**.
7. (solo macOS) Nella pagina Distribuisci, selezionare una delle seguenti opzioni di distribuzione:
    - Canale dispositivi: la configurazione è attiva per tutti gli utenti di un dispositivo (opzione tipica).
    - Canale utenti: la configurazione è attiva solo per l'utente attualmente registrato sul dispositivo.
8. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzata.
9. Fare clic su **Fine**.

Nella seguente tabella sono elencate le impostazioni Wi-Fi:

Impostazione	Operazione da eseguire
Nome Descrizione Identificatore del set di servizi (SSID)	Immettere un nome identificativo della configurazione. Immettere una descrizione esplicativa dello scopo della configurazione. Immettere il nome della rete wireless a cui si applicano tali impostazioni. Questo campo effettua la distinzione tra lettere maiuscole e minuscole.
Connessione automatica Rete nascosta	Selezionare quest'opzione se si desidera che i dispositivi si connettano automaticamente alla rete Wi-Fi corrispondente. Se quest'opzione non viene selezionata, gli utenti devono toccare il nome della rete sul dispositivo per collegarsi. Selezionare quest'opzione se si accede a reti non broadcast.
Disattiva rilevamento reti bloccate (iOS 10 e versioni successive)	Gli amministratori possono attivare o disattivare la modalità di bypass delle reti Wi-Fi bloccate. Quando Apple rileva la presenza di un portale bloccato, apre una schermata di login per richiedere l'accesso. È possibile disattivare il rilevamento dei portali bloccati, facendo in modo che l'utente debba avviare manualmente un browser che attivi l'accesso al portale della rete bloccata. Questa nuova impostazione è utile quando un portale bloccato ISE impedisce la visualizzazione della schermata di accesso, facendo credere agli utenti che i loro dispositivi non connessi siano in realtà collegati a Internet.
Configurazione proxy	Selezionare **Manuale** o **Automatico** per configurare un proxy. Se si seleziona **Manuale**, saranno disponibili i seguenti campi aggiuntivi: • **Server e porta:** immettere l'indirizzo di rete e il numero di porta del server proxy.* • **Autenticazione:** immettere un nome utente valido, se richiesto, per la connessione al proxy.* • **Password:** immettere una password valida, se richiesta, per la connessione al proxy. Per rimuovere il nome host aggiunto, fare clic sull'icona del segno meno (-). Se si seleziona **Automatico**, saranno disponibili i seguenti campi aggiuntivi: • **URL server proxy**: immettere l'URL completo del proxy.
Tipo di protezione	Selezionare il metodo di protezione richiesto per l'accesso alla rete: • Qualsiasi (personale) • Qualsiasi (aziendale) • WEP • WEP aziendale • WPA • WPA Enterprise • WPA2 • WPA2 Enterprise • WPA3

Impostazione	Operazione da eseguire
	• WPA3 Enterprise WPA3/WPA3 Enterprise è applicabile per iOS 13 e versioni successive. Windows supporta WPA, WPA Enterprise, WPA2 e WPA2 Enterprise.

WEP, WPA/WPA2/WPA3, qualsiasi impostazione (personale)

Impostazione	Operazione da eseguire
Password	(Facoltativo) Immettere la password per l'accesso alla rete. Altrimenti, all'utente del dispositivo verrà richiesto di immettere la password per accedere alla rete.

WEP Enterprise, WPA/WPA2/WPA3 Enterprise, qualsiasi impostazione (Enterprise)

Impostazione	Operazione da eseguire
Protocolli	
Tipi EAP accettati	Selezionare i tipi EAP che è possibile utilizzare per accedere alla rete: • TLS • TTLS - Nel campo Identità interna, selezionare uno dei protocolli di autenticazione, ad esempio Sistema operativo predefinito, PAP, CHAP, MSCHAP, MSCHAPv2 ed EAP. • PEAP • LEAP (non supportato per i dispositivi con registrazione AMAPI) • EAP-SIM • EAP-AKA • EAP-FAST (non supportato per dispositivi registrati con AMAPI)
EAP-FAST	Selezionare l'opzione EAP-FAST per definire i metodi di autenticazione: • **Utilizza PAC:**selezionare questa opzione per utilizzare una configurazione proxy automatica (PAC). • **Esegui provisioning PAC**: selezionare questa opzione per consentire il provisioning di una PAC. In alternativa, sarà possibile utilizzare soltanto una PAC per la quale è stato già eseguito il provisioning sul dispositivo. Quest'opzione è disponibile soltanto se è stata selezionata l'opzione Utilizza PAC. • **Esegui provisioning PAC in modo anonimo:** selezionare questa opzione per consentire il provisioning di una PAC senza eseguire l'autenticazione del server. Quest'opzione è disponibile soltanto se è stata selezionata l'opzione Esegui provisioning PAC.
Autenticazione	
Nome utente	Specificare il nome utente richiesto per l'accesso alla rete. Se questo campo viene lasciato vuoto, verrà richiesto all'utente di compilarlo.
Utilizza password per connessione	Selezionare quest'opzione per richiedere all'utente del dispositivo una password per ciascuna connessione. Quando il dispositivo si ricollega alla stessa rete, all'utente verrà richiesto di eseguire nuovamente l'autenticazione per ricollegarsi alla rete. Questa opzione non è supportata per dispositivi registrati con AMAPI.
Password	(Facoltativo) Immettere la password per l'accesso alla rete. Altrimenti, all'utente del dispositivo verrà richiesto di immettere la password per accedere alla rete.
Certificato di identità	(Facoltativo) Selezionare il certificato da utilizzare per le credenziali di identità. La configurazione tramite il **Certificato di identità** consente di definire ciascun certificato di identità disponibile.
Certificato di autenticazione (disponibile solo per i dispositivi Windows)	Selezionare uno dei tre Certificate Store seguenti per scegliere un certificato e connettersi a una rete Wi-Fi: • Computer o utente: se questa opzione è selezionata e l'utente non è connesso, il certificato di autenticazione verrà prelevato dall'archivio del computer. Se l'utente è connesso, il certificato specifico verrà prelevato dall'archivio utenti.

Impostazione	Operazione da eseguire
	• Computer: se questa opzione è selezionata, il certificato di autenticazione verrà prelevato dall'archivio del computer. • Utente: se questa opzione è selezionata, il certificato di autenticazione verrà prelevato dall'archivio dell'utente. Per impostazione predefinita, l'opzione Utente risulta selezionata.
Identità esterna	(Facoltativo) Per TLS, TTLS, PEAP e EAP-FAST, selezionare per consentire agli utenti del dispositivo di nascondere la propria identità. Il nome reale dell'utente viene visualizzato soltanto all'interno del tunnel crittografato. Questa opzione può aumentare la sicurezza dato che un aggressore non può vedere il nome dell'utente che si autentifica in chiaro.
Dominio	Supportato quando il tipo EAP è TLS e TTLS.
Contrassegna come attendibile	
Certificati attendibili (non supportati per i dispositivi con registrazione AMAPI)	Selezionare le caselle di controllo per selezionare più certificati dall'elenco.
Nomi dei certificati del server attendibili	Fare clic su **+ Aggiungi** per immettere i nomi di uno o più certificati server attendibili. (Opzionale) Selezionare **Consenti eccezioni attendibili** per consentire all'utente di prendere decisioni attendibili in una finestra di dialogo.

iOS, macOS e visionOS

Impostazione	Operazione da eseguire
Tutte le versioni	
Tipo di rete	Selezionare questa opzione se si desidera che la rete venga considerata come: • Standard • Hotspot legacy • Passpoint
Ricorso al PAC proxy consentito	(Facoltativo) Consente al dispositivo di connettersi direttamente alla destinazione se il file PAC non è raggiungibile.
Modalità di installazione (opzionale)	Un array di stringhe che contengono il tipo di modalità di connessione da allegare. • Sistema: il Wi-Fi è collegato prima che l'utente acceda al dispositivo. • Finestra accesso: il Wi-Fi è disponibile dopo che l'utente ha effettuato l'accesso al dispositivo. Attualmente, le modalità di impostazione funzionano solo quando sono abilitate entrambe le modalità Finestra di sistema e Finestra di accesso.
Impostazioni Passpoint	Le impostazioni in questa sezione vengono visualizzate se si è selezionato Passpoint come Tipo di rete.
Nome dominio	Immettere il nome dominio da utilizzare per la negoziazione di Passpoint.
Connetti a reti Passpoint partner in roaming	(Facoltativo) Selezionare quest'opzione per consentire la connessione ai fornitori dei servizi di roaming.
Identificatori Roaming Consortium Organization	(Facoltativo) Immettere gli identificatori assegnati dal codice IEEE alle entità supportate da questo profilo Wi-Fi.
Nomi dell'area di autenticazione dell'identificatore di accesso alla rete	(Facoltativo) Immettere i nomi dell'area di autenticazione dell'identificatore di accesso alla rete da utilizzare per la negoziazione di Passpoint.
Coppia MCC e MNC	(Facoltativo) Immettere le coppie Mobile Country Code (MCC)/Mobile Network Code (MNC) da utilizzare per la negoziazione di Passpoint. Ogni stringa deve contenere esattamente sei cifre.
Nome operatore visualizzato	(Facoltativo) Immettere il nome dell'operatore della rete da visualizzare.
Cisco QoS Fast Lane	Le impostazioni in questa sezione riguardano la configurazione di Cisco Fast Lane. Tali impostazioni includono le applicazioni per la creazione degli elenchi di elementi consentiti per il contrassegno L2 ed L3, oltre alla possibilità di inserire o meno tra gli elementi consentiti il traffico audio e video dei servizi audio/video incorporati, come FaceTime e Wi-Fi Calling.

Impostazione	Operazione da eseguire
Limita contrassegno QoS	Se l'opzione non è selezionata, tutte le app useranno il contrassegno L2 ed L3 quando la rete supporta Cisco QoS Fast Lane. Se, invece, è selezionata, utilizzare le impostazioni **Scegli app** visualizzate per inserire le app desiderate per il contrassegno L2 ed L3. Tutte le app non selezionate non useranno i contrassegni L2 ed L3.
Abilita contrassegno QoS	Disattiva il contrassegno L3 e usa solo il contrassegno L2 per il traffico inviato alla rete Wi-Fi. Quando l'opzione non è selezionata, il sistema considera la connessione Wi-Fi come non associata a una rete Cisco QoS Fast Lane.
Consenti chiamate audio/video Apple	Specifica se consentire o meno il traffico audio e video generato dai servizi audio/video integrati, come FaceTime e Wi-Fi Calling.
Scegli app	Consente di inserire le app desiderate per il contrassegno L2 ed L3. Tutte le app non selezionate non useranno il contrassegno L2 ed L3.
iOS 10 e versioni successive **Cisco QoS Fast Lane**	Le impostazioni in questa sezione riguardano la configurazione di Cisco Fast Lane. Tali impostazioni includono le applicazioni per la creazione degli elenchi di elementi consentiti per il contrassegno L2 ed L3, oltre alla possibilità di inserire o meno tra gli elementi consentiti il traffico audio e video dei servizi audio/video incorporati, come FaceTime e Wi-Fi Calling.
Limita contrassegno QoS	Se l'opzione non è selezionata, tutte le app useranno il contrassegno L2 ed L3 quando la rete supporta Cisco QoS Fast Lane. Se, invece, è selezionata, utilizzare le impostazioni **Scegli app** visualizzate per inserire le app desiderate per il contrassegno L2 ed L3. Tutte le app non selezionate non useranno i contrassegni L2 ed L3.
Abilita contrassegno QoS	Disattiva il contrassegno L3 e usa solo il contrassegno L2 per il traffico inviato alla rete Wi-Fi. Quando l'opzione non è selezionata, il sistema considera la connessione Wi-Fi come non associata a una rete Cisco QoS Fast Lane.
Consenti chiamate audio/video Apple	Specifica se consentire o meno il traffico audio e video generato dai servizi audio/video integrati, come FaceTime e Wi-Fi Calling.
Scegli app	Consente di inserire le app desiderate per il contrassegno L2 ed L3. Tutte le app non selezionate non useranno il contrassegno L2 ed L3.
Dispositivi supervisionati con iOS 10.3 o versioni successive	

Impostazione	Operazione da eseguire
Abilita creazione elenco reti Wi-Fi consentite	Consente di stabilire a quali reti Wi-Fi può connettersi il dispositivo. Se sono disponibili più configurazioni Wi-Fi, viene applicata quella più restrittiva.
iOS 14.0 e macOS 15.0 e versioni successive Disabilitazione della randomizzazione dell'indirizzo MAC	In iOS 14.0 e macOS 15.0 e nelle versioni successive, Apple ha modificato il comportamento predefinito di un dispositivo che segnala il proprio indirizzo MAC Wi-Fi, in modo da indicare un indirizzo casuale per le nuove connessioni invece dell'indirizzo MAC Wi-Fi effettivo del dispositivo. Questa funzionalità può pertanto determinare un comportamento imprevisto nelle aziende che utilizzano portali bloccati o il filtraggio degli indirizzi MAC. Gli amministratori possono **disabilitare la randomizzazione dell'indirizzo MAC** per una rete Wi-Fi modificando la configurazione Wi-Fi associata e attivando questa opzione (che per impostazione predefinita è false). Questo determina il repush della configurazione Wi-Fi a tutti i dispositivi. Questa opzione visualizza un avviso sulla privacy nelle impostazioni del dispositivo, per indicare che la rete offre una protezione limitata della privacy. L'utente può comunque attivare e disattivare questa opzione manualmente tramite le impostazioni del dispositivo.
Android 11+ Randomizzazione dell'indirizzo MAC	• Disattivato: il Wi-Fi è connesso prima che l'utente effettui l'accesso al dispositivo. • Abilitato - Automatico: il Wi-Fi è disponibile dopo che l'utente ha effettuato l'accesso al dispositivo. • Abilitato - Non persistente • Abilitato - Persistente

Digitare $ per visualizzare un elenco delle **variabili** supportate eventualmente disponibili per questo campo.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.7. Configurazione della rete cellulare

Argomenti della sezione:

- Configurazione APN
- Cellulare
- Cellular Private Network Configuration.htmConfigurazione della rete mobile privata
- Configurazione delle impostazioni delle telecomunicazioni iOS
- Configurazione eSIM

10.10.7.1. Configurazione APN

Una configurazione APN imposta il nome del punto di accesso cellulare per il dispositivo. Per iOS 7, utilizzare invece la **Configurazione cellulare**.

Impostazioni APN

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Nome del punto di accesso	Immettere il nome del punto di accesso corrispondente. Generalmente, il nome è definito dall'operatore che fornisce il servizio.
Nome utente punto di accesso	Inserisci un nome utente autorizzato per questo punto d'accesso.*
Password punto di accesso	Immettere la password corrispondente al nome utente inserito.
Porta e server proxy	Immettere l'indirizzo IP o l'URL e il numero di porta del proxy APN.
Abilita XLAT464	Selezionare la casella di controllo per abilitare l'Access Point Name (APN). Questa opzione fornisce servizi IPv4 su una rete solo IPv6.

Digitare $ per visualizzare un elenco delle **variabili** supportate eventualmente disponibili per questo campo.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.7.2. Cellulare

Applicabile a: iOS 7.0+ e watchOS 10.0+

Argomenti della sezione:

- Impostazioni cellulari per APN predefiniti
- Impostazioni cellulari per APN dati
- Controllo dell'accesso alla rete dati durante il roaming
- Controllo dell'accesso cellulare

La configurazione cellulare consente di impostare il profilo del cellulare di un dispositivo. Configurare le impostazioni della rete mobile sui dispositivi con iOS 7.0+ o watchOS 10.0+. Alcune aziende, grazie a contratti con gli operatori mobili, hanno accesso ad APN univoci (Access Point Name, nomi punto di accesso) per un accesso remoto alla rete o per piani di fatturazione speciali. Contattare l'operatore mobile per i parametri di configurazione.

- Non è possibile installare più di un profilo cellulare alla volta.
- Non è possibile installare un profilo cellulare se è già installato un profilo APN.

È possibile configurare le impostazioni cellulari per i seguenti tipi di APN dal menu a discesa **Tipi di APN configurati**:

- APN predefiniti e dati
- APN predefiniti
- APN dati

Per tutte le configurazioni, immettere un nome identificativo della configurazione e una descrizione facoltativa.

Impostazioni cellulari per APN predefiniti

Impostazioni APN predefinite	Operazione da eseguire
Nome APN	Immettere il nome del punto di accesso corrispondente. Generalmente, il nome è definito dall'operatore che fornisce il servizio.
Tipo di autenticazione APN	(Facoltativo) Selezionare una delle seguenti opzioni: • CHAP (Challenge Handshake Authentication Protocol) • PAP (Password Authentication Protocol)
Nome utente	(Facoltativo) Immettere un nome utente da utilizzare per l'autenticazione.
Password	(Facoltativo) Immettere una password da utilizzare per l'autenticazione.

Impostazioni cellulari per APN dati

Impostazioni APN dati	Operazione da eseguire
Nome APN	Immettere il nome del punto di accesso corrispondente. Generalmente, il nome è definito dall'operatore che fornisce il servizio.
Tipo di autenticazione APN	(Facoltativo) Selezionare una delle seguenti opzioni: • CHAP (Challenge Handshake Authentication Protocol) • PAP (Password Authentication Protocol)
Nome utente	(Facoltativo) Immettere un nome utente da utilizzare per l'autenticazione.
Password	(Facoltativo) Immettere una password da utilizzare per l'autenticazione.
Server proxy	Specificare il server proxy.
Porta server proxy	Specificare la porta del server proxy.
10.3+	
Maschera protocollo consentita	Selezionare IPv4, IPv6 o Entrambi.
Maschera protocollo consentita durante il roaming nazionale	Selezionare IPv4, IPv6 o Entrambi.
Maschera protocollo consentita durante il roaming	Selezionare IPv4, IPv6 o Entrambi.

Controllo dell'accesso alla rete dati durante il roaming

È possibile limitare l'accesso alla rete dati da parte di alcune o tutte le app gestite mentre il dispositivo è in roaming.

Procedura

1. Andare nella scheda **Configurazioni** nel menu principale di navigazione di Ivanti Neurons for MDM.
2. Fare clic su **+Aggiungi**
3. Inserire **Rete** nel campo di ricerca e fare clic sulla configurazione **Utilizzo di rete**.
4. Selezionare la casella di controllo **Non consentire tutte le app gestite** per bloccare l'accesso alla rete dati da parte delle app gestite quando il dispositivo è in roaming o in ogni momento.
5. Lasciare la casella di controllo deselezionata per specificare le app gestite per nome o ID bundle di cui bloccare l'accesso alla rete dati.
6. Utilizzare il menu a discesa nel campo App per cercare un'app in base al nome o all'ID bundle.

Controllo dell'accesso cellulare

È possibile limitare l'accesso alla rete dati da parte di alcune o tutte le app gestite in qualsiasi momento. Le app potranno comunque essere utilizzate in base alla limitazione, tuttavia non avranno accesso alla rete dati.

Procedura

1. Andare nella scheda **Configurazioni** nel menu principale di navigazione di Ivanti Neurons for MDM.

2. Fare clic su **+Aggiungi**
3. Inserire **Rete** nel campo di ricerca e fare clic sulla configurazione **Utilizzo di rete**.
4. Selezionare la casella di controllo **Non consentire tutte le app gestite** per bloccare l'accesso alla rete dati da parte delle app gestite in qualsiasi momento.
5. In via opzionale, lasciare deselezionata la casella di controllo per specificare a quali app gestite impedire l'accesso alla rete dati.
6. Utilizzare il menu a discesa nel campo App per cercare un'app in base al nome o all'ID bundle.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.7.3. Configurazione della rete mobile privata

Ivanti Neurons per MDM consente al payload di configurazione della rete mobile privata di fornire informazioni sul dispositivo in merito alle distribuzioni della rete privata, tra cui la posizione geografica, la preferenza rispetto al Wi-Fi e il tipo di distribuzione della rete.

Applicabile a

iOS 17.0 fino alla versione più recente supportata da Ivanti Neurons per MDM.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Rete mobile privata**.
3. Configurare le impostazioni della **Rete mobile privata** come da tabella seguente:

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Dati mobili preferiti	Selezionare la casella di controllo per attivare e utilizzare i dati mobili su Wi-Fi.
NR Standalone	Selezionare la casella di controllo se la rete dati mobili presenta l'opzione NR 5G Standalone.
Nome set di dati	Specificare il nome del set di dati che si identifica con questa configurazione.
Numero di versione	Specificare il numero di versione del set di dati per monitorare gli aggiornamenti del sistema.
GeoFence	Specificare la latitudine, la longitudine e il raggio per ciascun ID geografico per distribuire una rete privata in una posizione geografica. È possibile creare un elenco di un massimo di mille geofence per le reti private.

4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
5. Selezionare una delle opzioni di distribuzione per impostare la configurazione della **Rete privata mobile**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere **Utilizzo delle configurazioni**.
6. Fare clic su **Fine**.

10.10.7.4. Configurazione delle impostazioni delle telecomunicazioni iOS

La configurazione delle impostazioni delle telecomunicazioni iOS consente di impostare dei valori predefiniti per le limitazioni di roaming e di hotspot.

Impostazioni delle telecomunicazioni iOS

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Consenti ai dispositivi di utilizzare i servizi voce durante il roaming	Selezionare quest'opzione per abilitare le chiamate in roaming. La disponibilità delle chiamate in roaming dipende dall'operatore.
Consenti ai dispositivi di utilizzare il servizio dati durante il roaming	Selezionare quest'opzione per abilitare il roaming dati. L'abilitazione del roaming dati comporta anche l'abilitazione delle chiamate in roaming sul dispositivo.
Consenti agli utenti di attivare l'hotspot personale	Selezionare quest'opzione per attivare la funzione dell'hotspot personale. La disponibilità di questa funzione dipende dall'operatore.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.7.5. Configurazione Slicing di rete 5G migliorato

Ivanti Neurons for MDM fornisce una configurazione di slicing di rete 5G migliorato per impostare slice di rete 5G per Android, consentendo agli operatori di telefonia mobile di allocare segmenti di rete 5G dedicati, o "slice", per raggruppare diverse applicazioni con esigenze simili, come bassa latenza o elevata larghezza di banda, in una slice specifica per una migliore ottimizzazione delle risorse di rete. Ciò consente agli amministratori MDM e ai provider di rete di gestire direttamente le sezioni per migliorare le prestazioni delle app.

Funzioni chiave

1. **Rete dedicata**: invece di condividere la singola slice di rete con tutte le applicazioni, la suddivisione in slice di rete consente a diverse applicazioni di utilizzare la propria slice di rete su misura per i propri requisiti specifici

2. **Personalizzazione**: l'amministratore può configurare il modo in cui le app vengono assegnate a specifiche slice di rete in base ai loro requisiti individuali, ad esempio garantendo una bassa latenza per le app di comunicazione in tempo reale o un'elevata larghezza di banda per i servizi di streaming come YouTube. Una slice pensata per il gaming ad alte prestazioni potrebbe dare priorità alla bassa latenza, mentre una per lo streaming multimediale sarebbe ottimizzata per un'elevata larghezza di banda.

3. **Coinvolgimento partner**: questa funzione richiede spesso la collaborazione dei fornitori di rete che definiscono le slice e informano gli amministratori MDM sull'elenco delle slice e sul loro significato.

Creazione di una configurazione Slicing di rete 5G migliorato

Procedura

1. **Aggiungi configurazione**

- Andare in **Configurazioni >> +Aggiungi**. Viene visualizzata la pagina **Aggiungi configurazione**.
- Inserire **Slicing di rete migliorato** nella barra di ricerca per configurare lo Slicing di rete migliorato. Viene visualizzata la pagina **Crea configurazione Slicing di rete migliorato**.
- Fare clic su **+Aggiungi descrizione** per immettere una descrizione della configurazione.

2. **Configura applicazione**

- In **Configurazione >> App Catalog**, immettere il nome dell'applicazione desiderata.
- Fare clic su **Aggiungi manualmente** se l'applicazione non è disponibile nel Play Store o nell'App Store.
- Inserire **ID pacchetto** e selezionare la **Slice di rete** appropriata dal menu a discesa.
- Selezionare la slice desiderata dal menu a discesa **Seleziona slice**.
- Fare clic su **Aggiungi**. L'applicazione apparirà ora in **Configura slice di rete** sotto la slice di rete selezionata.
- Per rimuovere un'applicazione, fare clic su **Rimuovi** nella sezione **Configura slice di rete**.

3. **Distribuisci configurazione**

- Fare clic su **Avanti**, selezionare o deselezionare la casella di controllo "**Abilita questa configurazione**", scegliere un'opzione di distribuzione (Tutti i dispositivi, Nessun dispositivo o Personalizzato),
- Fare clic su **Fatto** per completare la configurazione.

Configurazione Slicing di rete migliorato per Blocco & Kiosk

La creazione di una configurazione Slicing di rete 5G migliorato consente di configurare i dispositivi in modo che funzionino in modo limitato, assicurando che gli utenti abbiano accesso solo ad applicazioni e impostazioni specifiche.

Durante i seguenti blocchi è presente una casella di controllo "**Abilita slicing di rete 5G**":

- **Profilo di lavoro**- Sui dispositivi di proprietà dei dipendenti con un profilo di lavoro configurato utilizzando Android Enterprise versione 12.0, la casella di controllo "Abilita slicing di rete 5G" si trova in **Impostazione configurazione > Impostazioni di blocco profilo di lavoro**.
- **Dispositivo gestito con profilo di lavoro/Profilo di lavoro su dispositivi di proprietà aziendale** - In Dispositivo gestito con profilo di lavoro/Profilo di lavoro su dispositivi di proprietà aziendale con versioni Android 12.0 abbiamo la casella di controllo "Abilita slicing di rete 5G".

Si tratta di un'impostazione legacy che consente ai dispositivi di utilizzare lo slicing della rete 5G. La sua correlazione con la nuova configurazione Slicing di rete 5G migliorato è la seguente:

Se uno qualsiasi dei blocchi sopra indicati viene applicato a un dispositivo e l'opzione *Abilita slicing di rete 5G* **non** è selezionata, la configurazione *Slicing di rete 5G migliorato* non riuscirà con un errore.

Esempi

- **Caso 1**: Se il blocco del dispositivo non viene distribuito e viene distribuita la configurazione Slicing di rete migliorato, verrà attivata la configurazione avanzata.
- **Caso 2**: Se il blocco del dispositivo viene distribuito ma la casella di controllo 5G non è selezionata (falso), la configurazione di rete 5G avanzata genererà un errore.
- **Caso 3**: Se prima viene distribuito lo Slicing di rete migliorato, seguito dal blocco del dispositivo con la casella di controllo abilitata, la configurazione Slicing di rete migliorato continuerà a funzionare. Altrimenti si verificherà un errore.

Dettagli di configurazione:

- Se il blocco del dispositivo viene distribuito e la configurazione Slicing di rete migliorato viene inviata/distribuita, gli utenti devono assicurarsi che la casella di controllo Abilita slicing di rete 5G sia abilitata per evitare errori.
- Se la casella di controllo non è abilitata e la configurazione viene inviata, si verificherà un errore sul dispositivo.

10.10.7.6. Configurazione eSIM

La configurazione eSIM permette di configurare le impostazioni della rete cellulare nei dispositivi tramite il comando RefreshCellularPlans. Prima di mappare la rete cellulare al dispositivo, l'amministratore deve procurarsi l'URL del gestore della eSIM.

Applicabile a: Android 15+, iOS, iPadOS e Windows 11

Procedura per dispositivi Android 15+

1. Andare in **Configurazioni** >**+Aggiungi**.
2. Digitare eSIM nel campo di ricerca, quindi fare clic sulla configurazione **eSIM**.
3. Immettere un Nome e una Descrizione per la configurazione.
4. Dall'elenco **Piattaforma**, selezionare **Android**.
5. Nella sezione **Impostazione configurazione**, immettere l'**URL vettore**.
6. **Abilitazione automatica** - Selezionare questa opzione per scaricare il profilo eSIM e abilitarlo sul dispositivo in modo automatico. Se questa opzione non è selezionata, il profilo eSIM verrà scaricato, ma non verrà abilitato sul dispositivo in modo automatico.

> Questa opzione NON è disponibile per i dispositivi in modalità Profilo di lavoro.

7. Selezionare e distribuire la configurazione utilizzando una delle seguenti opzioni di distribuzione:
   - Tutti i dispositivi
   - Nessun dispositivo (impostazione predefinita)
   - Personalizzato
8. Fare clic su **Fine**.

EID per dispositivi Android 13+

L'opzione **Richiesta EID** è ora disponibile nella pagina dell'elenco Dettagli dispositivo e Dispositivi. Questa opzione è supportata solo per i dispositivi compatibili con eSIM sulle modalità Profilo di lavoro, Dispositivo gestito dal lavoro e Profilo di lavoro su dispositivo di proprietà aziendale. Se un dispositivo è registrato, l'EID verrà selezionato automaticamente per il dispositivo registrato e visualizzato nella pagina Dettagli dispositivo. In caso contrario, questo campo sarà abilitato e sarà possibile richiedere l'EID facendo clic su **Richiedi EID**. È inoltre possibile esportare l'EID utilizzando l'opzione **Esporta in CSV** dalla pagina Elenco dispositivi.

> Nella pagina **Dettagli dispositivo**, l'opzione **Richiedi EID** è disponibile per i dispositivi Android 13+ con Ivanti Go R122 o versione successiva.

Conserva Piano dati eSIM (applicabile per iOS 11+ Android 15.0+): quando si tenta di cancellare un dispositivo registrato con una configurazione eSIM, l'azione **Cancella dispositivo** fornisce un'opzione aggiuntiva per preservare il piano dati. Se si seleziona **Conserva piano dati eSIM (applicabile per iOS 11+ e Android 15.0+)** e si fa clic su **Cancella**, il piano dati eSIM esistente viene conservato mentre tutti gli altri dati sul dispositivo vengono cancellati. È possibile accedere a questa opzione dalla pagina **Dettagli dispositivo** o selezionando il dispositivo, aprendo il menu **Azioni** e facendo clic su **Cancella**.

Procedura per dispositivi iOS e iPadOS

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Digitare eSIM nel campo di ricerca, quindi fare clic sulla configurazione eSIM.
3. Immettere un Nome e una Descrizione per la configurazione.

4. Selezionare **iOS/iPadOS**.
5. Digitare l'URL del gestore.
6. Fare clic su **Avanti**.
7. Selezionare l'opzione Abilita questa configurazione.
8. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato
9. Fare clic su Fine.

Procedura per i dispositivi Windows 11

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Digitare eSIM nel campo di ricerca, quindi fare clic sulla configurazione eSIM.
3. Immettere un Nome e una Descrizione per la configurazione.
4. Nella sezione Scegli sistema operativo, fare clic su **Windows**.
5. Nella sezione Impostazioni di configurazione, digitare l'URL del gestore telefonico nella casella di testo Nome server (in formato FQDN).
    - È un server di Individuazione - Selezionare per contrassegnare il server come individuabile.
    - Abilitazione automatica: selezionare questa opzione per abilitare il profilo sul dispositivo una volta scaricato.
6. Fare clic su **Avanti**.
7. Selezionare l'opzione Abilita questa configurazione.
8. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato
9. Fare clic su **Fine**.

Ripristinare l'eSIM allo stato di fabbrica (solo per dispositivi Windows 11)

Questa opzione è disponibile nella sezione Dettagli dispositivo di tutti i dispositivi. Facendo clic su questa opzione verranno eliminati tutti i profili eSIM scaricati sul dispositivo.

Note importanti - Applicabile solo alla configurazione eSIM di Windows

>

- Quando un dispositivo è registrato, la sezione **Dettagli dispositivo** ora visualizza se il dispositivo supporta o meno eSIM in **Compatibile ESIM**. Per i dispositivi compatibili con eSIM, i rispettivi dettagli dell'identificatore eSIM sono visualizzati anche in **Identificatori ESIM**.
- Quando un dispositivo registrato Ivanti Neurons per MDM viene cancellato e nuovamente registrato, il vecchio record di questo dispositivo (con lo stato Cancellato) dovrebbe essere eliminato dalla pagina Dispositivi per evitare problemi di provisioning con la configurazione eSIM, su questo dispositivo nuovamente registrato.

- Se si reinvia la stessa configurazione a un dispositivo che ha già scaricato i profili, questi non verranno scaricati nuovamente. Se l'amministratore desidera che il dispositivo scarichi nuovamente i profili, è consigliabile ripristinare prima il modulo eSIM allo stato di fabbrica e poi eseguire il push/repush della configurazione eSIM.
- Quando una configurazione eSIM viene eseguita correttamente su un dispositivo, prima di dismettere il dispositivo, l'amministratore deve eseguire l'azione di cancellazione dell'eSIM, per garantire che i profili eSIM scaricati vengano cancellati dal dispositivo.
- La rimozione della configurazione eSIM eliminerà semplicemente la configurazione dal dispositivo. Se sul dispositivo sono stati rilevati, scaricati e attivati profili eSIM, tali dispositivi rimarranno attivi finché non verrà eseguita la cancellazione dei dati dell'eSIM.
- Eseguendo un'azione di cancellazione eSIM vengono rimossi tutti i profili eSIM scaricati dal dispositivo. Tuttavia, la configurazione eSIM che si trova nello stato Installato rimane intatta sul dispositivo. L'amministratore deve annullare la distribuzione della configurazione eSIM per rimuovere la configurazione dal dispositivo.

10.10.8. Altra configurazione

Argomenti della sezione:

- Configurazione dei domini associati
- Configurazione del trasferimento di file Android
- Configurazione di Apple TV
- Configurazione di AirPlay
- Mirroring di AirPlay
- Impostazioni browser
- Configurazione della modalità Single-App per iOS
- Configurazione di un profilo MDM iOS
- Configurare un profilo MDM di macOS
- Cache dei contenuti
- Creazione di un collegamento per Android
- Impostazioni nome dispositivo
- Configurazione Ethernet (macOS)
- Configurazione Integrazione server EMA
- Configurazione dello sfondo del dispositivo
- Configurazione del messaggio schermata di blocco
- Crea configurazione screen saver
- Configura Screen Saver utente
- Configurazione delle estensioni di sistema macOS
- Solo MAM
- Configurazione Google Play gestito
- Impostazioni Assistente migrazione
- Configurazione delle notifiche
- Impostazioni della stampante
- Configurazione Rimuovi Bloatware
- Configurazione delle restrizioni per telefoni Samsung
- Configurazione della modalità Single-App
- Menu Start e barra delle applicazioni
- Configurazione aggiornamento di sistema
- Gestione aggiornamenti di Windows
- Pianificazione delle app Windows
- Configurazione del BIOS di Windows
- Windows BitLocker
- Configurazione tutto schermo Windows

- Configurazione licenza Windows
- Configurazione della frequenza di raccomandazione di aggiornamento software

10.10.8.1. Configurazione dei domini associati

Licenza: Gold

La configurazione Domini associati è un dizionario che mappa le app ai loro domini associati. I domini associati possono essere utilizzati con funzioni come Extensible AppSSO, collegamenti universali e Riempimento automatico password.

Le impostazioni dei domini associati sono le seguenti:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Identificatore applicazione	(Obbligatorio) L'identificatore delle app a cui associare i domini.
Domini associati	(Obbligatorio) I domini da associare all'app. Ogni stringa ha la forma di "service:domain". I domini dovrebbero essere nomi host completi, come www.esempio.com.
Abilita download diretto	Se vero, i dati per questo dominio dovrebbero essere scaricati direttamente invece che attraverso un CDN. Il valore del titolo per questo dominio deve essere impostato su service:domain?mode=managed o questo valore sarà ignorato. Disponibile su macOS 11 e versioni successive. **Impostazione predefinita**: false

10.10.8.2. Configurazione del trasferimento di file Android

Nell'ambito di Android 11, Google ha apportato modifiche significative all'accesso allo storage di un dispositivo da parte delle app, che hanno avuto un impatto anche sul modo in cui le aziende riescono a inviare file a specifiche app su questi dispositivi. Tenendo conto di questi cambiamenti, molte grandi aziende si trovano di fronte a problemi di distribuzione dei file ai dispositivi e alle app, dato che i dispositivi si stanno aggiornando ad Android 11 e oltre. Qualsiasi approccio che dipenda da API specifiche dei fornitori di hardware limita le imprese nell'avere lo stesso approccio su dispositivi di produttori e versioni di sistemi operativi diversi.

Ivanti ha sviluppato una soluzione per il trasferimento di file che non dipende dalla versione di Android e dal fornitore di hardware. Questa soluzione si basa sulla capacità standard *Content-Provider* di Android. *Provider del contenuto* consente all'app Go di Ivanti di generare una posizione unica sul dispositivo per ogni file inviato tramite UEM.

La configurazione di trasferimento dei file è disponibile per i dispositivi Android in modalità completamente gestita. Utilizzando questa configurazione, l'amministratore può fornire un'opzione per trasferire i file sul dispositivo da condividere tra le diverse app consentite presenti sullo stesso dispositivo. Altre app possono utilizzare i file per qualsiasi motivo. Un esempio di utilizzo è l'inizializzazione della configurazione dell'app tramite JavaScript o la visualizzazione di informazioni aziendali tramite PDF o video. Ogni file caricato nelle configurazioni di trasferimento file di Ivanti viene scaricato da Ivanti Go quando riceve la configurazione corrispondente e il file associato. Il file viene archiviato in modo sicuro all'interno di Ivanti Go.

Altre app non possono accedere a questo file in modo arbitrario.

Ogni file scaricato all'interno dell'app sandbox è referenziato da una posizione unica, indicata anche come *ContentURI* o *URI*. Gli attributi personalizzati sono usati per mantenere il valore ContentURI sul server per ogni file su un dispositivo e possono aiutare gli amministratori a determinare la disponibilità di un file sul dispositivo, a formare gruppi dinamici di dispositivi e sono necessari per comunicare il ContentURI all'app di destinazione usando la configurazione dell'app gestita, ecc.

> Per le app non Ivanti, gli amministratori devono verificare con gli sviluppatori di app di terze parti il supporto di questo approccio, comunemente chiamato "Consumo di ContentURI basato su FileProvider".

Prerequisiti:

- Aggiungere un nuovo attributo personalizzato basato sul dispositivo da utilizzare per l'operazione Trasferimento file. Per ogni configurazione di Trasferimento di file, deve essere creato un attributo personalizzato unico. Ogni attributo dispositivo personalizzato può memorizzare solo il contentURI (posizione del file) dal dispositivo per un solo file per configurazione.

Procedura

1. Andare in **Configurazioni** > **Aggiungi configurazione** > **Trasferimento file**. Si apre la pagina **Crea configurazione trasferimento file**.
2. Immettere un nome per la configurazione nella casella **Nome**.
3. Immettere una **Descrizione** per la configurazione.
4. **Impostazioni configurazione**
   Nella sezione **File da trasferire**, selezionare i file da trasferire utilizzando l'opzione Trascina e rilascia o sfogliando l'opzione **Scegli file**. Per impostazione predefinita, il limite massimo delle dimensioni dei file è di 50 MB.
5. Selezionare una o più delle seguenti opzioni **Scarica sul dispositivo** (facoltativo):

- **Consenti il download su una rete a pagamento** - Selezionare per continuare a scaricare il file anche su una rete a pagamento
- **Richiedi la ricarica** - Selezionare per assicurarsi che il dispositivo sia in carica durante la procedura di trasferimento dei file
- **Richiedi inattività dispositivo** - Selezionare per mantenere il dispositivo inattivo durante la procedura di trasferimento dei file

6. Per condividere un file con altre app, utilizzare una delle due opzioni seguenti
   - **Trasferimento tramite Configurazione app gestita di Android**- Utilizzare questa opzione solo se l'app di destinazione può consumare l'URI del contenuto tramite la sua Configurazione app gestita.
   - **Trasferimento tramite l'intento sul dispositivo** - Gli intenti sono specifici dell'app. Per condividere un file utilizzando questa opzione, consultare la documentazione dell'app di destinazione e fornire le informazioni nella sezione Intenti di seguito. Gli intenti consentono alle app Ivanti Go di trasmettere un messaggio sul dispositivo una volta che il file è disponibile per essere condiviso con le app.

Trasferimento con Configurazione app gestita da Android

Procedura

1. Nel campo **Scegliere un attributo personalizzato esistente basato sul dispositivo per condividere questo file con altre app**, inserire un nome di attributo esistente, ad esempio **Custom-Filename**. Per ulteriori informazioni, vedere Assegnazione di attributi personalizzati ai dispositivi.
2. Il nome dell'attributo personalizzato deve essere un attributo nuovo e unico, utilizzato esclusivamente per questa operazione di trasferimento di file. Ogni attributo dispositivo personalizzato può memorizzare solo il contentURI (posizione del file) dal dispositivo per un solo file per configurazione.
   Fornire l'accesso alle seguenti app e/o nomi di pacchetti: è possibile selezionare i nomi delle app dal selettore Nomi app e aggiungere Nomi di pacchetti.

> Questi saranno gli unici pacchetti autorizzati ad accedere al file.

- **Nomi app** - È possibile selezionare i nomi delle app dal selettore Nomi app.
- **Nomi dei pacchetti** - In quest'area è possibile inserire gli ID dei pacchetti, ad esempio,Separare i nomi di più pacchetti con il punto e virgola (;).

```bash
com.mobileiron.filetransfer.android3.
```

Fare clic su **Salva**. La nuova configurazione di Trasferimento file appare nella pagina Configurazioni.

Configurazione dell'app di destinazione

Procedura

1. Andare in **App > Catalogo app**.
2. Selezionare l'app di destinazione che riceverà il file.
3. Accedere a **Configurazioni app > Configurazioni gestite per Android**.
4. Creare una nuova configurazione o utilizzare una configurazione esistente.

5. Un'app può avere un'impostazione come "Info manifest" o altre proprietà in cui l'amministratore può definire la variabile di sostituzione e comunicare la posizione del file all'app di destinazione. Per l'app Ivanti Velocity, ad esempio, nella finestra di dialogo Configurazione app > **Ottieni configurazioni** campo **> Info Manifest** inserire la variabile di sostituzione. Ad esempio, $Custom-File-Name$.
   Selezionare la propria distribuzione.
6. Fare clic su **Salva**.

Trasferimento tramite Intento sul dispositivo

Procedura

1. Nel campo **Scegliere un attributo di dispositivo esistente per passare il percorso del file negli intenti extra**, inserire un nuovo nome di attributo personalizzato, ad esempio deviceIntentURI.
2. Gli attributi personalizzati sono utilizzati per mantenere il valore della posizione (URI / ContentURI) sul server per ogni dispositivo e possono aiutare gli amministratori a determinare la disponibilità di un file sul dispositivo. Per ulteriori informazioni, vedere Assegnazione di attributi personalizzati ai dispositivi.
   Nel campo **Fornire accesso a nome app o pacchetto specifico**, inserire il **Nome app** o il **Nome pacchetto**, ad esempio Velocity.

> Questi saranno gli unici pacchetti autorizzati ad accedere al file.

3. Nella sezione Intenti-Standard, fornire i seguenti dettagli:
   - **Tipo di operazione** - Dall'elenco a discesa, selezionare **Avvia attività** / **Avvia servizio** o un'altra scelta simile a seconda dell'app. Scegliere il valore corretto per questo campo in base alle indicazioni dello sviluppatore dell'app di destinazione o fare riferimento alla documentazione dell'app di destinazione.
   - **Nome classe** (facoltativo) - Scegliere il valore giusto per questo campo in base alle indicazioni dello sviluppatore dell'app di destinazione o fare riferimento alla documentazione dell'app di destinazione.
   - **Azione** - Imposta l'azione su:o simile, come da app.

     Bash

     ```
     com.wavelink.nameofapp.action.INSTALL_CONFIG
     ```

   - **Categoria** - Inserire i valori separati da un punto e virgola (;).
   - **Tipo Mime** (Facoltativo) - Nel server host dell'amministratore, il file custom.mobileconfig deve essere impostato con un tipo MIME di applicazione/configurazione, in modo che il profilo MDM per il dispositivo venga scaricato e installato sul dispositivo. Scegliere il valore corretto per questo campo in base alle indicazioni dello sviluppatore dell'app di destinazione o fare riferimento alla documentazione dell'app di destinazione.
   - **Flag** (Facoltativo) - Selezionare il numero di flag da utilizzare. Scegliere il valore corretto per questo campo in base alle indicazioni dello sviluppatore dell'app di destinazione.

Fornire i valori di **Intents-Extras** in KEY, TYPE e VALUE (opzionale). Per parametri più specifici, consultare la documentazione dell'app OEM. Scegliere il valore corretto per questo campo in base alle indicazioni dello sviluppatore dell'app di destinazione o fare riferimento alla documentazione dell'app di destinazione.

5. Fare clic su **Salva**.

6. Nella pagina Configurazioni, selezionare la nuova configurazione di trasferimento dei file e poi selezionare **Azioni** > **Applica all'etichetta**. Si apre la finestra di dialogo **Applica a etichetta**.
7. Selezionare l'etichetta adatta e fare clic su **Applica**.
   Il trasferimento/condivisione di file con altre app può essere verificato solo raccogliendo i log dall'app di destinazione o dal dispositivo.

Verifica dello stato di download dei file

Gli attributi personalizzati sono usati per mantenere il valore della posizione (ContentURI) sul server per ogni file su ogni dispositivo e possono aiutare gli amministratori a determinare la disponibilità di un file sul dispositivo.

Procedura

1. Andare in **Dispositivi** > **Dispositivi**.
2. Selezionare un dispositivo specifico su cui è stata distribuita la configurazione di Trasferimento file.
3. Nella pagina Dettagli dispositivo, selezionare il dispositivo e quindi selezionare **Azioni** > **Imponi il check-in del dispositivo**.
4. Nella scheda Configurazioni, verificare che la configurazione Trasferimento file sia visualizzata con lo stato **Applicato**.
5. Nella scheda Attributi personalizzati, verificare che venga visualizzato il nome del nuovo attributo personalizzato (ad esempio, "Custom-File-Name$") con il relativo valore. Questo fornisce informazioni sulla posizione di memorizzazione del file sul dispositivo e mostra che il file è stato scaricato localmente sul dispositivo disponibile all'interno della sandbox dell'app Ivanti Go.
   Il trasferimento/condivisione di file con altre app può essere verificato solo raccogliendo i log dall'app di destinazione o dal dispositivo.

10.10.8.3. Configurazione di Apple TV

Licenza: Silver

La configurazione di Apple TV consente di definire la lingua e le impostazioni locali della Apple TV.

Impostazioni di Apple TV:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Lingua	Immettere il codice della lingua di due caratteri per specificare la lingua dell'interfaccia utente.
Impostazioni locali	Immettere l'ID delle impostazioni locali per specificare la combinazione di Paese/lingua per l'interfaccia utente.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.8.4. Mirroring di AirPlay

Licenza: Gold

Mirroring di AirPlay è una funzionalità che consente di visualizzare lo schermo di un dispositivo iOS su un monitor utilizzando Apple TV. È necessario che Apple TV e il dispositivo iOS siano connessi alla stessa rete Wi-Fi. Questa funzionalità necessita dei seguenti dispositivi:

- Dispositivi con iOS 7 o versioni successive - con supervisione
- Dispositivi con macOS 10.10 e versioni successive (supervisionati)
- Versione Apple TV - con supervisione
- AirPlay

> L'inclusione della gestione dei dispositivi non-iOS è irreversibile.

Argomenti della sezione:

- **Configurazione di Apple AirPlay**
- **Configurazione di AirPlay sul dispositivo mobile**
- **Configurazione di un monitor per l'interazione con Apple TV**
- **Connessione del dispositivo iOS a Apple TV**

Configurazione di Apple AirPlay

Per ulteriori informazioni sulle impostazioni di configurazione di AirPlay, vedere **Configurazione di AirPlay**.

Procedura

1. Accedere a **Configurazioni**.
2. Fare clic su **+Aggiungi**.
3. Fare clic su **AirPlay**.
4. Immettere un nome e una descrizione per la configurazione nei campi appropriati.
5. Per tutte le versioni iOS supportate, immettere un nome del dispositivo e una password.
6. Fare clic su + **Aggiungi** per aggiungere un altro dispositivo, se necessario.
7. Per dispositivi con iOS 7+ (supervisionati) o macOS 10.10+, è possibile aggiungere ID dispositivo a un Elenco elementi consentiti.
8. Fare clic su **Avanti**.
9. Scegliere un livello di distribuzione.
10. Fare clic su **Fine**.

Configurazione di AirPlay sul dispositivo mobile

Procedura

1. Configurare **Apple Configurator**.
2. Andare a **Dispositivi > Dispositivi**.

3. Fare clic sul nome di un dispositivo iOS per visualizzare la pagina con le informazioni relative al dispositivo specifico.
4. Fare clic sull'icona ⋮.
5. Selezionare **Mirroring di AirPlay** per visualizzare la finestra di dialogo relativa al mirroring di AirPlay.
6. Selezionare un dispositivo Apple TV dal menu a discesa.
7. Immettere un tempo di scansione espresso in secondi per specificare un limite di tempo per la ricerca del dispositivo selezionato.
8. Immettere una password per il dispositivo Apple.
9. Fare clic su **Invia richiesta**.

Configurazione di un monitor per l'interazione con Apple TV

Procedura

1. Su un monitor connesso ad Apple TV, andare a **Impostazioni > Profilo**.
2. Selezionare **Ivanti Neurons for MDM Apple Configurator**.
3. Fare clic su **Aggiungi profilo**.
4. Fare clic sull'icona ⋮.
5. Selezionare **Mirroring di AirPlay** per visualizzare la finestra di dialogo relativa al mirroring di AirPlay.
6. Selezionare un dispositivo Apple TV dal menu a discesa.
7. Immettere un tempo di scansione espresso in secondi per specificare un limite di tempo per la ricerca del dispositivo selezionato.
8. Immettere una password per il dispositivo Apple.
9. Fare clic su **Invia richiesta**.

Connessione del dispositivo iOS a Apple TV

Procedura

1. Connettere il dispositivo Apple TV a un monitor.
2. Utilizzando il telecomando di Apple TV, andare su **Impostazioni > Account > Home Sharing** per abilitare l'Home Sharing.
3. **Connettere il dispositivo iOS** alla stessa rete Wi-Fi del **dispositivo Apple TV**.
4. Aprire l'applicazione Telecomando sul dispositivo **iOS**.
5. Abilitare **Home Sharing** dalla schermata **Impostazioni del telecomando**.

10.10.8.5. Impostazioni browser

Impostazioni browser permette di configurare le impostazioni e le restrizioni per Google Chrome, Mozilla Firefox, Microsoft Edge e Internet Explorer nei dispositivi Windows 10.

Questa funzione richiede Bridge. Per ulteriori dettagli, vedere **Ivanti Bridge**.

> Assicurarsi che i browser siano installati nel dispositivo prima di applicare le impostazioni del browser.

Per configurare le impostazioni del browser:

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Impostazioni browser**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Nella sezione Impostazioni configurazione, specificare le impostazioni rimanenti come descritto nella tabella seguente.

Impostazione	Operazione da eseguire
Browser	Selezionare il tipo di browser per cui è necessario applicare le impostazioni: • **Chrome** • **Firefox** • **Microsoft Edge** • **Internet Explorer**
Impostazioni browser	Configurare le opzioni seguenti: **Consenti browser**: • Consenti salvataggio delle password • Consenti modalità di navigazione sicura • Consenti ai plugin obsoleti di rimanere nel browser **Chrome e Firefox**: • **Consenti eliminazione cronologia del browser** **Chrome e Internet Explorer**: • **Consenti stampa del browser** • **Nuovo URL pagina scheda** **Solo Chrome**: • **Mostra scelte rapide app nella barra dei segnalibri** • **Mostra pulsante Home** • **Consenti sincronizzazione dei dati con Google** • **Continua a eseguire app in background quando Chrome è chiuso** **Solo Firefox**: • **Consenti installazione estensioni** **Solo Internet Explorer**: • **Consenti download dei dati da siti Web**
Preferiti browser	Fare clic su **+Aggiungi**. Viene visualizzata la finestra **Aggiungi preferiti browser**. Configurare i campi seguenti: • **Nome visualizzato**: digitare il nome visualizzato per preferito • **URL**: digitare l'URL del preferito del browser. Fare clic su **Aggiungi**. Le informazioni specifiche relative al preferito del browser aggiunto vengono visualizzate in questa pagina. Nella colonna **Azioni** fare clic sull'icona Modifica per modificare l'impostazione. Per eliminare il preferito del browser, fare clic sull'icona Elimina. **Nome cartella preferiti del browser**: digitare il nome della cartella preferiti del browser nella posizione in cui si desidera raccogliere i preferiti. È anche possibile aggiungere i preferiti browser in un formato CSV. Per caricare nel formato CSV: 1. Fare clic su Carica file CSV. Individuare e scegliere il file CSV da caricare. 2. Fare clic su **Carica**. Le informazioni dettagliate nel file CSV devono essere aggiunte nel seguente formato:

Impostazione	Operazione da eseguire
	• La prima colonna (Nome visualizzato) deve contenere il nome visualizzato del preferito. Ad esempio: "shopping". • La seconda colonna (URL) deve contenere l'URL del preferito. Ad esempio: "https://amazon.com".
Sicurezza del sito Web	Configurare le seguenti impostazioni di sicurezza del sito Web: **Tutti i siti Web (Chrome e Firefox)** • **Blocca cookie** • **Blocca Javascript** • **Blocca plugin** • **Blocca popup** Siti Web specifici (solo Chrome) **Siti web bloccati (Chrome e Edge)**: aggiungere il sito Web che si desidera bloccare. Fare clic su **+Aggiungi**. Viene visualizzata la finestra **Aggiungi sito Web all'elenco degli elementi non consentiti**. Digitare nel campo **URL sito Web** l'URL del sito Web che si desidera inserire nell'elenco degli elementi non consentiti. Nel campo **Accesso** selezionare **Blocca** per inserire il sito Web nell'elenco degli elementi non consentiti. L'opzione predefinita è **Consenti**. Fare clic su **Aggiungi**.
Estensioni browser	**Tipi di estensione consentiti (solo Chrome)**: selezionare una delle seguenti opzioni: • **Estensione** • **Script utente** • **Temi** • **App pacchetto** • **App ospitata** • **App piattaforma** **Sorgenti dell'estensione del browser (solo Chrome)**: Fare clic su **+Aggiungi** per aggiungere le origini dell'estensione browser. Dopo aver aggiunto le origini dell'estensione browser, è possibile modificarle o eliminarle facendo clic sulle relative opzioni nella colonna **Azioni**. **Imponi l'installazione delle estensioni (solo Chrome)**: Fare clic su **+Aggiungi** per aggiungere le estensioni per forzare l'installazione. Dopo aver aggiunto le estensioni per forzare l'installazione, è possibile modificare o eliminare le origini facendo clic sulle relative opzioni nella colonna **Azioni**.

6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni di distribuzione:

- Tutti i dispositivi
- Nessun dispositivo (impostazione predefinita)
- Personalizzato

8. Fare clic su **Fine**.

10.10.8.6. Configurazione della modalità Single-App per iOS

Licenza: Silver

La modalità Single-App limita i dispositivi iOS e tvOS per l'utilizzo dell'app specificata. Ad esempio, può essere opportuno configurare i dispositivi che possono utilizzare solo un'app personalizzata sviluppata dalla propria organizzazione.

Procedura

1. Andare a **Configurazioni > Aggiungi > Modalità Single-App**.
2. Utilizzare le linee guida seguenti per definire l'app e le impostazioni correlate.
3. Fare clic su **Avanti**.

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Scegli app	Selezionare il metodo da utilizzare per la scelta dell'app: • **Da Catalogo app e App di sistema**: selezionare questa opzione per cercare nel Catalogo app Ivanti Neurons for MDM e nelle app di sistema (preinstallate per impostazione predefinita sui dispositivi Apple). • Immettere il nome dell'app e selezionarla quando compare nell'elenco delle applicazioni. • **Inserisci ID bundle:** selezionare per inserire l'identificatore univoco per l'app di sistema che si desidera selezionare. Utilizzare questa opzione se non è possibile trovare l'app di sistema utilizzando l'opzione **Da App Catalog e app di sistema**.
Disattiva Touch	Selezionare questa opzione per disattivare lo schermo touch.
Disattiva rotazione dispositivo	Selezionare questa opzione per disattivare il sensore di rotazione del dispositivo.
Disattiva pulsanti volume	Selezionare questa opzione per disattivare i pulsanti del volume del dispositivo.
Disattiva interruttore suoneria/silenzioso	Selezionare questa opzione per disattivare l'interruttore suoneria/silenzioso del dispositivo.
Disattiva tasto accensione/spegnimento	Selezionare questa opzione per disattivare il tasto di accensione/spegnimento (in alto a destra sul lato del dispositivo).
Disattiva blocco automatico	Selezionare questa opzione per impedire lo standby del dispositivo dopo un periodo di inattività.
Attiva VoiceOver	Selezionare questa opzione per attivare il lettore schermo VoiceOver (funzione di accessibilità).
Attiva zoom	Selezionare questa opzione per attivare lo zoom (funzione di accessibilità).
Attiva Inverti colori	Selezionare questa opzione per attivare la regolazione dei colori (funzione di accessibilità).
Attiva Assistive Touch	Selezionare questa opzione per attivare Assistive Touch (funzione di accessibilità).
Attiva Pronuncia selezione	Selezionare questa opzione per attivare Pronuncia selezione (funzione di accessibilità).
Attiva audio mono	Selezionare questa opzione per passare dall'audio stereo all'audio mono (funzione di accessibilità).

Impostazione	Operazione da eseguire
Regolazioni VoiceOver	Selezionare questa opzione per consentire agli utenti di effettuare le regolazioni VoiceOver.
Regolazioni Zoom	Selezionare questa opzione per consentire agli utenti di effettuare le regolazioni dello zoom.
Regolazioni Inverti colori	Selezionare questa opzione per consentire agli utenti di invertire i colori.
Regolazioni Assistive Touch	Selezionare questa opzione per consentire agli utenti di effettuare le regolazioni Assistive Touch.

4. Nella schermata **Distribuzione**, selezionare i gruppi di dispositivi che riceveranno questa configurazione.
5. Fare clic su **Fine**.

Se si è configurata la connessione telefonica come app da utilizzare, il pulsante Home funziona quando il dispositivo entra in modalità singola app.

10.10.8.7. Configurazione di un profilo MDM iOS

La configurazione MDM iOS definisce i limiti di accesso per Ivanti Neurons per MDM. Esistono due tipi di configurazioni MDM iOS:

- **MDM iOS - Fornita in blocco:** per i dispositivi acquistati dall'azienda e forniti come parte di una distribuzione di massa.
- **MDM iOS - Fornita singolarmente:** per i dispositivi forniti uno per uno. Le impostazioni non verranno applicate ai dispositivi supervisionati o registrati dall'utente.

Viene fornita solo una configurazione per ciascun tipo, consentita in tutti gli spazi.

Modifica di una configurazione MDM iOS

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Accedere a **Configurazioni**.
3. Selezionare la configurazione MDM iOS da modificare.
4. Fare clic sull'icona matita (modifica) per modificare la configurazione.
5. Per apportare modifiche, utilizzare le linee guida seguenti:
6. Fare clic su **Fine**.

Impostazione	Operazione da eseguire
Diritti di accesso MDM	
Consenti blocco dispositivo e rimozione passcode	Deselezionare questa opzione per evitare l'imposizione di una configurazione di conformità del passcode.
Consenti eliminazione dispositivo	Deselezionare questa opzione per evitare l'imposizione di un'azione di cancellazione del dispositivo.
Consenti query delle informazioni di rete (numeri di telefono/SIM, indirizzo MAC)	Deselezionare questa opzione per escludere il dispositivo dalla creazione di report delle informazioni sulla rete. Se questa opzione è deselezionata, la visualizzazione dell'elenco dei dispositivi e la visualizzazione dei dettagli del dispositivo mostrerà N/D per le informazioni sulla rete di cui non sono più stati creati i report. Inoltre, le policy di roaming non potranno essere imposte ai dispositivi interessati.
Password rimozione profilo	
Password per rimuovere il profilo	Specificare una password. All'utente verrà richiesto di inserire la password durante l'eliminazione di un profilo dal dispositivo.
Aggiungi app richiesta (iOS 15 e versioni successive)	
Aggiungi da ricerca	Immettere il nome dell'app e cercarla nell'App Store, quindi selezionare l'app necessaria. È possibile aggiungere una sola app alla volta. La selezione di un'app disabilita le altre app.
Aggiungi manualmente	Immettere l'ID iTunes dell'app.

Le proprie modifiche si applicano solo ai dispositivi con provisioning a seguito della modifica.

10.10.8.8. Configurare un profilo MDM di macOS

La configurazione MDM macOS definisce i limiti di accesso per Ivanti Neurons per MDM. Le configurazioni MDM per macOS vengono fornite singolarmente per i dispositivi forniti uno per uno.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Accedere a **Configurazioni**.
3. Selezionare la configurazione MDM macOS che si desidera modificare.
4. Fare clic sull'icona matita (modifica) per modificare la configurazione.
5. Per apportare modifiche, utilizzare le linee guida seguenti:
6. Fare clic su **Fine**.

Impostazione	Operazione da eseguire
Consenti blocco dispositivo e rimozione passcode	Deselezionare questa opzione per evitare l'imposizione di una configurazione di conformità del passcode.
Consenti eliminazione dispositivo	Deselezionare questa opzione per evitare l'imposizione di un'azione di cancellazione del dispositivo.
Consenti query delle informazioni di rete (numeri di telefono/SIM, indirizzo MAC)	Deselezionare questa opzione per escludere il dispositivo dalla creazione di report delle informazioni sulla rete. Se questa opzione è deselezionata, la visualizzazione dell'elenco dei dispositivi e la visualizzazione dei dettagli del dispositivo mostrerà N/D per le informazioni sulla rete di cui non sono più stati creati i report. Inoltre, le policy di roaming non potranno essere imposte ai dispositivi interessati.
Password rimozione profilo	
Password per rimuovere il profilo	Specificare una password. All'utente verrà richiesto di inserire la password durante l'eliminazione di un profilo dal dispositivo.

Le proprie modifiche si applicano solo ai dispositivi con provisioning a seguito della modifica.

10.10.8.9. Cache dei contenuti

Licenza: Gold

Applicabile a: macOS 10.13.4 o versioni successive supportate.

Servizio di configurazione della cache dei contenuti per consentire copie locali del software App Store e abilitare i client connessi per un download più veloce di software e app.

Configurazione della cache dei contenuti

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **cache** nel campo di ricerca, quindi fare clic sulla configurazione **Cache dei contenuti**.
4. Immettere un nome e una descrizione per la configurazione.
5. Inserire le **impostazioni di configurazione della cache dei contenuti**.
6. Fare clic su **Avanti**.
7. Selezionare l'opzione **Abilita questa configurazione**.
8. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato
9. Fare clic su **Fine**.

Impostazioni di configurazione della cache dei contenuti

Utilizzare le impostazioni nella seguente tabella per configurare la cache dei contenuti. Per ulteriori informazioni su queste impostazioni, vedere la **documentazione di Apple**.

Impostazione	Descrizione
Consenti al sistema di eliminare contenuti dalla cache automaticamente (Disponibile in macOS 10.15 o versioni più recenti supportate).	Consente al sistema di eliminare automaticamente i contenuti dalla cache quando c'è bisogno di spazio su disco per altre applicazioni (es. quando lo spazio libero su disco si esaurisce sul computer). Di default questa opzione è abilitata.
Consenti la cache personale	Cache dei dati iCloud dell'utente. Potrebbe volerci del tempo (ore o giorni) prima che i client reagiscano ai cambiamenti a questa impostazione; non ha un effetto immediato. Di default questa opzione è abilitata.
Consenti la cache condivisa	Il contenuto non iCloud della cache, come ad esempio app e aggiornamenti software. Potrebbe volerci del tempo (ore o giorni) prima che i client reagiscano ai cambiamenti a questa impostazione; non ha un effetto immediato. Di default questa opzione è abilitata.
Consenti l'attivazione automatica della cache dei contenuti	Attiva automaticamente la cache dei contenuti quando possibile e impedisce che venga disabilitata.
Consenti l'auto-abilitazione della cache con tethering (Disponibile in macOS 10.15.4 o versioni successive supportate)	Attiva automaticamente la condivisione della connessione Internet quando possibile e ne impedisce la disattivazione.
Disattiva la cache con tethering	Disattiva la cache con tethering. L'opzione Disattiva la cache con tethering prevale sull'opzione Consenti l'auto-abilitazione della cache con tethering.
Limite della cache	Il numero massimo di byte di spazio su disco che saranno utilizzati per la cache dei contenuti. Il valore 0 indica uno spazio su disco illimitato. Valore standard: 0
Percorso dei dati	Il percorso alla directory utilizzata per memorizzare i contenuti nella cache. Cambiando questa impostazione in modo manuale non si spostano automaticamente i contenuti nella cache dalla vecchia posizione a quella nuova. Per spostare i contenuti automaticamente, utilizzare il riquadro Cache dei contenuti della preferenza di condivisione. Il valore deve essere (o terminare con) /Library/Application Support/Apple/AssetCache/Data.
Consenti la visualizzazione di avvisi (Disponibile in macOS	L'opzione Cache dei contenuti mostra le condizioni eccezionali (avvisi) come notifiche di sistema nell'angolo in alto dello schermo.

Impostazione	Descrizione
10.15 o versioni più recenti supportate).	
Tieni attivo il dispositivo (Disponibile in macOS 10.15 o versioni più recenti supportate).	Impedisce al computer di rimanere inattivo finché l'opzione Cache dei contenuti è attiva (Preferenze di sistema > Condivisione > Cache dei contenuti è attiva).
Intervalli di ascolto	Una serie di dizionari che descrivono un intervallo di indirizzi IP da servire.
Primo indirizzo IP	Primo indirizzo IP dei client negli intervalli di ascolto.
Ultimo indirizzo IP	Ultimo indirizzo IP dei client negli intervalli di ascolto.
Tipo di indirizzo IP	Selezionare una delle seguenti opzioni: • IPv4 (predefinito) • IPv6
Consenti solo intervalli di ascolto	La cache dei contenuti fornisce contenuti ai client solo negli intervalli di ascolto.
Consenti ascolto con colleghi e familiari	La cache dei contenuti fornisce contenuti ai client nell'unione di Intervalli di ascolto, Intervalli ascolto colleghi, e Familiari. Di default questa opzione è abilitata.
Consenti solo reti secondarie locali	La cache dei contenuti fornisce contenuti ai client solo sulla stessa rete locale immediata. Nessun contenuto viene offerto ai client su altre reti raggiungibili dalla cache dei contenuti. Se questa opzione è abilitata, gli intervalli di ascolto saranno ignorati. Di default questa opzione è abilitata.
Registra identità client	La cache dei contenuti registra l'indirizzo IP e il numero di porta dei client che richiedono il contenuto.
Policy di selezione dei familiari	Selezionare una delle seguenti opzioni di policy: • Primo orario disponibile • Hash percorso URL • Round-robin (predefinito) • Casuale • Sticky-disponibile
Familiari	Una serie di indirizzi IP locali di altre cache di contenuti da cui questa cache dovrebbe effettuare il download o l'upload, invece effettuare il download o l'upload su Apple direttamente. Fare clic su **+ Aggiungi** per aggiungere uno o più indirizzi IP.
Consenti solo reti secondarie locali di colleghi	La cache di contenuti si collega solo con altre cache di contenuti sulla stessa rete locale immediata, piuttosto che con le cache dei contenuti che utilizzano lo stesso indirizzo IP pubblico del dispositivo. Di default questa opzione è abilitata.

Impostazione	Descrizione
Porta	Il numero della porta TCP su cui la cache dei contenuti accetta le richieste di upload o download. Impostare la porta su 0 per scegliere una porta disponibile a caso. Valore standard: 0
Intervalli pubblici	Una serie di dizionari che descrivono un intervallo di indirizzi IP pubblici che i server Ivanti Neurons for MDM dovrebbero usare per la corrispondenza dei client con le cache di contenuti.
Primo indirizzo IP	Primo indirizzo IP dei server negli intervalli pubblici.
Ultimo indirizzo IP	Ultimo indirizzo IP dei server negli intervalli pubblici.
Tipo di indirizzo IP	Selezionare una delle seguenti opzioni: • IPv4 (predefinito) • IPv6

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.8.10. Creazione di un collegamento per Android

In modalità tutto schermo i collegamenti sono disponibili solo se si utilizza un browser consentito. Il browser deve essere consentito nella configurazione Blocco e

tutto schermo. I collegamenti rapidi appariranno nel launcher Ivanti Neurons per MDM Kiosk.

Procedura

1. Accedere a **Configurazioni**. **> +Aggiungi**
2. Fare clic su **Collegamento rapido Android** per visualizzare la pagina **Crea configurazione collegamento rapido Android**.
3. Immettere un nome per la configurazione nel campo **Nome**.
4. Immettere una descrizione della configurazione nel campo **Descrizione**.
5. Immettere un'etichetta univoca per il collegamento rapido nel campo **Etichetta**.
6. Immettere un URL per la destinazione del collegamento rapido nel campo **URL**.
7. In via opzionale, è possibile trascinare e rilasciare un file nel campo dell'icona o fare clic su **Scegli file** per navigare nel file e scegliere un'icona per il collegamento rapido.
8. Fare clic su **Avanti**.

10.10.8.11. Creazione delle configurazioni delle impostazioni di accessibilità

Questa configurazione consente alle aziende di limitare, modificare o configurare le impostazioni di accessibilità sui dispositivi Apple.

Procedura

1. Accedere a **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Fare clic su **Configurazioni delle impostazioni di accessibilità**.
4. Configurare le impostazioni specificate nella tabella seguente:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Selezionare una delle impostazioni di accessibilità	• **Impostazioni di accessibilità**: utilizzare questa impostazione per configurare le impostazioni di accessibilità sui dispositivi macOS. • **Restrizioni impostazioni accessibilità**: utilizzare questa opzione per limitare le modifiche alle impostazioni di accessibilità per i dispositivi iOS.
Impostazioni di accessibilità	**Impostazioni configurazione**
Vista da vicino Punto lontano	Il livello minimo di zoom nelle impostazioni zoom
Vista da vicino Punto vicino	Il livello massimo di zoom nelle impostazioni zoom
	Abilitare "Usa gesti di scorrimento" nelle opzioni di zoom
	Abilitare "Immagini uniformi" nelle opzioni di zoom
Valore di contrasto	Specificare il valore
    Dimensione cursore Ritardo iniziale del driver del mouse Velocità massima driver del mouse Abilitare "Tasto lento" nelle opzioni Tastiera Abilitare il "suono del tasto clic" per i tasti lenti Ritardo tasti lenti Specificare il valore in millisecondi	Selezionare la casella di controllo - Abilita "Flash schermo" nelle opzioni Audio Selezionare la casella di controllo - Abilita i tasti del mouse nelle opzioni Mouse e Trackpad Specificare il valore Selezionare la casella di controllo - Ignora trackpad incorporato Specificare il valore Specificare il valore Selezionare la casella di controllo Selezionare la casella di controllo Selezionare la casella di controllo Selezionare la casella di controllo
Selezionare la casella di controllo - Riproduci audio stereo come mono	Selezionare la casella di controllo
Abilitare i tasti permanenti nelle opzioni della tastiera	Selezionare la casella di controllo
Abilitare il segnale acustico quando viene impostato un tasto modificatore per i tasti	Selezionare la casella di controllo

Impostazione	Operazione da eseguire
permanenti	
Abilitare la visualizzazione dei tasti premuti sullo schermo per i tasti permanenti	Selezionare la casella di controllo
Attiva VoiceOver	Selezionare la casella di controllo
Abilitare l'inversione dei colori nelle sistemazioni di visualizzazione	Selezionare la casella di controllo
Restrizioni accessibilità	**Impostazioni configurazione**
Abilitare testo in grassetto	Selezionare la casella di controllo
Abilitare l'aumento del contrasto	Selezionare la casella di controllo
Abilitare il movimento ridotto	Selezionare la casella di controllo
Abilitare la trasparenza ridotta	Selezionare la casella di controllo
App di accessibilità dimensione testo che supporta l'uso del testo dinamico	Selezionare l'opzione dall'elenco a discesa
Abilitare le sistemazioni tattili	Selezionare la casella di controllo
Attiva VoiceOver	Selezionare la casella di controllo
Attiva zoom	Selezionare la casella di controllo

5. Selezionare l'opzione di distribuzione e specificare i dettagli richiesti se applicabile.
6. Fare clic su **Fine**.

10.10.8.12. Crea configurazione screen saver

La Configurazione screen saver consente di aggiungere opzioni come Password, Tempo di inattività, Percorso e nome del modulo.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Fare clic su **Configurazioni**.
3. Fare clic su +**Aggiungi**.
4. Digitare screen nel campo di ricerca, quindi fare clic su **Screen saver**:
   Viene visualizzata la pagina dei dettagli relativa alla configurazione Crea screen saver.
5. Configurare le impostazioni su questa pagina. Fare riferimento alla tabella presente nella sezione **Impostazioni configurazione screen saver** per istruzioni sui valori.
6. Fare clic su **Avanti** per configurare le impostazioni di distribuzione, quindi fare clic su **Fine**.

Impostazioni configurazione screen saver

Impostazione	Operazione da eseguire
Nome (obbligatorio)	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Richiesta casella di controllo password	Selezionare la casella di controllo per richiedere la password all'utente del dispositivo quando lo screen saver viene sbloccato o fermato. (Disponibile su macOS 10.13 e versioni successive).
Richiesta di ritardo per la password	Specificare la durata del ritardo in secondi.
Tempo di inattività della finestra di login	Specificare il tempo di inattività in secondi trascorso il quale deve apparire lo screen saver.
Percorso al modulo screen saver	Specificare il percorso al modulo screen saver.
Nome del modulo screen saver (obbligatorio)	Inserire il nome dello screen saver.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.8.13. Configura Screen Saver utente

La Configurazione screen saver utente consente di aggiungere opzioni come Password, Tempo di inattività, Percorso e nome del modulo.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Fare clic su **Configurazioni**.
3. Fare clic su +**Aggiungi**.
4. Digitare "screen" nel campo di ricerca, quindi fare clic su **Screen saver utente**:
   Viene visualizzata la pagina dei dettagli relativa alla configurazione Crea screen saver utente.
5. Configurare le impostazioni su questa pagina. Fare riferimento alla tabella presente nella sezione **Impostazioni configurazione screen saver utente** per istruzioni sui valori.
6. Fare clic su **Avanti** per configurare le impostazioni di distribuzione, quindi fare clic su **Fine**.

Impostazioni configurazione screen saver utente

Impostazione	Operazione da eseguire
Nome (obbligatorio)	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Tempo di inattività	Specificare il tempo di inattività in secondi trascorso il quale deve apparire lo screen saver.
Percorso al modulo screen saver	Specificare il percorso al modulo screen saver.
Nome del modulo screen saver (obbligatorio)	Inserire il nome dello screen saver.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.8.14. Impostazioni nome dispositivo

Licenza: Silver

Una configurazione predefinita del nome del dispositivo permette di creare una nuova configurazione che viene inoltrata al dispositivo al livello di registrazione o post-registrazione e permette la denominazione del dispositivo. L'amministratore può definire nomi di dispositivi predefiniti solo per i dispositivi **supervisionati con iOS 8**. È possibile utilizzare le variabili riportate di seguito per creare il nome del dispositivo:

- Numero di serie del dispositivo
- IMEI del dispositivo
- Modello dispositivo
- Ivanti Neurons per MDM Nome utente (solo utenti locali)
- Unità organizzativa (OU, Organizational Unit) LDAP
- Nome comune (CN, Common Name) LDAP

Ad esempio, si desidera immettere $-$ per i nomi dei dispositivi che iniziano con il numero di serie del dispositivo e finiscono con l'organizzazione dell'utente come definita in LDAP.

Impostazioni nome dispositivo predefinito (per iOS)

Impostazione	Operazione da eseguire
Nome Descrizione	Immettere un nome identificativo della configurazione. Immettere una descrizione esplicativa dello scopo della configurazione.
Nome dispositivo	Inserire il formato per il nome predefinito del dispositivo, incluso il dispositivo disponibile e gli attributi LDAP.* Se il nome dispositivo risultante supera i 63 caratteri, verrà troncato per assicurarne la corretta visualizzazione sul dispositivo.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.

Digitare $ per visualizzare un elenco delle **variabili** supportate eventualmente disponibili per questo campo.

Impostazioni nome dispositivo (Android)

Il nome del dispositivo Android può essere recuperato da Go app. Quando l'amministratore genera il rapporto Dettagli dispositivo, il nome effettivo del dispositivo viene mostrato al posto del modello del dispositivo o il nome del produttore. Se l'utente cambia il nome del dispositivo, il nuovo nome verrà mostrato la prossima volta in cui viene generato il report. Il rispettivo nome del dispositivo può essere visualizzato sotto **Dispositivi** > **Impostazioni** > **Nome dispositivo**.

10.10.8.15. Configurazione dello sfondo del dispositivo

Licenza: Silver

La configurazione dello sfondo del dispositivo definisce un'immagine di sfondo predefinita per la schermata principale e la schermata di blocco dei dispositivi Android 7.0 in modalità Proprietario dispositivo o dei dispositivi Company Owned Personal Enabled (COPE) (tranne i dispositivi in modalità Android 11 EPO).

Impostazioni dello sfondo di Android

Per definire un'immagine di sfondo predefinita per i dispositivi Android:

1. Accedere a **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Fare clic su **Sfondi dispositivo**.
4. Fare clic sull'icona Android per visualizzare la sezione delle impostazioni di configurazione di Android e configurare le seguenti impostazioni
5. Fare clic su **Avanti**

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Carica sfondo Android	
Utilizzare la stessa immagine per la schermata principale e la schermata di blocco	Selezionare per caricare un'immagine singola per entrambe le schermate.
Schermata principale	Trascinare l'immagine oppure fare clic su **Scegli file** per selezionarne una.
Schermata di blocco	Trascinare l'immagine oppure fare clic su **Scegli file** per selezionarne una.

6. Selezionare una delle seguenti opzioni di distribuzione:

- **Tutti i dispositivi**
- **Nessun dispositivo** (impostazione predefinita)
- **Personalizzato**

7. Fare clic su **Fine**.

> Le immagini caricate devono essere in formato .jpg o .png.

Impostazioni dello sfondo di iOS

È possibile definire un'immagine di sfondo predefinita per i dispositivi iOS.

> Questa impostazione è applicabile solo ai dispositivi supervisionati.

1. Accedere a **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Fare clic su **Sfondi dispositivo**.
4. Fare clic sull'icona iOS per visualizzare la sezione delle impostazioni di configurazione di iOS e configurare le seguenti impostazioni
5. Fare clic su **Avanti**.

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Carica sfondo iPhone	
Utilizzare la stessa immagine per la schermata principale e la schermata di blocco	Selezionare per caricare un'immagine singola per l'iPhone.
Schermata principale	Trascinare l'immagine oppure fare clic su **Scegli file** per selezionarne una.
Schermata di blocco	Trascinare l'immagine oppure fare clic su **Scegli file** per selezionarne una.
Carica sfondo iPad	
Utilizzare la stessa immagine per la schermata principale e la schermata di blocco	Selezionare per caricare un'immagine singola per l'iPad.
Schermata principale	Trascinare l'immagine oppure fare clic su **Scegli file** per selezionarne una.
Schermata di blocco	Trascinare l'immagine oppure fare clic su **Scegli file** per selezionarne una.

6. Selezionare una delle seguenti opzioni:

- **Tutti i dispositivi**
- **Nessun dispositivo** (impostazione predefinita)
- **Personalizzato**

7. Fare clic su **Fine**.

> Le immagini caricate devono avere dimensioni 640 (L) x 1136 (A) ed essere in formato .jpg o .png.

Impostazioni dello sfondo di macOS

Per definire un'immagine di sfondo predefinita per i dispositivi macOS:

1. Accedere a **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Fare clic su **Sfondi dispositivo**.
4. Fare clic sull'icona macOS per visualizzare la sezione Impostazioni configurazione per macOS.
5. Inserire il percorso dell'immagine per i desktop.
6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni:
    - **Tutti i dispositivi**
    - **Nessun dispositivo** (impostazione predefinita)
    - **Personalizzato**
8. Fare clic su **Fine**.

> È possibile modificare gli sfondi in base alla limitazione. Se risulta abilitata la configurazione delle limitazioni macOS **Consenti modifica del Wallpaper**, allora sarà possibile modificare il wallpaper.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.8.16. Configurazione Integrazione server EMA

La configurazione Integrazione server EMA consente ai dispositivi Windows 10 di connettersi al server Intel EMA configurato. Per collegare i dispositivi al server Intel EMA configurato, è necessario fornire la directory di installazione dell'agente EMA originale e caricare il file .msh dell'agente EMA dal nuovo server EMA.

Questa funzione richiede Bridge. Per ulteriori dettagli, vedere **Bridge**.

Procedura

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Integrazione server EMA**.
3. Immettere il nome per la configurazione.
4. Nella sezione Impostazioni di configurazione, fare clic su **Scegli file** per selezionare il file .msh dell'agente EMA.

> Il file msh è un file della policy agente che può essere scaricato dal server EMA.

5. Nel campo **directory di installazione agente EMA** originale, digitare la posizione in cui è installato il file EmaAgent.exe originale.
6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni di distribuzione:
   - Tutti i dispositivi
   - Nessun dispositivo (impostazione predefinita)
   - Personalizzato
8. Fare clic su **Fine**.

10.10.8.17. Configurazione risparmio energetico

Ivanti Neurons per MDM abilita la configurazione Risparmio energetico per il payload che si usa per configurare le impostazioni di risparmio energetico sui dispositivi Windows e macOS.

Applicabile a:

- Windows 10 fino alla versione più recente supportata da Ivanti Neurons per MDM.
- macOS 10.7 fino alla versione più recente supportata da Ivanti Neurons per MDM.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Risparmio energetico**.
3. Nella sezione Scegliere il sistema operativo, selezionare **Windows** o **macOS** e fare clic su **Avanti**.
4. Fare clic su **+ Aggiungi descrizione** per immettere una breve descrizione della configurazione.
5. Per Windows, configurare le seguenti impostazioni di **Risparmio energetico**:
   - **Dispositivo alimentato a batteria**
   - **Il dispositivo è collegato**
6. Configurare le seguenti impostazioni **Risparmio energetico**:
   - **Impostazioni di risparmio energia alimentazione CA desktop**
   - **Programmare le impostazioni di avvio o spegnimento del computer**
   - **Impostazioni di risparmio energia alimentazione CA portatile**
   - **Impostazioni di risparmio energia alimentazione batteria portatile**
7. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
8. Selezionare una delle opzioni di distribuzione per impostare la configurazione di **Risparmio energetico**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere **Utilizzo delle configurazioni**.
9. Fare clic su **Fine**.

Configurazione Risparmio energetico Windows

Quando si applica una nuova configurazione di Risparmio energetico a un dispositivo o si modificano le impostazioni di configurazione di Risparmio energetico esistenti, gli utenti devono riavviare i dispositivi affinché le modifiche abbiano effetto.

Dispositivo alimentato a batteria

Quando il dispositivo è alimentato a batteria, utilizzare le seguenti impostazioni di risparmio energetico riportate nella tabella:

Impostazione	Descrizione
Soglia batteria per attivare il risparmio energetico	Quando il dispositivo è alimentato a batteria, inserire il livello di carica della batteria per attivare il Risparmio energetico; è possibile inserire valori da 0 a 100. Inserire un valore percentuale che indica il livello di carica della batteria. Ad esempio, se impostato su 80, il Risparmio energetico si attiva quando la batteria ha una carica dell'80% o meno. Se non si inserisce un valore, Ivanti Neurons per MDM non cambia né aggiorna questa impostazione. Per impostazione predefinita, Windows la imposta al 70%.
Quando il coperchio è chiuso	• **Non intervenire**: il dispositivo rimane acceso e continua a utilizzare la batteria. • **Sospensione**: il dispositivo entra in modalità sospensione e utilizza una piccola quantità di carica della batteria. Il computer è ancora acceso e le app e i file aperti sono memorizzati nella RAM. • **Stato di sospensione in ibernazione**: il dispositivo passa in modalità di ibernazione. Le app e i file aperti vengono memorizzati sul disco rigido e il dispositivo si spegne. • **Arresta**: il dispositivo si spegne. Le app e i file aperti vengono chiusi senza essere salvati.
Quando viene selezionato il pulsante di alimentazione	• **Non intervenire**: il dispositivo rimane acceso e continua a utilizzare la batteria. • **Sospensione**: il dispositivo entra in modalità sospensione e utilizza una piccola quantità di carica della batteria. Il computer è ancora acceso e le app e i file aperti sono memorizzati nella RAM. • **Stato di sospensione in ibernazione**: il dispositivo passa in modalità di ibernazione. Le app e i file aperti vengono memorizzati sul disco rigido e il dispositivo si spegne. • **Arresta**: il dispositivo si spegne. Le app e i file aperti vengono chiusi senza essere salvati.
Quando viene selezionato il pulsante di sospensione	• **Non intervenire**: il dispositivo rimane acceso e continua a utilizzare la batteria. • **Sospensione**: il dispositivo entra in modalità sospensione e utilizza una piccola quantità di carica della batteria. Il computer è ancora acceso e le app e i file aperti sono memorizzati nella RAM. • **Stato di sospensione in ibernazione**: il dispositivo passa in modalità di ibernazione. Le app e i file aperti vengono memorizzati sul disco rigido e il dispositivo si spegne. • **Arresta**: il dispositivo si spegne. Le app e i file aperti vengono chiusi senza essere salvati.
Attiva la sospensione ibrida	• **Vero**: i dispositivi possono passare alla modalità di sospensione ibrida. Le app e i file aperti vengono memorizzati nella RAM e sul disco rigido. Utilizza una piccola quantità di carica della batteria. • **Falso**: impedisce ai dispositivi di passare alla modalità di sospensione ibrida.

Il dispositivo è collegato

Utilizzare le seguenti impostazioni della tabella quando il dispositivo è alimentato da una fonte di alimentazione esterna:

Impostazione	Descrizione
Soglia batteria per attivare il risparmio energetico	Quando il dispositivo è collegato, immettere il livello di carica della batteria per attivare il Risparmio energetico; è possibile immettere valori da 0 a 100. Inserire un valore percentuale che indica il livello di carica della batteria. Ad esempio, se impostato su 80, il Risparmio energetico si attiva quando la batteria ha una carica dell'80% o meno. Se non si inserisce un valore, Ivanti Neurons per MDM non cambia né aggiorna questa impostazione. Per impostazione predefinita, Windows la imposta al 70%.
Quando il coperchio è chiuso	• **Non intervenire**: il dispositivo rimane acceso e continua a utilizzare la fonte di alimentazione esterna. • **Sospensione**: il dispositivo entra in modalità sospensione e utilizza una piccola quantità di fonte di alimentazione esterna. Il computer è ancora acceso e le app e i file aperti sono memorizzati nella RAM. • **Stato di sospensione in ibernazione**: il dispositivo passa in modalità di ibernazione. Le app e i file aperti vengono memorizzati sul disco rigido e il dispositivo si spegne. • **Arresta**: il dispositivo si spegne. Le app e i file aperti vengono chiusi senza essere salvati.
Quando viene selezionato il pulsante di alimentazione	• **Non intervenire**: il dispositivo rimane acceso e continua a utilizzare la fonte di alimentazione esterna. • **Sospensione**: il dispositivo entra in modalità sospensione e utilizza una piccola quantità di fonte di alimentazione esterna. Il computer è ancora acceso e le app e i file aperti sono memorizzati nella RAM. • **Stato di sospensione in ibernazione**: il dispositivo passa in modalità di ibernazione. Le app e i file aperti vengono memorizzati sul disco rigido e il dispositivo si spegne. • **Arresta**: il dispositivo si spegne. Le app e i file aperti vengono chiusi senza essere salvati.
Quando viene selezionato il pulsante di sospensione	• **Non intervenire**: il dispositivo rimane acceso e continua a utilizzare la fonte di alimentazione esterna. • **Sospensione**: il dispositivo entra in modalità sospensione e utilizza una piccola quantità di fonte di alimentazione esterna. Il computer è ancora acceso e le app e i file aperti sono memorizzati nella RAM. • **Stato di sospensione in ibernazione**: il dispositivo passa in modalità di ibernazione. Le app e i file aperti vengono memorizzati sul disco rigido e il dispositivo si spegne. • **Arresta**: il dispositivo si spegne. Le app e i file aperti vengono chiusi senza essere salvati.
Attiva la sospensione ibrida	• **Vero**: i dispositivi possono passare alla modalità di sospensione ibrida. Le app e i file aperti vengono memorizzati nella RAM e sul disco rigido. Utilizza una piccola quantità di energia esterna. • **Falso**: impedisce ai dispositivi di passare alla modalità di sospensione ibrida.

Configurazione Risparmio energetico macOS

Impostazioni di risparmio energia alimentazione CA desktop

Utilizzare le seguenti impostazioni per configurare le impostazioni di risparmio energia del dispositivo desktop macOS:

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Avvia in automatico dopo un'interruzione di corrente	Consente al dispositivo di avviarsi in automatico dopo un'interruzione di corrente.
Sospendi un disco rigido dopo	Abilitare la casella di controllo per mettere in sospensione il disco rigido a intervalli fissi compresi tra 1 e 180 minuti. Un valore pari a 0 minuti non metterà mai in sospensione il disco rigido.
Spegni il display dopo	Abilitare la casella di controllo per spegnere il display a intervalli fissi compresi tra 1 e 180 minuti. Un valore di 0 minuti non spegnerà mai il display.
Power step dinamico	Selezionare la casella di controllo per abilitare il power step dinamico.
Riduci la velocità del processore	Selezionare la casella di controllo per ridurre la velocità del processore.
Sospendi il computer dopo	Abilitare la casella di controllo per mettere in sospensione il computer a intervalli fissi compresi tra 1 e 180 minuti. Un valore pari a 0 minuti non metterà mai in sospensione il computer.
Riattiva per l'accesso alla rete	Selezionare la casella di controllo per riattivare il computer per l'accesso alla rete.
Riattiva per lo squillo del modem	Selezionare la casella di controllo per riattivare il computer per lo squillo del modem.

Programmare le impostazioni di avvio o spegnimento del computer

Utilizzare le seguenti impostazioni per configurare i dispositivi macOS per l'avvio o lo spegnimento programmato dei dispositivi.

Impostazioni di disattivazione del dispositivo

Selezionare la casella di controllo **Disattiva il dispositivo** per spegnere i dispositivi a intervalli fissi.

Impostazione	Descrizione
Tipo di evento	Selezionare uno dei tipi di evento dall'elenco a discesa: • Sospendi • Riavvia • Arresta
Quando	Selezionare uno o più giorni della settimana per programmare un tipo di evento.
Alle	Selezionare l'ora in cui programmare un tipo di evento.

Avvio o riattivazione delle impostazioni del dispositivo

Selezionare la casella di controllo **Avvia o riattiva il dispositivo** per riattivare i dispositivi a intervalli fissi.

Impostazione	Descrizione
Tipo di evento	Selezionare uno dei tipi di evento dall'elenco a discesa: • Riattiva • Avvia/Riattiva
Quando	Selezionare uno o più giorni della settimana per programmare un tipo di evento.
Alle	Selezionare l'ora in cui programmare un tipo di evento.

Impostazioni di risparmio energia alimentazione CA portatile

Utilizzare le seguenti impostazioni per configurare le impostazioni di risparmio energia del dispositivo portatile macOS:

Impostazione	Descrizione
Avvia in automatico dopo un'interruzione di corrente	Consente al dispositivo di avviarsi in automatico dopo un'interruzione di corrente.
Sospendi un disco rigido dopo	Abilitare la casella di controllo per mettere in sospensione il disco rigido a intervalli fissi compresi tra 1 e 180 minuti. Un valore pari a 0 minuti non metterà mai in sospensione il disco rigido.
Spegni il display dopo	Abilitare la casella di controllo per spegnere il display a intervalli fissi compresi tra 1 e 180 minuti. Un valore di 0 minuti non spegnerà mai il display.
Power step dinamico	Selezionare la casella di controllo per abilitare il power step dinamico.
Riduci la velocità del processore	Selezionare la casella di controllo per ridurre la velocità del processore.
Metti in sospensione il portatile dopo	Abilitare la casella di controllo per mettere in sospensione il portatile a intervalli fissi compresi tra 1 e 180 minuti. Un valore pari a 0 minuti non metterà mai in sospensione il portatile.
Riattiva per l'accesso alla rete	Selezionare la casella di controllo per riattivare il portatile per l'accesso alla rete.
Riattiva per lo squillo del modem	Selezionare la casella di controllo per riattivare il portatile per lo squillo del modem.

Impostazioni di risparmio energia alimentazione batteria portatile

Utilizzare le seguenti impostazioni per configurare le impostazioni di risparmio energia della batteria del portatile macOS:

Impostazione	Descrizione
Avvia in automatico dopo un'interruzione di corrente	Consente al dispositivo di avviarsi in automatico dopo un'interruzione di corrente.
Sospendi un disco rigido dopo	Abilitare la casella di controllo per mettere in sospensione il disco rigido a intervalli fissi compresi tra 1 e 180 minuti. Un valore pari a 0 minuti non metterà mai in sospensione il disco rigido.
Spegni il display dopo	Abilitare la casella di controllo per spegnere il display a intervalli fissi compresi tra 1 e 180 minuti. Un valore di 0 minuti non spegnerà mai il display.
Power step dinamico	Selezionare la casella di controllo per abilitare il power step dinamico.
Riduci la velocità del processore	Selezionare la casella di controllo per ridurre la velocità del processore.
Sospendi il computer dopo	Abilitare la casella di controllo per mettere in sospensione la batteria del portatile a intervalli fissi compresi tra 1 e 180 minuti. Un valore pari a 0 minuti non metterà mai in sospensione la batteria del portatile.
Riattiva per l'accesso alla rete	Selezionare la casella di controllo per riattivare la batteria del portatile per l'accesso alla rete.
Riattiva per lo squillo del modem	Selezionare la casella di controllo per riattivare la batteria del portatile per lo squillo del modem.

10.10.8.18. Configurazione Ethernet (macOS)

Licenza: Gold

Applicabile a: macOS 10.13 o versioni successive supportate.

L'amministratore può configurare l'interfaccia Ethernet nelle variazioni. Per configurare l'Ethernet sono disponibili i payload seguenti:

- Ethernet globale
- Prima Ethernet attiva
- Prima Ethernet
- Seconda Ethernet attiva
- Seconda Ethernet
- Terza Ethernet attiva
- Terza Ethernet

> I vari payload per configurare l'Ethernet sono l'interfaccia Ethernet Globale, Prima, Prima attiva, Seconda, Seconda attiva, Terza e Terza attiva con fallback predefinito. Apple ha un problema noto esistente con l'installazione dell'interfaccia Ethernet Prima, Prima attiva, Seconda, Seconda attiva, Terza e Terza attiva.

Configurazione dell'Ethernet

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.
3. Digitare **Ethernet** nel campo di ricerca, quindi selezionare Configurazione **Ethernet**.
4. Immettere un nome e una descrizione per la configurazione.
5. Scegliere l'impostazione della configurazione dall'elenco a discesa.
6. Immettere le **impostazioni di configurazione dell'Ethernet**.
7. Fare clic su **Avanti**.
8. Selezionare l'opzione **Abilita questa configurazione**.
9. Selezionare una delle opzioni di canale seguenti per applicare la configurazione:
    - Canale del dispositivo (più comune)
    - Canale dell'utente (utente registrato corrente)
10. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato
11. Fare clic su **Fine**.

Impostazioni della configurazione dell'Ethernet

Utilizzare le impostazioni nella seguente tabella per configurare l'Ethernet. Per ulteriori informazioni su queste impostazioni, vedere la **documentazione di Apple**.

Impostazione	Descrizione
Protocolli	
Tipi EAP accettati	Selezionare i tipi EAP che è possibile utilizzare per accedere alla rete: • Transport Layer Security(TLS): TSL è un protocollo che stabilisce una sessione crittografata tra due computer su Internet. Verifica l'identità del server e impedisce agli hacker di intercettare i dati. • TTLS: campo **Identità interna**, selezionare uno dei protocolli di autenticazione, ad esempio Sistema operativo predefinito, PAP, CHAP, MSCHAP, MSCHAPv2 ed EAP. • PEAP • LEAP • EAP-SIM: nel campo **Numero EAP SIM di RAND**, selezionare il numero di rand dall'elenco a discesa. • EAP-AKA • EAP-FAST: selezionare l'opzione EAP-FAST per definire i metodi di autenticazione: ◦ **Utilizza PAC:** selezionare questa opzione per utilizzare una configurazione proxy automatica (PAC). ◦ **Esegui provisioning PAC:** selezionare questa opzione per consentire il provisioning di una PAC. In alternativa, sarà possibile utilizzare soltanto una PAC per la quale è stato già eseguito il provisioning sul dispositivo. Quest'opzione è disponibile soltanto se è stata selezionata l'opzione Utilizza PAC. ◦ **Esegui provisioning PAC in modo anonimo:** selezionare questa opzione per consentire il provisioning di una PAC senza eseguire l'autenticazione del server. Quest'opzione è disponibile soltanto se è stata selezionata l'opzione Esegui provisioning PAC.
Autenticazione	**Nome utente**: specificare il nome utente richiesto per l'accesso alla rete. Se questo campo viene lasciato vuoto, verrà richiesto all'utente di compilarlo. • Utilizza password per connessione: selezionare questa opzione per richiedere all'utente del dispositivo una password per ciascuna connessione. Quando il dispositivo si ricollega alla stessa rete, all'utente verrà richiesto di eseguire nuovamente l'autenticazione per ricollegarsi alla rete. Ogni volta che la connessione viene avviata, viene richiesta la password. • Richiedi password monouso quando connesso alla rete: la password viene richiesta solo una volta quando la configurazione viene trasmessa al dispositivo. La password non sarà richiesta a ogni connessione e disconnessione dalla rete. **Password**: (facoltativo) immettere la password per l'accesso alla rete. Altrimenti, all'utente del dispositivo verrà richiesto di immettere la password per accedere alla rete. **Identità esterna**: (facoltativo) per TTLS, PEAP e EAP-FAST, selezionare questa opzione per consentire agli utenti del dispositivo di nascondere la propria identità. Il nome reale dell'utente viene visualizzato soltanto all'interno del tunnel crittografato. Questa opzione può aumentare la sicurezza dato che un aggressore non può vedere il nome dell'utente che si autentifica in chiaro. **Identità fonte credenziali modalità sistema**: modalità sistema usata per l'autenticazione del computer. L'autenticazione con la modalità sistema si verifica prima dell'accesso al computer da parte dell'utente. Di norma modalità sistema è configurata per fornire l'autenticazione con il certificato X.509 (EAP-TLS) del computer emesso da un'autorità di certificazione locale.
Contrassegna	**Certificati attendibili:** selezionare le caselle di controllo per selezionare più certificati dall'elenco. **Nomi certificati server attendibile**: aggiungere il nome del certificato.

Impostazione	Descrizione
come attendibile	• **Consenti Eccezioni attendibilità**: consente all'utente di prendere decisioni basate sull'attendibilità (tramite finestra di dialogo). • **Richiedi certificato TLS** **Versione TLS massima consentita con l'autenticazione EAP** **Versione TLS minima consentita con l'autenticazione EAP** **Certificati attendibili TLS: certificato dell'Autorità di certificazione dell'agente MobileIron**

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.8.19. Configurazione di Google BeyondCorp

Ivanti Neurons per MDM può essere integrato con Google BeyondCorp per l'accesso condizionato. Ivanti Neurons for MDM invia un segnale di conformità dei dispositivi a Google BeyondCorp. Questo garantisce che solo i dispositivi conformi a N-MDM possano accedere alle applicazioni dell'area di lavoro di Google.

Applicabile a

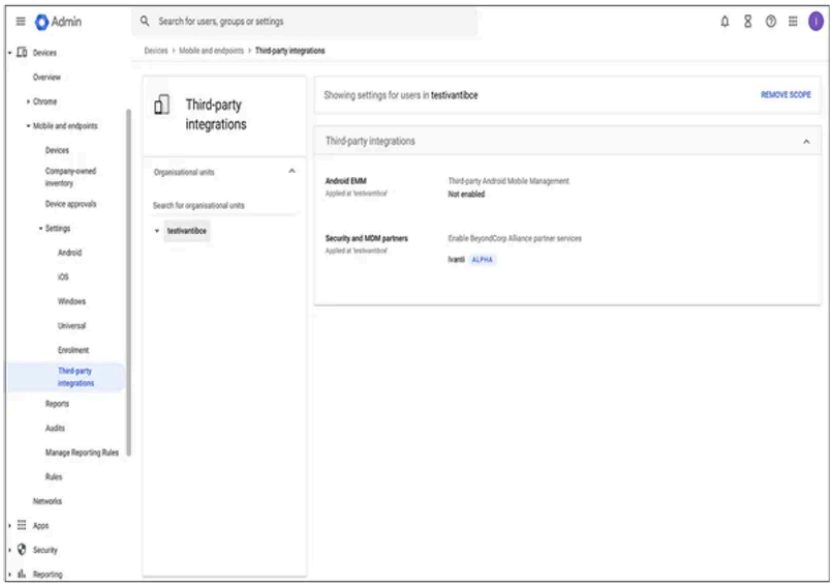
- iOS
- Android
- Windows

Prerequisiti

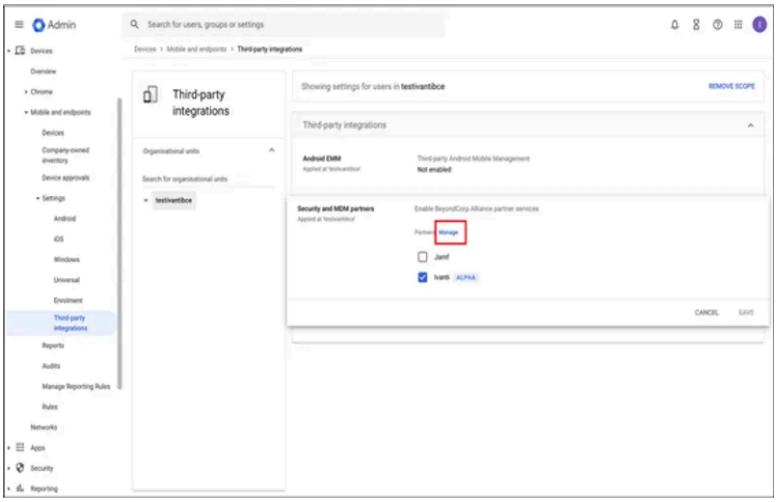
- Per Ivanti Neurons per MDM, è necessario disporre di una licenza Ivanti Professional Plus / Premium.
- Per Google, è necessario disporre della licenza BeyondCorp Enterprise, Google Workspace Enterprise o Cloud Identity Premium.
- Per Windows, è necessario che sul dispositivo siano installati i seguenti elementi:
  - Ivanti Bridge
  - Google Chrome

Procedura (Google)

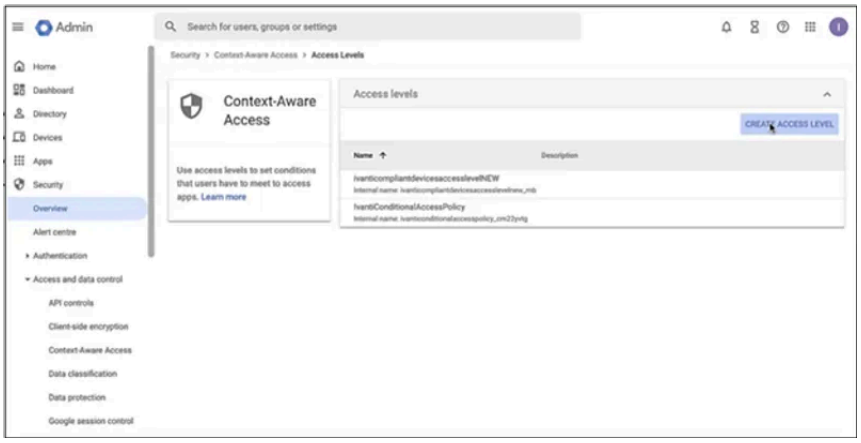
1. Accedere alla **console di Google Admin** con le credenziali di amministratore.
2. Accedere a **Dispositivi** > **Dispositivi mobili ed Endpoint** > **Impostazioni** > **Integrazioni di terze parti**.



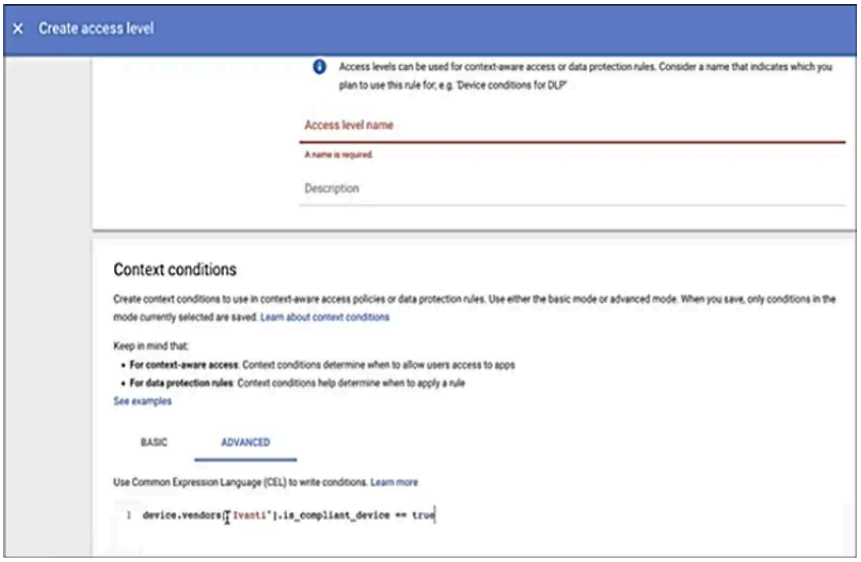
3. Fare clic su **Sicurezza e partner MDM** > **Gestisci**.



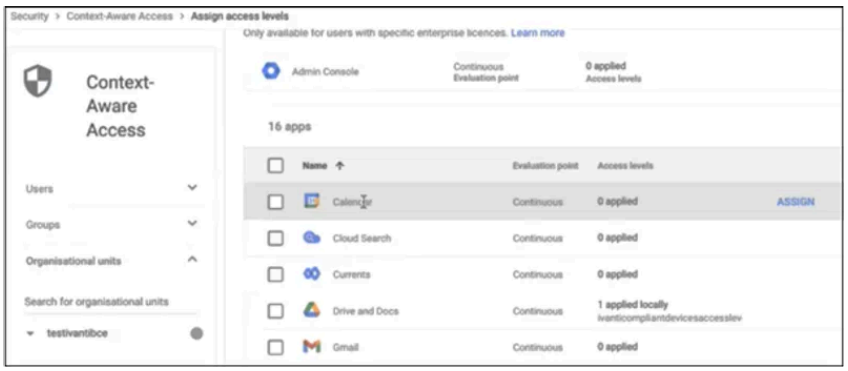
4. Nella finestra **Gestisci connessioni partner**, selezionare **Ivanti**.
5. Fare clic su **Apri connessione**.
   Si verrà reindirizzati alla pagina di accesso di Ivanti Neurons per MDM; inserire le credenziali di amministratore tenant. Una volta effettuato l'accesso al tenant, si vedrà che **Google BeyondCorp** è abilitato e collegato automaticamente al proprio account Google.
6. Nella console Google Admin, andare su **Sicurezza** > **Accesso consapevole del contesto** > **Livelli di accesso**.



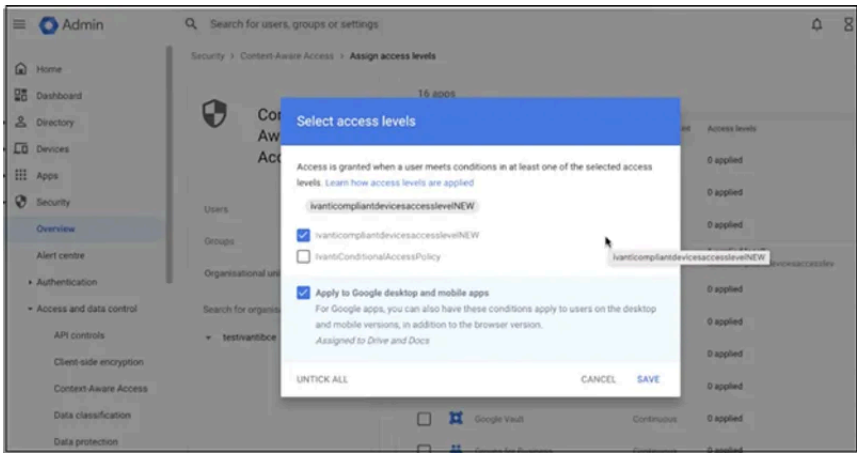
7. Fare clic su **Crea livello di accesso**.
   Nella finestra Crea livello di accesso, nella sezione Condizioni del contesto, fare clic su **AVANZATE** e fornire le informazioni richieste.



8. Accedere a **Sicurezza** > **Accesso consapevole del contesto** > **Livello di accesso**, selezionare l'applicazione per la quale si desidera assegnare il criterio.



9. Fare clic su **Assegna**.
10. Dalla finestra **Seleziona livelli di accesso**, selezionare i criteri che si desidera assegnare e fare clic su **Salva**.



Una volta completata l'impostazione di cui sopra, è possibile creare la configurazione di conformità del dispositivo partner utilizzando **Google BeyondCorp**.

Procedura (Ivanti Neurons per MDM**)**:

1. Andare in **Configurazioni** > **Aggiungi configurazione**.
2. Selezionare la configurazione **Conformità dispositivo partner**.
3. A schermo viene visualizzata la pagina di configurazione Conformità dispositivo partner.
   Immettere un nome per la configurazione.
4. Nell'elenco Scegli partner, selezionare **Google BeyondCorp**.
5. A schermo appare la sezione Impostazione configurazione. Assicurarsi che l'opzione Segnala stato di conformità per dispositivi iOS e Android sia impostata su ON.
   Fare clic su **Avanti**.
6. Selezionare **Abilita questa configurazione**.
7. Selezionare **Personalizza** come opzione di distribuzione
8. Selezionare **Utenti/gruppi di utenti** sotto l'opzione **Distribuzione personalizzata**.
9. Nella sezione **Selezionare sotto per distribuire questa configurazione**, selezionare utenti/gruppi di utenti dall'elenco.
10. Fare clic su **Fine**.

Il server Google BeyondCorp è in grado di individuare in modo univoco ogni dispositivo attraverso la configurazione P-List gestita dall'app.



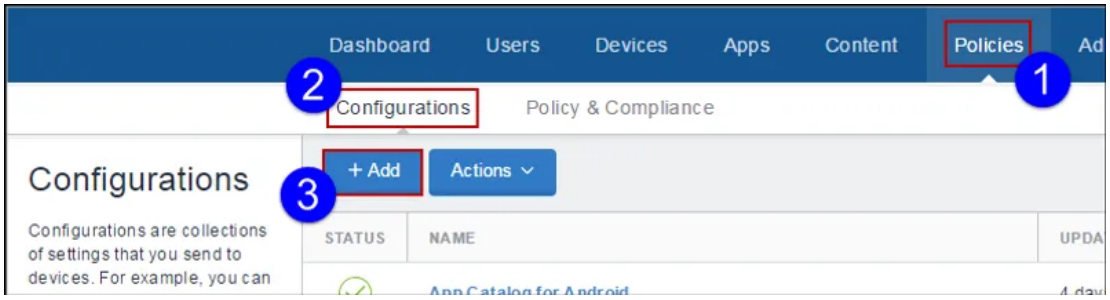
10.10.8.20. Configurazione del messaggio schermata di blocco

Visualizza un messaggio e le informazioni sul tag asset nelle schermate di accesso e di blocco. Questo vale per i dispositivi supervisionati che utilizzano iOS 9.3 o una versione successiva supportata.

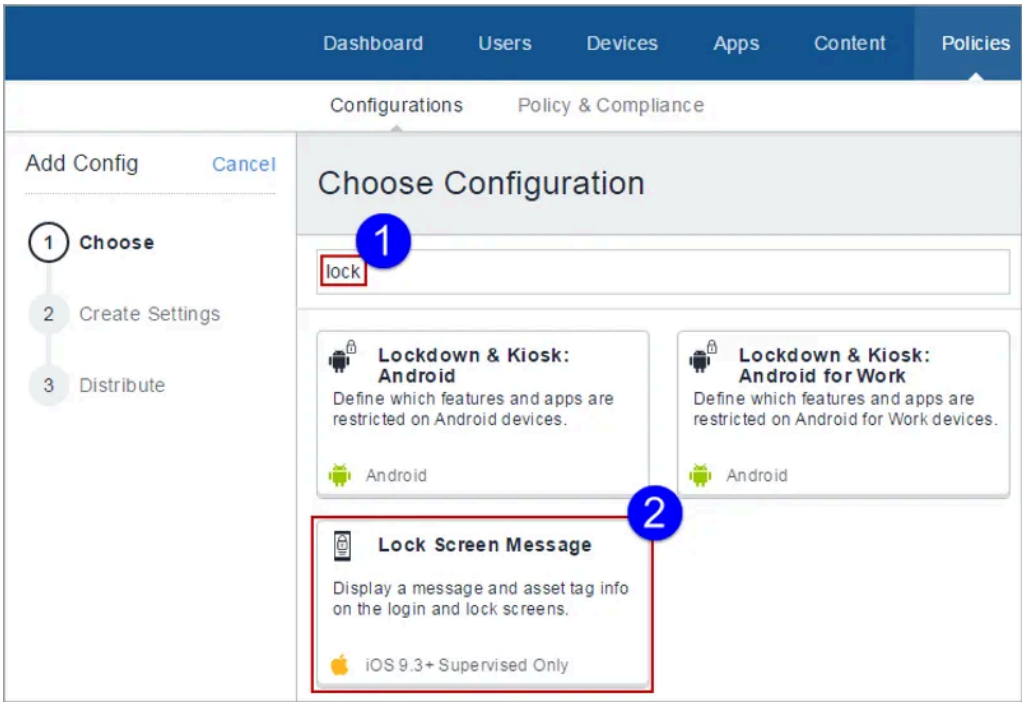
Creazione di una configurazione del messaggio schermata di blocco

Procedura

1. Selezionare **Configurazioni**.
2. Fare clic su **+ Aggiungi**.



Digitare **blocco** nel campo di ricerca, quindi fare clic sulla configurazione **Messaggio schermata di blocco**:



Viene visualizzata la pagina dei dettagli relativa alla configurazione del messaggio della schermata di blocco.
Configurare le impostazioni su questa pagina. Fare riferimento alla tabella presente nella sezione **Impostazioni di configurazione dei messaggi della schermata di blocco** per linee guida sui valori.

5. Fare clic su **Avanti** per configurare le impostazioni di distribuzione, quindi fare clic su **Fine**.

Impostazioni per la configurazione del messaggio schermata di blocco

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Nota a piè di pagina schermata di blocco	Questo testo viene visualizzato nella finestra di dialogo di accesso e nella schermata di blocco.
Informazioni sul tag asset	Questo testo viene visualizzato nella parte inferiore della finestra di dialogo di accesso e della schermata di blocco.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.8.21. Configurazione finestra di accesso - macOS

Procedura

1. Accedere a Ivanti Neurons per MDM.
2. Andare in **Configurazioni** > **Aggiungi configurazione**.
3. Fare clic su (o selezionare) **Finestra di accesso**.
4. Nel campo **Nome**, inserire un nome per la configurazione della finestra di login.
5. Fare clic su **+ Aggiungi descrizione** per aggiungere i dettagli.
6. Sotto la sezione **Impostazioni configurazione**, fornire i campi seguenti:
    - **Info host amministratore**: inserire il nome host o l'indirizzo IP o la versione del sistema.
    - **Consenti elenco**: elenco di GUID utente o GUID gruppo di utenti a cui il sistema consente di accedere. Una stringa con asterisco ('*') specifica tutti gli utenti o i gruppi.
    - **Password di accesso automatico**: inserire la password per l'accesso automatico.
    - **Elenco da rifiutare**: l'elenco dei GUID degli utenti o dei GUID dei gruppi di utenti a cui il sistema non consente l'accesso. Questo elenco ha la priorità sull'elenco della chiave 'Elenco consentiti'.
    - **Testo finestra di accesso**: inserire il testo della finestra di accesso.
    - Selezionare la casella di controllo per opzioni aggiuntive come:
        - **Disabilita accesso alla console**
        - **Disabilita Autologin FDE (FileVault Disk Encryption)**
        - **Disabilita funzioni di blocco immediato dello schermo**
        - **Nascondi utenti amministratori quando si mostra un elenco di utenti**
        - **Mostra solo gli utenti della rete e del sistema**
        - **Nascondi account mobili**
        - **Mostra utenti della rete**
        - **Disabilita la voce di menu disconnetti**
        - **Disabilita spegnimento quando l'utente è connesso**
        - **Disabilita voce di menu Riavvia quando l'utente è connesso**
        - **Disabilita voce Riavvio**
        - **Mostra la finestra di dialogo del nome e della password**
        - **Mostra agli altri utenti - gestito**
        - **Mostra menu di ingresso**
        - **Disabilita pulsante di spegnimento**
        - **Disabilita pulsante Sospendi**
        - **Disabilita pulsante menu spegnimento**
7. Fare clic su **Fine**.

10.10.8.22. Configurazione delle estensioni di sistema macOS

La configurazione delle estensioni di sistema consente l'installazione di tipi di estensioni quali Estensione driver, Estensione rete ed Estensione sicurezza endpoint, senza richiedere l'accesso a livello di kernel.

Procedura

Applicabile a: macOS 10.15 e versioni successive

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Digitare **estensione** nel campo di ricerca, quindi fare clic sulla configurazione **Estensioni di sistema**.
3. Immettere un **Nome** e una **Descrizione** per la configurazione.
4. In **Estensioni sistema consentite**, fare clic su **+Aggiungi** per aggiungere gli **Identificatori del team consentiti** e le **Estensioni sistema consentite**.
5. In **Tipi di estensioni sistema consentite**, fare clic su **+Aggiungi** per aggiungere gli **Identificatori del team consentiti** e i **Tipi di sistemi consentiti**.
6. Selezionare l'opzione **Consenti le sostituzioni da parte dell'utente**.
7. Fare clic su **Avanti**.
8. Selezionare l'opzione **Abilita questa configurazione**.
9. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzata.
10. Fare clic su **Fine**.

> In macOS 12, RemovableSystemExtensions permette alle applicazioni di disattivare la loro estensione di sistema senza l'approvazione dell'amministratore durante la disinstallazione dell'applicazione.

10.10.8.23. Solo MAM

Ivanti Neurons per MDM consente di specificare i dispositivi iOS e Android come solo MAM e fornisce Mobile App Management (MAM) a tali dispositivi. Un deployment solo MAM consente di distribuire e gestire app senza essere costretti a gestire il dispositivo stesso.

Soluzione solo MAM - Alternativa Ivanti AppStation

Come soluzione alternativa a Ivanti AppStation, Ivanti offre una soluzione moderna e flessibile di gestione delle applicazioni mobili (MAM) utilizzando Ivanti Go Client, disponibile per le piattaforme iOS e Android.

La nuova soluzione Solo MAM introduce un App Catalog integrato e la funzionalità Ivanti Neurons per MDM Web Clip, che insieme soddisfano i casi d'uso principali precedentemente affrontati da App Station, offrendo un'esperienza di gestione delle app semplificata, sicura e unificata sia per gli utenti che per gli amministratori.

Funzioni chiave

- **App Catalog in app**: ospita e distribuisce applicazioni approvate e gestite direttamente all'interno del client Go.
- **Configurazione e aggiornamenti app**: supporta la configurazione e gli aggiornamenti di versione a livello di applicazione, applicati tramite i criteri MAM.
- Ivanti Neurons per MDM **Requisito**: ideale per gli scenari BYOD e per gli appaltatori in cui la registrazione a Ivanti Neurons per MDM non è fattibile.

Utilizzo di Web Clip per facilitare l'accesso

- **Accesso diretto ad App Catalog**: distribuzione di clip Web tramite Ivanti Neurons per MDM per fornire un collegamento all'App Catalog o a specifiche app aziendali basate sul Web.
- **Collegamenti alle app personalizzate**: consente agli utenti di avviare rapidamente le risorse utilizzate più di frequente dalla schermata iniziale.

Esperienza amministrativa e utente migliorata

- **Interfaccia unificata**: combina App Catalog, accesso al Web e messaggistica di conformità in un'unica esperienza.
- **Amministrazione semplificata**: non è necessario mantenere soluzioni separate (ad esempio, App Station), riducendo la complessità e il rischio di deriva della configurazione.

Flessibilità e personalizzazione

- **Personalizza visualizzazioni catalogo**: personalizzazione dei contenuti dell'App Catalog in base ai ruoli degli utenti, alla geo-localizzazione o all'unità organizzativa.
- **Utilizza l'infrastruttura esistente**: sfrutta l'investimento esistente in Ivanti Neurons per MDM / MAM (non richiede un'infrastruttura separata).

Supporto per utenti con doppio ruolo

La soluzione Ivanti Solo MAM è progettata per supportare i moderni scenari di lavoro, compresi gli utenti con doppi ruoli:

- **Dipendente a tempo pieno - Org A**: accesso alle app aziendali tramite un Webclip (ad es., Apps@Work) distribuito tramite Ivanti Neurons per MDM.
- **Appaltatore - Org B**: utilizzare il client Ivanti Go in modalità Solo MAM per accedere in modo sicuro alle applicazioni gestite, senza richiedere la registrazione del dispositivo a Ivanti Neurons per MDM.

Ciò consente un accesso continuo e basato sui ruoli alle app necessarie, senza conflitti di profilo o sovrapposizioni nella gestione dei dispositivi.

Guida alla migrazione

Ivanti incoraggia caldamente i clienti di App Station a pianificare ed eseguire la transizione alla soluzione Solo MAM basata sul client Go. Per l'assistenza alla migrazione passo dopo passo, consultare le seguenti risorse:

- Soluzione Solo MAM di Ivanti
- **Configurazione di App Catalog nel client Go**
- **Creare una configurazione clip Web**

In caso di domande o di necessità di assistenza per la migrazione, contattare il **Supporto Ivanti** o il proprio Customer Success Manager.

10.10.8.24. Configurazione Google Play gestito

Gli amministratori possono configurare l'impostazione di aggiornamento automatico che Google Play Store utilizza per aggiornare le app sul dispositivo Android Enterprise.

Per configurare le impostazioni di aggiornamento automatico:

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Google Play gestito**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Nella sezione Impostazioni configurazione, selezionare l'opzione per aggiornare le app da Google Play.

Impostazione	Operazione da eseguire
Definito dall'utente	Per definire quali app aggiornare, l'utente del dispositivo può configurare l'impostazione di aggiornamento automatico nella finestra di manutenzione delle app 1. Nel campo **Ora di inizio**, selezionare l'orario in cui eseguire l'aggiornamento dell'app. 2. Nel campo **Durata**, selezionare la durata (in ore) entro la quale l'aggiornamento deve essere eseguito. L'intervallo minimo e massimo è compreso tra 1 ora e 24 ore. È possibile aggiornare le app in qualsiasi momento tra l'ora di inizio e la durata selezionata. Ad esempio, se il campo "Ora di inizio" è impostato su 6 PM e il campo "Durata" è impostato su 12 h, le app possono essere aggiornate in qualsiasi momento tra le 6 PM e le 6 AM.
Nessuno	Google Play Store non aggiorna mai le app automaticamente sul dispositivo.
Solo Wi-Fi	Google Play Store aggiorna automaticamente le app sul dispositivo ma solo tramite connessioni Wi-Fi e non della rete cellulare.
Sempre	Google Play Store aggiorna automaticamente le app sul dispositivo utilizzando le connessioni sia Wi-Fi sia della rete cellulare.

6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni di distribuzione:

- Tutti i dispositivi
- Nessun dispositivo (impostazione predefinita)
- Personalizzato

8. Fare clic su **Fine**.

10.10.8.26. Configurazione delle notifiche

Utilizzando la configurazione Notifiche, gli amministratori possono pianificare notifiche silenziose e visibili per i dispositivi iOS. La configurazione Notifiche può anche essere clonata, esportata o eliminata.

Procedura

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Notifiche**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Nella sezione Configurazione configurazione, selezionare una o entrambe le opzioni di **Pianificazione delle notifiche**:
    - Pianificazione notifiche silenziose - Le notifiche silenziose vengono utilizzate per supportare le operazioni di gestione del dispositivo in background dispositivo avviate da Ivanti Neurons per MDM. Abilitano azioni automatizzate come controlli di conformità, aggiornamenti dei criteri e aggiornamenti delle app senza richiedere l'interazione dell'utente.
      Ivanti Neurons per MDM invia notifiche silenziose al dispositivo al livello configurato.
    - Pianificazione notifiche visibili - Le notifiche visibili vengono utilizzate quando è richiesta la conoscenza o l'azione dell'utente per garantire la conformità, la protezione o la funzionalità del dispositivo. Le notifiche visibili vengono attivate solo dopo l'intervallo specificato, anche se si verificano più azioni o eventi durante quel periodo. Una notifica visiva viene visualizzata sul dispositivo solo se non è stata inviata una notifica silenziosa durante l'intervallo di notifica visibile.
6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato
8. Fare clic su **Fine**.

Contenuto di notifica visibile per i dispositivi MTD - Il dispositivo potrebbe essere vulnerabile alle minacce. Avviare l'applicazione Ivanti Go e controllare lo stato Difesa dalle minacce.

Contenuto di notifica visibile per dispositivi non MTD - Per ricevere funzionalità di protezione avanzate e garantire le misure di protezione più recenti, lanciare l'app sul dispositivo per un'esperienza utente più sicura.

10.10.8.27. Impostazioni della stampante

Ivanti Neurons for MDM consente di creare profili della stampante e di aggiungerli ai dispositivi. Questa funzione richiede Bridge. Per ulteriori dettagli, vedere Bridge.

> Quando il profilo della stampante viene inviato al dispositivo, la stampante deve essere attiva, in caso contrario il dispositivo non è in grado di individuarla.

Per impostare la configurazione Impostazioni della stampante per un dispositivo Windows:

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Impostazioni della stampante**.
3. Immettere un nome per la configurazione.
4. Selezionare l'opzione **Windows**.
5. Nella sezione **Impostazioni configurazione**, configurare le impostazioni seguenti:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Impostazioni della stampante Windows	
Stampante condivisa	Se l'opzione **Stampante condivisa** è selezionata, la stampante verrà condivisa con altri dispositivi. Configurare i campi seguenti: **Nome**: inserire il nome della configurazione della stampante. **Descrizione**: inserire una descrizione della stampante. **Server di stampa**: inserire l'indirizzo IP del server di stampa. **Nome della stampante condivisa**: inserire il nome della stampante.
Stampante collegata alla rete	Quando l'opzione **Stampante collegata alla rete** è selezionata, può essere effettuato l'accesso alla stampante solo da dispositivi all'interno della rete collegata. Configurare i campi seguenti: **Nome**: inserire il nome della configurazione della stampante. **Descrizione**: inserire una descrizione della stampante. **Nome della stampante**: inserire il nome della stampante nella rete. **Indirizzo host stampante**: inserire l'indirizzo IP dell'host della stampante. **Numero porta della stampante**: selezionare il numero di porta della stampante di rete. **Nome driver della stampante**: inserire il nome del driver della stampante. **URL driver della stampante**: inserire l'URL del driver della stampante. Per il driver della stampante, caricare un archivio ZIP contenente i file richiesti. L'archivio ZIP deve includere i seguenti file: • file .inf (informazioni driver) • file .cat (catalogo/firma) • Qualsiasi driver binario aggiuntivo a cui fa riferimento l'INF (come .dll, .sys, ecc.)

6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni di distribuzione:

- Tutti i dispositivi
- Nessun dispositivo (impostazione predefinita)
- Personalizzato

8. Fare clic su **Fine**.

Per impostare la configurazione Impostazioni della stampante per un dispositivo macOS:

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Impostazioni della stampante**.
3. Immettere un nome per la configurazione.
4. Selezionare l'opzione **macOS** .
5. Nella sezione **Crea configurazione stampante** configurare le impostazioni seguenti:

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Impostazioni configurazione	Per impostare la stampante per i dispositivi macOS, aggiornare i campi seguenti: • Consenti stampanti locali • Nome visualizzato stampante predefinita • Nome carattere piè di pagina • Dimensioni carattere piè di pagina • Elenco stampanti utente • + Aggiungi stampante

6. Fare clic su **Avanti**
7. Selezionare una delle seguenti opzioni di distribuzione:

- Tutti i dispositivi
- Nessun dispositivo (impostazione predefinita)
- Personalizzato

8. Fare clic su **Fine**.

10.10.8.28. Configurazione Rimuovi Bloatware

La configurazione Rimuovi Bloatware consente di selezionare l'elenco di applicazioni installate sui dispositivi che devono essere rimosse. È necessario disporre di una Bridge per impostare questa configurazione. Per ulteriori dettagli, vedere **Bridge**.

Per eseguire o disinstallare le app:

1. Nella scheda **Configurazione**, fare clic su **+Aggiungi**.
2. Selezionare la configurazione **Rimuovi Bloatware**. Viene visualizzata la pagina **Configurazione Rimuovi Bloatware**.
3. Nel campo **Nome**, digitare un nome appropriato per la configurazione.
4. Fare clic sul collegamento +**Aggiungi descrizione** per aggiungere una descrizione della configurazione. Questo campo è facoltativo.
5. Nella sezione **Impostazioni configurazione**, selezionare le app da rimuovere o disinstallare. In alternativa è possibile cercare un'app nel campo Ricerca utilizzando il nome dell'app visualizzato nell'elenco delle app desktop.

> Prima di creare la configurazione **Rimuovi Bloatware**, è necessario recuperare le app accedendo ad **App>App desktop>Recupera app**. In caso contrario, quando si crea la configurazione **Rimuovi Bloatware** non è disponibile alcuna applicazione da ricercare o selezionare.

A differenza dei file di tipo .exe, i tipi di file appx, .appxbundles, .xap e .msi possono essere rimossi.

6. Nelle Opzioni avanzate, configurare le seguenti opzioni:

Opzione	Descrizione
Esegui questa configurazione ogni	Impostare l'intervallo (in minuti) dopo il quale eseguire la configurazione.
Esegui all'accesso	Selezionare la casella di controllo per eseguire la configurazione all'accesso.
Elimina l'avvio forzato dopo la disinstallazione	Selezionare la casella di controllo per impedire il riavvio forzato dopo la disinstallazione dell'app.

10.10.8.29. Configurazione impostazioni ed estensione Safari

Estensione Safari

Ivanti Neurons per MDM consente di gestire le estensioni di Safari sui dispositivi iOS e macOS supervisionati. Gli amministratori possono gestire efficacemente le estensioni di Safari per la navigazione standard e privata.

Applicabile a:

- iOS 18.0 supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.
- macOS 15.0 supervisionato fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Impostazioni estensione Safari**.
3. Configurare le **Impostazioni di estensione Safari** come da tabella seguente:

Impostazione	Descrizione
Nome Descrizione	Immettere un nome identificativo della configurazione. Immettere una descrizione esplicativa dello scopo della configurazione.
ID estensione Stato estensione	Inserire l'identificativo dell'estensione composta. Ad esempio, "*Identificatore (TeamIdentifier)*." Immettere "*" per tutte le estensioni. Per generare questa stringa, utilizzare il segno di codice *-dv <path_to_appex>*. L'estensione del browser si trova nella cartella plug-in all'interno del bundle dell'app. Il formato previsto è "*Identificatore (TeamIdentifier)*." Per le estensioni non disponibili su macOS, lo sviluppatore dell'applicazione deve fornire queste informazioni. Selezionare una delle seguenti opzioni: • **Consentito**: l'utente può attivare o disattivare l'estensione. • **Sempre attivo**: l'estensione è sempre "attiva" per l'utente. • **Sempre spento**: l'estensione è sempre "spenta" per l'utente.
Stato navigazione privata	Selezionare una delle seguenti opzioni: • **Consentito**: l'utente può attivare o disattivare l'estensione nella Navigazione privata. • **Sempre attivo**: l'estensione è sempre "attiva" per l'utente anche durante la Navigazione privata. • **Sempre spento**: l'estensione non sarà disponibile.
Domini consentiti	Immettere i valori del dominio o del sottodominio per concedere l'accesso all'estensione Safari. È possibile inserire più valori di dominio o sottodominio. Le impostazioni del dominio consentito non sono applicabili al dispositivo se si inserisce "*" nel campo ID estensione.
Domini negati	Immettere i valori del dominio o del sottodominio per limitare l'accesso all'estensione Safari. È possibile inserire più valori di dominio o sottodominio. Le impostazioni del dominio negato non sono applicabili al dispositivo se si inserisce "*" nel campo ID estensione.

4. Fare clic su **+Add** per aggiungere più **estensioni**.
5. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
6. Selezionare una delle opzioni di distribuzione per impostare la configurazione di **Impostazioni estensione Safari**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere **Utilizzo delle configurazioni**.
7. Fare clic su **Fine**.

Impostazioni Safari

Ivanti Neurons per MDM consente di gestire le impostazioni di Safari sui dispositivi iOS e macOS supervisionati. Gli amministratori possono gestire efficacemente le estensioni di Safari per la navigazione standard e privata.

Applicabile a:

- Le versioni beta di iOS 26.0+, iPad 26.0+, macOS 26.0+, visionOS 26.0+ fino alla versione più recente supportata da Ivanti Neurons per MDM.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Impostazioni ed estensione Safari**.
3. Fare clic su **Impostazioni Safari**.
4. Configurare le **Impostazioni Safari** come da tabella seguente:

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Impostazioni di configurazione	Selezionare una delle seguenti opzioni per impostare il tipo di pagina iniziale: • **Avvio**: per utilizzare la pagina iniziale predefinita. Safari disattiva la pagina home esistente. • **Pagina home**: per utilizzare l'URL della pagina home specificato. Safari lo imposta come pagina home. • **Estensione**: per utilizzare la pagina specificata dall'estensione di Safari il cui identificatore è ExtensionIdentifier. Safari disattiva la pagina home esistente.

5. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
6. Selezionare una delle opzioni di distribuzione per impostare la configurazione di **Impostazioni Safari**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere **Utilizzo delle configurazioni**.
7. Fare clic su **Fine**.

Impostazioni privacy Safari

Le **Impostazioni sulla privacy di Safari** consentono di definire le autorizzazioni predefinite per fotocamere e microfoni per siti Web specifici in Safari utilizzando la Gestione dichiarativa dei dispositivi (DDM). Questa funzione aiuta le organizzazioni a gestire centralmente le autorizzazioni sulla privacy dei siti web e offre un'esperienza di navigazione più uniforme sui dispositivi Apple gestiti.

Applicabile a:

- iOS 27.0+ e macOS 27.0+ attraverso la versione più recente rilasciata come supportata da Ivanti Neurons per MDM.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione **Impostazioni ed estensione Safari**.
3. Fare clic su **Impostazioni privacy Safari**.
4. Configurare le **Impostazioni privacy di Safari** come da tabella seguente:

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.

Impostazioni di configurazione	• **Aggiungi URL**: immettere un URL per applicare l'impostazione.
	• **+Aggiungi valori predefiniti**: specificare i valori predefiniti che si desidera applicare a questa impostazione.
	  ◦ Fotocamera - Consenti/Rifiuta
	  ◦ Microfono - Consenti/Rifiuta
	  ◦ Giustificazione dell'organizzazione (obbligatoria)

5. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
6. Selezionare una delle opzioni di distribuzione per impostare la configurazione di **Impostazioni Safari**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere **Utilizzo delle configurazioni**.
7. Fare clic su **Fine**.

10.10.8.30. Configurazione delle restrizioni per telefoni Samsung

[Configurazioni]

La configurazione delle restrizioni per telefoni Samsung consente di impostare le eccezioni e le restrizioni di chiamata nei dispositivi Samsung. Tali restrizioni limitano i numeri di telefono da cui un utente può ricevere chiamate o a cui può effettuare chiamate.

Applicabile a: tutti i dispositivi Samsung con KNOX SDK 2.0 e versioni successive.

Per configurare le restrizioni per telefoni Samsung, procedere come segue:

1. Nella scheda **Configurazione**, fare clic su **+Aggiungi**.
2. Selezionare la configurazione **Restrizioni per telefoni Samsung**. Viene visualizzata la pagina **Configurazione delle restrizioni per telefoni Samsung**.
3. Nel campo **Nome**, digitare un nome appropriato per la configurazione.
4. Fare clic sul collegamento +**Aggiungi descrizione** per aggiungere una descrizione della configurazione. Questo campo è facoltativo.
5. Nella sezione **Impostazioni configurazione**, configurare le opzioni seguenti:
   Opzione
   Descrizione
   Chiamate in entrata
   Numeri bloccati
   Fare clic sull'icona Aggiungi per aggiungere i numeri e le espressioni regolari Java per definire le restrizioni sulle chiamate in entrata.
   Elenco dei numeri consentiti
   Fare clic sull'icona Aggiungi per aggiungere i numeri e le espressioni regolari Java per definire i numeri consentiti tra un insieme più ampio di numeri bloccati per le chiamate in entrata.
   Se non sono presenti numeri bloccati, questa opzione non ha effetto.
   Chiamate in uscita
   Numeri bloccati
   Fare clic sull'icona Aggiungi per aggiungere i numeri e le espressioni regolari Java per definire le restrizioni sulle chiamate in uscita.
   Elenco dei numeri consentiti
   Fare clic sull'icona Aggiungi per aggiungere i numeri e le espressioni regolari Java per definire i numeri consentiti tra un insieme più ampio di numeri bloccati per le chiamate in uscita.
   Se non sono presenti numeri bloccati, questa opzione non ha effetto.
6. Fare clic su **Fine** per inviare l'impostazione ai dispositivi selezionati.

> Quando un dispositivo viene dismesso, tutte le restrizioni alle chiamate vengono rimosse da tale dispositivo

Per ulteriori informazioni, vedere [Come creare una configurazione].

10.10.8.31. Configurazione predefinita browser - iOS e visionOS

Configurazione per modificare le impostazioni delle applicazioni predefinite sui dispositivi iOS e visionOS.

Prerequisiti

- Applicabile solo alle versioni iOS (18.2+) e visionOS 2.2.
- Queste app sono impostate sui dispositivi iOS in **Impostazioni** - **App** - **App predefinite**.

Procedura

1. Nella pagina **Dispositivi**, registrare un dispositivo iOS (18.2 +) o un dispositivo visionOS 2.2.
2. Accedere a **Configurazioni** > **Aggiungi configurazione** > **Impostazioni applicazione predefinita** per impostare il browser predefinito sui dispositivi iOS.
3. Fare clic su **Configurazioni** > **Crea impostazioni** > **Crea Configurazioni impostazioni predefinite applicazione**
4. Nella sezione Dettagli di configurazione, fornire il **Nome** e la **Descrizione**.
5. In Impostazioni di configurazione > Aggiungi app > Aggiungi per ricerca, cercare il browser desiderato. Viene visualizzato l'elenco dei browser.
6. Selezionare il browser desiderato dall'elenco.
7. Nella pagina **Crea Configurazione impostazioni predefinite applicazione**, fare clic su **Personalizzata** per distribuire la configurazione a un dispositivo specifico o a gruppi di dispositivi o a utenti o gruppi di utenti specifici.
8. In **Scegliere una di queste opzioni di distribuzione personalizzata**, selezionare l'opzione desiderata per specificare la distribuzione di questa configurazione a Utenti/Gruppi di utenti o a Dispositivi/Gruppi di dispositivi.
9. Selezionare l'opzione desiderata in **Tutti disponibili** per distribuire questa configurazione.
10. Fare clic su **Fine**.

10.10.8.32. Configurazione delle impostazioni host per la Condivisione schermo

La configurazione delle **Impostazioni host per la Condivisione schermo** consente agli amministratori di controllare in sicurezza le impostazioni di condivisione schermo macOS tra i dispositivi gestiti usando Ivanti Neurons per MDM. Questa funzione consente di specificare gli utenti autorizzati, i metodi di autenticazione e le restrizioni del servizio per garantire un accesso remoto conforme e sicuro.

Applicabile a: macOS 14.0 fino alla versione rilasciata più recente supportata da Ivanti Neurons per MDM.

Prima di iniziare: per l'integrazione diretta della configurazione delle **Impostazioni host per la Condivisione schermo**, l'utente deve abilitare '**Gestione remota**' sul proprio dispositivo. Nel proprio dispositivo, andare in **Impostazioni** > **Gestione remota** > **Abilita gestione remota**.

Procedura

1. Andare in **Configurazioni** > **+Aggiungi**.
2. Cercare e selezionare la configurazione delle **Impostazioni host per la Condivisione schermo**.
3. Configurare le **Impostazioni host per la Condivisione schermo** come da tabella seguente:

Impostazione	Descrizione
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Base porta	Inserire il numero della porta UDP iniziale per connettersi all'host. La condivisione schermo richiede più connessioni, quindi il sistema incrementa questo valore di 1 per ogni connessione aggiuntiva. Ciò non modifica il numero di porta che il sistema utilizza per stabilire inizialmente una connessione con un host, che è sempre la porta TCP 5900. **Valore base porta minimo**: 1024 **Valore base porta massimo**: 65535
Display virtuali massimi	È possibile utilizzare fino a due display virtuali.
Impedisci copia file da host	Selezionare la casella di controllo per impedire agli utenti di copiare file dall'host di condivisione schermo.
Impedisci copia file a host	Selezionare la casella di controllo per impedire agli utenti di copiare file all'host di condivisione schermo.
Impedisci connessioni ad altre prestazioni	Selezionare la casella di controllo per impedire agli utenti di stabilire connessioni ad alte prestazioni con l'host.

4. Fare clic su **Avanti** per configurare le impostazioni di distribuzione.
5. Selezionare una delle opzioni di distribuzione per impostare la configurazione delle **Impostazioni per l'host Condivisione schermo**. Per ulteriori informazioni sulla configurazione delle opzioni di distribuzione, vedere Utilizzo delle configurazioni.
6. Fare clic su **Fine**.

10.10.8.33. Configurazione della modalità Single-App

Configurazioni

Licenza: Silver

La modalità Single-App limita il numero di dispositivi iOS per l'utilizzo dell'app specificata. Ad esempio, può essere opportuno configurare i dispositivi che possono utilizzare solo un'app personalizzata sviluppata dalla propria organizzazione.

Configurazione della modalità Single-App

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo della configurazione.
Descrizione	Immettere una descrizione esplicativa dello scopo della configurazione.
Scegli app	Selezionare il metodo da utilizzare per la scelta dell'app: • **Da Catalogo app e App di sistema**: selezionare questa opzione per cercare nel Catalogo app Ivanti Neurons for MDM e nelle app di sistema (preinstallate per impostazione predefinita sui dispositivi Apple). • Immettere il nome dell'app e selezionarla quando compare nell'elenco delle applicazioni. • **Inserisci ID bundle:** selezionare per inserire l'identificatore univoco per l'app di sistema che si desidera selezionare. Utilizzare questa opzione se non è possibile trovare l'app di sistema utilizzando l'opzione **Da App Catalog e app di sistema**.
Disattiva Touch	Selezionare questa opzione per disattivare lo schermo touch.
Disattiva rotazione dispositivo	Selezionare questa opzione per disattivare il sensore di rotazione del dispositivo.
Disattiva pulsanti volume	Selezionare questa opzione per disattivare i pulsanti del volume del dispositivo.
Disattiva interruttore suoneria/silenzioso	Selezionare questa opzione per disattivare l'interruttore suoneria/silenzioso del dispositivo.
Disattiva tasto accensione/spegnimento	Selezionare questa opzione per disattivare il tasto di accensione/spegnimento (in alto a destra sul lato del dispositivo).
Disattiva blocco automatico	Selezionare questa opzione per impedire lo standby del dispositivo dopo un periodo di inattività.
Attiva VoiceOver	Selezionare questa opzione per attivare il lettore schermo VoiceOver (funzione di accessibilità).
Attiva zoom	Selezionare questa opzione per attivare lo zoom (funzione di accessibilità).
Attiva Inverti colori	Selezionare questa opzione per attivare la regolazione dei colori (funzione di accessibilità).
Attiva Assistive Touch	Selezionare questa opzione per attivare Assistive Touch (funzione di accessibilità).
Attiva Pronuncia selezione	Selezionare questa opzione per attivare Pronuncia selezione (funzione di accessibilità).
Attiva audio mono	Selezionare questa opzione per passare dall'audio stereo all'audio mono (funzione di accessibilità).

Impostazione	Operazione da eseguire
Regolazioni VoiceOver	Selezionare questa opzione per consentire agli utenti di effettuare le regolazioni VoiceOver.
Regolazioni Zoom	Selezionare questa opzione per consentire agli utenti di effettuare le regolazioni dello zoom.
Regolazioni Inverti colori	Selezionare questa opzione per consentire agli utenti di invertire i colori.
Regolazioni Assistive Touch	Selezionare questa opzione per consentire agli utenti di effettuare le regolazioni Assistive Touch.

Per ulteriori informazioni, vedere **Come creare una configurazione**.

10.10.8.34. Configurazione della frequenza di raccomandazione di aggiornamento software

Gli amministratori possono consentire agli utenti di visualizzare e aggiornare i dispositivi alla versione superiore (più recente), alla versione inferiore (meno recente) o a entrambe.

Applicabile a: iOS e iPadOS 14.5 fino alla versione 26.0 (supervisionata)

Procedura

1. Andare in Configurazioni > +Aggiungi.
2. Digitare Raccomandazione aggiornamento software nel campo di ricerca, quindi fare clic su Configurazione frequenza aggiornamento software.
3. Immettere un Nome e una Descrizione per la configurazione.
4. Selezionare la configurazione richiesta nel menu a discesa:
    - Presenta entrambe le versioni di aggiornamento
    - Presenta la versione di aggiornamento software inferiore (meno recente)
    - Presenta solo la versione di aggiornamento software superiore (più recente)
5. Fare clic su Avanti.
6. Selezionare l'opzione Abilita questa configurazione.
7. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzata.
8. Fare clic su Fine.

10.10.8.35. Menu Start e barra delle applicazioni

È possibile definire il layout del menu Start per gli utenti, per definire le applicazioni sicure da usare e rimuovere quelle non necessarie. Le versioni di Windows 10 e 11 supportano funzioni diverse, poiché i layout del menu Start sono diversi.

Per impostare la configurazione del menu Start e della barra delle applicazioni:

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Menu Start di Windows e barra delle applicazioni**.
3. Immettere un nome per la configurazione.
4. Selezionare la versione specifica per Windows.
5. **Dispositivi Windows 10**:
   Nella sezione **Impostazioni configurazione**, configurare le impostazioni seguenti:
   Impostazione
   Operazione da eseguire
   Nome
   Immettere un nome identificativo della configurazione.
   Descrizione
   Immettere una descrizione esplicativa dello scopo della configurazione.**Selezionare il dispositivo standard**
   Selezionare il dispositivo Windows 10 in cui sono presenti le app nel menu Start e nella barra delle applicazioni.
6. Fare clic su **Recupera layout del menu Start dal dispositivo** e configurare le opzioni seguenti.
7. **Impostazione**
   Operazione da eseguireLayout menu Start e barra delle applicazioni
   Selezionare una delle seguenti opzioni per nascondere l'elenco di app.
   - Nessuno
   - Nascondi tutti gli elenchi app
   - Nascondi tutti gli elenchi app e disabilita "Mostra elenco app nel menu Start" nell'app Impostazioni
   - Nascondi tutti gli elenchi app, rimuovi tutti i pulsanti delle app e disabilita "Mostra elenco app nel menu Start" nell'app Impostazioni

Layout menu StartPersonalizza il menu Start
Fare clic su **Sì** per personalizzare il menu Start e i parametri di layout.**Barra delle applicazioniPersonalizza barra delle applicazioni**Fare clic su **Sì** per personalizzare la barra delle applicazioni**Rimuovi i collegamenti rapidi fissati alla barra delle applicazioni prima di aggiungere quelli personalizzati**Fare clic su **Sì** per rimuovere i collegamenti rapidi fissati alla barra delle applicazioni prima di aggiungere la barra delle applicazioni personalizzata.**Tipo di app**Consente di specificare il tipo di app.**App**Consente di specificare l'ID dell'app.**Ripristina**
Fare clic sul link **Ripristina** per ripristinare la barra delle applicazioni dalla barra delle applicazioni originale del dispositivo Golden.
Fare clic e trascinare l'icona della freccia nella riga per spostare la posizione (in alto o in basso) della riga specifica.
Fare clic sull'icona Elimina per eliminare la riga.
Fare clic sul pulsante **Aggiungi nuovo** per aggiungere una nuova riga.

8. **Dispositivi Windows 11**
   Nella sezione **Impostazioni configurazione**, configurare le impostazioni seguenti:
   Impostazione
   Operazione da eseguire

Nome

Immettere un nome identificativo della configurazione.

Descrizione

Immettere una descrizione esplicativa dello scopo della configurazione.**Selezionare il dispositivo standard**

Selezionare il dispositivo Windows 11 che ha le app configurate nella sezione BLOCCATE del menu Start.**Layout menu Start e barra delle applicazioniLayout menu Start e barra delle applicazioni**

Selezionare una delle seguenti opzioni per visualizzare l'opzione di ricerca nella barra delle applicazioni:

- **Nascondi**
- **Icona Cerca**
- **Icona ed etichetta Cerca**
- **Casella di ricerca (predefinita)**

Selezionare la casella di controllo **Nascondi vista attività** per nascondere la vista attività.**App più utilizzate**

Selezionare una delle seguenti opzioni per configurare le app più utilizzate nel menu Start:

- **Non imporre la visibilità dell'elenco delle app più utilizzate in Start.**
- **Imponi visualizzazione dell'elenco delle app più utilizzate in Start.**
- **Imponi mancata visualizzazione dell'elenco delle app più utilizzate in Start.**

La casella di controllo **Consenti associazione alla barra delle applicazioni** è selezionata per impostazione predefinita.

Selezionare la casella di controllo **Nascondi sezione consigliata** per nascondere tutte le sezioni consigliate.

A causa di un problema del fornitore, la casella di controllo **Nascondi sezione consigliata** non avrà un impatto visibile sul dispositivo anche dopo che l'utente si è disconnesso o ha effettuato il login. Attualmente non è possibile nascondere la sezione consigliata.**Barra delle applicazioniTipo di app**

Selezionare una delle seguenti opzioni per specificare il tipo di app:

- **ID modello utente app**
- **Percorso di collegamento dell'applicazione desktop**

AppSpecifica l'ID o il percorso dell'app.**Ripristina**

Fare clic sul link **Ripristina** per ripristinare la barra delle applicazioni dalla barra delle applicazioni originale del dispositivo Golden.

Fare clic e trascinare l'icona della freccia nella riga per spostare la posizione (in alto o in basso) della riga specifica.

Fare clic sull'icona Elimina per eliminare la riga.

Fare clic sul pulsante **Aggiungi nuovo** per aggiungere una nuova riga.

9. Fare clic su **Recupera layout del menu Start dal dispositivo**.
10. Dopo aver recuperato le impostazioni dal Golden Device, tutte le app configurate nella sezione BLOCCATE del menu di avvio saranno visualizzate per essere esaminate dall'amministratore.
    Fare clic su **Avanti** e distribuire la configurazione a tutti i gruppi di dispositivi e utenti applicabili.

> A causa di un problema del fornitore, quando la configurazione non è distribuita, le app bloccate rimarranno configurate come in origine. Tuttavia, quando viene distribuita una nuova configurazione, il layout precedente viene sovrascritto e viene applicato il nuovo layout.

10.10.8.36. Configurazione aggiornamento di sistema

Gli amministratori possono impedire agli utenti dei dispositivi di gestire gli aggiornamenti di sistema sui dispositivi Android 6.0 o sulle versioni più recenti supportate. Questa funzione è applicabile solo ai dispositivi Android Enterprise.

Per la configurazione, procedere come segue:

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Aggiornamento del sistema**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Nella sezione Impostazioni configurazione, configurare le opzioni seguenti:

Impostazione	Descrizione
Automatico	Applicare l'aggiornamento del sistema in modalità invisibile all'utente ogni volta che è disponibile un nuovo firmware.
Posticipa	Posticipa l'installazione degli aggiornamenti del sistema per 30 giorni. Al termine del periodo di 30 giorni, il sistema richiede all'utente del dispositivo di installare l'aggiornamento.
Con finestra (ora locale)	Pianifica un periodo di tempo per applicare l'aggiornamento del sistema in modalità invisibile all'utente. Selezionare **Ora di inizio** e **Ora di fine**.

Impostazione	Descrizione
Aggiornamento manuale del sistema operativo (Android 10+) Non applicabile o non supportato sui dispositivi Samsung e Zebra	Selezionare per eseguire l'aggiornamento del sistema operativo manualmente su un numero limitato di dispositivi prima di distribuire l'aggiornamento a tutti i dispositivi. **File firmware** - Selezionare l'opzione **Attributo personalizzato** o **URL HTTPS**. Immettere i seguenti dettagli: • Posizione del firmware - Se è stato selezionato **Attributo personalizzato** come opzione File firmware, è necessario fornire l'attributo personalizzato utilizzato per il Trasferimento file. Il file del firmware può essere autocostruito o può essere caricato su Ivanti Neurons per MDM utilizzando la configurazione Trasferimento file. Per i dettagli, consultare la **Configurazione del trasferimento di file** per i dettagli. Il caricamento di file superiori a 50 MB su Ivanti Neurons per MDM richiede una licenza aggiuntiva. • Descrizione (opzionale) • Impronta digitale (obbligatoria) - Per convalidare che la versione del sistema operativo prevista sia installata sul dispositivo. L'impronta digitale può essere trovata nel file OTA decomprimendo la cartella OTA e aprendo il file /META-INF/com/android/metadata. Cercare una voce simile a quella qui sotto: "post-build=google/xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxxxx:user/release-keys" Nella voce sopra riportata, **google/ xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxx:user/release-keys** è l'impronta digitale e TQ3A.230805.001.S1 è l'ID di compilazione (l'ID di compilazione è il quarto valore da sinistra nei valori separati da '/' nell'impronta digitale). • Checksum (opzionale) **Impostazioni di aggiornamento** → **Richiesta di aggiornamento del sistema operativo** - Le impostazioni di questa sezione sono le stesse di Configurazione firmware Zebra. Fare riferimento alla sezione *Configurazione del firmware Zebra* in questa tabella. Se si seleziona **HTTPS URL** come opzione File firmware, è necessario fornire le seguenti informazioni: • Posizione del firmware - Inserire il percorso da cui è possibile scaricare il firmware senza richiedere l'autenticazione. Descrizione (opzionale) • Impronta digitale (obbligatoria) - Per convalidare che la versione del sistema operativo prevista sia installata sul dispositivo. • Checksum (opzionale) Sono disponibili le sezioni **Inizializza richiesta di download** e **Condizioni durante il download** oltre alla sezione "**Richiesta aggiornamento sistema operativo**". Le opzioni disponibili nelle sezioni **Inizializza richiesta di download** e **Durante le condizioni di download** sono le stesse della sezione **Configurazione firmware Zebra**. Una volta avviato l'aggiornamento del sistema nel dispositivo dopo il download, il riavvio del dispositivo tra un aggiornamento e l'altro interrompe il processo di aggiornamento.
Periodo di blocco	Blocca l'aggiornamento del sistema per un periodo di tempo specificato. Questa opzione è applicabile solo ai dispositivi Android 9.0 e versioni successive. Fare clic su **Aggiungi periodo di blocco**. Selezionare la **Data di inizio** e la **Data di fine** per il periodo di blocco. Il periodo di blocco non può essere superiore a 90 giorni e si possono aggiungere più periodi di blocco. Il periodo di blocco successivo può essere selezionato solo dopo 60 giorni di calendario dalla data di fine

Impostazione	Descrizione
	precedente. Per eliminare un periodo di blocco, fare clic sull'icona Elimina.
Configurazione firmware Zebra	Selezionare **Configura Zebra OTA** per aggiornare il firmware operativo dei dispositivi Zebra (che eseguono Android 8.0 o una versione successiva supportata). Ciò è applicabile solo in modalità Proprietario del dispositivo. Per configurare gli aggiornamenti di Zebra OTA, è necessario abilitare il servizio OTA per Ivanti Neurons for MDM in **Amministratore > Gestione firmware > Zebra OTA** e in Ivanti Neurons for MDM devono essere presenti dispositivi Zebra. È necessario immettere le proprie credenziali Zebra nella finestra popup. Per creare di nuovo le credenziali, contattare direttamente Zebra. Quando questa opzione è selezionata, viene visualizzato l'elenco dei dispositivi Zebra registrati. Per selezionare e applicare il firmware al modello del dispositivo: 1. Nella colonna **Azione** del dispositivo Zebra, eseguire una delle seguenti azioni: ◦ **Nessuna**: non viene eseguita alcuna azione per il modello del dispositivo. ◦ **Aggiornamento completo**. Nella finestra **Seleziona firmware Zebra di destinazione**, selezionare la versione firmware dell'aggiornamento completo da applicare al modello del dispositivo. Durante il processo di **Upgrade completo** è necessaria solo la porta 443. Nel campo **Cerca**, è possibile digitare i caratteri di un ID build per cercare gli aggiornamenti in base all'ID build. Gli ID build vengono ordinati e visualizzati in ordine decrescente (dal più recente al meno recente). L'opzione **Upgrade patch NON** sarà disponibile per i dispositivi Android 11+. 2. Configurare le opzioni seguenti desiderate: **Avvia richiesta di download** - Queste condizioni saranno valutate dal sistema Go app. ◦ **Livello minimo richiesto della batteria**: spostare il cursore per impostare il livello minimo di batteria richiesto dall'intervallo disponibile. ◦ **Richiedi che il dispositivo sia in carica**: selezionare questa opzione per mantenere il dispositivo in modalità di ricarica durante il processo. ◦ **Pianificazione download**: selezionare questa opzione per creare una pianificazione per avviare la richiesta di download e il download dei file. ◦ Le opzioni **Richiedi dispositivo inattivo**, **Richiedi ricarica** e **Consenti download su rete a pagamento** vengono trasferite ad Android Download Manager. Go app aggiungerà la richiesta di download ad Android Download Manager nella finestra indicata con i parametri sopra indicati. **Applica pianificazione per download**: selezionare i valori per **Giorno/i della settimana**, **Ora di inizio** e **Ora di fine** per pianificare il download. Per pianificare il download, è possibile selezionare più giorni. Ad esempio, se vengono selezionati Sabato e Domenica con ora di inizio e ora di fine tra le ore 00.00 e le ore 23.00, il download nei dispositivi Zebra viene effettuato solo durante questa fascia oraria nei giorni selezionati. In Go app, il download inizia come previsto quando la configurazione viene applicata al dispositivo. Non è previsto alcun limite di tempo per completare il download. Pertanto, l'operazione può essere completata dopo l'orario di fine pianificato. ◦ Applica pianificazione per download: selezionare i valori per **Giorno/i della settimana**, **Ora di inizio** e **Ora di fine** per pianificare l'installazione dell'aggiornamento firmware. Se il livello di carica della batteria del dispositivo è inferiore a 32, l'installazione viene posticipata.

Impostazione	Descrizione
	Se non viene configurata alcuna pianificazione per l'aggiornamento, l'installazione viene avviata immediatamente dopo il completamento del download del firmware. 3. Configurare le opzioni seguenti desiderate: **Condizioni durante il download**- Queste condizioni saranno valutate da Download Manager. È possibile effettuare la selezione in base ai criteri. ◦ **Richiedi stato di inattività del dispositivo** (selezionata per impostazione predefinita): consente di eseguire gli aggiornamenti firmware solo quando il dispositivo è inattivo. ◦ **Richiedi stato di ricarica** (selezionata per impostazione predefinita): consente di eseguire gli aggiornamenti firmware solo quando il dispositivo è in modalità di ricarica. ◦ **Consenti download su rete a pagamento**: selezionare questa opzione per consentire il download in modalità Wi-Fi. Questa opzione è deselezionata per impostazione predefinita. ◦ Le opzioni **Richiedi dispositivo inattivo**, **Richiedi ricarica** e **Consenti download su rete a pagamento** vengono trasferite ad Android Download Manager. Go app aggiungerà la richiesta di download ad Android Download Manager nella finestra indicata con i parametri sopra indicati. **Consenti di continuare il download al di fuori della 'pianificazione di download' specificata**: selezionare questa opzione per consentire il download al di fuori della pianificazione di download specificata. **Richiesta di aggiornamento del sistema operativo** ◦ **Livello minimo di batteria richiesto** - Selezionare questa opzione per impostare il livello minimo di batteria che deve essere disponibile per richiedere l'aggiornamento del sistema operativo. ◦ **Richiedi che il dispositivo sia in carica**: selezionare questa opzione per mantenere il dispositivo in modalità di ricarica durante la procedura ◦ **Crea pianificazione per avviare l'aggiornamento del sistema operativo sul dispositivo** - Selezionare questa opzione per impostare una pianificazione in cui l'aggiornamento del sistema operativo verrà avviato sul dispositivo. In Go app, il download inizia come previsto quando la configurazione viene applicata al dispositivo. Non è previsto alcun limite di tempo per completare il download. Pertanto, l'operazione può essere completata dopo l'orario di fine pianificato. Fare clic su **Applica**.
Configurazione Samsung e-FOTA	Selezionare **Configura Samsung e-FOTA** per aggiornare il firmware operativo dei dispositivi Samsung (su Knox 2.7.1 e versioni successive). Ciò è applicabile solo a un dispositivo gestito nella modalità Profilo di lavoro su dispositivo di proprietà dell'azienda. Se non è presente alcun dispositivo registrato compatibile con Samsung e-FOTA, viene visualizzato un messaggio con questa informazione nella pagina. Per configurare aggiornamenti di Samsung E-FOTA, è necessario attivare la licenza Samsung e-FOTA in **Amministratore > Gestione firmware > Samsung E-FOTA**. Se questa opzione è selezionata, viene visualizzato l'elenco dei dispositivi Samsung registrati. Per selezionare e applicare il firmware al modello del dispositivo: 1. Nella colonna **Azione** del dispositivo Samsung, eseguire una delle seguenti azioni: ◦ **Più recente**: viene applicata la versione firmware più recente. Questa opzione è selezionata per impostazione predefinita.

Impostazione	Descrizione
	◦ **Forza**: nella finestra Seleziona firmware Samsung di destinazione, selezionare la versione firmware specifica da applicare forzatamente (senza l'intervento dell'utente) al modello di dispositivo. Una volta eseguita questa operazione, viene eseguito il download del firmware entro quindici minuti. ◦ **Destinazione**: nella finestra Seleziona firmware Samsung di destinazione, selezionare la versione firmware specifica da applicare al modello di dispositivo. Durante l'esecuzione delle azioni "Forza" o "Destinazione", se non è presente alcun firmware per il dispositivo, viene visualizzato un messaggio con questa informazione nella pagina. 2. **Abilita Debug FW** (Opzionale): quando l'opzione **Abilita Debug FW** è attivata, e si applica la configurazione, il dispositivo viene aggiornato a un firmware provvisorio. La versione provvisoria del firmware del dispositivo Samsung consente all'amministratore di testare il comportamento di configurazione dell'aggiornamento di sistema sui dispositivi, senza realmente modificare nulla sul dispositivo. Per eseguire l'aggiornamento effettivo del firmware, al posto del firmware provvisorio, l'amministratore deve garantire che l'opzione **Abilita Debug FW** sia disattivata prima di applicare la configurazione 3. Fare clic su **Applica**.

6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni di distribuzione:

- Tutti i dispositivi
- Nessun dispositivo (impostazione predefinita)
- Personalizzato

8. Fare clic su **Fine**.

Configurazione Samsung E-FOTA (dismessa)

La configurazione Samsung E-FOTA sarà dismessa nel luglio 2022. Pertanto, tale configurazione non sarà disponibile per i nuovi dispositivi. I dispositivi con la configurazione esistente possono solo disattivare questa configurazione.

10.10.8.37. Gestione aggiornamenti di Windows 10

In quanto amministratore, è possibile visualizzare e approvare gli aggiornamenti segnalati dai dispositivi Windows 10 che si desidera aggiornare tramite Gestione aggiornamenti di Windows 10. Questa funzione consente di evitare l'installazione di aggiornamenti non necessari o non verificati nei dispositivi.

La funzione Gestione aggiornamenti richiede che i dispositivi siano impostati con la configurazione **Aggiornamenti software** e l'opzione **Richiedi approvazione aggiornamenti** attivata. I dispositivi riportano gli aggiornamenti da installare e attendono l'approvazione solo se viene applicata questa configurazione.

Gestione degli aggiornamenti

1. Andare su **Amministratore > Windows > Aggiornamenti di Windows**. Nella pagina vengono visualizzati i seguenti dettagli degli aggiornamenti.
   Data creazione: la data di creazione dell'aggiornamento.**Titolo**: descrive il tipo di aggiornamento e il numero dell'articolo Knowledge Base.

> Facendo clic sull'aggiornamento viene visualizzata la descrizione.

Classificazione: classifica il tipo di aggiornamento in una delle seguenti categorie:

- Aggiornamenti critici
- Aggiornamenti definizione
- Aggiornamenti driver
- Aggiornamenti sulla sicurezza
- Aggiornamenti
- Upgrade
- Rollup di aggiornamento

Distribuzione: la distribuzione eseguita per l'aggiornamento. Ad esempio, viene visualizzato **Tutti** quando l'aggiornamento è distribuito a tutti i dispositivi.

> Se l'aggiornamento viene distribuito a un numero specifico di gruppi, viene visualizzato il conteggio della distribuzione. Ad esempio, viene visualizzato 3 se la distribuzione è eseguita solo per 3 gruppi.

2. Inoltre, è possibile vedere se un aggiornamento è stato distribuito o meno ai dispositivi richiesti. Le colonne seguenti contengono numeri che indicano il numero di dispositivi presenti nelle diverse categorie di aggiornamenti:
   - Dispositivi idonei
   - Dispositivi installati
   - Dispositivi non riusciti
   - Dispositivi in attesa di riavvio

Facendo clic su uno di questi numeri, si verrà indirizzati alla vista filtrata della pagina Dispositivi per conoscere lo stato degli aggiornamenti ed eseguire le azioni richieste.
Rivedere gli aggiornamenti e selezionare la voce da distribuire ai dispositivi facendo clic sulla relativa casella di controllo.

3. In **Azioni**, fare clic su **Imposta distribuzione**.
4. Nella finestra **Distribuisci aggiornamenti Windows**, selezionare una delle seguenti opzioni di distribuzione:
   Tutti i dispositivi: gli aggiornamenti vengono distribuiti a tutti i dispositivi.
   Nessun dispositivo: gli aggiornamenti non vengono distribuiti ai dispositivi.**Personalizzata**: gli aggiornamenti vengono distribuiti a specifici gruppi di dispositivi.
5. Fare clic su **Salva**.

Ricerca e applicazione di filtri agli aggiornamenti

È possibile cercare ed applicare filtri agli aggiornamenti in base ai seguenti criteri:

- ID articolo Knowledge Base
- Distribuzione configurata

Applicazione di filtri in base ad ID articolo Knowledge Base

1. Nella pagina **Gestione aggiornamenti di Windows 10**, digitare l'ID della Base di conoscenza nel campo di ricerca rapida (solo il numero nel campo Cerca).
   Esempio: per KB4056892 digitare 4056892. L'aggiornamento corrispondente ai criteri di ricerca viene visualizzato nella pagina.

> È possibile cercare ulteriori informazioni sull'aggiornamento facendo clic sui collegamenti **Assistenza** e **Altre informazioni**. Il collegamento **Assistenza** indirizza alla pagina Web Microsoft che fornisce informazioni di supporto sui prodotti per l'aggiornamento, mentre il collegamento **Altre informazioni** indirizza alla pagina Web Microsoft che mostra ulteriori informazioni sull'aggiornamento, ad esempio l'articolo Knowledge Base.

Applicazione di filtri in base a distribuzione configurata:

Nella pagina **Gestione aggiornamenti di Windows 10**, selezionare una delle seguenti opzioni di filtraggio in base alla distribuzione configurata:

- **Tutti**: mostra tutti gli aggiornamenti.
- **Configurata**: mostra l'elenco degli aggiornamenti distribuiti ai dispositivi.
- **Non configurata**: mostra l'elenco degli aggiornamenti per i quali la distribuzione non è specificata.

> I filtri configurati e non configurati sono basati sulla distribuzione eseguita, che può anche essere impostata su **Nessuna**.

Visualizzazione di aggiornamenti per un dispositivo

Per visualizzare le informazioni dettagliate sugli aggiornamenti specifici per un dispositivo:

1. Andare in **Dispositivi > Dispositivi**.
2. Fare clic sul nome di un dispositivo per visualizzare la pagina dei dettagli.
3. Andare alla scheda **Aggiornamenti**. Vengono visualizzati gli aggiornamenti per il dispositivo in sospeso (aggiornamento approvato dall'amministratore ma non riportato come installato sul dispositivo), non riusciti e installati.

È inoltre possibile vedere le notifiche sui nuovi aggiornamenti di Windows disponibili nella pagina Notifiche sotto il Dashboard. La notifica include la data di creazione della notifica, il numero di notifiche disponibili e lo scopo della notifica. La notifica degli aggiornamenti Windows è visibile anche nell'angolo in alto a destra del portale Amministratori.

10.10.8.38. Pianificazione delle app Windows

Le app del desktop Windows possono essere di grandi dimensioni, aggiungendo così un carico ulteriore ed esteso su reti e server durante i tempi di utilizzo più importanti per l'azienda. La funzione di pianificazione delle app Windows consente agli utenti di pianificare un orario per installare le app, specialmente quelle di grandi dimensioni, nei dispositivi in un orario a scelta.

Per configurare la pianificazione delle app:

1. Andare in **App > Catalogo app**.
2. Fare clic su **Aggiungi**, selezionare un'app Windows e continuare con i passaggi successivi della procedura guidata **Aggiungi app**.
3. Al punto 5 (Configura), fare clic su **Impostazioni di configurazione Installa applicazione** per visualizzare la pagina **Impostazione configurazione**.
4. Selezionare la casella di controllo **Pianifica installazione**.

> La casella di controllo **Pianifica installazione** viene visualizzata solo quando l'installazione invisibile all'utente è abilitata.

5. Selezionare un **orario di inizio** e un **orario di fine** per pianificare l'orario in cui installare le app.
6. Selezionare una **Data di inizio** e una **Data di fine** per pianificare la data in cui installare le app.

> È inoltre possibile selezionare una delle due azioni seguenti, da eseguire in caso di mancato rispetto della data programmata: **Installa durante il prossimo check-in** o **Non installare**.

7. Selezionare un'opzione di distribuzione della configurazione app: **Tutti gli utenti con app**, **Nessuno** o **Personalizzata**.
8. Fare clic su **Fine**.

> Le app da pianificare non devono essere aggiunte in Apps@Work.
> La pianificazione delle app non è applicabile alle app del negozio poiché l'installazione invisibile di queste non è supportata.

10.10.8.39. Configurazione del BIOS di Windows

Gli amministratori possono configurare le impostazioni del BIOS di Windows sui dispositivi Lenovo. Per impostare questa configurazione è necessario che sia registrato almeno un dispositivo Lenovo che supporta le impostazioni del BIOS.

Per la configurazione, procedere come segue:

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **BIOS di Windows**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Nella sezione Choose device model, selezionare il modello di dispositivo dall'elenco a discesa.
6. Nella sezione Impostazioni configurazione, configurare le opzioni seguenti:

> L'elenco di impostazioni varia a seconda di ciò che è disponibile per il modello specifico di dispositivo che viene registrato. Per maggiori informazioni, consultare il sito web del dispositivo corrispondente.

Impostazione	Operazione da eseguire
Controllo AMT	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
CA gestione termica adattiva	Selezionare una delle seguenti opzioni: • **Bilanciato** • **Prestazioni ottimizzate**
Batteria gestione termica adattiva	Selezionare una delle seguenti opzioni: • **Bilanciato** • **Prestazioni ottimizzate**
USB sempre attiva	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
BIOSPasswordAtBootDeviceList	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Password BIOS al riavvio	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Password BIOS all'avvio non monitorato	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Aggiornamento del BIOS da parte dell'utente finale	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Accesso Bluetooth	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Opzione F12 per elenco dispositivi avvio	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**

Impostazione	Operazione da eseguire
Disp. visual. avvio	Selezionare una delle seguenti opzioni: • **DisplayPort** • **Display dock** • **HDMI** • **LCD**
Mod. avvio	Selezionare una delle seguenti opzioni: • **Diagnostica** • **Rapido**
Blocco ordine avvio	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
BootTimeExtension	Selezionare una delle seguenti opzioni: • **1** • **10** • **2** • **3** • **5** • **Disattiva**
Rilevata manomissione cover inferiore	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Risparmio energia CPU	Selezionare una delle seguenti opzioni: • **Automatico** • **Disattiva**
Attivazione modulo Computrace	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Protezione esecuzione programmi	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Accesso LAN Ethernet	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
ROM opzione LAN Ethernet	Selezionare una delle seguenti opzioni: • **Disattiva**

Impostazione	Operazione da eseguire
	• **Attiva**
Autenticazione password con impronta digitale	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Autenticazione con impronta digitale prima del desktop	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Accesso lettore impronte digitali	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Priorità lettore impronte digitali	Selezionare una delle seguenti opzioni: • **Esterno** • **Solo interno**
Modalità protezione impronte digitali	Selezionare una delle seguenti opzioni: • **Alta** • **Normale**
Scambio tasti Ctrl Fn	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
FnKeyAsPrimary	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
FnSticky	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Stack rete IPv4	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Stack rete IPv6	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Accesso fotocamera integrata	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**

Impostazione	Operazione da eseguire
InternalStorageTamper	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Segnale acustico tastiera	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Impostazione per blocco BIOS	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Accesso slot scheda di memoria	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Accesso microfono	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Lunghezza minima della password	Selezionare una delle seguenti opzioni: • 4 • 5 • 6 • 7 • 8 • 9 • 10 • 11 • 12 • **Disattiva**
NFFControl	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Accesso NFC	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Alimentazione tramite cavo CA	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**

Impostazione	Operazione da eseguire
PasswordBeep	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Errore per numero tentativi password superato	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Presenza fisica per cancellazione TPM	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Presenza fisica per provisioning TPM	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Tecnologia Rapid Start	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Avvio sicuro	Selezionare **Attiva**
Prevenzione rollback sicuro	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Chip protezione	Selezionare una delle seguenti opzioni: • **Attivo** • **Disattiva** • **Attiva** • **Inattivo**
Accesso slot Smart Card Slot	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
SpeedStep	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Tasti opzione avvio	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Funzionalità TXT	Selezionare una delle seguenti opzioni:

Impostazione	Operazione da eseguire
	• **Disattiva** • **Attiva**
Memoria grafica totale	Selezionare una delle seguenti opzioni: • **256 MB** • **512 MB**
TouchPad	Selezionare una delle seguenti opzioni: • **Automatico** • **Disattiva**
TrackPoint	Selezionare una delle seguenti opzioni: • **Automatico** • **Disattiva**
Modalità USB30	Selezionare una delle seguenti opzioni: • **Automatico** • **Disattiva** • **Attiva**
Supporto BIOS USB	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Accesso porta USB	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Priorità avvio PXE UEFI	Selezionare una delle seguenti opzioni: • **Prima IPv4** • **Prima IPv6**
Funzionalità VT-d	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Tecnologia di virtualizzazione	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**

Impostazione	Operazione da eseguire
Riattivazione da LAN	Selezionare una delle seguenti opzioni: • **Solo CA** • **CA e batteria** • **Disattiva** • **Attiva**
Accesso LAN wireless	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**
Accesso WAN wireless	Selezionare una delle seguenti opzioni: • **Disattiva** • **Attiva**

7. Fare clic su **Avanti**.
8. Selezionare una delle seguenti opzioni di distribuzione:
   - Tutti i dispositivi
   - Nessun dispositivo (impostazione predefinita)
   - Personalizzato
9. Fare clic su **Fine**.

10.10.8.40. Windows BitLocker

Con il ruolo di amministratore è possibile eseguire in blocco l'aggiornamento della chiave di ripristino per un insieme di dispositivi Windows 10 crittografati, caricando un file Excel con il GUID dispositivo e la password di ripristino.

Per caricare il file Excel per l'aggiornamento in blocco della chiave di ripristino:

1. Andare su **Amministratore > Windows BitLocker**.
2. Fare clic su **Scarica file csv di esempio** per scaricare e visualizzare un file CSV di esempio.
3. Creare e aggiungere i record per il file .csv delle chiavi di ripristino BitLocker.
4. Fare clic su **Carica password di ripristino**
5. Fare clic su **Scegli file** per caricare il file .csv creato.
6. Fare clic su **Carica**. Il caricamento di un nuovo file con le chiavi caricate in precedenza sovrascriverà le voci meno recenti.

> È possibile inviare massimo 1.000 record per ogni caricamento. Al termine del caricamento, è possibile rivedere le singole chiavi nei dettagli di ciascun dispositivo.

10.10.8.41. Configurazione tutto schermo Windows

Utilizzando la configurazione tutto schermo di Windows, è possibile configurare tutto schermo ad app singola o app multiple sui dispositivi con Windows 10. Applicando questa configurazione, gli utenti tutto schermo hanno un accesso limitato alle funzionalità al di fuori delle app tutto schermo. Questa configurazione richiede l'abilitazione di Windows Bridge.

Di seguito sono riportati 3 modi in cui la configurazione può essere applicata.

- Applicazione singola
- Applicazioni multiple (recupera elenco di applicazioni dal dispositivo Windows)
- Applicazioni multiple (seleziona un layout esistente dalla configurazione del menu Start)

> Le applicazioni utilizzate per una configurazione tutto schermo di Windows dovrebbero essere già presenti sul dispositivo prima di entrare in una modalità tutto schermo Windows configurata.

Per impostare la configurazione tutto schermo di Windows:

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **tutto schermo Windows**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. Nella sezione Impostazioni configurazione, specificare le impostazioni rimanenti come descritto nella tabella seguente.

Impostazione	Operazione da eseguire
Selezionare la modalità tutto schermo: selezionare una delle seguenti 3 opzioni.	
Applicazione singola	Selezionare questa opzione per configurare la modalità tutto schermo ad applicazione singola per un dispositivo. 1. Nella sezione **Selezionare il dispositivo Windows (facoltativo)**, scegliere un dispositivo con Windows 10. Fare clic su **Recupera app dal dispositivo** per recuperare l'elenco delle app da un dispositivo. Per riuscire a recuperare i dati delle app, il dispositivo selezionato deve essere sottoposto a supervisione e richiede il check-in. Per saltare questi passaggi, selezionare la casella di controllo **Saltare questo passaggio. Se lo si desidera, è possibile eseguirlo in un secondo momento**. 2. Fare clic su **Aggiungi da elenco di app recuperato** per aggiungere app dall'elenco recuperato. 3. Selezionare una singola app facendo clic sul relativo pulsante nella colonna **Nome** dell'app. Fare clic su **Aggiungi nuovo** per aggiungere una nuova app all'elenco. Per eliminare un'app dall'elenco, fare clic sull'icona Elimina.
Applicazioni multiple (recupera elenco di applicazioni dal dispositivo Windows)	Selezionare questa opzione per configurare la modalità tutto schermo ad applicazioni multiple per un dispositivo. 1. Nella sezione **Selezionare il dispositivo Windows (facoltativo)**, scegliere un dispositivo con Windows 10. Fare clic su **Recupera app dal dispositivo** per recuperare l'elenco delle app da un dispositivo. Per recuperare correttamente i dati delle app, il dispositivo selezionato deve essere sottoposto a supervisione e richiede il check-in. Per saltare questi passaggi, selezionare la casella di controllo **Saltare questo passaggio. Se lo si desidera, è possibile eseguirlo in un secondo momento**. 2. In **App tutto schermo e layout del menu Start**, fare clic su **Aggiungi da elenco di app recuperato**. Viene visualizzata la finestra **Selezionare app tutto schermo**. Selezionare le app dall'elenco recuperato e fare clic su **Usa l'app selezionata**. 3. Nella sezione Altre app consentite, fare clic su **Aggiungi da elenco di app recuperato**. Viene visualizzata la finestra **Selezionare app tutto schermo**. Selezionare le app dall'elenco recuperato e fare clic su **Usa l'app selezionata**. Le altre app consentite sono le app considerate come dipendenze delle app selezionate in **App tutto schermo e layout del menu Start**. Senza "app consentite", il sistema operativo non permette di eseguire l'applicazione anche quando l'icona dell'applicazione viene visualizzata nel menu Start. 4. Fare clic su **Aggiungi nuovo** per aggiungere una nuova app all'elenco. Per eliminare un'app dall'elenco, fare clic sull'icona Elimina. È possibile trascinare e spostare un'app in una qualsiasi posizione nell'elenco. 5. In **Altre impostazioni per app multiple**, selezionare le opzioni desiderate: ◦ **Nascondi pulsante di accensione** ◦ **Nascondi riquadro utente**

Impostazione	Operazione da eseguire
	◦ **Nascondi barra delle applicazioni** In Microsoft Windows 11, l'opzione della modalità tutto schermo multi app "**Nascondi barra delle attività**" non è supportata.
Applicazioni multiple (seleziona un layout esistente dalla configurazione del menu Start)	Se è stata creata la configurazione di un layout del menu Start, è possibile importarla e utilizzarla per configurare la modalità ad applicazioni multiple selezionando questa opzione. 1. Nella sezione **Seleziona layout**, selezionare un layout che è stato precedentemente impostato come configurazione del menu Start. Le configurazioni create in precedenza con parametri del layout applicabili vengono visualizzate nell'elenco a discesa riportato di seguito. 2. In Altre impostazioni per app multiple, selezionare le opzioni desiderate: ◦ **Nascondi pulsante di accensione** ◦ **Nascondi riquadro utente** ◦ **Nascondi barra delle applicazioni** In Microsoft Windows 11, l'opzione della modalità tutto schermo multi app "**Nascondi barra delle attività**" non è supportata.

6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni di distribuzione:

- Tutti i dispositivi
- Nessun dispositivo (impostazione predefinita)
- Personalizzato

8. Fare clic su **Fine**.

> Affinché la configurazione diventi effettiva, il dispositivo deve essere riavviato dopo aver applicato o aggiornato una configurazione tutto schermo Windows. A seconda delle applicazioni nella configurazione tutto schermo ad app multiple, può essere necessario riavviare il dispositivo una seconda volta. Alcune icone possono essere assenti al primo accesso, ma verranno comunque visualizzate all'accesso dopo il secondo riavvio.

Il dispositivo deve essere riavviato dopo l'applicazione, l'eliminazione o l'aggiornamento di una configurazione tutto schermo. L'operazione può essere eseguita mediante il comando Riavvia/Arresta dispositivo dal menu delle azioni del dispositivo. Senza il riavvio:

- Il dispositivo non entra automaticamente nella modalità tutto schermo dopo aver applicato una configurazione tutto schermo.
- Il dispositivo non esce automaticamente dalla modalità tutto schermo dopo aver eliminato una configurazione tutto schermo applicata.
- Il dispositivo non modifica la configurazione tutto schermo in esecuzione.

Se un dispositivo con una configurazione tutto schermo applicata riceve una configurazione aggiornata, il sistema operativo Windows sul dispositivo rimuove un utente tutto schermo esistente e ricrea un nuovo utente tutto schermo con una nuova configurazione tutto schermo. La sessione dell'utente attuale deve essere terminata in modo esplicito con il riavvio del dispositivo.

È preferibile utilizzare file ".lnk" nel caso di una configurazione tutto schermo ad app multiple e file ".exe" nel caso di una configurazione tutto schermo ad app singola. Una configurazione del menu Start importata da un dispositivo utilizza il formato ".lnk".

Le voci del menu Start create manualmente per le applicazioni ".exe" a volte potrebbero non essere visualizzate nel menu Start di una configurazione tutto schermo ad app multiple, a seconda dell'applicazione ".exe".

Ad esempio, Windows Media Player può essere aggiunto al menu Start utilizzando uno dei seguenti file ".lnk":

- %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Media Player.lnk
- %ALLUSERSPROFILE%\Microsoft\\Windows\Start Menu\Programs\Windows Media Player.lnk

Se questa app viene aggiunta direttamente con uno dei seguenti file ".exe", non verrà visualizzata un'icona corrispondente anche se il percorso del primo file ".exe" viene utilizzato internamente nei file ".lnk" riportati qui sopra:

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
- C:\Program Files\Windows Media Player\wmplayer.exe

Nel caso di una configurazione tutto schermo ad app singola, è possibile aggiungere argomenti al file exe. E.g. '%ProgramFiles%\Internet Explorer\iexplore.exe -k www.bing.com'. Tuttavia, l'icona dell'app .exe con argomenti non viene visualizzata nel menu Start nel caso di una configurazione ad app multiple. Se in una configurazione tutto schermo ad app multiple è necessaria un'app .exe con argomenti, utilizzare un file ".lnk" che può avere argomenti all'interno. Il file ".lnk" non funziona in caso di una configurazione tutto schermo ad app singola.

Dipendenze nella modalità tutto schermo ad app multiple

Le applicazioni Win32/64 potrebbero richiedere l'aggiunta di dipendenze nella sezione Altre app consentite nel caso della modalità tutto schermo ad app multiple. Altre app consentite non sono necessarie nella modalità tutto schermo ad app singola.

Esempio 1: per l'app Windows Media Player, nella modalità tutto schermo ad app multiple sono necessarie le seguenti dipendenze:

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\setup_wm.exe

La prima dipendenza è costituita dai file binari dell'app chiamati dal file ".lnk file" corrispondente. La seconda è una procedura guidata da eseguire una sola volta, chiamata dalla prima dipendenza.

Senza "App consentite", il sistema operativo non consente di eseguire questa applicazione, anche quando l'icona dell'applicazione viene visualizzata nel menu Start.

Esempio 2: per Internet Explorer, la relativa icona viene visualizzata nel menu Start se è configurata con una qualsiasi delle voci dell'elenco seguente:

- %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 richiede le seguenti dipendenze:

- 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 prima dipendenza è costituita dai file binari dell'app necessari solo per la voce ".lnk", le altre dipendenze sono per la procedura guidata da eseguire una sola volta. Senza la prima dipendenza, il sistema operativo blocca le app con un messaggio popup. Senza le altre dipendenze, l'applicazione viene chiusa subito dopo l'avvio senza ulteriori notifiche dal sistema operativo.

10.10.8.42. Configurazione licenza Windows

La configurazione della licenza di Windows aggiorna il sistema operativo in uso sul dispositivo come da Windows 10 Pro a Windows 10 Enterprise. In aggiunta, questa configurazione offre la possibilità di attivare o modificare il codice prodotto dei dispositivi desktop Windows 10.

Per aggiornare una licenza di Windows:

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare la configurazione **Licenza Windows**.
3. Immettere un nome per la configurazione.
4. Nella sezione **Impostazioni configurazione**, digitare il **codice Product Key** di Windows.
5. Fare clic su **Avanti**.
6. Selezionare una delle seguenti opzioni di distribuzione:
    - Tutti i dispositivi
    - Nessun dispositivo (impostazione predefinita)
    - Personalizzato
7. Fare clic su **Fine**.

11. Criteri

I criteri consentono di definire i requisiti per i dispositivi, oltre alle situazioni che si verificano se un dispositivo non è conforme a tali requisiti. Ciascun criterio è composto da una regola e da un'azione di conformità (ciò che accade in caso di violazione della regola). Utilizzare la pagina **Criteri** per selezionare, configurare e distribuire i criteri.

> Con la procedura automatizzata di check-in dei dispositivi, tenere presenti le seguenti modifiche:

- Verranno valutati solo i dispositivi registrati negli ultimi 90 giorni.
- Solo il comando Check-in forzato verrà attivato sui dispositivi che sono stati registrati dopo 90 giorni e prima di un anno.
- Nessuna azione sui dispositivi che non sono stati registrati nell'ultimo anno.

Argomenti della sezione:

- **Utilizzo di policy**
- **Policy personalizzata**
- **Monitoraggio e controllo delle app consentite**
- **Assegnazione della priorità alle policy**
- **Policy Hardware Windows**

11.1. Utilizzo di policy

Argomenti della sezione:

- Implementazione di policy
- Azioni di conformità
- Ricerca di una policy esistente
- Aggiunta di una policy
- Modifica di una policy
- Eliminazione di una policy

Implementazione di policy

I criteri consentono di definire i requisiti per i dispositivi, oltre alle situazioni che si verificano se un dispositivo non è conforme a tali requisiti. Ciascun criterio è composto da una regola e da un'azione di conformità (ciò che accade in caso di violazione della regola). Utilizzare la pagina **Criteri** per selezionare, configurare e distribuire i criteri.

Sono disponibili i seguenti tipi di policy:

Tipo	Funzioni
Dispositivi compromessi	Priorità (1 = più elevata) Violazione 1 Plugin compromesso 2 Client manomesso 3 Produttore dispositivo sconosciuto: sconosciuto 4 Rilevata cartella sospetta: [percorso] 5 File binario sospetto trovato in: [percorso] 6 Cartella/dati sfogliabili O cartella /dati/dati sfogliabili 7 Trovato/sistema/app/Superuser.apk 8 Gestione pacchetto compromessa 9 Trovata app sospetta: [pacchetto] Segnala dispositivi che hanno subito jailbreak (iOS) o con root (Android). Per visualizzare la motivazione della violazione per cui il sistema ha segnalato un dispositivo Android come compromesso perché ne è stata violata la root: 1. Fare clic sulla scheda **Policy** 2. Fare clic sul collegamento **Dispositivi compromessi**. 3. Fare clic sulla scheda **Violazioni attive**. 4. Verificare la motivazione della violazione nella colonna Violazione. Per visualizzare la motivazione della violazione per cui il sistema ha segnalato un dispositivo Android come compromesso perché ne è stata violata la root: 5. Fare clic sulla scheda **Policy**. 6. Fare clic sul collegamento **Dispositivi compromessi**. 7. Fare clic sulla scheda **Violazioni attive**. 8. Verificare la motivazione della violazione nella colonna **Violazione**. Si tratterà di una delle motivazioni seguenti:
Protezione dei dati/Crittografia disabilitata (solo macOS)	Consente di contrassegnare i dispositivi macOS che non hanno un passcode o la crittografia abilitati.
Roaming internazionale MDM/Amministrazione dispositivo disattivata	Consente di contrassegnare i dispositivi ai quali potrebbero venire applicati dei costi per il roaming internazionale. Lo stato si aggiorna quando il dispositivo effettua il check-in. Per iOS, il servizio utilizza il contrassegno del roaming come impostato e segnalato da iOS. L'azione di conformità è azionata solo dalla prima violazione. Se l'MDM è disattivato sul dispositivo, allora questo non sarà esaminato per valutare eventuali altre policy o l'elaborazione delta di configurazioni o app durante i check-in.
Non in contatto	Contrassegna i dispositivi che non sono rimasti in contatto con Ivanti Neurons for MDM per l'intervallo di tempo specificato. Scegliere le azioni da intraprendere nel caso in cui il dispositivo non effettui il check-in da un numero di ore (da 2-3 a 23-24) o giorni specificato.

Tipo	Funzioni
Client MI Non in contatto (solo iOS)	Contrassegna i client Ivanti Neurons per MDM che non sono rimasti in contatto con Ivanti Neurons for MDM per l'intervallo di tempo specificato. Scegliere le azioni da intraprendere nel caso in cui il client non effettui il check-in da un numero di ore (da 2-3 a 23-24) o giorni specificato. Questa opzione si applica anche ai dispositivi registrati tramite iReg. La policy contrassegna il dispositivo come non conforme se non vi sono client o il client non effettua il check-in per un periodo definito di tempo.
App consentite	Consente di contrassegnare i dispositivi che violano le regole in base alle quali le app sono consentite o richieste.
Policy personalizzata	Consente di creare una policy personalizzata in base alle condizioni e alle azioni correlate specificate.

Azioni di conformità

Sono disponibili le seguenti azioni di conformità:

Azione di conformità	Funzioni
Esegui monitoraggio	Contrassegnare il dispositivo nella pagina Dispositivi di Ivanti Neurons for MDM. Di default, questa azione è attivata.
Blocca	Indica ad Access e/o Sentry di bloccare un dispositivo se questo tenta di accedere a una risorsa tramite Sentry o Access dopo che il criterio è stato violato negli ultimi dettagli di check-in.

Invia un messaggio all'utente	• Contrassegnare il dispositivo nella pagina Dispositivi di Ivanti Neurons for MDM.
	• Consente di inviare un'e-mail al proprietario del dispositivo.
	• Oltre ai criteri esistenti, il selettore "**Usa il modello di e-mail dei criteri di conformità**" è ora disponibile anche per i seguenti criteri:
	  ◦ Protezione dei dati/Crittografia disabilitata
	  ◦ Roaming internazionale
	  ◦ MDM/Amministrazione dispositivo disattivata
	  ◦ Non in contatto
	  ◦ Client MI Non in contatto
	  Consente di inviare una notifica push al dispositivo.

Quarantena	• Consente di rimuovere la maggior parte delle configurazioni dal dispositivo. ◦ Eccezioni: configurazioni del passcode, configurazioni Wi-Fi per i dispositivi solo Wi-Fi, configurazioni delle limitazioni (iOS). • Rimuove tutte le app installate da Ivanti Neurons for MDM. • Rimuove tutti i contenuti distribuiti da Ivanti Neurons for MDM, inclusi file iBook ed ePub. • Blocca l'accesso ai cataloghi Ivanti Neurons for MDM. • Consente di sospendere le richieste di installazione di app aggiuntive. • Blocca l'accesso alle app con abilitazione AppConnect. • Include il supporto per le app con abilitazione AppConnect. • Se abilitata, sospende le app personali sul lato personale del dispositivo in quarantena per indicare che l'utente del dispositivo deve risolvere i problemi di conformità sul dispositivo per renderlo funzionale. Supportato su dispositivi Android 11 o versione superiore forniti come Profilo di lavoro su dispositivo di proprietà dell'azienda.
Azioni di quarantena aggiuntive (facoltative):	**Blocca download nuove app** - Impedisce il download di qualsiasi nuova app nel dispositivo. **Applicazioni di quarantena gestite** - Rimuove dal dispositivo le app gestite da Ivanti Neurons for MDM e attiva l'opzione Blocca download nuove app per impedire che le app vengano reinstallate sul dispositivo. Selezionare una delle seguenti opzioni: • **Tutte le applicazioni** • **Rimuovi tutte le app tranne le seguenti** - Rimuove tutte le applicazioni tranne quelle che vengono aggiunte all'elenco delle applicazioni. • **Applicazioni designate**: consente di aggiungere una o più app manualmente (utilizzando l'ID bundle o il nome pacchetto) oppure eseguendo una ricerca. Fare clic sulla scheda **Visualizza app** per esaminare

Azione di conformità	Funzioni
	l'elenco delle app aggiunte. L'azione di quarantena Blocca accesso ad App Store non è più disponibile. In alcuni dispositivi l'azione di quarantena non rimuove l'applicazione dal dispositivo, a causa di specifiche limitazioni del dispositivo. Per impostazione predefinita, questa opzione è selezionata (per tutte e tre le opzioni: Tutte le applicazioni, Rimuovi tutte le app tranne le seguenti e Applicazioni designate) e non può essere deselezionata. Questo impedisce la reinstallazione delle app sul dispositivo. **Rimuovi configurazioni** - Rimuove le configurazioni di Ivanti Neurons for MDM dal dispositivo. Selezionare una delle seguenti opzioni: • **Tutte le configurazioni** • **Configurazioni designate** - Selezionare una o più configurazioni dall'elenco per ricercarle. Fare clic sulla scheda **Configurazioni selezionate** per esaminare l'elenco delle configurazioni selezionate. **Esegui push configurazioni designate** - Distribuisce le configurazioni designate nell'ambito della conformità personalizzata. Questo elenco contiene configurazioni che soddisfano i criteri seguenti: • Configurazione abilitata • Configurazione non di sistema • Configurazione isolabile in quarantena • Configurazioni create nello spazio corrente o delegate dallo spazio predefinito Per l'elenco delle configurazioni non isolabili in quarantena, vedere Configurazioni non isolabili in quarantena. **Rimuovi contenuto** - Rimuove dal dispositivo tutto il contenuto e i supporti associati alle app distribuite da Ivanti Neurons for MDM. **Sospendi app personali** - Sospende le app sul lato personale del dispositivo in quarantena per indicare che l'utente del dispositivo deve risolvere i problemi di conformità sul dispositivo per renderlo funzionale. Supportato su dispositivi Android 11 o versione superiore forniti come Profilo di lavoro su dispositivo di proprietà dell'azienda.

Ricerca di una policy esistente

È possibile utilizzare i filtri e la funzione di ricerca nella pagina Policy per trovare una o più policy esistenti.

Procedura

1. Andare a **Criteri**.
2. Per filtrare un elenco di policy che soddisfino determinati criteri, fare clic su **Filtri**.
3. Selezionare uno o più criteri di filtro.
4. Per cercare una policy esistente in base al nome, immettere il relativo nome nel campo **Cerca**.

Aggiunta di una policy

Procedura

1. Andare a **Criteri**.

2. Fare clic su +**Aggiungi** (in alto a destra).
3. Selezionare un tipo di criterio.
4. Completare le impostazioni.
5. Selezionare i gruppi di dispositivi che si desidera che ricevano questo criterio.

> È possibile distribuire al massimo 100 file di configurazione contemporaneamente.

6. Fare clic su **Fine**.

Modifica di una policy

Procedura

1. Andare a **Criteri**.
2. Per la policy necessaria, fare clic sull'icona (matita) **Modifica** sotto la colonna Azioni.
3. Apportare le modifiche desiderate.
4. Salvare le modifiche.

Eliminazione di una policy

Procedura

1. Andare a **Criteri**.
2. Per la policy necessaria, fare clic sull'icona **Rimuovi** sotto la colonna Azioni.
3. Fare clic su **Sì** per confermare.

Se non è possibile visualizzare la pagina Policy, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione dispositivi
- Dispositivo di sola lettura

Per ulteriori informazioni, vedere **Definire le priorità delle policy**.

11.2. Policy personalizzata

Criteri

Licenza: Platinum

Dispositivi idonei: Android, iOS, MacOS e Windows.

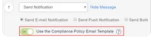
Consente di creare una policy personalizzata in base agli attributi dei dispositivi e degli utenti, ai criteri di selezione, ai valori e alle azioni di conformità specificate.

> Anche l'impostazione Livello di patch di sicurezza Android può essere utilizzata per definire una policy personalizzata.

Aggiunta di una policy personalizzata

1. Andare a **Criteri**.
2. Fare clic su **+ Aggiungi**.
3. Selezionare **Criterio personalizzato**.
4. Assegnare un nome al criterio personalizzato.
5. Fare clic su **+ Aggiungi descrizione** per inserire ulteriori dettagli, se lo si desidera.
6. Utilizzare il Generatore di regole per definire le condizioni che attivano le azioni considerate vere. Vedere **Comprensione delle impostazioni delle condizioni** per istruzioni sulla creazione delle condizioni. L'amministratore di Ivanti Neurons for MDM visualizza il numero di gruppi di utenti duplicati e il numero corrispondente di GUID per identificare gruppi duplicati quando si seleziona l'attributo Nome gruppo di utenti nel Generatore di regole. Inoltre, una tabella sotto questa regola visualizza l'elenco di gruppi di utenti duplicati e i relativi dettagli, ad esempio Nome gruppo di utenti, GUID, Origine e Nome distinto (DN).
7. Selezionare una delle azioni di conformità (vedere di seguito Azioni predefinite) da eseguire quando sono soddisfatte le condizioni specificate. L'aggiunta dell'azione "**Attendi**" fra un'azione e l'altra permette agli utenti dei dispositivi di correggere il dispositivo in uso e di ripristinarne la conformità prima di intraprendere ulteriori azioni. Ad esempio, è possibile inviare un messaggio di avviso e attendere 24 ore prima di applicare un'azione di quarantena.
8. Selezionare l'opzione **Inviare una notifica quando il dispositivo è di nuovo conforme**, che è deselezionata per impostazione predefinita.

- **Invia notifica e-mail** - Invia un'e-mail all'indirizzo e-mail dell'utente del dispositivo, per avvisarlo che è di nuovo conforme.
  - Attivare l'opzione **Usa modello e-mail sulle policy di conformità** per inserire il messaggio configurato qui nel modello e-mail di notifica delle policy come descritto in **Personalizzazione di un modello e-mail** in **Personalizzazione dei modelli e-mail**. Per una panoramica, consultare la sezione **Configurazione e utilizzo di e-mail di notifica sulla conformità delle policy**.



  - È possibile personalizzare i messaggi includendo variabili di sostituzione facoltative per fornire ai destinatari maggiori dettagli sulle violazioni della policy e altre informazioni rilevanti. Fare clic sui tipi di attributo seguenti per visualizzare l'elenco completo di variabili:
    - Attributi policy, inclusi $, $ e $.
    - Attributi utente, inclusi $, $ e $.
    - Attributi dispositivo, inclusi $, $ e $.
    - Attributi LDAP/utente/dispositivo personalizzati, creati dalla pagina **Amministratore > Attributi**.

- **Invia notifica push** - Invia una notifica push al dispositivo quando il dispositivo è di nuovo conforme.
- **Invia entrambe** - Invia una notifica push al dispositivo e un'e-mail all'indirizzo dell'utente del dispositivo per avvisarlo che il dispositivo è di nuovo conforme. È possibile personalizzare i messaggi includendo variabili di sostituzione facoltative per fornire ai destinatari maggiori dettagli come descritto in precedenza per l'azione Invia e-mail.

9. Specificare le seguenti opzioni dalla tabella per notificare agli amministratori e ai proprietari dei dispositivi registrati se questi ultimi violano le regole del criterio:

Opzione	Descrizione
Oggetto	Inserire il testo dell'oggetto. Ad esempio, "Hai violato una politica!".
Corpo	Inserire il messaggio come necessario. Ad esempio, "Azione necessaria!".
Invia notifica e-mail solo agli amministratori	Selezionare questa opzione per inviare notifiche e-mail solo agli amministratori.
CC agli amministratori	Questa casella di testo non sarà disponibile se è stata selezionata l'opzione "Invia notifica e-mail solo agli amministratori".
Immettere gli indirizzi e-mail degli amministratori	Inserire l'ID e-mail degli amministratori. Utilizzare un punto e virgola (;) come separatore per aggiungere più indirizzi e-mail.
Anteprima e-mail	Fare clic sul pulsante **Anteprima e-mail** per visualizzare l'indirizzo e-mail.

10. Fare clic su **Avanti** per salvare i dettagli della policy.

Azioni predefinite:

1. Fare clic sulla casella di controllo **Sì** per dichiarare che si comprende che, se questa policy è stata attivata in precedenza su un dispositivo, aggiungendo la policy a livelli verranno ripristinate le policy e tutte le azioni di conformità applicate in precedenza. La nuova policy personalizzata diventerà effettiva al successivo check-in del dispositivo. Se si è selezionata l'azione Dismetti, fare clic su **Sì** per dichiarare che si comprende che non è possibile annullare l'azione.

- **Monitor** - Attualmente è sempre selezionata. Con Sentry 9.0.0 o versioni successive è richiesto l'utilizzo delle azioni di conformità a livelli.
- **Nessuna azione**
- **Invia notifica**
- **Invia e-mail** - Consente di inviare un'e-mail all'indirizzo dell'utente del dispositivo, per avvisarlo che il dispositivo non è conforme.
  - È possibile utilizzare il modello e-mail di notifica delle policy come descritto in precedenza.
  - È possibile personalizzare i messaggi includendo variabili di sostituzione facoltative per fornire ai destinatari maggiori dettagli sulle violazioni della policy e altre informazioni rilevanti. Ciò fornisce agli utenti dei dispositivi non conformi informazioni rilevanti sulla violazione dei criteri, in modo che possano intraprendere azioni correttive. Fare clic sui tipi di attributo seguenti per visualizzare l'elenco completo di variabili:
    - Attributi policy, inclusi $, $ e $.
    - Attributi utente, inclusi $, $ e $.
    - Attributi dispositivo, inclusi $, $ e $.
    - Attributi LDAP/utente/dispositivo personalizzati, creati dalla pagina **Amministratore > Attributi**.

- **Invia notifica push**: invia una notifica push al dispositivo non conforme.
- **Invia entrambi** - Consente di inviare una notifica push al dispositivo e un'e-mail all'indirizzo dell'utente del dispositivo per avvisarlo che il dispositivo non è conforme. È possibile personalizzare i messaggi includendo variabili di sostituzione facoltative per fornire ai destinatari maggiori dettagli come descritto in precedenza per l'azione Invia e-mail.
- **Blocca** - Utilizza Sentry per impedire ai dispositivi gestiti di accedere alle e-mail e alle applicazioni con abilitazione AppConnect. Sentry 9.0.0 o versione successiva richiede l'utilizzo dell'azione di blocco.
- **Dismetti**: consente di dismettere il dispositivo. **Questa azione non può essere annullata**. Ad esempio, può essere impostata una regola per dismettere i dispositivi per tutti gli utenti disattivati utilizzando la condizione Utente abilitato.
- **Attendi**: ritarda l'azione per un periodo di tempo specificato (ore o giorni), in modo da consentire agli utenti di correggere la violazione prima che vengano intraprese altre azioni se il dispositivo rimane in uno stato di non conformità.
- **Quarantena**: rimuove l'accesso ad app, contenuti e server secondo le seguenti azioni:

Azioni di quarantena aggiuntive (facoltative)	Descrizione
Applicazioni gestite in quarantena	Rimuove dal dispositivo tutte le app gestite da Ivanti Neurons for MDM e attiva l'opzione Blocca nuovi download delle app per impedire che le app vengano reinstallate nel dispositivo. Selezionare una delle seguenti opzioni: • **Tutte le applicazioni** • **Applicazioni designate**: consente di aggiungere una o più app manualmente (utilizzando l'ID bundle o il nome pacchetto) oppure eseguendo una ricerca. Fare clic sulla scheda **Visualizza app** per esaminare l'elenco delle app aggiunte. L'azione di quarantena Blocca accesso ad App Store non è più disponibile. In alcuni dispositivi l'azione di quarantena non rimuove l'applicazione dal dispositivo, a causa di specifiche limitazioni del dispositivo.
Blocca nuovi download delle app	Impedisce il download di qualsiasi nuova app nel dispositivo. Selezionare una delle seguenti opzioni: • **Tutte le applicazioni** • **Applicazioni designate**: consente di aggiungere una o più app manualmente (utilizzando l'ID bundle o il nome pacchetto) oppure eseguendo una ricerca. Fare clic sulla scheda **Visualizza app** per esaminare l'elenco delle app aggiunte. L'azione di quarantena Blocca accesso ad App Store non è più disponibile. Questa opzione è selezionata per impostazione predefinita (sia per Tutte le applicazioni, sia per Applicazioni designate) e non può essere deselezionata. Questo impedisce la reinstallazione delle app sul dispositivo.
Rimuovi configurazioni	Consente di rimuovere le configurazioni di Ivanti Neurons for MDM dal dispositivo. Selezionare una delle seguenti opzioni: • **Tutte le configurazioni** • **Configurazioni designate** - Selezionare una o più configurazioni dall'elenco per ricercarle. Fare clic sulla scheda **Configurazioni selezionate** per esaminare l'elenco delle configurazioni selezionate.
Invia configurazioni designate	Distribuisce le configurazioni designate nell'ambito della conformità personalizzata. Questo elenco contiene configurazioni che soddisfano i criteri seguenti: • Configurazione abilitata • Configurazione non di sistema • Configurazione isolabile in quarantena • Configurazioni create nello spazio corrente o delegate dallo spazio predefinito Per l'elenco delle configurazioni non isolabili in quarantena, vedere **Configurazioni non isolabili in quarantena.** Per ulteriori informazioni, vedere la sezione **Invio di una configurazione designata** dopo questa procedura.
Rimuovi contenuto	Rimuove dal dispositivo tutto il contenuto e i supporti associati alle app distribuite da Ivanti Neurons for MDM.

Azioni di quarantena aggiuntive (facoltative)	Descrizione
Sospendere app personali	Sospende le app sul lato personale del dispositivo in quarantena per indicare che l'utente del dispositivo deve risolvere i problemi di conformità sul dispositivo per renderlo funzionale. Supportato su dispositivi Android 11 o versione superiore forniti come Profilo di lavoro su dispositivo di proprietà dell'azienda.
Azioni di quarantena predefinite - queste azioni vengono eseguite sempre.	
Blocca accesso ad app Store	Impedisce al dispositivo di accedere agli app store tramite Ivanti Neurons for MDM.
Blocca accesso a Store contenuto	Impedisce al dispositivo di accedere allo Store del contenuto tramite Ivanti Neurons for MDM.
Blocca AppConnect	Impedisce al dispositivo di utilizzare le funzioni di AppConnect.
Blocca AppTunnel	Impedisce alle applicazioni sul dispositivo di accedere al contenuto e ai server tramite AppTunnel.
Blocca ActiveSync	Impedisce al dispositivo di accedere alle e-mail tramite il server ActiveSync.

2. Fare clic su **Avanti** per configurare i dispositivi ai quali verranno applicate le policy e le azioni.
3. Fare clic su **Fine**.

La tabella seguente illustra il comportamento di quarantena su vari dispositivi Android quando l'azione di quarantena viene avviata da Ivanti Neurons per MDM:

Dispositivi	Comportamento di quarantena
Dispositivi Samsung in modalità Amministratore del dispositivo tramite l'app client Go	• Disinstalla sia le app pubbliche gestite che quelle interne • Rimuove determinati profili (tranne Mobile Threat Defense e altri)
Dispositivi non Samsung in modalità Amministratore del dispositivo tramite l'app client Go MAM tramite l'app AppStation	• Non è possibile disinstallare o nascondere le app pubbliche gestite né quelle interne • Rimuove determinati profili (tranne Mobile Threat Defense e altri)
Android Enterprise tramite l'app client Go	• Nasconde sia le app pubbliche gestite che quelle interne • Rimuove determinati profili (tranne Mobile Threat Defense e altri)

Invio di una configurazione designata

Distribuisce le configurazioni designate nell'ambito della conformità personalizzata. Configurare la policy personalizzata in modo da distribuire un determinato set di configurazioni quando un dispositivo risulta non conforme. Reimposta lo stato precedente del dispositivo nell'ambito dell'azione correttiva eseguita per riportarlo dallo stato non conforme allo stato conforme.

> Si verifica un errore quando un amministratore tenta di delegare una policy personalizzata che include configurazioni non delegate nella scheda Invia configurazioni designate.

Di seguito sono elencati i comportamenti che si verificano quando le configurazioni vengono inviate tramite policy personalizzate in determinate condizioni.

Condizioni	Comportamento
Sono selezionate due configurazioni dello stesso tipo che hanno la priorità impostata	Al dispositivo viene inviata la configurazione con la massima priorità.
Sono selezionate due configurazioni dello stesso tipo per cui non è impostata alcuna priorità	Entrambe le configurazioni verranno inviate al dispositivo. Può dare luogo a comportamenti inaspettati.
Quando un dispositivo ha già una configurazione dello stesso tipo che supporta la priorità definita nella Policy personalizzata	Ha la precedenza la configurazione definita nella policy personalizzata, che viene inviata al dispositivo. La configurazione presente sul dispositivo viene rimossa indipendentemente dalla priorità (anche se tale priorità è più alta di quella definita nella policy personalizzata).
Quando un dispositivo ha già una configurazione dello stesso tipo che non supporta la priorità definita nella policy personalizzata	Al dispositivo viene inviata la configurazione definita nella policy personalizzata. Entrambe le configurazioni saranno presenti sul dispositivo. Può dare luogo a comportamenti inaspettati.
Se la priorità di una configurazione è cambiata dopo la creazione della Policy personalizzata	Al check-in del dispositivo, la configurazione con la priorità più alta sarà inviata se fa parte della Policy personalizzata.
Quando entrambe le condizioni sono soddisfatte: • Condizione A: quando a un dispositivo con una violazione è stata inviata una configurazione nell'ambito di una policy personalizzata (e tale configurazione ha avuto la precedenza rispetto a una configurazione dello stesso tipo già presente sul dispositivo). • Condizione B: la violazione è stata corretta e il dispositivo non è più in quarantena.	La configurazione definita nella Policy personalizzata sarà rimossa e quella dello stesso tipo presente nel dispositivo prima della quarantena sarà inviata tramite l'applicazione di gruppi di dispositivi esistenti, riportando il dispositivo al suo stato originale.

Nell'azione di quarantena, se si seleziona Rimuovi configurazioni insieme a Invia configurazioni designate, valgono le regole seguenti:

- Rimuovi tutte le configurazioni + Invia configurazioni designate: in questo scenario, tutte le configurazioni del dispositivo vengono rimosse e le configurazioni selezionate nella scheda Invia configurazioni designate vengono inviate al dispositivo.
- Rimuovere le configurazioni designate (in un criterio personalizzato) + Eseguire il push delle configurazioni designate (in un altro criterio personalizzato) con una configurazione comune nella selezione di entrambe: Poiché le configurazioni sono selezionate in due diversi criteri di conformità, verrebbe adottato l'approccio più restrittivo, cioè la configurazione (o le configurazioni) saranno rimosse dal dispositivo.

È possibile delegare una policy personalizzata dallo **spazio** predefinito a uno spazio personalizzato. È possibile delegare una policy personalizzata solo se le configurazioni menzionate nella scheda Invia configurazioni designate della policy personalizzata sono state delegate agli spazi.

Nella pagina **Dispositivi**, è possibile fare clic sul nome del dispositivo per accedere alla relativa pagina dei dettagli. Nella scheda Configurazioni, la colonna Metodo di distribuzione indica il metodo di distribuzione utilizzato per una configurazione inviata al dispositivo, che può essere "Gruppo di dispositivi" o "Azione di conformità".

Nella pagina Configurazioni, per ciascuna configurazione Ivanti Neurons per MDM mostra il numero dei dispositivi che hanno ricevuto la configurazione tramite un gruppo di dispositivi e quelle che l'hanno ricevuta tramite un'azione di conformità.

Comprensione delle impostazioni delle condizioni

Nella tabella seguente sono descritti alcuni dei campi disponibili per la generazione delle regole:

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
Supporto APNS	Il valore di questo campo indica se il dispositivo supporta APNS.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	iOS/macOS/ Android
Stato nativo anti-phishing	Questo campo visualizza lo stato nativo anti-phishing	Gli operatori possibili sono: • è uguale a • non è uguale a Valori possibili sono: • Non abilitato • N/A • Attivato • Sconosciuto	iOS/Android
Stato anti-phishing	Questo campo visualizza lo stato anti-phishing	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono: • Non abilitato • N/A • Attivato • Sconosciuto	iOS/Android
Stato VPN anti-phishing	Questo campo visualizza lo stato VPN anti-phishing	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono: • Non abilitato • N/A • Attivato • Sconosciuto	iOS/Android
Informazioni batteria	Questo campo ha i seguenti attributi: • Livello batteria - Visualizza il livello di carica della batteria corrente come segnalato dal sistema operativo Android	Per informazioni sui valori possibili, vedere **Utilizzo della ricerca avanzata**.	Android

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
	• Stato integrità batteria - Come segnalato dal sistema operativo Android • Stato carica batteria - Come segnalato dal sistema operativo Android • Percentuale integrità batteria (specifico per OEM) - Integrità batteria in percentuale per i produttori di dispositivi supportati come i dispositivi Zebra • Data di produzione batteria (OEM) - Dat di produzione della batteria per i produttori di dispositivi supportati come i dispositivi Zebra • Cicli di carica della batteria (OEM) - Numero di cicli completati in totale per i produttori di dispositivi supportati come i dispositivi Zebra		
Stato di integrità banda base	Questo campo indica lo stato di integrità della banda base del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono OK o Errore.	Dispositivi supervisionati iOS 27.0+
Token bootstrap disponibile	Il valore di questo campo indica se è disponibile un token bootstrap per un dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	macOS
Registrato come Autopilot	Questo campo indica se il dispositivo è registrato o meno per Autopilot.	• è uguale a • non è uguale a I valori possibili sono Sì e No.	Windows
Ultimo check-in bridge	Questo campo indica l'orario dell'ultimo check-in bridge del client.	Gli operatori possibili sono: • è inferiore a • è inferiore o uguale a • è superiore a	Windows

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
		• è superiore o uguale a • è compreso nell'intervallo • non è compreso nell'intervallo Inserire il valore numerico dell'orario dell'ultimo check-in bridge. Selezionare una delle seguenti opzioni per la durata: • ore • giorni Esempio: l'ultimo check-in bridge risale a meno di 12 ore fa.	
Stato integrità videocamera	Questo campo indica lo stato di integrità della videocamera del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono: • OK • Errore • Non originale (se non è un componente Apple originale)	Dispositivi supervisionati iOS 27.0+
Ultimo check-in del client	Questo campo indica l'orario dell'ultimo check-in del client.	Gli operatori possibili sono: • è inferiore a • è superiore a Inserire il valore numerico dell'orario dell'ultimo check-in. Selezionare una delle seguenti opzioni per la durata: • ore • giorni Esempio: l'ultimo check-in del client risale a meno di 12 ore fa.	iOS/macOS/ Android
Client registrato	Questo campo indica lo stato del client registrato.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	iOS/macOS/ Android
Compromesso	Il valore di questo campo indica se il dispositivo è sottoposto a root/compromesso.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono: • soggetto a jailbreak o a rooting	iOS/Android

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
		• non compromesso	
Nome paese attuale	Questo campo indica il nome del paese corrente, che corrisponde al Mobile Country Code (MCC) o al Mobile Network Code (MNC) a cui risulta attualmente connesso il dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a Il valore possibile è una voce di un elenco a discesa, che indica il nome del paese principale.	iOS/macOS/ Android
MCC attuale	Questo campo indica il Mobile Country Code (MCC) attuale	Immettere il valore dell'attributo da verificare. Gli operatori possibili sono: • è uguale a • non è uguale a	iOS/macOS/ Android
MNC attuale	Questo campo indica il Mobile Network Code (MNC) attuale	Immettere il valore dell'attributo da verificare. Gli operatori possibili sono: • è uguale a • non è uguale a	iOS/macOS/ Android
Attributo dispositivo personalizzato	Questo campo consente di aggiungere un attributo dispositivo personalizzato esistente come condizione di una regola per verificarne il valore.	Immettere il valore dell'attributo da verificare. Gli operatori possibili sono: • è uguale a • non è uguale a • contiene • non contiene Il valore può essere una stringa di caratteri ASCII, inclusi spazi e caratteri Unicode.	iOS/macOS/ Android/Windows
Attributo LDAP personalizzato	Questo campo consente di aggiungere un attributo LDAP personalizzato esistente come condizione di una regola per verificarne il valore.	Immettere il valore dell'attributo da verificare. Gli operatori possibili sono: • è uguale a • non è uguale a • contiene • non contiene Il valore può essere una stringa di caratteri ASCII, inclusi spazi e caratteri Unicode.	iOS/macOS/ Android/Windows
Attributo utente personalizzato	Questo campo consente di aggiungere un attributo utente personalizzato esistente come condizione di una regola per verificarne il valore.	Immettere il valore dell'attributo da verificare. Gli operatori possibili sono: • è uguale a • non è uguale a • contiene	iOS/macOS/ Android/Windows

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
		• non contiene Il valore può essere una stringa di caratteri ASCII, inclusi spazi e caratteri Unicode.	
Roaming dati	Questo campo attiva il roaming dati da utilizzare come condizione di una regola per verificarne il valore.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No. Il valore predefinito è No se il dispositivo supportato non indica informazioni relative a questo campo.	iOS/Android
Tipo di dispositivo	Il valore di questo campo indica il modello del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a • inizia con • termina con È possibile specificare valori di testo.	iOS/macOS/ Android/Windows
Tipo di dispositivo (Apple)	Questo campo rappresenta il nome descrittivo del modello del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a • inizia con • termina con È possibile specificare valori di testo.	iOS/macOS
Visualizza stato di integrità	Questo campo indica lo stato di integrità del display del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono: • OK • Errore • Non originale (se non è un componente Apple originale)	Dispositivi supervisionati iOS 27.0+
Crittografia abilitata	Il valore di questo campo determina se il dispositivo è abilitato per la protezione dei dati/crittografia.	Sì - il dispositivo è abilitato per la protezione dei dati/crittografia. No - il dispositivo non è abilitato per la protezione dei dati/crittografia.	iOS/Android/ Windows
GUID	Questo campo indica il GUID del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a	iOS/macOS/ Android/Windows

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
		• inizia con • termina con	
Stato integrità Face ID	Questo campo indica lo stato di integrità Face ID del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono OK o Errore.	Dispositivi supervisionati iOS 27.0+
Nome paese principale	Questo campo indica il nome del paese principale, che corrisponde al Mobile Country Code (MCC) o al Mobile Network Code (MNC) programmato nella SIM o nella eSIM del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a Il valore possibile è una voce di un elenco a discesa, che indica il nome del paese principale.	iOS/Android/Windows
Windows Update non riuscito	Questo campo indica se il dispositivo non è conforme alle regole per gli aggiornamenti più recenti.	Sì: il dispositivo non è conforme all'ultimo aggiornamento. No: il dispositivo è conforme all'ultimo aggiornamento.	Windows
MCC nazionale	Questo campo indica il MobileCountry Code (MCC).	Immettere il valore dell'attributo da verificare. Gli operatori possibili sono: • è uguale a • non è uguale a	iOS/macOS/Android
MNC nazionale	Questo campo indica il MobileNetwork Code (MNC)	Immettere il valore dell'attributo da verificare. Gli operatori possibili sono: • è uguale a • non è uguale a	iOS/macOS/Android
IMEI	Questo campo indica il numero IMEI del primo slot SIM.	Gli operatori possibili sono: • è uguale a • non è uguale a • inizia con • termina con	iOS/Android/Windows
IMEI2	Questo campo indica il numero IMEI del secondo slot SIM.	Gli operatori possibili sono: • è uguale a • non è uguale a • inizia con • termina con	Android
IMSI	Questo campo indica il numero IMSI della SIM card.	Gli operatori possibili sono: • è uguale a	Android/Windows

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
		• non è uguale a • inizia con • termina con	
Chiave recupero istituzionale abilitata	Questo campo indica se la chiave di recupero istituzionale è abilitata o meno sul dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a	macOS
Ultimo check-in	Questo campo consente di impostare le condizioni correlate all'orario dell'ultimo check-in del dispositivo gestito tramite il canale MDM.	Gli operatori possibili sono: • è inferiore a • è superiore a • è vuoto Inserire il valore numerico dell'orario dell'ultimo check-in. Selezionare una delle seguenti opzioni per la durata: • ore • giorni Esempio: l'ultimo check-in risale a più di 12 ore fa.	iOS/macOS/Android/Windows
ID ultimo hotfix	Questo campo consente di impostare le condizioni relative all'ID dell'ultimo hotfix.	Gli operatori possibili sono: • è uguale a • non è uguale a • è inferiore a • è inferiore o uguale a • è superiore a • è superiore o uguale a • contiene • non contiene • inizia con • non inizia con • termina con • non termina con	Windows
Data installazione ultimo hotfix	Questo campo permette di impostare le condizioni relative all'ultimo hotfix installato.	Gli operatori possibili sono: • è inferiore a • è superiore a	Windows

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
Servizio di localizzazione abilitato	Il valore di questo campo indica se il dispositivo dispone di un servizio di localizzazione dei dispositivi (ad esempio, Trova il mio iPhone) abilitato.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	iOS
Produttore	Questo campo consente di impostare le condizioni relative al produttore del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono: • Samsung • NOKIA • HTC • LGE • Apple Inc	iOS/macOS/Android/Windows
Stato attivazione MTD	Questo campo rappresenta lo stato di attivazione MTD	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono: • N/A • Errore • In sospeso • Protetto	iOS/Android
Gestito da MDM	Il valore di questo campo determina se il dispositivo è abilitato per Gestione dispositivi mobili/amministratore dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	iOS/macOS/Android
Tipo di registrazione MDM	Questo campo indica il tipo di registrazione del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono: • Utente • Dispositivo • Supervisionato • Nessuno	iOS 27.0+, macOS 27.0+, tvOS 27.0+, visionOS 27.0+ e watchOS 27.0+
Torna al servizio	Questo campo indica lo stato del dispositivo per il ritorno al servizio	Gli operatori possibili sono: • è uguale a	iOS 27.0+ e visionOS

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
MDM	MDM con la conservazione dell'app.	• non è uguale a I valori possibili sono Vero o Falso.	27.0+
Modalità multiutente	Questo campo indica se il dispositivo (iPad) utilizza la modalità multiutente.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	iOS 27.0+
Stato di integrità vicino al campo	Questo campo indica lo stato di integrità NFC del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono OK o Errore.	Dispositivi supervisionati iOS 27.0+
Sistema operativo	Il valore di questo campo indica il tipo di sistema operativo del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono: • macOS • Android • iOS • Windows • visionOS	iOS/macOS/visionOS/Android/Windows
Versione build sistema operativo	Il valore di questo campo indica la versione build del sistema operativo del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a • è inferiore a • è inferiore o uguale a • è superiore a • è superiore o uguale a • contiene • non contiene • inizia con • non inizia con • non è vuoto • è vuoto • termina con • non termina con	iOS/macOS/visionOS/Android/Windows

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
Versione SO	Il valore di questo campo indica la versione del sistema operativo del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a • è inferiore a • è inferiore o uguale a • è superiore a • è superiore o uguale a • è compreso nell'intervallo • non è compreso nell'intervallo È possibile specificare un valore di testo.	iOS/macOS/visionOS/Android/Windows
Sistema operativo con versione	Questo campo rappresenta il sistema operativo e la relativa versione del dispositivo	Gli operatori possibili sono: • è uguale a • non è uguale a • è inferiore a • è inferiore o uguale a • è superiore a • è superiore o uguale a • è compreso nell'intervallo • non è compreso nell'intervallo È possibile specificare un valore di testo.	iOS/macOS/visionOS/Android/Windows
Proprietà	Il valore di questo campo indica il tipo di proprietà del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono: • di proprietà dell'utente • non impostata • di proprietà dell'azienda	iOS/macOS/Android/Windows
Chiave di recupero personale abilitata	Questo campo indica se la chiave di recupero personale è abilitata o meno.	Gli operatori possibili sono: • è uguale a • non è uguale a	macOS
Passcode conforme con i profili	Il valore di questo campo indica se il passcode del dispositivo è conforme ai profili.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	iOS/macOS/Android

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
Hotspot personale abilitato	Il valore di questo campo indica se la funzione Hotspot personale è abilitata sul dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No. L'impostazione Hotspot personale è disponibile solo per alcuni gestori telefonici.	iOS
N. di telefono	Questo campo indica il numero di telefono del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a • contiene • inizia con • termina con	iOS/Android/Windows
Indirizzo IP pubblico	Questo campo indica l'indirizzo IP pubblico. Se il dispositivo utilizza una connessione VPN o un server proxy per collegarsi a Ivanti Neurons per MDM, mostra l'indirizzo IP WAN del proxy.	Gli operatori possibili sono: • è compreso nell'intervallo • non è compreso nell'intervallo • non è vuoto • è vuoto	Android/ChromeOS
Roaming	Il valore di questo campo indica lo stato del roaming del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	iOS/Android/Windows
Modalità blocco sicurezza	Questo campo indica se la modalità di blocco è abilitata o disabilitata per un dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Vero o Falso.	iOS 27.0+ e macOS 27.0+
Sentry bloccato	Indica se il dispositivo è bloccato da Sentry.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	iOS/macOS/Android/Windows
Stato	Questo campo indica lo stato della registrazione.	Gli operatori possibili sono: • è uguale a • non è uguale a Il possibile valore predefinito è "Attiva". Nei criteri personalizzati, limita lo stato del dispositivo ad Attivo, rimuovendo tutti gli altri valori potenziali,	iOS/macOS/Android

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
		poiché la valutazione dei criteri avviene quando il dispositivo effettua il check-in per gli stati Attivo, In attesa di ritiro e In attesa di cancellazione, e questi dispositivi avranno i loro criteri valutati al momento del check-in.	
Numero di serie	Questo campo indica il numero di serie del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a • inizia con • termina con	iOS/macOS/ Android/Windows
Supervisionato	Il valore di questo campo indica se il dispositivo è supervisionato.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	iOS/macOS
Versione di build supplementare	Questo campo rappresenta la versione di build supplementare del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a • è inferiore a • è inferiore o uguale a • è superiore a • è superiore o uguale a • contiene • non contiene • inizia con • non inizia con • termina con • non termina con • non è vuoto • è vuoto	iOS/macOS
Sistema operativo /Versione supplementare Extra	Questo campo rappresenta la versione di build del sistema operativo supplementare del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a • è inferiore a • è inferiore o uguale a • è superiore a	iOS/macOS

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
		• è superiore o uguale a • contiene • non contiene • inizia con • non inizia con • termina con • non termina con • non è vuoto • è vuoto	
Toccare stato integrità ID	Questo campo indica lo stato di integrità Touch ID del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono: • OK • Errore • N/D (se è un iPhone)	Dispositivi supervisionati iOS 27.0+
Utente abilitato	Il valore di questo campo indica se l'utente è abilitato.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	iOS/macOS/Android/Windows
Gruppo di utenti	Questo campo rappresenta il gruppo di utenti.	Gli operatori possibili sono: • è uguale a • non è uguale a	iOS/macOS/Android/Windows
Stato di integrità banda ultra larga	Questo campo indica lo stato di integrità banda ultra larga del dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono OK o Errore.	Dispositivi supervisionati iOS 27.0+
Chiamate in roaming	Il valore di questo campo indica se le chiamate in roaming sono abilitate sul dispositivo.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No. L'impostazione per le chiamate in roaming è disponibile solo per alcuni gestori telefonici. La disattivazione delle chiamate in roaming comporta anche la disattivazione del roaming dati. Il valore predefinito è "non è uguale a" se il dispositivo	iOS

Campo UI	Descrizione	Valori possibili	Piattaforme supportate
		supportato non indica informazioni relative a questo campo.	
Accesso bloccato	Indica se il dispositivo è bloccato da Access.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	iOS/macOS/ Android/Windows
Conformità	Indica se il dispositivo è conforme o meno.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Conformità e Non conformità.	iOS/macOS/ Android/Windows
Azione di conformità bloccata	Indica se il dispositivo è bloccato o meno.	Gli operatori possibili sono: • è uguale a • non è uguale a I valori possibili sono Sì e No.	iOS/macOS/ Android/Windows

Configurazioni non isolabili in quarantena

Nella tabella seguente sono elencate le configurazioni non isolabili in quarantena:

Sistema operativo	Configurazioni non isolabili in quarantena
Android	• Catalogo app Android • Cifratura Android • Versione aziendale di Android • App Android Enterprise • Android Zebra • Protezione anti-phishing • Richiesta di verifica di Android Work • Passcode dispositivo • Download dei file • Blocco e tutto schermo: modalità di amministrazione del dispositivo Android • Blocco e tutto schermo: Samsung Knox Standard • Solo MAM • Dispositivo gestito con Profilo di lavoro/Profilo di lavoro su dispositivo di proprietà dell'azienda • Dispositivi di lavoro gestito (proprietario del dispositivo) • Restrizioni telefoni Samsung • Attestazione SafetyNet • Profilo di lavoro su dispositivo di proprietà dell'azienda
iOS e macOS	• Protezione anti-phishing (iOS) • Notifiche app (iOS) • Siti AppStation (iOS) • Chiave di ripristino FileVault (macOS) • FileVault 2 (macOS) • Proxy globale (iOS e tvOS) • Layout schermata iniziale (iOS e tvOS) • Controllo app iOS • Restrizioni iOS • Aggiornamenti software iOS (iOS) • Firewall macOS • Aggiornamenti software macOS • Solo MAM (iOS) • Privacy MI client (iOS/macOS) • Uso della rete (iOS) • Creazione account Office 365 (macOS) • Modalità app singola (iOS e tvOS) • Controllo policy di sistema (macOS)

Sistema operativo	Configurazioni non isolabili in quarantena
	• Gestito da policy di sistema (macOS) • Opzioni Regola policy di sistema (macOS) • Server di riferimento orario (macOS) • Filtro contenuto Web (iOS)
Windows	• Controllo dell'app di Windows • Restrizioni di Windows DDF (Data Definition File) • Windows Firewall • Proxy di rete Windows • Restrizioni di Windows • Aggiornamenti di Windows
Tutti	• Active Directory • Servizi client • Gestione dei dispositivi mobili • Attivazione Mobile Threat Defense • Azioni locali Mobile Threat Defense • Passcode • Privacy • Informativa sulla privacy • ServiceConnect • Sincronizza

Se non è possibile visualizzare la pagina Policy, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione dispositivi
- Dispositivo di sola lettura

11.3. Monitoraggio e controllo delle app consentite

Licenza: Silver

Per controllare le app installate sui dispositivi, creare un criterio App consentite. Questa policy supporta anche le app macOS interne di MobileIron Packager (MIP). Il criterio contiene le seguenti informazioni:

- {{app consentite}}
- {{app non consentite}}
- {{app richieste}}
- {{azioni di conformità}}

Se un'app si trova sia tra le app richieste sia tra quelle non consentite, viene data la priorità alla valutazione dell'app rispetto all'elenco delle app richieste. Ad esempio, se l'app A1 è presente sia nell'elenco delle app richieste sia in quello delle app non consentite, la valutazione della policy delle app per questo dispositivo avviene come segue:

- Se A1 è installata sul dispositivo, il dispositivo è conforme.
- Se A1 non è installata sul dispositivo, il dispositivo non è conforme.

Dispositivi supportati

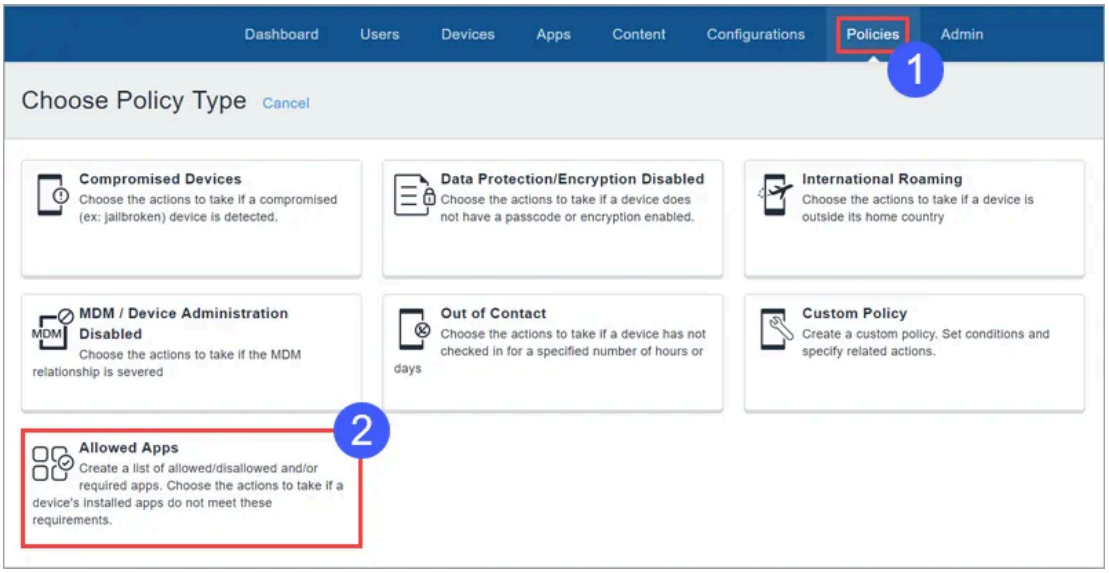
- Android 4.2 o versioni più recenti supportate
- iOS 8.0 o versioni più recenti supportate
- macOS 10.12 o versioni più recenti supportate
- Windows 10 o versioni successive supportate

Prerequisiti

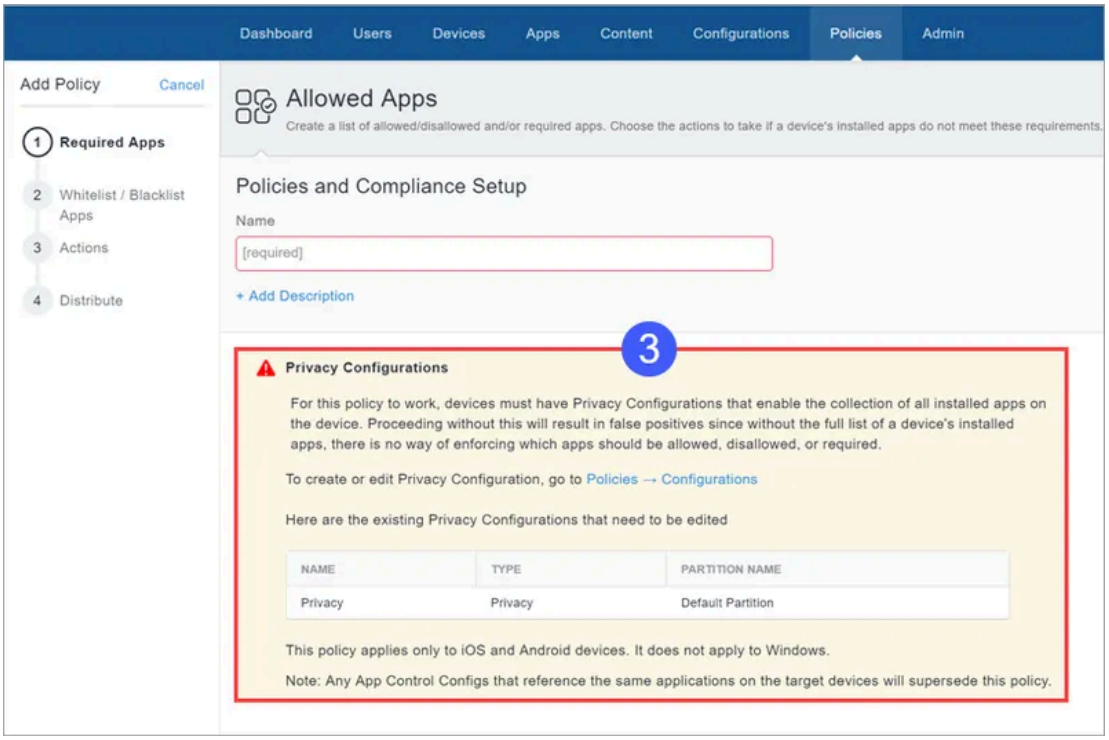
- La **configurazione della privacy** assegnata a un dispositivo deve consentire la raccolta di informazioni sulle app per il corretto funzionamento del criterio App consentite. Controllare le configurazioni della privacy assegnate ai dispositivi a cui verrà applicato il criterio App consentite.

Se non si è certi di quali configurazioni sono interessate:

1. Andare a **Criteri**.



Far clic su **App consentite**.



3. In **Configurazioni della privacy**, annotare le configurazioni da modificare.
4. Accedere a **Configurazioni**.
5. Per ciascuna configurazione della privacy annotata:
    1. Selezionare la configurazione.
    2. Fare clic su **Modifica**.
    3. Sotto **Raccogli inventario app,** selezionare **Per tutte le app sul dispositivo**.
    4. Fare clic su **Fine**.

Creazione di un criterio App consentite

Prerequisiti

- Consentire ad Android Enterprise di accedere a Google Play Store e aggiungere nuove applicazioni alla policy per le app consentite.

Procedura

1. Andare a **Policy**, quindi fare clic su **+ Aggiungi**.

2. Far clic su **App consentite**.

3. Nel campo **Nome** digitare un nome per il criterio.
4. Nel campo **Descrizione** digitare testo facoltativo per spiegare lo scopo del criterio.
5. Scegliere le app da consentire o non consentire facendo clic su una o entrambe le seguenti schede:

- Fare clic su Aggiungi da ricerca per cercare e scegliere le app dall'app Store o dall'App Catalog.
  Assicurarsi di attivare Android Enterprise per accedere a Google Play Store

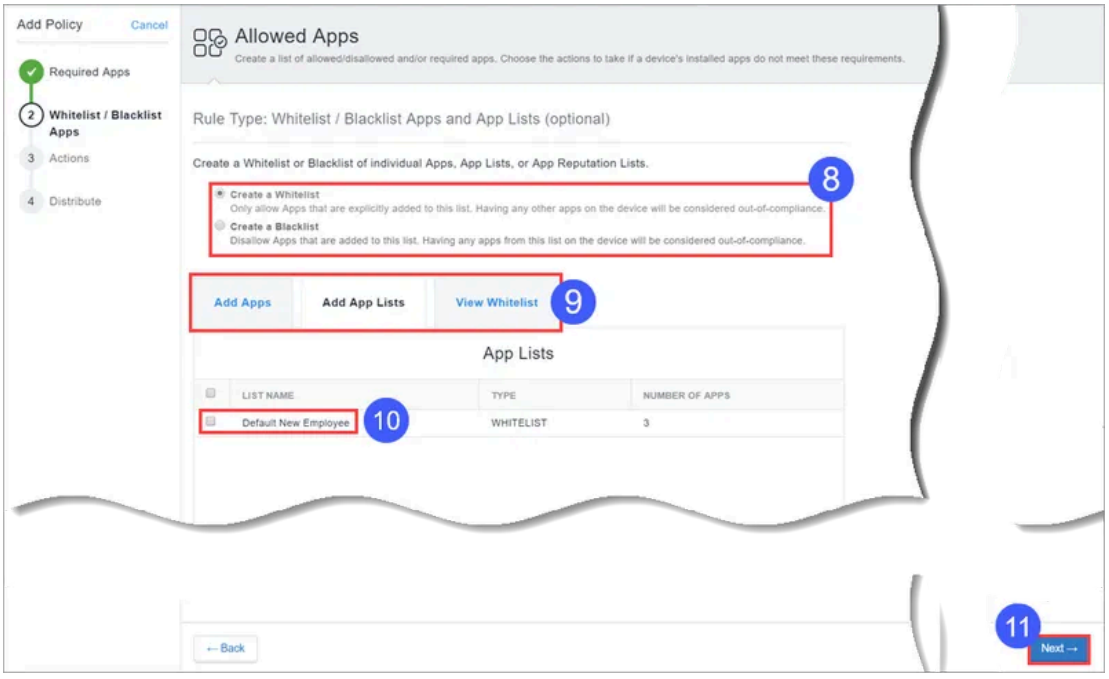
- Fare clic su **Aggiungi manualmente** per scegliere le app inserendo l'ID del bundle per le app di sistema Android, Windows, iOS o macOS.

Selezionare la scheda **Aggiungi elenchi di app**, quindi selezionare gli elenchi di app desiderati.

6. Utilizzare i campi risultanti per selezionare le app richieste o gli elenchi di app.
7. Fare clic su **Avanti**

> Fare clic sulla scheda **Visualizza elenco richiesto** per consultare un elenco delle app selezionate finora.

8. Scegliere se creare un elenco di app consentite o non consentite.



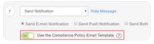
9. Utilizzare la sezione **App consentite/non consentite ed Elenchi di app** per selezionare le app e gli elenchi di app.

> Non è possibile disporre contemporaneamente di un elenco di app consentite e di un elenco di app non consentite per un dispositivo. Se si crea un elenco di app consentite, tutte le altre app non sono consentite.

10. Utilizzare i campi risultanti per selezionare le app richieste o gli elenchi di app.
    - Selezionare la scheda **Aggiungi elenchi di app**, quindi selezionare gli elenchi di app desiderati.
11. Fare clic su **Avanti**.

> Fare clic sulla scheda **Visualizza app consentite o non consentite** per mostrare l'elenco delle app selezionate finora.

12. Selezionare le azioni da intraprendere quando un dispositivo non è conforme:

Azione	Operazione da eseguire
Monitoraggio	Attualmente è sempre selezionata. Con Sentry 9.0.0 o versioni successive è richiesto l'utilizzo delle azioni di conformità a livelli.
Nessuna azione	Selezionare questa opzione per non intraprendere alcuna azione se il dispositivo non è conforme.
Invia notifica	
Invia e-mail	Selezionare questa opzione per inviare un'e-mail all'indirizzo dell'utente del dispositivo, per avvisarlo che il dispositivo non è conforme. • Attivare l'opzione **Usa modello e-mail sulle policy di conformità** per inserire il messaggio configurato qui nel modello e-mail di notifica delle policy come descritto in **Personalizzazione di un modello e-mail** in **Personalizzazione dei modelli e-mail**. Per una panoramica, consultare la sezione **Configurazione e utilizzo di e-mail di notifica sulla conformità delle policy**.  • È possibile personalizzare i messaggi includendo variabili di sostituzione facoltative per fornire ai destinatari maggiori dettagli sulle violazioni della policy e altre informazioni rilevanti. Ciò fornisce agli utenti dei dispositivi non conformi informazioni rilevanti sulla violazione dei criteri, in modo che possano intraprendere azioni correttive. Fare clic sui tipi di attributo seguenti per visualizzare l'elenco completo di variabili: ◦ Attributi policy, inclusi $, $ e $. ◦ Attributi utente, inclusi $, $ e $. ◦ Attributi dei dispositivi, inclusi $, $ e $.
Invia notifica push	Selezionare questa opzione per inviare una notifica push al dispositivo non conforme.
Invia entrambi	Selezionare questa opzione per inviare una notifica push al dispositivo e un'e-mail all'indirizzo dell'utente del dispositivo per avvisarlo che il dispositivo non è conforme. È possibile personalizzare i messaggi includendo variabili di sostituzione facoltative per fornire ai destinatari maggiori dettagli come descritto in precedenza per l'azione Invia e-mail.
Attendi	Selezionare questa opzione per ritardare l'azione per un periodo di tempo specifico e consentire agli utenti di correggere la violazione prima che siano intraprese altre azioni se il dispositivo rimane in uno stato di non conformità.
Blocca	Utilizza Sentry per impedire ai dispositivi gestiti di accedere alle e-mail e alle applicazioni con abilitazione AppConnect.
Quarantena	Selezionare questa opzione per rimuovere l'accesso ad app, contenuti e server secondo le azioni indicate nella tabella seguente. L'azione Rimuovi tutte le app non è consentita.
Inviare una notifica quando il dispositivo è di nuovo conforme	

Azione	Operazione da eseguire
Invia e-mail	Invia un'e-mail all'indirizzo e-mail dell'utente del dispositivo, per avvisarlo che è di nuovo conforme. • È possibile utilizzare il modello e-mail di notifica delle policy come descritto in precedenza. • È possibile personalizzare i messaggi includendo variabili di sostituzione facoltative per fornire ai destinatari maggiori dettagli sulle violazioni della policy e altre informazioni rilevanti. Fare clic sui tipi di attributo seguenti per visualizzare l'elenco completo di variabili: ◦ Attributi policy, inclusi $, $ e $. ◦ Attributi utente, inclusi $, $ e $. ◦ Attributi dei dispositivi, inclusi $, $ e $. ◦ Attributi LDAP/utente/dispositivo personalizzati, creati dalla pagina **Amministratore > Attributi**.
Invia notifica push	Invia una notifica push al dispositivo quando il dispositivo è di nuovo conforme.
Invia entrambi	Invia una notifica push al dispositivo e un'e-mail all'indirizzo dell'utente del dispositivo per avvisarlo che il dispositivo è di nuovo conforme. È possibile personalizzare i messaggi includendo variabili di sostituzione facoltative per fornire ai destinatari maggiori dettagli come descritto in precedenza per l'azione Invia e-mail.

Se si dispone della licenza Platinum, la policy App consentite supporta le **azioni di conformità a livelli**.

Azioni di quarantena aggiuntive (facoltative)	Descrizione
Applicazioni gestite in quarantena	Rimuove dal dispositivo tutte le app gestite da Ivanti Neurons for MDM e attiva l'opzione Blocca nuovi download delle app per impedire che le app vengano reinstallate nel dispositivo. Selezionare una delle seguenti opzioni: • **Tutte le applicazioni** • **Applicazioni designate**: consente di aggiungere una o più app manualmente (utilizzando l'ID bundle o il nome pacchetto) oppure eseguendo una ricerca. Fare clic sulla scheda **Visualizza app** per esaminare l'elenco delle app aggiunte. L'azione di quarantena Blocca accesso ad App Store non è più disponibile. In alcuni dispositivi l'azione di quarantena non rimuove l'applicazione dal dispositivo, a causa di specifiche limitazioni del dispositivo.
Blocca nuovi download delle app	Impedisce il download di qualsiasi nuova app nel dispositivo. Selezionare una delle seguenti opzioni: • **Tutte le applicazioni** • **Applicazioni designate**: consente di aggiungere una o più app manualmente (utilizzando l'ID bundle o il nome pacchetto) oppure eseguendo una ricerca. Fare clic sulla scheda **Visualizza app** per esaminare l'elenco delle app aggiunte. L'azione di quarantena Blocca accesso ad App Store non è più disponibile.
Rimuovi configurazioni	Consente di rimuovere le configurazioni di Ivanti Neurons for MDM dal dispositivo. Selezionare una delle seguenti opzioni: • **Tutte le configurazioni** • **Configurazioni designate** - Selezionare una o più configurazioni dall'elenco per ricercarle. Fare clic sulla scheda **Configurazioni selezionate** per esaminare l'elenco delle configurazioni selezionate.
Rimuovi contenuto	Rimuove dal dispositivo tutto il contenuto e i supporti associati alle app distribuite da Ivanti Neurons for MDM.
Sospendere app personali	Sospende le app sul lato personale del dispositivo in quarantena per indicare che l'utente del dispositivo deve risolvere i problemi di conformità sul dispositivo per renderlo funzionale. Supportato su dispositivi Android 11 o versione superiore forniti in modalità Profilo di lavoro su dispositivo di proprietà dell'azienda.
Azioni di quarantena predefinite - queste azioni vengono eseguite sempre.	
Blocca accesso ad app Store	Impedisce al dispositivo di accedere agli app store tramite Ivanti Neurons for MDM.
Blocca accesso a Store contenuto	Impedisce al dispositivo di accedere allo Store del contenuto tramite Ivanti Neurons for MDM.

Azioni di quarantena aggiuntive (facoltative)	Descrizione
Blocca AppConnect	Impedisce al dispositivo di utilizzare le funzioni di AppConnect.
Blocca AppTunnel	Impedisce alle applicazioni sul dispositivo di accedere al contenuto e ai server tramite AppTunnel.
Blocca ActiveSync	Impedisce al dispositivo di accedere alle e-mail tramite il server ActiveSync.

Fare clic su **Avanti**.

14. Configurare la distribuzione.
15. Fare clic su **Fine**.

Per ulteriori informazioni sull'aumento o la diminuzione delle priorità di una policy App consentite, vedere **Definire le priorità delle policy**.

11.4. Assegnazione della priorità alle policy

La policy App consentite supporta una priorità, simile a Configurazioni. Una priorità viene utilizzata per determinare quale policy dello stesso tipo viene distribuita a più gruppi di dispositivi, e il caso in cui lo stesso dispositivo appare nei diversi gruppi di dispositivi. Ad esempio, una priorità di policy è utile per determinare la distribuzione della policy nel caso in cui:

- "App A richiesta" deve essere distribuita al gruppo di dispositivi 1,
- "App B richiesta" deve essere distribuita al gruppo di dispositivi 2, e
- il dispositivo dell'utente fa parte di entrambi i gruppi di dispositivi.

È possibile assegnare la priorità alle policy come segue:

1. Andare su **Criteri > Criterio e conformità**.
2. Selezionare **Azioni > Assegna priorità alle policy**. Se l'opzione **Azioni** non viene visualizzata, significa che non sono disponibili più criteri che necessitano di priorità.
3. Usare le frecce per elencare le priorità dalla più alta (in alto) alla più bassa (in basso). Un'icona a forma di lucchetto indica che non è possibile modificare la priorità della policy senza modificare l'impostazione di distribuzione Tutti i dispositivi all'interno della policy.
4. Fare clic su **Salva**.

11.5. Policy Hardware Windows

Couldn't convert your doc.

12. Amministratore

La sezione Amministratore consente di gestire utenti, dispositivi e configurazioni nel portale Ivanti Neurons per MDM. Le seguenti sezioni contengono l'elenco di tutte le attività che è possibile eseguire come amministratore:

- Sistema
- Infrastruttura
- Impostazioni (Apple)
- Utilizzo di dispositivi Windows
- Configurazione con Microsoft Azure
- Connessione a Google Apps
- Lavorare con i dispositivi ChromeOS
- Gestione firmware
- Sospensione tenant
- Gestisci script e file
- Personalizzazione
- Aggiunta della gestione di dispositivi non iOS

12.1. Sistema

Argomenti della sezione:

- Attributi
- Impostazioni pulizia dispositivo
- Profili GDPR
- E-mail di notifica
- Gestione dei ruoli
- Spazi
- Amministratori di supporto
- Admin > Notifica di utilizzo del sistema

12.1.1. Attributi

Utilizzare la pagina Attributi per eseguire le seguenti operazioni:

- Gestire i tipi di informazioni che è possibile registrare per utenti, dispositivi e app.
- Visualizzare i tipi di informazioni standard tracciati da Ivanti Neurons per MDM.

Gli attributi utente personalizzati includono informazioni quali il reparto o un ID interno. Ciascun attributo dispone di una variabile corrispondente che è possibile utilizzare per creare gruppi o distribuire configurazioni.

> Durante la creazione dei criteri di un gruppo di regole utente, se gli attributi personalizzati hanno un valore numerico, Ivanti Neurons per MDM non supporta le operazioni sui numeri interi.

Creazione di attributi personalizzati

È possibile creare attributi personalizzati dal portale amministrativo Ivanti Neurons per MDM.

Procedura

1. Accedere al Portale amministrativo.
2. Navigare in **Amministratore** > **Sistema** > **Attributi**.
3. In **Attributi personalizzati**, fare clic su **+Aggiungi**.
4. Nel campo **Nome attributo**, immettere il testo che rappresenta l'attributo.

> Il testo immesso sarà utilizzato per creare la variabile corrispondente nel campo **Utilizzo**.

Selezionare qualsiasi tipo di attributo dalle seguenti opzioni di **Tipo di attributo**.

   - **Utente**
   - **Dispositivo**
   - **App**
   - **IDP** (per ulteriori informazioni, vedere Provisioning utente con SCIM o Collegare Ivanti Neurons per MDM con origine utente Entra ID)

Se il tipo di attributo è Dispositivo, selezionare una delle seguenti opzioni **Tipo di dati**:

   - **Numerico**
   - **Testo**

7. **Conserva attributo** (facoltativo): questa opzione può essere utilizzata solo quando il tipo di attributo è **Dispositivo**. Selezionare questa opzione per preservare l'attributo personalizzato anche quando viene eseguita un'operazione di cancellazione / ritiro su un dispositivo.
8. Fare clic su **Aggiungi**.
   L'attributo utente personalizzato creato viene visualizzato nella sezione **Amministratore Aggiunto** nella pagina Attributi.

> La combinazione di attributi personalizzati $ + $ + $ + ${Static String} è supportata in qualsiasi ordine.

Assegnazione di un nuovo nome a un attributo personalizzato

Se si rinomina un attributo personalizzato, verranno rinominati tutti i riferimenti a quell'attributo personalizzato utilizzati nelle seguenti entità:

- Policy personalizzata
- Gruppo di utenti
- Gruppi di dispositivi
- Filtro di distribuzione delle app
- Spazi

> I riferimenti all'attributo personalizzato in qualsiasi altra entità, come configurazioni, modelli di e-mail di invito, messaggi push ed e-mail nelle azioni di conformità delle policy e così via, non verranno aggiornati.

Procedura

1. In **Amministratore aggiunto**, fare clic su **+Modifica** accanto all'attributo da rinominare.
2. Nel campo **Nome attributo**, immettere il nuovo nome che rappresenta l'attributo.

> Il testo immesso sarà utilizzato per creare la variabile corrispondente nel campo **Utilizzo**.

Fare clic su **Salva**.

Eliminazione di un attributo personalizzato

L'eliminazione di un attributo personalizzato rimuoverà i suoi valori da tutti gli utenti o dispositivi associati. Questa operazione non può essere annullata.

Non è possibile eliminare un attributo personalizzato, se questo attributo è utilizzato in una delle seguenti entità:

- Policy personalizzata
- Gruppo di utenti
- Gruppi di dispositivi
- Filtro di distribuzione delle app
- Spazi

Rimuovere l'attributo personalizzato dalle entità prima di tentare di eliminare l'attributo personalizzato.

Se l'attributo da eliminare non ha riferimenti in nessuna delle suddette entità, verrà visualizzata una finestra popup di conferma dell'azione quando si fa clic su **Elimina** accanto all'attributo. Confermare l'azione e fare clic su **Elimina**.

> I nomi dei campi dei seguenti attributi personalizzati sono ordinati nei generatori di regole applicabili:

- Attributo LDAP personalizzato
- Attributo utente personalizzato
- Attributo dispositivo personalizzato
- Attributo IdP personalizzato

- Attributo app personalizzato

Visualizzazione degli attributi di sistema

Gli attributi di sistema sono attributi predefiniti da utilizzare come variabili nelle configurazioni. L'elenco completo è disponibile nella sezione **Attributi di sistema** della pagina **Amministratore** > **Sistema** > **Attributi**. Gli attributi di sistema includono i seguenti tipi di attributi:

- Attributi utente
- Attributi dispositivo
- Attributi modello e-mail
- Attributi di sistema
- Attributi data e ora
- Attributi utente Entra ID personalizzati
- Attributi policy

Attributi utente

Usare gli attributi utente per specificare informazioni sugli utenti.

Chiave	Descrizione
$	attributo reparto (richiede Entra ID)
$	Scambio elettronico di dati-Identificatore personale
$	ID Apple gestito dall'utente
$	Attributo sAMAccountName (richiede Active Directory)
$	Attributo Nome comune (CN) estratto dal nome distinto (richiede LDAP)
$	Nome visualizzato
$	Nome distinto (richiede LDAP)
$	La parte di dominio dell'indirizzo e-mail (la parte dopo '@')
$>	La parte locale dell'indirizzo e-mail (la parte prima di '@')
$	Indirizzo e-mail
$	Nome
$	Cognome
$	Impostazioni locali
$	Attributo Unità organizzativa (UO) estratto dal nome distinto (richiede LDAP)
$	Informazioni Kerberos Realm (richiede Active Directory)
$	La parte di dominio dell'ID login (la parte dopo '@')
$	La parte locale dell'ID login (la parte prima di '@')
$	ID login (formato indirizzo e-mail)
$	Attributo userPrincipalName (richiede Active Directory)

Attributi dispositivo

Usare gli attributi del dispositivo per specificare informazioni su un dispositivo mobile.

Chiave	Descrizione
$	Data ultimo check-in client (check-in più recente - MDM o Client)
$	Numero di serie alternativo
$	Identificatore utilizzato dall'applicazione client
$	Identificatore dispositivo globalmente univoco
$	ICCID
$	IMEI2
$	IMEI
$	IMSI
$	Data ultimo check-in dispositivo (check-in più recente - MDM o Client)
$	Identificatore dispositivo interno
$	Identificatore utilizzato per MDM
$	MEID
$	Modello
$	Nome dispositivo
$	Numero di telefono dispositivo
$	Identificatore dispositivo univoco cluster
$	Numero di serie
$	iOS UDID
$	Indirizzo MAC Wi-Fi
	Numero di telefono 2
	ICCID 2

Quando si crea un attributo personalizzato e si fa riferimento a questo attributo in una configurazione dell'app gestita, se il valore dell'attributo viene aggiornato, anche l'attributo a cui si fa riferimento nella configurazione dell'app gestita viene aggiornato e la configurazione dell'app gestita viene inviata nuovamente al dispositivo.

Quando gli attributi Personalizzato o Dispositivo vengono aggiornati e la configurazione viene inviata a un dispositivo, anche la configurazione del marchio Android Kiosk deve essere aggiornata.

Attributi app

Utilizzare gli attributi delle app per specificare le informazioni sulle applicazioni e creare gruppi di applicazioni personalizzate.

Chiave	Descrizione
$	L'Applicazione data è stata aggiunta al Catalogo app
$	Nome dell'applicazione
$	Sistema operativo applicazione
$	Bundle applicazione o ID pacchetto
$	Descrive l'origine da cui è stata importata l'applicazione
$	Descrive se un'applicazione iOS o macOS è VPP o meno

Attributi modello e-mail

Chiave	Descrizione
$	Corpo e-mail
$	Oggetto e-mail

Attributi data e ora

Chiave variabile	Descrizione
$	Timestamp corrente (millisecondi dal periodo)

Attributi modelli criteri

Chiave	Descrizione
$	Nome criterio violato
$	Prossima azione conformità a livello (diversa da attendi e ritira) da intraprendere dopo l'invio del messaggio
$	Conteggio di giorni in cui il dispositivo è rimasto in uno stato di non conformità
$	Timestamp relativo alla prima attivazione della violazione del criterio (formato UTC GG-MM-AAAA)
$	Definizione regola (interroga la stringa nel modo in cui appare ora)

Argomenti correlati:

- Assegnazione di attributi personalizzati agli utenti
- Assegnazione di attributi personalizzati ai dispositivi
- Rimozione di attributi personalizzati dagli utenti
- Rimozione di attributi personalizzati dai dispositivi

- Variabili

12.1.2. Impostazioni pulizia dispositivo

La pulizia dei dispositivi automatizza il ciclo di vita dei dispositivi inutilizzati. È possibile ritirare i dispositivi che non sono stati contattati per un numero di giorni stabilito dall'utente. È possibile eliminare i dispositivi ritirati da un numero di giorni specificato dall'utente. La pagina Audit Trail acquisisce le impostazioni di Ritira dispositivo, Elimina dispositivo e Elimina dispositivo cancellato.

La tabella seguente fornisce informazioni sui dispositivi Android che supportano le impostazioni di pulizia del dispositivo:

Modalità	Ritira se Non conforme	Elimina ritirati	Imponi ritiro o in attesa di ritiro	Elimina cancellati	Elimina in attesa di cancellazione
Profilo di lavoro Android (Proprietario del profilo)	**SÌ**	**SÌ**	**SÌ**	**NO**	**NO**
Amministratore dispositivo/Profilo di lavoro su dispositivo di proprietà dell'azienda	**SÌ**	**SÌ**	**SÌ**	**SÌ**	**SÌ**
Dispositivo gestito dal lavoro/Dispositivo gestito Android con profilo di lavoro	**NO**	**NO**	**NO**	**SÌ**	**SÌ**

Prerequisiti

Per accedere a questa impostazione è necessario disporre delle autorizzazioni del ruolo di gestione del sistema.

Ritira dispositivi

Procedura

1. Andare in **Amministratore** > **Sistema** > **Pulizia dispositivi**. Si apre la pagina Pulizia dispositivo.
2. Selezionare **Ritira dispositivo**.
3. Utilizzare la tabella **Ritira dispositivi** per specificare i dettagli.
4. Fare clic su **Mostra elenco dispositivi privi di check-in**. Mostra l'elenco dei dispositivi che non hanno effettuato il check-in per il numero di giorni specificato.
5. Fare clic su **Dispositivi ritirati ora**; in alternativa, è possibile pianificare il ritiro del dispositivo.
6. Il portale amministrativo Ivanti Neurons per MDM ritirerà i dispositivi specificati.
7. Fare clic su **Salva** per salvare le impostazioni.
8. (Opzionale) Se si aggiornano i valori, è possibile fare clic su **Reimposta** per ripristinare le impostazioni iniziali.

Ritira dispositivi

Campo	Descrizione
Seleziona piattaforme	Selezionare la piattaforma richiesta su cui applicare le impostazioni di pulizia del dispositivo. Questa opzione è attualmente disponibile solo sulle impostazioni **Ritira dispositivo** e **Ritira dispositivo in sospeso**.
Ritira i dispositivi che non hanno effettuato il check-in per più di (giorni)	Giorni: 30 giorni è l'impostazione predefinita, 365 giorni è il numero massimo di giorni consentito.
Dispositivi massimi da ritirare in ogni sessione	Selezionare 100, 500 o 1000 (predefinito - 100).
Ritiro automatico dei dispositivi in base a una pianificazione	Selezionare la casella di controllo per ritirare i dispositivi in base a una pianificazione predefinita.
Configurazione programma di ritiro	Selezionare una delle seguenti opzioni per impostare la frequenza dei ritiri: • **Giornaliero -** Impostare il ritiro quotidiano dei dispositivi. • **Settimanale -** Specificare il giorno della settimana in cui pianificare il ritiro. • **Mensile -** Impostare il ritiro dei dispositivi il primo giorno di ogni mese.

Elimina dispositivi ritirati

Procedura

1. Andare in **Amministratore** > **Sistema** > **Pulizia dispositivi**. Si apre la pagina Pulizia dispositivo.
2. Selezionare **Elimina dispositivo ritirato**.
3. Usare la tabella **Elimina dispositivi ritirati** per specificare i dettagli.
4. Fare clic su **Mostra elenco dispositivi ritirati**. Mostra l'elenco dei dispositivi ritirati per il numero di giorni specificato.
5. Fare clic su **Elimina ora dispositivi ritirati**; in alternativa, è possibile pianificare l'eliminazione del dispositivo.
6. Il portale amministrativo Ivanti Neurons per MDM eliminerà i dispositivi specificati.
7. Fare clic su **Salva** per salvare le impostazioni.
8. (Opzionale) Se si aggiornano i valori, è possibile fare clic su **Reimposta** per ripristinare le impostazioni iniziali.

Elimina dispositivi ritirati

Campo	Descrizione
Elimina dispositivi ritirati da più di (giorni)	Giorni: 30 giorni è l'impostazione predefinita, 365 giorni è il numero massimo di giorni consentito.
Dispositivi massimi ritirati da eliminare in ogni sessione	Selezionare 100, 500 o 1000 (predefinito - 100)
Eliminazione automatica dei dispositivi ritirati in base a una pianificazione	Selezionare la casella di controllo per ritirare i dispositivi in base a una pianificazione predefinita.
Elimina configurazione pianificazioni	Selezionare una delle seguenti opzioni per impostare la frequenza di eliminazione: • **Giornaliero -** Impostare l'eliminazione dei dispositivi ogni giorno. • **Settimanale -** Specificare il giorno della settimana in cui pianificare l'eliminazione. • **Mensile -** Impostare l'eliminazione dei dispositivi ritirati il primo giorno di ogni mese.

Elimina dispositivi cancellati

Procedura

1. Andare in **Amministratore** > **Sistema** > **Pulizia dispositivi**. Si apre la pagina Pulizia dispositivo.
2. Selezionare **Elimina dispositivo cancellato**.
3. Utilizzare la tabella **Elimina dispositivi cancellati** per specificare i dettagli.
4. Fare clic su **Mostra elenco dispositivi cancellati**. Mostra l'elenco dei dispositivi ritirati per il numero di giorni specificato.
5. Fare clic su **Elimina dispositivi cancellati ora**; in alternativa, è possibile pianificare l'eliminazione dei dispositivi cancellati.
6. Il portale amministrativo Ivanti Neurons per MDM eliminerà i dispositivi specificati.
7. Fare clic su **Salva** per salvare le impostazioni.
8. (Opzionale) Se si aggiornano i valori, è possibile fare clic su **Reimposta** per ripristinare le impostazioni iniziali.

Elimina dispositivi cancellati

Campo	Descrizione
Eliminare i dispositivi cancellati da più di (giorni)	Giorni: 30 giorni è l'impostazione predefinita, 365 giorni è il numero massimo di giorni consentito.
Dispositivi massimi cancellati da eliminare in ogni sessione	Selezionare 100, 500 o 1000 (predefinito - 100)
Eliminazione automatica dei dispositivi cancellati in base a una pianificazione	Selezionare la casella di controllo per eliminare i dispositivi cancellati in base a una pianificazione predefinita.
Elimina configurazione pianificazioni cancellate	Selezionare una delle seguenti opzioni per impostare la frequenza di eliminazione: • **Giornaliero -** Impostare l'eliminazione dei dispositivi cancellati ogni giorno. • **Settimanale -** Specificare il giorno della settimana in cui pianificare l'eliminazione. • **Mensile -** Impostare l'eliminazione dei dispositivi cancellati il primo giorno di ogni mese.

Elimina dispositivi in attesa di cancellazione

Procedura

1. Andare in **Amministratore** > **Sistema** > **Pulizia dispositivi**. Si apre la pagina Pulizia dispositivo.
2. Selezionare **Elimina dispositivo in attesa di cancellazione**.
3. Utilizzare la tabella **Elimina dispositivi in attesa di cancellazione** per specificare i dettagli.
4. Fare clic su **Mostra elenco dispositivi in attesa di cancellazione**. Mostra l'elenco dei dispositivi che devono essere cancellati per il numero di giorni specificato.
5. Fare clic su **Elimina ora dispositivi in attesa di cancellazione**, in alternativa, è possibile pianificare l'eliminazione dei dispositivi in sospeso.
6. Il portale amministrativo Ivanti Neurons per MDM eliminerà i dispositivi specificati.
7. Fare clic su **Salva** per salvare le impostazioni.
8. (Opzionale) Se si aggiornano i valori, è possibile fare clic su **Reimposta** per ripristinare le impostazioni iniziali.

Elimina dispositivi in attesa di cancellazione

Campo	Descrizione
Eliminare i dispositivi in attesa di cancellazione da più di (giorni)	Giorni: 30 giorni è l'impostazione predefinita, 365 giorni è il numero massimo di giorni consentito.
Dispositivi massimi in attesa di cancellazione da eliminare in ogni sessione	Selezionare 100, 500 o 1000 (predefinito - 100)
Eliminazione automatica dei dispositivi in attesa di cancellazione in base a una pianificazione	Selezionare la casella di controllo per eliminare i dispositivi cancellati in base a una pianificazione predefinita.
Elimina configurazione pianificazioni in attesa di cancellazione	Selezionare una delle seguenti opzioni per impostare la frequenza di eliminazione: • **Giornaliero -** Impostare l'eliminazione dei dispositivi in attesa di cancellazione ogni giorno. • **Settimanale -** Specificare il giorno della settimana in cui pianificare l'eliminazione. • **Mensile -** Impostare l'eliminazione dei dispositivi in attesa di cancellazione il primo giorno di ogni mese.

Ritira i dispositivi in attesa di ritiro

Procedura

1. Andare in **Amministratore** > **Sistema** > **Pulizia dispositivi**. Si apre la pagina Pulizia dispositivo.
2. Selezionare **Ritira il dispositivo in attesa di ritiro**.
3. Utilizzare la tabella **Ritira i dispositivi in attesa di ritiro** per specificare i dettagli.
4. Fare clic su **Mostra ritiro elenco dispositivi in attesa**. Mostra l'elenco dei dispositivi che devono essere ritirati per il numero di giorni specificato.
5. Fare clic su **Imponi ora ritiro dei dispositivi in attesa di ritiro**, in alternativa è possibile pianificare il ritiro delle periferiche in sospeso.
6. Il portale amministrativo Ivanti Neurons per MDM ritirerà i dispositivi specificati.
7. Fare clic su **Salva** per salvare le impostazioni.
8. (Opzionale) Se si aggiornano i valori, è possibile fare clic su **Reimposta** per ripristinare le impostazioni iniziali.

Ritira i dispositivi in attesa di ritiro

Campo	Descrizione
Ritira i dispositivi in attesa di ritiro che non hanno effettuato il check-in per più di (giorni)	Giorni: 30 giorni è l'impostazione predefinita, 365 giorni è il numero massimo di giorni consentito.
Dispositivi massimi in attesa di ritiro in ogni sessione	Selezionare 100, 500 o 1000 (predefinito - 100)
Ritiro automatico dei dispositivi in attesa di ritiro in base a una pianificazione	Selezionare la casella di controllo per ritirare i dispositivi in attesa di ritiro in base a una pianificazione predefinita.
Configurazione Pianificazione Ritira dispositivi in attesa di ritiro	Selezionare una delle seguenti opzioni per impostare la frequenza di eliminazione: • **Giornaliero -** Impostare il ritiro dei dispositivi in attesa ogni giorno. • **Settimanale -** Specificare il giorno della settimana in cui pianificare il ritiro dei dispositivi in sospeso. • **Mensile -** Impostare il ritiro dei dispositivi in sospeso il primo giorno di ogni mese.

Quando un dispositivo viene ritirato e se il check-in è avvenuto molto tempo fa, quell'ultimo tempo di check-in verrà considerato solo per determinare l'eliminazione del dispositivo. Ad esempio, se il dispositivo è stato controllato l'ultima volta dopo 30 giorni e se il dispositivo è stato ritirato oggi (può essere dovuto all'opzione "Ritira dispositivi che non sono stati controllati più di (giorni)") e se "Elimina dispositivi ritirati da più di (giorni)" è impostato su 30 giorni, il dispositivo verrà eliminato immediatamente dopo l'esecuzione del processo "Elimina dispositivo ritirato".

12.1.3. Profili GDPR

Il portale amministrativo Ivanti Neurons per MDM contiene ora la pagina Profili GDPR che consente di assegnare i profili GDPR ai gruppi di utenti. È possibile assegnare il profilo GDPR solo ai gruppi di utenti e non ai singoli utenti.

Tenere presenti i seguenti punti:

- È necessario prima abilitare i profili GDPR per assegnarli a un gruppo di utenti specifico.
- Se si disattiva il profilo GDPR, si disattivano tutte le restrizioni del profilo già assegnate al gruppo di utenti.
- Dopo aver abilitato il profilo GDPR, la funzionalità di modifica di alcuni campi sarà limitata o disabilitata.

Campi che vengono nascosti dopo l'assegnazione del profilo GDPR

Se un utente ha un profilo GDPR, Ivanti Neurons per MDM nasconde i seguenti campi per impostazione predefinita quando si visualizzano le informazioni sull'utente:

- **ID utente**
- **Nome utente**
- **Indirizzo e-mail**
- **Numero di serie**
- **ICCID**
- **IMSI**
- **MEID**
- **Indirizzo IP**
- **Numero di telefono**
- **IMEI**
- **Identificatore eSIM**
- **Posizione**

> Se la posizione viene aggiunta al profilo GDPR, i campi Posizione dispositivo Ultima posizione, Latitudine e Longitudine vengono mascherati nei dettagli del dispositivo per gli utenti assegnati al profilo GDPR.

Abilitazione del profilo GDPR

È possibile abilitare il profilo GDPR e selezionare campi specifici che devono essere nascosti dal portale amministrativo Ivanti Neurons per MDM e dai dispositivi.

ProcedureProcedura

1.	**Accedere al portale amministrativo Ivanti Neurons per MDM.**
2.	**Andare in Amministratore > Sistema > Profili GDPR.**

	3.	Fare clic su **Abilita**.

	4.	Fare clic sull'icona di modifica (matita).

5.	Selezionare i campi che devono essere nascosti.

6.	Fare clic su **Salva**. I campi selezionati saranno mascherati e non visualizzeranno i valori per gli utenti specifici.

Assegna profilo GDPR a gruppi di utenti

Dopo aver abilitato il profilo GDPR, è possibile assegnarlo a gruppi di utenti specifici.

ProcedureProcedura

	1.	Accedere al portale amministrativo Ivanti Neurons per MDM.

2.	Andare a **Utenti** > **Gruppi di utenti**.

3.	Selezionare un gruppo di utenti dall'elenco.

	4.	Fare clic sull'elenco a discesa **Azioni** e selezionare **Assegna Profilo GDPR**. Il profilo GDPR viene assegnato a tutti gli utenti di quel gruppo specifico e tutti i valori selezionati saranno mascherati dalla vista nel portale amministrativo e nei dispositivi degli utenti. Poiché l'amministratore è anche nel gruppo Tutti gli utenti, non assegnare i profili GDPR al gruppo Tutti gli utenti.

12.1.4. E-mail di notifica

Licenza: Silver

È possibile configurare l'elenco di indirizzi e-mail degli utenti che devono ricevere e-mail di notifica in base al livello di importanza della notifica.

La funzione E-mail di notifica è facoltativa ed è possibile attivarla o disattivarla come richiesto. Per utilizzare questa funzione, è necessario disporre del ruolo di gestione di sistema.

1. Selezionare **Admin > Sistema > E-mail di notifica**. Viene visualizzata la pagina **E-mail di notifica**.
2. Nella sezione Impostazioni delle e-mail di notifica, fare clic su **ON** per attivare la funzione E-mail di notifica.
3. Fare clic su **Aggiungi destinatario**. Viene mostrata la finestra popup **Aggiungi destinatario**.
4. Nella finestra **Aggiungi destinatario**, aggiornare i seguenti campi:
    - ID e-mail destinatario: immettere l'ID e-mail del destinatario a cui deve essere inviata la notifica.
    - Tipi di notifica da inviare: selezionare il tipo di notifica selezionando la casella di controllo. Sono disponibili i seguenti tipi di notifica: **Notifica critica, Notifiche di avviso, Notifiche informazioni**.
5. Fare clic su **OK**. Verranno mostrati i dettagli delle impostazioni in una tabella.
6. Fare clic su **Salva** per applicare le modifiche.

12.1.5. Gestione dei ruoli

I ruoli sono pacchetti di gruppi di autorizzazioni che permettono di concedere un set di autorizzazioni a utenti amministrativi, limitandone contemporaneamente l'accesso per il controllo di aree di funzionalità specifiche. Ivanti Neurons for MDM fornisce una serie di ruoli di sistema, che possono essere assegnati o modificati, e offre la possibilità di creare ruoli personalizzati. È possibile cercare un'autorizzazione specifica in base alla categoria, in modo da visualizzare tutte le opzioni associate a un ruolo o un'autorizzazione specifici nell'interfaccia utente. Viene visualizzata una descrizione comando per le autorizzazioni aggiunte come autorizzazioni dipendenti.

> La pagina Gestione ruoli e le opzioni associate sono nascoste per i tenant che hanno accesso sia a Ivanti Neurons for UEM che a Ivanti Neurons per MDM.

Sono disponibili due tipi di autorizzazioni, pertanto esistono due tipi di ruoli.

- **Ruoli specifici per lo spazio** - Poiché le autorizzazioni sono specifiche per lo spazio, vengono applicate solo a uno spazio specifico. Ne sono esempi Gestione dei dispositivi e Gestione delle app in uno spazio.
- **Ruoli tra gli spazi**: tendenzialmente, le autorizzazioni si applicano a tutti i ruoli. Ne sono esempi le applicazioni a livello di tenant come i certificati MDM e le impostazioni dell'App Catalog.

Creazione di un ruolo personalizzato

È possibile creare ruoli tra gli spazi personalizzati o ruoli specifici per lo spazio. Quando si seleziona un'autorizzazione, le autorizzazioni dipendenti verranno selezionate automaticamente. Di conseguenza, un utente a cui è stato assegnato un ruolo personalizzato può eseguire solo le azioni specifiche (quali dismissione o cancellazione) disponibili quando l'utente visita la pagina Dispositivi o la pagina Dettagli dispositivo.

Quando si applica il ruolo personalizzato Visualizza PIN di registrazione utente, gli utenti possono visualizzare il PIN di altri utenti con lo stesso livello di accesso o con privilegi inferiori e non possono creare PIN per altri utenti.

> Il ruolo personalizzato appena creato non può essere automaticamente assegnato a tutti. Il super-amministratore del tenant deve assegnarlo agli utenti amministrativi appropriati, che possono quindi assegnarlo ad altri utenti come necessario.

Procedura

1. Andare su **Amministratore** > **Gestione dei ruoli**.
2. Fare clic su **+Aggiungi ruolo personalizzato**.
3. Nella pagina **Crea ruolo**, immettere il **Nome** del nuovo ruolo.
4. (Facoltativo) aggiungere una descrizione per il nuovo ruolo.
5. In **Tipo di ruolo** selezionare uno dei tipi di ruolo seguenti:
   - **Ruolo tra gli spazi**
   - **Ruolo specifico per lo spazio**
6. In **Autorizzazioni**, selezionare le autorizzazioni granulari obbligatorie.
7. Per le autorizzazioni di amministratori e utenti, vedere la tabella seguente.
   Fare clic su **Salva**.

La tabella seguente elenca le autorizzazioni, i ruoli e gli attributi utilizzabili per creare un ruolo personalizzato:

Tipo di ruolo	Categoria autorizzazioni	Autorizzazioni granulari
Ruolo tra gli spazi		
Amministratore		
	Gestisci attributi personalizzati	• Aggiungi attributo personalizzato • Elimina attributo personalizzato • Modifica attributo personalizzato • Visualizza attributo personalizzato
	Amministratori di supporto	• Aggiungi amministratori di supporto • Elimina amministratori di supporto • Disattiva amministratori di supporto • Visualizza gli amministratori di supporto e mostra la cronologia di accesso
	Certification Authority	• Aggiungi autorità di certificazione • Elimina autorità di certificazione
	Connettore	• Aggiungi registri Connettore • Elimina registri Connettore • Visualizza Connettore • Aggiorna Connettore
	Gestione LDAP	• Aggiungi utente/gruppo/unità organizzativa • Aggiungi server • Esplora server • Elimina server • Cerca server

Tipo di ruolo	Categoria autorizzazioni	Autorizzazioni granulari
		• Sincronizza server • Rimuovi utente/gruppo/unità organizzativa • Visualizza Serve Tutte le autorizzazioni LDAP in questa sezione richiedono l'autorizzazione Visualizza Connettore. Sarà selezionata automaticamente nella sezione Connettore quando si seleziona una di queste autorizzazioni LDAP.
	Gestione delle licenze	Visualizza licenze
	Gestisci distribuzione app	**Aggiorna distribuzione app** L'autorizzazione **Aggiorna distribuzione app** è ora disponibile per i ruoli personalizzati in **Gestisci distribuzione app.** Gli utenti con il ruolo Gestione sistema ricevono questa autorizzazione in automatico per impostazione predefinita. La pagina di distribuzione app ora include la casella di controllo **Consenti amministrazione spazio per modificare la distribuzione**, attivata per impostazione predefinita per le nuove app. Gli utenti a cui è stato assegnato un ruolo personalizzato con questa nuova autorizzazione, nonché quelli con il ruolo App Management (senza accesso a Gestione sistema), possono modificare questa opzione. Per ciascuna versione dell'applicazione, la disponibilità dell'impostazione Blocca distribuzione app viene visualizzata nella pagina di distribuzione e tutti i tentativi di valutazione vengono ora acquisiti nell'Audit Trail.
Utenti		
	Azioni di gestione utenti	• Visualizza utente • Aggiorna utente • Invia un messaggio all'utente • Aggiungi/Assegna ruoli all'utente • Crea utente • Elimina utente • Invita utente • Visualizza PIN di registrazione utente
	Assegna attributo utente	• Elimina attributo • Visualizza attributo • Aggiungi/Modifica attributo

Tipo di ruolo	Categoria autorizzazioni	Autorizzazioni granulari
	personalizzato	
Dispositivi	Gruppi di utenti	• Visualizza gruppo di utenti • Modifica gruppo di utenti • Aggiungi/Assegna ruoli a gruppo di utenti • Crea gruppo di utenti • Elimina gruppo di utenti
	Gestione dei report	• Crea report • Modifica report • Esegui report • Elimina record report • Visualizza report • Elimina report • Scarica record report
	Registrazione in blocco	• Crea Registrazione in blocco • Aggiorna Registrazione in blocco • Assegna utente a Registrazione in blocco • Visualizza Registrazione in blocco • Elimina Registrazione in blocco
Ruolo specifico per lo spazio **Dispositi**		

Tipo di ruolo	Categoria autorizzazioni	Autorizzazioni granulari
vi		
	Azioni relative ai dispositivi	• Assegna dispositivo all'utente • Cancella blocco attivazione dispositivo • Elimina dispositivo • Disabilita modalità di smarrimento dispositivo • Abilita modalità di smarrimento dispositivo • Check-In forzato del dispositivo • Blocca dispositivo • Sblocca dispositivo • Uscita forzata del dispositivo • Reinstalla app del sistema del dispositivo • Riavvia dispositivo • Programma aggiornamenti dispositivo iOS • Rinuncia alla proprietà del dispositivo • Ritira dispositivo • Annulla dismissione dispositivo • Arresta dispositivo • Visualizza dispositivo • Elimina dispositivo • Annulla cancellazione dispositivo • Aggiorna versione OS dispositivo • Assegna in blocco tramite caricamento • Avviare la sessione di TeamViewer • Passa in modalità tutto schermo • Esci dalla modalità tutto schermo
	Assegna attributi dispositivo perso	• Aggiungi/Modifica attributo personalizzato dispositivo • Elimina attributo personalizzato del dispositivo • Visualizza attributo personalizzato del dispositivo Tutte le autorizzazioni Assegna attributo dispositivo personalizzato in questa sezione richiedono l'autorizzazione di lettura del dispositivo. Sarà selezionata automaticamente nella sezione Azioni dispositivo quando si seleziona una delle autorizzazioni Assegna attributo dispositivo personalizzato.

Tipo di ruolo	Categoria autorizzazioni	Autorizzazioni granulari
	nalizzati	
	Configurazioni dispositivi	• Escludi profilo • Invia profilo • Invia profilo escluso • Riprova installazione all'errore
	Gruppi di dispositivi	• Aggiungi gruppo dispositivi • Elimina gruppo di dispositivi • Modifica gruppo di dispositivi • Visualizza gruppo di dispositivi
	Registrazione in blocco	• Crea Registrazione in blocco • Aggiorna Registrazione in blocco • Assegna utente a Registrazione in blocco • Visualizza Registrazione in blocco • Elimina Registrazione in blocco
	Inventario delle applicazioni	• Visualizza inventario app
Configurazioni		
Criteri	Configurazioni	• Visualizza/Esporta configurazioni • Modifica/Definisci priorità configurazioni • Aggiungi/Clona configurazioni • Elimina configurazioni
	Criteri	• Visualizza politiche • Modifica/Definisci priorità policy

Tipo di ruolo	Categoria autorizzazioni	Autorizzazioni granulari
		• Aggiungi/Clona policy • Elimina policy

Per modificare un ruolo, andare alla pagina Amministrazione, Gestione ruoli e fare clic sull'icona di modifica in **Azioni** in corrispondenza del nome del ruolo. Un utente non può trasformare un ruolo tra gli spazi in un ruolo specifico per lo spazio e viceversa.

Argomenti correlati:

- Per assegnare un ruolo personalizzato a un utente, vedere **Assegnazione di ruoli**.
- Vedere **Ruoli utente** per un elenco dei ruoli predefiniti.
- **Utilizzo di report personalizzati**
- **Utilizzo di report pianificati**

12.1.6. Spazi

Argomenti della sezione:

- Spazi
- Gestione degli spazi
- Esempi di spazi
- Delega di dispositivi
- Delega di app

12.1.6.1. Spazi

Licenza: Silver

Gli spazi vengono utilizzati per dividere un sistema Unified Endpoint Management (UEM) in entità gestite separatamente, allo scopo di delegare l'amministrazione. Gli spazi possono essere creati in modo da rispecchiare una gerarchia organizzativa. Ivanti Neurons for MDM supporta la delega a un solo livello con un'entità di gestione centrale indicata come Spazio predefinito e un numero di entità di gestione subordinate indicate come Spazi delegati. Ciascun sistema UEM viene creato con uno spazio predefinito.

> La pagina Spazi e le opzioni associate sono nascoste per i tenant convergenti che hanno accesso sia a Ivanti Neurons for UEM che a Ivanti Neurons per MDM.

Uno spazio permette l'amministrazione delegata dei seguenti componenti di sistema. Al momento gli utenti e i gruppi di utenti non possono essere delegati.

- Dispositivi
- Configurazioni
- Criteri
- Gruppi di dispositivi
- Applicazioni
- Un Catalogo app
- Un token di Apple App e libri

Quando un amministratore accede al portale Amministratori Ivanti Neurons per MDM su un tenant con almeno un singolo spazio delegato, visualizza una finestra a comparsa promozionale di accesso al portale Amministratori. La finestra a comparsa promozionale non verrà visualizzata dopo la creazione di uno spazio delegato e durante l'accesso utente se uno spazio delegato è già stato creato.

Ruoli per amministratori di spazi delegati e globali

Un utente amministratore con i ruoli appropriati per accedere allo spazio predefinito viene indicato come amministratore globale. L'accesso allo spazio predefinito può essere di sola lettura o di lettura-scrittura. Un amministratore globale con i ruoli amministrativi appropriati può creare spazi delegati e assegnare amministratori delegati per gestirli. Un amministratore con delega può essere assegnato alla gestione di uno o più spazi delegati.

Gli spazi a cui un determinato amministratore può accedere sono elencati nel menu a discesa Spazi, nell'angolo in alto a sinistra delle schede Dispositivi e Applicazioni. Per visualizzare e gestire uno spazio, utilizzare il menu a discesa Spazi per passare allo spazio desiderato.

Un amministratore globale ha visibilità e controllo sugli spazi delegati, oltre allo spazio predefinito. Un amministratore con delega ha visibilità e controllo solo sugli spazi che gli sono stati assegnati da un amministratore globale. Un amministratore globale mantiene il controllo centrale sugli spazi delegati mentre un amministratore con delega può gestire in autonomia gli spazi che gli sono stati delegati. Il livello di autonomia viene stabilito in base alla provenienza della delega, cioè se questa è stata ereditata o copiata dallo spazio predefinito.

Di seguito sono indicati i vari ruoli utente e i task che possono eseguire:

App ereditata in uno spazio delegato

- Le valutazioni o recensioni esistenti al momento della delega vengono ereditate e sono visibili agli utenti nello spazio delegato, incluso il nome utente dell'autore.
- L'amministratore delegato non può eliminare le valutazioni/recensioni di un'app ereditata.
- L'amministratore delegato non può esportare le valutazioni/recensioni di un'app ereditata.
- Gli utenti negli spazi delegati possono aggiungere valutazioni/recensioni all'app ereditata.
- Gli utenti negli spazi delegati possono visualizzare le valutazioni/recensioni aggiunte dagli utenti negli spazi delegati, incluso il nome utente dell'autore.

App in uno spazio delegato (aggiunta, non ereditata)

- Solo l'amministratore globale può attivare o disattivare le recensioni da **App > Impostazioni catalogo > Valutazioni e recensioni.**
- Gli utenti negli spazi delegati possono aggiungere valutazioni/recensioni.
- L'amministratore delegato può eliminare le recensioni aggiunte dagli utenti nello stesso spazio delegato.
- Gli utenti in altri spazi delegati, incluso quello predefinito, non possono visualizzare le valutazioni o recensioni aggiunte dagli utenti in ciascuno spazio delegato.
- L'amministratore delegato può esportare le recensioni aggiunte da tutti gli utenti, inclusi i nomi utente.

App delegata in uno spazio predefinito

- L'amministratore globale può eliminare le valutazioni o recensioni aggiunte da un utente in uno spazio delegato.
- L'amministratore globale può esportare tutte le valutazioni o recensioni, incluse quelle aggiunte dagli utenti negli spazi delegati.
- Gli utenti nello spazio predefinito possono visualizzare le valutazioni/recensioni aggiunte dagli utenti negli spazi delegati, incluso il nome utente.

Priorità di uno spazio delegato

Lo spazio predefinito in un sistema UEM ha sempre la priorità più bassa. La priorità di uno spazio delegato rispetto ad altri spazi delegati viene impostata da un amministratore globale e può essere modificata in qualsiasi momento. Gli spazi delegati vengono elencati in ordine di priorità, dal livello di priorità più alto a quello più basso, nella pagina degli spazi sotto la scheda Amministratore nel portale Amministratori.

Delega tramite eredità o copia

Un concetto chiave dell'amministrazione delegata è se un componente di sistema viene ereditato o copiato dallo spazio predefinito.

12.1.6.2. Gestione degli spazi

Gli spazi consentono di designare i dispositivi per la gestione tramite diversi amministratori (amministrazione delegata). L'amministratore di una partizione dei dispositivi può definire le configurazioni e le policy applicate ai dispositivi nella partizione. Una volta creati gli spazi, è possibile assegnare ognuno di essi all'amministratore corretto.

Questa pagina dello spazio include:

- Funzionalità di ricerca per individuare rapidamente gli spazi.
- Controlli di paginazione per navigare in un gran numero di spazi.
- Controlli di prioritizzazione dello spazio per la gestione dell'ordine dello spazio delegato.
- Opzioni per selezionare ed eliminare più spazi.

> Lo spazio predefinito non può essere eliminato.

- Ordinamento alfabetico degli spazi.
- Un elenco di spazi visualizzati di recente nel selettore di spazi.
- Selezione dello spazio persistente tra le pagine Dispositivi, Configurazioni, Criteri e Contenuto, riducendo la necessità di riselezionare uno spazio durante la navigazione tra le pagine.

> L'utente può visualizzare solo gli spazi assegnati e non tutti gli spazi disponibili. A partire da ora, questa impostazione si applica solo ai moduli **Dispositivi**, **Gruppi di dispositivi**, **App**, **Inventario app**, **Contenuto**, **Configurazioni**, **Criteri** e **Gestione dei certificati**. Gli spazi selezionati dall'elenco Spazi durante la visualizzazione di uno di questi moduli sono salvati come selezione predefinita preferita dall'amministratore per quel modulo. Queste preferenze non sono solo salvate per la sessione di login corrente, ma anche per le sessioni future.

Gli spazi creati ereditano tutte le configurazioni dallo spazio predefinito. Pertanto, ogni configurazione creata successivamente nello spazio predefinito è idonea a essere applicata agli altri spazi. Tuttavia, le modifiche apportate a configurazioni già esistenti non vengono ereditate.

Gli spazi creati ricevono copie delle sole policy esistenti nello spazio predefinito in quel momento. Ogni policy creata successivamente nello spazio predefinito si applica solo allo spazio predefinito.

Creare le regole che definiscono i dispositivi presenti all'interno dello spazio. È possibile filtrare le regole utilizzando gli operatori applicabili, inclusi "inizia con", "termina con", "contiene", "non contiene", "non inizia con", "non termina con", "è inferiore a", "è superiore a", "è compreso" e "è uguale a" e "non è uguale a". Le regole possono essere nidificate insieme utilizzando le opzioni QUALSIASI (OR) o TUTTO (AND). È possibile verificare l'accuratezza delle regole utilizzando il testo visualizzato alla fine delle regole.

Il portale per l'amministratore di Ivanti Neurons for MDM visualizza il numero di gruppi di utenti duplicati e il numero corrispondente di GUID per identificare gruppi duplicati quando si seleziona l'attributo Nome gruppo di utenti nel Generatore di regole. Inoltre, una tabella sotto questa regola visualizza l'elenco di gruppi di utenti duplicati e i relativi dettagli, ad esempio Nome gruppo di utenti, GUID, Origine e Nome distinto (DN).

Le regole consentono di identificare i dispositivi mediante:

- Entra ID registrato
- Supporto APNS

- Numero di serie alternativo (solo Android, applicabile ai dispositivi Samsung nella modalità Amministratore del dispositivo o Proprietario dispositivo)
- Abilita Sezionamento rete Android 5G
- Dispositivo Android di lavoro gestito in modalità non GMS (AOSP) abilitato
- Dispositivi dedicati Android
- Compatibile con Android Enterprise
- Dispositivo gestito Android con profilo di lavoro
- Tipo di attestazione SafetyNet di Android
- Android for Work abilitato
- Livello di patch di sicurezza di Android (dispositivi Android)
- Dispositivi di lavoro gestiti Android (proprietario del dispositivo) abilitati
- Profilo di lavoro Android abilitato
- Profilo di lavoro Android abilitato su dispositivi di proprietà dell'azienda abilitati
- Stato nativo anti-phishing
- Stato anti-phishing
- Stato VPN anti-phishing
- Registrato con Registrazione automatica dispositivo
- Automated Registrazione dispositivi abilitato
- Registrato come Autopilot
- Codice stato client Azure
- Ora report di conformità dispositivo Azure
- Stato di conformità dispositivo Azure
- Identificatore dispositivo Azure
- Sentry bloccato
- Accesso bloccato
- Token bootstrap disponibile
- Tipo di provisioning in blocco (Configuratore Apple o Nessuno)
- Gestore telefonico
- Ultimo check-in del client
- Client registrato
- Conformità
- Azione di conformità bloccata
- Nome paese attuale (selezionare il nome del paese dall'elenco a discesa)
- MCC attuale
- MNC attuale
- Attributo dispositivo personalizzato
- Attributo LDAP personalizzato

- Attributo utente personalizzato
- Roaming dati
- Origine dispositivo
- Tipo di dispositivo
- Tipo di dispositivo (Apple)
- Nome visualizzato
- Crittografia abilitata
- Nome paese principale (selezionare il paese principale dall'elenco a discesa)
- MCC nazionale
- MNC nazionale
- IMEI
- IMEI2 (solo su dispositivi Android con doppia porta SIM e applicabile a dispositivi Android 8.0 o superiori)
- Chiave recupero istituzionale abilitata
- Indirizzo IP
- Modalità tutto schermo
- Ultimo check-in
- Modalità smarrimento abilitata
- Solo MAM
- Produttore
- Stato attivazione MTD
- Modalità multiutente
- Sistema operativo
- Versione SO
- Sistema operativo con versione
- Proprietà
- Chiave di recupero personale abilitata
- N. di telefono
- In quarantena
- Blocco di ripristino abilitato
- Roaming
- Stato Secure Apps
- Numero di serie
- Stato
- Supervisionato
- Versione di build supplementare
- Sistema operativo/Versione supplementare Extra
- Token di sblocco disponibile (iOS)

- Registrazione utente completata
- Gruppo di utenti
- Nome utente
- Chiamate in roaming
- Chiave di ripristino personale macOS depositata
- Tipo chiave di ripristino macOS

> Queste regole sono disponibili solo per licenza **Silver** e superiore.

Creazione di uno spazio

Procedura

1. Andare in **Amministratore** > **Sistema** > **Spazi**.
2. Fare clic su **Crea spazio**.
3. Immettere un nome Spazio.
4. Configurare le regole e le impostazioni appropriate per lo spazio.
5. Fare clic su **Salva**.

Assegnazione della priorità agli spazi

Ivanti Neurons for MDM valuta gli spazi in ordine di apparizione

Procedura

1. Fare clic su **Assegna priorità spazi**.
2. Selezionare l'icona su o giù accanto a uno spazio per regolarne la priorità.
3. Fare clic su **Salva**.

Eliminazione di spazi

1. Andare in **Amministratore** > **Sistema** > **Spazi**.
2. Selezionare uno o più spazi utilizzando le caselle di controllo.
3. Fare clic su **Elimina**. Confermare l'eliminazione quando richiesto

Assegnazione di un amministratore a uno spazio

Procedura

1. Andare a **Utenti**.
2. Cercare l'utente che diventerà l'amministratore.
3. Fare clic sul collegamento per la visualizzazione dei dettagli dell'utente.
4. Selezionare **Azioni** > **Assegna ruoli**.
5. Selezionare **Gestione dispositivi**.
6. In **Gestione dispositivi**, selezionare lo spazio per l'amministratore.

7. Fare clic su **Fine**.

Quando l'amministratore effettua l'accesso, saranno visibili solo i dispositivi, le configurazioni e le policy nello spazio assegnato.

Clonazione di una configurazione o una policy

È possibile clonare una configurazione o una policy se è necessario duplicarle con poche differenze. È inoltre possibile associare la configurazioni o le policy clonate a diversi gruppi di dispositivi. Tutte le policy possono essere clonate all'interno di uno spazio. Tutte le configurazioni, tranne il certificato di identità fornito dall'utente e Threat Defense, possono essere clonate all'interno di uno spazio. Anche le seguenti configurazioni possono essere clonate tra spazi dallo spazio predefinito:

- Restrizioni iOS
- Clip Web
- Certificato
- Passcode
- SCEP (iOS e Windows)
- Certificato di identità (generato dinamicamente)

- Il nome di una configurazione o policy dovrebbe essere univoco in uno spazio. Tutte le altre proprietà di una configurazione o policy possono essere clonate.
- Le configurazioni verranno clonate per tutti gli spazi a cui l'amministratore ha accesso. Non è necessario essere un Amministratore globale per la clonazione di una configurazione.

Procedura

1. Andare a **Configurazioni** o **Policy** in base a ciò che si desidera clonare.
2. Fare clic sul collegamento della configurazione o policy per visualizzare i dettagli.
3. Fare clic sull'icona **Clona**.
4. Nella finestra a comparsa, immettere un **nome** ed eventualmente una **descrizione**.
5. Fare clic su **Avanti**.
6. Modificare la configurazione o la policy secondo le proprie esigenze.
7. Fare clic su **Avanti**.
8. Configurare la distribuzione.
9. Fare clic su **Fine**.

Per ulteriori informazioni, vedere Esempi di spazi.

12.1.6.3. Esempi di spazi

Questo argomento fornisce esempi relativi a come gli spazi possono essere utilizzati dagli amministratori.

Amministratore per posizione

ACME, Inc. ha uffici in Nord America e in Europa. A causa di problemi relativi alla lingua e al fuso orario, ACME vuole un amministratore negli Stati Uniti per la gestione dei dispositivi dell'America del Nord e un amministratore in Germania per la gestione dei dispositivi dell'Europa.

Per impostare tali spazi, ACME ha apportato le modifiche seguenti:

1. È stato creato un gruppo di utenti in Ivanti Neurons for MDM per gli utenti in Europa.
2. È stato creato un gruppo di utenti in Ivanti Neurons for MDM per gli utenti in Nord America.
3. Spazio dell'Europa creato con la regola seguente:
4. Gruppo utenti = Europa
   Spazio dell'America del Nord creato con la regola seguente:
5. Gruppo utenti = America del Nord
   Ruolo di Gestione dispositivi per ogni spazio assegnato all'amministratore corretto.

Attualmente ACME dispone dei seguenti spazi:

- Europa
- America del Nord
- Predefinito

Amministratore per sistema operativo per posizione

ACME ha deciso che i dispositivi Android saranno amministrati solo da esperti Android. Un esperto Android è stato aggiunto all'organizzazione dell'America del Nord e un altro esperto è stato aggiunto all'organizzazione europea. Per questo motivo sono necessari due nuovi spazi.

Per aggiungere gli spazi, ACME ha apportato le seguenti modifiche:

1. Spazio dell'Europa-Android creato con la regola seguente:
2. Gruppo utenti = Europa
   SO = Android
   Spazio dell'America del Nord-Android creato con la regola seguente:
3. Gruppo utenti = America del Nord
   SO = Android
   Ruolo di Gestione dispositivi per ogni spazio assegnato all'amministratore corretto.

Attualmente ACME dispone dei seguenti spazi:

- Europa-Android
- America del Nord-Android
- Europa
- America del Nord

- Predefinito

Amministratore per manager

I manager ACME hanno deciso di volere un servizio speciale da un amministratore speciale. Solo i manager più importanti compaiono su questo elenco.

Per aggiungere questo spazio, ACME ha apportato le seguenti modifiche:

1. Spazio dei dirigenti creato con la regola seguente:
2. Nome utente = jdoe@acme.com
   Nome utente = gkunz@acme.com
   Nome utente = prizzo@acme.com
   Nome utente = fvanhoff@acme.com
   Spazio spostato in cima all'elenco nella pagina **Spazi**.
3. Altrimenti, i manager con dispositivi Android avrebbero l'ammministratore sbagliato.
   Ruolo di Gestione dispositivi per lo spazio assegnato all'amministratore speciale.

Attualmente ACME dispone dei seguenti spazi:

- Manager
- Europa-Android
- America del Nord-Android
- Europa
- America del Nord
- Predefinito

Amministratore per tutti gli altri dispositivi

Quando ACME aprirà un nuovo ufficio in Giappone, i dispositivi aggiunti verranno assegnati all'amministratore dello spazio predefinito fino alla creazione di uno spazio del Giappone.

12.1.6.4. Delega di dispositivi

Gli spazi vengono utilizzati per dividere i dispositivi in entità gestite separatamente. L'appartenenza agli spazi viene determinata dalle regole create. La delega dei dispositivi consente a un amministratore globale di dividere e gestire separatamente i dispositivi in un sistema UEM. Quando i dispositivi sono delegati, è possibile assegnarne l'accesso a un sottoinsieme di amministratori delegati, distribuendo in questo modo le responsabilità di amministrazione.

I dispositivi delegati possono essere raggruppati in gruppi di dispositivi ed è possibile applicare loro diverse configurazioni personalizzate senza incidere sui dispositivi situati nello spazio predefinito o in altri spazi.

Creazione di regole per la delega dei dispositivi

Le regole definite per uno spazio determinano quali dispositivi appartengono allo spazio. Un dispositivo può appartenere soltanto a uno spazio. I dispositivi che non soddisfano le regole degli spazi creati automaticamente appartengono allo spazio predefinito.

1. Selezionare **Qualsiasi** se si desidera che i dispositivi vengano inclusi in questa definizione se soddisfano una regola qualsiasi.
2. Selezionare **Tutte** se si desidera che i dispositivi vengano inclusi in questa definizione soltanto se soddisfano tutte le regole.
3. Selezionare uno dei tipi di regola seguenti dal menu a discesa:
    - **Attributo LDAP personalizzato:** per le regole basate sugli attributi LDAP.
    - **Sistema operativo**: per le regole basate sul sistema operativo del dispositivo.
    - **Gruppo di utenti**: per le regole basate sul gruppo di utenti del dispositivo (come definito nel servizio di gestione del dispositivo).
    - **Nome utente**: per le regole basate sul nome utente associato al dispositivo.
4. Definire i criteri per il tipo di regola selezionato:
    - **Attributo LDAP personalizzato:** immettere il nome dell'attributo LDAP personalizzato configurato nelle impostazioni LDAP.
    - **SO**: selezionare Android, iOS, macOS o Windows .
    - **Gruppo di utenti**: selezionare uno dei gruppi di utenti visualizzati nel menu a discesa. Questi sono i gruppi di utenti definiti in **Utenti > Gruppi di utenti**.
    - **Nome utente**: digitare un nome utente.
5. Per aggiungere un'altra regola per lo spazio, fare clic sul pulsante + accanto alla regola precedente.
6. Fare clic su **Anteprima** per visualizzare quali dispositivi verranno assegnati allo spazio.
7. Fare clic su **Salva** se tutti i dispositivi desiderati si trovano all'interno dello spazio.

I dispositivi che non corrispondono più alle regole di uno spazio vengono spostati automaticamente nello spazio corrispondente successivo. Se il dispositivo non soddisfa le regole di nessuno spazio esistente, verrà spostato nello spazio predefinito. Ad esempio, rimuovere un utente da un gruppo di utenti potrebbe causare lo spostamento del dispositivo dell'utente in un altro spazio. Gli spostamenti in spazi diversi possono causare modifiche delle policy e delle configurazioni.

12.1.6.5. Delega di app

La delega delle app consente a un amministratore globale di dividere e gestire separatamente le app in Ivanti Neurons for MDM. L'amministratore globale può acquisire e distribuire a livello centrale app pubbliche e interne, mantenendo allo stesso tempo la separazione e il controllo offerti dagli spazi delegati.

Distribuendo un'app a livello centrale, l'amministratore globale può definire in anticipo il comportamento di gestione dell'app tramite le configurazioni delle app nonché le regole di distribuzione delle app. L'app può quindi essere delegata e resa disponibile nell'App Catalog dello spazio delegato.

L'app delegata viene quindi distribuita agli utenti all'interno di un determinato spazio delegato. Quando le applicazioni sono delegate, è possibile assegnarne l'accesso a un sottoinsieme di amministratori delegati, distribuendo in questo modo le responsabilità di amministrazione.

La delega delle app richiede che prima vengano definiti uno o più spazi delegati. Quando un'applicazione viene delegata, viene assegnata a tutti gli spazi. Lo spazio di delega delle app è classificato come segue:

- Spazio predefinito
- Spazi delegati

Aggiunta di un'app a uno spazio delegato

Un'applicazione può essere aggiunta a uno spazio delegato da un amministratore delegato o globale. L'app viene visualizzata solo nell'App Catalog dello spazio delegato a cui è stata aggiunta. Se si aggiunge un'app precedentemente delegata da uno spazio predefinito a uno spazio delegato, verrà restituito un errore. In questo caso, è necessario prima disattivare l'eredità dell'app nello spazio predefinito in modo che possa essere aggiunta a uno spazio delegato. Per ulteriori informazioni, consultare **Aggiunta di una configurazione** in **Utilizzo delle configurazioni**.

Distribuzione di app in uno spazio delegato

Quando un'app viene delegata da uno spazio predefinito, le relative regole di distribuzione vengono ereditate. Tale app verrà distribuita a tutti i dispositivi assegnati allo spazio delegato che corrisponde alle regole di distribuzione dell'app.

Gli amministratori globali possono delegare gli amministratori di spazi per modificare il certificato di identità generato dinamicamente per tutti i dispositivi e per l'opzione di distribuzione personalizzata.

> Le modifiche alla distribuzione sono applicabili solo allo spazio specifico. Tutti gli altri spazi continuano a ereditare le impostazioni di distribuzione predefinite.

> Impostazioni di approvazione app per le app Android: le impostazioni di approvazione app per spazio per le app Android non sono supportate. Le app approvate nello spazio personalizzato hanno effetto in tutti gli spazi.

> App del catalogo Android esistenti: sui tenant in cui sono già state aggiunte app Android pubbliche nello spazio predefinito, le app non devono risultare delegate prima che l'app pubblica possa essere aggiunta in un altro spazio non predefinito.

Le app Android Enterprise possono essere aggiunte solo dall'amministratore a livello di tenant e **non** dall'amministratore a livello di spazio. Managed Google Play è configurato a livello di organizzazione, non per spazio delegato. Di conseguenza, le nuove app Android Enterprise possono essere approvate solo nello spazio predefinito. Gli amministratori delegati possono assegnare e gestire app già approvate all'interno dei propri spazi, ma non possono approvare o aggiungere nuove app Android Enterprise all'interno di spazi delegati. Tutte le nuove app devono prima essere approvate nello spazio predefinito e solo allora possono essere assegnate ai gruppi appropriati.

Per ulteriori informazioni, consultare **Aggiunta di una configurazione** in **Utilizzo delle configurazioni**.

12.1.7. Amministratori di supporto

Creare un amministratore di supporto temporaneo per consentire al team di assistenza di accedere con i ruoli e le autorizzazioni in uso dall'utente. Questo account utente scade automaticamente dopo 7 giorni; è possibile tuttavia, terminarne l'accesso in qualsiasi momento. La creazione di un amministratore di supporto semplifica la risoluzione di problemi da parte del team di assistenza.

Creazione di un amministratore di supporto

Procedura

1. Nella pagina **Amministratori di supporto**, fare clic su **Aggiungi utente di supporto**.
2. Fare clic su **Crea utente** per confermare.

In seguito a questo passaggio, viene inviata un'e-mail al team di supporto per la gestione del dispositivo.

> Il campo **Nome visualizzato** rimane "(disattivato)" finché un membro del team di supporto non attiva il nuovo account. Il nome visualizzato risultante sarà nel formato seguente:

support-[random_ID]-[your_username]@[your_company].com

Dopo aver creato l'amministratore di supporto, selezionando **Amministratore > Amministratori di supporto** si verrà reindirizzati direttamente all'elenco degli amministratori di supporto esistenti. Pertanto, se è necessario creare ulteriori utenti di supporto, andare direttamente al passaggio 2 descritto sopra.

> Gli account Amministratore supporto creati di recente sono di sola lettura per impostazione predefinita. I ruoli personalizzati non sono assegnati automaticamente, riducendo il rischio di modifiche non intenzionali alla configurazione. Un amministratore può aggiungere ruoli e autorizzazioni in un secondo momento, se necessario.

Visualizzazione della cronologia utente

Nella pagina **Support Administrators**, fare clic su **Cronologia utente** per visualizzare la cronologia di accesso degli amministratori del supporto. La disponibilità dei dati della cronologia di accesso nella pagina Support Administrators è limitata agli ultimi 90 giorni di dati.

Interruzione dell'accesso per un amministratore di supporto

Procedura

1. Nella pagina **Amministratori di supporto**, fare clic sul collegamento **Elimina** a destra dell'account che si desidera rimuovere.
2. Quando richiesto, fare clic su **Rimuovi utente** per confermare.

Sospensione dell'accesso per un amministratore di supporto

Nella pagina **Amministratori di supporto**, fare clic sul collegamento **Disattiva** a destra dell'account che si desidera sospendere.

12.1.8. Admin > Notifica di utilizzo del sistema

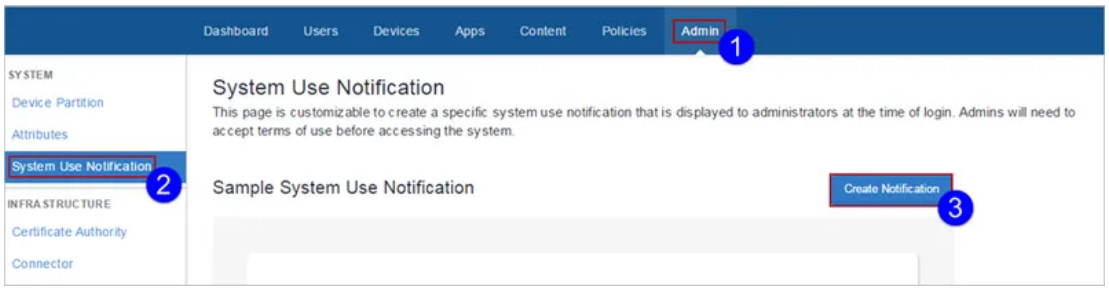
Licenza: Silver

Utilizzare la funzione Notifica di utilizzo del sistema per creare una notifica di utilizzo del sistema personalizzata che venga mostrata all'amministratore al momento dell'accesso. Prima di accedere al sistema, l'amministratore dovrà accettare le condizioni di utilizzo.

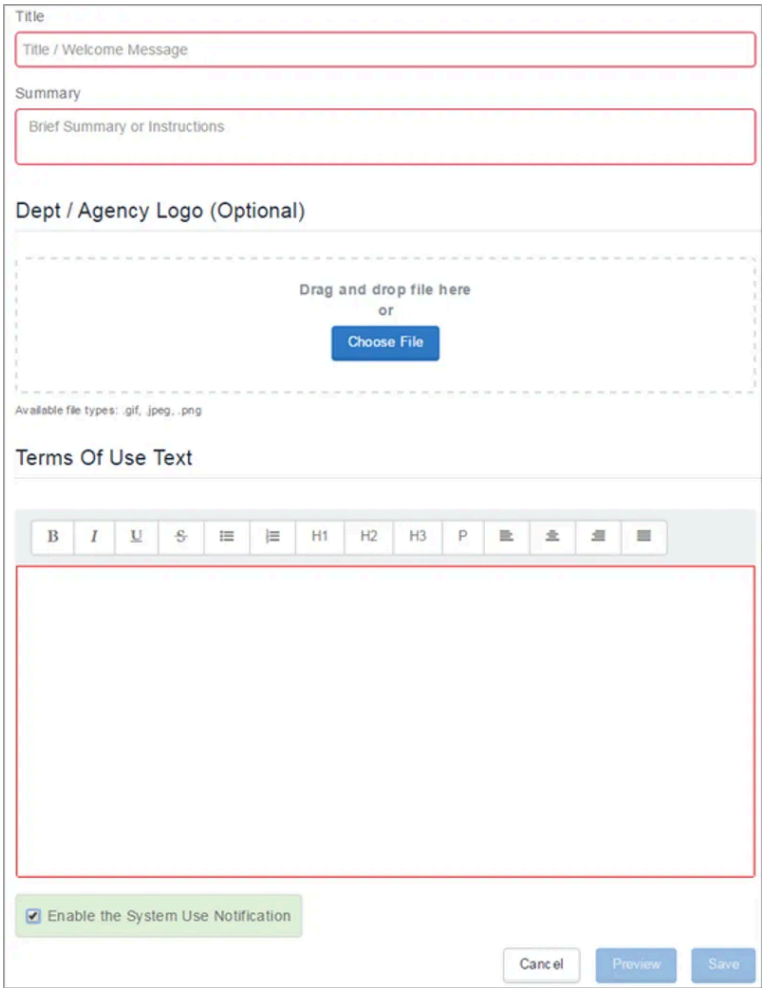
Creazione di una notifica di utilizzo del sistema

Procedura

1. Selezionare **Amministratore > Notifica di utilizzo del sistema**.
2. Fare clic su **Crea notifica**.



Viene visualizzata la pagina Dettagli di notifica di utilizzo del sistema.



Immettere un titolo nel campo **Titolo**.

4. Immettere un riepilogo o istruzioni nel campo **Riepilogo**.
5. Se lo si desidera, scegliere un logo.
6. Immettere il testo relativo alle condizioni di utilizzo nel campo **Testo relativo alle condizioni di utilizzo**. Si tratta del testo che l'amministratore dovrà accettare al momento dell'accesso.
7. Posizionare un segno di spunta nella casella di controllo **Abilita la notifica di utilizzo del sistema** per attivare le notifiche.
8. Fare clic su **Anteprima** per visualizzare un'anteprima della notifica di utilizzo del sistema.
9. Fare clic su **Salva** quando si è soddisfatti della notifica di utilizzo del sistema.

12.2. Infrastruttura

Argomenti della sezione:

- Accesso
- Elenchi di app
- Esportazione degli Audit trail
- Gestione certificati
- Configurazione SCEP per autorità di certificazione esterna
- Provider di credenziali derivate
- Connettore
- Utilizzo del comando httpproxy per Connettore
- Help@Work
- Identità dell'infrastruttura
- Configurazione del server LDAP
- Sentry
- Abilitare l'Autenticazione Kerberos tra Ivanti Neurons per MDM e il server SCEP

12.2.1. Accesso

Applicabile a: dispositivi iOS e Android.

Access garantisce la sicurezza dei dati aziendali consentendo allo stesso tempo un'esperienza utente semplificata e produttiva s qualunque dispositivo o app. Inoltre stabilisce un confine per i dati che impedisce agli utenti di accedere ai servizi cloud aziendali su dispositivi, app o servizi cloud non sicuri.

Documentazione più recente

Visitare la pagina della **Documentazione dei prodotti** e fare clic su Access per ulteriori informazioni su Access e su come configurarlo. Selezionare il documento appropriato per la versione di Access desiderata.

12.2.2. Elenchi di app

Licenza: Silver

È possibile creare elenchi di app consentite, non consentite e richieste da utilizzare con la **policy App consentite**. Questi elenchi possono essere utilizzati nella policy per specificare le azioni da eseguire quando le app installate su un dispositivo non soddisfano i requisiti indicati negli elenchi di app. Non è possibile modificare gli elenchi di app dopo averli creati perché vi si può fare riferimento nelle **policy App consentite**. Analogamente, non è possibile eliminare gli elenchi di app a cui si fa riferimento in una qualsiasi delle policy App consentite.

Creazione di elenchi di app

Procedura

1. Fare clic su **Amministratore > Infrastruttura > Elenchi app**.
2. Fare clic su **Crea nuovo elenco**.
3. Nella casella **Nome elenco app**, inserire un nome per l'elenco.
4. Selezionare il tipo di elenco, **Lista bianca**, **Lista nera** o **Richiesti**.
5. Nella sezione **Aggiungi app**, selezionare il tipo di app, **App Store**, **OS X store**, **Google Play** o **Catalogo app**.
6. Immettere i criteri di ricerca per restringere le opzioni di scelta.
7. Utilizzare le caselle per selezionare le app. È possibile utilizzare ricerche multiple e selezionare più di una casella.
8. Fare clic sulla scheda **Visualizza app** per consultare un elenco delle app selezionate finora.
   Fare clic su **Salva**.

È possibile utilizzare questo elenco quando si configura la policy **App consentite**.

Se non è possibile visualizzare la pagina **Elenchi di app**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione sistemi
- Sistema di sola lettura

12.2.3. Esportazione degli Audit trail

L'esportazione degli Audit trail è una funzionalità utilizzata per esportare e caricare tutte le informazioni degli Audit trail in un percorso specifico del server. Il server è accessibile dalla porta predefinita. Gli utenti possono configurare le impostazioni di esportazione degli Audit trail per attivare il caricamento automatico giornaliero degli Audit trail in un percorso specifico.

> L'esportazione degli Audit trail è supportata sui server SFTP basati su Linux e basati su Windows.

Per configurare le impostazioni di esportazione degli Audit trail, procedere come segue:

1. Selezionare **Amministratore > Infrastruttura > Audit trail**. Viene visualizzata la pagina **Audit trail**.
2. Nella pagina **Audit trail**, fare clic su **ON** per attivare l'esportazione degli Audit trail.
3. Nella sezione **Esporta**, aggiornare i campi seguenti:

Funzionalità	Descrizione
Formato di esportazione	Selezionare uno dei seguenti formati in cui i dati degli Audit trail devono essere esportati: • **JSON** • **CEF** (Formato evento comune) Il messaggio di registro CEF contiene i seguenti valori predefiniti: ◦ Versione: numero di versione del formato CEF. V25 è la versione corrente supportata. ◦ Fornitore dispositivo: Ivanti Inc ◦ Prodotto dispositivo: Ivanti Neurons for MDM ◦ Versione del dispositivo: Ultima versione di Ivanti Neurons for MDM al momento della generazione di un evento. ◦ ID classe evento dispositivo: ID entità univoco per itinerario ◦ Nome: nome di entità e di azione per itinerario. Esempio: creazione impostazioni di configurazione per la distribuzione di una promozione. ◦ Gravità: specifica l'importanza dell'evento. Esempio: Bassa. Il messaggio di registro CEF include anche i campi di estensione che sono una raccolta delle seguenti coppie chiave-valore: ◦ CS1 e CS1Label: metadati degli Audit trail, createdAt, entityType, entityName e actionType. ◦ CS2 e CS2Label: informazioni attore. ◦ CS3 e CS3Label: prima dello stato di azione. ◦ CS4 e CS4Label: dopo lo stato di azione. Nell'esportazione di CEF, se uno qualsiasi dei campi (ad esempio: le chiavi CS3 o CS4) supera i limiti specificati, il valore effettivo viene sostituito con il testo "Il valore di questa chiave supera la lunghezza consentita della chiave dizionario mappata".
Server	Immettere il nome del server per esportare gli Audit trail.
Utente	Immettere il nome utente per accedere al server.
Password	Immettere la password di accesso al server.
Percorso server	Immettere il percorso del server e assicurarsi che tale percorso esista. Esempio: /Utenti/Test/Esportazione.
Algoritmo di scambio chiave	Selezionare l'elenco degli algoritmi di scambio chiave per l'esportazione dell'itinerario di controllo per la configurazione SFTP in uscita. I seguenti algoritmi di scambio chiave sono selezionati per impostazione predefinita: • **diffie-hellman-group-exchange-sha1** • **diffie-hellman-group14-sha1** • **curve25519-sha256** • **diffie-hellman-group-exchange-sha256** (selezionato per impostazione predefinita)
Algoritmi di cifratura	Selezionare l'elenco degli algoritmi di cifratura per l'esportazione dell'itinerario di controllo per la configurazione SFTP in uscita. I seguenti algoritmi di cifratura sono selezionati per impostazione predefinita:

Funzionalità	Descrizione
	• **aes128-ctr** • **aes192-ctr** • **aes256-ctr** (selezionato per impostazione predefinita)
HMAC	Selezionare l'elenco degli algoritmi HMAC per l'esportazione dell'itinerario di controllo per la configurazione SFTP in uscita. • **hmac-sha1 (selezionata per impostazione predefinita)** • **hmac-sha2-256** • **hmac-sha2-512**

I campi menzionati sopra saranno in modalità di sola lettura, se già configurati. Per modificare i campi configurati, fare clic sul pulsante **Modifica**. Se l'amministratore ha già configurato l'esportazione SFTP, dopo l'aggiornamento sono selezionati tutti gli algoritmi chiave.

Fare clic su **Verifica connessione e Salva** per verificare la connessione del server e salvare la configurazione di esportazione degli Audit trail.

I file degli Audit trail archiviati sono disponibili nel formato JSON in un file .zip.

Verificare le impostazioni di configurazione in tutti i campi prima di salvare le impostazioni di esportazione degli Audit trail. Viene visualizzato un messaggio di errore se uno dei valori dei campi inseriti non è valido.

Abilita Audit trail per la registrazione dispositivo e l'annullamento della registrazione negli spazi

Se abilitato, il movimento del dispositivo tra gli spazi viene registrato come audit, inclusi gli eventi attivati dalla registrazione del dispositivo, dall'eliminazione del dispositivo e dall'aggiornamento o eliminazione dello spazio. Gli amministratori dello spazio possono individuare i dispositivi interessati, filtrare i registri per spazio e tipo di attività ed esportare i record di audit in CSV.

12.2.4. Gestione certificati

Licenza: Silver

L'utilizzo dell'autenticazione tramite certificato è un modo efficace per proteggere i dispositivi mobili. I certificati sono più sicuri rispetto alle password e consentono di utilizzare una singola credenziale a protezione di VPN, reti wireless, e-mail ecc. Se l'organizzazione ha accesso a un'autorità di certificazione esterna, è possibile accedervi tramite un Connettore. Se l'organizzazione non ha accesso a un'autorità di certificazione, è possibile utilizzare Ivanti Neurons per MDM come autorità di certificazione. È possibile inoltre utilizzarlo come autorità di certificazione intermedia per altre autorità di certificazione. I certificati generati da Ivanti Neurons per MDM sono denominati certificati autofirmati.

- I certificati SHA-1 perdono l'approvazione quando si creano i certificati d'identità. È possibile scegliere altri algoritmi. Mentre si aggiornano i certificati, se quelli più datati utilizzano SHA-1, può essere utilizzato lo stesso algoritmo SHA-1. Se i certificati meno recenti utilizzano un algoritmo superiore a SHA-1, il ripristino di SHA-1 non è consentito.
- Durante la configurazione dell'autorità di certificazione locale o esterna, selezionare l'opzione **Identità cache su** Ivanti Neurons per MDM per memorizzare i certificati con il servizio Ivanti Neurons per MDM. Svuotare la cache per generare i certificati ogni volta che è necessario.
- I certificati verranno riemessi implicitamente.
- Per migliorare l'efficienza del sistema, i certificati delle configurazioni create dall'amministratore vengono generati non in linea, tramite una coda First In First Out (FIFO). Durante il periodo in cui vengono generate le configurazioni offline, lo stato della configurazione nella colonna **Stato** della scheda **Configurazioni** della pagina **Dettagli dispositivo** sarà **In attesa di generazione certificato**. Una volta generati i certificati, le configurazioni passano allo stato **Installazione in sospeso** e vengono inviate, insieme ai certificati, nei dispositivi tramite check-in forzati automatici.
- Tutti i certificati delle autorità di certificazione, inclusi i certificati firmati dalle autorità di certificazione esterne Piattaforma DigiCert PKI o GlobalSign, vengono revocati quando un dispositivo viene dismesso o cancellato e quando i certificati vengono rigenerati.

L'amministratore può generare certificati Ivanti Neurons for MDM per l'accesso tramite smart card e ID oggetto (OID, Object ID) personalizzati. È possibile generare certificati per le seguenti opzioni di autenticazione:

- Autenticazione client - Abilitata per impostazione predefinita
- IPSEC - Facoltativo, può essere abilitato dall'amministratore
- Accesso smart card - Facoltativo, può essere abilitato dall'amministratore
- OID personalizzati - Facoltativi, possono essere abilitati dall'amministratore

Questa funzionalità è applicabile solo per le seguenti autorità di certificazione:

- Autorità di certificazione locale
- Autorità di certificazione intermedia
- Autorità di certificazione esterna - Configurare le policy di applicazione del modello CA nel server NDES per il supporto di IPSEC, Accesso smart card e OID personalizzati

In Amministratore dispositivi, App Station o altre modalità Enterprise non Android, la Gestione dei certificati non è supportata sui dispositivi Samsung che utilizzano le API Samsung. Si raccomanda di verificare il passaggio ad Android Keystore in base alle raccomandazioni di Samsung.

Per ulteriori informazioni, vedere Configurazione dei certificati.

Connessione a un'autorità di certificazione SCEP in loco

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Installare e configurare un Connettore (**Amministratore > Connettore**). Per ulteriori informazioni, vedere Connettore.
3. Andare in **Amministratore** > **Infrastruttura** > **Gestione certificati**.
4. Fare clic su **Aggiungi** sotto la sezione **Autorità certificato**.
5. Selezionare **Aggiungi un'autorità di certificazione SCEP in loco** e fare clic su **Continua:**
6. Immettere un nome identificativo della configurazione.
7. Selezionare uno dei seguenti tipi di autorità di certificazione:
   - Microsoft
   - EJBCA
   - Server SCEP generico
     È possibile utilizzare l'opzione di server SCEP generico con la maggior parte dei server SCEP avendo una password sfida statica.

Compilare il modulo visualizzato.

9. Fare clic su **Fine**.

Creazione di un'autorità di certificazione esterna

Scegliere questa opzione se si desidera utilizzare un'autorità di certificazione di terze parti.

Procedura

1. Nella pagina **Gestione certificazione**, fare clic su **Aggiungi** nella sezione **Autorità di certificazione**.
2. Nella pagina Aggiungi autorità di certificazione, in Crea un'autorità di certificazione esterna, fare clic su **Continua**.
3. Selezionare GlobalSign o la Piattaforma DigiCert PKI come autorità di certificazione esterna.
4. Compilare i campi rimanenti del modulo visualizzato.
5. Fare clic su **Fine**.

Visualizzazione di un certificato dell'autorità di certificazione esterna

È possibile visualizzare i dettagli di un certificato e caricare il certificato radice intermedio/alternativo per tale autorità di certificazione, con cui sostituire la copia archiviata esistente.

Procedura

1. Nella sezione **Autorità di certificazione**, nella pagina **Gestione certificazione**, fare clic su **Azioni** accanto all'autorità di certificazione esterna, quindi fare clic su **Visualizza certificato**. Viene visualizzata la finestra **Visualizza certificato**.
2. Nella finestra **Visualizza certificato**, fare clic su **Carica certificato**. Viene visualizzata la finestra **Upload Certificate: External CA** (Carica certificato: autorità di certificazione esterna).
3. Fare clic su **Scegli file** per selezionare il certificato da caricare.

4. Fare clic su **Fine**.

Creazione di un'autorità di certificazione intermediaria

- Se è necessario un certificato, generare una CSR e inviarla all'autorità di firma. Caricare il certificato dopo averlo ricevuto dall'autorità di firma.
- Se si dispone già del certificato necessario, caricarlo.

Generare una CSR (certificate signing request, o richiesta di firma di un certificato)

Procedura

1. Nella sezione **Autorità di certificazione**, nella pagina **Gestione certificazione**, fare clic su **Aggiungi**.
2. In Crea un'autorità di certificazione intermediaria nella sezione Aggiungi autorità di certificazione, fare clic su **Genera CSR**.
3. Compilare il modulo visualizzato.
4. Fare clic su **Genera**.
5. Copiare il contenuto compreso tra BEGIN CERTIFICATE REQUEST ed END CERTIFICATE REQUEST in un file di testo.
6. Caricare il file di testo sull'autorità di certificazione.
7. Fare clic su **Fine**.

Caricamento del certificato firmato

Una volta ricevuto il certificato firmato dall'autorità di certificazione, sarà possibile caricarlo.

Procedura

1. Nella sezione **Autorità di certificazione**, nella pagina **Gestione certificazione**, trovare la voce per il CSR generato.
2. Nella sezione, selezionare **Azioni > Carica nuovo certificato firmato**.
3. Fare clic su **Scegli file**.
4. Selezionare il nuovo certificato firmato.
5. Fare clic su **Fine**.

Caricamento di un certificato esistente

Questo argomento descrive come caricare un certificato firmato.

Procedura

1. Nella sezione **Autorità di certificazione**, nella pagina **Gestione certificazione**, fare clic su **Aggiungi**.
2. In Crea un'autorità di certificazione intermediaria nella sezione Aggiungi autorità di certificazione, fare clic su **Carica identità esistente**.
3. Nel campo **Nome**, immettere un nome per il certificato che lo distingua dagli altri.
4. Fare clic su **Carica**.
5. Selezionare il certificato.
6. Immettere la password per il certificato.
7. Fare clic su **Carica**.

Visualizzazione di un certificato dell'autorità di certificazione intermedia

È possibile visualizzare i dettagli di un certificato e ottenere l'URL dell'elenco di revoche di certificati dell'autorità di certificazione.

Procedura

1. Nella sezione **Autorità di certificazione**, fare clic su **Azioni** accanto all'autorità di certificazione e fare clic su **Visualizza certificato**. Viene visualizzata la finestra **Visualizza certificato**.
2. Nella finestra **Visualizza certificato**, è possibile visualizzare l'URL nel campo **URL CRL**.
3. Fare clic su **Copia** per copiare l'URL negli appunti e incollarlo in un'altra applicazione. Questo URL può essere utilizzato per configurare Office 365 in modo che accetti i certificati emessi dall'autorità di certificazione.

Creazione di un'autorità di certificazione indipendente

Scegliere questa opzione se si desidera creare un'autorità di certificazione nuova e completamente indipendente (locale e autofirmata).

Procedura

1. Nella sezione **Autorità di certificazione**, nella pagina **Gestione certificazione**, fare clic su **Aggiungi**.
2. Nella pagina Aggiungi autorità di certificazione, in Crea un'autorità di certificazione indipendente, fare clic su **Continua**.
3. Compilare il modulo visualizzato.
4. Fare clic su **Genera**.

Notifica scadenza autorità di certificazione indipendente

Le informazioni sulla scadenza dell'autorità di certificazione indipendente (locale) sono ora visibili come descrizione comando sotto la colonna **DATA DI SCADENZA** se la data di scadenza del certificato è inferiore a 30 giorni.

Se la data di scadenza è inferiore a 365 giorni, oltre alla notifica inviata, queste informazioni possono essere visualizzate sotto **Dashboard** > **Notifiche**. Selezionare **Scadenza** come filtro.

Configurazione del periodo di scadenza del certificato emesso dall'autorità di certificazione indipendente

È possibile configurare il periodo di validità dell'autorità di certificazione (locale) indipendente.

Procedura

1. Nella pagina **Autorità di certificazione**, nella pagina **Gestione certificazione**, fare clic su **Azioni** accanto all'autorità di certificazione standalone.
2. Fare clic su **Modifica**.
   Viene visualizzata la finestra **Modifica autorità di certificazione**.
3. Nella sezione Modello del certificato client, immettere il nuovo periodo di validità in giorni nel campo **Durata del certificato**.
4. Fare clic su **Salva**.

È possibile ricevere notifiche ed e-mail (se tale opzione è abilitata) quando i certificati emessi da un'autorità di certificazione locale stanno per scadere o sono già scaduti.

- Notifica relativa ai giorni di scadenza dei certificati - Le notifiche vengono generate a intervalli prestabiliti entro la finestra di scadenza dei certificati. La prima notifica viene inviata 365 giorni prima della scadenza, seguita da ulteriori notifiche 180 giorni,

60 giorni, 45 giorni e 7 giorni prima della scadenza. L'utente continuerà a ricevere la notifica finché non sostituisce il certificato accedendo ad **Amministrazione > Gestione certificazione > Azioni > Carica nuovo certificato firmato**.

- Notifica relativa al certificato scaduto - Ricevi una notifica alla scadenza del certificato. Per ripristinare il servizio normale è necessario sostituire il certificato.
- Notifica relativa al caricamento di un nuovo certificato valido - La notifica viene inviata quando il nuovo certificato firmato viene caricato.

Visualizzazione di un certificato dell'autorità di certificazione indipendente

È possibile visualizzare i dettagli di un certificato e ottenere l'URL CRL (elenco di revoche di certificati) dell'autorità di certificazione locale.

Procedura

1. Nella sezione **Autorità di certificazione**, nella pagina **Gestione certificazione**, fare clic su **Azioni** accanto all'autorità di certificazione locale, quindi fare clic su **Visualizza certificato**. Viene visualizzata la finestra **Visualizza certificato**.
2. Nella finestra **Visualizza certificato**, è possibile visualizzare l'URL nel campo **URL CRL**.
3. Fare clic su **Copia** per copiare l'URL negli appunti e incollarlo in un'altra applicazione. Questo URL può essere utilizzato per configurare Office 365 in modo che accetti i certificati emessi dall'autorità di certificazione locale.

Visualizzazione della durata di un elenco di revoche dei certificati per un'autorità di certificazione

È possibile visualizzare e modificare la durata dell'elenco di revoche dei certificati di un'autorità di certificazione locale o intermedia.

Procedura

1. Nella sezione **Autorità di certificazione**, nella pagina **Gestione certificazione**, fare clic su **Azioni** accanto all'autorità di certificazione locale, quindi fare clic su **Modifica**. Viene visualizzata la finestra **Modifica autorità di certificazione**.
2. Nella finestra **Modifica autorità di certificazione**, è possibile vedere il valore della durata dell'elenco di revoche dei certificati. Il valore minimo predefinito è di 24 ore. Il massimo valore che è possibile inserire è 10950 ore.
3. Modificare il valore della durata dell'elenco di revoche dei certificati e fare clic su **Salva**.

Creazione di un'autorità di certificazione cloud

Selezionare questa opzione se si desidera utilizzare un'autorità di certificazione cloud.

Procedura

1. Andare in **Amministratore** > **Infrastruttura** > **Gestione certificati**.
2. Nella sezione **Autorità di certificazione**, nella pagina **Gestione certificazione**, fare clic su **Aggiungi**.
3. Nella pagina **Aggiungi autorità di certificazione**, sotto **Connetti a un'autorità di certificazione cloud di fiducia pubblica**, fare clic su **Continua**.
4. Inserire un nome nella casella **Nome**.
5. Selezionare un'Autorità di certificazione cloud scegliendo fra le opzioni seguenti:
   - **CMS IDnomic Atos**
   - **Piattaforma DigiCert One PKI**
   - **Piattaforma DigiCert PKI**

- **Affida**
- **GlobalSign**

6. Inserire l'URL di base e caricare i dati del certificato.
7. Fare clic su **Fine**.

Utilizzo della Ricerca avanzata per i certificati

È possibile utilizzare l'opzione Ricerca avanzata per cercare i certificati emessi, in base a determinate regole, allo scopo di identificare e visualizzare i certificati che soddisfano criteri specifici. Le regole possono essere costruite utilizzando gli operatori applicabili, tra cui "inizia con", "termina con", "contiene", "non contiene", "non inizia con", "non termina con", "è inferiore a", "è superiore a", "è compreso" e "è uguale a" e "non è uguale a". Le opzioni delle regole possono essere nidificate insieme utilizzando le opzioni QUALSIASI (O) o TUTTO (E). I certificati emessi che soddisfano le regole vengono visualizzati sotto la sezione. A partire dalla release 76 di Ivanti Neurons per MDM, gli operatori per tutti i modelli di gestione certificati hanno operatori standard. Gli operatori dei seguenti modelli sono standardizzati in questa versione:

- Amministratore > Gestione certificati > Certificati emessi > Ricerca avanzata

Ricerca avanzata per i certificati emessi

Procedura

1. Nella sezione **Certificati emessi** della pagina **Gestione certificati**, fare clic sul collegamento **Ricerca avanzata**.
2. Fare clic su **Qualsiasi** se i certificati devono soddisfare almeno una delle regole oppure fare clic su **Tutto**, se devono soddisfare tutte le regole.
3. Creare una regola che definisca i criteri di ricerca per gli attributi seguenti:
   - **CA**
   - **Nome configurazione**
   - **Scadenza**
   - **Chiave privata**
   - **Sistema operativo**
   - **Numero di serie**
   - **Stato**
   - **Tipo di utilizzo**
   - **Utente**
4. (Opzionale) Fare clic su + per creare altre regole, se necessario.
5. (Opzionale) Fare clic **Salva** per salvare la query.
6. Fare clic su **Cerca**. L'elenco degli utenti che soddisfano i criteri di ricerca viene visualizzato nella pagina.

Ricerca avanzata per i certificati forniti dall'utente

Procedura

1. Nella sezione **Certificati utente forniti** della pagina **Gestione certificati**, fare clic sul collegamento **Ricerca avanzata**.
2. Fare clic su **Qualsiasi** se i certificati devono soddisfare almeno una delle regole oppure fare clic su **Tutto**, se devono soddisfare tutte le regole.

3. Creare una regola che definisca i criteri di ricerca per gli attributi seguenti:
    - **Nome certificato**
    - **Data di scadenza**
    - **Emesso da**
    - **Caricato il**
4. (Opzionale) Fare clic su + per creare altre regole, se necessario.
5. (Opzionale) Fare clic **Salva** per salvare la query.
6. Fare clic su **Cerca**. L'elenco degli utenti che soddisfano i criteri di ricerca viene visualizzato nella pagina.

Caricamento delle query di ricerca per i certificati emessi

Per visualizzare l'elenco delle query di ricerca salvate.

Procedura

1. Nella sezione **Certificati emessi** della pagina **Gestione certificati**, fare clic sul collegamento **Ricerca avanzata**.
2. Fare clic sull'icona "Cartella". Viene visualizzata la finestra **Ricerca avanzata**. L'elenco delle query di ricerca create viene visualizzato nella sezione **Carica query**. In questa sezione vengono visualizzati i seguenti dettagli:
    - **Nome query**: nome della query caricata.
    - **Contenuto query**: mostra il contenuto delle regole che definiscono la query di ricerca.
    - **Azioni**: selezionare l'azione da eseguire per la query.
3. Fare clic su **Carica query** nella colonna **Azioni** per visualizzare l'elenco dei certificati emessi che soddisfano i criteri della query caricata.
   Per eliminare una query caricata, fare clic sull'icona Elimina.

> Fare clic su **Esporta in CSV** per scaricare il contenuto del report dei risultati della ricerca in un file CSV, per l'analisi o la consultazione successiva.

Visualizzazione del periodo di scadenza dei certificati emessi

Nella sezione **Certificati emessi**, nella colonna **Scade tra (giorni)** è possibile visualizzare i giorni restanti prima della scadenza del certificato se la data di scadenza è entro i prossimi 30 giorni. Se il certificato era già scaduto negli ultimi 30 giorni, la colonna **Scade tra (giorni)** del certificato mostra il numero di giorni trascorsi dalla data di scadenza.

Per ulteriori informazioni, vedere Configurazione di SCEP per le autorità di certificazione esterne.

Esporta in CSV

È possibile esportare i certificati in un file CSV per successivo riferimento o analisi.

Procedura

1. Nella pagina **Gestione certificati**, passare a una delle seguenti schede.
    - **Certification Authority**
    - **Certificati emessi**
    - **Certificati forniti dall'utente**

2. Fare clic su **Esporta in CSV**.
3. Fare clic su **Download**.
4. (Opzionale) Fare clic su **Elimina** per eliminare il report.

12.2.5. Configurazione SCEP per autorità di certificazione esterna

Questa funzione permette di supportare la configurazione del Simple Certificate Enrollment Protocol (SCEP) per le autorità di certificazione esterne per i dispositivi Windows 10.

> Per questa configurazione è disponibile l'opzione di delega con distribuzione personalizzata. Per ulteriori informazioni, vedere l'argomento *Distribuzione della configurazione* in **Utilizzo delle configurazioni**.

Impostazione di un'autorità di certificazione esterna

È innanzitutto necessario impostare una CA esterna. Se si dispone già di una CA esterna, è possibile passare alla sezione successiva.

1. Andare in **Amministratore > Infrastruttura > Gestione certificati**.
2. Fare clic su **+Aggiungi**.
3. Immettere un nome per l'autorità di certificazione.
4. Utilizzare il menu a discesa per selezionare Microsoft come **Tipo di autorità di certificazione**.
5. Immettere l'**URL SCEP**.
6. Immettere **Nome utente** e **Password**.
7. Immettere **l'URL di verifica**.
8. Fare clic su **Salva**.

Configurazione SCEP

Ora si può procedere con la configurazione SCEP.

1. Andare a **Configurazione > +Aggiungi**.
2. Selezionare l'icona Windows.
3. Selezionare **Certificato di identità** per andare alla pagina **Crea configurazione del certificato di identità**.
4. Immettere un nome per la configurazione.
5. Selezionare **Configurazione Windows** dall'elenco di configurazioni SCEP dal menu a discesa **Distribuzione dei certificati**.
6. Selezionare la CA esterna
7. Inserire i dettagli della distribuzione dei certificati.
    - Inserire l'oggetto. Ad esempio: CN=$
    - Selezionare il numero di tentativi nel menu a discesa **Riprova**.
    - Selezionare il numero di secondi da attendere prima di ciascun inserimento nel menu a discesa **Intervallo tra tentativi**.
    - Selezionare una dimensione chiave nel menu a discesa **Lunghezza della chiave**.
    - Selezionare almeno un'opzione di utilizzo della certificazione.
    - Inserire la durata nel campo **Validità** e nel menu a discesa.
    - Inserire l'identificazione personale CA.

- Andare all'URL richiesta SCEP, copiare l'identificazione personale CA e incollarla qui o fare clic su **Crea da certificato**... per caricare il certificato da cui può essere creata l'identificazione personale CA.
  Selezionare almeno un algoritmo hash nelle opzioni **Famiglia di algoritmi hash**.

8. Fare clic su **Avanti**.

12.2.6. Provider di credenziali derivate

Nella pagina Provider di credenziali derivate è visualizzato l'elenco dei provider di credenziali derivate utilizzati per la distribuzione dei certificati. È possibile specificare il provider di credenziali derivate da impostare come predefinito e aggiungere gli altri provider di credenziali derivate personalizzati in uso.

Per impostare un provider di credenziali derivate come predefinito:

1. Accedere ad **Amministratore > Provider di credenziali derivate**. Nella pagina sono elencati i provider di credenziali seguenti.
    - **Affida**
    - **Intercede**
    - **Purebred**
2. Per il provider che si desidera impostare come predefinito, fare clic su **Imposta come predefinito** nella colonna **Azioni**. Quando è impostata, l'icona del segno di spunta viene visualizzata sotto la colonna **Provider predefinito** per il provider, a indicare che si tratta del provider di credenziali predefinito.

Per aggiungere un provider di credenziali derivate personalizzato:

1. Accedere ad **Amministratore > Provider di credenziali derivate**.
2. Fare clic su **+Aggiungi**.
3. Digitare il nome del provider di credenziali derivate nel campo di testo nella colonna **Nome**.
4. Fare clic su **Salva**.
   Dopo l'aggiunta, il provider di credenziali derivate personalizzato è disponibile come opzione selezionabile nel campo **Marchio** durante la configurazione dell'opzione di distribuzione delle credenziali derivate, nella configurazione **Certificato di identità**.

Per eliminare un provider di credenziali derivate, fare clic su **Elimina** in **Azioni**.

> Il provider di credenziali derivate impostato come predefinito non può essere eliminato.

12.2.7. Connettore

Licenza: Silver

Il connettore Ivanti Neurons for MDM fornisce l'accesso dal servizio Ivanti Neurons for MDM alle risorse aziendali, ad esempio un server LDAP o un'autorità di certificazione (CA). Configurare un Connettore per ciascuna risorsa a cui si desidera accedere.

Se si utilizza Microsoft Active Directory o un server LDAP ospitato in Amazon Web Services (AWS), è possibile ospitare il connettore di Ivanti Neurons for MDM in AWS. Non è richiesto un connettore locale.

Il Connettore viene automaticamente aggiornato all'ultima versione del software.

Per la guida più recente all'installazione di Ivanti Neurons for MDM, visitare **https://help.ivanti.com/#106** e cercare "Connettore".

Opzioni di hosting del Connettore

È possibile ospitare il connettore di Ivanti Neurons for MDM a livello locale nel data center o in Amazon Web Services (AWS):

- Ospitare il Connettore in AWS, se si utilizza Microsoft Active Directory ospitato in AWS o Microsoft Active Directory gestito autonomamente in AWS. In questo caso, non è necessario disporre di un connettore locale.
- Per accedere alle risorse locali, ad esempio un server LDAP o un'autorità di certificazione (CA), configurare il connettore localmente.

Ospitare il Connettore in AWS

I clienti possono ospitare il Connettore in AWS per l'utilizzo con le seguenti opzioni di Microsoft Active Directory ospitate da AWS:

- Servizio Directory AWS per Microsoft Active Directory
- Microsoft Active Directory gestito da cliente in Amazon VPC

Per ulteriori informazioni sul Servizio Directory AWS per Microsoft Active Directory, visitare il sito **https://aws.amazon.com/directoryservice**. Consultare la documentazione di AWS relativa all'hosting di Microsoft Windows Server e Microsoft Active Directory in una sezione di Amazon VPC. Il connettore Ivanti Neurons for MDM supporta Windows Server 2012, 2012 R2, 2015.

Configurazione Connettore AMI Ivanti Neurons for MDM in AWS

Per configurare il Connettore AMI in Ivanti Neurons for MDM:

1. Accedere ad AWS con le credenziali amministratore.
2. Nella pagina dei servizi AWS, selezionare **EC2** in **Calcola**.
3. Espandere **Immagini** e selezionare **AMI** nel riquadro a sinistra.
4. Selezionare **Immagini pubbliche** dall'elenco a discesa nel riquadro a destra.
5. Cercare il connettore Ivanti Neurons per MDM utilizzando parole chiave come "mobileiron-kocab".
6. Selezionare l'ultima versione del Connettore dall'elenco e fare clic su **Avvia**.
7. Seguire le istruzioni per l'installazione del Connettore nella sezione "Distribuzione del connettore Ivanti Neurons for MDM in AWS" nella *Guida all'installazione del connettore Ivanti Neurons for MDM* disponibile all'indirizzo https://help.ivanti.com/mi/help/en_us/cld/*<version>*/inst/default.htm, dove *version* è la versione del connettore Ivanti Neurons for

MDM che si sta installando. Ad esempio, per la versione 74 del connettore Ivanti Neurons for MDM, la guida è disponibile all'indirizzo https://help.ivanti.com/mi/help/en_us/cld/**74**/inst/default.htm.

Ospitare il connettore a livello locale

Per ospitare il connettore Ivanti Neurons for MDM locale nel proprio datacenter, fare clic su **Scarica connettore** per scaricare e impostare il connettore Ivanti Neurons for MDM. Estrarre il contenuto del pacchetto scaricato e seguire le istruzioni di configurazione nella Guida all'installazione del connettore Ivanti Neurons for MDM inclusa nel pacchetto.

Accesso ai registri del Connettore

È possibile accedere ai registri del connettore dal servizio Connettore per contribuire a risolvere i problemi relativi al Connettore. È necessario disporre del ruolo Gestore di sistema o Sistema di sola lettura.

1. Andare in **Amministratore > Connettore** per visualizzare la pagina del Connettore.
   L'interfaccia del Connettore mostra lo stato del Connettore (abilitato o disabilitato), il nome del Connettore, la connessione (connesso o non connesso), il numero di versione, il livello di registrazione e le azioni (disabilitare o rimuovere il Connettore).
2. Utilizzare il menu a discesa **Livello di registrazione** per scegliere un livello.
   I livelli di registrazione disponibili vengono visualizzati nel menu a discesa nell'ordine che va dal livello di registrazione più basso a quello più alto:
   - Errore
   - Avviso
   - Informazioni
   - Debug
   - Traccia

Il livello di registrazione predefinito è Informazioni. Se si sceglie un altro livello di registrazione, viene visualizzata un'icona di sincronizzazione rotante, per indicare che verranno raccolte informazioni al livello di registrazione selezionato. Dopo un'ora, il livello di registrazione viene reimpostato al livello di informazioni. Il Livello di traccia è l'impostazione del livello di registrazione più alto. Utilizzare questo livello per raccogliere tutti i messaggi presenti su tutti gli altri livelli. L'icona di sincronizzazione viene visualizzata per l'intera durata della richiesta.

3. Se necessario, spostare il mouse sull'icona di sincronizzazione per visualizzare l'icona di annullamento . Fare clic sull'icona di annullamento per annullare la modifica del livello di registrazione.
4. Passare con il mouse sull'icona della richiesta per visualizzare l'opzione Richiedi informazioni. Fare clic sull'icona di richiesta per richiedere i file della cartella dei registri corrente sotto forma di file ZIP.
   I file di registro vengono aggiunti a un file zip quando viene eseguita una richiesta. Quando si esegue una nuova richiesta, il file zip della richiesta precedente viene eliminato.
5. Se necessario, spostare il mouse sull'icona di richiesta per visualizzare l'icona di annullamento . Fare clic sull'icona di annullamento per interrompere la richiesta.
   Se una richiesta viene annullata prima del completamento, l'icona di download non viene visualizzata perché il file ZIP di registro precedente era stato eliminato dal server. I file di registro originali presenti sul Connettore sono ancora disponibili per la richiesta.
6. Fare clic sull'icona di download per scaricare il file ZIP di registro contenente i file di registro raccolti durante l'ultima richiesta.
   Il nome del file di registro è nel formato: kocab.log. Il nome del file zip scaricato è composto da nome del server, versione della connessione e da un indicatore data e ora che include giorno, mese, anno e l'ora del giorno nel formato:

<Connector_Hostname>_<Connector_Version>_<TimeStamp>.zip. Il nome del file zip archiviato è nel formato: kocab.aaaa-mm-gg.0.log.gz.

7. A scelta, utilizzare il menu a discesa **Azioni** per disabilitare o rimuovere il Connettore.

Se non è possibile visualizzare la pagina **Connettore**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione sistemi
- Sistema di sola lettura

Per ulteriori informazioni, vedere **Utilizzo del comando httproxy per Connettore**.

12.2.8. Utilizzo del comando httpproxy per Connettore

È stato introdotto un nuovo comando klish della shell per aiutare a modificare la configurazione del Connettore per l'installazione di Ivanti Neurons for MDM. Usare tale comando per modificare le informazioni di accesso e altri parametri per configurare il Connettore.

Il comando httpproxy è ora disponibile in questa release con questi requisiti.

- klish shell

Per configurare il Connettore

1. Accedere alla shell klish.
2. Inserire un ? per un elenco dei comandi di shell klish disponibili.
3. Immettere **httpproxy** per visualizzare il valore attuale di tali parametri:
    1. attivato
    2. schema
    3. server
    4. authtype
    5. nome utente
    6. Password
4. Immettere **httpproxy ?** per visualizzare un elenco di comandi disponibili da utilizzare con httpproxy.
    1. authtype - Impostare il tipo di autenticazione del proxy http su NONE, BASIC o NTLM
    2. disabilita - disabilitazione del proxy http
    3. abilita - abilitazione del proxy http
    4. host - impostazione dell'host del proxy http - deve essere un FQDN o un IP http o https
    5. password - impostazione della password di autenticazione del proxy http
    6. porta - impostazione della porta del proxy http
    7. schema - impostazione dello schema del proxy http - deve essere http o https
    8. mostra - visualizzazione delle impostazioni del proxy http attuali
    9. nome utente - impostazione del nome utente di autenticazione del proxy http
5. Usare i comandi sopra elencati per configurare l'istanza del Connettore.

12.2.9. Help@Work

Licenza: Platinum

Supportato su: i dispositivi Android e iOS sono supportati da Ivanti Neurons per MDM

Utilizzare Help@Work per Android per offrire assistenza remota agli utenti di dispositivi Android e iOS. Help@Work per Android/iOS si basa sull'app TeamViewer QuickSupport. Per utilizzare Help@Work per Android/iOS, è necessario un account TeamViewer. Se non si dispone di un account, visitare teamviewer.com per i dettagli.

Help@Work trasforma l'esperienza di help desk per i dispositivi iOS 11.0+ e Android, consentendo agli utenti di chiedere assistenza con un clic e condividere la schermata con un operatore dell'help desk. Gli utenti non devono più perdere tempo a descrivere il problema e lo staff IT può risolvere i problemi dei dispositivi in modo più efficiente. Questo non è supportato per i dispositivi iOS solo MAM.

> TeamViewer è supportato sui dispositivi Android gestiti dal proprietario in modalità tutto schermo.

> Se l'app esiste o il dispositivo si riavvia, i comandi di avvio di TeamViewer vengono eliminati.

> Nei dispositivi Android, se l'app Teamviewer QuickSupport non è installata all'utente viene richiesto di scaricarla. Nei dispositivi iOS è necessario eseguire il push dell'app tramite il catalogo app. Se è già installata nel dispositivo, deve essere convertita in app gestita.

> Per essere utilizzata per l'applicazione, l'app Teamviewer QuickSupport deve essere in primo piano per la sessione. L'applicazione host TeamViewer è necessaria per la modalità Automatica.

> Per supportare le sessioni remote, la versione desktop dell'applicazione installata dall'amministratore deve essere compatibile con la versione di QuickSupport installata nel dispositivo client.

Configurazione di Help@Work per Android o iOS

Di seguito è riportata la procedura di configurazione da eseguire una sola volta per la personalizzazione e la distribuzione di Help@Work per Android o iOS:

1. Andare alla scheda **Amministrazione**.
2. In Infrastruttura, fare clic su **Help@Work**.
3. **Help@Work** richiede l'utilizzo di TeamViewer. Nella sezione Attiva TeamViewer, attivare l'opzione **TeamViewer Automatica** o **TeamViewer Manuale (solo Android)** facendo clic sul pulsante **Attiva ora** .
4. Leggere il contratto di licenza di TeamViewer e fare clic su **Accetto** per continuare. Ora la licenza Enterprise viene attivata. Questo identifica i clienti Ivanti per TeamViewer, concedendo loro l'accesso.

> L'opzione **Rimuovi attivazione** diventa disponibile all'attivazione di TeamViewer. Quando si fa clic su **Rimuovi attivazione** sotto la sezione **Attiva TeamViewer**, la finestra **Conferma Rimuovi attivazione** appare a schermo. Fare clic su **Rimuovi attivazione** per rimuovere l'attivazione di TeamViewer, che a sua volta rimuoverà la funzionalità Help@Work su tutti i dispositivi supportati. Tuttavia, è possibile attivare TeamViewer utilizzando un account esistente o un account diverso in un secondo momento.

> Se si desidera eliminare l'account **TeamViewer** in modalità Non in presenza, è necessario effettuare il de-provisioning dei dispositivi associati per i quali è abilitata la modalità Non in presenza. Per annullare il provisioning dei dispositivi associati, è necessario annullare la distribuzione dell'app **TeamViewer** dai dispositivi associati ed eseguire un check-in forzato. Assicurarsi che l'app TeamViewer sia stata eliminata da tutti i dispositivi e quindi eliminare l'associazione dell'account dalla console amministrativa.

Distribuire l'app TeamViewer agli utenti con cui si desidera avviare sessioni remote utilizzando il flusso di lavoro standard per la distribuzione delle app. Ciò risulta specifico delle modalità **Manuale** e **Automatica**. Se l'amministratore vuole controllare il dispositivo, il componente aggiuntivo universale o il componente aggiuntivo specifico per OEM/modello di TeamViewer deve essere distribuito anche sul dispositivo. Per istruzioni, vedere Configurazione delle app.

Avvio di una sessione remota utilizzando Help@Work per Android o iOS

Una tipica sessione di Help@Work per Android o iOS inizia con la richiesta di assistenza da parte di un utente finale.

Per avviare una sessione di Help@Work con il dispositivo dell'utente:

1. In Ivanti Neurons per MDM, andare su **Dispositivi**.
2. Nella pagina con l'elenco dei dispositivi, fare clic sul dispositivo che richiede supporto.
3. Dal menu Azioni, fare clic su **Avvia controllo remoto di TeamViewer**, per i dispositivi Android, o su **Visualizzazione remota** per i dispositivi iOS. Appariranno due opzioni:
    - Modalità Manuale (predefinita) - Questa opzione richiede che l'applicazione **TeamViewer Quick Support** sia installata e inserita nella lista bianca del dispositivo di destinazione.
    - Modalità Automatica (disponibile solo su Android) - Questa opzione richiede che l'applicazione **TeamViewer Host** sia installata e inserita nella lista bianca del dispositivo di destinazione.

> Se si desidera inserire nella whitelist i nomi di host o ignorare i criteri di sicurezza dei contenuti, contattare il team di supporto.

> L'opzione modalità Automatica funziona anche in modalità tutto schermo. Dovrebbe essere abilitata dalla pagina di integrazione di TeamViewer. Il controllo remoto Automatico richiede l'applicazione host TeamViewer sul dispositivo, un'attivazione una tantum su un dispositivo e una licenza aggiuntiva MI. Per l'attivazione una tantum, la richiesta di autorizzazione verrà visualizzata quando l'applicazione host di TeamViewer viene installata e avviata per la prima volta. L'amministratore può utilizzare l'opzione "Avvio automatico (impostazioni nella configurazione App gestite)". TeamViewer dopo l'installazione, se lo desidera. Il numero di licenze è calcolato in base alla distribuzione dell'app host di TeamViewer. Se l'applicazione host di TeamViewer viene distribuita su un dispositivo, viene consumata una licenza di sessione host remota Automatica. Oltre all'app host di TeamViewer, possono essere necessarie altre app aggiuntive che devono essere consentite in modalità a tutto schermo o schermo condiviso. Potrebbero essere necessari altri componenti aggiuntivi a seconda del modello e del produttore del dispositivo.

> I dispositivi Google Pixel non conservano questa autorizzazione e richiedono il consenso per ogni sessione.

Se l'amministratore dispone di un token TeamViewer valido, il client desktop inizia con una sessione di supporto per il dispositivo. In caso contrario, l'amministratore dovrà effettuare l'accesso con TeamViewer e concedere le autorizzazioni.

Per avviare rapidamente una sessione remota, gli amministratori possono effettuare prima l'accesso all'applicazione desktop.

Installare TeamViewer

Installare l'app TeamViewer sul desktop per accedere ai dispositivi remoti degli utenti e fornire supporto. Per installare TeamViewer:

1. Scaricare dall'indirizzo seguente il pacchetto di installazione della versione completa di TeamViewer per Mac, Windows o Android:
   https://www.teamviewer.com/it/download
2. Lanciare il programma di installazione di TeamViewer.
3. Selezionare **Installazione di base**.
4. Selezionare **Azienda/Uso commerciale**.
5. Fare clic su **Accetta- fine**.

Richiedere un account TeamViewer

Per fornire supporto con TeamViewer, è necessario disporre di un account di TeamViewer. Per ottenere un account TeamViewer:

1. Visitare il sito https://login.teamviewer.com/.
2. Inserire indirizzo e-mail, nome e password.
3. Fare clic su **Accedi**
4. Utilizzare l'account e-mail inserito nel passaggio 2 per ricevere un'e-mail di attivazione dell'account di TeamViewer.
5. Completare le istruzioni nell'e-mail per attivare l'account TeamViewer.

Confermare l'ID di sessione TeamViewer

TeamViewer genera un'ID di sessione quando si stabilisce una connessione tra il computer dell'amministratore e il dispositivo mobile dell'utente.

1. Quando viene generato l'ID di sessione, Ivanti Neurons per MDM lo passa all'app TeamViewer QuickSupport tramite la configurazione dell'app gestita, che a sua volta lo utilizza per richiamare il client TeamViewer sul dispositivo. Per iOS, l'ID di sessione scade dopo 30 minuti.
2. All'utente viene chiesto di accettare l'EULA di TeamViewer.

12.2.10. Identità dell'infrastruttura

Argomenti della sezione:

12.2.10.1. Configurare il provider di identità

Licenza: Silver

Configurare un provider di identità (IdP) per autenticare gli utenti che desiderano registrare dispositivi con Ivanti Neurons for MDM, accedere al portale Amministratori o accedere al portale self-service. È necessaria una directory utente locale compatibile con LDAP. Ivanti Neurons for MDM funziona con qualsiasi IdP compatibile con SAML 2.0. È stato verificato che l'autenticazione di Microsoft Entra ID (Entra ID), Microsoft ADFS (Active Directory Federation Services), Okta, OneLogin, PingOne e PingFederate di Ping Identity funziona con Ivanti Neurons for MDM.

Nelle versioni precedenti, se si imposta Autenticazione SAML/IdP, l'autenticazione SAML viene utilizzata sia per la registrazione del dispositivo che per l'autenticazione nel portale. Ora, viene fornito un selettore che consente di scegliere metodi di autenticazione diversi per l'accesso al portale Amministratori e la registrazione del dispositivo. Il pulsante di bypass è applicabile solo alla registrazione del dispositivo.

Durante la registrazione del dispositivo, l'amministratore può bypassare l'opzione del provider di identità e fornire all'utente l'opzione di autenticarsi usando un PIN invece di autenticarsi usando la pagina del provider di identità.

Panoramica

- Se si usa Microsoft AD o un'altra directory LDAP locale, è necessario configurare un Connettore per connettersi e importare gli utenti in Ivanti Neurons for MDM. Se non è già stato fatto, configurare un Connettore o **LDAP**.
- Quando viene aggiunto un IdP, l'autenticazione utente passa automaticamente da LDAP a IdP.
- È consentito un solo provider IdP.
- Se l'IdP diventa inaccessibile, utilizzare l'account amministratore tenant (TA, Tenant Admin) di Ivanti Neurons for MDM per accedere al portale Amministratori e risolvere il problema. L'account TA è un account locale e non richiede autenticazione esterna. L'account TA viene creato durante la distribuzione di Ivanti Neurons for MDM e le informazioni vengono fornite al contatto del supporto tecnico dell'organizzazione o a una persona equivalente. Se non si dispone delle informazioni del proprio account TA, contattare il rappresentante dell'assistenza di riferimento.
- Ivanti Neurons for MDM supporta Microsoft Entra ID (Entra ID) per l'autenticazione degli utenti durante la registrazione di dispositivi con Windows 10.

> Impostare il tipo di autenticazione per gli utenti LDAP utilizzando gli strumenti forniti dal proprio fornitore IdP. Lo schema di autenticazione per l'IdP in uso ha la precedenza sulle impostazioni di Ivanti Neurons for MDM. Le impostazioni di autenticazione di Ivanti Neurons for MDM sono disponibili qui: **Utenti > Impostazioni utente > Impostazioni registrazione dispositivo > Tipo di autenticazione per registrazione dispositivi**.

- Le registrazioni dei dispositivi Apple Registrazione dispositivi e Configurator non utilizzano un IdP per l'autenticazione utente.
- Per configurare un provider di identità per la registrazione dei dispositivi iOS e macOS di Apple Business Manager, è necessario abilitare l'opzione **Abilita registrazione personalizzata** e le relative impostazioni **Pagina web Ivanti Hosted** che si trovano in **Amministratore > Apple > Registrazione dispositivi >** *Modifica profilo registrazione dispositivo*. Vedere **Registrazione dispositivo** per maggiori informazioni:



Tipi di configurazione di IdP

La pagina Identità Ivanti Neurons for MDM guida l'utente nella configurazione dei tipi di provider IdP seguenti:

- **Configurazione IdP Ivanti Neurons for MDM**- I provider di identità supportati per Ivanti Neurons for MDM sono Entra ID, OneLogin, Okta e PingOne.
- **Configurazione dell'IdP locale** - I fornitori IdP locali supportati sono ADFS 3,0, PingFederate 8.2.1 e PingFederate 8.1.3.
- **Configurazione dell'IdP generico** - Si tratta di un percorso di configurazione generico da seguire se non si usano Microsoft ADFS, Okta, OneLogin o PingFederate.

Configurazione di un provider di identità (IdP)

Procedura

1. Passare in **Amministratore** > **Identità** > **Autenticazione SAML**.
2. Fare clic su un tipo di impostazione del provider di identità:
    - **Configurazione IDP di Ivanti Neurons for MDM**
    - **Configurazione IDP locale**
    - **Configurazione IDP generico**
3. Selezionare un IdP corrispondente. Se si è selezionato **Configurazione IDP generico** nel punto 3, saltare questo passaggio e continuare dal passaggio 5.
4. Seguire le istruzioni a schermo che appaiono per il proprio IdP prescelto.
5. Fare clic su **Fine**.

> Gli amministratori possono effettuare un Single Sign-On per un massimo di 2 ore dall'autenticazione iniziale con l'IdP.

Attività di configurazione necessarie

In base all'IdP prescelto, si verrà guidati attraverso le seguenti pagine e passaggi associati:

IdP	Procedura
• Entra ID • Okta • One Login • Ping One	• Generazione di una chiave da caricare sull'IdP. • Accesso all'IdP e caricamento della chiave generata. • Esportazione di un file di metadati dall'IdP e importazione del file in Ivanti Neurons for MDM.
• ADSF 3.0 • Ping Federate 8.2.1 • Ping Federate 8.1.3	• Scaricare il file di metadati da Ivanti Neurons for MDM. • Configurazione di un'opzione "Attendibilità del componente" su ADFS o di un'opzione "Connessione SP" su PingFederate e importazione del file di metadati di Ivanti Neurons for MDM. • Esportazione del file di metadati dall'IdP e importazione del file in Ivanti Neurons for MDM.
• IdP generico	1. Scaricare il file di metadati da Ivanti Neurons for MDM. 2. Seguire le istruzioni fornite dal provider di identità (IdP) per configurare il server/servizio IdP in modo da comunicare con il servizio Ivanti Neurons for MDM come "Provider di servizi". Ciò può includere: 1. Caricamento del file di metadati dal Passaggio 1 precedente nel proprio IdP. Questo file di configurazione contiene le informazioni fondamentali per abilitare Ivanti Neurons for MDM, come Provider di servizi SAML 2.0, e comunicare con il Provider di identità SAML 2.0. Gli URL SAML 2.0 standard, i certificati e le impostazioni sono inclusi nel file di metadati. Ivanti Neurons per MDM un IdP compatibile con SAML 2.0 deve essere in grado di importare ed elaborare un file di metadati XML esportato da un Provider di servizi. 2. Configurazione dell'IdP in modo che utilizzi l'algoritmo di crittografia RSA-SHA1 per la firma delle richieste di autenticazione SAML. Le informazioni relative al Certificato di firma utilizzato per verificare le richieste di autenticazione sono incluse nel file di metadati scaricato nel Passaggio 1. 3. Configurare l'IdP in modo che includa un nome utente nelle risposte SAML inviate a Ivanti Neurons per MDM. Impostazione del nome utente nell'elemento [Name Id] della risposta SAML dall'IdP. Esportare un file di metadati dall'IdP e importarlo in Ivanti Neurons per MDM. 3. (Facoltativo) - Includi nome utente nella richiesta di autenticazione SAML: per includere il nome utente dell'utente che si autentica nella richiesta di autenticazione e rimuovere un input aggiuntivo per l'utente durante l'autenticazione con un IdP. Se si attiva questa opzione, è possibile che si verifichino errori di autenticazione. Se si è certi della convalida IdP, selezionare l'opzione **Sono consapevole dell'impatto di questa modifica** e

IdP	Procedura
	attivare/disattivare l'opzione **Includi nome utente nella richiesta di autenticazione SAML** su **ON**. Ivanti Access è un IdP convalidato per questa impostazione.

Autorizzazione per gli utenti locali di aggirare l'autenticazione IdP

Se la connettività di Ivanti Neurons for MDM o dell'IdP si interrompe ed è necessario risolvere il problema sul lato Ivanti Neurons for MDM, alcuni amministratori devono poter accedere a Ivanti Neurons for MDM senza dipendere per l'autenticazione da sistemi esterni, quali LDAP o IdP. Solo gli utenti locali con ruoli di amministratore di sistema possono aggirare l'autenticazione IdP.

Creare un elenco di utenti locali per aggirare l'autenticazione IdP.

Procedura

1. Fare clic su **Amministratore > Identità**.
2. Nella sezione Gli utenti locali aggirano l'autenticazione IdP, fare clic su **+Aggiungi utenti**.
3. Dall'elenco che mostra solo gli utenti locali con il ruolo di amministratore di sistema, selezionare alcuni utenti.
4. Fare clic su **Salva**.

> Per rimuovere un utente dall'elenco di utenti locali che aggirano l'autenticazione IdP, fare clic sull'icona di rimozione accanto alla voce che si desidera eliminare.

Se non è possibile visualizzare la pagina Identità, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione sistemi
- Sistema di sola lettura

12.2.10.2. Provisioning utente con SCIM

Argomenti della sezione:

- Provisioning utente
- Generare un token da Ivanti Neurons per MDM
- Cambia lo Stato token
- Visualizza lo stato del token da audit trail
- Configurare gli attributi nel provisioning SCIM

Provisioning utente

Provisioning utente utilizza il protocollo SCIM per sincronizzare un IdP con Ivanti Neurons per MDM e permette la sincronizzazione parziale di utenti e gruppi. Provisioning utente utilizza il protocollo SCIM per creare e aggiornare automaticamente gli oggetti utente e gruppo da un IdP a Ivanti Neurons for MDM. Proprio come l'attuale integrazione con Entra ID e Okta, il processo di provisioning di utenti e gruppi è automatizzato; se vengono apportate modifiche all'utente o al gruppo in IdP, le stesse modifiche si riflettono in Ivanti Neurons for MDM.

> Il nome utente di un utente fornito tramite SCIM può essere rinominato nel provider di identità (IdP) se il nome utente è univoco in Ivanti Neurons per MDM.

> Gli utenti e i gruppi SCIM possono ora essere ricercati utilizzando i rispettivi ID esterni.

Generare un token da Ivanti Neurons per MDM

Per avviare il Provisioning utente per un IdP, generare un token e l'URL di destinazione da Ivanti Neurons per MDM.

> Assicurarsi di salvare il token e l'URL di destinazione.

> In un determinato momento, è possibile generare al massimo 2 token.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Andare in **Amministratore** > **Identità** > **Provisioning utente**.
3. Selezionare Identity Provider (IdP) dall'elenco a discesa.
4. Per generare un nuovo token, fare clic su **Genera**. Appare un messaggio di notifica, fare clic **Genera**. Si apre una nuova pagina con i dettagli del Token e l'URL SCIM di destinazione.
5. Fare clic su **Copia** per copiare il token o l'URL SCIM.
6. Aggiornare la pagina. La pagina **Provisioning utente** visualizza la tabella Stato token.

Cambia lo Stato token

È possibile cambiare lo stato di un token esistente.

Procedura

1. Fare clic sul menu dell'elenco a discesa **Seleziona** sulla pagina **Provisioning utente Entra ID**.
2. Fare clic su **Seleziona** ed effettuare le seguenti modifiche al token:
    - **Imposta su Attivo**
    - **Imposta su Inattivo**
    - **Rinnova**
    - **Rimuovi**

Visualizza lo stato del token da audit trail

È possibile visualizzare i registri delle azioni / eventi che hanno avuto luogo su un token SCIM dalla sezione Audit trail. Il token SCIM può presentare uno dei seguenti stati:

- Token SCIM creato - È stato creato un token SCIM.
- Token SCIM abilitato - Il token SCIM è stato abilitato.
- Token SCIM disabilitato - Il token SCIM è stato disabilitato.
- Token SCIM rinnovato - Il token SCIM è stato rinnovato.
- Token SCIM eliminato - Il token SCIM è stato eliminato.

La colonna DETTAGLI elenca anche il nome del fornitore SCIM (IDP), come Azure, Okta, ecc. che semplifica la comunicazione con Ivanti Neurons per MDM.

Configurare gli attributi nel provisioning SCIM

Questa sezione descrive come creare attributi personalizzati e aziendali per un IdP durante il provisioning degli utenti.

Attributi di mapping

Dopo aver stabilito la connessione, è possibile mappare gli attributi tra IdP e Ivanti Neurons per MDM. Ivanti Neurons per MDM supporta i seguenti attributi dell'utente:

Attributi core

- id
- nome utente
- displayname
- attivo
- nome fornito
- nome famiglia
- emails

> Per Entra ID IdP, è supportato l'IdP esterno.

Elenco degli attributi per i quali è consentita l'operazione di aggiornamento

- nome utente
- displayName
- emails
- nome fornito
- nome famiglia
- attivo
- urn:ietf:params:scim:schemas:extension:ivanti:2.0:User
- urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Attributo personalizzato

Schema - urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<CustomAttribute123Name>

Attributo aziendale

Attualmente è supportato solo l'attributo Dipartimento.

Schema - urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department

12.2.10.2.1. Provisioning utente per Entra ID IdP

Argomenti della sezione:

- Stabilire una connessione con Ivanti Neurons per MDM
- Provisioning di utenti e gruppi assegnati
- Provisioning di tutti gli utenti e gruppi assegnati
- Verificare il provisioning degli utenti assegnati
- Provisioning utente per Entra ID IdP
- Modifica impostazioni
- Configurare gli attributi personalizzati e aziendali
- Considerazioni sulla migrazione
- Considerazioni sulla migrazione
- Note importanti

Stabilire una connessione con Ivanti Neurons per MDM

Dopo aver creato gli utenti e i gruppi nell'applicazione Entra ID Enterprise, è possibile stabilire la connessione fra Entra ID e Ivanti Neurons for MDM.

Procedura

1. Accedere al portale Entra ID.
2. Andare su **Applicazione aziendale** > fare clic su **+ Crea la tua applicazione**. Si apre la finestra Create la tua applicazione.
3. Specificare il nome della propria applicazione (**Predefinito: Non galleria**) e fare clic su **Crea**. Ad esempio, Provisioning utente Ivanti Neurons for MDM.
4. Andare a **Provisioning** > **Modifica provisioning** > **Credenziali amministratore**.
5. Copiare e incollare l'URL SCIM di destinazione dal portale Amministratori di Ivanti Neurons per MDM nel campo **URL tenant** del portale Entra ID.
6. Copiare e incollare il Token da Ivanti Neurons per MDM nel campo **Token segreto** nel portale Entra ID.
7. Eseguire una delle operazioni seguenti:
    - Selezionare **Sincronizza solo gli utenti e i gruppi assegnati**. Per ulteriori informazioni, vedere Provisioning utenti e gruppi assegnati
    - Selezionare **Sincronizza tutti gli utenti e i gruppi**. Per ulteriori informazioni, vedere Provisioning di tutti gli utenti e gruppi assegnati.

    > Selezionare l'opzione Sincronizza tutti gli utenti e i gruppi per la migrazione degli utenti.

Fare clic su **Verifica connessione**. Viene visualizzata una finestra pop-up con un segno di spunta verde per confermare la connessione.

9. Fare clic su **Salva**.
10. Espandere **Mapping** dalla pagina **Provisioning** del portale Entra ID.

11. Fare clic su **Provisioning utenti Entra ID**. Si apre la pagina Mapping attributi.
12. Fare clic su **Elimina** per eliminare gli attributi non supportati.

Provisioning di utenti e gruppi assegnati

Una volta stabilita la connessione tra Entra ID e Ivanti Neurons per MDM, è possibile eseguire il provisioning di utenti o gruppi.

> Durante il provisioning dei gruppi, Entra ID non aggiunge i membri dei gruppi nidificati al gruppo selezionato. Durante il processo di sincronizzazione, Entra ID aggiunge i membri immediati e i nomi dei gruppi solo al gruppo e non i membri del sottogruppo.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Nell'applicazione, andare su **Utenti e gruppi** > fare clic su **+ Aggiungi utente/gruppo**. Viene visualizzata la pagina Aggiungi assegnazione.
3. Cercare l'utente o il gruppo utilizzando il campo **Cerca**, fare clic su **Seleziona** e quindi su **Assegna**. Viene visualizzata la pagina Utenti e gruppi.
4. Selezionare la casella di controllo dell'utente o del gruppo corrispondente.
5. Fare clic su **Provisioning** e quindi su **Avvia provisioning**. Vengono visualizzati i dettagli della configurazione riuscita.

Provisioning di tutti gli utenti e gruppi assegnati

Dopo che la connessione è stata stabilita tra Entra ID e Ivanti Neurons for MDM, è possibile eseguire il provisioning di utenti o gruppi.

Procedura

- Fare clic su **Provisioning** e quindi su **Avvia provisioning**. Viene visualizzata una pagina con informazioni dettagliate sulla corretta esecuzione del provisioning e viene eseguito il provisioning dell'utente a Ivanti Neurons for MDM.

Verificare il provisioning degli utenti assegnati

Dopo che un utente assegnato ha effettuato il provisioning sul portale Entra ID, verificare il provisioning sul portale amministrativo Ivanti Neurons per MDM.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Nel menu principale, selezionare la scheda **Utenti**. L'utente di cui è stato eseguito il provisioning risulta incluso nell'elenco degli utenti visualizzato in questa pagina.

> Il processo di provisioning può richiedere fino a un'ora.

Verificare provisioning gruppo

Dopo che un gruppo ha effettuato il provisioning sul portale Entra ID, verificare il provisioning su Ivanti Neurons per MDM.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.

2. Andare alla scheda **Utenti** > **Gruppi di utenti**. Il gruppo di cui è stato eseguito il provisioning risulta incluso nell'elenco dei gruppi visualizzato in questa pagina.

> Il processo di provisioning può richiedere fino a un'ora.

Modifica impostazioni

Questo argomento aiuta a configurare le impostazioni Entra ID.

Procedura

1. Andare su **Amministratore > Microsoft Azure > Provisioning utente Entra ID**.
2. Fare clic su **Genera Token** e copiare il token.
3. Aggiornare la pagina. Si apre la pagina Impostazioni Entra ID.
4. Fare clic su **Modifica impostazioni**.
5. Impostare **Invita gli utenti importati da Entra ID automaticamente** - Indicare se gli utenti importati da Entra ID a Ivanti Neurons per MDM vengono automaticamente invitati a registrarsi tramite e-mail.
6. Impostare **ID Apple gestito** - Questa opzione è disattivata per impostazione predefinita. Fare clic sul pulsante per attivarlo. L'ID Apple gestito può essere impostato durante il provisioning tramite:
   - **Indirizzo e-mail utente**
     - (Facoltativo) selezionare l'opzione Includi sottodominio "appleid" per evitare un conflitto con gli ID Apple esistenti.
   - Mapping ad **Attributo personalizzato**

     > L'attributo personalizzato deve essere valutato come un indirizzo e-mail unico.
7. (Facoltativo) Fare clic su **Aggiungi attributo personalizzato** - Specificare gli attributi utente personalizzati dal servizio directory che si desidera applicare alla gestione del dispositivo. È possibile fare riferimento a ciascun attributo con $ nei campi della configurazione in grado di supportare le variabili. L'uso di questa opzione richiede l'implementazione coerente degli attributi personalizzati sui server Entra ID. Se un server Entra ID incluso nella propria implementazione non utilizza questo attributo, le funzioni dipendenti da tale attributo potrebbero non funzionare come previsto. La colonna **Tipo attributo** visualizza un attributo **IDP** nella tabella **Attributi personalizzati** nella sezione **Modifica impostazioni**.
8. Fare clic su **Salva modifiche** dopo aver modificato le impostazioni Entra ID.

Configurare gli attributi personalizzati e aziendali

Procedura

1. Andare in **Amministratore** > **Identità** > **Provisioning utente**.
2. Sotto **Modifica impostazioni**, fare clic su **+Aggiungi attributo personalizzato**.
3. Inserire un nome nel campo **Nome attributo** (ad esempio, custAttr1) e fare clic su **Salva modifiche**. L'attributo è elencato e disponibile nella pagina **Amministratore** > **Sistema** > **Attributo**. L'attributo è indicato come attributo IdP ed è possibile eseguire solo l'azione Elimina.
4. Accedere al portale **Entra ID**.
5. Accedere a **Home** > **Applicazione enterprise** > Fare clic sull'applicazione SCIM.
6. Fare clic su **Provisioning utenti Entra ID** dalla sezione **Mapping**.

7. Selezionare la casella di controllo **Mostra opzioni avanzate**.
8. Fare clic su **Modifica elenco attributi per customappsso**.
9. Inserire una nuova voce per l'attributo personalizzato creato nell'interfaccia utente Ivanti Neurons for MDM.
10. Aggiungere lo schema per l'attributo Custom/ Enterprise (Dipartimento) come segue:
    Attributo personalizzato - **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<custAttr1> -** Fare riferimento al punto 3.
    Attributo aziendale - **urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department**
11. Fare clic su **Salva modifiche**.
12. Fare clic su **Aggiungi nuovo mapping** e selezionare gli attributi Sorgente e Destinazione dal menu a discesa.
13. Fare clic su **Ok** e su **Salva mapping**.
14. Accedere a **Home** > **Applicazione enterprise** > Fare clic sull'applicazione SCIM > **Utenti e gruppi**.
15. Fare clic su Nome utente. Si apre la pagina Profilo.
16. Verificare se il valore associato all'attributo appare nella pagina Profilo.
17. (Facoltativo) Fare clic sull'applicazione SCIM > Provisioning > Fornisci su richiesta, cercare l'utente specifico e fare clic su Provisioning. Per convalidare i nuovi mapping degli attributi eseguiti nei passaggi precedenti.
18. Accedere al portale amministrativo Ivanti Neurons per MDM.
19. Accedere a **Utente** > **Utenti** > Selezionare l'utente.
20. Fare clic sulla scheda **Attributi** e verificare il valore dell'attributo. L'attributo è mappato per l'utente specifico.

Considerazioni sulla migrazione - Da origine utente Entra ID a SCIM di provisioning utente

- Quando si migra da Origine utente Entra ID a Provisioning utente Entra ID (SCIM), selezionare Sincronizza tutti gli utenti e i gruppi.
- Dopo che gli utenti e i gruppi sono stati aggiornati con un'origine SCIM Entra ID, tornare alla pagina Provisioning Azure in Azure e impostare gli utenti e i gruppi specifici da gestire con Provisioning utente Entra ID usando l'opzione Sincronizza solo utenti e gruppi assegnati.
- Una volta completata la sincronizzazione, è possibile rimuovere gli utenti e i gruppi che non sono definiti in Azure dagli elenchi Utenti e gruppi Ivanti Neurons per MDM.
- Quando inizia la migrazione, la pagina Origine utente Entra ID è accessibile in uno stato di sola lettura.

Considerazioni sulla migrazione - Da LDAP a SCIM di provisioning utente

Prerequisiti:

1. L'opzione **Abilita questo server LDAP** è selezionata per impostazione predefinita. Questa opzione deve essere deselezionata prima della migrazione.
2. Creare un'app Enterprise in Entra ID, aggiungere gli utenti/gruppi LDAP sincronizzati (gli stessi utenti/gruppi LDAP presenti in Ivanti) all'app SCIM. Avviare il provisioning.

Considerazioni chiave per la migrazione da LDAP a SCIM

- LDAP non acquisisce tutte le informazioni per gli utenti/gruppi sincronizzati, mentre SCIM registra gli eventi degli utenti/gruppi nei registri di audit.
- L'utente LDAP con attributo personalizzato ha il tipo definito ldap, mentre per SCIM è IdP. Quindi, quando gli utenti con attributi personalizzati vengono migrati da LDAP a SCIM, l'attributo personalizzato dell'IdP corrispondente deve essere creato nell'App

SCIM e gli utenti verranno migrati. Se l'utente desidera aggiornare l'attributo personalizzato ldap in un secondo momento, il valore dell'attributo ldap.custom non verrà aggiornato in MDM dopo la migrazione. Il valore dell'attributo IdP verrà aggiornato.

- Migrare gli utenti LDAP associati a uno o più attributi personalizzati, in particolare "ldap.custAttr1", che indica la registrazione del dispositivo LDAP e la configurazione (Identity Certificate Configuration) inviata al dispositivo con il Tipo SAN corrispondente al valore dell'attributo personalizzato LDAP.
- Migrare un utente LDAP in cui l'Id Apple gestito è associato all'indirizzo e-mail - Quindi, prima della migrazione da LDAP a SCIM, se l'utente vuole mantenere il valore dell'ID Apple gestito dell'utente LDAP, è necessario attivare l'impostazione ID Apple gestito in SCIM e salvare le impostazioni.
- Quando l'utente LDAP viene rimosso dal server LDAP, l'utente è ancora attivo ma il flag Nessuna sincronizzazione è impostato su true per quel particolare utente LDAP sincronizzato. Nel caso di SCIM, quando viene eliminato un utente con provisioning, lo stato dell'utente viene disabilitato.
- Una volta configurato SAML come Identity Provider (IdP) per gli utenti SCIM, tutti gli utenti provenienti da varie fonti come Local e LDAP saranno autenticati tramite SAML. Solo gli utenti locali possono essere aggiunti a un elenco di eccezioni per bypassare il flusso di autenticazione dell'IdP. Questa configurazione può essere gestita nella pagina SAML sotto **Amministratore** > **Identità** > **SAML**.
- Una volta configurato SAML per gli utenti IDP (SCIM) migrati, la registrazione del dispositivo può essere bypassata (non tramite IDP) per altri utenti provenienti da fonti diverse, come Local e LDAP. Ciò può essere gestito in **Utenti** > **Impostazioni utente**.
- In LDAP sono supportati Utenti, Gruppi e UO, mentre in SCIM sono supportati Utenti e Gruppi, ma non UO.
- La procedura di provisioning di gruppo annidato non è supportata in SCIM.

Note importanti - SCIM

- L'indirizzo e-mail è un campo obbligatorio per il provisioning e la migrazione di utenti o membri.
- SCIM fornisce un provisioning unidirezionale da Microsoft Entra ID a Ivanti Neurons for MDM. Ivanti Neurons for MDM non offre alcuna opzione di sincronizzazione. Se si elimina un gruppo o un utente fornito da SCIM da Ivanti Neurons for MDM, assicurarsi di rimuovere l'utente o il gruppo anche da Microsoft Entra ID.
- È possibile utilizzare un attributo (origine o destinazione) solo una volta nella finestra di mapping delle applicazioni SCIM in Microsoft Entra ID. La stessa sorgente non può essere mappata due volte su uno specifico attributo di destinazione.
- Gli utenti inattivi non possono essere forniti o migrati su Ivanti Neurons for MDM utilizzando SCIM.
- Attualmente, Ivanti Neurons for MDM non supporta la notifica degli eventi SCIM.
- La durata della migrazione o del provisioning dipende dal numero di utenti o gruppi coinvolti.
- Microsoft Azure controlla l'intervallo di provisioning ed è di circa 40 minuti o più.
- Durante il re-provisioning, Microsoft Entra ID riprova solo le voci non riuscite. È possibile scaricare i registri di provisioning per verificare gli utenti il cui provisioning è riuscito o meno da Microsoft Entra ID.
- I gruppi duplicati provenienti da origini diverse non sono ammessi in SCIM.
- Quando un utente con provisioning viene eliminato da Microsoft Entra ID, l'utente viene disattivato in Ivanti Neurons for MDM.
- Quando si elimina un gruppo di utenti con provisioning da Microsoft Entra ID, il gruppo viene eliminato in Ivanti Neurons for MDM e i membri indipendenti che appartengono al gruppo eliminato vengono disattivati e associati al gruppo Tutti gli utenti.
- Quando un membro di un gruppo provvisto viene eliminato in Microsoft Entra ID, il membro viene disattivato in Ivanti Neurons for MDM, ma il membro è ancora associato al gruppo in Ivanti Neurons for MDM.
- Quando il mapping di un attributo (attributo Enterprise o attributo personalizzato) viene rimosso da un'app, il valore dell'attributo rimosso si riflette ancora in Ivanti Neurons for MDM.

- Quando un attributo utente di un utente con provisioning viene aggiornato con un valore vuoto o indeterminato, il valore dell'attributo aggiornato non viene riflesso in Ivanti Neurons for MDM.
- Se gli attributi utente FName e LName (name.formatted) sono vuoti durante la migrazione o l'aggiornamento da Microsoft Entra ID a SCIM, la migrazione o l'aggiornamento non riuscirà.
- Se si elimina un utente in Entra ID, l'API SCIM corrispondente non elimina l'utente in modo permanente, ma esegue un'eliminazione soft e cambia lo stato dell'utente da attivo a inattivo. Se si desidera eliminare definitivamente l'utente, accedere al portale amministrativo Ivanti Neurons for MDM ed eliminare manualmente l'utente inattivo/disabilitato.
- Quando un utente locale esiste già in Ivanti Neurons for MDM con un determinato ID utente, un utente simile con lo stesso ID utente verrà fornito da Entra ID a MDM, dopodiché l'origine utente verrà aggiornata da Locale a SCIM Entra ID.
- Entra ID con la sottoscrizione "Entra ID Premium P1" è autorizzato a eseguire il provisioning del gruppo da assegnare e fornire.

12.2.10.2.2. Provisioning utente per Okta IdP

Argomenti della sezione:

- Stabilire una connessione con Ivanti Neurons per MDM
- Provisioning utenti e gruppi
- Verificare il provisioning degli utenti assegnati
- Verificare provisioning gruppo
- Modifica impostazioni
- Configurare gli attributi personalizzati/aziendali nel provisioning degli utenti SCIM

Stabilire una connessione con Ivanti Neurons per MDM

Dopo aver creato gli utenti e i gruppi nell'applicazione **Okta**, è possibile stabilire la connessione fra **Okta** e Ivanti Neurons per MDM.

Procedura

1. Accedere a **Okta**.
2. Accedere ad **Applicazioni** > **Applicazioni** > **Sfoglia App Catalog**.
3. Cercare **Aggiungi SCIM 2.0 Test App** (OAuth Bearer Token) e installare l'app.
4. Fare clic sull'app e andare in **Provisioning** > **Integrazione**.
5. Fare clic su **Modifica** e fornire l'url di base e incollare il token generato.
6. Fare clic su **Salva**.
7. Andare in **Provisioning** e fare clic su **Modifica**.
8. Abilitare le azioni utente necessarie e fare clic su **Salva**.

Provisioning utenti e gruppi

Una volta stabilita la connessione tra **Okta** e Ivanti Neurons per MDM, è possibile eseguire il provisioning di utenti o gruppi.

Procedura

1. Andare su **Assegnazioni** > **Assegna** > **Assegna a persone** o **Assegna a gruppo**.
2. 2. Selezionare o cercare un utente o un gruppo esistente e fare clic su **Assegna**.
3. Ripetere la procedura per aggiungere altri **Utenti** o **Gruppi**.
4. Fare clic su **Fine**.
5. Selezionare il gruppo e fare clic su **Esegui push gruppo per nome** per salvare e sincronizzare il gruppo.

Verificare il provisioning degli utenti assegnati

Dopo che un utente assegnato ha effettuato il provisioning sul portale Okta, verificare il provisioning utente sul portale amministrativo Ivanti Neurons per MDM.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.

2. Nel menu principale, selezionare la scheda **Utenti**. L'utente di cui è stato eseguito il provisioning risulterà incluso nell'elenco degli utenti visualizzato in questa pagina.

Verificare provisioning gruppo

Dopo che un gruppo ha effettuato il provisioning sul portale Okta, verificare il provisioning su Ivanti Neurons per MDM.

Procedura

1. Accedere al portale amministrativo Ivanti Neurons per MDM.
2. Andare sulla scheda **Utenti** e fare clic su **Gruppi di utenti**. Il gruppo di cui è stato eseguito il provisioning risulterà incluso nell'elenco dei gruppi visualizzato in questa pagina.

Modifica impostazioni

Questo argomento aiuta a configurare le impostazioni Okta.

Procedura

1. Andare in **Amministratore** > **Identità** > **Provisioning utente Okta**.
2. Fare clic su **Modifica impostazioni**.
3. Impostare **Invita gli utenti importati da Okta** - Indicare se gli utenti importati da Okta a Ivanti Neurons per MDM vengono automaticamente invitati a registrarsi tramite e-mail.
4. (Facoltativo) Fare clic su **Aggiungi attributo personalizzato** - Specificare gli attributi utente personalizzati dal servizio directory che si desidera applicare alla gestione del dispositivo. È possibile fare riferimento a ciascun attributo con $ nei campi della Configurazione in grado di supportare le variabili. L'uso di questa opzione richiede l'implementazione coerente degli attributi personalizzati sui server Okta. Se un server Okta incluso nella propria implementazione non utilizza l'attributo personalizzato, le funzioni dipendenti dall'attributo personalizzato potrebbero non funzionare come previsto. La colonna **Tipo attributo** visualizza un attributo **IDP** nella tabella **Attributi personalizzati** nella sezione **Modifica impostazioni**.
5. Fare clic su **Salva modifiche** dopo aver modificato le impostazioni Okta.

Configurare gli attributi personalizzati/aziendali nel provisioning degli utenti SCIM

Procedura

1. Andare in **Amministratore** > **Identità** > **Provisioning utente**.
2. Fare clic su **Modifica impostazioni**.
3. Immettere l'attributo personalizzato (ad esempio, custAttr1) e fare clic su **Salva modifiche**.
4. Dal portale Okta, fare clic su **Directory** > **Editor profili**.
5. Fare clic sull'app **SCIM 2.0 Test App utente (OAuth Bearer Token)**.
6. Fare clic su **Aggiungi attributo**.
7. Aggiungere i seguenti valori di attributi personalizzati, ad esempio:
    - Nome visualizzato (lo stesso valore dell'attributo personalizzato fornito in N-MDM, fare riferimento al passaggio 3).
    - Nome variabile: custAttr1
    - Nome esterno: custAttr1
    - Spazio nome esterno **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User**

    - Autorizzazione utente: (Lettura / Scrittura)
8. Fare clic su **Salva attributo**.
9. Fare clic su **Editor profili** > **Mapping**. Si vedranno due sezioni per i mapping (SCIM e Okta).
10. Mappare gli attributi personalizzati creati in N-MDM con gli attributi definiti in Okta e salvare i mapping.
11. Accedere a **Utenti** e fare clic sull'utente desiderato.
12. Fare clic su **Profilo** > **Modifica** per modificare gli attributi.
13. Accedere all'app **Applicazioni** > **SCIM 2.0 Test App (OAuth Bearer Token)**.
14. Nella scheda **Assegnazioni**, fare clic su **Assegna** e selezionare **Assegna a persone**.
    Sullo schermo appare la finestra **Assegna SCIM 2.0 Test App (OAuth Bearer Token) a persone**.
15. Selezionare l'utente richiesto e fare clic su **Assegna**.
16. Fare clic su **Fine**.

Per verificare l'attributo personalizzato e il suo mapping in Ivanti Neurons per MDM:

- Accedere a **Utenti** > **Utente** (qualsiasi utente specifico) > **Attributi**. Assicurarsi che l'attributo personalizzato mappato per Okta sia visibile nella sezione Attributi utente.

12.2.11. Configurazione del server LDAP

Licenza: Silver

La configurazione di un server LDAP e di un Connettore consente di importate utenti e gruppi dalla directory aziendale. Dopo aver installato almeno un Connettore, sarà possibile aggiungere uno o più server LDAP.

L'aggiunta di un server LDAP consente di configurare:

- la *connessione* al server LDAP
- i *termini di ricerca necessari* per la visualizzazione dei dati della directory di destinazione
- la porzione di directory da *importare*
- se *invitare automaticamente gli utenti* nella porzione di selezione della directory

Una volta aggiunto un server LDAP, è possibile ritornare su questa pagina per **modificare le informazioni del server LDAP** oppure **modificare gli utenti LDAP selezionati**.

> Gli utenti LDAP devono essere importati dopo la configurazione di un utente LDAP. Vedere **Importazione di utenti LDAP**.
> I nomi utente LDAP, come i nomi utente locali, devono essere univoci a livello globale. Verificare che gli utenti non dispongano già di un account locale con lo stesso nome utente oppure, nel caso di organizzazioni con più tenant, che il nome utente non sia già stato associato a un altro tenant.

Aggiunta di un server LDAP

Procedura

1. Fare clic su **+Aggiungi server**.
2. Immettere le informazioni seguenti:
3. Fare clic su **Verifica connessione e Continua**.

Impostazione	Operazione da eseguire
Nome	Immettere un nome identificativo del server.
Descrizione	Immettere una descrizione che chiarisca lo scopo del server.
URL directory	Immettere l'URL della directory. Utilizzare uno dei formati seguenti: ldap://indirizzo IP o ldaps://indirizzo IP o Esempio: ldap://ilmioserver1.lamiaazienda.com:389
ID utente	Immettere l'ID utente di un account con le caratteristiche seguenti: • gestito dal server LDAP • è in grado di associarsi al server LDAP e di cercare i sottoalberi relativi a utente, gruppo e unità organizzativa Si tratta generalmente di un account con Credenziali di amministratore directory (DN o nome distinto e password).
Password	Immettere la password dell'account.
Conferma password	Immettere nuovamente la password dell'account.
Tipo di directory	Selezionare il tipo di directory dall'elenco delle directory supportate. • Microsoft Active Directory • Apri LDAP • Altro (compatibile con Apri LDAP)

4. Questo passaggio convalida le informazioni fornite fino a questo momento.

- Se le informazioni sono valide, il servizio recupera il contesto di denominazione LDAP e lo utilizza per il completamento di alcuni campi nella pagina successiva.
- Se l'URL LDAP non riesce a connettersi, è possibile comunque procedere con i passaggi successivi. Tuttavia, le funzionalità potrebbero essere limitate finché non viene stabilita la connessione.

Completare le impostazioni rimanenti:

5. Fare clic su **Avanti**.

Impostazione	Operazione da eseguire
URL failover della directory	Immettere l'URL della directory secondaria. Utilizzare il formato seguente: ldap://indirizzo IP o Esempio: ldap://ilmioserver2.lamiaazienda.com:389
Intervallo di sincronizzazione	Immettere l'intervallo di tempo tra ciascun tentativo di sincronizzazione dei dati LDAP dal server LDAP. Il valore predefinito è di 15 minuti. Prendere in considerazione un aumento dell'intervallo di tempo in seguito alla sincronizzazione corretta di tutti i dati LDAP di destinazione e se si è sicuri che la configurazione LDAP si adatti alle proprie esigenze.
Abilita eliminazione della sincronizzazione	Selezionare quest'opzione per eliminare automaticamente i dati della sincronizzazione LDAP se la serie di dati ricaricata subisce un calo notevole. Quest'opzione assicura che il comportamento anormale del sistema LDAP non comporti aggiornamenti non necessari e improvvisi del servizio e la rimozione delle configurazioni dai dispositivi registrati. Accertarsi che quest'opzione non sia selezionata se si intende apportare modifiche consistenti alla configurazione LDAP o al server LDAP.
Abilita questo server LDAP	Selezionare quest'opzione per utilizzare questo server LDAP con il servizio. Deselezionare quest'impostazione se si desidera dismettere questo server LDAP o toglierlo dal servizio. Anche se è possibile sostituire automaticamente il server mediante un failover configurato su un secondo server LDAP, l'abilitazione di quest'opzione consente di effettuare pianificazioni in anticipo ed evitare una breve mancanza di connettività durante il failover.
Invita automaticamente gli utenti quando vengono importati	Selezionare questa impostazione per inviare automaticamente inviti agli utenti quando vengono importati dal server LDAP.
Carica certificato AC	Fare clic su **Scegli file** per caricare il certificato TLS emesso dall'autorità di certificazione installato su questo server LDAP. È possibile caricare più certificati AC.
Cerca riferimenti	Si applica soltanto se si sta utilizzando un dominio a più foreste. Questa opzione indica se si desidera utilizzare controller di dominio alternativi nel caso in cui il controller di dominio assegnato non disponga della copia dell'oggetto richiesto. • Selezionare **Segui** se si desidera utilizzare i riferimenti. • Selezionare **Ignora** se non si desidera utilizzare i controller di dominio alternativi. • L'opzione **Genera** al momento ha gli stessi effetti dell'opzione **Ignora**. Se si seleziona l'opzione **Segui**, si verificherà un ritardo dell'autenticazione LDAP.
Timeout dei risultati della ricerca	Aumentare il timeout se si verificano dei problemi relativi alle prestazioni o se i risultati non sono completi quando si esplorano i dati sincronizzati dal server LDAP.
Conteggio risultati di ricerca	Impostare quest'opzione sul numero massimo di record che il server LDAP deve restituire alla volta. Tra gli scenari che potrebbero richiedere la modifica di quest'impostazione per il miglioramento delle prestazioni vi sono:

Impostazione	Operazione da eseguire
	• Il server LDAP si trova lontano o dietro un collegamento ad alta latenza. In questo caso, per recuperare i risultati di ricerche di grandi dimensioni, sarà necessario più tempo rispetto a quanto necessario per recuperare quelli di ricerche di dimensioni ridotte. Di conseguenza, la definizione di un insieme di dimensioni ridotte consentirà di visualizzare più rapidamente i sottoinsiemi dei dati aggiornati. • La dimensione del server LDAP è notevole e ogni ricerca restituisce un insieme di risultati molto vasto. In questo caso, se le prestazioni non rappresentano un problema, la definizione di un insieme di risultati più vasto renderebbe possibile la restituzione di tutti i dati con un numero inferiore di ricerche.

Per l'ambiente Sandbox, l'intervallo di sincronizzazione LDAP non può essere programmato per meno di 8 ore.

6. Utilizzare le linee guida seguenti per configurare l'integrazione con il server LDAP:
7. Fare clic su **Sfoglia** oppure su **Cerca**.

Impostazione	Operazione da eseguire
Formato membro del gruppo	Selezionare **DN** o **UID** per indicare se utilizzare nella ricerca il nome distinto o l'ID utente.
Attributi di ricerca OU	Specificare i criteri di ricerca a livello di unità organizzativa.
DN di base	Immettere il nome distinto per il livello iniziale che si desidera faccia da radice per la ricerca o da cui si desidera che quest'ultima inizi. La scelta determinerà i valori predefiniti di numerosi altri campi che, se necessario, sarà possibile modificare.
GUID oggetto	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP. Si tratta dell'attributo che identifica in modo univoco un'unità organizzativa nel tempo e attraverso le modifiche apportate al nome dell'OU.
Nome attributo	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Descrizione	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Attributo DN	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Filtro di ricerca	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Ambito di ricerca	Selezionare la porzione della gerarchia LDAP da prendere come destinazione: • **Base** (soltanto il livello della voce della base di ricerca) • **Un livello** (il livello al di sotto della base di ricerca) • **Sottoalbero** (il sottoalbero dell'albero delle informazioni della directory al di sotto del DN della base di ricerca)
Attributi di ricerca dell'utente	Specificare i criteri della ricerca degli utenti in un determinato livello di directory.
DN di base	Immettere il nome distinto del livello iniziale in cui si desidera effettuare la ricerca.
Attributo UID	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
GUID oggetto	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP. Si tratta dell'attributo che identifica in modo univoco un utente nel tempo e attraverso le modifiche apportate al nome.
Attributo DN	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Nome	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Cognome	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.

Impostazione	Operazione da eseguire
Nome visualizzato	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Indirizzo e-mail	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Nome principale	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Impostazioni locali	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Membro di	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Filtro di ricerca	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Ambito di ricerca	Selezionare la porzione della gerarchia LDAP da prendere come destinazione: • **Base** (soltanto il livello della voce della base di ricerca) • **Un livello** (il livello al di sotto della base di ricerca) • **Sottoalbero** (il sottoalbero dell'albero delle informazioni della directory al di sotto del DN della base di ricerca)
ID Apple gestito	Scegliere di sincronizzare l'ID Apple gestito per gli utenti LDAP. • **Nessuno** • **Modello** - ◦ **Indirizzo e-mail utente** ◦ **UPN utente** Facoltativamente, selezionare l'opzione **Includi sottodominio "appleid"** per evitare un conflitto con gli ID Apple esistenti.
+Aggiungi attributo personalizzato	(Facoltativo) Consente di specificare dal servizio directory fino a 7 attributi utente personalizzati che si desidera applicare alla gestione del dispositivo. È possibile fare riferimento a ciascun attributo con $ nei campi della configurazione in grado di supportare le variabili. **Importante:** l'uso di questa opzione richiede l'implementazione coerente degli attributi personalizzati sui server LDAP. Se un server LDAP incluso nella propria implementazione non utilizza questo attributo, le funzioni dipendenti da tale attributo potrebbero non funzionare come previsto.
Attributi di ricerca del gruppo	
DN di base	Immettere il nome distinto del livello iniziale in cui si desidera effettuare la ricerca.
GUID oggetto	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP. Si tratta dell'attributo che identifica in modo univoco un gruppo nel tempo e attraverso le modifiche apportate al nome.

Impostazione	Operazione da eseguire
Attributo DN	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Nome attributo	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Descrizione	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Membro	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Filtro di ricerca	Se necessario, modificare il valore predefinito in modo che corrisponda all'ambiente LDAP.
Ambito di ricerca	Selezionare la porzione della gerarchia LDAP da prendere come destinazione: • **Base** (soltanto il livello della voce della base di ricerca) • **Un livello** (il livello al di sotto della base di ricerca) • **Sottoalbero** (il sottoalbero dell'albero delle informazioni della directory al di sotto del DN della base di ricerca)

8. Accertarsi che la configurazione restituisca i dati previsti.
9. È possibile effettuare tale operazione sfogliando o cercando un oggetto conosciuto all'interno della directory.

Fare clic su **Avanti**.

Eliminazione di un attributo LDAP personalizzato

È possibile eliminare un attributo LDAP personalizzato e rimuoverne i valori dagli utenti o dispositivi associati.

Procedura

1. Andare ad **Amministratore > Attributi**.
2. Nella sezione **Attributi personalizzati**, fare clic sul collegamento **Elimina** accanto all'attributo LDAP da eliminare. Viene visualizzata una finestra di conferma.
3. Fare clic su **Elimina** per confermare l'eliminazione.

> il pulsante **Elimina** è disattivato per impostazione predefinita. È necessario selezionare la casella di controllo nell'opzione **Sono consapevole del fatto che non sarà possibile annullare l'eliminazione dell'attributo personalizzato** per abilitare il pulsante **Elimina**.

Modifica delle informazioni del server LDAP

Procedura

1. Andare in **Amministratore > LDAP**.
2. Alla voce del server LDAP, selezionare l'icona **Modifica** nella colonna **Azioni** per visualizzare la pagina Collega server LDAP.
3. Apportare le modifiche necessarie.

4. Fare clic su **Verifica connessione e Continua**.
   Se l'URL LDAP non riesce a connettersi, è possibile procedere con i passaggi successivi. Tuttavia, le funzionalità potrebbero essere limitate finché non viene stabilita la connessione.
5. Fare clic su **Sfoglia** oppure su **Cerca**.
6. Accertarsi che la configurazione restituisca i dati previsti.
   È possibile effettuare tale operazione sfogliando o cercando un oggetto conosciuto all'interno della directory.
7. Fare clic su **Fine**.

Importazione di utenti LDAP

Procedura

1. Andare a **Utenti**.
2. Fare clic su **+Aggiungi > Invita utenti da LDAP**.
3. Fare clic su **Seleziona utenti** alla voce del server LDAP.
4. Nella pagina Aggiungi utenti LDAP, immettere il nome dell'utente, gruppo o unità organizzativa nella casella di ricerca.
5. Per aggiungere nuovi utenti o gruppi, fare clic su **+Aggiungi** accanto alla voce che si desidera aggiungere.
6. Fare clic su **Avanti**.
7. Scegliere se inviare o meno l'invito:
   - Non invitare nessuno
     Per inviare gli inviti in un secondo momento, andare su **Utenti > Utenti** e selezionare **Azioni > Invia invito** per inviare gli inviti.
   - Invita tutti

Fare clic su **Fine**.

Aggiornamento di utenti, gruppi o unità organizzative selezionati

Procedura

1. Andare in **Amministratore > LDAP**.
2. Alla voce del server LDAP, selezionare l'icona **Gestisci utenti** nella colonna **Azioni** per visualizzare la pagina Aggiungi utenti LDAP.
3. Per aggiungere nuovi utenti o gruppi, immettere il nome dell'utente o del gruppo nel campo di ricerca.
4. Fare clic su **+Aggiungi** accanto alla voce che si desidera aggiungere.
5. Per rimuovere un utente, un gruppo o un'unità organizzativa, fare clic sull'icona di eliminazione accanto alla voce che si desidera eliminare.
6. Fare clic su **Fine**.

Abilitazione della notifica di eliminazione della sincronizzazione LDAP

L'abilitazione della notifica di eliminazione della sincronizzazione LDAP aiuta a impedire interruzioni causate da modifiche non intenzionali su larga scala all'ambiente LDAP.

Procedura

1. Andare in **Amministratore > LDAP**.

2. Alla voce del server LDAP, selezionare l'icona **Modifica** nella colonna **Azioni** per visualizzare la pagina Collega server LDAP.
3. Selezionare la casella di controllo **Abilita eliminazione della sincronizzazione**.
4. Immettere un valore per la percentuale di dati LDAP ricaricati per attivare l'eliminazione della sincronizzazione.
5. Fare clic su **Verifica connessione e Continua**.
   Se l'URL LDAP non riesce a connettersi, è possibile comunque procedere con i passaggi successivi. Tuttavia, le funzionalità potrebbero essere limitate finché non viene stabilita la connessione.
6. Fare clic su **Fine**.
7. Fare clic sull'icona **Sincronizza adesso** alla voce del server LDAP.
   Se la differenza delle modifiche da sincronizzare da LDAP a Ivanti Neurons for MDM supera la percentuale di scarto impostata, viene generato un AVVISO. Quando le modifiche vengono ripristinate a un valore al di sotto della percentuale impostata, l'avviso viene CANCELLATO.

Trigger	Gravità	Tipo di notifica	Tipo di componente	Componente
Eliminazione della sincronizzazione LDAP	Avviso	Sincronizzazione dati	LDAP	Nome del server LDAP
Ripristino della sincronizzazione LDAP	Informazioni	Sincronizzazione dati	LDAP	Nome del server LDAP

La notifica di eliminazione della sincronizzazione parziale viene generata quando non è possibile eseguire da LDAP la sincronizzazione dei record di uno o più utenti. In questo caso viene allegato un file CSV con un elenco di utenti che non sono riusciti ad eseguire la sincronizzazione. Se un utente viene eliminato a causa di attributi mancanti, nel file CSV esportato viene incluso anche l'elenco degli attributi mancanti.

Sincronizzazione delle modifiche dal server LDAP

Dalla pagina LDAP, fare clic sull'icona **Sincronizza adesso** alla voce server LDAP.

> Se il nome visualizzato è superiore a 128 caratteri, la sincronizzazione LDAP ignorerà tale utente e procederà con la sincronizzazione di altri utenti o gruppi di utenti.

Risoluzione dei problemi relativi alla connettività al server LDAPS

Se si riscontrano problemi di connessione al server LDAPS (LDAP o SSL), è possibile che si tratti di un problema di certificazione.

Per risolvere il problema:

- Verificare che il certificato che si sta utilizzando sul server LDAPS non sia autofirmato.
- Verificare che il certificato LDAPS non sia scaduto o non sia stato revocato Verificare la corrispondenza del nome host.

Dopo avere eseguito la verifica, attendere la sincronizzazione automatica di LDAP oppure eseguire la sincronizzazione manualmente utilizzando l'icona **Amministratore > LDAP > Sincronizza adesso** alla voce del server LDAP.

Se non è possibile visualizzare la pagina LDAP, è probabile che non si disponga delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione sistemi
- Sistema di sola lettura

12.2.12. Sentry

Sentry è un componente che funge da gateway tra i dispositivi mobili e il sistema di posta elettronica abilitato daActiveSync. Utilizzare Sentry per verificare a quali dispositivi è consentito l'accesso alle e-mail. È disponibile per il download come file ISO che è possibile installare su una macchina virtuale. Le organizzazioni devono considerare l'utilizzo di un bilanciamento del carico per mantenere più server Sentry (ridondanza).

Licenza: Silver

Documentazione più recente

Per le istruzioni più recenti per Sentry, visitare la pagina della **documentazione dei prodotti** e fare clic su Sentry.

Per le istruzioni più recenti sull'installazione di Sentry, selezionare la versione corrispondente della *Guida all'installazione locale di Standalone Sentry*.

Per istruzioni sull'aggiornamento di Sentry, selezionare la versione corrispondente della *Guida di Sentry*. Consultare le sezioni seguenti nella Guida di Sentry:

- Per le istruzioni sull'aggiornamento tramite l'interfaccia utente di Gestore di sistema di Standalone Sentry, consultare "Aggiornamenti software di Standalone Sentry".
- Per le istruzioni per l'aggiornamento tramite l'interfaccia a riga di comando (CLI) di Standalone Sentry, consultare "Aggiornamento mediante CLI".

Prima di eseguire l'aggiornamento, consultare le note di rilascio di Standalone Sentry per la versione da aggiornare.

12.3. Impostazioni Apple

Argomenti della sezione:

- Apple Configurator
- Registrazione dispositivo
- Configurazione dell'assistente di installazione
- Installa certificato MDM
- Dispositivi iPad condivisi per business
- School Manager
- Impostazioni (Apple)

12.3.1. Apple Configurator

Da questa pagina è possibile preparare Apple Configurator per la configurazione della gestione dei dispositivi Ivanti Neurons for MDM sui dispositivi iOS. Con Apple Configurator è più semplice distribuire grandi quantità di dispositivi iOS. Inoltre, Configurator consente agli amministratori di controllare i dispositivi iOS per garantire un più alto livello di configurazione e capacità di gestione. Per ulteriori informazioni su Apple Configurator, visitare il Mac App Store.

I passaggi di base sono:

1. Esportare il profilo MDM dal proprio tenant Ivanti Neurons for MDM.
2. Importazione del profilo MDM nel Configurator.
3. Utilizzo del Configurator per applicare il profilo MDM ai dispositivi con tethering.

Definizione di un utente predefinito per i dispositivi

I dispositivi configurati mediante Apple Configurator vengono assegnati all'utente nessuno in Ivanti Neurons for MDM, a meno che non venga scelto un altro utente:

1. Fare clic sul campo **Assegna dispositivi configurati a**.
2. Iniziare a digitare il nome utente dell'utente di Ivanti Neurons for MDM che si desidera selezionare.
3. Quando viene visualizzato nell'elenco a discesa, selezionare il nome utente.
4. Fare clic su **Salva**.

Installazione di app utilizzando Apple Configurator

Prima di installare le app utilizzando Apple Configurator:

- L'accesso all'app store Apple è limitato dalle configurazioni del dispositivo.
- L'installazione delle app è concesso dalle configurazioni del dispositivo.
- È necessario che Apple Configurator sia installato sul computer utilizzato per configurare i dispositivi.

Per installare le app utilizzando Apple Configurator:

1. In Ivanti Neurons for MDM, passare a **Amministratore > Apple Configurator**.
2. Spostare l'interruttore dei dispositivi di registrazione su On.
3. Fare clic su una delle seguenti opzioni:
    - **Plist dell'utente predefinito**.
    - **Plist specifico dell'utente**: immettere l'ID e-mail o il nome utente dell'utente specifico.

In Apple Configurator, andare su **Prepara > App**,

5. Andare su **Prepara > Impostazioni e disabilitare Supervisione**.
6. Selezionare l'opzione **Non aggiornare mai il dispositivo** in Aggiorna iOS.
7. Fare clic su **Prepara** (in fondo a Apple Configurator).
   Le app saranno visibili nell'elenco delle app installate sul dispositivo dopo il check-in del dispositivo.

Installazione di app utilizzando il server UEM

Per installare le app utilizzando il server UEM:

1. Caricare un'app dallo store in house nella scheda App.
2. Selezionare l'app.
3. Fare clic sulla scheda **Configurazioni app**.
4. Selezionare **Installa su dispositivo**.
   Completare le impostazioni di configurazione.
5. Selezionare **Azioni > Forza il check-in**.

Operazioni richieste all'utente finale

Apple richiede all'utente finale di avviare l'app Go almeno una volta per garantire il corretto funzionamento della funzione Posizione Ivanti Neurons for MDM. Ciò consente all'utente finale di sapere che la propria posizione è monitorata.

Attenzione: se i dispositivi sono distribuiti in modalità single app utilizzando Configurator, non sarà possibile adottare questo approccio.

Se non è possibile visualizzare la pagina **Installa Apple Configurator**, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione sistemi
- Sistema di sola lettura

12.3.2. Registrazione guidata dall'account

Questa sezione si applica alle registrazioni di Utenti e Dispositivi guidate dall'account.

Dispositivi supportati

- Dispositivi con iOS 15+ (per la registrazione dell'utente guidata dall'account) e iOS17+ (per la registrazione del dispositivo guidata dall'account)
- Dispositivi con macOS 14+
- Dispositivi con visionOS 1.1+

Prerequisiti:

Per la registrazione utenti guidata dall'account

- Un account utente in Ivanti Neurons per MDM con ID Apple gestito (utenti in Apple Business Manager o Apple School Manager).
- Nella sezione **Registrazione Apple**, selezionare **Registrazione utenti** dall'elenco a discesa **Seleziona tipo di registrazione Apple**.
- In **Utenti** → **Impostazioni utente** → impostare **Impostazioni proprietario dispositivo** su **ON** > selezionare l'opzione **Proprietario utente**.

Registrazione dispositivi guidata dall'account

- Un account utente in Ivanti Neurons for MDM con ID Apple gestito (utenti in Apple Business Manager o Apple School Manager).
- Nella sezione **Registrazione Apple**, selezionare **Registrazione dispositivi** dall'elenco a discesa **Seleziona tipo di registrazione Apple**.
- In **Utenti** → **Impostazioni utente** → impostare **Impostazioni proprietario dispositivo** su **ON** > selezionare l'opzione **Proprietario azienda**.

La **registrazione utenti guidata dall'account** per i dispositivi iOS 15+, macOS 14+ e visionOS 1.1+ è un'opzione di registrazione pensata per le aziende che implementano il BYOD (Bring Your Own Device). La registrazione degli utenti basata su account è una versione modificata del protocollo MDM e di Registrazione utenti con Apple Business Manager, che presta una maggiore attenzione alla privacy degli utenti e viene implementata con il livello di sicurezza necessario all'azienda.

Registrazione dispositivi guidata dall'account per i dispositivi iOS 17+, macOS 14+ e visionOS 1.1+ è un'opzione di registrazione progettata per le aziende per registrare i dispositivi di proprietà della società / azienda. La registrazione dispositivi guidata dall'account è una versione modificata del protocollo MDM e di Registrazione dispositivi con Apple Business Manager che presta una maggiore attenzione alla privacy degli utenti e viene implementata con il livello di sicurezza necessario all'azienda. Gli utenti finali possono registrare i propri dispositivi utilizzando la funzione Account di lavoro nelle Impostazioni.

Configurazione del servizio di individuazione

Se la propria azienda ha un nome di dominio aziendale, ad esempio acme.com, l'ID e-mail per il proprio dispositivo è nomedispositivo@acme.com.

1. L'utente inserisce nomeutente@acme.com per accedere al proprio account di lavoro o scolastico, quindi il dispositivo effettua una richiesta HTTP GET all'URL:
   https://acme.com/.well-known/com.apple.remotemanagement?user-identifier=user@acme.com
   Per ulteriori informazioni, vedere -
   https://developer.apple.com/documentation/devicemanagement/discover_authentication_servers

2. Sul dominio acme.com configurare la regola di reindirizzamento per l'URI - /.well-known/com.apple.remotemanagement per reindirizzarlo al seguente URL:
   https://<n-MDM cluster>/.well-known/com.apple.remotemanagement

Individuazione semplificata dei servizi per la registrazione dei dispositivi in base all'account

> Applicabile ai dispositivi iOS 18.2+, macOS 15.2+ e visionOS 2.2+.

Per la registrazione guidata dall'account, quando un utente inserisce l'e-mail dell'organizzazione per accedere all'account di lavoro o di scuola, il dispositivo cerca innanzitutto una risorsa HTTP nota nel dominio dell'organizzazione, che contiene un link all'URL di registrazione all'MDM.

Procedura

1. Accedere all'account Lavoro o Scuola.
2. Verificare i domini in **Apple Business Manager** e **Apple School Manager** - Si applica solo ai domini verificati in Apple Business Manager o Apple School Manager. Se un dominio è verificato, il dispositivo può controllare con Apple Business Manager /Apple School Manager per ottenere un URL di registrazione MDM alternativo.
3. Impostare un'assegnazione predefinita Ivanti Neurons per MDM per i tipi di piattaforma **Mac**, **Apple Vision Pro**, **iPhone** e **iPad**. Per impostare un'assegnazione predefinita dei dispositivi, attenersi alla seguente procedura:
   1. In **Apple Business Manager** / **Apple School Manager**, accedere con un utente che ha il ruolo di Amministratore o Gestione iscrizioni dispositivi.
   2. Selezionare il proprio nome nella parte inferiore della barra laterale, selezionare Preferenze, quindi eseguire una delle seguenti operazioni:
      - Selezionare Assegnazione del servizio di gestione dispositivi sotto Servizi di gestione dispositivi, quindi selezionare Modifica accanto a Assegnazione del servizio di gestione dispositivi predefiniti.
      - Selezionare un servizio esistente in Servizi gestione dispositivi, quindi selezionare Cambia in Assegnazione dispositivi predefiniti.
   3. Se non si dispone di altri servizi di gestione dei dispositivi configurati, modificare tutte le assegnazioni automatiche dei dispositivi al servizio selezionato, quindi selezionare **Salva**.
4. Nella console Ivanti Neurons per MDM, navigare su **Amministratore** > **Apple** > **Registrazione dispositivi**. Nella schermata **Registrazione dispositivi** vengono aggiunte le colonne **ADDE URL** e **ADDE URL SET TIME**.

> **Prima preferenza**: il dispositivo controlla la risorsa HTTP nota nel dominio dell'organizzazione.

Opzione di ripiego: se il primo metodo non riesce, il dispositivo contatta Apple ABM/ASM per recuperare la destinazione alternativa specificata da Ivanti Neurons per MDM.

5. In **Azioni**, selezionare **Configura URL ADDE**.
6. Aggiornare la pagina.

Istruzioni per l'utente del dispositivo

Questo argomento descrive le azioni che l'utente del dispositivo deve intraprendere per la registrazione tramite Registrazione utenti guidata dall'account o Registrazione dispositivi guidata dall'account.

Procedura

1. Sul dispositivo, accedere a uno dei seguenti elementi:
    - Per dispositivo **iOS** - **Impostazioni** > **Generale** > **VPN** e **Gestione dispositivi**.
    - Per dispositivo **macOS** - **Impostazioni di sistema** > **Privacy e sicurezza** > **Profili**.
    - Per dispositivo **visionOS** - **Impostazioni** > **Generale** > **VPN** e **Gestione dispositivi**.
2. Andare ad **Accedi ad account scolastico o aziendale**.
3. Digitare l'indirizzo e-mail dell'account scolastico o aziendale. Assicurarsi che l'indirizzo e-mail sia conforme al formato seguente: nomeutente@<enterprise domain name>, per esempio, nomeutente@acme.com.
4. La pagina di accesso abbina automaticamente l'ID Apple gestito e guida l'utente nel flusso iReg. Assicurarsi di aver inserito le credenziali di Ivanti Neurons for MDM.
5. Digitare le credenziali dell'account scolastico o aziendale e fare clic su **Continua**.
6. Dopo l'autenticazione a 2 fattori la registrazione del dispositivo è terminata.

12.3.3. Registrazione dispositivo

Registrazione dispositivi, parte di Apple Business Manager, consente ai clienti di acquistare dispositivi in blocco e di registrare automaticamente tali dispositivi in MDM durante l'attivazione. Se si sceglie di aderire al programma, si può utilizzare Ivanti Neurons per MDM come server MDM per la gestione di tali dispositivi. Per ulteriori informazioni, vedere https://business.apple.com/.

Connessione di Ivanti Neurons per MDM a Registrazione dispositivi

Per utilizzare Ivanti Neurons per MDM come server MDM per Registrazione dispositivi, configurare il token server di Apple Business Manager in Ivanti Neurons per MDM.

Per ciascun server Apple Business Manager, sono disponibili le azioni seguenti in Ivanti Neurons per MDM:

- Verifica connessione
- Aggiungi un profilo Registrazione dispositivi
- Scarica chiave pubblica
- Sincronizzazione completa di Registrazione dispositivi - Avvia sincronizzazione completa. Il completamento dell'operazione può richiedere del tempo. Una volta completata la sincronizzazione, è possibile visualizzare le informazioni nella colonna Ultima sincronizzazione. Non è possibile avviare la sincronizzazione completa se questa è già in corso.

> Ivanti Neurons per MDM notifica agli amministratori quando la sincronizzazione di un server DEP non riesce, semplificando l'identificazione delle problematiche. Se si elimina un server DEP, il sistema elimina anche le relative notifiche.

- Carica nuovo token
- Elimina

> Le azioni **Modifica autenticazione** e **Assegna attributo dispositivo di Registrazione dispositivi** sono ora disponibili per i profili di registrazione dispositivo al posto della registrazione del dispositivo (server MDM).

Procedura

1. Andare in **Amministratore** > **Apple** > **Registrazione dispositivi**.
2. Fare clic su **Scarica chiave**.
3. Salvare la chiave di Ivanti Neurons per MDM.
4. Fare clic su **business.apple.com**.
5. Effettuare l'accesso utilizzando le credenziali Apple idonee per Registrazione dispositivi.
6. Nel sito Apple Registrazione dispositivi:
7. In Ivanti Neurons per MDM, fare clic su **Carica**.
8. Fare clic su **Inizia**.
9. Selezionare il telefono attendibile da utilizzare per l'autenticazione al servizio Apple.
10. Immettere il codice di verifica inviato al telefono selezionato.
11. Fare clic su **Aggiungi server MDM**.
12. Immettere un nome per l'identificazione del server virtuale MDM da utilizzare con il servizio.

13. Fare clic su **Avanti**.
14. Caricare la chiave pubblica scaricata precedentemente.
15. Fare clic su **Avanti**
16. Fare clic su **Server del token** per scaricare il token.
17. Fare clic su **Fine**.
18. Fare clic su **Avanti**.
19. Selezionare un'opzione di autenticazione:

- **Richiedere all'utente la registrazione / il login**

> Non supporta i dispositivi che operano con la piattaforma visionOS. Per registrare un dispositivo, utilizzare invece **Ignora login utente**.

> Agli utenti verranno richiesti il nome utente e la password. Gli utenti possono immettere una password o un PIN nel campo della password. Per i dispositivi macOS 15+, sono disponibili anche opzioni aggiuntive come **Face ID**, **Touch ID** o **chiave di sicurezza** per gli utenti iDP su identity provider supportati da passkey. Le preferenze per la password e il PIN possono essere configurate in **Utenti** > Impostazioni utente relative all'autenticazione.

- **Ignora login utente**

> I dispositivi assegnati a un utente anonimo o a un utente definito possono essere riassegnati a un utente specifico in un momento successivo nella pagina **Dispositivi**.

Selezionare una delle seguenti opzioni:

  - **Definisci un utente a cui assegnare tutti i dispositivi**
  - **Assegna tutti i dispositivi a un utente anonimo**

10. L'opzione selezionata sostituisce le selezioni in Impostazioni utente.

Fare clic su **Carica** per installare la chiave ricevuta al punto 3.

11. Compilare il modulo visualizzato per definire il profilo dei dispositivi Registrazione dispositivi:
12. Definire quali passaggi può saltare l'utente durante l'attivazione del dispositivo per le opzioni di configurazione seguenti:

Impostazione	Operazione da eseguire
Nome	Immettere un nome che identifichi il profilo Registrazione dispositivi.
Descrizione	Immettere una descrizione per il profilo.
Dipartimento	Immettere il dipartimento della propria organizzazione associato a questo profilo.
Modalità di supervisione	Abilita il controllo amministrativo aggiuntivo su configurazioni e restrizioni. Per i dispositivi iOS 13+ e macOS 10.15+, questa opzione è abilitata per impostazione predefinita.
iOS 17+	**Versione del sistema operativo per la registrazione** • **Richiedi la versione minima del sistema operativo per la registrazione**: l'amministratore può impostare una versione minima del sistema operativo richiesta per la registrazione dei dispositivi. Se il dispositivo non soddisfa i criteri di versione minima del sistema operativo, il sistema chiederà all'utente di aggiornare alla versione richiesta. Se l'utente rifiuta l'aggiornamento, la registrazione viene bloccata. **Versione più recente**: l'amministratore può impostare la versione più recente del sistema operativo per la registrazione dei dispositivi. Se il dispositivo non soddisfa i più recenti criteri di versione del sistema operativo, il sistema chiederà all'utente di aggiornare alla versione richiesta. Se l'utente rifiuta l'aggiornamento, la registrazione viene bloccata. **Versione specifica**: l'amministratore può impostare una versione minima del sistema operativo richiesta per la registrazione dei dispositivi. Se il dispositivo non soddisfa i criteri di versione minima del sistema operativo, il sistema chiederà all'utente di aggiornare alla versione richiesta. Se l'utente rifiuta l'aggiornamento, la registrazione viene bloccata. • **iOS minimo**: se la versione della build non è coerente con la versione del sistema operativo specificata nella chiave '**OSVersion**', la versione del sistema operativo avrà la precedenza. • **Versione build minima**: se la versione della build non è coerente con la versione del sistema operativo specificata nella chiave '**OSVersion**', la versione del sistema operativo avrà la precedenza. Questo campo è opzionale, se si inserisce un numero di build errato. • **Messaggio**: una descrizione dell'errore adatta a essere visualizzata dall'utente. Se necessario, ◦ il client farà un tentativo per visualizzare il messaggio, ma potrebbe non ◦ riuscirci, a causa delle condizioni locali. Come prassi si dovrebbe aggiungere il messaggio. • **Aggiungi dispositivi al programma beta** **Programmi beta per iOS**: applica le versioni software beta su iOS durante la Registrazione automatica dispositivi.
macOS 14+	**Versione del sistema operativo per la registrazione** • **Richiedi la versione minima del sistema operativo per la registrazione**: l'amministratore può impostare una versione minima del sistema operativo richiesta per la registrazione dei dispositivi. Se il dispositivo non soddisfa i criteri di versione minima del sistema operativo, il sistema chiederà all'utente di aggiornare alla versione richiesta. Se l'utente rifiuta l'aggiornamento, la registrazione viene bloccata. **Versione più recente**: l'amministratore può impostare la versione più recente del sistema operativo per la registrazione dei dispositivi. Se il dispositivo non soddisfa i più recenti criteri di versione del sistema operativo, il sistema chiederà all'utente di aggiornare alla versione richiesta. Se l'utente rifiuta l'aggiornamento, la registrazione viene bloccata.

Impostazione	Operazione da eseguire
	Versione specifica: l'amministratore può impostare una versione minima del sistema operativo richiesta per la registrazione dei dispositivi. Se il dispositivo non soddisfa i criteri di versione minima del sistema operativo, il sistema chiederà all'utente di aggiornare alla versione richiesta. Se l'utente rifiuta l'aggiornamento, la registrazione viene bloccata. • **macOS minimo**: se la versione della build non è coerente con la versione del sistema operativo specificata nella chiave '**OSVersion**', la versione del sistema operativo avrà la precedenza. • **Versione build minima**: se la versione della build non è coerente con la versione del sistema operativo specificata nella chiave '**OSVersion**', la versione del sistema operativo avrà la precedenza. Questo campo è opzionale, se si inserisce un numero di build errato. • **Messaggio**: una descrizione dell'errore adatta a essere visualizzata dall'utente. Se necessario, ◦ il client farà un tentativo per visualizzare il messaggio, ma potrebbe non ◦ riuscirci, a causa delle condizioni locali. Come prassi si dovrebbe aggiungere il messaggio. • **Aggiungi dispositivi al programma beta** **Programmi beta per macOS**: applica le versioni software beta su macOS durante la Registrazione automatica dispositivi.
Scarica e installa automaticamente aggiornamenti iOS	(Solo iOS 9.0) Se sul dispositivo è selezionata l'opzione Download automatici in **Impostazioni > iTunes & App Store**, gli aggiornamenti del sistema operativo verranno scaricati automaticamente, ma non installati, anche se l'opzione Profilo di registrazione dispositivo è disattivata. Questa impostazione sarà preferita quando è presente una configurazione Aggiornamenti software iOS applicabile ai dispositivi supervisionati con registrazione Registrazione dispositivi. Qualsiasi modifica a questa impostazione sarà applicabile al dispositivo supervisionato con registrazione Registrazione dispositivi, anche senza reimpostazione del dispositivo.
MDM rimovibile	Definisce la possibilità per l'utente di annullare la registrazione da MDM dopo aver eseguito la registrazione del dispositivo. Questa impostazione non è applicabile agli **iPad condivisi**.
MDM obbligatorio	Definisce l'impossibilità per l'utente di saltare i passaggi relativi all'installazione di MDM durante il processo di attivazione. Per i dispositivi iOS 13+ e macOS 10.15+, questa opzione è abilitata per impostazione predefinita.
Non utilizzare il profilo dal backup	Se abilitato, il dispositivo non utilizza questo profilo quando si ripristina il dispositivo da un backup. Applicabile solo per dispositivi iOS 26+ e visionOS 26+.
Consenti abbinamento	(Non applicabile per iOS 13+ e macOS 10.15+) Consente le funzioni di abbinamento host, come la sincronizzazione con iTunes. L'abbinamento è sempre consentito per gli host che dispongono di certificati di abbinamento validi.
Torna al servizio	Impostare **Torna al servizio** su **Vero** per garantire che l'applicazione venga conservata quando viene eseguita l'azione **Torna al servizio**. Ciò consente al dispositivo di acquisire un'istantanea delle applicazioni e di offrire un'esperienza più rapida durante il processo Torna al servizio. Se il dispositivo disabilitato è ancora in grado di

Impostazione	Operazione da eseguire
	effettuare l'azione Torna al servizio, l'applicazione deve essere scaricata nuovamente durante il processo di nuova registrazione. Per sfruttare la funzione **Apple Migration ABM**, questa funzione deve essere disabilitata. Il dispositivo non può essere migrato se **Torna al servizio** è impostato su **Vero**. Applicabile solo per dispositivi iOS 26+ e visionOS 26+.
Certificato	Fare clic su **+ Aggiungi** per caricare certificati.
Numero di telefono di assistenza	Fornire un numero di telefono che gli utenti possono chiamare per ricevere assistenza.
Indirizzo e-mail assistenza	Specificare un indirizzo e-mail a cui gli utenti possono scrivere per ricevere assistenza.
Personalizza registrazione	(iOS 13.0 e versioni successive e macOS 10.15 e versioni successive) Creare pagine Web di registrazione personalizzate. Specificare una pagina Web (visualizzazione Web) personalizzata per eseguire l'autenticazione di utenti durante la registrazione di dispositivi. Utilizzare questa pagina per visualizzare informazioni personalizzate, ad esempio il tipo di autenticazione, la personalizzazione, il testo del consenso e l'Informativa sulla privacy. Per ulteriori dettagli, consultare la sezione "*Aggiunta di una pagina Registrazione dispositivi personalizzata*" seguendo la procedura descritta. • Per abilitare la funzione, selezionare **Abilita registrazione personalizzata**. • Immettere l'**URL**, ad esempio https://mycustomweburl.com. Questo URL definisce il valore dell'URL personalizzato da mostrare all'utente in una visualizzazione Web.
Multiutente	(iOS 13.4 e versioni successive) iPad condiviso per le aziende La funzione consente alle aziende di condividere dispositivi tra vari dipendenti continuando a fornire un'esperienza personalizzata. Selezionare **Modalità multiutente** per consentire iPad condiviso in un dispositivo. Per ulteriori informazioni, vedere **iPad condiviso per le aziende**. • Questa impostazione non è applicabile ad Apple Education. • Seleziona l'impostazione **Modalità supervisionata** per modificare l'impostazione multiutente.
Dimensione quota	(iOS 13.4 e versioni successive) iPad condiviso per le aziende. Il valore è espresso in megabyte (MB) e indica la memoria allocata per un utente in un dispositivo. Se il valore è troppo piccolo, il dispositivo assegna una quota predefinita.
Utenti residenti	(iOS 13.4 e versioni successive) iPad condiviso per le aziende Il valore indica il numero di utenti che possono essere mantenuti o risiedere nel dispositivo. Se questo valore è superiore al numero massimo di utenti supportato dal dispositivo, il server MDM utilizza tale valore (numero massimo di utenti) come impostazione predefinita. Gli amministratori possono specificare il valore di Dimensione quota o quello di Utenti residenti. Se vengono specificati entrambi i valori, il server MDM utilizza Dimensione quota come impostazione predefinita.

Impostazione	Operazione da eseguire
Timeout sessione utente	(iOS 14.5 e versioni successive) iPad condiviso per le aziende Mostra il timeout di una sessione utente in secondi. Dopo il periodo di inattività specificato, la sessione utente si chiude automaticamente. Il valore minimo è 30 secondi. Se questo valore viene impostato su 0, il timeout viene rimosso e viene impostato il timeout predefinito del dispositivo. I valori da 1 a 29 non sono validi. Se viene specificato uno di questi valori, viene impostato il timeout predefinito del dispositivo.
Timeout sessione temporanea	(iOS 14.5 e versioni successive) iPad condiviso per le aziende Mostra il timeout in secondi di una sessione guest o temporanea. Dopo il periodo di inattività specificato, la sessione temporanea si chiude automaticamente. Il valore minimo è 30 secondi. Se questo valore viene impostato su 0, il timeout viene rimosso e viene impostato il timeout predefinito del dispositivo. I valori da 1 a 29 non sono validi. Se viene specificato uno di questi valori, viene impostato il timeout predefinito del dispositivo.
Consenti solo sessioni temporanee	(iOS 14.5 e versioni successive) iPad condiviso per le aziende Se ha valore True, l'utente vede solo il riquadro di benvenuto per l'ospite e può effettuare l'accesso solo come utente guest. Se ha valore False, l'utente può effettuare l'accesso utilizzando un ID Apple gestito (il comportamento attuale). Impostazione predefinita: false
Domini predefiniti Apple ID gestiti	(iOS 16.0+) iPad condiviso per le aziende Specificare un elenco di domini. Gli utenti possono selezionare il dominio del proprio account dall'elenco dei domini nella tastiera QuickType.
Periodo di tolleranza di autenticazione online	(iOS 16.0+) iPad condiviso per le aziende Specificare il numero di giorni in cui l'utente può accedere senza connettersi alla rete. Impostando questo valore a zero, l'autenticazione online viene eseguita ogni volta. **Predefinito**: 0
Tempo blocco automatico	(iOS 17.0+) Specifica il tempo (in secondi) dopo il quale il dispositivo passa alla modalità di sospensione. Il valore minimo è 120 secondi.
Periodo di tolleranza per il blocco del passcode	Specifica il tempo (in secondi) dopo il quale l'utente del dispositivo deve inserire il passcode per sbloccarlo. Il valore minimo è 0 secondi e il valore massimo è 14400 secondi.
Fuso orario	Specificare il fuso orario a cui deve appartenere il dispositivo. **Esempio**: Pacific/Midway

Opzioni di configurazione

- Salta immissione del passcode - Se si seleziona questa opzione, vengono automaticamente abilitate Ignora configurazione Apple Pay e Ignora Touch ID.
- Salta servizi di geolocalizzazione
- Salta ripristino dal backup
- Salta "Passa ad iOS" da Android
- Salta Condizioni per l'utilizzo del servizio
- Salta accesso ad AppleID e iCloud - Selezionando questa opzione si attiva automaticamente Ignora configurazione Apple Pay.
- Ignora configurazione Touch ID (solo iPhone 5s, 6, 6+, iPad Air 2, iPad Mini 3) - Selezionando questa opzione si attiva automaticamente Ignora configurazione Apple Pay.
- Ignora configurazione Apple Pay (solo iPhone 6, 6+, iPad Air 2, iPad Mini 3)
- Ignora configurazione zoom
- Salta Siri
- Ignora intelligenza (iOS 18+ e macOS 15+)
- Salta invio automatico di informazioni di diagnostica
- Salta archiviazione cloud (iOS 10.3 e versioni successive, macOS 10.13.4 e versioni successive)
- Salta configurazione toni display (iOS 9 e versioni successive, macOS 10.14 e versioni successive)
- Salta sensibilità pulsante Home
- Salta schermata di selezione tastiera
- Salta schermate di inserimento informative - Si tratta di informazioni per la formazione dell'utente. Ad esempio: copertina, multitasking e Centro di Controllo.
- Salta la schermata per la migrazione di Apple Watch
- Salta la schermata Preferenze aspetto (iOS 13.0+ e macOS 10.14+)
- Salta Tempo allo schermo (versioni iOS 12.0+ e macOS 10.15+)
- Salta privacy (macOS 10.13.4 e versioni successive, tvOS 11.3+ e versioni successive)
- Ignora abilitazione modalità blocco (iOS 17.1+ e macOS 14.0+)
- Salta aggiornamento software (iOS 12.0+ & macOS 15.4+)
- Ignora il riquadro relativo all'aggiunta del piano cellulare (iPhone Xs, iPhone Xs Max, iPhone XR)
- Mostra il testo personalizzato nella pagina di accesso. Selezionare questa opzione per immettere un messaggio di testo personalizzato nella casella di testo. Questo messaggio verrà visualizzato nella pagina di accesso sul dispositivo durante la configurazione Registrazione dispositivi per fornire eventuali informazioni aggiuntive agli utenti finali e guidarli nel processo.
- Configurazione Avanzamento automatico: selezionare questa opzione per configurare l'assistente in modo che avanzi automaticamente tra le schermate di configurazione del dispositivo. L'impostazione predefinita è impostata su false. Supportata su tvOS e macOS 11 e versioni successive. La configurazione Avanzamento automatico non funziona su una connessione Wi-Fi, il dispositivo deve essere connesso a una rete Ethernet.
- Termini di indirizzo - Ignora il riquadro Termini di indirizzo. (iOS 16+)
- Saltare il riquadro Liquid Glass (iOS 27.0+ e macOS 27.0+)

Opzioni di configurazione
iOS
• Salta riquadro Inizia (13.0+) • Salta iMessage e FaceTime (12,0+) • Ignora lingua parlata (13.0+) • Salta Ripristino completato (14.0+) • Salta Aggiornamento completato (14.0+) • Ignora sicurezza (16.0+) • Ignora il riquadro di impostazione del pulsante Azione (17.0+) • Ignora riquadro filtraggio contenuti web (18.2+) • Salta riquadro sicurezza e gestione (18.4+) • Ignora il riquadro multitasking (26.0+) • Ignora il riquadro Showcase sistema operativo (26.0+) • Saltare il riquadro Aspetto accessibilità (27.0+) **macOS** • Salta la schermata iCloud Analytics • Salta la schermata True Tone Display (10.13.6+): (opzionale) selezionare questa opzione per saltare la finestra True Tone Display. • Ignora Accessibilità (11.0+) • Ignora sblocco con Watch (12.0+) • Ignora abilitazione modalità blocco (14.0+) • Ignora selezione sfondo (14.1+) • Ignora il riquadro Privacy impostazioni aggiuntive (26.0+) • Salta Aggiornamento completato (26.0+) **tvOS**
• Salta la schermata di sincronizzazione layout della schermata iniziale di Apple TV • Salta la schermata di accesso del provider di Apple TV • Salta opzione Tocca per configurare • Salta Configurazione screen saver modalità aereo
Opzioni assistente configurazione account macOS
• Salta creazione account amministratore • Salta creazione account configurazione principale • Crea account principali come utenti regolari (come amministratore se la casella non è selezionata)
Attendere la configurazione del dispositivo durante l'Impostazione registrazione dispositivo

Opzioni di configurazione
• Attendere che le configurazioni e le applicazioni ad alta priorità siano inviate ai dispositivi - Selezionare per inviare le configurazioni e le applicazioni ad alta priorità al dispositivo prima di continuare con le altre schermate di impostazione Registrazione dispositivo. Questa impostazione impedisce all'utente finale di utilizzare il dispositivo prima che le configurazioni richieste e le applicazioni ad alta priorità vengano trasferite sul dispositivo. • Limite di tempo: il limite di tempo predefinito è di 3 minuti. Il tempo massimo è di 10 minuti. Per attivare questa funzione, selezionare l'opzione **Modalità di supervisione** durante la modifica del profilo Registrazione dispositivi.

Fare clic su **Salva**.

La tabella seguente viene popolata nella pagina **Amministratore** > **Apple** > **Registrazione dispositivo**:

Impostazione	Operazione da eseguire
Nome (Fare clic sull'intestazione della colonna per ordinarla in senso alfanumerico.) Utilizzare il campo Ricerca per ricercare gli elementi da questa colonna	Nome server MDM
Nome account Apple (Fare clic sull'intestazione della colonna per ordinarla in senso alfanumerico.) Utilizzare il campo Ricerca per ricercare gli elementi da questa colonna	ID Apple gestito
Numero di dispositivi	Conteggio dispositivi assegnati
Profilo(i) di registrazione	Conteggio profili registrazione dispositivi assegnati
Ultima sincronizzazione (Fare clic sull'intestazione della colonna per ordinarla in senso alfanumerico.)	Ora ultimo contatto
Scadenza token (Fare clic sull'intestazione della colonna per ordinarla in senso alfanumerico.)	Data di scadenza token

- Quando si aggiungono nuovi dispositivi a Registrazione dispositivi Apple, potrebbero essere necessari fino a 15 minuti prima che Ivanti Neurons per MDM riesca a individuarli. Ai nuovi dispositivi viene quindi assegnato un profilo di registrazione. Se non è possibile aggiungere nuovi dispositivi a Registrazione dispositivi, andare a **Dashboard > Notifiche** per verificare la presenza di notifiche Apple per Registrazione dispositivi. Se sono disponibili aggiornamenti al Contratto di licenza con l'utente finale, l'utente riceverà una notifica tramite e-mail con i passaggi per accettare il nuovo Contratto di licenza con l'utente finale.
- È possibile visualizzare tutti gli attributi personalizzati del dispositivo esistenti nel tenant e assegnarli ai dispositivi durante la registrazione mediante Apple Registrazione dispositivi.
- Nei dispositivi macOS condivisi, il comando ListUsers mostra un elenco di tutti gli utenti locali sul dispositivo e solo i dettagli dell'ultimo check-in dell'utente che ha registrato il dispositivo.

Modifica del profilo Registrazione dispositivi

Procedura

1. Andare in **Amministratore** > **Apple** > **Registrazione dispositivi**.
2. Individuare il nome del server Apple Business Manager (creato nel sito Apple) nella colonna Nome account Apple.
3. Fare clic sul collegamento numerato nella colonna Profilo/i registrazione.
4. Per un profilo specifico, selezionare **Azioni** > **Modifica profilo registrazione dispositivi**.
5. Aggiornare e salvare il profilo.

- Se un profilo Registrazione dispositivi viene modificato, il numero di dispositivi per il profilo modificato viene aggiornato dopo pochi istanti.
- Se si aggiorna il token del server sul sito Apple, il token esistente non sarà più valido. Tuttavia, il contenuto della pagina Registrazione dispositivi, inclusa la data di scadenza del token, continuerà a essere visualizzato fino al caricamento del nuovo token.
- Se viene creato o modificato un profilo di registrazione del dispositivo, le modifiche apportate al profilo possono essere visualizzate nella sezione Audit Trails. Facendo clic sul link in Dettagli, è possibile visualizzare gli Attributi e le modifiche apportate agli attributi nelle colonne Prima e Dopo. È possibile notare lo stato di ciascun Profilo di registrazione dispositivo come Creato (per un nuovo profilo), Aggiornato (per la modifica di un profilo esistente) o Eliminato (per l'eliminazione di un profilo esistente). Per filtrare i Profili di registrazione dispositivi in Audit Trails, è necessario selezionare Sistema amministratore come Categoria e Tipo registrazione dispositivo automatizzato come Tipo.

Il Profilo registrazione dispositivi contiene i seguenti dettagli:

Impostazione	Operazione da eseguire
Nome profilo (Fare clic sull'intestazione della colonna per ordinarla in senso alfanumerico.)	Immettere un nome che identifichi il profilo Registrazione dispositivi.
Descrizione (Fare clic sull'intestazione della colonna per ordinarla in senso alfanumerico.)	Immettere una descrizione per il profilo.
Dipartimento (Fare clic sull'intestazione della colonna per ordinarla in senso alfanumerico.)	Immettere il dipartimento della propria organizzazione associato a questo profilo.
Numero di telefono di assistenza (Fare clic sull'intestazione della colonna per ordinarla in senso alfanumerico.)	Fornire un numero di telefono che gli utenti possono chiamare per ricevere assistenza.
Numero di dispositivi	Visualizza il numero di dispositivi per il profilo
Azioni	Gestisci profili

Gestione di più profili Registrazione dispositivi

È possibile creare più profili Registrazione dispositivi per ciascun server Apple Business Manager. In questo modo è possibile assegnare configurazioni diverse a set di dispositivi diversi. È inoltre possibile spostare i dispositivi da un profilo Registrazione dispositivi all'altro.

Procedura

1. Andare in **Amministratore** > **Apple** > **Registrazione dispositivi**.
2. Individuare il nome del server Apple Business Manager nella colonna Nome account Apple.
3. Fare clic sul collegamento numerato nella colonna Profilo/i registrazione.

4. Per creare un nuovo profilo Registrazione dispositivi da associare al server selezionato, fare clic su **Crea nuovo profilo**. Creare e salvare il profilo.
5. Per gestire i singoli profili, fare clic su **Azioni** e selezionare una delle opzioni seguenti:
    - **Imposta come profilo predefinito**: consente di impostare il profilo selezionato come predefinito all'interno dello stesso server virtuale. Tale profilo predefinito verrà assegnato alla registrazione dei nuovi dispositivi.
    - **Modifica profilo**: consente di aggiornare il profilo esistente.
    - **Modifica autenticazione** - Modifica l'impostazione di autenticazione di Registrazione dispositivi.
    - **Assegna attributo dispositivo di Registrazione dispositivi** - Gli amministratori utilizzano gli attributi personalizzati per i dispositivi per associare le proprietà aggiuntive con questi oggetti. È possibile utilizzare queste proprietà per creare gruppi o distribuire configurazioni.
    - **Elimina:** il profilo predefinito non può essere eliminato. Quando viene eliminato un profilo non predefinito, tutti i dispositivi associati vengono riassegnati al profilo predefinito.
6. Per spostare un dispositivo registrato da un profilo all'altro all'interno dello stesso server virtuale (e non fra server Apple Business Manager diversi), fare clic sul collegamento numerato nella colonna Numero di dispositivi. La riassegnazione dei profili è applicabile ai dispositivi che non sono ancora stati registrati.
    1. Per spostare un singolo dispositivo, fare clic su **Assegna profilo registrazione** accanto al dispositivo specifico, selezionare il profilo dall'elenco a discesa, quindi fare clic su **Assegna**.
    2. Per spostare più dispositivi, selezionarli e fare clic su **Azioni** > **Assegna profilo di registrazione**, selezionare il profilo nell'elenco a discesa, quindi fare clic su **Assegna**.

- Se un profilo Registrazione dispositivi viene modificato, il numero di dispositivi per il profilo modificato viene aggiornato dopo pochi istanti.
- Se si aggiorna il token del server sul sito Apple, il token esistente non sarà più valido. Tuttavia, il contenuto della pagina Registrazione dispositivi, inclusa la data di scadenza del token, continuerà a essere visualizzato fino al caricamento del nuovo token.

Aggiunta di una pagina Web Registrazione dispositivi personalizzata

Applicabile a: iOS 13.0 e macOS 10.15 e versioni successive supportate

Nella sezione Personalizza registrazione, è possibile specificare una pagina Web (visualizzazione Web) personalizzata per eseguire l'autenticazione di utenti durante la registrazione di dispositivi. Utilizzare questa pagina per visualizzare informazioni personalizzate, ad esempio il tipo di autenticazione, la personalizzazione, il testo del consenso e l'Informativa sulla privacy.

Procedura

1. Andare in **Amministratore** > **Apple** > **Registrazione dispositivi**.
2. Trovare il nome del server creato sul sito Apple.
3. Selezionare **Azioni** > **Modifica profilo registrazione dispositivi**.
4. Nella sezione Personalizza registrazione, selezionare **Abilita registrazione personalizzata**.
5. Selezionare una delle seguenti opzioni:
    - **Pagina Web ospitata di MobileIron**: si viene reindirizzati a un provider di identità (IDP), se la registrazione utilizza un provider di identità come Microsoft Active Directory Federation Services (ADFS) o Okta. Si può anche essere reindirizzati al portale

self-service nel caso di un Ivanti Neurons per MDMutente con autenticazione non basata su IDP.

- **URL personalizzato**: inserire un URL, ad esempio https://mycustomweburl.com. Questo URL definisce il valore dell'URL personalizzato da mostrare all'utente in una visualizzazione Web caricata durante la configurazione iniziale di un nuovo dispositivo Registrazione dispositivi o di un dispositivo cancellato. Utilizzare questo campo per definire la propria interfaccia utente di autenticazione con il metodo di autenticazione. Una volta autenticato l'utente, viene scaricato il profilo di registrazione MDM.

Flusso di lavoro della pagina Web Registrazione dispositivi personalizzata

In questa sezione viene descritto il comportamento della pagina Web Registrazione dispositivi personalizzata e la procedura per creare una pagina Web (visualizzazione Web) personalizzata.

Inizialmente, quando la pagina Web personalizzata specificata nel campo **URL** viene caricata:

- L'URL Web di configurazione presenta uno schema **https** e corrisponde a una richiesta **GET**. La pagina Web deve utilizzare un certificato pubblicamente attendibile.
- Un'intestazione personalizzata **x-apple-aspen-deviceinfo** viene aggiunta alla richiesta GET dal dispositivo Apple in cui è stata avviata la registrazione. Tale intestazione contiene la codifica base64 di una busta CMS (Cryptographic Message Syntax) contenente un plist con attributi dispositivo. Si tratta delle stesse informazioni, nello stesso formato, contenute nella richiesta POST iniziale con registrazioni di dispositivi basate su token.

Successivamente, quando la pagina Web personalizzata viene caricata:

- L'utente del dispositivo interagisce con la pagina Web (visualizzazione Web) finché il server host dell'amministratore fornisce un file **custom.mobileconfig** al client. Il server Ivanti Neurons per MDM restituisce il codice byte del profilo MDM. Nel server host dell'amministratore, il file custom.mobileconfig deve essere impostato con il tipo MIME **application/x-apple-aspen-config** affinché il profilo MDM del dispositivo venga scaricato e installato sul dispositivo.
- Per l'autenticazione con Ivanti Neurons per MDM, la pagina Web deve contenere le credenziali (nome utente e password) di autenticazione. Si consiglia di creare un utente separato in Ivanti Neurons per MDM e assegnare il ruolo Personalizza registrazione all'utente che recupera il profilo MDM con l'URL del server Ivanti Neurons per MDM (ad esempio, https://micloudDomain.com/c/i/dep/custom.mobileconfig).
- Per la registrazione di dispositivi e per ottenere il profilo MDM da Ivanti Neurons per MDM, il server Web host dell'amministratore deve effettuare una chiamata POST all'URL del server Ivanti Neurons per MDM. Inoltre, deve inoltrare l'intestazione x-apple-aspen-deviceinfo con il valore fornito dal dispositivo quando quest'ultimo utilizza GET URL per caricare la pagina Web personalizzata. Se l'ID utente di registrazione non viene fornito, il dispositivo viene assegnato a un utente anonimo. Dettagli aggiuntivi:
  - Se un dispositivo utilizza l'URL Web personalizzato configurato nel profilo Registrazione dispositivi, il server Web host dell'amministratore deve acquisire l'intestazione "x-apple-aspen-deviceinfo" presentata dal dispositivo.
  - Per ottenere il profilo MDM del dispositivo e il relativo utente, il server Web host dell'amministratore deve effettuare una chiamata POST all'URL del server Ivanti Neurons per MDM con l'intestazione x-apple-aspen-deviceinfo. Inoltre, deve contenere informazioni di autenticazione di base utilizzando un ID utente Ivanti Neurons per MDM come parametro di richiesta (ad esempio, https://miCloudDomain.com/c/i/dep/custom.mobileconfig?user=name@company.com). L'utente deve essere assegnato al ruolo Personalizza registrazione.
  - Una volta che il server Web host dell'amministratore ha ricevuto il codice byte, deve scaricare quest'ultimo sul dispositivo impostando intestazioni di risposta, Content-Disposition = attachment;filename="profile.mobileconfig" e Content-Type = application/x-apple-aspen-config.

- La visualizzazione Web viene chiusa e il sistema operativo tenta di installare il profilo (che deve essere un profilo di registrazione MDM).

> Ivanti Neurons per MDM non esegue l'autenticazione dell'ID utente per cui viene restituito il profilo MDM. Pertanto, gli amministratori devono eseguire necessariamente l'autenticazione dell'ID utente prima di richiedere il profilo MDM.

Per iOS, questo flusso di lavoro è supportato durante la configurazione iniziale di un dispositivo cancellato. Per macOS, questo flusso di lavoro è supportato all'interno di Assistente configurazione e tramite il riquadro Preferenze profili, se la funzione Registrazione dispositivi è stata ignorata durante l'esecuzione di Assistente configurazione.

Per informazioni dello sviluppatore relative alla creazione di una pagina Web personalizzata, consultare i seguenti riferimenti alla documentazione Apple:

- **Visualizzazioni Web**
- **Autenticazione tramite visualizzazioni Web**
- **Esempio di codice per implementare un esempio di browser Web per iPad in grado di visualizzare la versione desktop o mobile di un sito Web**

Modifica dell'impostazione di autenticazione di Registrazione dispositivi

Procedura

1. Andare in **Amministratore** > **Apple** > **Registrazione dispositivi**.
2. Trovare il nome del server creato sul sito Apple.
3. Selezionare **Azioni** > **Modifica autenticazione**.

Gestione dei token bootstrap per gli account dei dispositivi mobili

Applicabile a: dispositivi macOS 10.15 e versioni successive supportate, registrati in MDM tramite Apple School Manager o Apple Business Manager.

Ivanti Neurons per MDM supporta la gestione dei token bootstrap per gli account dei dispositivi mobili. I token bootstrap consentono di utilizzare gli account dei dispositivi mobili per accedere a dispositivi macOS che utilizzano FileVault. Quando si utilizza questa funzionalità, tutti gli account per dispositivi mobili che effettuano l'accesso ricevono automaticamente un token sicuro. Questa funzionalità è utile quando più utenti effettuano l'accesso a un sistema cifrato.

Quando un account amministratore gestito tenta di effettuare l'accesso a un dispositivo:

- Al primo accesso, viene richiesto il token bootstrap al server MDM.
- Se il server MDM fornisce il token bootstrap, il dispositivo crea automaticamente un token sicuro per l'account.
- Il dispositivo abilita FileVault per l'utente.

Token bootstrap disponibile è un campo disponibile nella pagina dei dettagli del dispositivo e come attributo di filtraggio durante la creazione di un nuovo gruppo di dispositivi o di una policy personalizzata.

Ai fini della risoluzione dei problemi e della verifica, accedere ai dettagli del dispositivo. Utilizzare la pagina Registri per limitare il numero di registri dei dispositivi applicando filtri basati sui nomi delle azioni Imposta token bootstrap e Recupera token bootstrap.

Impostazione dell'account amministratore macOS gestito mediante Registrazione dispositivi

Ivanti Neurons per MDM supporta la registrazione Registrazione dispositivi nei dispositivi su cui sono state reimpostate le impostazioni di fabbrica predefinite o che sono stati attivati per la prima volta. Registrazione dispositivi consente di creare un account amministratore sul dispositivo macOS. Ivanti Neurons per MDM supporta solo la registrazione facoltativa per macOS e, di conseguenza, Ivanti Neurons per MDM ignora il campo **MDM obbligatorio**, nel profilo Registrazione dispositivi poiché è valido solo per i dispositivi iOS.

Procedura

1. Andare in **Amministratore > Apple > Registrazione dispositivi**.
2. Trovare il nome del server creato sul sito Apple.
3. Selezionare **Azioni > Modifica profilo registrazione dispositivi**.
4. Selezionare una delle seguenti opzioni dell'assistente configurazione per l'account macOS:
    - **Salta creazione account amministratore** - Selezionare questa opzione per non consentire di creare un account amministratore, che sia visibile o nascosto. Deselezionare questa opzione per consentire la creazione di un account amministratore nella sezione **Configura account amministratore macOS gestito** (descritta di seguito).
    - **Salta creazione account configurazione principale**. Selezionare questa opzione per saltare l'impostazione dell'account principale nel dispositivo macOS. Non viene creato alcun account utente oltre all'account amministratore. Viene visualizzata la sezione aggiuntiva **Configura account amministratore MacOS gestito** (descritta di seguito) per creare l'account amministratore macOS gestito. L'account può inoltre essere nascosto da Utenti e gruppi.
    - **Crea account principali come utenti regolari (come amministratore se la casella non è selezionata)** - Selezionare questa opzione per creare un account standard non amministratore come parte della registrazione. In ogni caso l'amministratore può creare un account amministratore e inviarlo al dispositivo. Viene visualizzata la sezione aggiuntiva **Configura account amministratore MacOS gestito** (descritta di seguito) per creare l'account amministratore macOS gestito. L'account può inoltre essere nascosto da Utenti e gruppi.

Dopo avere selezionato una delle opzioni riportate sopra, immettere i seguenti dettagli nella sezione **Configura account amministratore macOS gestito** se si desidera creare un account amministratore macOS gestito:

- Nome completo
- Nome account
- Password
- Conferma password
- (Facoltativo) Nascondi account amministratore gestito in Utenti e gruppi

Se non si seleziona **Salta creazione account configurazione principale**, inserire i seguenti dettagli nella sezione **Configura account primario**. Questo aggiunge il supporto del canale utente per l'account di amministrazione gestito impostando il nome breve dell'utente locale gestito sul nome breve di un amministratore.

- **Nome completo**
- **Nome breve**
- (Facoltativo) **Impedisci modifica da parte dell'utente finale** - Questa impostazione sarà sovrascritta se "Nome completo" e/o "Nome breve" hanno variabili di sostituzione e sono valutati come vuoti. Se si seleziona questa opzione, confermare di avere compreso che questa configurazione di account amministratore primario è applicabile solo se una delle opzioni indicate di seguito è impostata correttamente:

    1. La voce Richiedi registrazione/accesso utente è selezionata nella vista di configurazione di Autenticazione.
    2. La pagina Web ospitata di MobileIron è selezionata per la personalizzazione della registrazione.
7. Selezionare **Salta creazione account configurazione principale** per abilitare il supporto del canale utente per l'account di amministrazione gestito. È possibile impostare il nome breve dell'utente locale gestito sul nome breve di un amministratore.
8. Fare clic su **Salva**.

Modifica della password dell'account amministratore macOS locale

Gli amministratori possono modificare la password locale di un account amministratore macOS locale creata dall'assistente alla configurazione durante la registrazione Registrazione dispositivi.

Applicabile a: macOS 10.11 o versioni successive supportate.

Procedura

1. Andare su **Dispositivi**.
2. Fare clic sul nome utente al quale è associato il dispositivo per visualizzare la pagina dei dettagli del dispositivo.
3. Nel menu Azioni, fare clic su **Imposta password amministratore macOS**. Questa azione può essere eseguita anche nella pagina Elenco dispositivi selezionando uno o più dispositivi.
4. Immettere la password.
5. Fare clic su **Salva**.

Esporta in CSV

Ivanti Neurons per MDM consente di esportare i dispositivi Dispositivo registrato in un file CSV.

Procedura

1. Andare in **Amministratore** > **Apple** > **Registrazione dispositivi**.
2. Fare clic sul collegamento di conteggio dei dispositivi specifici sotto la colonna **Numero di dispositivi**.
3. Fare clic sull'opzione **Esporta in CSV** per esportare l'elenco di dispositivi e i dettagli correlati in un file CSV. Una volta che il report è pronto, all'utente verrà mostrato un messaggio per scaricare o eliminare il report. Si riceverà anche un'e-mail contenente un link per scaricare il report.
4. Fare clic su **Download**.
5. (Opzionale) Fare clic su **Elimina** per eliminare il report.

12.3.4. Registrazione alla beta

Ivanti Neurons per MDM può registrare automaticamente i dispositivi da remoto in un secondo momento se il dispositivo è supervisionato e utilizza iOS 18, iPadOS 18, macOS 15 o versioni successive. Se necessario, un dispositivo supervisionato può essere rimosso dai programmi beta e impedire a un utente di registrarsi manualmente. In questo modo si elimina la necessità di passaggi manuali da parte dell'utente e si semplifica il processo durante l'intero ciclo di vita del beta testing.

Prerequisiti

- La registrazione del dispositivo è obbligatoria per la registrazione Beta. Per maggiori informazioni sulla registrazione dei dispositivi, vedere **Registrazione dispositivo**.
- Per offrire le versioni beta di AppleSeed per IT senza la necessità di un account Apple, un amministratore di Apple Business Manager o Apple School Manager deve accedere al portale AppleSeed per IT e accettare i termini e le condizioni per conto della propria organizzazione per l'attuale periodo beta.

Collegamento Ivanti Neurons per MDM alla registrazione Beta

Per utilizzare Ivanti Neurons per MDM come server MDM per la registrazione alla versione beta, configurare il token del server Apple Business Manager o Apple School Manager in Ivanti Neurons per MDM.

Sezione di registrazione alla beta

Nome	Descrizione
Nome organizzazione	Nome dell'organizzazione.
Ultima sincronizzazione	Data e ora in cui è stata eseguita la sincronizzazione.
Stato	Stato della sincronizzazione.
Sincronizzazione del token di registrazione alla versione beta	Fare clic su **Sincronizza** per sincronizzare i nuovi token di registrazione Beta disponibili per gli aggiornamenti beta.

12.3.5. Configurazione dell'assistente di installazione

L'assistente di configurazione permette di selezionare le schermate di configurazione da saltare o includere durante la configurazione del dispositivo per i dispositivi iOS e macOS.

Procedura

1. Accedere alla console amministrativa Ivanti Neurons per MDM .
2. Accedere a **Configurazioni**.
3. Selezionare **Assistente di configurazione**.
4. Fare clic sull'icona della matita (modifica).
5. Selezionare le caselle di controllo per saltare le schermate di configurazione specifiche del dispositivo.
6. Fare clic su **Fine**.
7. Selezionare **Canale dispositivo**.
8. Selezionare **Tutti i dispositivi**. La configurazione di Assistente configurazione viene inoltrata ai dispositivi e la scheda Configurazione nella pagina Dettagli dispositivo mostra lo stato Installato.
9. Accedere al dispositivo. Tutte le schermate di impostazione iniziale vengono saltate.

12.3.6. Installa certificato MDM

Per gestire i dispositivi iOS, e necessario richiedere e installare un certificato Apple MDM. È inoltre necessario rinnovare tale certificato con cadenza annuale. (L'account Apple utilizzato per creare il certificato riceve una notifica dal sito Apple quando la data di scadenza si avvicina). Usa la pagina del certificato MDM per aggiungere o rinnovare questo certificato.

Acquisizione e installazione del certificato MDM

Procedura

1. Utilizzare la pagina **Certificato MDM** per scaricare una richiesta di firma del certificato (CSR) dal proprio tenant Ivanti Neurons for MDM.
2. Caricare la CSR su Apple per creare un nuovo certificato.
3. Sul sito Apple, aggiungere una nota in cui è indicato l'oggetto di riferimento del certificato. Questa nota sarà di supporto al momento del rinnovo del certificato.
   Salvare il certificato risultante.
4. Installare il certificato per il proprio tenant Ivanti Neurons for MDM.

Rinnovo del certificato MDM

Procedura

1. Fare clic su **Rinnova certificato**.
2. Scaricare una richiesta di firma del certificato (CSR) dal tenant di Ivanti Neurons for MDM.
3. Caricare il CSR su Apple per rinnovare il certificato corrispondente.
4. Sul sito Apple, assicurarsi che si stia rinnovando il certificato corretto. Se si carica un certificato diverso in Ivanti Neurons for MDM, tutti i dispositivi iOS registrati vengono dismessi.
   Installare il certificato per il proprio tenant Ivanti Neurons for MDM.

Se si tenta di caricare il certificato sbagliato, verrà visualizzato un avviso.

Se non è possibile visualizzare la pagina **Installa certificato MDM**, è probabile che non si disponga delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:

- Gestione sistemi
- Sistema di sola lettura

12.3.7. Dispositivi iPad condivisi per business

I dispositivi iPad condivisi per le aziende sono disponibili per gli ID Apple gestiti che vengono creati in Apple Business Manager con iOS 13.4 o versioni più recenti supportate.

- I dispositivi iPad condivisi permettono alle aziende di condividere i dispositivi tra più dipendenti, pur fornendo un'esperienza personalizzata.
- I dipendenti possono accedere con un ID Apple gestito per iniziare a caricare i loro dati, compresi gli account di posta, i file, la libreria fotografica iCloud, i dati delle app e altro ancora.
- I dati sono memorizzati in iCloud, quindi i dipendenti possono accedere a qualsiasi dispositivo iPad condiviso appartenente all'organizzazione.

I dispositivi iPad condivisi possono essere utilizzati in applicazioni sanitarie, di vendita al dettaglio e industriali. Per esempio, medici e infermieri possono condividere un dispositivo iPad, dato che ognuno può accedere in modo sicuro al profilo utente progettato unicamente per le proprie mansioni. Nei negozi al dettaglio, i lavoratori in prima linea possono essere autorizzati ad accedere alle informazioni sui prodotti, alle risorse e alle competenze per poter venire incontro alle esigenze dei clienti e fornire una migliore esperienza di acquisto.

Come funziona

- I dispositivi iPad vengono aggiunti ad Apple Business Manager e vengono registrati utilizzando un profilo di registrazione automatica con la modalità condivisa attiva.
- I dipendenti accedono al dispositivo iPad condiviso con un ID Apple gestito e una password forniti dall'azienda. L'amministratore di Apple Business Manager può creare manualmente gli account per gli utenti o delegare la creazione degli account a un provider di identità come Entra ID.
- Ogni utente può avere il suo profilo personalizzato quando è connesso al dispositivo iPad condiviso. Gli amministratori possono distribuire le app in base al ruolo, alle responsabilità e al reparto degli utenti.
- Gli utenti possono accedere come utenti ospiti su un dispositivo iPad condiviso. Il log-in dell'utente ospite è abilitato per impostazione predefinita. Un utente ospite non ha bisogno di accedere con un ID Apple gestito e una password. Il login dell'utente ospite può essere disabilitato impostando l'opzione **Consenti sessione guest per iPad condiviso** su **Falso** nella configurazione **Limitazioni iOS**.
- Andare su Ivanti Neurons per MDM **> Dispositivi**, fare clic sul nome di un dispositivo iPad condiviso e fare clic sulla scheda **Utenti** per visualizzare l'elenco degli utenti sul dispositivo e i loro dettagli (come ID Apple gestito, Dati disponibili in byte, Dati utilizzati in byte, Presenta dati da sincronizzare in Ivanti Neurons for MDM).
- Andare alla scheda **Registri** e dai filtri selezionare l'azione **Segnala elenco utenti** per visualizzare ulteriori dettagli sugli utenti.
- Il log-in dell'utente ospite in un dispositivo iPad condiviso è diverso dalla gestione dell'utente ospite da parte di Ivanti Neurons per MDM. Per impostazione predefinita, l'account di utente guest è disattivato in Ivanti Neurons per MDM. Per gestire un utente ospite in un dispositivo iPad condiviso, abilitare l'account utente ospite.
- La registrazione dello schermo è disponibile dal Centro di controllo sui dispositivi iPad condivisi.
- Ivanti Neurons per MDM supporta una variabile di sostituzione per l'ID Apple gestito, `${managedAppleID}`. Questa variabile di sistema viene visualizzata nella sezione degli attributi di sistema e nella sezione degli attributi del dispositivo.
- Ivanti Neurons per MDM limita un amministratore dal cambiare l'ID Apple gestito degli utenti residenti che erano collegati al dispositivo iPad condiviso in passato insieme agli utenti attualmente collegati. Se si prova a cambiare l'ID Apple gestito, un messaggio di errore indica che l'ID Apple gestito dell'utente non può essere cambiato poiché l'utente sta usando un dispositivo iPad condiviso.

- In caso di **Apple App e libri**, App e libri viene installata sui dispositivi iPad condivisi sulla base delle licenze basate sul dispositivo, indipendentemente dal fatto che le licenze basate sul dispositivo siano selezionate o meno.

Prerequisiti

Verificare che i prerequisiti seguenti siano soddisfatti:

- Un dispositivo iPad condiviso richiede l'ID Apple gestito. Gli amministratori possono creare manualmente gli account o delegare un provider di identità come Entra ID.
- I dispositivi iPad condivisi devono contenere iOS 13.4 o versioni più recenti supportate.
- I dispositivi devono essere associati agli account Apple Business Manager.
- I dispositivi devono contenere un'unità di archiviazione da almeno 32 GB.

Tenere presenti i seguenti punti:

- Ivanti Neurons per MDM limita alcune configurazioni, come il Passcode, per i dispositivi iPad condivisi, poiché Apple non le supporta. Tali configurazioni non vengono inviate ai dispositivi (Dispositivi > fare clic sul collegamento a un nome dispositivo > scheda Configurazioni).
- La configurazione **Passcode** non si applica ai dispositivi iPad condivisi, in quanto richiedono ID Apple gestiti, associati a password e non a passcode. L'azione Sblocca dal portale amministrativo Ivanti Neurons per MDM non cancellerà il passcode su un dispositivo iPad condiviso.
- Selezionare il canale dispositivo o il canale utente durante la distribuzione della configurazione **Limitazioni iOS** ai dispositivi iPad condivisi. È possibile distribuire configurazioni separate e applicare restrizioni che sono applicabili solo al canale dispositivi o al canale utenti.
- Ivanti Neurons per MDM verifica gli account scaduti e ritira i dispositivi con account scaduti come proprietari. Tuttavia, per un dispositivo iPad condiviso, il proprietario del dispositivo è l'ultimo utente loggato e potrebbe non essere il proprietario legale. Se un account proprietario scade, Ivanti Neurons per MDM esclude i dispositivi iPad condivisi dal ritiro.
- Il client Go for iOS non è supportato per i dispositivi iPad condivisi.
- Gli utenti non possono eseguire azioni come il ritiro e la cancellazione sui dispositivi iPad condivisi. Solo gli amministratori possono eseguire azioni di ritiro e cancellazione dal portale amministrativo Ivanti Neurons per MDM.
- Gli amministratori non possono cambiare il proprietario del dispositivo iPad condiviso dal portale amministrativo Ivanti Neurons per MDM.
- Zero sign-on non è supportato per i dispositivi iPad condivisi.
- Quando il comando ListUsers è abilitato, tutti gli ID utente gestiti e il loro orario di check-in sono visualizzati in Registrazione dispositivo (parte di Apple Business Manager) sotto la scheda **Amministratore**.

Configurazione di un dispositivo iPad condiviso

È possibile impostare un dispositivo iPad condiviso e configurare le impostazioni.

Procedura

1. Andare in **Amministratore** > **Apple** > **Registrazione dispositivi**.
2. Aggiungere il dispositivo ad Apple Business Manager registrando il dispositivo con un profilo per la registrazione automatica dei dispositivi. Per informazioni su questa procedura, vedere **Registrazione dispositivi**.

3. Nelle impostazioni di Registrazione dispositivi, attivare:
    - **Modalità di supervisione**.
    - **Modalità multiutente** sotto **Dispositivo iPad condiviso per business**.
4. (Facoltativo) Creare un account utente locale. Il dispositivo sarà registrato per questo utente. L'autenticazione per questo utente avviene solo una volta durante la registrazione.
5. Reimpostare l'iPad condiviso.

> Il processo di registrazione inizia solo dopo la reimpostazione. Sono necessari alcuni minuti perché il dispositivo sia registrato e configurato come un dispositivo iPad condiviso.

6. Il proprietario legale è assegnato all'account utente che ha registrato il dispositivo. L'amministratore può cambiare il proprietario legale dalla pagina **Dispositivi**.
7. Nella schermata di accesso al dispositivo, inserire le credenziali dell'ID Apple gestito dall'utente.
    - In modo simile ai dispositivi macOS, è possibile eseguire il push delle configurazioni sui dispositivi iPad condivisi attraverso entrambi i canali dispositivo e utente.
    - Le variabili di sostituzione dell'utente non vengono sostituite per le configurazioni (compresa la configurazione dell'App gestita) spinte nel canale del dispositivo.
    - Se l'utente connesso in un dispositivo iPad condiviso non è un utente gestito - l'ID Apple gestito non appartiene a nessun utente nel portale amministrativo Ivanti Neurons per MDM, il dispositivo non è assegnato a nessuno. Gli utenti non saranno gestiti - l'amministratore non può eseguire il push delle configurazioni del canale utente da Ivanti Neurons per MDM.
    - Per impostazione predefinita, l'utente guest predefinito creato da Ivanti Neurons per MDM è disabilitato. Quando accede un utente ospite, il dispositivo non è assegnato ad alcun utente e l'utente non è gestito. Se l'utente ospite deve essere gestito, l'utente ospite predefinito creato da Ivanti Neurons per MDM deve essere abilitato e il dispositivo viene assegnato all'utente ospite predefinito dopo che l'utente ospite ha effettuato il login. L'utente può quindi essere gestito.
    - Le informazioni sul proprietario del dispositivo sono visualizzate nella pagina Ivanti Neurons per MDM > **Dispositivi** e nei registri del dispositivo (pagina dei dettagli del dispositivo > **Registri**).

Gestione dei proprietari legali per iPad condivisi

È possibile cercare e visualizzare i proprietari legali dei dispositivi iPad condivisi usando i loro ID e-mail dalla pagina di elenco dei dispositivi. È possibile cambiare i proprietari legali dei dispositivi iPad condivisi riassegnando i proprietari legali esistenti ai nuovi proprietari legali. Se il proprietario legale di un dispositivo iPad non condiviso viene riassegnato, Ivanti Neurons per MDM ignora l'assegnazione.

Procedura

1. Andare su **Dispositivi**.
2. Fare clic sull'icona dell'ingranaggio per selezionare e aggiungere la colonna **Proprietario legale** alla pagina dell'elenco dei dispositivi.
3. Selezionare i dispositivi iPad condivisi.
4. Fare clic su **Azioni > Assegna a proprietario legale**.

Invio di un'e-mail al proprietario legale di un dispositivo iPad condiviso

È possibile inviare e-mail al proprietario legale di un dispositivo iPad condiviso.

Procedura

1. Andare su **Dispositivi**.
2. Fare clic sul nome del dispositivo iPad condiviso.
3. Fare clic sull'icona dell'**e-mail**.
4. Comporre l'e-mail.
5. Fare clic su **Invia**.

Utilizzo dell'attributo Modalità multiutente

È possibile usare l'attributo Modalità multiutente dei dispositivi iPad condivisi in Ivanti Neurons per MDM.

Procedura

1. Nella pagina **Dispositivi**, usare l'attributo **modalità multiutente**.
2. Fare clic su **Ricerca avanzata** e creare una regola per trovare i dispositivi utilizzando l'attributo **Modalità multiutente**.
3. Nella pagina **Dispositivi > Gruppi di dispositivi** creare un gruppo di dispositivi dinamici per i dispositivi iPad condivisi usando l'attributo **Modalità multiutente**. Ad esempio, è possibile utilizzare questo gruppo come un filtro di distribuzione per distribuire configurazioni.
4. Nella pagina **Criteri**, creare un criterio personalizzato per i dispositivi iPad condivisi usando l'attributo **Modalità multiutente**.
5. In **App > Distribuzione Filtro**, usare l'attributo **modalità multiutente** per limitare il numero di applicazioni disponibili per l'installazione.

- Ivanti Neurons per MDM non supporta la modalità multiutente per i dispositivi Apple School Manager. Non è consigliabile attivare l'impostazione e inviare il profilo Registrazione dispositivi ai dispositivi Apple School Manager.
- La configurazione Secure Sign-In multiutente per iOS non è applicabile ai dispositivi iPad condivisi.

Eliminare gli utenti da un dispositivo iPad condiviso

È possibile eliminare un utente o più account utente dai dispositivi iPad condivisi. Nella scheda Elenco utenti, l'etichetta **Attivo** viene visualizzata per l'utente attualmente connesso. L'opzione Elimina non è applicabile all'utente attualmente connesso sul dispositivo iPad condiviso. Gli utenti possono essere eliminati dalla scheda **Dispositivi** o dalla scheda **Utenti**.

Eliminare gli utenti dalla scheda Dispositivi

Procedura

1. Andare alla scheda **Dispositivi** > **Dettagli dispositivo**.
2. Passare alla scheda **Utenti**. Viene visualizzato l'elenco degli utenti.
3. Fare clic su **Elimina tutti gli utenti**.
4. Fare clic sul segno meno "**-**" per eliminare utenti specifici.
    - (Opzionale) Nella finestra **Elimina utente** selezionare l'opzione **Imponi eliminazione dell'utente anche se la sincronizzazione dei dati con Ivanti Neurons for MDM è in sospeso** e fare clic su **Sì**.

> Selezionando **Imponi eliminazione dell'utente anche se la sincronizzazione dei dati con Ivanti Neurons for MDM è in sospeso** si forzerà l'eliminazione dell'utente anche se i dati non sono già sincronizzati con il portale amministrativo Ivanti Neurons for MDM.

Eliminare gli utenti dalla scheda Utenti

Procedura

1. Passare alla scheda **Utenti**.
2. Selezionare un utente o più utenti, andare al menu a discesa **Azioni** e fare clic su **Elimina**. Appare un messaggio di conferma. Dopo aver confermato il comando di eliminazione dell'utente viene emesso ai dispositivi.
3. Andare su **Registri dispositivi** nei dettagli del dispositivo e verificare che il comando Elimina utente sia inviato agli utenti selezionati del dispositivo iPad condiviso.

Disconnessione degli utenti da un dispositivo iPad condiviso

L'amministratore può effettuare la disconnessione degli utenti da un dispositivo iPad condiviso.

Procedura

1. Nella pagina **Dispositivi** selezionare un dispositivo iPad condiviso.
2. Selezionare **Foza disconnessione** dal menu **Azioni**. Verrà visualizzata una finestra pop-up per confermare la disconnessione degli utenti dal dispositivo iPad condiviso.
3. Fare clic su **OK** per confermare la disconnessione forzata.

12.3.8. School Manager

Licenza: Gold

Valido per: dispositivi supervisionati iOS 9.3 e versioni successive

Apple School Manager è un servizio cloud di Apple appositamente concepito per il mondo dell'istruzione allo scopo di fornire servizi, tra cui l'acquisto di app in Apple App e libri, la registrazione di dispositivi iPad mediante Apple Registrazione dispositivi e la creazione di ID Apple gestiti. Grazie all'integrazione completa con Apple School Manager, la soluzione Ivanti Neurons per MDM UEM fornisce un metodo semplice per la gestione completa dei dispositivi iPad appositamente creati per insegnanti e studenti sfruttando l'ecosistema e le app di School Manager come Classroom.

> Apple Books non è supportato.

Configurazione di School Manager

1. Andare a **Amministratore > School Manager**.
2. Fare clic sull'opzione **Configura Education**, se disattivata.
3. Selezionare una delle seguenti opzioni:
   - **Sincronizzarsi con l'account di Apple School Manager per importare le informazioni sull'istituto scolastico**:
     1. Accedere ad **Amministratore > Apple > Registrazione dispositivi** per scaricare i file principali dell'organizzazione.
     2. Per generare chiavi di crittografia, caricare i file principali nell'account Apple School Manager.
     3. Scaricare le chiavi di cifratura da Apple School Manager, quindi caricarle su Ivanti Neurons for MDM (**Amministratore > Apple > Registrazione dispositivi**).

        > È possibile riutilizzare gli account Apple Registrazione dispositivi esistenti per Apple Education. Quando si accede ad Apple School Manager, Apple offre l'opzione di eseguire l'aggiornamento dell'account Registrazione dispositivi per includere le funzionalità di Education. Per le istruzioni relative all'upgrade, visitare l'indirizzo https://support.apple.com/it-it/HT206960.

     Una volta accettate le chiavi di cifratura, viene visualizzato il pulsante **Sincronizza adesso**.

     4. Fare clic su **Sincronizza adesso** per avviare la sincronizzazione dei dati con Apple School Manager.
   - **Importare i dati dai file CSV**:
     1. (Facoltativo) Fare clic su **Scarica il file ZIP dei modelli CSV** per scaricare un file ZIP con i modelli di tutti i tipi di dati.
     2. Fare clic su **Seleziona file**...
     3. Aggiungere i seguenti sei file CSV:
        - File di dati degli studenti (students.csv)
        - File di dati dei registri (roster.csv)
        - File di dati del personale (staff.csv)
        - File di dati delle classi (classes.csv)
        - File di dati dei corsi (courses.csv)
        - File di dati delle sedi (locations.csv)

> È necessario selezionare sempre tutti e sei i file CSV insieme prima di caricarli.

Fare clic su **Carica**.

4. (Facoltativo) Se è necessario apportare modifiche ai file CSV, mantenere tutti i dati obbligatori in tutti i sei file precedentemente caricati. Apportare le modifiche necessarie e caricare nuovamente i file insieme.

Ricercare i dati dalla scheda **Classi** e **Individui**.

> Le persone (studenti e personale) appaiono anche nella pagina **Utenti** di Ivanti Neurons per MDM.

5. Creare due gruppi di dispositivi per i dispositivi che saranno utilizzati per l'istruzione da studenti e personale come segue:
    1. Andare a **Amministratore > Attributi personalizzati**.
    2. Creare attributi personalizzati per gli studenti e il personale, che saranno utilizzati per creare gruppi di dispositivi gestiti dinamicamente.
    3. andare a **Dispositivi > Gruppi di dispositivi**.
    4. Fare clic su **Aggiungi+**.
    5. Creare ciascuno dei gruppi di dispositivi gestiti dinamicamente per studenti e personale utilizzando come filtri gli attributi personalizzati creati in precedenza.
6. Assegnare i dispositivi registrati agli studenti e al personale dalla pagina **Dispositivi** utilizzando l'opzione **Azioni > Assegna a utente**.
7. Creare una configurazione Responsabile (personale) e una configurazione Membro (studenti) aggiungendo i payload **Configurazioni > Education**.
8. Distribuire le configurazioni Responsabile (personale) e Membro (studenti) ai gruppi di dispositivi del personale e degli studenti. Mediante questa distribuzione vengono inviate le configurazioni e vengono installati i certificati sui rispettivi dispositivi.

> Se non è presente alcun valore per il campo Nome classe nella pagina **Amministratore > School Manager**, tale valore verrà ricavato dai campi dell'identificatore di origine del sistema della classe e dell'identificatore del corso. Questi campi sono facoltativi in Apple School Manager o nel file CSV. Tuttavia, è consigliabile inserire sempre un valore poiché verrà utilizzato come identificatore predefinito in mancanza di un nome della classe.

Invio dell'app Classroom agli insegnanti

Mediante l'app Classroom, gli insegnanti (Responsabile) possono gestire i seguenti scenari:

- Funzionalità di gestione per il controllo delle app e dei dispositivi iPad da remoto.
- Possibilità di creare un gruppo della classe.
- Possibilità per l'insegnante di visualizzare gli studenti membri di tale gruppo.
- Possibilità per l'insegnante di inviare contenuti agli studenti di tale gruppo.
- Limitare le app e i contenuti visualizzabili dagli studenti.

È possibile eseguire il push dell'app Classroom dall'App Store di Apple.

Procedura

1. Andare alla pagina **App > App Catalog**.

2. Fare clic sul pulsante **+Aggiungi**.
3. Cercare e selezionare l'app Classroom di Apple.
4. Fare clic su **Avanti**.
5. Immettere la categoria e la descrizione.
6. Fare clic su **Avanti**.
7. Distribuire l'app al gruppo di dispositivi degli insegnanti creato in precedenza.
8. Configurare le impostazioni dell'app nella pagina Configurazioni delle app.
9. Fare clic su **Fine**.

Disabilitazione di School Manager

Se si disabilita School Manager, vengono cancellati tutti i dati correnti. Svolgere questa operazione con cautela.

1. Andare a **Amministratore > School Manager**.
2. Fare clic sull'opzione **Configura Education**, se disattivata.
3. Fare clic su **Sì**.

12.3.9. Impostazioni (Apple)

Gli amministratori possono configurare, abilitare e disabilitare varie impostazioni per i dispositivi Apple.

Registrazione invisibile (solo per macOS)

La registrazione invisibile per dispositivi macOS è bloccata come Abilitata. Questo vale per le nuove registrazioni dei dispositivi nel tenant ed è possibile in Mobile@Work 1.4 e nelle versioni successive supportate.

Impostazioni generali

Disabilita riconciliazione dispositivo - Gli amministratori possono ora conservare le voci del dispositivo se desiderano registrare nuovamente lo stesso dispositivo. Questa opzione non è selezionata per impostazione predefinita. Selezionare questa opzione per conservare i dati del dispositivo inattivo.

> Quando Disabilita riconciliazione dispositivo non è abilitato e se un dispositivo viene nuovamente registrato con lo stesso utente, verrà creata una nuova voce. In caso contrario, la voce del dispositivo verrà aggiornata con nuove informazioni di registrazione.

Impostazioni profilo

Se il profilo MDM non è installato, gli amministratori possono abilitare o disabilitare l'invio di e-mail agli utenti finali e di notifiche ai client macOS e Go per iOS. La funzione notifiche nel profilo MDM è abilitata per impostazione predefinita.

Procedura

1. Andare in **Amministratore > Impostazioni**.
2. Selezionare o deselezionare l'opzione **Invia un'e-mail all'utente e una notifica al client se il profilo MDM non è installato**.
3. Selezionare un valore da 1 a 4 per specificare il numero massimo di e-mail/notifiche.
4. Fare clic su **Salva**.

Aggiornamenti del sistema operativo per la registrazione automatica dei dispositivi (solo iOS)

Gli amministratori possono attivare gli aggiornamenti del sistema operativo iOS per la registrazione automatica dei dispositivi. Se questa opzione è abilitata, i dispositivi Registrazione dispositivi utilizzeranno la configurazione **Aggiornamenti software**, anziché l'impostazione Pianifica aggiornamenti del sistema operativo nel profilo Registrazione dispositivi.

L'opzione è disabilitata per impostazione predefinita. In tal caso, viene utilizzata l'impostazione Pianifica aggiornamenti del sistema operativo nel profilo Registrazione dispositivi. L'attivazione di questa impostazione è permanente e non può essere disattivata. Questa impostazione comporta la disattivazione dell'opzione Pianifica aggiornamenti del sistema operativo in tutti i profili Registrazione dispositivi disponibili.

> I dispositivi non Registrazione dispositivi supervisionati utilizzano la configurazione Aggiornamenti software.

Procedura

1. Andare in **Amministratore > Impostazioni**.
2. Selezionare o deselezionare l'opzione **Usa configurazione Aggiornamenti software per registrazione automatica dispositivi**.

3. Fare clic su **Sì** per confermare.
4. Fare clic su **Salva**.

Accesso sicuro multiutente

Gli amministratori possono cancellare la password del dispositivo quando un utente si disconnette dalla web clip Accesso sicuro multiutente su dispositivi iOS condivisi selezionando l'opzione "**Cancella il passcode dopo l'accesso utente**" nella sezione "**Accesso sicuro multiutente**" in Amministratore > Apple > Impostazioni.

Impostazioni di priorità per la configurazione delle limitazioni

L'amministratore può abilitare la priorità per più configurazioni di restrizioni per iOS e macOS, selezionando le opzioni **Configurazione delle limitazioni per iOS** o **Configurazione delle limitazioni per macOS** nella sezione **Impostazioni di priorità per la configurazione delle limitazioni** di **Amministratore > Apple > Impostazioni**. Questa opzione è disabilitata per impostazione predefinita. Per ulteriori informazioni sul funzionamento delle priorità, vedere Assegnazione della priorità alle configurazioni.

Procedura

1. Andare ad **Amministrazione > Apple > Impostazioni**.
2. Nella sezione **Impostazioni di priorità per la configurazione delle limitazioni**, selezionare l'opzione **Configurazione delle limitazioni per iOS** o **Configurazione delle limitazioni per macOS**.
3. Fare clic su **Salva** per abilitare la priorità. Viene visualizzato il banner "**Sono state abilitate le impostazioni di priorità per la configurazione delle limitazioni (iOS o macOS)**". Prima dell'**approvazione** della priorità:
    - **Modificare il riepilogo della distribuzione (se applicabile)**: quando l'impostazione delle priorità è abilitata, il riepilogo della distribuzione per la configurazione delle limitazioni selezionata viene modificato da "**Applica ai dispositivi negli altri spazi**" ad "**Applica a tutti i dispositivi in altri spazi come massima priorità**" per impostazione predefinita.
    - **La priorità predefinita viene assegnata in ordine di creazione**: per la configurazione del tipo di limitazione selezionato, viene assegnata una priorità predefinita esistente, in base all'ordine con cui è stato creato.
    - **Sospensione della gestione della configurazione**: la gestione della configurazione delle limitazioni (ad esempio la configurazione delle limitazioni per iOS) rimane sospesa finché non si approva la priorità.

> Una volta abilitata la priorità, eventuali modifiche alle limitazioni non vengono elaborate fino a quando non sono state approvate. Prima dell'approvazione, l'amministratore può modificare la distribuzione, il riepilogo della distribuzione o la priorità della configurazione delle limitazioni nella sezione **Configurazioni**.

4. Selezionare l'opzione **Approva** per rendere effettiva la priorità.
5. Fare clic su **Salva**.

> L'opzione **Approvazione** non è disponibile quando si deseleziona un'opzione di configurazione delle limitazioni per iOS o macOS e le modifiche vengono applicate immediatamente.

Se alle configurazioni non è associata alcuna priorità, l'impostazione delle priorità viene disabilitata. Se applicabile, viene eseguito il push di tutte le configurazioni delle limitazioni (alla successiva sincronizzazione dei dispositivi).

- **Riepilogo della distribuzione (se applicabile): Quando l'impostazione delle priorità è disabilitata per la configurazione delle limitazioni, il riepilogo della distribuzione viene modificato da Applica a tutti i dispositivi in altri spazi come massima priorità o Applica a tutti i dispositivi in altri spazi come minima priorità ad "Applica ai dispositivi negli altri spazi".**

- **Nessuna priorità assegnata**: la priorità assegnata viene rimossa per la configurazione delle limitazioni selezionata.

12.4. Utilizzo di dispositivi Windows

Argomenti della sezione:

- Configurazione di profili Windows Autopilot
- Audit trail sui profili di Windows Autopilot
- CSP TenantLockdown
- Browser ADMX (GPO)
- Configurazione degli intervalli dell'inventario app
- Inventario hardware

12.4.1. Configurazione di profili Windows Autopilot

Windows Autopilot è una funzione di Microsoft che consente agli amministratori di configurare e preconfigurare nuovi dispositivi per renderli subito operativi. La funzione Autopilot consente di eseguire un provisioning rapido, semplice e affidabile dei dispositivi Windows Desktop o HoloLens2. Inoltre, la funzione Autopilot consente di eseguire le seguenti attività:

- Unisce automaticamente i dispositivi a Entra ID (Entra ID)
- Registrare automaticamente dispositivi a servizi MDM
- Creare e assegnare automaticamente dispositivi a gruppi di configurazioni in base al profilo del dispositivo
- Personalizzare l'esperienza di registrazione
- Applicare configurazioni e policy
- Installare applicazioni essenziali

Prerequisiti

Per utilizzare la pagina Windows Autopilot, consultare le fasi del partner Ivanti Neurons for MDM e i requisiti di licenza Azure. Assicurarsi che i seguenti prerequisiti siano soddisfatti affinché la funzione Autopilot venga eseguita come previsto:

- **Requisiti per le licenze Azure per Autopilot**: verificare la presenza di "Requisiti per le licenze Windows per Autopilot".
- **Registrazione dei dispositivi Azure Windows Autopilot**: verificare la presenza di "Panoramica della registrazione di Windows Autopilot".
- **Rivenditori che aggiungono dispositivi all'account del cliente**: verificare la presenza di "Utilizzare i profili Windows Autopilot sui nuovi dispositivi per personalizzare l'esperienza out-of-box del cliente".

Requisiti aggiuntivi

1. Integrare i tenant di Entra ID e Ivanti Neurons per MDM. Per ulteriori informazioni, consultare **Configurazione con Microsoft Azure**.
2. Assicurarsi di disporre di un account amministratore in Ivanti Neurons for MDM e Entra ID.
3. Per sfruttare i profili di autodistribuzione, creare un utente falso per la registrazione di dispositivi autodistribuiti senza utente in Ivanti Neurons for MDM.
4. Creare e sincronizzare un utente fittizio, fooUser@Entra IDPrimaryDomain.com dal dominio primario Entra ID.

> Le licenze Microsoft non sono necessarie per creare e sincronizzare un utente fittizio.

5. La pagina "Nomi di dominio personalizzati" di Entra ID visualizza il dominio primario dell'ambiente Entra ID.
6. Assicurarsi che l'utente possa registrare i dispositivi e che non sia disabilitato. Ad esempio, se il dominio primario è contoso.com, l'utente risultante sarà fooUser@contoso.com. Se il dominio primario è contoso.onmicrosoft.com, l'utente risultante sarà fooUser@contoso.onmicrosoft.com.
7. Per effettuare il provisioning dell'utente con SCIM in Ivanti Neurons for MDM, modificare i dettagli dell'utente in Entra ID e aggiungere l'indirizzo e-mail. In genere, l'indirizzo e-mail sarà lo stesso dell'UPN.
8. Assicurarsi che tutti gli utenti, compreso fooUser, siano presenti in Azure e in Ivanti Neurons for MDM.
9. Gli amministratori possono creare profili Autopilot utilizzando Microsoft Store for Business o Ivanti Neurons for MDM. Per creare profili utilizzando Ivanti Neurons for MDM, gli amministratori devono disporre delle autorizzazioni di amministratore globale di

Entra ID e di Intune.

> Gli amministratori devono disporre di Azure P1 o P2 e di licenze Ivanti Neurons for MDM Secure UEM o Secure UEM Premium. La licenza Intune non è necessaria per gli amministratori.

> In Neurons for MDM, la funzione di creazione dei profili di Autopilot sfrutta le API Microsoft Graph per Autopilot, ancora in fase beta.

Modalità di registrazione ad Autopilot

Dopo aver associato i dispositivi a un gruppo specifico di profili utente in base all'utilizzo del dispositivo, è possibile configurare la modalità di registrazione ad Autopilot per consentire agli utenti di iniziare a utilizzare rapidamente il proprio dispositivo. Ivanti Neurons for MDM offre le seguenti modalità di registrazione ad Autopilot:

- Modalità di distribuzione automatica
- Guidato dall'utente (modalità Pre-provisioning)
- Gestita dall'utente

Modalità autopilota con distribuzione automatica - La modalità di registrazione del dispositivo Autopilot con distribuzione automatica assicura una distribuzione senza problemi di un dispositivo aziendale per un utente, bypassando l'impostazione iniziale del dispositivo e inviando tutti i file di configurazione necessari per l'avvio sicuro del dispositivo. Questa modalità consente di proteggere i componenti hardware, connettere il dispositivo alla rete aziendale e registrare il dispositivo in Entra ID (Entra ID), nel servizio MDM e nel portale amministratore di Ivanti Neurons for MDM utilizzando un ID utente fittizio. Tutti i file di configurazione necessari vengono inviati al dispositivo prima dell'accesso dell'utente. Una volta inviati i file di configurazione obbligatori al dispositivo, quest'ultimo viene riavviato, quindi viene visualizzata la schermata di accesso affinché l'utente aziendale possa iniziare a utilizzarlo. È possibile attivare la modalità di distribuzione automatica per utilizzare un dispositivo come dispositivo tutto schermo o firmato digitalmente.

Modalità profilo pre-provisioning guidato dall'utente - Una volta creato un profilo pre-provisioning guidato dall'utente, l'amministratore assegna il profilo a un gruppo di utenti e l'ID hardware del dispositivo viene caricato e assegnato al gruppo Entra ID. Il dispositivo verrà associato al profilo con pre-provisioning gestito dall'utente. Questa modalità viene utilizzata dall'amministratore per configurare un dispositivo prima che venga consegnato all'utente aziendale.

Procedura

Seguire la procedura per la distribuzione con pre-provisioning:

1. Connettere il nuovo dispositivo hardware alla rete LAN, quindi premere il pulsante Windows cinque volte.
2. Il dispositivo visualizza una domanda. Selezionare l'opzione Provisioning Windows Autopilot, quindi fare clic su Continua. Entra ID rileva la modalità del profilo di pre-provisioning guidato dall'utente e tutte le impostazioni di configurazione di base vengono distribuite nel dispositivo. Viene visualizzata la schermata Configurazione Windows Autopilot.
3. Fare clic su Continua. Il dispositivo continua il processo e protegge i componenti hardware, viene connesso alla rete aziendale e viene registrato in Entra ID (Entra ID), nel servizio MDM e nel portale amministratore di Ivanti Neurons for MDM utilizzando un ID utente fittizio. Tutti i file di configurazione necessari vengono inviati al dispositivo e viene visualizzato un messaggio di conferma.
4. Ora è possibile consegnare il dispositivo all'utente. Quando l'utente accede al dispositivo, l'ID utente viene registrato nel portale amministratore di Ivanti Neurons for MDM con i dettagli del dispositivo.

Le seguenti configurazioni vengono inviate automaticamente prima che l'utente acceda al dispositivo:

Certificato di identità

Wi-Fi

Windows Hello for Business

Restrizioni di Windows

> Le altre configurazioni sono in stato In sospeso e vengono inviate dopo che l'utente ha effettuato l'accesso al dispositivo utilizzando un indirizzo e-mail.

> Durante il processo di registrazione di Autopilot nelle modalità Distribuzione automatica e Guidata dall'utente (pre-provisioning), le app .MSI e .EXE assegnate verranno installate sul dispositivo per completare il processo di registrazione. Quando si installano le applicazioni .MSI e .EXE durante la procedura di registrazione di Autopilot, se le app effettuano o meno un report durante l'installazione, il processo di Autopilot viene completato e il pulsante Reseal viene attivato.

Creazione di profili utente di Windows Autopilot

Dopo aver configurato l'origine utente Entra ID (Entra ID) e sincronizzato gli utenti e i gruppi di utenti Entra ID con il tenant di Ivanti Neurons for MDM, è possibile creare i profili Autopilot.

Procedura

1. Accedere al portale amministratore di Ivanti Neurons for MDM.
2. Andare in **Amministrazione > Microsoft Azure > Gestione dispositivi Windows**.

> Se non si configura l'origine utente Entra ID, il pulsante **Aggiungi** viene disabilitato. È necessario configurare l'Origine utente utilizzando l'opzione **Gestione dispositivi Windows** presente sotto la sezione **Microsoft Azure**.

3. Fare clic su **Aggiungi**.
   Viene visualizzata la pagina **Aggiungi profilo Windows Autopilot** sullo schermo.
4. Inserire un nome profilo nella casella **Nome**.
5. Completare le **Impostazioni profilo** utilizzando la tabella riportata sotto questa procedura.
6. Fare clic su **Avanti**.
   Viene visualizzata a schermo una pagina con tutti i gruppi di dispositivi Entra ID.
7. Selezionare uno o più gruppi di dispositivi Entra ID a cui assegnare il profilo Autopilot.
8. È anche possibile creare un gruppo di dispositivi Entra ID e assegnare il profilo Autopilot a questo gruppo appena creato. Vedere per ulteriori informazioni.
   Se si desidera assegnare il profilo Autopilot a tutti i gruppi Entra ID, selezionare l'opzione **Assegna a tutti i gruppi Entra ID**.

> Non è possibile assegnare più di un profilo a "Tutti i gruppi" a causa di una limitazione di Microsoft.

9. Fare clic su **Fine**.

Impostazione	Descrizione
Tipo di dispositivo	Selezionare una delle due opzioni seguenti a seconda del dispositivo: • **PC Windows** • **HoloLens**: se si seleziona questa opzione, la modalità di distribuzione predefinita deve essere impostata su **Distribuzione automatica**. In rari casi, durante la registrazione di dispositivi HoloLens 2 utilizzando Autopilot, la registrazione potrebbe bloccarsi nella schermata "Configurazione del dispositivo per il lavoro". In questo raro caso, l'utente deve spegnere e riaccendere il dispositivo premendo il pulsante di accensione. Il dispositivo mostra quindi la schermata di accesso, in cui l'utente deve inserire le credenziali Entra ID per completare la registrazione.
Modalità di distribuzione	• **Distribuzione automatica**: in questa modalità, la distribuzione del dispositivo viene eseguita senza alcun intervento manuale (o quasi). • **Gestita dall'utente**: gli amministratori possono utilizzare questa opzione per selezionare la modalità di registrazione e configurare un nuovo dispositivo prima di consegnarlo all'utente.
Tipo di account utente	• **Amministratore**: selezionare questa opzione se l'utente deve completare il controllo dopo la distribuzione del dispositivo. • **Standard**: selezionare questa opzione se l'utente necessita dell'autorizzazione per utilizzare le opzioni di base dopo la distribuzione del dispositivo.
Lingua	Per impostazione predefinita, la lingua sarà quella specifica del sistema operativo. È possibile impostare una lingua differente selezionandola nell'elenco.
Converti tutti i dispositivi di destinazione in Autopilot	Selezionare questa opzione per convertire tutti i dispositivi del gruppo assegnato in Autopilot.
Consenti pre-provisioning	Selezionare questa opzione per registrare dispositivi ad Autopilot utilizzando il processo di registrazione normale. Questa opzione non è disponibile quando la funzione **Distribuzione automatica** è selezionata.
Configura tastiera automaticamente	Selezionare **Sì** per ignorare la selezione della tastiera quando l'opzione **Lingua** è impostata su un valore diverso da quello predefinito.
Modello nome dispositivo	Inserire un nome modello da utilizzare durante il processo di registrazione del dispositivo.
Condizioni di licenza software Microsoft	È possibile mostrare o nascondere questa opzione solo nella modalità Distribuzione gestita dall'utente.
Impostazioni sulla privacy	È possibile mostrare o nascondere questa opzione solo nella modalità Distribuzione gestita dall'utente.

Impostazione	Descrizione
Modifica opzioni account	È possibile mostrare o nascondere questa opzione solo nella modalità Distribuzione gestita dall'utente e quando il tipo di account utente è impostato su Standard.

Gestione dispositivi Windows

L'amministratore può configurare la funzione Autopilot su un tenant utilizzando la nuova opzione Gestione dispositivi di Windows. Questa opzione facilita l'integrazione con Ivanti Neurons for MDM se l'utente ha un ambiente Entra ID.

Per accedere a questa opzione, **Amministratore** > **Microsoft Azure** > **Gestione dispositivi Windows**.

Questa integrazione concede le autorizzazioni a Ivanti Neurons for MDM per gestire i dispositivi, i profili Autopilot, controllare la conformità dei dispositivi Windows e convalidare il tenant Azure.

Argomenti correlati

- CSP TenantLockdown

Creazione di gruppi di dispositivi Entra ID

L'amministratore può creare gruppi di dispositivi Entra ID, se necessario, dalla sezione Gruppi di dispositivi Entra ID. La convalida del tenant Entra ID deve essere stata configurata nella sezione Conformità dispositivi per creare gruppi di dispositivi Entra ID.

Procedura

1. Andare in **Amministratore** > **Microsoft Azure** > **Gruppi di dispositivi Entra ID**.
2. A schermo appare la pagina **Gruppi dispositivi Entra ID**.
   Fare clic su **AGGIUNGI**.
3. La pagina **Impostazioni gruppi** appare a schermo.
   Fornire i seguenti dettagli:
   - Nome del gruppo
   - Descrizione del gruppo
   - Tipo di appartenenza
     - Dispositivo statico - L'amministratore otterrà l'elenco dei dispositivi statici disponibili sulla finestra **Assegna membri al gruppo**. Selezionare i dispositivi richiesti e fare clic su **Salva**.
     - Dispositivo dinamico - L'amministratore deve fornire determinati criteri dalla finestra **Query dinamica**.

Il nuovo gruppo di dispositivi Entra ID verrà creato e l'amministratore potrà aggiungere dispositivi al gruppo appena creato.

> Dopo aver creato un gruppo dinamico, i dispositivi saranno elencati nella scheda Dispositivi del gruppo di dispositivi specifico dopo qualche tempo.

Modifica di dispositivi Autopilot

Gli utenti possono modificare i dispositivi Autopilot dal portale amministrativo di Ivanti Neurons per MDM.

Prerequisiti

Assicurarsi che siano soddisfatti i seguenti prerequisiti:

- L'utente IT amministratore deve disporre delle autorizzazioni Amministratore globale Azure e Amministratore Intune.
- È possibile impostare un nome descrittivo solo se è impostato l'utente.
- Il nome dispositivo non può essere modificato una volta impostato.

Procedura

1. Accedere al portale amministrativo di Ivanti Neurons for MDM.
2. Andare ad **Amministratore** > **Windows** > **Autopilot**. I dispositivi Autopilot sono elencati nella scheda Dispositivi Autopilot.
3. Fare clic su **Modifica** (icona della matita). Viene visualizzata la pagina Modifica.
4. Modificare i dettagli seguenti:
    - **Utente**
    - **Nome descrittivo**
    - **Nome dispositivo**
    - **Tag gruppo**

Fare clic su **Salva**. I dettagli del dispositivo vengono aggiornati.

Eliminazione di dispositivi Autopilot

Gli utenti possono eliminare i dispositivi Autopilot dal portale amministrativo di Ivanti Neurons for MDM.

1. Accedere al portale amministrativo di Ivanti Neurons for MDM.
2. Andare ad **Amministratore** > **Windows** > **Autopilot**. I dispositivi Autopilot sono elencati nella scheda Dispositivi Autopilot.
3. Fare clic su **Elimina**. I dettagli del dispositivo vengono eliminati.

12.4.2. Audit trail sui profili di Windows Autopilot

Audit trail tiene traccia di tutte le attività svolte su tutte le entità all'interno di Ivanti Neurons for MDM. Queste attività includono l'aggiunta, l'eliminazione, l'aggiornamento di nuovi dispositivi, ecc.

Per ulteriori informazioni, vedere **Audit trail**.

L'amministratore può eseguire le seguenti attività utilizzando Audit trail su tutti i dispositivi Windows iscritti nella modalità Autopilot:

Profili Autopilot

- Crea
- Modifica
- Elimina
- Assegnare il profilo ai gruppi

Dispositivi di Autopilot

- Carica CSV
- Modifica
- Elimina

12.4.3. CSP TenantLockdown

L'amministratore può bloccare tutti i dispositivi Windows nei tenant utilizzando la funzione CSP TenantLockdown. Per utilizzare questa funzione, è necessario registrare i dispositivi utilizzando l'opzione Autopilot. È possibile effettuare questa configurazione a livello di dispositivo.

Nelle modalità Autopilot di distribuzione automatica e Gestita dall'utente, l'amministratore può bloccare i dispositivi direttamente nei tenant. Ciò è utile quando i dispositivi vengono rubati o smarriti. In questi casi, anche se il dispositivo viene ripristinato, l'utente viene forzato a connettersi al tenant e la creazione dell'account locale non è supportata in modalità di distribuzione automatica. Tuttavia, per impedire la creazione dell'account nella modalità Gestita dall'utente, l'amministratore deve abilitare l'opzione **Nascondi** nell'impostazione **Modifica opzioni account** durante la configurazione del profilo Autopilot.

L'amministratore può abilitare la funzione CSP TenantLockdown creando una configurazione delle restrizioni per Windows e selezionando l'opzione **Richiedere agli utenti di connettersi alla rete durante la configurazione del dispositivo (profilo Autopilot necessario)** in **Altre restrizioni**.

Per rimuovere un dispositivo da CSP TenantLockdown, l'amministratore deve rimuovere manualmente il dispositivo dal gruppo o modificare le restrizioni.

12.4.4. Browser ADMX (GPO)

Con il browser ADMX (GPO) è possibile visualizzare le impostazioni GPO organizzate in base agli oggetti ADMX che esistono nel tenant. Per definire la visualizzazione delle impostazioni GPO è possibile cercare e visualizzare gli oggetti ADMX predefiniti, nonché aggiungere (caricare) file ADMX personalizzati che forniscono una struttura basata su XML

Per caricare l'oggetto ADMX personalizzato:

1. Selezionare **Amministratore > Browser ADMX (GPO)**. Viene visualizzata la pagina **Browser ADMX (GPO)**.
2. Fare clic su **Aggiungi**. Viene visualizzata la pagina **Aggiungi oggetti ADMX (GPO) personalizzati**.
3. Fare clic su **Scegli file** per selezionare il file ADMX da caricare.

> Assicurarsi che il file ADMX sia un file zip.

4. Fare clic su **Aggiungi**. Viene visualizzato un messaggio di conferma relativo alla riuscita del caricamento.

> Assicurarsi che la cartella principale contenga il file di estensione *.admx* dopo aver decompresso il file zip.

Ricerca delle impostazioni GPO

Nel browser ADMX (GPO), è possibile cercare e selezionare un GPO facendo clic sul componente pertinente dalla struttura gerarchica GPO nel riquadro sinistro. La struttura gerarchica GPO rappresenta il percorso delle impostazioni dei criteri. In alternativa, è possibile cercare un'impostazione GPO specifica digitando il nome GPO o il nome del file ADMX nel campo di ricerca. I dettagli dell'impostazione GPO selezionata vengono visualizzati nel riquadro destro.

12.4.5. Configurazione degli intervalli dell'inventario app

È possibile impostare gli intervalli della raccolta inventario delle app di Windows 10 per più inventari tipo di origine delle app. Gli intervalli sono utilizzati quando la configurazione della privacy è impostata per la raccolta di tutte le app dal dispositivo.

1. Accedere ad **Amministrazione > Intervalli inventario app**.
2. Selezionare l'intervallo (in ore) per raccogliere l'inventario delle app dall'elenco a discesa per i tipi di origine delle app seguenti.
   - **Intervallo inventario non App Store**
   - **Intervallo inventario App Store**
   - **Intervallo inventario sistema**
   - **Intervallo inventario Win32**
     Le opzioni di intervallo per la raccolta dell'inventario delle app Windows sono comprese tra **24** e **48** ore. Il valore predefinito è **24** ore.

12.4.6. Inventario hardware

È possibile abilitare la raccolta di informazioni sull'hardware dai dispositivi Windows 10. I dettagli dell'inventario hardware vengono recuperati mediante Bridge.

1. Andare su **Amministratore > Inventario hardware**.
2. Abilitare l'opzione **Abilita la raccolta dell'inventario hardware**.
3. In **Intervallo inventario**, selezionare la frequenza della raccolta dell'inventario hardware. Di seguito sono indicate le opzioni disponibili:
    - **Una volta al giorno**(predefinito)
    - **Una volta alla settimana**
    - **Ogni 30 giorni**

Quando l'opzione relativa all'inventario hardware è abilitata, è possibile visualizzare i dettagli dell'hardware del dispositivo nella scheda **Hardware** nella pagina dei dettagli del dispositivo.

12.5. Configurazione con Microsoft Azure

Argomenti della sezione:

- Utilizzo di Microsoft Azure
- Configurazione di Entra ID Windows 10 Unified Endpoint Management
- Assegnazione dell'app Entra ID UEM
- Collegare Ivanti Neurons per MDM con origine utente Entra ID
- Tenant Azure
- Amministratore > Microsoft Azure > Sicurezza delle app Office 365

12.5.1. Utilizzo di Microsoft Azure

Ivanti Neurons per MDM può essere configurato con Microsoft Azure per una registrazione diretta per i propri utenti sui loro dispositivi Windows desktop e tablet in esecuzione su Windows 10. Attenersi ai passaggi di seguito descritti per configurare e connettere le istanze.

Argomenti della sezione:

Configurazione dell'account Entra ID

Per configurare Entra ID:

1. Andare al sito **https://azure.microsoft.com/it-it/pricing/purchase-options/** per acquistare l'account Azure.
2. Utilizzare l'account Hotmail o Outlook.com esistente o creare un account nuovo e registrarsi come nuovo utente.
3. Acquistare un account Azure utilizzando uno dei metodi di pagamento indicati e seguire i passaggi per la verifica.
4. Richiedere a Microsoft di inserire nell'elenco dei programmi consentiti Ivanti Neurons for MDM tenant.
5. Utilizzare lo stesso account Hotmail o Outlook.com impiegato nel passaggio 2 per accedere come amministratore a Entra ID, all'indirizzo **https://manage.windowsazure.com/https://manage.windowsazure.com/**.
6. Andare alla scheda **Dominio**.
   Viene creato un dominio predefinito, TestMiBGLRoutlook.onmicrosoft.com, per il proprio account e gli utenti creati apparterranno a questo dominio. Se necessario, è possibile ricreare un dominio personalizzato.

Creazione di utenti su Entra ID

Per creare utenti su Entra ID:

1. Andare ad Active Directory → **Directory predefinita → Utenti**.
2. Selezionare l'opzione Aggiungi utente → Seleziona nuovo utente nell'organizzazione.
3. Immettere il nome utente. Fare clic su **(→)**.
   Viene visualizzata la pagina **Profilo utente**.
4. Aggiungere le informazioni sull'utente come nome, cognome e nome visualizzato.
5. Utilizzare il menu a discesa per assegnare all'utente il ruolo appropriato.
6. Generare la password temporanea.
   Verrà chiesto all'utente di modificare la password al primo accesso.

Connessione di Entra ID a UEM per i dispositivi Windows 10

Per collegare Entra ID a UEM:

1. **Andare in Amministratore > Microsoft Azure > Registrazione e conformità Windows usando Entra ID.**
2. Completare la procedura di configurazione di UEM descritta nella sezione **Configurazione di Entra ID Windows 10 Unified Endpoint Management**
3. Completare la configurazione di **Assegnazione dell'app Entra ID UEM** nel portale Azure.
4. Nel portale Amministratori di Ivanti Neurons per MDM, digitare il nome di dominio del proprio account Entra ID, quindi fare clic su Connetti portale Azure e selezionare la casella di controllo.

5. Una volta completata la procedura di accesso, acconsentire a permettere a MobileIron AD Tenant Validation APP di verificare che Ivanti Neurons for MDM UEM APP sia configurata. Viene visualizzato un messaggio che indica che la connessione è avvenuta correttamente.

Microsoft Passport for Work per dispositivi Windows 10

Microsoft Passport for Work è stato sostituito da Windows Hello for Business. Per ulteriori informazioni, vedere **Configurazione di Windows Hello for Business**.

Registrazione Entra ID del dispositivo Windows

Prerequisiti

Gli utenti devono essere registrati in Ivanti Neurons for MDM.

Collegare il proprio dominio per registrare gli utenti sui loro dispositivi Windows 10+.

1. Fare clic su **Unisciti a Entra ID**.
2. Immettere nome utente e password.
3. Fare clic su **Accesso**.
4. Accettare il Contratto di licenza con l'utente finale
5. Fare clic su **Crea PIN**.
    - Se è stata abilitata la complessità del PIN di Microsoft Passport for Work, verrà chiesto di configurare un PIN complesso secondo la policy configurata.
    - Entra ID esegue l'autenticazione dell'utente e scarica un JWT (token Web JSON) sul dispositivo.
    - Il dispositivo è ora registrato.
    - L'utente viene contattato tramite il dispositivo per la verifica.
6. Immettere il PIN e confermare.
7. Fare clic su **OK**.

Supporto multiutente per dispositivi Windows

Ivanti Neurons per MDM supporta le funzionalità multiutente per i dispositivi iscritti a Windows 10 Entra ID. Questa funzionalità include il push di determinati profili, quali VPN, Wi-Fi, profili client e-mail predefiniti e certificati a un singolo utente anziché a un dispositivo. Inoltre supporta la distribuzione di app interne e pubbliche per gli utenti che hanno eseguito l'accesso. Ogni volta che un nuovo utente di Entra ID si collega a un dispositivo, Ivanti Neurons per MDM valuta non solo il dispositivo ma anche l'utente. Se l'utente è nuovo, Ivanti Neurons per MDM aggiorna il dispositivo per quell'utente. Se l'utente esiste già nel dispositivo, verranno valutate le eventuali modifiche al dispositivo e le impostazioni utente che devono essere aggiornate dopo l'ultimo accesso.

I dettagli dell'utente Entra ID che ha effettuato l'accesso al dispositivo sono riportati nel portale Amministratori Ivanti Neurons per MDM . Quando l'utente si disconnette dal dispositivo e il secondo utente esegue l'accesso, i dettagli del secondo utente vengono aggiornati nella pagina dei dettagli del dispositivo.

Configurazione di Microsoft Store per le aziende con UEM

Microsoft Store per le aziende è un portale fornito da Microsoft come parte di Azure. Gli amministratori possono accedere a questo portale e acquistare e distribuire app a tutti i dispositivi gestiti. Ivanti Neurons per MDM può essere configurato con Microsoft Store for Business per gestire le applicazioni dall'interno del portale Amministratori Ivanti Neurons per MDM impostando i passaggi seguenti.

Passaggio 1: registrare un'applicazione Entra ID nel portale di Microsoft Azure

1. Aprire il primo browser e accedere al portale di Microsoft Azure (https://portal.azure.com/https://portal.azure.com/).
2. Fare clic sul riquadro a sinistra **Registrazioni per l'app**.
3. Fare clic su **+Registrazione nuova applicazione**
4. Immettere le seguenti informazioni per registrare MobileIron come app Azure:
    - **Nome**: immettere un nome per l'app MobileIron. (questo campo richiede almeno 4 caratteri).
    - **Tipo di applicazione:** selezionare app Web/API.
    - **URL di accesso:** immettere l'URL a cui gli utenti di dispositivi devono accedere per entrare in MobileIron (obbligatorio).
5. Fare clic su **Crea** per aggiungere l'app e tornare alla home page di Azure.
6. Passare a Impostazioni e creare una nuova chiave.

Passaggio 2: aggiungere l'applicazione come strumento di gestione

1. Nelle impostazioni di Microsoft Store per le aziende, fare clic su Gestisci
2. Impostazioni di distribuzione
3. In Aggiungi strumento di gestione attivare l'applicazione creata.

Collegare l'account nel portale Amministratori

1. Andare in **Amministratore > Microsoft Azure> Microsoft Store per le aziende**.
2. Nel passaggio 1, **Registrare un'applicazione Entra ID**, selezionare la casella di controllo **Sì, ho completato questo passaggio**.
3. Nel passaggio 2, **Aggiungere strumento di gestione**, selezionare la casella di controllo **Sì, ho completato questo passaggio**
4. Nel passaggio 3, Collegare l'account, aggiornare i seguenti campi:
    - Dominio Entra ID
    - Identificatore applicazione
    - Chiave applicazione
    - Intervallo di sincronizzazione (ore)
5. Fare clic su **Connetti**. Verrà visualizzato un messaggio che conferma che lo store MobileIron per le aziende è stato configurato correttamente.
6. Fare clic su **Sincronizza app**. Quando la sincronizzazione viene completata correttamente, lo stato viene visualizzato come **Applicazioni sincronizzate correttamente**.

Quando il Microsoft Store per le app viene inviato al dispositivo, i dettagli delle app sono disponibili nella scheda **App installate** nei dettagli del dispositivo. Ogni app di Microsoft Store per le aziende segnalata dal dispositivo può essere identificata come **Microsoft Store per le aziende** nella colonna **Origine**.

12.5.2. Configurazione di Entra ID Windows 10 Unified Endpoint Management

Per configurare Windows 10 Unified Endpoint Management (UEM):

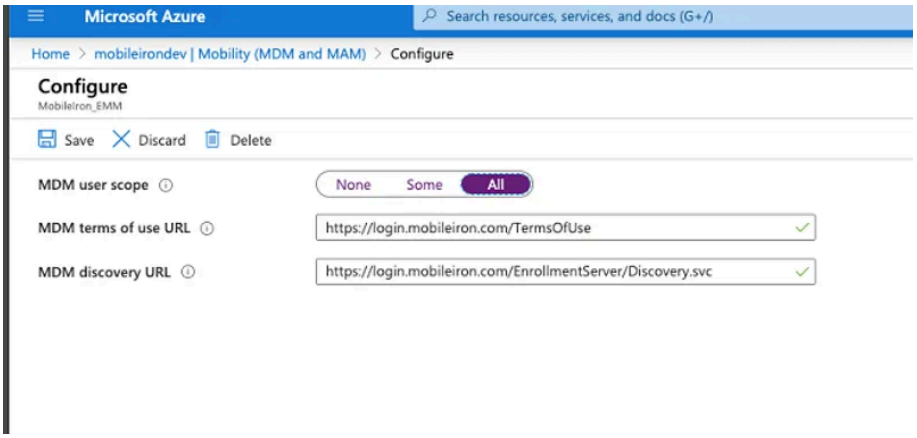
1. Accedere a https://portal.azure.com/ come utente amministratore e selezionare Entra ID.
2. Selezionare "Mobility (MDM and MAM)" nel riquadro a sinistra e quindi **+ Add Application**.

3. Selezionare l'applicazione MobileIron_UEM dalla gallery delle app e fare clic su **Add**.


12.5.3. Assegnazione dell'app Entra ID UEM

Per completare la configurazione dell'assegnazione agli utenti:

1. Fare clic sull'app MobileIron UEM creata nel passaggio 2 nella configurazione di **Configurazione di Entra ID Windows 10 Unified Endpoint Management**.
2. Nell'ambito degli utenti MDM, assegnarla ai gruppi di utenti personalizzati o selezionare **All**.



12.5.4. Collegare Ivanti Neurons per MDM con origine utente Entra ID

Per lavorare con Entra ID (Entra ID), è necessario configurare Ivanti Neurons per MDM con i dettagli dell'account Microsoft Entra ID. È necessario un account Microsoft Entra ID esistente e configurato. Questa soluzione non richiede alcun LDAP o connettore locale.

Argomenti della sezione:

- Casi di utilizzo
- Utilizzo di Entra ID
- Impostazioni Entra ID

Casi di utilizzo

È possibile connettere Ivanti Neurons per MDM a Entra ID per uno dei seguenti casi d'uso:

- Utilizzo con Microsoft Office 365
- Configurare Microsoft Entra ID, Microsoft ADFS o un altro provider di identità (IdP) SAML 2.0 per l'autenticazione utente
- Configurare Microsoft Entra ID come origine utente
- Sincronizzare gli utenti da Microsoft Entra ID e iniziare. Tutti gli utenti e i gruppi nel dominio Entra ID verranno sincronizzati nell'istanza di Ivanti Neurons per MDM in uso
  Viene visualizzata una notifica nella pagina **Notifiche** se durante la sincronizzazione Entra ID si verifica un errore dovuto ai motivi seguenti:
  - Il servizio Entra ID non è raggiungibile
  - Tutti gli attributi dell'utente non sono sincronizzati con Entra ID
  - Alcuni attributi dell'utente non sono sincronizzati con Entra ID
- Gli ambienti con più IdP al momento non sono supportati.
- Se non si utilizza Microsoft Entra ID come origine utente, è possibile utilizzare account locali o utenti di origine da LDAP. A tale scopo è necessario configurare un connettore di Ivanti Neurons for MDM per accedere alle risorse LDAP locali.
- L'uso di Microsoft Entra ID solo per l'autenticazione utente e di un LDAP locale per la directory utenti al momento non è supportato.

Utilizzo di Entra ID

Per utilizzare Entra ID, configurare il proprio Provider di identità per l'autenticazione utente con uno dei seguenti metodi:

- Per utilizzare Microsoft Entra ID per l'autenticazione di utente e origine utente, configurare Entra ID come IdP. Andare in **Amministratore > Identità > Configurazione IdP di Ivanti Neurons for MDM** e selezionare **Entra ID** dal menu.
- Per utilizzare Microsoft Entra ID per l'origine utente e ADFS per l'autenticazione utente, configurare ADFS come IdP. Andare in **Amministratore > Identità > Configurazione IdP locale** e selezionare ADFS dal menu.
- Per utilizzare un IdP SAML 2.0 diverso da Entra ID e utilizzare ADFS per l'autenticazione utente, andare in **Amministratore > Identità >Configurazione IdP generico** e seguire le istruzioni nella pagina.

Per ulteriori informazioni, vedere Configurare il provider di identità.

Impostazioni Entra ID

Questo argomento aiuta a configurare le impostazioni Entra ID.

Procedura

1. Andare in **Amministratore > Microsoft Azure > Origine utente Entra ID**.
2. Specificare i seguenti dettagli:
    1. **Nome Entra ID**.
    2. **Intervallo di sincronizzazione** - Modificare la frequenza con cui Ivanti Neurons per MDM sincronizza i dati utente dal proprio Entra ID.
    3. **Abilita questo Entra ID** - Utilizzare questa opzione per abilitare o disabilitare l'istanza Entra ID.
    4. Selezionare **Invita gli utenti importati da Entra ID automaticamente** - Indicare se gli utenti importati da Entra ID a Ivanti Neurons per MDM vengono automaticamente invitati a registrarsi tramite e-mail.
    5. Selezionare **ID Apple gestito** - Scegliere di sincronizzare l'ID Apple gestito per gli utenti Entra ID.
        - **Nessuno**
        - **Modello** -
            - **Indirizzo e-mail utente**
            - **UPN utente**
            - (Facoltativo) selezionare l'opzione Includi sottodominio "appleid" per evitare un conflitto con gli ID Apple esistenti.
    6. (Facoltativo) Fare clic su **Aggiungi attributo personalizzato** - Specificare gli attributi utente personalizzati dal servizio directory che si desidera applicare alla gestione del dispositivo. È possibile fare riferimento a ciascun attributo con $ nei campi della configurazione in grado di supportare le variabili. L'uso di questa opzione richiede l'implementazione coerente degli attributi personalizzati sui server Entra ID. Se un server Entra ID incluso nella propria implementazione non utilizza questo attributo, le funzioni dipendenti da tale attributo potrebbero non funzionare come previsto.

Fare clic su **Salva** dopo aver modificato le impostazioni Entra ID.

12.5.5. Tenant Azure

Argomenti della sezione:

- Requisiti
- Applicare la licenza Intune agli utenti dei dispositivi
- Aggiunta di MobileIron come partner di conformità
- Creazione di un criterio di accesso condizionale in Microsoft Endpoint Manager
- Connessione di Microsoft Azure a Ivanti Neurons per MDM
- Creazione di una policy di conformità dispositivo partner
- Segnalazione stato dispositivi da Ivanti Neurons for MDM ad Azure
- Deprovisioning del tenant Azure

12.5.5.1. Azure Tenant Requirements

Questa sezione descrive la configurazione di Ivanti Neurons for MDM con un tenant Microsoft Azure.

Requisiti

Microsoft

I clienti che utilizzano Ivanti Neurons for MDM devono disporre di un abbonamento valido per Microsoft Intune e assegnare una licenza Microsoft Intune agli utenti dei dispositivi.

MobileIron

- Ivanti Neurons for MDM - Ivanti Neurons for MDM versione 75 fino alla versione più recente, come supportato da MobileIron.
- Licenze aggiuntive - Conformità dispositivo Azure è un'offerta Premium ed è disponibile per i clienti **Secure UEM Premium** e Platinum. Una licenza Platinum è sufficiente per i clienti esistenti.
- Go per iOS (client) o Go per Android (client), dalla versione 75.0 alla versione più recente supportata da MobileIron.

Supporto per più versioni di Ivanti Neurons for MDM

Se si dispone di più Ivanti Neurons for MDM collegati alla stesso tenant Azure, disconnettersi da tutti gli Ivanti Neurons for MDM o disabilitare il criterio di conformità per l'integrazione della conformità Entra ID da uno specifico (singolo) Ivanti Neurons for MDM, in modo da non caricare i dati del dispositivo su Azure

> Assicurarsi di disattivare la policy di conformità prima di scollegare Ivanti Neurons for MDM.

Procedura per gli amministratori di Ivanti Neurons for MDM

La procedura dal punto di vista dell'amministratore di Ivanti Neurons for MDM:

1. L'amministratore applica le licenze Intune agli utenti dei dispositivi. Vedere **Applicare la licenza Intune agli utenti dei dispositivi**.
2. L'amministratore esegue l'accesso nel portale di Azure.
3. L'amministratore aggiunge MobileIron come partner di conformità Azure. Vedere **Aggiunta di MobileIron come partner di conformità**.
4. L'amministratore crea il criterio di accesso condizionale per le app. Vedere **Creazione di un criterio di accesso condizionale in Microsoft Endpoint Manager**.
5. L'amministratore imposta il collegamento tra MobileIron e Azure. Vedere **Connessione di Microsoft Azure a Ivanti Neurons per MDM**.
6. L'amministratore crea la policy di conformità del dispositivo in Ivanti Neurons for MDM. Vedere **Creazione di una policy di conformità dispositivo partner**.
7. Il criterio di accesso condizionale entra in vigore. A seconda se il dispositivo è conforme o no, l'accesso alle app viene concesso o negato.

> Ivanti consiglia agli amministratori di eseguire test su ogni app Microsoft.

12.5.5.2. Applicare la licenza Intune agli utenti dei dispositivi

- Non utilizzare questa funzione se:
  - si sta cambiando gli utenti o gestendo situazioni in cui gli utenti potrebbero cambiare
  - il dispositivo è di proprietà di più utenti
- Ivanti consiglia di non eseguire l'opzione Assegna a utente e di non distribuire la configurazione di conformità del dispositivo a dispositivi multi-utente, quali:
  - dispositivi con Secure Sign-In WebClip
  - dispositivi iPad condivisi
  - Dispositivi in modalità tutto schermo Android

Ivanti Neurons per MDM requisiti per le licenze

Conformità del dispositivo è un'offerta Premium ed è disponibile per i clienti Secure UEM Premium e Platinum. Per i clienti esistenti, una licenza Platinum è sufficiente.

Assegnare licenze in blocco agli utenti dei dispositivi esistenti

Per assegnare licenze in blocco agli utenti dei dispositivi esistenti:

Assegnazione basata sui gruppi

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

Assegnazione basata su 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. Aggiunta di MobileIron come partner di conformità

Prerequisiti

- avere installato una licenza di Microsoft Intune. Vedere **Applicare la licenza Intune agli utenti dei dispositivi**.
- avere creato degli utenti in Microsoft Azure
- aver creato dei gruppi in Microsoft Azure

Procedura

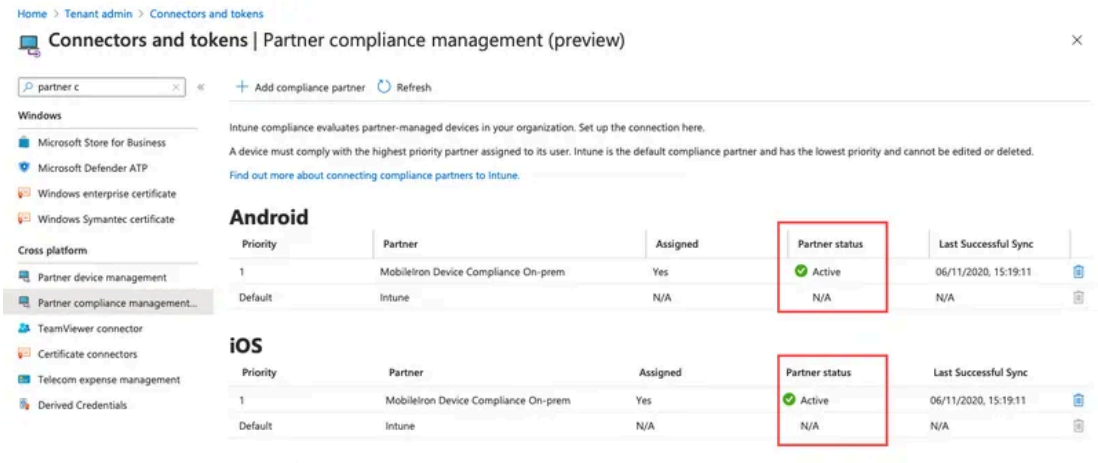
1. Accedere a: **https://endpoint.microsoft.com**.
2. Nel pannello di sinistra della pagina centrale di amministrazione di Microsoft Endpoint Manager, fare clic su Tenant Administrator. Fare clic su Connettori e token > Gestione conformità partner.

3. A destra del campo di ricerca, fare clic su + Add compliance partner.

4. Nella scheda Informazioni di base, selezionare MobileIron Device Compliance Cloud dal menu a discesa del campo del partner di conformità.

5. Nel campo Platform, selezionare iOS o Android e quindi fare clic su Next.
6. Fare clic sulla scheda Assignments. Nel menu a discesa Assign to, selezionare l'utente/il gruppo di utenti dei dispositivi a cui si applica lo stato di conformità. Selezionare l'utente/il gruppo in possesso della licenza.

7. Selezionare Next.
8. Fare clic su Crea. Viene visualizzato il nuovo partner di conformità sulla pagina di gestione della conformità dei partner.



12.5.5.4. Creazione di un criterio di accesso condizionale in Microsoft Endpoint Manager

Procedura

1. Accedere a Microsoft Endpoint Manager **https://endpoint.microsoft.com**.
2. Nella pagina del centro di amministrazione di Microsoft Endpoint Manager, andare a Home > Sicurezza degli endpoint > Accesso condizionale.
3. Fare clic su Criteri e quindi fare clic su + Nuovo criterio.

4. Immettere il nome del criterio di accesso condizionale.

5. In Assegnazioni, fare clic per assegnare il criterio a utenti e gruppi.

6. Fare clic su App cloud o azioni, quindi fare clic su Seleziona. Cercare e selezionare le app che devono essere protette.

7. Fare clic su Condizioni, quindi fare clic su Piattaforma dispositivo. Selezionare le piattaforme dei dispositivi appropriate.

8. Nella pagina Nuovo criterio di accesso condizionale > Controlli di accesso, fare clic su Concedi ed effettuare le selezioni per l'accesso e il blocco.

9. Per abilitare la nuova policy, fare clic su Attiva.

10. Fare clic su Crea.

12.5.5.5. Connessione di Microsoft Azure a Ivanti Neurons per MDM

Procedura

1. Accedere a Ivanti Neurons per MDM e passare ad **Amministratore** > **Microsoft Azure**.
2. Nel riquadro di navigazione di sinistra, fare clic su **Microsoft Azure** > **Conformità dispositivo**.
3. Sotto la sezione Connetti account, fornire i seguenti dettagli:
    - **ID tenant Azure** - Si trova nell'istanza di Microsoft Azure.
    - **URL di registrazione (facoltativo)** - Se il dispositivo non è registrato nell'MDM, gli utenti del dispositivo saranno indirizzati a questo URL per la registrazione. Durante la configurazione, utilizzare il formato HTTPS. Se la propria organizzazione dispone di una pagina per reindirizzare gli utenti dei dispositivi alle informazioni di registrazione, aggiungere il link qui.
    - **URL di correzione (facoltativo)** - Se il dispositivo non è conforme, gli utenti del dispositivo verranno indirizzati a questo URL per la correzione. Durante la configurazione, utilizzare il formato HTTPS. Se la propria organizzazione dispone di una pagina per reindirizzare gli utenti dei dispositivi alle informazioni di correzione, aggiungere il link qui.
4. Fare clic su **Collega account**. Si apre la finestra di dialogo Convalida tenant Azure.

> I tenant attualmente connessi ad Azure e che desiderano aggiungere la conformità dei dispositivi per i dispositivi macOS devono scollegare l'account e ristabilire la connessione.

5. Nella finestra di dialogo Convalida tenant Azure, fare clic sul **collegamento** presente al punto 1.
6. **Accedere**.
7. Controllare le autorizzazioni e poi fare clic su **Accetta**.

> Se si effettua il login e la pagina richiede di effettuare nuovamente il login, chiudere la scheda/finestra del browser.

8. Tornare a Ivanti Neurons per MDM. Nella finestra di dialogo Collega account Azure, selezionare la casella di controllo **Ho fornito il consenso**. Fare clic su **Conferma**.

- Per modificare l'account, fare clic su **Modifica account**.
- Per scollegare l'account, fare clic su **Disconnetti account**. Per ulteriori istruzioni, vedere Deprovisioning del tenant Azure.
- Tutte le attività di aggiunta, modifica e disattivazione di un account sono registrate nei Registri.

12.5.5.6. Creazione di una policy di conformità dispositivo partner

Creare un criterio di conformità del dispositivo partner in Ivanti Neurons per MDM e applicare l'etichetta desiderata. Il criterio di conformità partner riporta lo stato di conformità del dispositivo a Azure o BeyondCorp per l'accesso condizionato.

Applicabile a

- iOS
- Android
- Windows

Prerequisiti

È necessario disporre di un ID Azure Tenant o di un ID Google BeyondCorp. Per ulteriori informazioni sulla conformità dei dispositivi partner Azure, consultare **Connessione di Microsoft Azure a Ivanti Neurons per MDM**.



Procedura

1. Accedere a Ivanti Neurons per MDM, passare a **Configurazioni**.
2. Fare clic su **Aggiungi** e cercare la configurazione **Conformità dispositivo partner**.
3. Inserire i seguenti dettagli nella pagina **Crea configurazione conformità dispositivo partner**:

Elemento	Descrizione
Nome	Immettere un nome.
+ Aggiungi descrizione	Inserisci una spiegazione.
Scegli partner	Selezionare **Conformità Microsoft Azure**. o **Conformità Google BeyondCorp - Beta**.
Impostazioni configurazione Segnalare lo stato di conformità ad Azure per dispositivi iOS, macOS e Android	Attivata per impostazione predefinita. Se questo campo non viene visualizzato, è necessario impostare il proprio ID Tenant Azure. Se l'opzione Segnala stato di conformità per dispositivi iOS, macOS e Android è attivata e il criterio di conformità è applicato al client, quest'ultimo visualizzerà "Microsoft 365 Access" nei dispositivi in Impostazioni. Lo stato di conformità del dispositivo viene segnalato quando: • il dispositivo non è conforme • il dispositivo è conforme • il dispositivo torna a essere conforme • sono trascorse 24 ore. Se lo stato non cambia, viene inviato un report una volta alla settimana / ogni sette giorni.
Segnalare lo stato di conformità a Google BeyondCorp per dispositivi iOS, macOS, Android e Windows	Attivata per impostazione predefinita. Lo stato di conformità del dispositivo viene segnalato quando: • il dispositivo non è conforme • il dispositivo è conforme • il dispositivo torna a essere conforme • sono trascorse 24 ore. Se lo stato non cambia, viene inviato un report ogni 24 ore.

4. Fare clic su **Avanti**.
5. L'opzione **Abilita questa configurazione** è selezionata per impostazione predefinita.
6. Scegliere un livello di distribuzione per la configurazione. Per ulteriori informazioni sulla distribuzione della configurazione, vedere **Aggiunta di una configurazione**.
7. Fare clic su **Fine**.

12.5.5.7. Segnalazione stato dispositivi da Ivanti Neurons for MDM ad Azure

Per i seguenti casi, Ivanti Neurons for MDM segnala l'inventario del dispositivo e lo stato di conformità.

- Modifica dello stato di conformità sul dispositivo
- Modifica dell'inventario sul dispositivo
- Una volta alla settimana, Ivanti Neurons for MDM segnala lo stato di conformità e dell'inventario

In base all'azione scelta nella policy di conformità, verrà inviato il seguente stato del dispositivo:

Azione **(si applica la più restrittiva)**	**Cosa invia Ivanti Neurons for MDM**
Blocco email, App AppConnect, Quarantena	Dispositivo non conforme
Invia l'avviso	Conforme ad Azure
Ritira dispositivo	Dati del dispositivo rimossi dalla piattaforma Azure

Pagina dei dettagli del dispositivo

Per visualizzare le informazioni di Azure sul dispositivo, andare alla pagina Dettagli dispositivo. La descrizione dei campi e i loro possibili valori:

Campo	Descrizione
Identificatore dispositivo Azure	L'ID del dispositivo indicato da Microsoft al dispositivo iOS o Android. Ad esempio: 007c8232-9489-4074-9b35-345b16f0a72d. Ivanti Neurons for MDM riceve questo ID del dispositivo poiché gli utenti dei dispositivi sono tenuti a registrarsi nell'applicazione Microsoft Authenticator per utilizzare questa funzione. Se non è possibile recuperare l'ID del dispositivo, il campo viene lasciato vuoto.
Stato di conformità dispositivo Azure	Elenca lo stato di conformità del dispositivo in Azure. Valori possibili: • In corso • Operazione riuscita • Non riuscito
Codice stato client Azure	Indica se il dispositivo è collegato ad Azure. Valori possibili: • Success - In grado di recuperare l'ID del dispositivo. • Internal_Error - Si è verificato un errore irreversibile all'interno del client o lato server. • Workplace_Join_Required - Registrazione dispositivo necessaria. L'utente del dispositivo può attenuare questo stato. • Interaction_Required - È necessario un accesso interattivo. L'utente del dispositivo può attenuare questo stato. • Server_Declined_Scopes - Accesso non concesso ad alcuni ambiti. • Server_Protection_Policies_Required - La risorsa richiesta è protetta da una policy Intune Conditional Access. • User_Canceled - L'utente del dispositivo ha annullato la sessione di autenticazione Web toccando il pulsante "Fine" o "Annulla" nel browser web. • Account_logged_out - Account disconnesso.
Ora report di conformità dispositivo Azure	Ora in cui Ivanti Neurons for MDM ha segnalato lo stato di conformità del dispositivo a Microsoft Intune. Un campo vuoto indica una delle condizioni seguenti: • quella funzione è disabilitata • Ivanti Neurons for MDM ha ricevuto i dati e deve ancora chiamare l'API di Microsoft • è presente un errore come user_Cancelled o Errore interno

12.5.5.8. Deprovisioning del tenant Azure

Se più versioni di Ivanti Neurons for MDM sono abilitate per l'uso dello stesso tenant Azure, eliminare il provisioning d tutte le versioni di Ivanti Neurons for MDM. Se si desidera interrompere l'utilizzo di Azure per un solo Ivanti Neurons for MDM, è possibile disattivare la policy di conformità del partner solo per quel determinato Ivanti Neurons for MDM.

Se l'amministratore esegue una disconnessione su Ivanti Neurons for MDM, Ivanti Neurons for MDM blocca la segnalazione dell'inventario del dispositivo e dello stato di conformità ad Azure.

Prerequisiti

- Verificare che tutti i dispositivi siano non gestiti
- Verificare che tutti i dispositivi siano non conformi

Procedura

Microsoft

1. Accedere a Microsoft Azure.
2. Andare a Intune > Accesso condizionale. Assicurarsi che il criterio di accesso condizionale sia disabilitato.

Ivanti Neurons per MDM

1. Accedere a Ivanti Neurons for MDM e passare ad Amministratore.
2. Nel riquadro di navigazione a sinistra, fare clic su Microsoft Azure > Conformità dispositivo per iOS e Android.
3. Fare clic su Disconnetti account.



4. Fare clic su Sì.

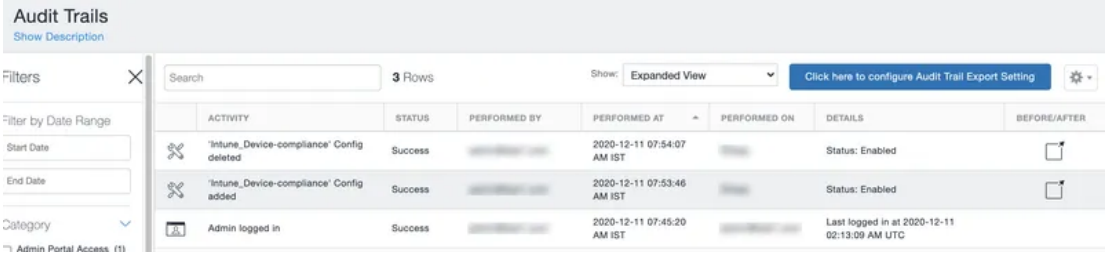
Dismettere un dispositivo in Azure

Al momento della dismissione di un dispositivo, Ivanti Neurons for MDM segnala ad Azure che il dispositivo non è più sotto gestione ed è non conforme.

Azure elimina la voce relativa al dispositivo dismesso dopo 90 giorni.

Attività dell'account Azure registrate nei registri

Tutte le attività vengono registrate nei registri.



12.5.6. Amministratore > Microsoft Azure > Sicurezza delle app Office 365

Licenza: Gold

È possibile configurare le policy di sicurezza delle app Office 365 per proteggere i dati aziendali. Le policy applicano i controlli di prevenzione della perdita dei dati (DLP) per le app Microsoft Office 365 mediante le API Microsoft Graph. Alcune di queste API Graph consentono agli amministratori di applicare la protezione delle app iOS e Android native che sfruttano l'SDK Graph.

Utilizzare questa funzionalità per applicare policy come:

- Impedire agli utenti di stampare dalle app Office 365.
- Impedire la condivisione di dati in uscita dalle app Office 365.
- Applicare il PIN per le app Office 365.
- Disattivare la sincronizzazione dei contatti dalle app Office 365.

Prerequisiti per l'utilizzo della Sicurezza delle app Office 365

Per utilizzare la Sicurezza delle app Office 365 sono necessari:

- Una licenza MobileIron valida
- Funzionalità di protezione app di Office 365 abilitata in Ivanti Neurons for MDM
- Un abbonamento a Intune o a Microsoft EMS che includa Intune.
    - Ogni uso per cui la policy viene applicata richiede una licenza, tuttavia abilitare e testare l'integrazione richiede solo una singola licenza.
- Un abbonamento valido a Office Enterprise o Business con accesso alle app Office 365 da dispositivo mobile
- Una o più app Office 365
- Sincronizzazione degli utenti di Active Directory con il proprio Entra ID.
- Installazione di One Drive for Business sui dispositivi per proteggere i dati su Word, Excel, e PowerPoint Non è obbligatoria.
- Eseguire l'accesso al portale Microsoft Azure (**https://portal.azure.com/**) per configurare le policy di protezione delle app Intune.
- App Intune Company Portal installata sui dispositivi Android.
  Gli utenti dei dispositivi non sono obbligati ad accedere, ma l'app deve essere installata sui dispositivi per proteggerne i dati. Sarà possibile applicare la protezione quando l'utente accede all'app.

Registrazione di MobileIron come app Azure

In questa sezione viene spiegato come registrare e memorizzare le credenziali del tenant Azure con il software Ivanti Neurons for MDM e come gestire da remoto le policy di protezione delle app nel cloud di Microsoft Azure per le app Office 365 di iOS e Android. Anche se non è necessario, è possibile aprire due browser per eseguire i passaggi descritti nelle seguenti procedure. Utilizzare il primo browser per accedere al portale di Microsoft Azure. Utilizzare il secondo browser per accedere al portale Amministratori di Ivanti Neurons for MDM.

Procedura per il portale di Microsoft Azure

Microsoft potrebbe modificare l'interfaccia utente del portale Azure di tanto in tanto. Queste istruzioni presuppongono che si abbia familiarità con Microsoft Azure Portal e si possano effettuare gli adeguamenti necessari quando si registra MobileIron come un'app Azure.

1. Aprire il primo browser e accedere al portale di Microsoft Azure (**https://portal.azure.com/**).
2. Fare clic sul riquadro a sinistra **Registrazioni per l'app**.
3. Fare clic su **+Registrazione nuova applicazione**.
4. Immettere le seguenti informazioni per registrare MobileIron come app Azure.
    - **Nome:** immettere un nome per l'app MobileIron. (questo campo richiede almeno 4 caratteri).
    - **Tipo di applicazione:** selezionare App Web/API.
    - **URL di accesso:** immettere l'URL a cui gli utenti di dispositivi devono accedere per entrare in MobileIron (obbligatorio).

Fare clic su **Crea** in fondo al riquadro per aggiungere l'app e tornare alla home page di Azure.

6. Fare clic sull'app MobileIron appena creata nella home page di Azure.
7. Ritornare alla home page di Azure per assegnare le autorizzazioni all'app MobileIron Azure.
8. Per impostare le autorizzazioni API necessarie per l'app MobileIron appena creata, fare clic sul nome dell'app in Registrazioni app.
9. Fare clic su **Autorizzazioni API** > **Aggiungi un'autorizzazione**.
10. Nella sezione **Microsoft Graph > Autorizzazioni delegate > App gestione dispositivi** selezionare l'autorizzazione **DeviceManagementApps.Read.All** e fare clic su **Salva**. Per impostazione predefinita, l'autorizzazione user.Read è abilitata per l'app.
11. Fare clic sul pulsante per **concedere il consenso dell'amministratore per MobileIron**.
12. Eseguire la seguente procedura per il portale Amministratori di Ivanti Neurons per MDM.

Procedura per il portale Amministratori di Ivanti Neurons for MDM

1. Aprire il secondo browser e accedere al portale Amministratori di Ivanti Neurons for MDM.
2. Andare in **Amministratore > Microsoft Azure > Protezione delle app Office 365**.
3. Incollare **ID applicazione** nel portale Amministratori Ivanti Neurons per MDM.
4. **Procedura**
    1. Andare al portale di Azure.
    2. Selezionare l'app MobileIron > **Proprietà**.
    3. Copiare l'**ID applicazione**.
    4. Tornare ad **Amministratore > Microsoft Azure > Sicurezza delle app Office 365** nel portale Amministratori.
    5. Incollare l'**ID applicazione** nel campo corrispondente.

Incollare il **Segreto applicazione** (Segreto client) nel portale Amministratori di Ivanti Neurons per MDM.

5. **Procedura**
    1. Andare al portale di Azure.
    2. Selezionare l'app MobileIron.
    3. Fare clic su **Chiavi** e immettere un nome in **Descrizione chiave** e selezionare un periodo di validità in **Durata**.

4. Fare clic su **Salva** e copiare il valore **Chiave**.
5. Tornare ad **Amministratore > Microsoft Azure > Sicurezza delle app Office 365** nel portale Amministratori.
6. Incollare il valore nel campo **Segreto applicazione** (Segreto client).

Incollare l'**ID tenant** nel portale Amministratori di Ivanti Neurons per MDM.

6. **Procedura**
    1. Andare al portale di Azure.
    2. Fare clic su Entra ID nel riquadro di sinistra e poi su Proprietà.
    3. Copiare l'ID directory.
    4. Tornare ad **Amministratore > Microsoft Azure > Sicurezza delle app Office 365** nel portale Amministratori.
    5. Incollare il valore nel campo **ID tenant**.

Immettere il **nome utente** e la **password** dell'amministratore di Intune.

- L'account Azure deve avere diritti di amministratore globale o di amministrazione limitato + diritti di amministrazione del servizio Intune.
- Ivanti consiglia di creare un account Azure locale a cui vengono concessi solo i diritti di amministrazione del servizio Intune. Microsoft non supporta l'autenticazione con le API Graph per gli account utente federati a un provider di identità.

Fare clic su **Autentica e salva**.
Se la data di invio non è corretta, viene visualizzato un messaggio di errore.

Policy per Sicurezza delle app di Office 365

Dopo aver configurato le credenziali di Microsoft Graph, selezionare **App > Sicurezza delle app Office 365** per aggiungere nuove policy di protezione delle app Office 365 ai dispositivi iOS o Android per gruppi di utenti diversi.

Le policy sono elencate nella pagina **App > Sicurezza Office 365** nella scheda **Policy app**. L'elenco delle policy fornisce dettagli tabulari quali attributi data e ora aggiornati, piattaforma, app assegnate e gruppi utenti distribuiti.

Aggiunta di una policy per Sicurezza delle app Office 365 su dispositivi iOS

Procedura

1. Andare in **App > Sicurezza Office 365**.
2. Fare clic su **Policy app > + Aggiungi**.
3. Immettere un **Nome** e una **Descrizione** facoltativa per la policy.
4. In Scegli sistema operativo, fare clic su **iOS**.
5. In **Rilocazione dati**, selezionare le seguenti opzioni e impostazioni:
    - Impedisci backup di iTunes e iCloud
    - Consenti all'app di trasferire i dati ad altre app: Tutte le app (predefinita), App gestite dalle policy, Nessuna
    - Consenti all'app di ricevere i dati da altre app: Tutte le app (predefinita), App gestite dalle policy, Nessuna
    - Impedisci "Salva con nome"
    - Limita taglia, copia e incolla con altre app: Qualsiasi app (predefinita), Bloccate, App gestite dalle policy, Gestita dalla policy con incolla in

- Limita contenuto Web da visualizzare nel browser gestito
- Crittografa dati dell'app: Quando il dispositivo è bloccato (predefinita), Quando il dispositivo è bloccato e sono presenti file aperti, Dopo il riavvio del dispositivo, Usa impostazioni dispositivo
- Disabilita sincronizzazione contatti
- Disabilita stampa

6. In **Accesso**, seleziona le seguenti opzioni e impostazioni:
   - Richiedi PIN per l'accesso
   - Numero di tentativi prima delle reimpostazioni del PIN (5 per impostazione predefinita)
   - Consenti PIN semplice
   - Lunghezza PIN (4 caratteri per impostazione predefinita)
   - Consenti impronta digitale invece del PIN (iOS 8+)
   - Disabilita PIN dell'app quando il PIN del dispositivo è gestito
   - Richiedi credenziali aziendali per l'accesso
   - Impedisci l'esecuzione di app gestite su dispositivi soggetti a jailbreak o a rooting
   - Ricontrolla requisiti di accesso dopo (Minuti)
     - Timeout: deve essere un valore compreso tra 1 e 65535 (30 per impostazione predefinita)
     - Periodo di tolleranza offline: deve essere un valore compreso tra 1 e 65535 (720 per impostazione predefinita)
     - Intervallo offline (giorni) prima della cancellazione dei dati dell'app: deve essere un valore compreso tra 1 e 65535 (90 per impostazione predefinita)

   Richiedi almeno sistema operativo iOS
   - Richiedi almeno sistema operativo iOS (solo avviso)
   - Richiedi versione minima dell'app
   - Richiedi versione minima dell'app (solo avviso)
   - Richiedi almeno versione SDK della policy di protezione app di Intune

Fare clic su **Avanti**.

8. Selezionare e assegnare le app a cui applicare la policy.
9. Fare clic su **Avanti**.
10. Selezionare i gruppi di utenti a cui applicare la policy.
11. Fare clic su **Fine**.

Aggiunta di una policy per Sicurezza delle app Office 365 sui dispositivi Android

Procedura

1. Andare in **App > Sicurezza Office 365**.
2. Fare clic su **Policy app > + Aggiungi**.
3. Immettere un **Nome** e una **Descrizione** facoltativa per la policy.
4. In Scegli sistema operativo, fare clic su **Android**.
5. In **Rilocazione dati**, selezionare le seguenti opzioni e impostazioni:

- Impedisci backup di Android
- Consenti all'app di trasferire i dati ad altre app: Tutte le app (predefinita), App gestite dalle policy, Nessuna
- Consenti all'app di ricevere i dati da altre app: Tutte le app (predefinita), App gestite dalle policy, Nessuna
- Impedisci "Salva con nome"
- Limita taglia, copia e incolla con altre app: Qualsiasi app (predefinita), Bloccate, App gestite dalle policy, Gestita dalla policy con incolla in
- Limita contenuto Web da visualizzare nel browser gestito
- Crittografa dati dell'app
- Disabilita cifratura dell'app quando è abilitata la cifratura del dispositivo
- Disabilita sincronizzazione contatti
- Disabilita stampa

6. In **Accesso**, seleziona le seguenti opzioni e impostazioni:
   - Richiedi PIN per l'accesso
   - Numero di tentativi prima delle reimpostazioni del PIN (5 per impostazione predefinita)
   - Consenti PIN semplice
   - Lunghezza PIN (4 caratteri per impostazione predefinita)
   - Consenti impronta digitale invece del PIN (Android 6+)
   - Disabilita PIN dell'app quando il PIN del dispositivo è gestito
   - Richiedi credenziali aziendali per l'accesso
   - Impedisci l'esecuzione di app gestite su dispositivi soggetti a jailbreak o a rooting
   - Ricontrolla requisiti di accesso dopo (Minuti)
     - Timeout: deve essere un valore compreso tra 1 e 65535 (30 per impostazione predefinita)
     - Periodo di tolleranza offline: deve essere un valore compreso tra 1 e 65535 (720 per impostazione predefinita)
     - Intervallo offline (giorni) prima della cancellazione dei dati dell'app: deve essere un valore compreso tra 1 e 65535 (90 per impostazione predefinita)
   - Blocca acquisizione schermo e assistente Android
   - Richiedi almeno sistema operativo Android
   - Richiedi almeno sistema operativo Android (solo avviso)
   - Richiedi versione minima dell'app
   - Richiedi versione minima dell'app (solo avviso)
   - Richiedi almeno versione SDK della policy di protezione app di Intune
7. Fare clic su **Avanti**.
8. Selezionare e assegnare le app a cui applicare la policy.
9. Fare clic su **Avanti**.
10. Selezionare i gruppi di utenti a cui applicare la policy.
11. Fare clic su **Fine**.

Modifica di una policy di sicurezza delle app Office 365

Procedura

1. Andare in **App > Sicurezza Office 365**.
2. Fare clic su **Policy app**.
3. Fare clic sul nome della policy da modificare.
4. Nella pagina dei dettagli della policy, fare clic su **Modifica**.
5. Modificare le impostazioni di configurazione della policy.
6. Fare clic su **Avanti**.
7. Modificare l'elenco di app a cui applicare la policy.
8. Fare clic su **Avanti**.
9. Modificare i gruppi di utenti a cui applicare la policy.
10. Fare clic su **Fine**.

Eliminazione di una policy di sicurezza delle app Office 365

Procedura

1. Andare in **App > Sicurezza Office 365**.
2. Fare clic su **Policy app**.
3. Nella colonna **Azioni**, fare clic sull'icona di rimozione corrispondente al nome della policy da eliminare.
4. Fare clic su **Sì** per confermare.

Configurazioni delle app Office 365

Andare alla pagina **App > Sicurezza Office 365**, alla scheda **Configurazione delle app** per aggiungere, modificare o eliminare le configurazioni delle app Office 365 per diversi gruppi di utenti. Nelle configurazioni delle app gli amministratori possono aggiungere un elenco di coppie chiave-valore e assegnare le configurazioni a una o più app Office 365. Nella scheda Configurazione delle applicazioni sono elencate le configurazioni con dettagli tabulari, quali attributi data e ora, app assegnate e stato della distribuzione.

Aggiunta di una configurazione delle app Office 365

Procedura

1. Andare in **App > Sicurezza Office 365**.
2. Fare clic su **Configurazione app > + Aggiungi**.
3. Immettere un **Nome** e una **Descrizione** facoltativa per la configurazione.
4. Immettere le coppie chiave-valore.
5. Fare clic su **Avanti**.
6. Selezionare le app a cui verrà applicata questa configurazione.
7. Fare clic su **Avanti**.
8. Seleziona i gruppi di utenti a cui verrà applicata questa configurazione.
9. Fare clic su **Fine**.

Modifica di una configurazione delle app Office 365

Procedura

1. Andare in **App > Sicurezza Office 365**.
2. Fare clic su **Configurazione delle app**.
3. Fare clic sul nome della configurazione da modificare.
4. Nella pagina dei dettagli della configurazione, fare clic su **Modifica**.
5. In alternativa, fare clic sulle schede **Distribuzione delle app** o **Distribuzione gruppi utenti**. Fare clic su **Modifica** per modificare solo quelle impostazioni e su **Salva**.
6. Modificare le impostazioni di configurazione.
7. Fare clic su **Avanti**.
8. Modificare l'elenco di app a cui applicare la configurazione.
9. Fare clic su **Avanti**.
10. Modificare i gruppi di utenti a cui verrà applicata questa configurazione.
11. Fare clic su **Fine**.

Eliminazione di una configurazione delle app Office 365

Procedura

1. Andare in **App > Sicurezza Office 365**.
2. Fare clic su **Configurazione delle app**.
3. Nella colonna **Azioni**, fare clic sull'icona di rimozione corrispondente al nome della configurazione da eliminare.
4. Fare clic su **Sì** per confermare.

Utenti con app Office 365 non conformi

Gli amministratori possono rivedere l'elenco degli utenti e dei relativi dispositivi non conformi. Utilizzare questa pagina per cancellare eventuali app Office 365 su tali dispositivi contrassegnati.

Cancellazione di app Office 365

Procedura

1. Andare in **App > Sicurezza Office 365**.
2. Fare clic su **Utenti non conformi**.
3. Eseguire una delle operazioni seguenti:
   - Selezionare gli utenti dall'elenco e fare clic su **Cancella app Office 365**.
   - Fare clic sul nome utente per visualizzare l'elenco di dispositivi con app non conformi. Nella colonna **Azione**, fare clic sull'icona **Cancella app Office 365** per i dispositivi specifici.
   - Fare clic sul nome utente per visualizzare l'elenco di dispositivi con app non conformi. Fare clic sul nome di un dispositivo specifico per visualizzare le app elencate con ID bundle/nomi pacchetto e i motivi contrassegnati. Fare clic su **Cancella app Office 365**.
4. Fare clic su **Sì** per confermare l'azione.

In alternativa, procedere come segue:

1. Andare a **Utenti**.
2. Fare clic sul nome dell'utente per aprire la relativa pagina dei dettagli.
3. Fare clic su **Azione > Cancella app Office 365**.
4. Selezionare i dispositivi per i quali cancellare le app Office 365.
5. Fare clic su **OK** per confermare l'azione.

Annullamento di richieste di cancellazione di app Office 365

Procedura

1. Andare a **Utenti**.
2. Fare clic sul nome dell'utente per aprire la relativa pagina dei dettagli.
3. Fare clic sulla scheda **Sicurezza Office 365**.
4. Nella casella a discesa **Seleziona tipo di report**, selezionare il report **Richieste di cancellazione** per visualizzarne le informazioni.
5. Selezionare i dispositivi per cui si desidera annullare le richieste di cancellazione. È possibile selezionare solo i dispositivi con stato Cancellazione in sospeso.
6. Fare clic su **Annulla cancellazione**.
7. Fare clic su **OK** per confermare l'azione.

Aggiunta di report per utenti con Sicurezza delle app Office 365

Gli amministratori possono selezionare uno dei seguenti report per rivedere l'elenco di utenti con Sicurezza delle app Office 365 e relative informazioni:

- Report policy delle app
- Report configurazioni delle app
- Cancella richieste

Le informazioni contenute nei report delle app includono ID bundle/nome pacchetto, nome dispositivo, tipo di dispositivo, policy o configurazioni (distribuite al dispositivo), stato (Sincronizzato, Sincronizzato ma non aggiornato o Non sincronizzato) e l'ora dell'ultimo check-in. È possibile esportare le informazioni dei report delle app in un file CSV per successivo riferimento o analisi.

Le informazioni nel report Richieste di cancellazione include nome visualizzato, nome utente, nome del dispositivo, tipo di dispositivo e stato della cancellazione (Cancellazione in sospeso o Cancellazione completata).

Per visualizzare uno dei report, procedere come segue:

1. Andare a **Utenti**.
2. Fare clic sul nome dell'utente per aprire la relativa pagina dei dettagli.
3. Fare clic sulla scheda **Sicurezza Office 365**.
4. Nella casella a discesa **Seleziona tipo di report**, selezionare uno dei report per visualizzarne le informazioni.
5. (Facoltativo) Nella pagina del report Richieste di cancellazione, selezionare i dispositivi per cui si desidera annullare le richieste di cancellazione, quindi fare clic su **Annulla cancellazione**. È possibile selezionare solo i dispositivi con stato Cancellazione in sospeso.
6. (Facoltativo) Fare clic su **Esporta in CSV** per scaricare il contenuto del report in un file CSV per successivo riferimento o analisi.

12.6. Connessione a Google Apps

Argomenti della sezione:

- Account Google Play gestiti (account Android Enterprise)
- Registrazione di dispositivi Android
- API di gestione Android
- API Google App
- Amministratore - Android Enterprise

12.6.1. Account Google Play gestiti (account Android Enterprise)

Licenza: Silver

Gli account Google Play gestiti sono richiesti per consentire l'utilizzo e la configurazione dei dispositivi con Android Enterprise. Non è più necessario utilizzare Google Apps Directory Sync (GADS) o gli account Google per registrare i dispositivi.

Importante: se è già stata configurata Android Enterprise, è necessario annullare la registrazione e dismettere i dispositivi per potere utilizzare questa funzionalità.

Configurazione di Android Enterprise utilizzando l'account Google Play gestito

Procedura

1. Accedere al portale Ivanti Neurons per MDM.
2. Andare in **Amministratore > Google > Android Enterprise**.
3. In **Account Google Play gestito**, fare clic su **Autorizza Google** per visualizzare la pagina di **Google Play for Work**.
4. Immettere l'**ID e-mail dell'account Google Play**.
5. Fare clic su **Inizia**.
6. Accettare il contratto di Android Enterprise.
7. Fare clic su **Conferma**.
8. Fare clic su **Completa registrazione**.
   La sezione **Configurazione Android Enterprise** visualizza le seguenti informazioni:
   - **Stato**
   - **E-mail amministratore**
   - **Tipo di azienda**
   - **ID Google Enterprise**

Se Android Enterprise viene configurato con un account Google Play gestito, il numero di dispositivi registrati con Android Enterprise è limitato. Per ignorare la limitazione, selezionare l'opzione **Account dispositivi con Android Enterprise** durante la creazione di un nuovo utente per assegnare automaticamente a un account dispositivo Google le registrazioni di dispositivi con Android Enterprise gestiti associate all'account.

Gli account dei dispositivi vengono utilizzati per distribuzioni COSU (monouso) (ad esempio con la modalità tutto schermo). È possibile che gli utenti con account dei dispositivi abbiano accesso limitato a Google Play.

Di tanto in tanto, un account Google Play gestito o il relativo token scade per vari motivi, come la scadenza del token di autenticazione o l'eliminazione dell'account o dell'azienda. In tali scenari i servizi Google Play inviano una notifica al client tramite un'azione broadcast che induce il client a ripetere il provisioning del dispositivo, rimuovendo l'account esistente e aggiungendo un account con un nuovo token ottenuto dal server UEM.

Se la ripetizione del provisioning dell'account non riesce perché non è possibile rimuovere l'account precedente o sono stati eseguiti troppi tentativi di ripetere il provisioning, all'utente verrà richiesto di ricominciare dall'inizio, ritirando il client o ripristinando le impostazioni di fabbrica del dispositivo, a seconda che il dispositivo sia in modalità Profilo di lavoro o in modalità Dispositivo gestito, rispettivamente.

Eseguire la migrazione dell'account Google Play gestito esistente all'account di dominio Google gestito (BTE)

Questa funzione consente di migrare gli account e i dispositivi Android Enterprise dall'**Account Google Play gestito** all'**Account Dominio Google gestito**.

La migrazione è composta da:

- Upgrade account
- Migrazione del dispositivo

Prerequisiti

- I dispositivi devono essere registrati in modalità Dispositivo gestito dal lavoro o Profilo di lavoro; i dispositivi registrati in modo Profilo di lavoro su dispositivo di proprietà aziendale (WPCOD) devono eseguire Android 12 o versioni successive.
- Ai dispositivi vengono assegnati ID e-mail corporate o business validi.

> Se il dispositivo è assegnato a un ID e-mail non aziendale, l'amministratore deve riassegnare un ID e-mail aziendale valido affinché il dispositivo sia idoneo per la migrazione.

Upgrade dell'account Android Enterprise

Effettuare l'upgrade dell'account Android Enterprise dall'account Google Play gestito all'account Dominio Google gestito.

Procedura

1. Andare in **Amministratore** → **Google** → **Android Enterprise**.
2. Fare clic su **Esegui upgrade account**.
3. Accedere utilizzando un ID e-mail corporate o business valido.
4. Completare il processo di upgrade.
5. Aggiornare la pagina.

Applicare la configurazione di migrazione del dispositivo

Procedura

1. Andare in Configurazioni.
2. Selezionare **Android Enterprise; migrazione dispositivo dalla configurazione Google Play gestito ad Account Google gestito** > **Modifica** > **Avanti** > **Tutti i dispositivi o personalizzato** > **Distribuzione rollout lento** > Per impostazione predefinita, l'opzione **Rollout manuale** è selezionata > Scegliere dal menu a discesa > **% personalizzata di dispositivi nel riepilogo di selezione (rollout lento)** o **Tutti i dispositivi nel riepilogo di selezione**.
3. Fare clic su **Fine**.

Migrazione completa dei dispositivi

Procedura

1. Sul dispositivo, toccare **Continua** quando viene richiesto "Aggiungere il proprio account di lavoro".
2. Verificare l'**ID e-mail aziendale**.
3. Immettere la **password**.
4. Completare l'**autenticazione a due fattori (2FA)**, se disponibile.
5. Completare la procedura di configurazione dell'account.

Verifica migrazione

Sul dispositivo

1. Aprire **Google Play Store**.
2. Confermare che il tipo di account sia cambiato da account di lavoro ad account di dominio aziendale.

Nella console di amministrazione

- Per visualizzare lo stato di configurazione di **Android Enterprise: migrazione dallo stato di configurazione Google Play gestito ad Account Google gestito**, accedere a **Dispositivi** > **Dispositivi** > **Dettagli dispositivi** > **Configurazione** > **Android Enterprise: migrazione dei dispositivi dall'account Google Play gestito a Google gestito)**. Assicurarsi che lo stato di configurazione sia Installato.

Monitoraggio dello stato di migrazione

Gli amministratori possono monitorare l'avanzamento della migrazione (**Migrato all'Account Google gestito**) utilizzando:

- **Dettagli dispositivo** - visualizza lo stato di migrazione per dispositivo
- **Ricerca avanzata** - filtro dispositivi migrati e non migrati
- **Gruppi dispositivo** - raggruppamento di dispositivi migrati e non migrati

Queste opzioni aiutano a identificare i dispositivi che richiedono ulteriori azioni.

Nuova Registrazione con account di dominio Google gestito (BTE)

Android Enterprise può essere configurato utilizzando l'**account di dominio Google gestito** con o senza autenticazione Google.

Procedura

1. Accedere al portale.
2. Andare in **Amministratore** > **Google** > **Android Enterprise**.
3. In **Account Google Play gestito**, fare clic su **Autorizza**.
4. Immettere l'ID e-mail **Corporate** o **Business** e fare clic su **Avanti**.
5. Selezionare **Crea una nuova associazione con...** nella pagina **Seleziona un'opzione di associazione**.
6. Fare clic su **Conferma**. Verranno visualizzate le opzioni **Salta** e **Abilita**.

- **Salta**- Per continuare senza autenticazione
- **Abilita** - Per continuare con l'autenticazione

La sezione Android Enterprise visualizza le seguenti informazioni:

- **Stato**: visualizza lo stato di connessione.

- **E-mail amministratore**: visualizza l'ID e-mail corporate o business.
- **Tipo di azienda**: visualizza il tipo di azienda.
- **Impostazioni di autenticazione Google**: visualizza No/Sì in base ai requisiti di autenticazione.
- **Google Enterprise ID**: visualizza un ID aziendale Google univoco.
- **Nome azienda**: visualizza il nome dell'azienda.

12.6.2. Registrazione di dispositivi Android

Se per completare la registrazione di un dispositivo Android è necessaria l'autorizzazione da parte dell'utente per accedere al codice IMEI, al numero di telefono e ad altri identificatori del telefono, è possibile configurare questa opzione. Se configurata, all'utente del dispositivo verrà chiesto di concedere l'autorizzazione al client di Go per accedere agli identificatori del dispositivo.

> Questa configurazione è valida solo per le nuove registrazioni di tutti i dispositivi Android con Android 6.0 o versioni successive.

1. Selezionare **Amministratore > Google > Registrazione**.
2. Selezionare **Richiedi gli identificatori dei dispositivi Android durante la registrazione (Profilo di lavoro e Amministratore dispositivo)**.
3. Fare clic su **Salva**.

Per ulteriori informazioni sulla modalità Smarrimento, vedere **Gestione dispositivi Android in Modalità smarrimento**.

12.6.3. API di gestione Android

Android Management API (AMAPI) è l'API della piattaforma cloud di Google che integra le funzioni di Google Android UEM in Ivanti Neurons per MDM. Nella configurazione di Android Enterprise, è possibile attivare il framework dell'API di gestione Android per gestire i dispositivi Android Enterprise senza la necessità di installare un'app client sui dispositivi per la loro gestione. Attualmente, Go app non è supportato per il push al dispositivo per altre funzionalità come MTD, ecc.

Quando nella configurazione è impostato un account Android Enterprise, sarà possibile attivare e utilizzare il framework dell'API di gestione Android. Dopo l'attivazione, è possibile:

- Aggiungere un profilo di registrazione per utilizzare il codice QR per la registrazione dei dispositivi.
- Creare una configurazione dispositivo dedicata (monouso di proprietà aziendale, o COSU) per il dispositivo registrato che serva a uno scopo specifico.

L'API di gestione Android attualmente è supportata solo su dispositivi che eseguono Android versione 9 o superiore e che hanno Google Play installato e con provisioning in Modalità dedicata. La modalità Dedicata aziendale è anche indicata come modalità Monouso di proprietà dell'azienda (COSU) ed è una versione della modalità Proprietario del dispositivo. Questa funzione supporta anche le seguenti azioni del dispositivo:

- Blocca
- Riavvia
- Sincronizza su server
- Cancella

I check-in del dispositivo sono previsti a intervalli regolari (ogni ora). Per un intervento immediato, utilizzare l'azione del dispositivo "Sincronizza su server" nella pagina dei dettagli del dispositivo. I dispositivi AMAPI non inviano check-in obbligatori a Ivanti Neurons per MDM. Gli aggiornamenti di inventario vengono eseguiti se e quando viene svolta un'attività sul dispositivo.

Attivazione dell'API di gestione Android

Per abilitare l'API Gestione Android, andare in **Amministratore > Android Enterprise > Autorizza Google (richiede un indirizzo Google valido) > Abilitazione Android Enterprise**.

Lo stato della funzionalità API Gestione Android abilitata (**Sì** per abilitata e **No** per disabilitata) è mostrato anche nella pagina Dettagli dispositivo.

> Gli account GSuite attualmente non sono supportati con COSU.

Aggiunta di un profilo di registrazione

È necessario creare un profilo di registrazione per registrare il dispositivo Android utilizzando la scansione del codice a barre o la stringa alfanumerica del token. I profili di registrazione possono essere creati solo se l'API di gestione Android è abilitata. È inoltre possibile creare attributi dei dispositivi personalizzati da associare al profilo di registrazione.

1. Selezionare **Amministratore > Android Enterprise > Profili di registrazione**.
2. Configurare le seguenti impostazioni nella finestra **Profilo di registrazione - Dispositivo dedicato di proprietà dell'azienda**.
3. Fare clic su **Salva**. La finestra **Riepilogo profilo** mostra i seguenti dettagli del token:

Impostazione	Descrizione
Nome	Immettere un nome identificativo per il profilo di registrazione.
Descrizione	Immettere una descrizione con cui spiegare lo scopo di questo profilo di registrazione.
Nome utente	Inserire le prime lettere di un nome utente valido e selezionarlo dai risultati corrispondenti che vengono visualizzati. Un nome utente valido potrebbe essere un utente locale o un utente LDAP. I profili di registrazione contrassegnano i dispositivi registrati utilizzando il codice QR nel profilo da visualizzare come dispositivo appartenente all'utente per cui è stato creato il profilo di registrazione.
Validità token	Inserire il numero di giorni di validità della scansione del codice QR del token di autenticazione. Il numero inserito deve essere compreso fra 1 e 30. Il dispositivo viene reimpostato se si utilizza il token o il profilo di registrazione dopo il periodo di scadenza.
Attributi dispositivo personalizzati	Nella colonna Azioni, fare clic su **+Aggiungi nuovo** per aggiungere attributi del dispositivo personalizzati da associare al profilo di registrazione. 1. Selezionare l'attributo del dispositivo personalizzato dall'elenco a discesa nella colonna **Nome attributo**. 2. Nella colonna **Valore**, immettere il valore dell'attributo personalizzato. 3. Fare clic su **Salva**. L'attributo del dispositivo personalizzato aggiunto viene visualizzato nella tabella. Per eliminarlo, fare clic su **Elimina** nella colonna Azioni. Gli attributi personalizzati possono essere aggiunti a un profilo di registrazione solo durante la creazione del profilo. I campi attributo non possono essere modificati dopo la creazione del profilo.

- Nome
- Descrizione
- Nome utente
- Data di creazione token
- Data di scadenza token
- Valore del token
- Codice QR
- Attributi dispositivo personalizzati.

> I dispositivi vengono reimpostati se non è possibile acquisire una configurazione corretta per il dispositivo entro un intervallo di tempo di 10 minuti dopo la registrazione. In questi casi, sarebbe necessario registrarsi di nuovo utilizzando il token di registrazione/codice QR

Quando si crea un profilo di registrazione, questo viene indicato nella pagina **Profili di registrazione**. È possibile eseguire una qualsiasi delle seguenti azioni nella colonna **Azioni**.

- Fare clic sull'icona Visualizzazione per visualizzare i dettagli del profilo di registrazione nella finestra Riepilogo profilo. Anche il codice QR viene visualizzato in questa finestra.
- Fare clic sull'icona Modifica per modificare i dettagli del profilo di registrazione.

> È possibile modificare solo la validità del token. Altri attributi non possono essere modificati.

Fare clic sull'icona Elimina per eliminare il profilo di registrazione.

Creazione della configurazione COSU

Gli amministratori possono configurare i dispositivi dedicati che possono essere utilizzati per uno scopo specifico utilizzando Android Enterprise e la configurazione dei dispositivi dedicati (monouso di proprietà dell'azienda o COSU). La configurazione COSU viene distribuita ai dispositivi di lavoro gestiti (modalità Proprietario del dispositivo) per rendere disponibile una sola app per gli utenti in modalità tutto schermo. I dispositivi in modalità Profilo di lavoro su dispositivo di proprietà dell'azienda non sono supportati.

Con questa configurazione, l'amministratore può configurare i dispositivi in modo da bloccare l'app sullo schermo così che l'utente in modalità tutto schermo non possa sbloccarla e uscirne per passare ad altre schermate del dispositivo o utilizzare qualsiasi altra app sul dispositivo.

> Può essere inoltre forzata l'installazione di altre app sul dispositivo AMA selezionando l'opzione "Installa sul dispositivo" in Opzioni avanzate e Configurazione app, tuttavia l'utente non sarà in grado di interagire con tali app mentre l'app tutto schermo è bloccata sullo schermo tramite la configurazione. Per tutto schermo multi-app, si consiglia di utilizzare la funzionalità tutto schermo del dispositivo di lavoro gestito (modalità Proprietario del dispositivo). Ciò consente un maggior controllo sulle app e sulle impostazioni del dispositivo e può essere esteso a una modalità multi-utente.

Gli amministratori possono apportare modifiche alla configurazione, come ad esempio consentire la navigazione di sistema e la possibilità di utilizzare altre app inviate al dispositivo per l'utente finale tramite Google DPC, esaminando le varie opzioni in base alle esigenze.

Le configurazioni COSU sono determinate dalla priorità loro assegnata. La configurazione con la massima priorità viene utilizzata nell'invio della configurazione delle policy a Google. Le configurazioni COSU vengono applicate ai dispositivi all'interno dello spazio definito. Possono essere delegate ad altri spazi, se definite nello spazio predefinito.

Per configurare:

1. Andare a **Configurazione > +Aggiungi**.
2. Nella **configurazione Blocco e tutto schermo: Android Enterprise**, fare clic su **Dispositivi dedicati (monouso di proprietà dell'azienda o COSU)**.
3. Immettere un nome per la configurazione.
4. Immettere una descrizione.
5. È possibile configurare le seguenti impostazioni facendo clic sulle schede pertinenti:

- **Impostazioni app**
- **Blocchi generali**
- **Personalizzazione tutto schermo**
- **Impostazioni di sistema**

La seguente tabella fornisce i dettagli dei campi configurabili:

Impostazione	Descrizione
Impostazione app **Nome app** **Blocchi generali**	Selezionare l'app da bloccare sul dispositivo digitando il nome dell'app (digitare la lettera iniziale del nome dell'app finché non compare l'app desiderata nel menu a discesa). Se l'app non viene visualizzata nel menu a discesa, assicurarsi che l'app che si desidera distribuire sia un'app privata/pubblica disponibile nel Play Store e sia aggiunta ad App Catalog. Questo campo è obbligatorio. Non sarà permesso creare la configurazione se non si seleziona un'app da aggiungere in questo campo. È possibile aggiungere solo app pubbliche e private. Non è possibile aggiungere app interne e Web (private).
Tieni attivo display **Personalizzazione tutto schermo**	Configurare le modalità di collegamento batteria per l'alimentazione del dispositivo. Selezionare una delle seguenti opzioni: • **AC** - La fonte di alimentazione è un caricabatterie AC • **Wireless** • **USB** - La fonte di alimentazione è una porta USB • **Qualunque** - La fonte di alimentazione è un caricabatterie AC, una porta USB o un caricabatterie wireless.
Personalizza barra di stato	Selezionare una delle seguenti opzioni per personalizzare la barra di stato sui dispositivi di destinazione: • **Notifiche e informazioni di sistema attivate** - Per mostrare le informazioni di sistema e le notifiche sulla barra di stato. • **Solo informazioni di sistema attivate** - Per visualizzare solo le informazioni di sistema sulla barra di stato.
Personalizza navigazione di sistema **Attiva azioni globali**	Selezionare una delle seguenti opzioni per specificare l'accesso alle funzioni di navigazione (Home, e pulsanti Panoramica) in modalità tutto schermo: • **Attivato** - Consente la navigazione dei pulsanti Home e Panoramica. Gli utenti possono uscire dall'app specificata se questa opzione è selezionata. • **Disattivato** - Disabilita la navigazione dei pulsanti Home e Panoramica. • **Solo pulsante Home** - Consente solo la navigazione del pulsante Home. Il pulsante Indietro è disponibile con tutte queste opzioni. Selezionare per consentire le azioni globali in modalità tutto schermo. Le funzionalità di riavvio e arresto associate ai pulsanti di accensione sono controllate tramite questa opzione.
Attiva finestre di dialogo per errori di sistema	Selezionare per consentire le finestre di dialogo per le app che restituiscono un errore o non rispondono in modalità tutto schermo.

Impostazione	Descrizione
Impostazioni di sistema **Impostazioni aggiornamenti del sistema**	Configurare le seguenti impostazioni per gestire gli aggiornamenti di sistema: • **Aggiornamento del sistema** - Per selezionare il tipo di aggiornamento di sistema richiesto. ◦ **Automatico** - Installa automaticamente non appena è disponibile un aggiornamento. ◦ **Posticipa** - Per posticipare l'installazione automatica per un massimo di 30 giorni. ◦ **Con finestra** - Per installare automaticamente all'interno di una finestra di manutenzione quotidiana. Impostare le ore di inizio e di fine per il periodo della finestra di manutenzione. Gli aggiornamenti installati sui dispositivi potrebbero variare in base al set di funzionalità supportato, alla versione di Android e alla versione di Google DPC installati sul dispositivo. • **Periodo di blocco** - Quando un dispositivo si trova all'interno del periodo di blocco, tutti gli aggiornamenti di sistema in arrivo sono bloccati e non vengono installati. Fare clic su **Aggiungi periodo di blocco** per impostare la **Data d'inizio** e la **Data di fine** del periodo di blocco. Quando un dispositivo è al di fuori del periodo di blocco, viene applicato il comportamento di aggiornamento normale. Se la data di fine è prima della data d'inizio, allora il periodo di blocco si estende tra l'anno corrente e quello successivo. Il periodo di blocco può essere impostato per un massimo di 90 giorni. Due periodi di blocco consecutivi devono essere separati da un minimo di 60 giorni.

6. Fare clic su **Avanti**.
7. Selezionare una delle seguenti opzioni di distribuzione:

- **Tutti i dispositivi**
- **Nessun dispositivo** (impostazione predefinita)
- **Personalizzato**

8. Fare clic su **Fine**.

Gestione delle app su dispositivi AMAPI

Quando la configurazione COSU viene distribuita nei dispositivi, le app vengono inviate e bloccate sullo schermo sul dispositivo AMA. Indipendentemente dall'invio della configurazione COSU al dispositivo, le app installate sul dispositivo AMA possono ancora essere gestite. Di seguito sono riportati i dettagli sulla gestione delle app su questi dispositivi:

- Sono supportate solo le app pubbliche e private; le app interne e le clip Web non sono supportate.
- Le app vengono inviate solo se nelle impostazioni di installazione sono attivate le opzioni "Installa sul dispositivo" o "Installazione invisibile". Le app assegnate all'utente/dispositivo senza una di queste opzioni abilitate non saranno visibili sul dispositivo o nel Play Store del dispositivo per qualsiasi azione da parte dell'utente.
- Le configurazioni delle app supportate sono Google Play gestito e Impostazioni dispositivo di lavoro gestito (Android for Work). Sono supportate le configurazioni gestite per le app, compreso il supporto della configurazione gestita per le app OEMConfig.

> Il tempo per il completamento dell'installazione e della disinstallazione delle configurazioni potrebbe variare in base alle notifiche di Google (servizio di messaggistica) sull'esecuzione dell'azione desiderata.

- Go app verrà ora installato per impostazione predefinita come parte della registrazione del dispositivo AMA. Durante la procedura di registrazione, l'app verrà bloccata a schermo e, una volta completata la configurazione, verrà eseguita in background.

> Le policy, fatta eccezione per l'applicazione del requisito di registrazione del dispositivo in base al produttore, la versione del sistema operativo e il livello delle patch di sicurezza non sono supportati. L'elenco dei dispositivi consentiti che permette solo ai dispositivi ammessi di registrarsi con Ivanti Neurons per MDM è supportato.

Gestione del supporto feedback app su dispositivi AMAPI

Il supporto feedback app può essere gestito su dispositivi AMAPI (COSU). Quando un dispositivo viene registrato in modalità AMAPI (COSU), la configurazione app gestita verrà inviata a Ivanti Neurons per MDM direttamente da Google senza alcun intervento da parte di Go app. Le informazioni di Feedback app gestite possono essere visualizzate a livello di dispositivo da **Dettagli dispositivo > App installate > Visualizza feedback**, oppure possono essere visualizzate a livello di singola app navigando alla specifica app Android nel Catalogo app sotto la scheda "Feedback configurazione app" per il report complessivo su tutti i dispositivi. Per informazioni sul meccanismo di feedback app, vedere **Sincronizzazione e recupero del feedback per un'app**.

Limitazioni AMAPI

Attualmente, AMAPI presenta i seguenti limiti:

- Sono supportati solo i dispositivi dedicati (modalità COSU).

Configurazioni supportate

Le configurazioni seguenti sono supportate per AMAPI:

- Distribuzione app (app singole o multiple)
- Configurazione di app gestite per app inviate al dispositivo
- Configurazione Wi-Fi
- Configurazione (COSU) Dedicata/Blocco Android Enterprise
- Configurazione VPN Always-on

12.6.4. API Google App

È possibile che i clienti Google che utilizzano il servizio Single Sign-On (SSO) per autenticare l'accesso utente ai servizi Google Apps non riescano a utilizzare Exchange per connettere gli utenti a e-mail, contatti e calendario, a causa di limitazioni nel protocollo che impediscono ai dispositivi di supportare reindirizzamenti ai servizi di autenticazione esterni attivati dal servizio SSO. Questo servizio indirizza questa condizione tramite la creazione e la gestione di password account per la connettività ActiveSync.

Prerequisiti

Prima di provare a configurare la funzionalità API Google App, è necessario:

- Accedere con diritti di amministratore a un account su https://console.developers.google.com/.
- Accedere con diritti di amministratore a un account su https://admin.google.com.

Attivazione della funzionalità API Google App

Procedura

1. Selezionare **Amministratore > Google > API Google App**.
2. Fare clic su **Passaggio 1: Google Dev** in fondo al rettangolo con etichetta numero 1 a sinistra.
3. Passaggio 1: viene visualizzata la pagina Dispositivo Google.
   Seguire le istruzioni visualizzate al passaggio 1: pagina Dispositivo Google, quindi fare clic su **Fine**.
4. Fare clic su **Passaggio 2: Amministratore Google** in fondo al rettangolo centrale con etichetta numero 2.
5. Passaggio 2: viene visualizzata la pagina Amministratore Google.
   Seguire le istruzioni visualizzate al passaggio 2: pagina Amministratore Google, quindi fare clic su **Fine**.
6. Immettere il nome utente dell'amministratore Google nel campo **Immetti nome utente dell'amministratore Google** nel rettangolo con etichetta numero 3 a destra.
7. Nello stesso rettangolo, fare clic su **Scegli file** per caricare il file JSON scaricato al passaggio 1.
8. Fare clic su **Salva**.
9. Se non è possibile visualizzare la pagina API di Google Apps, probabilmente non si dispone delle autorizzazioni necessarie. È necessario disporre di uno dei **ruoli** seguenti:
   - Gestione sistemi
   - Sistema di sola lettura

12.6.5. Amministratore - Android Enterprise

Licenza: Silver

- Le app di produttività basate su Ivanti, Inc Android Enterprise come Email+, Docs@Work e Web@Work richiedono la licenza Gold.
- Tunnel per Android Enterprise richiede la licenza Platinum.

Android Enterprise permette l'uso e la configurazione delle app Android Enterprise. Gli utenti di Android Enterprise possono visualizzare e installare app dal catalogo app e tramite Google Play.

Se si è un nuovo cliente, la distribuzione delle app è impostata per dispositivo per impostazione predefinita. Non è possibile modificare questa impostazione. I clienti che eseguono un aggiornamento hanno la possibilità di scegliere tra la distribuzione delle app per utente, che è selezionata per impostazione predefinita, o per dispositivo. Molti utenti hanno più dispositivi. Se un utente dispone di più dispositivi, quando la distribuzione delle app è impostata per dispositivo, è possibile rendere disponibile un insieme diverso di app su ciascun dispositivo.

Argomenti della sezione:

- Configurazione di Android Enterprise
- Configurazione del Profilo di lavoro di Android Enterprise

Configurazione di Android Enterprise

1. Nel portale Ivanti Neurons for MDM, fare clic su **Amministratore > Google > Android Enterprise**.
2. Selezionare una delle seguenti opzioni:
    - **Account Google Play gestito:** per le imprese prive di una sottoscrizione a G Suite, questo metodo permette di iscrivere gli utenti ad Android Enterprise senza inviare alcuna informazione personale (indirizzi e-mail a Google). Ivanti Neurons for MDM esegue il provisioning e gestisce automaticamente gli utenti con Google. All'utente viene chiesto di autorizzare Android Enterprise utilizzando un account amministratore Google.
    - **Account Google gestito:** per le imprese con una sottoscrizione a G Suite, questo metodo permette agli utenti di iscriversi ad Android Enterprise con i loro account Google. Ogni utente deve avere un account Google per iscriversi ad Android Enterprise.

Per completare la procedura di configurazione, seguire le indicazioni riportate sullo schermo:

4. Nel caso del metodo automatico, la procedura include le seguenti operazioni:
    - Abilitazione dell'API UEM e creazione delle credenziali aziendali.
    - Registrazione in Google mediante l'autorizzazione del proprietario dell'integrazione. Deve essere utilizzato un account IT anziché un account personale.
    - Impostazione delle credenziali mediante il trascinamento dell'ID client JSON dell'account del servizio.

Nel caso del metodo alternativo, la procedura include le seguenti operazioni:

- Fare riferimento all'ID CLIENT nella sezione sottostante e aggiungerlo a Google Admin.
- Cercare il proprio token MDM in Google Admin e l'account del servizio nella Google Cloud Console.
- In Ivanti Neurons for MDM, inserire il proprio token MDM, il dominio Google aziendale e l'indirizzo e-mail di Enterprise Admin per connettersi al servizio Google.
- In Ivanti Neurons for MDM, trascinare e rilasciare il proprio ID client Service Account JSON.

- In Ivanti Neurons for MDM, autorizzare Ivanti Neurons for MDM a visualizzare e/o gestire i propri Utenti Google facendo clic su **Autorizza**.

L'interfaccia utente di Ivanti Neurons for MDM guida l'utente in tutti questi passaggi.

CLIENT ID per associare Ivanti Neurons for MDM all'Account Google gestito

Aggiungere l'id client come **140561810807-tiiglke17laibbrt5darupmvo4ae7cbj.apps.googleusercontent.com** nell'Admin Console per associare il tenant Ivanti Neurons for MDM all'account Google gestito.

Configurazione del Profilo di lavoro di Android Enterprise

1. Nel portale Ivanti Neurons for MDM, passare a **Configurazioni**.
2. Fare clic su **+Aggiungi**.
3. Selezionare la configurazione **Blocco e tutto schermo: Android Enterprise**.
4. Immettere un nome e una descrizione della configurazione.
5. Fare clic sul tipo di blocco **Profilo di lavoro**.
   Selezionare le **impostazioni di blocco** che si desidera applicare ai dispositivi di destinazione.
   Importante: quando un utente aggiunge un account Google con l'opzione Aggiungi account in Impostazioni, il server di autenticazione Google verifica se il dominio dell'account è registrato come dominio gestito da UEM. Verificare che la casella di controllo **Imponi policy UEM sui dispositivi Android** sia selezionata. Se è selezionata, il client Go viene automaticamente installato o aggiornato (se non è già installato nel dispositivo) e avviato. Una volta che l'utente completa il processo di registrazione, gli viene chiesto di creare un profilo di lavoro, al quale viene automaticamente eseguita la migrazione dell'account Google.

12.7. Lavorare con i dispositivi ChromeOS

Argomenti della sezione:

- ChromeOS e Ivanti Neurons per MDM
- Distribuire applicazioni Android su dispositivi ChromeOS
- Configurazione del Progetto ChromeOS
- Azioni relative ai dispositivi
- Domande frequenti
- Passi consigliati per la valutazione

12.7.1. ChromeOS e Ivanti Neurons per MDM

ChromeOS è un sistema operativo basato su Linux creato e distribuito da Google. Ivanti Neurons per MDM supporta dispositivi funzionanti su Android, Windows, iOS e macOS. Questo supporto è stato ora esteso anche ai dispositivi ChromeOS.
Ivanti Neurons per MDM fornisce una soluzione unificata e semplice di gestione della mobilità per configurare e gestire i dispositivi ChromeOS. Ivanti offre una soluzione unificata, semplice e ricca di funzionalità per i dispositivi ChromeOS, simile ai flussi di lavoro di amministrazione disponibili per iOS, Android, Windows e Mac su Ivanti Neurons per MDM. L'amministratore può semplicemente connettersi a Ivanti Neurons per MDM con il proprio Google Cloud (chiamato anche console Google Admin) utilizzando una semplice integrazione da **Amministratore > Google > Gestione ChromeOS**.

Prerequisiti

1. Deve avere un account Google Admin gestito.
2. Gli utenti e le UO LDAP devono essere importati nella console Google Admin. Ivanti Neurons per MDM supporta solo le UO importate da un'origine LDAP. Le UO locali non sono supportate.
3. L'amministratore deve aver sincronizzato le unità organizzative (gruppi di utenti) in Ivanti Neurons for MDM. Ciò può avvenire configurando il server LDAP e aggiungendo le unità organizzative.

Autorizzazione di Google

I dispositivi ChromeOS disponibili sulla console Google Admin non possono essere registrati direttamente su Ivanti Neurons for MDM. Questi dispositivi sono invece registrati presso Google e le informazioni su di essi vengono sincronizzate tra Google e Ivanti Neurons per MDM. L'amministratore deve autorizzare Google a importare i dispositivi e a eseguire altre azioni come l'assegnazione di app, configurazioni, ecc.

Procedura

1. Accedere a **Amministratore → Google > Gestione ChromeOS**.
2. Fare clic su **Autorizza Google**.
3. Selezionare l'account Google Admin che si desidera autorizzare.
4. Fare clic su **Continua** per accettare le autorizzazioni a fornire i servizi richiesti.
   Sullo schermo viene visualizzata la conferma **ChromeOS è stato configurato con successo**. Le informazioni sul dominio si trovano anche sotto la conferma.

Sincronizzazione dei dispositivi ChromeOS da Google

L'amministratore deve sincronizzare i dispositivi ChromeOS dalla console Google Admin. Quando si utilizza la console Google Admin per accedere ai dispositivi ChromeOS per la prima volta, l'amministratore deve sincronizzare manualmente i dispositivi utilizzando l'opzione Sincronizza ora dalla pagina Gestione ChromeOS.

> Dopo aver sincronizzato manualmente i dispositivi per la prima volta, le successive sincronizzazioni avverranno automaticamente su base oraria.

Eliminazione dell'integrazione di Google Admin Console con Ivanti Neurons per MDM

L'eliminazione dell'integrazione revoca il token OAuth ricevuto da Google per accedere alle risorse di Google. Elimina i dispositivi ChromeOS, l'inventario associato alla configurazione Blueprint e alla configurazione app e i metadati di registrazione. La

configurazione Blueprint e le app caricate non vengono eliminate.

Se la registrazione del tenant non viene eliminata, sarà possibile creare un ticket per verificare il problema.

Procedura

1. Accedere a **Amministratore → Google > Gestione ChromeOS**.
2. Nella sezione Registrazione Ivanti Neurons per MDM ChromeOS, fare clic su **Elimina**.
   A schermo apparirà un pop-up che indica se si desidera procedere con l'operazione di eliminazione, dopodiché tutti i dispositivi associati a questa integrazione verranno eliminati. Selezionare **Ok**.

12.7.2. Distribuire applicazioni Android su dispositivi ChromeOS

L'amministratore può distribuire applicazioni Android dal Catalogo app ai dispositivi ChromeOS.

Prerequisiti

1. Android Enterprise deve essere configurato. Per informazioni sulla configurazione di Android Enterprise, vedere **Configurazione di Android Enterprise**.
2. Le app Android devono essere presenti nel Catalogo app.
3. Assicurarsi che l'utente del dispositivo ChromeOS (Chromebook) faccia parte di un gruppo di utenti (indicato anche come unità organizzativa) prima di distribuire le app Android e la configurazione del Progetto ChromeOS.

Una volta identificata l'app Android, è necessario distribuirla seguendo il processo analogo a quello seguito per la distribuzione di qualsiasi altra app. Quando si distribuisce l'app Android, assicurarsi di selezionare i gruppi di utenti a cui si desidera distribuire l'app ed eseguire un'installazione invisibile all'utente sul dispositivo.

> Se la distribuzione dell'app Android esistente è impostata per essere distribuita a dispositivi/gruppi di dispositivi o utenti, è necessario modificare la distribuzione in base ai gruppi di utenti. Questo può avere un impatto sulle distribuzioni esistenti se l'app è già in uso. Si consiglia di eseguire questa operazione prima su un'app completamente nuova.

> Impostazioni di installazione consente agli amministratori di controllare l'installazione invisibile all'utente finale ed è necessario per eseguire il push dell'app ai dispositivi ChromeOS. I gruppi di utenti devono essere selezionati qui.

12.7.3. Aggiungere e distribuire app di estensione per ChromeOS

L'amministratore può aggiungere app di estensione ChromeOS al Catalogo app e distribuirle ai dispositivi ChromeOS.

Procedura

1. Andare in **App** > **Catalogo app**.
2. Fare clic su **+ Aggiungi**.
3. Selezionare **ChromeOS** dall'elenco. Sullo schermo appare la pagina **Aggiungi dettagli app ChromeOS**.
4. Fornire i seguenti dettagli: **Nome app** - Nome app di estensione per ChromeOS, **ID estensione** - È possibile ottenere queste informazioni dal Chrome web store.
5. Fare clic su **Avanti**. Sullo schermo appare la pagina **Configurazioni app**. Sarà possibile selezionare un aggiornamento immediato che verrà eseguito al successivo check-in del dispositivo, oppure è possibile scegliere di aggiornare l'app automaticamente quando nuove versioni diventano disponibili.
6. Selezionare una delle opzioni di distribuzione dell'app e fornire i dettagli richiesti.

> La distribuzione dell'app ChromeOS è supportata solo per i gruppi di utenti LDAP.

Una volta identificata l'app di estensione ChromeOS, è necessario distribuirla seguendo il processo analogo a quello seguito per la distribuzione di qualsiasi altra app. Quando si distribuisce l'app di estensione ChromeOS, assicurarsi di selezionare i gruppi di utenti a cui si desidera distribuire l'app ed eseguire un'installazione invisibile all'utente sul dispositivo.

> Impostazioni di installazione consente agli amministratori di controllare l'installazione invisibile all'utente finale ed è necessario per eseguire il push dell'app ai dispositivi ChromeOS. I gruppi di utenti devono essere selezionati qui.

È possibile modificare le informazioni relative a un'app di estensione ChromeOS o eliminare un'app di estensione ChromeOS dal Catalogo app. È necessario seguire la stessa procedura che si segue per modificare o eliminare qualsiasi altra app dal Catalogo app.

Modifica di un'app di estensione ChromeOS

1. Andare in **App > Catalogo app > Dettagli**.
2. Fare clic su **Modifica**. Apportare le modifiche desiderate e fare clic su **Salva**.

Per informazioni sull'eliminazione di un'app, vedere **Eliminazione di app dal Catalogo app**.

12.7.4. Configurazione del Progetto ChromeOS

La configurazione del Progetto ChromeOS presenta le seguenti impostazioni:

- Impostazioni dispositivo
- Impostazioni utente e browser
- Impostazioni della sessione guest gestita

È possibile applicare la configurazione di ChromeOS a gruppi di utenti specifici (detti anche Unità Organizzative). Quando si cerca di distribuire la configurazione del Progetto ChromeOS, sarà disponibile solo la sezione Gruppi di utenti e tutti i gruppi di utenti LDAP che sono associati alla console Google Admin autorizzata saranno elencati in questa sezione. È possibile selezionare uno o più gruppi tra quelli elencati e applicare la configurazione.

Procedura

1. Andare in **Configurazioni > Aggiungi**.
2. Selezionare **Google ChromeOS** nella sezione OS. Sullo schermo viene visualizzata la scheda **Configurazione del Progetto ChromeOS**.
3. Fare clic su **Progetto ChromeOS**. Sullo schermo viene visualizzata la pagina **Crea configurazione Progetto ChromeOS**.
4. Immettere un nome per la configurazione nella casella **Nome**.
5. In Impostazione configurazione, è possibile modificare le impostazioni del dispositivo, le impostazioni dell'utente e del browser e le impostazioni della sessione guest gestita, secondo le necessità, e attivare il pulsante "Esegui push al dispositivo" per applicare le impostazioni modificate.
6. Fare clic su **Avanti**.
7. Selezionare **Personalizzato** per le opzioni di distribuzione.

> Solo i gruppi di utenti LDAP saranno disponibili per distribuire la configurazione.

> Nel caso in cui si voglia distribuire la configurazione a tutti, è possibile farlo solo per i gruppi di utenti LDAP disponibili in Ivanti Neurons per MDM e nella console Google Admin.

Selezionare uno o più gruppi e fare clic su **Fine**.

> Quando viene annullata la distribuzione per le impostazioni distribuite, le impostazioni applicate non vengono ripristinate.

> È possibile caricare i file nella Configurazione Blueprint ChromeOS.

12.7.5. Azioni relative ai dispositivi

Le seguenti azioni sono supportate sui dispositivi ChromeOS:

- **Cancella** - L'azione Cancella elimina tutti i dati da un dispositivo e il dispositivo viene riportato alle impostazioni di fabbrica. Per ulteriori informazioni, vedere **Cancellazione di un dispositivo**.
- **Blocca** - L'azione Blocca limita l'esecuzione di qualsiasi altra azione sul dispositivo. Per ulteriori informazioni, vedere **Blocco di un dispositivo**.
- **Sblocca** - L'azione Sblocca libera il dispositivo per un ulteriore utilizzo. Per ulteriori informazioni, vedere **Cancellazione di un dispositivo**.

12.7.6. Domande frequenti

Questa sezione elenca alcune delle domande più comuni che si possono avere quando si utilizzano i dispositivi ChromeOS su Ivanti Neurons per MDM.

- In che modo la gestione Chromebook è diversa da quella degli altri sistemi operativi?
- Google consente solo la distribuzione di configurazioni basate su gruppi di utenti LDAP e l'amministratore deve assicurarsi che quando lavora con configurazioni o app, la distribuzione sia basata su gruppi di utenti LDAP. I gruppi di utenti locali e i gruppi di dispositivi non sono supportati per la gestione dei dispositivi ChromeOS.
  Di quali licenze ho bisogno per gestire i dispositivi ChromeOS con Ivanti?
- I dispositivi ChromeOS devono avere licenze come Chrome Enterprise Upgrade o Chrome Education Upgrade. Possono essere acquistate dai rivenditori come parte dell'hardware o come licenze indipendenti. Per ulteriori informazioni, consultare la documentazione di Google. Per iniziare a gestire i dispositivi Chrome, è necessaria la licenza Secure UEM (Unified Endpoint Management) con Ivanti.
  Sarà disponibile Mobile Threat Defense (MTD) o una soluzione simile? Ho bisogno di una licenza separata per MTD?
- Questa funzione non è attualmente disponibile nel prodotto; fare riferimento alle limitazioni attuali. Forniremo maggiori informazioni sulle modifiche apportate alle funzionalità tramite le FAQ e gli annunci di rilascio.
  Perché la scheda configurazioni e app non contiene dettagli come per gli altri dispositivi?
- Poiché le configurazioni sono distribuite ai gruppi di utenti e non vengono applicate in base all'utente connesso, al momento le configurazioni non vengono mostrate nei dettagli del dispositivo. Le app seguono la stessa logica di distribuzione e hanno le stesse limitazioni. Forniremo maggiori informazioni sulle modifiche apportate con tali limitazioni tramite le FAQ e gli annunci di rilascio.
  Quante configurazioni sono attualmente supportate per ChromeOS?
- Con ChromeOS, abbiamo ridotto il numero di riquadri di configurazione disponibili e le attività di amministrazione associate alla configurazione. Ci riferiamo a questa configurazione come "Progetto ChromeOS". Progetto ChromeOS supporta quasi 700 configurazioni su questi dispositivi. Per le opzioni di configurazione, consultare la documentazione di Google.
  Come è possibile gestire facilmente una configurazione per tutti i dispositivi?
- Gli amministratori possono semplicemente clonare una configurazione esistente e modificarla (se necessario) per i rispettivi gruppi di utenti. Non è necessario partire da zero.
  Come si aggiunge la configurazione VPN ai dispositivi Chrome?
- Ciò può avvenire utilizzando le applicazioni Android e non utilizzando la VPN nativa.
  Le azioni del dispositivo, come il ritiro e la cancellazione, funzionano su questi dispositivi?
- I Chromebook in ambito aziendale sono sempre gestiti da un'organizzazione e i dati su tale dispositivo sono considerati completamente organizzativi. Tenendo presente questo aspetto:
  - Il ritiro è bloccato
  - La cancellazione è consentita
  - Il blocco è consentito
  - Lo sblocco è consentito
  - Altre azioni - non sono supportate

Quali Chromebook, in termini di hardware, sono supportati da Ivanti?

- I dispositivi supportati dalle soluzioni di gestione dei dispositivi di Google Cloud dovrebbero essere intrinsecamente supportati da Ivanti. Attualmente Ivanti non pubblica un elenco di hardware specifici supportati dalla soluzione Ivanti.

Quale versione di Chrome OS è supportata?

- Google Cloud supporta solo l'ultima versione stabile di ChromeOS e il supporto di Ivanti segue il modello supportato da Google a causa della natura delle integrazioni di backend.
  È possibile elencare le limitazioni attuali, visto che si tratta del primo lancio di questa funzionalità?

Con il nuovo supporto per Chrome OS, stiamo lavorando duramente per fornire le funzionalità che i nostri clienti attendono con ansia. Di seguito sono riportate alcune limitazioni di cui gli amministratori dovrebbero tenere conto:

- Le estensioni di Chrome OS (applicazioni del browser) non sono attualmente supportate (come "app") per la distribuzione.
- La configurazione gestita delle app per le applicazioni Android non è attualmente supportata.
- L'API di configurazione Wi-Fi è stata rilasciata di recente e non è attualmente supportata.
- La distribuzione dei certificati non è attualmente supportata.
- La distribuzione dell'app Android Ivanti Go (precedentemente nota come MobileIron Go) non è attualmente supportata.
- L'app Ivanti Tunnel (VPN) non è attualmente supportata.
- Gli spazi e la delega degli spazi non sono attualmente supportati.
- La soluzione Mobile Threat Defense non è attualmente supportata.
- La soluzione Zero Sign-on di Ivanti è supportata su questi dispositivi, classificati come dispositivi non gestiti.
- Le azioni associate ai criteri non sono pienamente supportate.

12.7.7. Passi consigliati per la valutazione

Per convalidare una soluzione, si consiglia di seguire le seguenti fasi:

1. Creare una UO (gruppo di utenti) separata con un utente di prova nell'origine della directory (ad esempio, Active Directory). In questo modo si eviterà l'impatto sulle Unità Organizzative attive.
2. Sincronizzazione degli utenti tra Ivanti, Google e la fonte della directory (LDAP). Verificare che la "UO di prova" sia disponibile nei Gruppi di utenti.
3. Integrare Ivanti Neurons for MDM con Google come evidenziato nei passaggi precedenti.
4. Creare la configurazione di Progetto ChromeOS e distribuirla solo al gruppo di utenti "test UO".
5. Avviare un Chromebook (nuovo o precedentemente registrato). Assicurarsi che sia disponibile nell'elenco dei dispositivi.
6. Verificare che le impostazioni del Progetto ChromeOS siano disponibili sul dispositivo.
7. Seguire una procedura simile per la distribuzione delle app Android.

12.8. Gestione firmware

Argomenti della sezione:

- Registrazione al servizio OTA Zebra
- Gestione licenze Samsung E-FOTA (dismesso)

12.8.1. Registrazione al servizio OTA Zebra

Dopo la registrazione al servizio OTA (Over The Air) Zebra, è possibile abilitare la configurazione OTA Zebra per ricevere e aggiornare i dettagli del firmware dei dispositivi Zebra registrati in Ivanti Neurons for MDM.

Procedura

1. Accedere ad **Amministratore > Infrastruttura > Zebra OTA**. Viene visualizzata la pagina **Servizio Zebra OTA**.
2. Sotto **Link al servizio OTA di Zebra**, fare clic su **Inizia**.
3. Immettere le credenziali OTA Zebra per effettuare l'accesso e seguire la procedura per richiedere l'approvazione all'utilizzo dei servizi Zebra.
4. Fare clic su **Completa verifica** per richiedere la conferma della connessione al servizio Zebra. Una volta confermata la connessione, lo stato della registrazione viene visualizzato nella pagina Servizio OTA Zebra.

Per revocare la registrazione, fare clic su **Revoca** nella colonna **Azioni**. L'azione **Revoca** rimuove tutte le configurazioni OTA di Zebra dalle configurazioni esistenti. Per registrarsi nuovamente al servizio OTA Zebra, fare clic su **Aggiorna**. L'azione di aggiornamento non ha alcun impatto sulle configurazioni esistenti.

Dopo la registrazione è possibile abilitare la configurazione del firmware Zebra che il client Go riceve e applica ai dispositivi Zebra (che eseguono Android 8.0 o una versione successiva supportata) in modalità Proprietario del dispositivo. Quando viene applicata la configurazione, il firmware viene scaricato e installato sui dispositivi, come pianificato nella configurazione. Per ulteriori informazioni sull'abilitazione della configurazione del firmware Zebra, consultare la sezione **Configurazione degli aggiornamenti del sistema**.

Al completamento dell'aggiornamento firmware, è possibile visualizzare lo stato dell'aggiornamento sul dispositivo Zebra nella colonna **Aggiornamento sistema** della pagina Dispositivi. Possono essere visualizzati gli stati seguenti:

- **Sconosciuto** - Non supportato dal client o dal sistema operativo
- **Aggiornato** - Nel dispositivo è installato l'ultimo aggiornamento disponibile
- **In sospeso** - La configurazione degli aggiornamenti del sistema è stata applicata ma l'aggiornamento non è stato scaricato o applicato
- **Download** - È in corso il download dell'aggiornamento del sistema nel client
- **Disponibile** - L'aggiornamento del sistema è attualmente disponibile per il dispositivo
- **Errore** - Errore durante il download o l'installazione.

Le informazioni relative alla patch Zebra sul dispositivo sono visualizzate nella colonna **Versione patch Zebra** della pagina Dispositivi.

> La versione **Zebra Patch** non è supportata per i dispositivi con Android 11 e successivi; è supportata solo la versione **Upgrade completo Zebra**.

12.8.2. Gestione licenze Samsung E-FOTA (dismesso)

Il servizio Samsung E-FOTA verrà dismesso nel luglio 2022. Per ulteriori informazioni, vedere l'annuncio Samsung.

> Impossibile configurare il servizio Samsung E-FOTA da ora. Tuttavia, in caso di configurazione E-FOTA esistente, sarà possibile disattivare la configurazione navigando in **Amministratore** > **Gestione firmware** > **Samsung E-FOTA** e facendo clic sull'opzione **Disattiva**.

12.9. Gestisci script e file

Gli amministratori possono gestire gli script e i file utilizzabili in Configurazioni e inviati ai dispositivi.

Argomenti della sezione:

Tutti gli script

File

12.9.1. Tutti gli script

Applicabile a: dispositivi macOS e Windows

Nella pagina **Amministratore > Script e file > Tutti gli script**, Ivanti Neurons per MDM consente agli utenti con ruolo Gestione sistemi di creare o caricare e gestire script utilizzabili nelle configurazioni e distribuiti ai dispositivi. È possibile associare attributi personalizzati agli script e assegnare i valori risultanti ai dispositivi configurati. Utilizzare Audit Trail per visualizzare i registri delle modifiche allo script e la pagina Dettagli dispositivo per visualizzare i risultati dell'esecuzione.

È possibile creare uno script che configura qualunque impostazione sui dispositivi. Ad esempio, è possibile eseguire script che:

- imporre agli utenti del dispositivo di cambiare la password mensilmente,
- bloccare lo schermo dopo 5 minuti di inattività o
- configurare una rete WiFi protetta.

Argomenti della sezione:

- Aggiunta di uno script
- Modifica di uno script
- Utilizzo di variabili script (applicabili a Windows e macOS)
- Test di script
- Verifica dei risultati dell'esecuzione di uno script

Aggiunta di uno script

È possibile creare o caricare un repository di script bash (per macOS) e script ps1 (per Windows). Tale repository può essere utilizzato in una configurazione per selezionare uno script e distribuirlo per l'esecuzione sui dispositivi in base alla pianificazione specificata nella configurazione.

Ad esempio, è possibile creare uno script della shell da eseguire nei dispositivi. Se necessario, è possibile utilizzare wrapper. L'esecuzione di file binari dall'interno di uno script della shell non è supportata.

> Ivanti raccomanda vivamente di testare gli script della shell prima di eseguirli sui dispositivi, per verificarne la qualità e l'affidabilità. Eseguire lo script localmente e correggere eventuali errori che risultano.

Procedura

1. Andare in **Amministratore > Script > Tutti gli script**.
2. Fare clic su **+ Aggiungi**.
3. Immettere un nome e una descrizione per lo script.
4. Sotto Tipo di piattaforma, selezionare macOS o Windows.
5. Selezionare uno degli **Script Type** seguenti:
    - **bash**
    - **zsh**
    - **python**
    - **swift**

- **ps1**

6. Selezionare la casella di controllo **Esegui come utente root** per eseguire lo script come utente root sui dispositivi. Per impostazione predefinita, questa opzione è cancellata.
7. Nell'**Editor script** è possibile digitare, trascinare o copiare e incollare uno script nella casella di testo.
8. In alternativa, fare clic su **Importa codice da uno script** per trascinare un file di script esistente oppure fare clic su Scegli file per cercare e selezionare il file dello script da caricare in Ivanti Neurons per MDM. Qualsiasi script esistente nell'editor di script verrà sostituito. Questa azione non può essere annullata. Fare clic su **Importa**. Il codice dello script caricato verrà visualizzato nell'editor di script.
9. (Facoltativo) Nella sezione **Attributi personalizzati disponibili** selezionare uno o più attributi personalizzati dei dispositivi per associarli allo script. Tali attributi possono essere utilizzati per assegnare i valori dei risultati dell'esecuzione dello script agli attributi personalizzati dei dispositivi configurati. Fare clic su **Codice esempio per attributi personalizzati** per visualizzare un esempio di codice che utilizza attributi personalizzati in uno script.
10. Fare clic su **Salva**.

I nomi degli attributi personalizzati nello script devono scritti in lettere minuscole. Gli attributi personalizzati referenziati in uno script non possono essere rimossi. Se si modifica un attributo personalizzato associato a uno script (ad esempio, si cambia il nome), è necessario apportare le modifiche corrispondenti anche agli script associati.

Modifica di uno script

Per modificare o rimuovere uno script:

1. Andare in **Amministratore > Script > Tutti gli script**.
2. Nella colonna **Azioni** dello script, fare clic sull'icona corrispondente all'azione di modifica o eliminazione.
3. Seguire le istruzioni visualizzate per completare l'azione.

Quando uno script viene modificato (contenuto, nome, descrizione), tutte le configurazioni associate allo script vengono redistribuite ai dispositivi.

Utilizzo di variabili script (applicabili a Windows e macOS)

Definire e memorizzare gli input di script come le variabili di ambiente e sostituzione nel repository degli script. Nella configurazione degli script Mobile@Work for macOS o nella configurazione di Ivanti Bridge for Windows Scripts and Actions, a seconda dello script collegato, le variabili script correlate saranno disponibili per l'uso come richiesto. Per macOS, questa funzionalità richiede **Mobile@Work per macOS** 1.71.0 fino alla versione più recente supportata da Ivanti Neurons per MDM. Per Windows, questa funzione richiede **Ivanti Bridge**.

Utilizzare le variabili per eseguire uno script con valori diversi ogni volta che viene eseguito. Ad esempio, un amministratore può creare uno script per utilizzare la variabile di ambiente $ come variabile di script e associarla a Mobile@Work per la configurazione di script macOS o la configurazione Windows. Quando la configurazione viene distribuita e installata su ciascun dispositivo degli utenti, Ivanti Neurons per MDM invia un indirizzo e-mail utente registrato diverso per ogni dispositivo perché siano intraprese determinate azioni. Il portale amministrativo di Ivanti Neurons per MDM supporta le variabili personalizzate.

Per aggiungere una variabile di script:

1. Andare in **Amministratore > Script > Tutti gli script**.
2. Nella sezione Input script, fare clic su **+ Aggiungi**.
3. Nella pagina pop-up Aggiungi input script - Variabile di ambiente, inserire i seguenti dati:

- Etichetta da mostrare - Questo testo verrà visualizzato come etichetta nella pagina di configurazione script di Mobile@Work per macOS. Ad esempio, Inserire cartella SO, Inserire numero Apache, e così via.
- Nome variabile di ambiente - Per esempio, JAVA_HOME, OS_VERSION, e così via. Ivanti Neurons per MDM sostituisce i valori delle variabili di script durante l'invio dei dettagli di configurazione a un dispositivo di destinazione, mentre i valori vengono mantenuti nel database.
- Valore predefinito variabile di ambiente - Per esempio, 1024, $, e così via. Le variabili di input possono essere utilizzate nello script caricato o modificato da un amministratore. Vedere anche le seguenti note.

Nell'area Anteprima, rivedere come il valore di una variabile di ambiente verrà mostrato come input script nella pagina di configurazione.

5. Fare clic su **Salva**.

In questo modo, solo l'etichetta e il valore predefinito sono disponibili per la configurazione e non il nome della variabile di ambiente, che fornisce un livello di astrazione.

- Un valore alfanumerico (per esempio, 1024 bin/java, root@localhost) o attributi di sistema (per esempio, $) sono accettabili come valori della variabile di ambiente.
- Il valore della variabile di ambiente può essere modificato o eliminato durante il deployment nella pagina di configurazione.
- Se il valore della variabile di ambiente non viene fornito, assicurarsi che venga fornito un valore durante il deployment dello script. In caso contrario, allo script verrà passato un valore vuoto.
- Dopo che una configurazione dello script è stata distribuita e installata sul dispositivo, la modifica delle variabili di ambiente nella pagina **Amministratore > Script e file > Tutti gli script** non avrà alcun impatto sulle configurazioni esistenti associate allo script. Vedere anche **Configurazione di script in Mobile@Work per macOS**. Per Windows, vedere **Configurazione di Ivanti Bridge for Windows Scripts and Actions**.

Modifica di una variabile di script

Per modificare una variabile di script, fare clic sull'icona di modifica (matita) accanto alla variabile e salvare le modifiche.

Se una configurazione di script si riferisce a uno script con variabili di script, la modifica dell'etichetta di una variabile di script esistente si rifletterà anche nella configurazione dello script. Tuttavia:

- Un cambiamento nel valore predefinito della variabile di script non si rifletterà nelle configurazioni esistenti.
- Un cambiamento nel valore predefinito della variabile di script si rifletterà in tutte le nuove configurazioni create con lo script precedente.

Eliminazione di una variabile di script

Per eliminare una variabile di script, fare clic sull'icona di eliminazione (segno meno) accanto alla variabile e confermare.

Una variabile di script appena creata, o l'eliminazione di una variabile di script esistente, si rifletterà anche in una configurazione già esistente.

Test di script

Eseguire il test di uno script nello strumento di debug velocemente prima di testarlo su un dispositivo e senza necessariamente salvare gli script.

Prerequisiti

- For macOS, questa funzionalità richiede **Mobile@Work per macOS** 1.67 fino alla versione più recente supportata da Ivanti Neurons per MDM.
- Per Windows, questa funzione richiede la **Configurazione di Ivanti Bridge per Windows Scripts and Actions.**

Procedura

1. Andare in **Amministratore > Script > Tutti gli script**.
2. Nell'editor di script, aggiungere o importare uno script.
3. Se il tenant include più spazi, selezionare uno spazio.
4. Nella sezione Test script, selezionare **macOS** o **Windows** come piattaforma.
5. Nel campo di testo **Trova dispositivi**, trovare e selezionare il dispositivo in cui è possibile testare lo script. È possibile cercare il dispositivo in base al numero di serie, al nome utente, al nome dispositivo e alla versione del sistema operativo.
6. Fare clic su **Effettua test**. In questo modo, una variabile di ambiente può essere aggiunta, modificata ed eliminata e lo script può essere testato con quello stato (senza nemmeno salvare le modifiche apportate). Per lo Script **Windows**, a schermo viene visualizzata una finestra pop-up in cui verrà avviata l'esecuzione dello Script e dopo qualche tempo sarà possibile visualizzare lo stato dalla scheda Registri dettagli dispositivo.
7. Fare clic su **Salva**.
8. Per macOS, attendere che lo script venga inviato ed eseguito nel dispositivo.
9. Esaminare i risultati del test pubblicati nelle sezioni Input script (contenente i dettagli della variabile di ambiente), Output script, e Attributi personalizzati sezioni. Vengono visualizzati anche i valori predefiniti delle variabili di ambiente.

Verifica dei risultati dell'esecuzione di uno script

Per visualizzare i registri dei risultati dell'esecuzione di uno script:

1. Andare su **Dispositivi**.
2. Fare clic sul nome del dispositivo.
3. Fare clic sulla scheda **Registri**.
4. Nella riga che mostra l'azione Esecuzione script, è possibile verificare le informazioni seguenti:
   - Nome dello script nella colonna Dettagli.
   - Stato di esecuzione dello script nella colonna Stato.
   - Data e ora di esecuzione dello script nella colonna Data.
   - Registri di esecuzione dello script (plist di registri del dispositivo), facendo clic sull'icona dell'occhio nella colonna Azione.

Utilizzare i filtri per visualizzare le righe **Esecuzione script**. I registri di tali righe includono l'output (plist) per l'output standard e gli errori standard per gli script.

6. Per visualizzare le righe **Elaborazione risultato esecuzione script**, utilizzare i filtri. I registri di tali righe includono i dettagli (plist) relativi alla modalità di elaborazione dei risultati.
   - Se a uno script non sono associati attributi personalizzati, non viene generato alcun risultato da elaborare. Tali script non vengono visualizzati nell'elenco delle righe filtrate.
   - Se a uno script sono associati attributi personalizzati e tali attributi sono nel formato previsto, gli attributi personalizzati dei risultati vengono mappati e viene visualizzato lo stato Operazione riuscita. Gli attributi personalizzati mappati e i relativi valori possono essere verificati nella scheda **Attributi**.

- Se a uno script sono associati attributi personalizzati e tali attributi non sono nel formato previsto, gli attributi personalizzati dei risultati non vengono mappati e viene visualizzato lo stato Errore.
- Se il formato dei risultati è corretto ma non tutti gli attributi personalizzati associati vengono inviati nel risultato, viene visualizzato lo stato Errore.
- Se una variabile di script viene inviata con lo script, i registri Elaborazione risultato esecuzione script includeranno dettagli (plist) della variabile di script.

Argomenti correlati:

- **Configurazione dello script di Mobile@Work per macOS**
- **Come creare una configurazione**
- **Configurazione di Ivanti Bridge for Windows Scripts and Actions**

12.9.2. File

Applicabile a: dispositivi macOS

Ivanti Neurons per MDM consente agli utenti con ruolo di Gestione sistema di creare o caricare e gestire i file utilizzati per la configurazione e la distribuzione ai dispositivi.

Procedura

1. Andare in **Amministratore** > **Script e file** > **File**.
2. Nella pagina **File**, fare clic su **+ Aggiungi**.
3. Nella finestra **Crea file**, inserire i seguenti dettagli:
    1. Nel campo **Nome**, inserire un nome per identificare il file.
    2. Nel campo **Descrizione**, inserire una descrizione che chiarisca lo scopo di questo file.
    3. Nel riquadro **Carica file**, fare clic su **Scegli un file** per caricare il file .zip. In alternativa, è possibile trascinare e rilasciare un file dal proprio dispositivo.
4. Fare clic su **Salva**.
   Il file appena aggiunto appare sulla pagina **File**.

Modifica di un file

1. Andare in **Amministratore** > **Script e file** > **File**.
2. Selezionare il file che si desidera modificare e fare clic su **Modifica**.
   Appare la finestra **Modifica file**.
3. (facoltativo) È possibile modificare i campi **Nome** e **Descrizione**.
4. Nel riquadro **Carica file**, fare clic su **Scegli un file diverso** per caricare il file .zip. In alternativa, è possibile trascinare e rilasciare un file dal proprio dispositivo.
5. Fare clic su **Aggiorna**.

Eliminazione di un file

Per eliminare i **File** esistenti, navigare in **Amministratore** > **Script e file** > **File**, selezionare tutti i file che si desidera eliminare e fare clic su **+ Elimina**.

Se i **File** sono associati a una configurazione, Ivanti Neurons per MDM visualizzerà un messaggio di **Avviso**, **"Il file non può essere eliminato poiché è in uso da parte di altri criteri."**

12.10. Personalizzazione

Argomenti della sezione:

- Amministratore > Catalogo app Apple (Personalizzazione)
- Personalizzazione dell'App Catalog Android
- Amministratore > Personalizzazione tutto schermo Android
- Personalizzazione dei modelli e-mail
- Portale self-service
- Portale self-service (personalizzazione)
- Personalizzazione dell'accesso multiutente (clip Web)
- Organizzazione

12.10.1. Amministratore > Catalogo app Apple (Personalizzazione)

Licenza: Gold

È possibile personalizzazione l'{{App Catalog}} Apple per conferirgli un aspetto più familiare agli utenti finali dei dispositivi iPhone, iPad e Mac. È possibile personalizzare i seguenti oggetti nel Catalogo app Apple:

- Icona dell'app (immagine PNG quadrata da 360 px)
- Nome app
- Immagine banner app (PNG, 360x64)
- Colore del testo

> L'App Catalog Apple è disponibile in due modalità: App Catalog Standalone e App Catalog integrato. L'App Catalog Standalone è disponibile sui dispositivi iPhone, iPad e Mac. Il Catalogo app integrato è disponibile solo sui dispositivi iOS e Mac.

Personalizzazione del Catalogo app Apple

Le modifiche apportate a questa pagina vengono riflesse nella schermata iniziale e di avvio del dispositivo e nella schermata iniziale dell'app. La procedura per l'App Catalog Standalone è simile a quella per l'App Catalog integrato.

Procedura

1. Nella pagina **Personalizzazione dell'App Catalog Apple**, fare clic su **Personalizza** (in alto a destra).
2. Nella sezione **Icona app**, trascinare il file del logo sulla casella punteggiata oppure fare clic su **Scegli file** per selezionarlo nel file system. L'icona dell'app viene visualizzata nella schermata iniziale del dispositivo iOS
3. Nella sezione **Nome app**, modificare il testo **Nome App Catalog** per sostituire l'etichetta mostrata nella schermata di avvio.
4. Il nome e l'icona vengono applicati nel banner della schermata iniziale. Per cambiare un'immagine banner personalizzata, deselezionare l'opzione **Applica nome e icona nel banner della schermata iniziale**. Questo visualizzerà la sezione **Immagine banner app**.
5. Per cambiare l'immagine banner dell'app, trascinare il file della nuova immagine banner sulla casella punteggiata oppure fare clic su **Scegli file** per selezionarlo nel file system. L'immagine banner dell'app viene visualizzata nella barra superiore della schermata iniziale dell'app.
6. Nella sezione **Colore del testo**, fare clic sulla casella del codice colore esadecimale per selezionare un colore oppure immettere il codice colore esadecimale da assegnare al testo e alle icone. Questo colore verrà applicato al testo nella schermata di avvio, al nome dell'app, al banner e al pulsante Azioni.
7. Fare clic su **Salva modifiche**.

Il nome dell'App Catalog inserito verrà applicato ad Android, iOS e macOS.

12.10.2. Personalizzazione dell'App Catalog Android

Licenza: Gold

È possibile personalizzare il {{catalogo delle app}} Android per ottenere un aspetto più familiare all'utente finale. È possibile personalizzare i seguenti oggetti nel Catalogo app Android:

- logo del catalogo (PNG, 360 x 64)
- nome del catalogo
- colore della barra delle azioni
- icona del collegamento
- nome del collegamento

Personalizzazione del Catalogo app Android

Procedura

1. Nella schermata **Personalizzazione App Catalog Android**, fare clic su **Personalizza** (in alto a destra).
2. Per modificare il logo del Catalogo app, trascinare il file con il logo sulla casella tratteggiata oppure fare clic su **Scegli file** per selezionarlo dal file system.
3. Fare clic sul campo **Colore della barra delle azioni** per visualizzare la tavolozza dei colori da cui scegliere o inserire il numero esadecimale per il colore preferito.
4. Modificare il testo del **Nome del catalogo app** per cambiare l'etichetta del catalogo.
5. Il nome dell'App Catalog inserito verrà applicato ad Android, iOS e macOS.
   Per modificare l'icona del collegamento, trascinare il file con l'icona sulla casella tratteggiata oppure fare clic su **Scegli file** per selezionarlo dal file system.
6. Per modificare l'etichetta del collegamento dell'app, modificare il testo **Nome collegamento**.
7. Fare clic su **Salva modifiche**.

12.10.3. Amministratore > Personalizzazione tutto schermo Android

Licenza: Silver

È possibile personalizzare la pagina tutto schermo Android per renderne l'aspetto più familiare all'utente finale. È possibile personalizzare gli elementi seguenti:

- logo del banner (PNG, 840x114) o testo
- colore del bordo del banner
- colore di sfondo del banner
- colore di sfondo della schermata
- immagine di sfondo della schermata (1280x800)
- formato dello sfondo della schermata

Personalizzazione della schermata tutto schermo Android

Procedura

1. Accedere ad **Amministratore > Tutto schermo Android**.
2. Nella pagina **Personalizzazione modalità tutto schermo**, fare clic su **Crea personalizzazione**.
3. Nel campo **Nome**, digitare il nome della personalizzazione della modalità tutto schermo.
4. Se si vuole disattivare il banner, deselezionare **Abilita Banner superiore.**
5. Fare clic sul campo **Colore di sfondo del banner** per visualizzare la tavolozza dei colori da cui scegliere o in cui inserire il numero esadecimale per il colore preferito.
6. Fare clic sul campo **Colore bordo del banner** per visualizzare la tavolozza dei colori da cui scegliere o in cui inserire il numero esadecimale per il colore preferito.
7. Selezionare **Immagine/Logo** o **Testo** per impostare il contenuto del banner.
8. Se si seleziona **Immagine/Logo**, trascinare l'immagine oppure fare clic su **Scegli file** per selezionarne una.
9. Se si seleziona **Testo**, digitare il testo che si desidera che venga visualizzato nel banner.
10. Fare clic sulla scheda **Sfondo**.
11. Fare clic sul campo **Colore di sfondo** per visualizzare la tavolozza dei colori da cui scegliere o in cui inserire il numero esadecimale per il colore preferito.
12. Per modificare l'immagine di sfondo:
13. a. Eliminare l'immagine predefinita.
    b. Trascinare l'immagine prescelta o fare clic su **Scegli file** per selezionarne una.
    c. Selezionare il layout preferito.
    Fare clic su **Salva modifiche**.
    La personalizzazione della modalità tutto schermo creata viene visualizzata nella pagina **Personalizzazione modalità tutto schermo**. Per modificare ulteriormente la personalizzazione, fare clic sull'icona Modifica nella colonna **Azioni**. Per eliminare la personalizzazione, fare clic sull'icona Elimina. Quando si elimina la personalizzazione di tutto schermo, verranno ripristinati i valori predefiniti della configurazione relativa alla personalizzazione.

12.10.4. Personalizzazione dei modelli e-mail

È possibile personalizzare l'invito per e-mail inviato all'utente finale per ottenere un aspetto più familiare. Fare clic su **Ripristina impostazioni predefinite** per cancellare le personalizzazioni.

È possibile personalizzare i seguenti modelli e-mail in tutte le lingue supportate:

- **Invito utente finale**: consente di invitare un utente a connettersi ai dispositivi per ottenere l'accesso alle app e alle configurazioni.
- **Notifica di reimpostazione password**: il sistema invia e-mail di promemoria 7 giorni e 24 ore prima della scadenza della password degli account locali. Questo non si applica agli account LDAP.
- **Conferma registrazione**: messaggio e-mail inviato dopo che un utente ha completato la registrazione. È possibile utilizzare questa funzione allo scopo di ringraziare gli utenti per la registrazione e indirizzarli verso ulteriori risorse di apprendimento.
- **Notifica sulla conformità delle policy**: messaggio e-mail inviato quando i dispositivi non sono conformi.

Argomenti della sezione:

- Anteprima e test del modello di e-mail
- Personalizzazione delle intestazioni dei messaggi
- Personalizzazione di un modello e-mail
- Variabili e-mail supportate

Anteprima e test del modello di e-mail

È possibile visualizzare in anteprima e testare i modelli di e-mail. Il test permette di inviare un'e-mail basata sul modello a un indirizzo e-mail indicato.

Per visualizzare in anteprima e testare un modello e-mail, procedere come segue:

1. Fare clic su **Amministratore**.
2. Nella pagina Modelli e-mail, fare clic su **Invito utente finale**, **Notifica di reimpostazione password**, **Conferma registrazione** o **Notifica sulla conformità delle policy**.
3. Fare clic sul collegamento **Anteprima e test** associato al modello e-mail che si desidera visualizzare in anteprima e testare.
4. Visualizzare il modello nel riquadro apposito.
5. Specificare un indirizzo e-mail di prova a cui inviare l'e-mail di prova.
   Se l'indirizzo e-mail specificato appartiene a un utente corrente, l'e-mail di prova sostituisce i valori della maggior parte delle variabili del modello di e-mail, offrendo un'idea molto accurata dell'esperienza utente dell'e-mail. Tuttavia, l'e-mail di prova non sostituisce i valori delle variabili generate da Ivanti Neurons for MDM nel momento in cui genera un invito per e-mail reale.
6. Fare clic su **Invia e-mail di prova**.

Personalizzazione delle intestazioni dei messaggi

1. Fare clic su **Amministratore**.
2. Fare clic su **Modelli di e-mail**.
3. Fare clic sul collegamento dell'icona **Modifica** (nella colonna Azioni) associato al modello di e-mail che si desidera modificare.
4. Fornire le nuove impostazioni desiderate per **Nome visualizzazione e-mail**, **Da indirizzo e-mail**, **Indirizzo e-mail rispondi a** e **Imposta configurazione e-mail SMTP**.

5. Se si personalizzano gli indirizzi e-mail Da e Rispondi a, è consigliabile inserire il servizio Mail Relay nell'elenco degli elementi consentiti, per evitare che i messaggi e-mail vengano bloccati dai servizi del filtro antispam. Per ulteriori informazioni, consultare il presente documento.
   Fare clic su **Salva**.
6. Verificare l'anteprima del modello e-mail e fare clic su **Salva**.

Utilizzo configurazione SMTP

È stato aggiunto **Imposta configurazione e-mail SMTP** per consentire all'amministratore di configurare l'integrazione del proprio server e-mail per le notifiche in uscita.

1. Accedere a **Amministratore > Branding > Impostazioni e-mail**, attivare l'opzione **Imposta configurazione e-mail SMTP**.
2. Aggiornare i seguenti campi:
   - Server SMTP
   - Porta server SMTP
   - Protocollo
   - Nome utente
   - Password
3. Fare clic su **Test** per inviare un messaggio di prova; viene visualizzata la schermata a comparsa **Test e-mail**.
4. Inserire il nome del **Destinatario** e il **Corpo** del messaggio, quindi fare clic su **Salva**.

> Se le credenziali non sono corrette, viene visualizzato un messaggio di errore.

5. Fare clic su **Salva**

La tabella seguente riassume i campi e le descrizioni della finestra Configurazione SMTP:

Campi	Descrizione
Server SMTP	Specificare l'indirizzo IP o il nome host completamente qualificato del server SMTP utilizzato da Ivanti Neurons for MDM Server.
Porta server SMTP	Specificare la porta configurata per il server SMTP.
Protocollo	Se il server SMTP che si sta configurando è un server protetto, cioè utilizza il protocollo SMTPS, selezionare il pulsante SMTPS. Altrimenti, lasciare selezionato SMTP.
Nome utente	Inserire il nome utente richiesto per l'autenticazione SMTP.
Password	Inserire la password richiesta per l'autenticazione SMTP.

Personalizzazione di un modello e-mail

1. Selezionare **Amministratore > Personalizzazione > Modelli e-mail**.
2. Selezionare il modello da modificare: **Invito utente finale**, **Notifica di reimpostazione password**, **Conferma registrazione** o **Notifica sulla conformità delle policy**.

3. Fare clic sull'icona di modifica a forma di penna accanto al modello di e-mail che si desidera personalizzare.

4. Modificare l'oggetto come desiderato.
5. Modificare il modello e-mail contenente gli elementi HTML nel riquadro del corpo per personalizzare il contenuto del messaggio.

È possibile utilizzare le variabili visualizzate a destra nel corpo dell'e-mail. Vedere **Variabili e-mail supportate**.

6. Fare clic su **Anteprima** per visualizzare in anteprima il modello e-mail in base alle iterazioni create.
7. Quando si è pronti a salvare il modello, fare clic su **Anteprima**. Viene visualizzata l'anteprima ed è possibile salvarla.

8. Se si è soddisfatti dell'anteprima, fare clic su **Salva**.

Contenuti consentiti e non consentiti negli inviti utente personalizzati

Durante la personalizzazione del modello e-mail per gli inviti utente, in **Invito utente finale** sono disponibili un elenco di attributi e tag HTML consentiti e un elenco di stringhe che non è possibile utilizzare negli inviti utente al fine di prevenire la vulnerabilità XSS (Cross Site Scripting).

Nell'e-mail di invito è possibile utilizzare solo gli attributi e i tag HTML consentiti. I tag consentiti e gli attributi consentiti corrispondenti sono riportati nella tabella seguente.

> Alcuni tag Allowlisted (Esempio: <big>) non dovrebbero avere alcun attributo Allowlisted e quindi vengono visualizzati vuoti.

Tag consentiti	Attributi consentiti
<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"]

Tag consentiti	Attributi consentiti
	[]
	[]
<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"]

Di seguito sono riportate le stringhe che non è consentito utilizzare negli inviti utente personalizzati.

- Script, @import, ¼script¾, script>, <script, <script>, </script>, javascript, alert(, moz-binding, expression(, +ADw-SCRIPT+AD4-,+ADw-/SCRIPT+AD4-, xml:base
- Caratteri speciali e ricerca per JavaScript o script
- L'attributo di metacontenuto contenente "url=", senza distinzione tra maiuscole e minuscole
- L'attributo img src non contenente .svg
- Il valore di attributo contenente "\00"

Se il contenuto HTML dell'invito per l'utente include una qualsiasi delle stringhe non consentite indicate in precedenza, quando si fa clic su **Anteprima** viene visualizzato un messaggio di errore, che riporta il contenuto HTML non consentito nell'invito per l'utente finale. Per proseguire, modificare e rimuovere il contenuto HTML non consentito e fare clic su **Anteprima**.

> Non è possibile salvare i modelli modificati che includono contenuto HTML non consentito.

Variabili e-mail supportate

Ivanti Neurons for MDM offre diverse variabili utilizzabili per personalizzare i modelli e-mail.

Variabili invito utente finale

Variabile	Descrizione
$	URL di attivazione utente: è il collegamento ipertestuale visualizzato attorno al testo $.
$	URL di registrazione cluster: NON è disponibile nel modello predefinito, ma esiste un riferimento indiretto (tramite la variabile $).
$	Il nome del marchio del prodotto - definito come il tag <title> nell'intestazione del modello predefinito.
$	URL del logo aziendale: è una singola immagine contenuta nel modello predefinito, che fa riferimento a un'immagine nel CDN di MobileIron. L'aggiornamento delle impostazioni **Branding utente** modifica il valore a cui fa riferimento **$**.
${message:$	Il registro del titolo del dispositivo utente.
${message:$}	Il titolo dell'invito e-mail.
${message:$}	Verifica della registrazione dell'utente sul dispositivo.
${message:$}	Testo introduttivo dell'invito e-mail.
${message:$}	Istruzioni per l'accesso e la registrazione.
${message:$}	Informazioni relative ai messaggi e-mail e alle app inviate al dispositivo.
${message:$}	Informazioni di registrazione se l'utente non è registrato sul proprio dispositivo. Tali informazioni includono l'URL di registrazione cluster.
${message:$}	Piè di pagina dell'invito e-mail che include l'etichetta del sito Web dell'azienda.
$	URL di registrazione cluster: NON è disponibile nel modello predefinito, ma esiste un riferimento indiretto (tramite la variabile $).

Variabili notifica scadenza password

Variabile	Descrizione
$	L'URL di reimpostazione della password.
$	Il nome del marchio del prodotto - definito come il tag <title> nell'intestazione del modello predefinito.
$	URL del logo aziendale: è una singola immagine contenuta nel modello predefinito, che fa riferimento a un'immagine nel CDN di MobileIron. L'aggiornamento delle impostazioni **Branding utente** modifica il valore a cui fa riferimento **$**.
${message:$}	Il titolo della notifica di scadenza password.
${message:$}	Il paragrafo introduttivo della notifica di scadenza password.
${message:$}	Il nome dell'URL di reimpostazione password.
${message:$}	Piè di pagina dell'invito e-mail che include l'etichetta del sito Web dell'azienda.
$	URL di registrazione cluster: NON è disponibile nel modello predefinito, ma esiste un riferimento indiretto (tramite la variabile $).

Variabili conferma registrazione

Variabile	Descrizione
$	Il nome del marchio del prodotto - definito come il tag <title> nell'intestazione del modello predefinito.
$	URL del logo aziendale: è una singola immagine contenuta nel modello predefinito, che fa riferimento a un'immagine nel CDN di MobileIron. L'aggiornamento delle impostazioni **Branding utente** modifica il valore a cui fa riferimento **$**.
${message:$}	Il titolo del messaggio di conferma della registrazione.
${message:$}	Il paragrafo introduttivo del messaggio di conferma della registrazione.

Variabili conformità delle policy

Variabile	Descrizione
$	Questa variabile verrà sostituita dal contenuto visualizzato nella riga dell'oggetto, nell'ambito dell'azione di invio dell'e-mail sulla conformità prevista dalla policy.
$	Questa variabile verrà sostituita dal contenuto visualizzato nella parte del messaggio, nell'ambito dell'azione di invio dell'e-mail sulla conformità prevista dalla policy.
$	Il nome del marchio del prodotto - definito come il tag <title> nell'intestazione del modello predefinito.
$	URL del logo aziendale: è una singola immagine contenuta nel modello predefinito, che fa riferimento a un'immagine nel CDN di MobileIron. L'aggiornamento delle impostazioni **Branding utente** modifica il valore a cui fa riferimento **$**.
${message:$}	Piè di pagina dell'invito e-mail che include l'etichetta del sito Web dell'azienda.
$	URL di registrazione cluster: NON è disponibile nel modello predefinito, ma esiste un riferimento indiretto (tramite la variabile $).

Variabili degli attributi utente personalizzati

Gli amministratori possono utilizzare gli **attributi utente personalizzati** come variabili e-mail nel modello e-mail personalizzato, alle condizioni seguenti:

- Gli attributi utente personalizzati si trovano nella pagina **Amministrazione > Attributi**.
- L'amministratore ha **assegnato gli attributi utente personalizzati agli utenti**, con i valori specificati per gli attributi utente personalizzati per ogni utente.

12.10.5. Portale self-service

L'invito alla registrazione include un collegamento al portale self-service. Gli utenti possono utilizzare il portale per eseguire le seguenti attività:

- Blocca
- Sblocca
- Visualizza posizione (se abilitata nella **Configurazione privacy**)
- Cancella
- Ritira
- Modifica informazioni account (nome, password, indirizzo e-mail)
- Imponi check-in
- Aggiungere certificati di crittografia e per la firma

Per registrare dispositivi aggiuntivi, gli utenti finali devono fare clic sul collegamento al portale di registrazione nel Portale self-service.

Se l'utente finale perde l'URL del portale self-service, indirizzarlo al sito **https://mydevices.mobileiron.com/user/login.html**. Per gli utenti iOS, prendere in considerazione la creazione di una **configurazione Clip Web** per il portale self-service.

Caricamento di certificati di crittografia e per la firma

Si può consentire agli utenti finali di caricare i propri certificati di crittografia e per la firma delle e-mail nel portale self-service nell'ambito della configurazione Certificati specificati dall'utente. Questa impostazione può essere configurata utilizzando la configurazione Certificati specificati dall'utente. Dopo la configurazione, gli utenti finali possono caricare i propri certificati di crittografia e per la firma delle e-mail.

1. Nella scheda **Certificati personali**, fare clic su **Aggiungi certificato**. Viene visualizzata la finestra **Aggiungi certificato**.
2. Aggiornare i seguenti campi:

Nome del campo	Descrizione
Tipo di certificato	Selezionare il tipo di certificato da caricare. Sono disponibili le seguenti opzioni: • **Certificato di crittografia** • **Certificato per la firma** Queste opzioni sono create dal portale Amministratori di Ivanti Neurons per MDM. Per ulteriori informazioni vedere **Configurazione del certificato di identità**.
Certificato da caricare	Fare clic su **Scegli file** per selezionare il file del certificato da caricare. Assicurarsi che il formato del file sia PKCS12.
Password	Immettere la password utilizzata per il file.

3. Fare clic su **Carica**.

Dopo il caricamento, è possibile visualizzare l'elenco di certificati in una tabella con i seguenti dettagli.

Nome del campo	Descrizione
Nome certificato	Specifica se il certificato è del tipo **Crittografia** o **Firma**.
Emesso da	I dettagli del certificato emesso.
Caricato il	La data in cui è stato caricato il certificato.
Data di scadenza	La data di scadenza del certificato.
Azioni	È possibile eseguire queste azioni: • **Modifica certificato**: consente di modificare i dettagli del certificato. • **Cancella chiave privata** - elimina la chiave privata dal pacchetto di certificati (PKCS#12). • **Elimina certificato** - consente di eliminare il certificato dal server Ivanti Neurons per MDM.

Quando l'utente carica una configurazione del certificato, il server invia nuovamente la configurazione che utilizza il certificato.

> Se un utente elimina e cancella la chiave privata, le configurazioni non vengono inviate nuovamente.

Per ulteriori informazioni, vedere **Personalizzazione del portale self-service**.

12.10.6. Portale self-service (personalizzazione)

Licenza: Silver

È possibile personalizzare il **portale self-service** con il logo della propria organizzazione. Se non si aggiunge il proprio logo, sul portale self-service verrà visualizzato il logo predefinito del servizio.

Personalizzazione del portale self-service

Procedura

1. Nella schermata Personalizzazione del portale self-service, fare clic su **Personalizza** (in alto a destra).
2. Trascinare il file con il logo (PNG, 182x34) sulla casella tratteggiata oppure fare clic su **Scegli file** per selezionarlo dal proprio file system.
3. Fare clic su **Salva modifiche**.

12.10.7. Personalizzazione dell'accesso multiutente (clip Web)

Personalizzare l'accesso sicuro multiutente per iOS aggiungendo un nuovo titolo e un'icona clip Web.

Procedura

1. Andare ad **Amministrazione > Accesso multiutente (clip Web)**.
2. Nella schermata Accesso multiutente (clip Web), fare clic su **Personalizza**.
3. Trascinare il file con il logo sulla casella tratteggiata oppure fare clic su **Scegli file** per selezionarlo dal proprio file system.
4. Per cambiare l'etichetta, modificare il testo **Accesso sicuro**.
5. Per cambiare l'icona della clip Web, trascinare e rilasciare il file della clip Web nella casella tratteggiata o fare clic su **Scegli file** per selezionarlo dal file system.
6. Visualizzare in anteprima gli aggiornamenti e fare clic su **Salva modifiche**.

Per i dispositivi touch iPhone e iPod, creare icone con dimensioni di 120 x 120 pixel o di 60 x 60 pixel (risoluzione standard).

Per i dispositivi iPad, creare icone con dimensioni di 152 x 152 pixel o di 76 x 76 pixel (risoluzione standard).

Per ulteriori informazioni, vedere **Accesso sicuro multiutente per iOS**.

12.10.8. Organizzazione

È possibile fornire il nome del brand dell'organizzazione o personalizzare gli oggetti delle e-mail di avviso del sistema incorporando in ogni oggetto identificatori specifici del tenant (ad es., il nome del cliente). Se non si aggiorna il nome dell'organizzazione, nella schermata Organizzazione verrà visualizzato il valore predefinito.

Applicazione del brand dell'organizzazione

Procedura

1. Nella schermata Organizzazione, inserire il nome desiderato nel campo **Nome**.
2. Per aggiungere un prefisso, fare clic su **Modifica** e attivare l'opzione **Aggiungere come prefisso il nome dell'organizzazione in tutte le e-mail generate dal sistema, ad es. Scadenza licenza**.
3. Fare clic su **Salva** per applicare le modifiche.

12.11. Aggiunta della gestione di dispositivi non iOS

Licenza: Gold

Al momento è in uso una versione di Ivanti Neurons for MDM ottimizzata per i dispositivi iOS. Questa sezione descrive come eseguire il passaggio per consentire la gestione di dispositivi non-iOS. Dopo il passaggio, si sarà in grado di gestire anche i seguenti dispositivi:

- Android 5.0 o versioni più recenti supportate
- Windows 10 e versioni successive

L'inclusione della gestione dei dispositivi non-iOS è irreversibile.

Per passare a includere i dispositivi non-iOS:

1. Fare clic su **Admin > Piattaforme consentite**.
2. Fare clic sul pulsante **Consenti la gestione di tutte le piattaforme**.
3. Selezionare **Sono consapevole del fatto che non sarà possibile annullare questa operazione** per confermare che si è al corrente/consapevoli del fatto che questa operazione è irreversibile
4. Fare clic sul pulsante **Consenti la gestione di tutte le piattaforme**.

13. Pacchetti

Argomenti della sezione:

- Aggiornamento
- Pacchetti Secure UEM e Secure UEM Premium
- Pacchetti legacy Bronze, Silver e Gold
  - Silver
  - Gold
  - Platinum
- Sandbox per anteprima o test

Pacchetti Secure UEM e Secure UEM Premium

I pacchetti Secure UEM e Secure UEM Premium offrono le seguenti funzionalità:

	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)		✓

Questi pacchetti sono soggetti a cambiamento. Contattare **Ivanti Sales** per confermare lo schema corrente.

Pacchetti legacy Bronze, Silver e Gold

Questa sezione descrive i pacchetti legacy Bronze, Silver e Gold. I pacchetti si sono evoluti allo schema **Secure UEM e Secure UEM Premium**.

Bronze

Le funzionalità di base Ivanti Neurons for MDM vengono fornite con il pacchetto Bronze. È possibile espandere il pacchetto Bronze:

- aggiungendo altri dispositivi
- aggiungendo Silver
- aggiungendo Gold

- aggiunta di Platinum

Queste aggiunte consentono di espandere la soluzione mobile oltre la configurazione di base del dispositivo.

Gli amministratori possono contattare il **supporto** se desiderano attivare una o più **funzionalità on-demand** sui propri tenant che sono disattivate per impostazione predefinita.

Silver

Con l'aggiornamento a Silver vengono aggiunte le seguenti funzioni:

- **LDAP e Connettore:** supporto per l'aggiunta di directory aziendali e autorità certificato per Ivanti Neurons for MDM.
- **Sentry:** supporto per il controllo degli accessi e-mail.
- **Spazi:** supporto per la designazione di dispositivi per la gestione da parte di amministratori diversi (amministrazione delegata).
- **Modalità di supervisione:** supporto a livello di dispositivo per configurazioni specifiche, inclusa la modalità Single-App.
- **Personalizzazione del portale self-service:** utilizzare il proprio logo nel portale self-service.
- **Autorità di certificazione:** utilizzare Ivanti Neurons for MDM come autorità di certificazione.
- **Installazione/disinstallazione dell'applicazione in modalità invisibile all'utente:** consente di distribuire e rimuovere automaticamente le app da un dispositivo mobile.
- **App consentite/non consentite/richieste:** consente di monitorare e identificare le app installate nei dispositivi.
- **Filtro contenuto Web:** consente di applicare a tutti i browser Web le policy relative agli elenchi di elementi consentiti e non consentiti.
- **Funzionalità specifica di Apple:** consente di abilitare o limitare l'utilizzo di AirPlay, AirDrop, la distribuzione di sfondi iOS e Apple TV.
- **Gestione Apri in:** consente di controllare quali app mobili possono aprire determinati contenuti aziendali.
- **Apple App e libri:** è possibile distribuire licenze di app mobili a dispositivi, nonché recuperare e riassegnare tali licenze quando un dispositivo viene dismesso.
- **Supporto per Android enterprise (Android for Work)**
- **Registrazione dispositivi**: consente ai clienti di acquistare dispositivi Apple in blocco e registrarli automaticamente in MDM durante l'attivazione.
- **Configurazione per app:** è possibile distribuire le app mobili configurate in scala, con pochissime azioni o nessuna azione richiesta da parte dell'utente finale.
- **VPN per app di terzi:** la protezione VPN è adesso immediata, invisibile e specifica per le app mobili.
- **Azioni a livello di policy**
- Filtri distribuzione app
- **Audit trail**
- **Modalità tutto schermo Android:** supporto per la configurazione dei dispositivi Android per il funzionamento in modalità tutto schermo.
- **Personalizzazione tutto schermo Android**: consente di modificare lo sfondo e il banner della schermata tutto schermo visualizzata quando il dispositivo funziona in modalità tutto schermo.
- **Prevenzione della perdita dei dati (DLP) di Office 365 mediante le API Graph**: consente di applicare i controlli DLP per le app Office 365 mediante le API Graph.

Gold

L'aggiornamento a Gold consente di aggiungere le funzionalità fornite da Silver, oltre alle funzionalità seguenti:

- **Single sign on:** gli utenti effettuano l'autenticazione una sola volta e verranno connessi automaticamente alle altre app mobili dell'azienda.
- **Personalizzazione dell'App Catalog per iOS e Android:** visualizzazione del logo della propria azienda nell'App Catalog.
- **Limite dei contenuti aumentato:** 50 file, 25 MB ognuno.
- **AppConnect per iOS:** protezione e configurazione delle app con abilitazione AppConnect.
- **AppTunnel per iOS:** accesso app sicuro alle risorse aziendali.
- **Docs@Work per iOS:** consente agli utenti di visualizzare, archiviare e condividere documenti.
- **Single Sign-On basato sul certificato di iOS 8**
- **Gestione iBook/ePub di iOS 8**
- **Supporto macOS**
- **Personalizzazione degli utenti**
- **Mobile Application Management (MAM) con AppConnect**
- **Credenziali derivate**
- **Supporto per Windows 10 (include Bridge)**

Platinum

L'aggiornamento a Platinum consente di aggiungere le funzionalità fornite da Gold, oltre alle funzionalità seguenti:

- **Tunnel:** consente di configurare l'accesso specifico dell'app ai dati aziendali.
- **Help@Work**
- **Monitoraggio**
- **ServiceConnect (ServiceNow, Splunk)**

Sandbox per anteprima o test

I clienti che utilizzano Ivanti Neurons for MDM possono ottenere un tenant sandbox per vedere in anteprima e testare le nuove versioni prima che entrino in produzione quando viene acquistato il supporto **Premium Plus**.

13.1. Aggiornamento

Argomenti della sezione:

- Aggiornamento di una licenza
- Richiesta di un aggiornamento
- Aggiornamento da una versione precedente

Aggiornamento di una licenza

Le funzionalità di base vengono fornite con il pacchetto Bronze. È possibile espandere il pacchetto Bronze:

- aggiungendo altri dispositivi
- aggiungendo Silver
- aggiungendo Gold
- aggiunta di Platinum

Queste aggiunte consentono di espandere la soluzione mobile oltre la configurazione di base del dispositivo.

Richiesta di un aggiornamento

Procedura

1. Selezionare **Opzioni di aggiornamento** dal menu amministratore a discesa.
2. Fare clic su **Richiedi aggiornamento/Aggiungi dispositivi** (in alto a destra).
3. Selezionare gli elementi da aggiungere e immettere il numero di telefono.

Entro 24 ore circa si verrà contattati da un rappresentante che fornirà tutti i dettagli.

Aggiornamento da una versione precedente

Se si esegue l'aggiornamento da una versione precedente, le impostazioni nella pagina **Modifica profilo Registrazione dispositivi** non vengono mantenute. Prima di eseguire l'aggiornamento, annotare le impostazioni delle opzioni.

- Se l'opzione **Salta accesso ad AppleID e iCloud** è abilitata prima dell'aggiornamento, l'opzione **Ignora configurazione Apple Pay** verrà abilitata dopo l'aggiornamento.
- Se l'opzione **Salta immissione del passcode** è abilitata prima dell'aggiornamento, le opzioni **Ignora Touch ID** e **Ignora configurazione Apple Pay** verranno abilitate dopo l'aggiornamento.

Procedura

1. Al termine dell'aggiornamento, tornare alla pagina **Modifica profilo Registrazione dispositivi** per modificare il profilo Registrazione dispositivi e ripristinare le impostazioni desiderate.
2. Fare clic su **Salva**.

Sono interessate diverse impostazioni di configurazioni dopo l'aggiornamento.

- Le opzioni di promozione sono impostate su **Off**.
  Le impostazioni di installazione sono impostate su **On**.

L'opzione **Non mostrare in App Catalog** non è più selezionata.

L'**Installazione invisibile all'utente su Android Samsung Knox** è impostata su Falso.

I contrassegni della gestione iOS sono impostati su:

- Backup su iCloud.
- Rimuovere in caso di annullamento della registrazione.

Le impostazioni dei contrassegni di gestione di iOS possono essere selezionati singolarmente per ciascuna app.

Impostazioni delle app:

- Ora le impostazioni delle app sono denominate Configurazioni.
- Tutte le altre impostazioni delle app rimangono invariate anche dopo l'aggiornamento.

Per ulteriori informazioni, vedere **Pacchetti**.

14. Licenze dispositivo

Ivanti Neurons per MDM Le licenze basate sui dispositivi definiscono il numero di dispositivi che è possibile registrare, la quantità di contenuti che è possibile configurare per la distribuzione ai dispositivi e le funzionalità disponibili. Se si raggiunge il limite di dispositivi, viene visualizzato un triangolo rosso nella pagina Amministratore. Se si raggiunge il limite di contenuto, il servizio impedirà l'aggiunta di ulteriori contenuti e visualizzerà un messaggio per segnalare il raggiungimento del limite.

14.1. Sospensione tenant

Ivanti Neurons for MDM potrebbe sospendere l'accesso a un tenant utilizzato con una licenza di valutazione o di produzione. Le licenze di valutazione possono essere sospese allo scadere del periodo di valutazione o quando si supera l'utilizzo consentito. Le licenze di produzione possono essere sospese allo scadere del periodo di sottoscrizione o quando si supera l'utilizzo consentito. Ivanti Neurons for MDM ripristinerà il tenant sospeso quando la licenza verrà rinnovata o quando verranno acquistate licenze aggiuntive, in caso di eccedenze.

Quando una licenza tenant viene sospesa:

- I dispositivi registrati esistenti continueranno a funzionare normalmente.
- Gli amministratori non possono accedere al portale Amministratori.
- Non è possibile registrare nuovi dispositivi.
- L'accesso delle API al tenant è bloccato.
- Gli utenti finali possono continuare ad accedere al portale self-service.

Azione di sospensione dei tenant e messaggi di errore

Azione di sospensione	Errore	Messaggio di errore visualizzato	Posizione
Accesso all'API di integrazione dell'utente finale bloccato.	Chiamate API non riuscite.	Accesso negato. La licenza di prova è scaduta. Rinnovare la licenza per riabilitare l'accesso all'API. Per i dettagli, contattare l'amministratore del sistema.	Errore API 401.
Impossibile registrare nuovi dispositivi.	Il messaggio di errore viene visualizzato sulla schermata di registrazione.	Impossibile registrare il dispositivo. La licenza per il sistema in uso è scaduta. Per i dettagli, contattare l'amministratore di sistema. I dispositivi registrati in precedenza continueranno a funzionare in modo normale.	È richiesta la verifica password.
L'amministratore non può accedere al portale Amministratori.	Il messaggio di errore viene visualizzato sulla schermata di accesso.	Impossibile effettuare l'accesso. La licenza è scaduta. Rinnovare la licenza per ottenere nuovamente l'accesso al portale Amministratori e registrare nuovi dispositivi. I dispositivi che in precedenza hanno registrato dispositivi continueranno a funzionare normalmente. Contattare il rappresentante commerciale per rinnovare le licenze. Tenere presente che la password amministratore scade dopo un anno (365 giorni).	È richiesta la verifica password.

15. Apertura di un ticket di supporto

Visitare il **Portale supporto Ivanti** per aprire un ticket di supporto.

16. Attributi di terze parti

Ivanti Neurons for MDM include componenti sviluppati da terze parti. È possibile consultare l'elenco **qui**.

17. Apps@Work

A partire dalla versione 83 di Ivanti Neurons for MDM, è possibile eseguire la transizione all'esperienza nativa Apps@Work dall'applicazione Go. Per i tenant creati di recente, la configurazione Apps@work Webclip non viene distribuita per impostazione predefinita per i dispositivi iOS installati mediante iReg o client. L'amministratore deve distribuire manualmente la configurazione della webclip ai dispositivi registrati mediante iReg o client. Tenere presenti i seguenti punti:

Ivanti Neurons per MDM **portale amministrativo**:

- Per impostazione predefinita, solo i nuovi tenant ottengono la configurazione Catalogo app per client nativo distribuita ai dispositivi iOS.
- Per i tenant esistenti, per impostazione predefinita, l'applicazione Apps@Work Native non viene distribuita.
- L'amministratore deve eseguire il push della configurazione di Catalogo app per client nativi ai dispositivi al fine di rendere Apps@Work disponibile in un'esperienza Appstore nativa.

Client:

- L'applicazione Go ora visualizza una scheda per Apps@Work.
- La configurazione Catalogo app per client nativi presenta il certificato Identità Catalogo app per client nativi e il certificato di identità App Station. Ivanti Neurons per MDM esegue il push dei certificati con la configurazione Catalogo app per client nativo.

Funzionalità di Apps@Work

La scheda Apps@Work presenta le seguenti caratteristiche:

- **Accedere alla scheda Apps@Work dall'applicazione Go**
- **Cerca**
- **Installazione di un'app - Stati pulsante**
- **Applicazioni e banner in evidenza**
- **Notifica aggiornamento applicazione**
- **Notifica aggiornamento applicazione**

Accedere alla scheda Apps@Work dall'applicazione Go

- Una nuova scheda è aggiunta in Go app per Apps@Work.
- In Apps@Work sono disponibili due schede: Tutte le app e Categorie.
- La scheda Tutte le app elenca le app in ordine alfabetico.
- La scheda Categorie visualizza solo le categorie che contengono applicazioni.
- Ciascuna categoria visualizza il numero di applicazioni presenti al suo interno.
- MyApps sotto Categorie è un elemento elenco contenente tutte le applicazioni installate. MyApps sarà sempre la prima categoria, mentre il resto delle categorie viene elencato alfabeticamente.
- Quando non viene installata alcuna applicazione, l'elenco MyApps mostra Nessuno.
- Quando si fa clic su una categoria, tutte le applicazioni specifiche per la categoria vengono elencate con l'opzione Installa. La procedura guidata consente di installare ciascuna applicazione singolarmente o di fare clic su Installa tutto per installare tutte le applicazioni nella categoria. Verrà richiesta l'autorizzazione a installare ciascuna applicazione.

Cerca

- Toccare l'icona di ricerca (lente) per ricercare quanto segue:
  - Nuovi rilasci - un elenco delle app rilasciate di recente appare quando non viene digitato alcun testo nella barra di ricerca
  - Digitare qualsiasi testo e il campo ricerca predirà dinamicamente e visualizzerà le applicazioni corrispondenti.
  - Il conteggio risultato ricerca viene visualizzato come intestazione secondaria
  - È possibile toccare il pulsante Installa per installare un'applicazione senza navigare nella pagina dettagli.

Installazione di un'app - Stati pulsante

- Poiché l'installazione dell'app richiede che il server elabori la richiesta ed effettui il push dell'app sul dispositivo, il pulsante di installazione non mostrerà i progressi in tempo reale
- Il pulsante di installazione cambia stato da Installa > Richiesto > Installato.
- Appare un messaggio di avviso, per la prima volta, a indicare che è richiesta un'installazione.
- L'avviso appare anche quando si tocca il pulsante "Richiesto".
- Lo stato Installato non è un pulsante.

Applicazioni e banner in evidenza

- La scheda Funzionalità è visibile in base alla configurazione dell'amministratore.
- La scheda In evidenza è la pagina di destinazione predefinita quando non sono disponibili aggiornamenti.
- Il Banner app in evidenza visualizza un'applicazione nel banner.
- L'app in evidenza contiene un elenco di tutte le applicazioni in evidenza.

Notifica aggiornamento applicazione

- Go invia una notifica quando sono disponibili aggiornamenti delle applicazioni. La notifica non visualizza il nome dell'applicazione.
- Se si tocca la notifica aggiornamento applicazione, si passerà alla pagina Tutte le app in Apps@Work.
- Nell'applicazione Go, l'icona della scheda Apps@Work mostra un conteggio badge del numero di applicazioni con aggiornamenti in sospeso.
- Nella scheda Apps@Work, la sezione secondaria Aggiornamenti disponibili appare sotto la scheda Tutte le app e visualizza il conteggio delle applicazioni disponibili per l'aggiornamento.
- Un'icona con un punto rosso viene visualizzata per ogni applicazione che richiede un aggiornamento.

Impostazioni-Dispositivi personali

- La scheda Dispositivi personali è stata ora spostata sotto Impostazioni.
- Se si tocca la notifica aggiornamento applicazione, si passerà alla pagina Tutte le app in Apps@Work.
- Nell'applicazione Go, l'icona della scheda Apps@Work mostra un conteggio badge del numero di applicazioni con aggiornamenti in sospeso.
- Nella scheda Apps@Work, la sezione secondaria Aggiornamenti disponibili appare sotto la scheda Tutte le app e visualizza il conteggio delle applicazioni disponibili per l'aggiornamento.
- Un'icona con un punto rosso viene visualizzata per ogni applicazione che richiede un aggiornamento.

18. Abilitare l'Autenticazione Kerberos tra Ivanti Neurons per MDM e il server SCEP

È possibile utilizzare l'autenticazione Kerberos per comunicare tra Ivanti Neurons per MDM e SCEP. Le sezioni seguenti illustrano come abilitare l'autenticazione Kerberos sui server SCEP e Ivanti Neurons per MDM.

> Questa funzione sarà attiva quando sarà disponibile la versione 93 del Connettore Ivanti Neurons per MDM.

Passaggi di pre-configurazione

1. Controllare quale account di servizio è in uso per il servizio SCEP sul server SCEP.
2. Sul server SCEP, verificare che l'account di servizio sia membro del gruppo IIS_USRS locale.
3. Sul modello di certificato del server CA in fase di provisioning, verificare che l'account di servizio abbia l'autorizzazione di registrazione.

Configurazione dei server Windows

1. Eseguire il seguente comando su un controller di dominio:
   setspn -s http/<SCEP-SERVER-FQDN> <domain>\<service account>
2. In **Utenti e computer Active Directory**, fare clic sulla scheda **Delegazione** dell'account di servizio:
   1. Sotto **Ritenere affidabile questo utente solo per la delega ai servizi specificati**, selezionare **Usa solo Kerberos**.
   2. Fare clic su **Aggiungi** e aggiungere il nome del server SCEP.
   3. Selezionare il servizio HTTP.
   4. Fare clic su **OK**.
3. Eseguire le seguenti operazioni sul server IIS per assicurarsi che le credenziali di Pool di applicazione siano utilizzate per decifrare i ticket Kerberos:
   1. Verificare che il Pool di applicazione SCEP sia in esecuzione con l'account di servizio verificato in precedenza.
   2. Per abilitare useAppPoolCredentials, sulla pagina web Microsoft SCEP Admin (mscep_admin) o Microsoft SCEP (mscep), selezionare **Editor configurazioni > System.webServer > Sicurezza > Autenticazione > Autenticazione Windows** e impostare il valore su useAppPoolCredentials=True.
4. Disabilitare **Autenticazione anonima** sulla pagina web Microsoft SCEP Admin (mscep_admin) selezionando **Autenticazione > Autenticazione anonima** e facendo clic su **Disabilita**.
5. Disabilitare l'autenticazione in modalità Kernel nelle impostazioni avanzate dell'autenticazione di Windows.

> Assicurarsi di utilizzare **Negozia** come prima opzione nel servizio di autenticazione.

6. Disabilitare l'autenticazione in modalità Kernel nella pagina web delle impostazioni avanzate di autenticazione Windows.
7. Riavviare il servizio IIS.

Configurazione di Kerberos

Questa sezione illustra come configurare Kerberos sul server Ivanti Neurons per MDM.

Configurazione delle impostazioni di Kerberos in Ivanti Neurons per MDM

Navigare in **Amministratore > Infrastruttura > Kerberos**, inserire le seguenti impostazioni come indicato nella tabella:

Sezione IU	Scelta
L'area di autenticazione Kerberos di Active Directory	IVANTI.COM
Server del centro distribuzione chiavi (KDC) corrispondente	kdc.ivanti.com
Credenziali utente servizio	utente@areadiautenticazione Ad esempio: utenteservizio@IVANTI.COM
Domini per la comunicazione in uscita con Servizi certificati Microsoft AD (i nomi host non fanno distinzione tra maiuscole e minuscole e devono terminare con .ivanti.com o .IVANTI.COM) Server SCEP o NDES: è possibile utilizzare anche nomi di host, ad esempio: ndes.ivanti.com o scep.ivanti.com.	

Abilitazione dell'autenticazione Kerberos sulla configurazione di Registrazione certificato Microsoft SCEP su un'autorità di certificazione esistente

Eseguire le seguenti operazioni per abilitare l'autenticazione Kerberos su un'autorità di certificazione esistente:

1. In Ivanti Neurons per MDM, selezionare **Amministratore > Infrastruttura > Gestione certificati**.
2. Selezionare il tipo di autorità di certificazione con l'opzione **Esterna**.

> Questi tipi di autorità di certificazione esterna devono essere indicati come Microsoft.

3. Dal menu a discesa **Azioni**, selezionare **Modifica**.
4. Nella finestra **Modifica CA esterna**, selezionare la casella di controllo **Preferisci autenticazione Kerberos** per abilitare l'autenticazione Kerberos.

Abilitazione dell'autenticazione Kerberos sulla configurazione di Registrazione certificato Microsoft SCEP per una nuova autorità di certificazione

Eseguire le seguenti operazioni per abilitare l'autenticazione Kerberos per una nuova autorità di certificazione:

1. In Ivanti Neurons per MDM, selezionare **Amministratore > Infrastruttura > Gestione certificati**.
2. Selezionare l'opzione **+Aggiungi**.
3. Nella finestra **Aggiungi autorità di certificazione**, selezionare l'opzione **Connetti a un'Autorità di certificazione SCEP in loco**.
4. Fare clic su Continua.
5. Nella finestra **Aggiungi autorità di certificazione esterna**, eseguire i seguenti passaggi:
    1. Selezionare l'opzione **Microsoft** dal menu a tendina **Tipo autorità di certificazione**.
    2. Selezionare la casella di controllo **Preferisci autenticazione Kerberos** per abilitare l'autenticazione Kerberos.
    3. Compilare tutti i campi richiesti.

4. Fare clic su **Fine**.

19. Guida per l'amministratore a Ivanti Neurons for MDM 127

Settembre 2026

Con un approccio moderno alla sicurezza mobile, Ivanti Neurons for MDM offre soluzioni per la Unified Endpoint Management (UEM) in un'infrastruttura altamente scalabile, sicura e semplice da aggiornare, che supporta milioni di dispositivi in tutto il mondo.

{{Se la propria lingua non è disponibile}}

Riepilogo delle nuove funzionalità

Visualizza come PDF

Video

20. Welcome

21. Welcome CSH

22. Gestione aggiornamenti di Windows

In quanto amministratore, è possibile visualizzare e approvare gli aggiornamenti segnalati dai dispositivi Windows che si desidera aggiornare tramite Gestione aggiornamenti di Windows. Questa funzione consente di evitare l'installazione di aggiornamenti non necessari o non verificati nei dispositivi.

La funzione Gestione aggiornamenti richiede che i dispositivi siano impostati con la configurazione **Aggiornamenti software** e l'opzione **Richiedi approvazione aggiornamenti** attivata. I dispositivi riportano gli aggiornamenti da installare e attendono l'approvazione solo se viene applicata questa configurazione.

Gestione degli aggiornamenti

1. Andare su **Amministratore > Aggiornamenti di Windows**. Nella pagina vengono visualizzati i seguenti dettagli degli aggiornamenti.
   Data creazione: la data di creazione dell'aggiornamento.**Titolo**: descrive il tipo di aggiornamento e il numero dell'articolo Knowledge Base.

> Facendo clic sull'aggiornamento viene visualizzata la descrizione.

Classificazione: classifica il tipo di aggiornamento in una delle seguenti categorie:

- Aggiornamenti critici
- Aggiornamenti definizione
- Aggiornamenti driver
- Aggiornamenti sulla sicurezza
- Aggiornamenti
- Upgrade
- Rollup di aggiornamento

Distribuzione: la distribuzione eseguita per l'aggiornamento. Ad esempio, viene visualizzato **Tutti** quando l'aggiornamento è distribuito a tutti i dispositivi.

> Se l'aggiornamento viene distribuito a un numero specifico di gruppi, viene visualizzato il conteggio della distribuzione. Ad esempio, viene visualizzato 3 se la distribuzione è eseguita solo per 3 gruppi.

2. Inoltre, è possibile vedere se un aggiornamento è stato distribuito o meno ai dispositivi richiesti. Le colonne seguenti contengono numeri che indicano il numero di dispositivi presenti nelle diverse categorie di aggiornamenti:
   - Dispositivi idonei
   - Dispositivi installati
   - Dispositivi non riusciti
   - Dispositivi in attesa di riavvio

Facendo clic su uno di questi numeri, si verrà indirizzati alla vista filtrata della pagina Dispositivi per conoscere lo stato degli aggiornamenti ed eseguire le azioni richieste.
Rivedere gli aggiornamenti e selezionare la voce da distribuire ai dispositivi facendo clic sulla relativa casella di controllo.

3. In **Azioni**, fare clic su **Imposta distribuzione**.
4. Nella finestra **Distribuisci aggiornamenti Windows**, selezionare una delle seguenti opzioni di distribuzione:
   Tutti i dispositivi: gli aggiornamenti vengono distribuiti a tutti i dispositivi.
   Nessun dispositivo: gli aggiornamenti non vengono distribuiti ai dispositivi.**Personalizzata**: gli aggiornamenti vengono distribuiti a specifici gruppi di dispositivi.
5. Fare clic su **Salva**.

Ricerca e applicazione di filtri agli aggiornamenti

È possibile cercare ed applicare filtri agli aggiornamenti in base ai seguenti criteri:

- ID articolo Knowledge Base
- Distribuzione configurata

Applicazione di filtri in base ad ID articolo Knowledge Base

1. Nella pagina **Gestione aggiornamenti di Windows**, digitare l'ID della Base di conoscenza nel campo di ricerca rapida (solo il numero nel campo Cerca).
   Esempio: per KB4056892 digitare 4056892. L'aggiornamento corrispondente ai criteri di ricerca viene visualizzato nella pagina.

> È possibile cercare ulteriori informazioni sull'aggiornamento facendo clic sui collegamenti **Assistenza** e **Altre informazioni**. Il collegamento **Assistenza** indirizza alla pagina Web Microsoft che fornisce informazioni di supporto sui prodotti per l'aggiornamento, mentre il collegamento **Altre informazioni** indirizza alla pagina Web Microsoft che mostra ulteriori informazioni sull'aggiornamento, ad esempio l'articolo Knowledge Base.

Applicazione di filtri in base a distribuzione configurata:

Nella pagina **Gestione aggiornamenti di Windows**, selezionare una delle seguenti opzioni di filtraggio in base alla distribuzione configurata:

- **Tutti**: mostra tutti gli aggiornamenti.
- **Configurata**: mostra l'elenco degli aggiornamenti distribuiti ai dispositivi.
- **Non configurata**: mostra l'elenco degli aggiornamenti per i quali la distribuzione non è specificata.

> I filtri configurati e non configurati sono basati sulla distribuzione eseguita, che può anche essere impostata su **Nessuna**.

Visualizzazione di aggiornamenti per un dispositivo

Per visualizzare le informazioni dettagliate sugli aggiornamenti specifici per un dispositivo:

1. Andare in **Dispositivi > Dispositivi**.
2. Fare clic sul nome di un dispositivo per visualizzare la pagina dei dettagli.
3. Andare alla scheda **Aggiornamenti**. Vengono visualizzati gli aggiornamenti per il dispositivo in sospeso (aggiornamento approvato dall'amministratore ma non riportato come installato sul dispositivo), non riusciti e installati.

È inoltre possibile vedere le notifiche sui nuovi aggiornamenti di Windows disponibili nella pagina Notifiche sotto il Dashboard. La notifica include la data di creazione della notifica, il numero di notifiche disponibili e lo scopo della notifica. La notifica degli aggiornamenti Windows è visibile anche nell'angolo in alto a destra del portale Amministratori.