ivanti

NMDM Admin Guide ZHTW

ivanti

CONTENTS

1. 關於 Ivanti Neurons for MDM 9
2. 新功能摘要 10
3. 影片 13
4. 開始使用 16
    4.1. 設定 macOS 裝置 23
    4.2. 設定和使用註冊確認電子郵件 26
    4.3. 設定和使用原則遵循通知電子郵件 27
    4.4. 隨選即用功能 28
    4.5. 準備 Android Enterprise 裝置支援 29
5. 儀表板 30
    5.1. 使用小工具 31
    5.2. App 深入解析 36
    5.3. 使用排程報告 40
    5.4. 使用自訂報告 46
6. 使用者 53
    6.1. 新增使用者 54
    6.2. 使用者群組 58
    6.3. 使用者設定 62
    6.4. 使用者品牌 71
    6.5. 透過 Apple 商務管理進行使用者註冊 72
    6.6. 使用者授權 80
    6.7. 管理使用者 81
        6.7.1. 新增用於 Cisco ISE 作業的 API 使用者 82
        6.7.2. 指派角色至使用者 83
        6.7.3. 使用者角色 85
        6.7.4. 搜尋與篩選使用者 87
        6.7.5. 指派使用者至使用者群組 90
        6.7.6. 邀請使用者 91
        6.7.7. 啟用與停用使用者 92
        6.7.8. 針對多次的管理員登入進行管理 94
        6.7.9. 變更密碼 95
        6.7.10. 傳送訊息 97
        6.7.11. 將使用者從使用者群組中移除 99
        6.7.12. 刪除使用者 100
        6.7.13. 匯出使用者 101
        6.7.14. 指派自訂屬性給使用者 102
        6.7.15. 移除使用者的自訂屬性 103
        6.7.16. 變更使用者地區設定 104
        6.7.17. 編輯使用者名稱 105
        6.7.18. 退出位置資料收集 106
        6.7.19. 逾時資訊 107
        6.7.20. 退出系統使用量分析 108
        6.7.21. 透過產生 PIN 進行裝置註冊 109
7. 裝置 110
    7.1. 開始使用裝置 111
    7.2. 裝置群組 124
    7.3. 未受管理的裝置 130
    7.4. App 庫存 131
    7.5. 管理裝置 134
        7.5.1. 部署 Apple 裝置 136
        7.5.2. 部署 Windows 裝置 144
        7.5.3. 在 macOS 裝置上設定 Apple 遠端桌面 147
        7.5.4. 裝置註冊 (iOS、macOS 及 Android) 148
        7.5.5. 裝置註冊（Windows 10+ PC 和 Microsoft HoloLens 2） 151
        7.5.6. 本機管理密碼解決方案 (LAPS) 154
        7.5.7. 佈建使用 PIN 碼註冊套件 156
        7.5.8. 使用 Windows 裝置大量註冊 159
            7.5.8.1. Ivanti 大量註冊 160
        7.5.9. 變更密碼設定 162

7.5.10. 變更裝置名稱 163
7.5.11. 搜尋與篩選裝置 164
7.5.12. 使用裝置擁有者 166
7.5.13. 搭配工作描述檔的受管理裝置 172
7.5.14. 使用 Android 大量註冊 173
7.5.15. 使用 CSV 檔案上傳進行大量註冊 175
7.5.16. Device_to_User_BulkEnrollment 177
7.5.17. 使用 Samsung Knox Mobile Enrollment 178
7.5.18. 註冊 Oculus 裝置 179
7.5.19. 在裝置上啟用 Bluetooth 181
7.5.20. 排程 iOS 更新 182
7.5.21. 重新安裝 iOS 系統 App 183
7.5.22. 指派裝置給新使用者 184
7.5.23. 重新指派 Android 裝置 185
7.5.24. 強制裝置登記 186
7.5.25. 定位裝置 187
7.5.26. 鎖定裝置 188
7.5.27. 管理遺失模式下的 Apple 裝置 189
7.5.28. 管理遺失模式下的 Android 裝置 191
7.5.29. 要求偵錯日誌 193
7.5.30. Apple_Enhanced_Logging 194
7.5.31. 淘汰裝置 195
7.5.32. 放棄裝置擁有權 196
7.5.33. 清除裝置 197
7.5.34. 刪除裝置 198
7.5.35. 解除鎖定裝置 199
7.5.36. 重新啟動或關閉裝置 201
7.5.37. 清除限制密碼 (僅限 iOS) 203
7.5.38. 刪除裝置的 Sentry 關聯 204
7.5.39. 指派自訂屬性給裝置 205
7.5.40. 移除裝置的自訂屬性 206
7.5.41. 同步並擷取 App 回饋 207
7.5.42. 設定韌體密碼 208
7.5.43. 重新發行新的個人復原金鑰 209
7.5.44. 設定或者變更復原鎖定 210
7.5.45. Apple 存取權限管理 211
7.5.46. 群組原則註冊 212
8. App 213
8.1. 「App Catalog「 214
8.2. 宣告式裝置管理 (DDM) 應用程式管理 230
8.2.1. DDM 應用程式管理設定 232
8.3. Apps@Work (iOS、Android、Windows 和 macOS) 235
8.4. iOS Apps@Work AppStore 功能 238
8.5. iOS Go 進階功能 241
8.6. 檢視 App 詳細資料 246
8.7. App 配置 249
8.8. 將自訂屬性指派給應用程式 264
8.9. Android 受管理的配置 265
8.10. 管理 Google Play app 270
8.11. 從 App Catalog 刪除 App 271
8.12. 升級內部開發的 App 272
8.13. 搜尋 Android App 的套件名稱 273
8.14. 類別 274
8.15. 發佈篩選 275
8.16. 排除或分發應用程式 278
8.17. 評論 279
8.18. Apple Apps and Books 281
8.19. 目錄設定 289
8.20. 部署 app 相依性 292
8.21. 使用 Android Enterprise 部署 Divide Productivity 295
8.22. 設定 Provisioner app 297
8.23. 管理 Windows 應用程式 299

8.24. Ivanti Bridge 302
9. 內容 307
9.1. 管理內容 308
9.2. 類別 310
10. 組態 311
10.1. 使用配置 312
10.2. 建立使用者自助式入口網站配置 323
10.3. 自訂配置 324
10.4. 使用自訂組態將 SyncML 推送至裝置 326
10.5. 首頁畫面版面配置 327
10.6. App 控制配置：控制每台裝置要安裝哪些 App 329
10.7. App 通知配置 331
10.8. 滙出配置 333
10.9. 優先排序配置 334
10.10. 管理配置 335
10.10.1. 配置類型 336
10.10.2. 變數 347
10.10.3. AppConnect 組態 352
10.10.3.1. AppConnect 概覽 353
10.10.3.2. AppConnect 密碼 354
10.10.4. 安全性配置 355
10.10.4.1. Android Enterprise 357
10.10.4.2. Apple 金輪證明 358
10.10.4.3. 應用程式隱私權預設值 359
10.10.4.4. 編輯 Android Enterprise 預設組態 361
10.10.4.5. 設定 Android Enterprise 362
10.10.4.6. Android Enterprise: 工作受控裝置非 GMS 模式 (AOSP) 368
10.10.4.7. Android 工作挑戰 369
10.10.4.8. 憑證配置 374
10.10.4.9. 憑證透明度 376
10.10.4.10. 憑證撤銷檢查配置 377
10.10.4.11. 建立自發的單一應用程式模式組態 378
10.10.4.12. 建立 DNS Proxy 組態 379
10.10.4.13. 裝置記錄組態 380
10.10.4.14. 磁碟管理組態 382
10.10.4.15. Android 加密 383
10.10.4.16. 加密 DNS 384
10.10.4.17. 外部智慧設定 387
10.10.4.18. 威脅防護 388
10.10.4.19. FileVault 2 389
10.10.4.20. FileVault 復原金鑰 390
10.10.4.21. FileVault 選項配置 391
10.10.4.22. 身份憑證 392
10.10.4.23. Apple 啟用鎖定配置 397
10.10.4.24. iOS 自訂配置 400
10.10.4.25. 智慧設定 401
10.10.4.26. iOS 限制 404
10.10.4.27. 會議室顯示器 419
10.10.4.28. 鍵盤設定 420
10.10.4.29. 鎖定與單一應用：Android 裝置管理模式 422
10.10.4.30. 設定 Android 的單一應用模式 425
10.10.4.31. 設定 Android 共用裝置單一應用 427
10.10.4.32. 鎖定與單一應用：Android Enterprise 428
10.10.4.33. 鎖定與單一應用：Samsung Knox Standard 447
10.10.4.34. 本機管理員密碼解決方案組態 451
10.10.4.35. macOS 防火牆 452
10.10.4.36. macOS 限制 453
10.10.4.37. macOS AppStore 限制 459
10.10.4.38. macOS 燒錄光碟限制 460
10.10.4.39. 允許的媒體控制 (已棄用) 461
10.10.4.40. macOS Finder 設定 464
10.10.4.41. macOS 核心擴充原則 465

10.10.4.42. 適用於 macOS 的 Mobile@Work ... 466
10.10.4.43. macOS 軟體更新規則配置 ... 471
10.10.4.44. 憑證偏好設定 ... 472
10.10.4.45. Active Directory (macOS) ... 473
10.10.4.46. 身分偏好設定 ... 476
10.10.4.47. Office 365 自動帳戶建立 (macOS) ... 477
10.10.4.48. 驗證 ... 479
10.10.4.49. Apple 應用程式目錄 ... 480
10.10.4.50. 受管理的網域 ... 481
10.10.4.51. 密碼組態 ... 482
10.10.4.52. 隱私權偏好設定 (macOS) ... 485
10.10.4.53. 隱私權配置 ... 487
10.10.4.54. 用戶端隱私權聲明資訊 ... 490
10.10.4.55. Ivanti Go Client 設定 ... 491
10.10.4.56. Siri 設定 ... 493
10.10.4.57. 服務組態檔案組態 ... 494
10.10.4.58. 軟體更新 ... 495
10.10.4.59. 軟體更新設定組態 ... 502
10.10.4.60. 安全性喜好設定配置 ... 505
10.10.4.61. 時間伺服器 ... 506
10.10.4.62. Web 內容篩選 ... 507
10.10.4.63. Windows 防火牆 ... 510
10.10.4.64. Windows 資訊保護 ... 513
10.10.4.65. Windows 限制 ... 517
10.10.4.66. Windows Desktop 的限制 ... 522
10.10.4.67. Windows 10 的桌面設定 ... 524
10.10.4.68. Windows Hello 企業版配置 ... 526
10.10.4.69. Windows AI 管理組態 ... 527
10.10.4.70. Play Integrity (前身為 SafetyNet Attestation) ... 529
10.10.4.71. 進階 Android 密碼與鎖定畫面 ... 530
10.10.4.72. Microsoft Defender for Endpoint ... 531
10.10.4.73. 憑證型驗證 ... 532
10.10.5. 使用者資源配置 ... 533
10.10.5.1. CalDAV 配置 ... 534
10.10.5.2. CardDAV 配置 ... 535
10.10.5.3. Google 配置 ... 536
10.10.5.4. 電子郵件配置 ... 537
10.10.5.5. Exchange 組態 ... 540
10.10.5.6. 字型配置 ... 544
10.10.5.7. 訂閱的行事曆配置 ... 545
10.10.5.8. 建立 Web 剪輯組態 ... 546
10.10.5.9. Office 365 安裝 ... 548
10.10.5.10. Windows GPO 設定 ... 550
10.10.5.11. BitLocker Encryption 配置 ... 552
10.10.6. 企業網路存取配置 ... 556
10.10.6.1. AirPlay 配置 ... 557
10.10.6.2. AirPrint 配置 ... 558
10.10.6.3. Always-on VPN 組態 ... 559
10.10.6.4. 預設的 App 執行時期權限 ... 562
10.10.6.5. 教育 ... 564
10.10.6.6. 全域 Proxy 配置 ... 565
10.10.6.7. 全域 Proxy 組態 - Android ... 566
10.10.6.8. LDAP 配置 ... 567
10.10.6.9. macOS Server 配置 ... 568
10.10.6.10. Tunnel ... 569
10.10.6.11. 設定 AppTunnel ... 570
10.10.6.12. 個別 App VPN 組態 ... 575
10.10.6.13. 單一登入配置 ... 583
10.10.6.14. 網路轉送組態 ... 590
10.10.6.15. iOS 多位使用者安全登入 ... 592
10.10.6.16. Android APN 設定配置 ... 594
10.10.6.17. VPN 組態 ... 598

10.10.6.18. 隨選即用 VPN ... 610
10.10.6.19. Wi-Fi 組態 ... 617
10.10.7. 行動網路配置 ... 625
10.10.7.1. APN 配置 ... 626
10.10.7.2. 行動數據 ... 627
10.10.7.3. 行動數據私人網路組態 ... 630
10.10.7.4. iOS 電信商預設配置 ... 631
10.10.7.5. 增強型 5G 網路切片組態 ... 632
10.10.7.6. eSIM 配置 ... 634
10.10.8. 其他配置 ... 636
10.10.8.1. 相關聯網域組態 ... 638
10.10.8.2. Android 檔案傳輸組態 ... 639
10.10.8.3. Apple TV 配置 ... 642
10.10.8.4. AirPlay 鏡像 ... 643
10.10.8.5. 瀏覽器設定 ... 645
10.10.8.6. 設定 iOS 的單一 App 模式 ... 648
10.10.8.7. 設定 iOS MDM 描述檔 ... 651
10.10.8.8. 設定 macOS MDM 設定檔 ... 652
10.10.8.9. 內容快取 ... 653
10.10.8.10. 建立 Android 捷徑 ... 656
10.10.8.11. 建立輔助工具設定組態 ... 657
10.10.8.12. 建立螢幕保護程式組態 ... 660
10.10.8.13. 設定使用者的螢幕保護程式 ... 661
10.10.8.14. 裝置名稱設定 ... 662
10.10.8.15. 裝置桌布配置 ... 663
10.10.8.16. EMA 伺服器整合配置 ... 666
10.10.8.17. 省電組態 ... 667
10.10.8.18. 乙太網路組態 (macOS) ... 673
10.10.8.19. Google BeyondCorp 組態 ... 675
10.10.8.20. 鎖定畫面訊息配置 ... 679
10.10.8.21. 登入視窗組態 - macOS ... 681
10.10.8.22. macOS 系統延伸配置 ... 682
10.10.8.23. 僅限 MAM ... 683
10.10.8.24. 受管理的 Google Play 配置 ... 685
10.10.8.25. 移轉助手設定 ... 686
10.10.8.26. 通知組態 ... 687
10.10.8.27. 列印設定 ... 688
10.10.8.28. 移除膨脹配置 ... 690
10.10.8.29. Safari 擴充功能和設定組態 ... 691
10.10.8.30. Samsung 手機限制配置 ... 694
10.10.8.31. 預設瀏覽器組態 - iOS 和 visionOS ... 695
10.10.8.32. 螢幕共用主機設定組態 ... 696
10.10.8.33. 單一 App 模式配置 ... 697
10.10.8.34. 軟體更新建議頻率配置 ... 699
10.10.8.35. 開始功能表和工作列 ... 700
10.10.8.36. 系統更新組態 ... 702
10.10.8.37. Windows 10 更新管理 ... 706
10.10.8.38. Windows app 排程 ... 708
10.10.8.39. Windows BIOS 配置 ... 709
10.10.8.40. Windows BitLocker ... 717
10.10.8.41. Windows 單一應用配置 ... 718
10.10.8.42. Windows 授權配置 ... 722
11. 政策 ... 723
11.1. 使用原則 ... 724
11.2. 自訂原則 ... 730
11.3. 監控與控制允許的 App ... 750
11.4. 優先排序原則 ... 755
11.5. Windows 硬體原則 ... 756
12. 管理 ... 757
12.1. 系統 ... 758
12.1.1. 屬性 ... 759
12.1.2. 裝置清理設定 ... 764

12.1.3. GDPR 設定檔 ... 768
12.1.4. 通知電子郵件 ... 770
12.1.5. 角色管理 ... 771
12.1.6. 空間 ... 777
12.1.6.1. 空間 ... 778
12.1.6.2. 管理空間 ... 780
12.1.6.3. 空間範例 ... 785
12.1.6.4. 委派裝置 ... 787
12.1.6.5. 委派 App ... 788
12.1.7. 支援管理員 ... 789
12.1.8. 管理 > 系統使用通知 ... 790
12.2. 基礎架構 ... 792
12.2.1. 存取 ... 793
12.2.2. App 清單 ... 794
12.2.3. 匯出稽核追蹤 ... 795
12.2.4. 憑證管理 ... 798
12.2.5. 適用於外部認證授權中心的 SCEP 配置 ... 805
12.2.6. 衍生的憑證提供者 ... 806
12.2.7. 連接器 ... 807
12.2.8. 對 Connector 使用 httpproxy 命令 ... 809
12.2.9. Help@Work ... 810
12.2.10. 基礎架構身份識別 ... 813
12.2.10.1. 設定身份識別提供者 ... 814
12.2.10.2. 使用 SCIM 進行使用者佈建 ... 818
12.2.10.2.1. Entra ID IdP 的使用者佈建 ... 821
12.2.10.2.2. Okta IdP 使用者佈建 ... 826
12.2.11. 設定 LDAP 伺服器 ... 829
12.2.12. Sentry ... 837
12.3. Apple 設定 ... 838
12.3.1. Apple Configurator ... 839
12.3.2. 帳戶導向註冊 ... 841
12.3.3. 裝置註冊 ... 843
12.3.4. 測試版註冊 ... 856
12.3.5. 設定安裝小幫手 ... 857
12.3.6. 安裝 MDM 憑證 ... 858
12.3.7. 商務共享 iPad 裝置 ... 859
12.3.8. School Manager ... 863
12.3.9. 設定 (Apple) ... 866
12.4. 使用 Windows 裝置 ... 868
12.4.1. 設定 Windows Autopilot 描述檔 ... 869
12.4.2. Windows Autopilot 設定檔上的稽核追蹤 ... 875
12.4.3. TenantLockdown CSP ... 876
12.4.4. ADMX (GPO) 瀏覽器 ... 877
12.4.5. 配置 app 庫存間隔 ... 878
12.4.6. 硬體庫存 ... 879
12.5. 使用 Microsoft Azure 進行設置 ... 880
12.5.1. 使用 Microsoft Azure ... 881
12.5.2. Entra ID Windows 10 統一端點管理設定 ... 884
12.5.3. 指派 Entra ID UEM 應用程式 ... 885
12.5.4. 將 Ivanti Neurons for MDM 連線至 Entra ID 使用者來源 ... 886
12.5.5. Azure 租戶 ... 888
12.5.5.1. Azure Tenant Requirements ... 889
12.5.5.2. 將 Intune 授權套用至裝置使用者 ... 890
12.5.5.3. 將 MobileIron 新增為合規性合作夥伴 ... 891
12.5.5.4. 在 Microsoft Endpoint Manager 中建立條件式存取原則 ... 892
12.5.5.5. 將 Microsoft Azure 連線至 Ivanti Neurons for MDM ... 893
12.5.5.6. 建立合作夥伴裝置合規性原則 ... 894
12.5.5.7. 從 Ivanti Neurons for MDM 到 Azure 的裝置狀態報告 ... 896
12.5.5.8. 取消佈建 Azure 租戶 ... 898
12.5.6. 管理 > Microsoft Azure > Office 365 App 保護 ... 899
12.6. 連接 Google App ... 907
12.6.1. 受管理的 Google Play 帳戶 (Android Enterprise 帳戶) ... 908

12.6.2. Android 裝置註冊 911
12.6.3. Android 管理 API 912
12.6.4. Google Apps API 918
12.6.5. 管理 - Android Enterprise 919
12.7. 使用 ChromeOS 裝置 921
12.7.1. ChromeOS 和 Ivanti Neurons for MDM 922
12.7.2. 將 Android 應用程式發佈至 ChromeOS 裝置 923
12.7.3. 新增和分發 ChromeOS 擴充功能應用程式 924
12.7.4. ChromeOS 藍圖組態 925
12.7.5. 裝置動作 926
12.7.6. 常見問題 927
12.7.7. 建議的評估步驟 929
12.8. 韌體管理 930
12.8.1. 註冊 Zebra OTA 服務 931
12.8.2. Samsung E-FOTA 授權管理 (已停用) 932
12.9. 管理指令碼和檔案 933
12.9.1. 所有指令碼 934
12.9.2. 檔案 938
12.10. 品牌化 939
12.10.1. 管理 > Apple 應用程式目錄 (品牌) 940
12.10.2. 將 Android App Catalog 品牌化 941
12.10.3. 管理 > Android 單一應用品牌化 942
12.10.4. 將電子郵件範本品牌化 943
12.10.5. 自助式入口網站 951
12.10.6. 自助式入口網站 (品牌化) 953
12.10.7. 多位使用者登入 (Webclip) 品牌 954
12.10.8. 組織 955
12.11. 新增非 iOS 裝置管理 956
13. 套件 957
13.1. 升級 961
14. 裝置授權 963
14.1. 租戶停權 964
15. 開啟支援票證 965
16. 第三方屬性 966
17. Apps@Work 967
18. 在 Ivanti Neurons for MDM 和 SCEP 伺服器之間啟用 Kerberos 驗證 969
19. Ivanti Neurons for MDM 127 管理員指南 971
20. Welcome 972
21. Welcome CSH 973
22. Windows Update 管理 974

1. 關於 Ivanti Neurons for MDM

Ivanti Neurons for MDM 是確保行動安全的新型方式，在高度可擴充、安全且方便更新的基礎架構中提供統一端點管理 (UEM) 解決方案，該基礎架構支援全球數百萬部裝置。

- 立即更新：獲得自動軟體與安全性更新，並使用新推出的新功能。
- 隨選擴充性：視業務需求擴充您的部署，無需擔心容量規劃。
- 將硬體成本降至最低：無需維護內部部署硬體，雲端型服務無需管理。
- 高運作時間和高可用性。
- 將現有的投資提升到最大：將 IT 資源從硬體維護重新分配給更多策略性工作，為公司帶來附加價值。

您可以檢視此版本中可用新功能的摘要。

2. 新功能摘要

本節摘述本版本包含的新功能與增強功能。 此外，也會在這些功能和增強功能的參照說明文件可用時提供。

一般功能與增強功能

Android 功能

iOS、macOS、watchOS、visionOS 和 tvOS 功能

Windows 功能

ChromeOS 功能

行動威脅防護功能

一般功能與增強功能

- **目錄層級控制**: 新增受監管 iOS 裝置上 **AllowDownloadsOverCellular** 的目錄層級控制項 (在 iOS 26.0 中引入)，以及 AlwaysOn、AlwaysOff 和 StoreSettings 選項 (預設 StoreSettings)。 安裝應用程式組態預設會繼承目錄的目前選取，並在設定後，會覆寫目錄；升級後，新增的應用程式會繼承目錄選取。 由使用者啟動的安裝和更新始終遵循儲存區設定。
- **增強的 macOS 套件 ID 處理**: 透過在應用程式上傳期間自動偵測和填入正確的套件 ID，並確保將相同的套件 ID 傳送至裝置，改善 macOS 內部 PKG 應用程式部署。 這可提高應用程式識別準確性、解決伺服器與裝置之間的安裝狀態不相符問題，並改善安裝狀態報告。 部署後鎖定之前，可以在上傳期間檢閱和編輯套件 ID。
- v已安裝應用程式的套件 ID 可見性：裝置詳細資料頁面的已安裝應用程式區段現在包含「套件 ID」欄，可在頁面設定中顯示或隱藏。
- **自動重試失敗的 Android 應用程式安裝**: 進入錯誤安裝狀態的 Android 應用程式安裝現在會在裝置註冊後一小時自動重試。 安裝命令每 30 分鐘重新傳送一次，最多嘗試五次，以提高應用程式部署成功率。
- **空間裝置移動稽核追蹤**：新增「在空間中啟用裝置註冊和取消註冊的稽核追蹤」設定，以追蹤裝置在空間之間的移動。 如需更多資訊，請參閱匯出稽核追蹤。
- **裝置清理設定的作業系統平台篩選器**: 管理員現在可以在移除已淘汰和待淘汰裝置時，依作業系統平台篩選裝置清理動作。 預設情況下，所有支援的平台都會保持選取狀態，保留現有的行為。 管理員可以修改選擇，並根據需要將清理操作限制在特定平台上。 如需詳細資訊，請參閱裝置清理設定。
- **Office 365 應用程式保護原則同步**: 以前，管理員可以在建立或修改應用程式保護原則時直接在 內選取應用程式。 Microsoft 已淘汰用來擷取可用應用程式清單的 API，導致 中的受保護應用程式清單顯示為空白。 Microsoft Office 365 應用程式保護原則管理已更新，以符合 Microsoft Intune 中的變更。 Intune 中設定的應用程式現在會自動同步到 ，以確保受保護應用程式持續可見。 雖然仍可從 移除應用程式，但新的應用程式指派必須在 Microsoft Intune 中設定，並會自動同步顯示。
- **空間裝置移動稽核記錄**: 管理員現在可以透過稽核記錄追蹤空間之間的裝置移動。 啟用後，每當裝置從一個空間移除並新增至另一個空間時，新的稽核設定都會記錄事件，以便更清楚地檢視自動化和規則式空間指派。 如需更多資訊，請參閱稽核追蹤。
- **使用裝置群組進行自動自訂屬性指派**: 管理員現在可以在裝置群組層級指派自訂屬性。 屬於裝置群組成員的裝置會自動繼承設定的屬性值，減少手動設定，並協助確保裝置分類一致。 有關更多資訊，請參閱裝置群組。
- **作業系統層級裝置註冊限制**: 依平台限制裝置註冊，僅允許核准的 **Apple**、**Android** 和 **Windows** 裝置註冊。 如需詳細資訊，請參閱使用者設定。

Android 功能

- **支援執行緒網路**: 現在支援工作受管理裝置模式和受管理裝置模式下的**執行緒網路**。 如需更多資訊，請參閱鎖定與 Kiosk: Android Enterprise。

- **增強了鎖定與 Kiosk**：在**鎖定與 Kiosk：Android Enterprise 組態**中新增了**禁止變更近場通訊**鎖定設定。
  如需更多資訊，請參閱鎖定與 Kiosk: Android Enterprise。
- **Ivanti Go Android 中的支援索引標籤**: 現在 **Ivanti Go 用戶端設定組態**中提供了**支援聯絡人組態**欄位。 如需更多資訊，請參閱 Ivanti Go 用戶端設定。
- **增強了 SIM 卡通知**: 裝置報告 SIM 移除或 SIM 停用狀態時， 現在會通知管理員。 通知包含**裝置詳細資訊**、**使用者名稱**、**日期和時間**、**SIM 插槽資訊** (SIM 插槽 1 或 SIM 插槽 2)、**SIM 類型** (eSIM 或實體 SIM) 和 **SIM 電話號碼**。 此增強功能可協助管理員快速識別和檢閱受管理裝置上的 SIM 相關變更。 如需詳細資訊，請參閱開始使用裝置。
- **使用應用程式時避免更新**：管理員現在可防止受管理的 Android 應用程式在使用者使用期間進行更新。 啟用了**應用程式在使用中時不更新**時，應用程式更新會延遲，直到使用者關閉應用程式或將其移至背景，有助於減少使用中工作階段期間的中斷。 如需更多資訊，請參閱應用程式組態。
- **鎖定原則變更後維持 Kiosk 模式**：新增在鎖定原則變更後維持 Kiosk 模式的支援。 裝置在鎖定原則更新後會自動返回資訊站模式，減少手動干預，並將專用裝置的中斷情況降至最低。 如需更多資訊，請參閱鎖定與 Kiosk: Android Enterprise。
- **啟用未遮蔽內容的通知**：新增在裝置擁有者裝置上設定鎖定畫面通知可見性的支援。 管理員可以在鎖定畫面上顯示、隱藏或遮蔽通知內容，在維持通知功能的同時協助保護敏感資訊。 如需資訊，請參閱進階 Android 密碼與鎖定畫面。
- **大量註冊描述檔期間的裝置至使用者對應支援**：新增對大量註冊描述檔中裝置至使用者對應的支援。 管理員可以透過大量註冊 CSV 檔案或在手動新增裝置期間將特定使用者指派給每個裝置，以便在註冊期間啟用自動使用者指派，並減少註冊後管理工作。 管理員也可以在裝置註冊前更新使用者指派。 如需詳細資訊，請參閱大量註冊描述檔中的裝置至使用者對應。

iOS、macOS、watchOS、visionOS 和 tvOS 功能

- **改善了 VPP 應用程式的通知**: 現在當 VPP 應用程式與已經作為內部開發的應用程式存在的應用程式相符時， 會通知您。 當您上傳 VPP 權杖或同步包含相同應用程式的套組 ID 時，系統會顯示通知，協助您識別應用程式項目。 如需更多資訊，請參閱 Apple Apps and Books。
- **裝置註冊描述檔的新略過機碼**: 管理員現在可以在建立裝置註冊描述檔時使用下列略過機碼:
  - **略過 Liquid Glass 窗格** (iOS 27.0+ 和 macOS 27.0+)
  - **略過輔助使用外觀窗格** (iOS 27.0+)
    這些略過鍵可讓管理員在裝置註冊期間隱藏特定設定窗格，有助於簡化註冊體驗。 如需詳細資訊，請參閱裝置註冊。
- **支援 DDM 裝置系統健康狀態**: 現在**裝置詳細資訊**頁面上支援 DDM 裝置系統健康狀態。 管理員可以在**裝置組件健康狀況**區段下檢視此狀態，以監控受監管裝置所報告的系統健康狀態。 如需詳細資訊，請參閱開始使用裝置。
- **新增 Apple 裝置的新裝置詳細資料欄位**: 新增**裝置詳細資料**欄位，以便更清楚地檢視 Apple 裝置管理狀態。 管理員現在可以檢視下列詳細資料:
  - 在 iOS 27.0+ 上運作之裝置的**多位使用者模式**。 此欄位指出 iPad 是否設定為共用裝置。
  - 在 iOS 27.0+、macOS 27.0+、tvOS 27.0+、visionOS 27.0+ 和 watchOS 27.0+ 上運作的裝置適用的 **MDM 註冊類型**。
  - **MDM 返回服務**，為 iOS 27.0+ 和 visionOS 27.0+ 上運作的裝置保留應用程式。
    這些欄位可協助管理員直接從裝置詳細資訊頁面檢閱裝置組態和註冊資訊。 如需詳細資訊，請參閱開始使用裝置。
- **支援應用程式隱私權預設值**: 管理員現在可以使用 Apple 裝置宣告式管理 (DDM) 為一個或多個應用程式設定**應用程式隱私權預設值**。 應用程式首次啟動時，使用者會收到單一同意提示，以允許或延遲受支援隱私元件的建議權限，例如相機、麥克風、位置、藍牙和本機網路存取。 如需更多資訊，請參閱應用程式隱私權預設值。

> macOS 27.0+ 受監管裝置現在支援應用程式隱私權預設值組態。

- **新增新的 DDM 應用程式管理屬性**: 將 DDM 應用程式管理屬性 **Apple DDM 應用程式已啟用**欄位新增至「進階搜尋」和裝置清單頁面。 此欄位顯示哪些裝置具有透過 DDM 發佈的應用程式。 管理員可以透過使用者設定開啟此功能。 如需詳細資訊，請參閱開始使用裝置。

- **增強的 macOS 可延伸 SSO 組態**: 更新 macOS 可延伸 SSO 組態以正確對應權杖屬性，例如 **preferred_username** 和 **name**。 這樣可以解決因權杖對使用者對應無效而導致的設定錯誤，並允許將 SSO 描述檔成功部署到裝置。
- **Apple 增強型記錄**: 管理員可以使用 AppleCare 提供的權杖，在支援的 Apple 裝置上啟動 Apple 增強型記錄收集。 裝置詳細資料顯示工作階段狀態、權杖和時間戳記資訊，如有需要，可取消使用中的工作階段。 如需更多資訊，請參閱 Apple 增強型記錄。
- **鎖定模式狀態** (iOS 27+、macOS 27+)：新增支援使用**裝置詳細資料**頁面、**進階搜尋**和裝置群組規則中的**安全鎖定模式**欄位，依鎖定模式狀態檢視和篩選裝置。 此欄位指出裝置是啟用 (**true**) 還是停用 (**false**) 鎖定模式。 如需資訊，請參閱開始使用裝置、裝置群組和自訂原則。
- **macOS 軟體更新設定支援更新**：**macOS 軟體更新設定**組態不再支援 macOS 27 及更新版本的裝置。 此組態現在僅適用於 macOS 26.x 及更早的支援版本。 如需資訊，請參閱 macOS 軟體更新規則組態。
- **限制支援更新** (iOS 27+、macOS 27+)：更新**允許安裝背景安全性改進**和**允許移除背景安全性改進**限制，指出 iOS 27 及更新版本與 macOS 27 及更新版本的裝置不再支援這些限制。 如需資訊，請參閱 iOS 限制和 macOS 限制。
- **Siri 設定組態的更新** (iOS 27.0+、macOS 27.0+、tvOS 27.0+ 和 visionOS 27.0+): 在 Siri 設定組態中新增對於新限制設定的支援。 如需更多資訊，請參閱 Siri 設定。
- **Intelligence 設定組態更新** (iOS 27.0+、macOS 27.0+ 和 visionOS 27.0+)：在 Intelligence 設定組態中新增對新限制設定的支援。 如需資訊，請參閱 Intelligence 設定。
- **Safari 隱私權設定** (iOS 27.0+、macOS 27.0+): 新增對 Safari 擴充和設定組態中的 Safari 隱私權設定的支援，允許管理員使用 Apple 宣告裝置管理 (DDM) 為特定網站設定預設相機和麥克風權限。 如需資訊，請參閱 Safari 擴充功能和設定組態。

Windows 功能

- **支援 Windows 復原備份管理**: 現在可讓您在裝置設定期間啟用 Windows 備份復原，允許加入 Microsoft Entra 的裝置在初始裝置設定期間檢視和復原可用備份，以獲得一致的復原體驗。 如需更多資訊，請參閱部署 Windows 裝置。
- **Windows AI 管理組態**: Windows AI 管理現在支援管理 Microsoft Copilot、Windows Recall 和 Microsoft Paint AI 功能的其他 Windows AI CSP 原則。 管理員可以停用 Copilot 硬體按鍵、移除 Microsoft Copilot 應用程式、停用 Recall 的 AI 資料分析、設定 Recall 快照儲存限制，以及停用 Paint 中的 Image Creator、Cocreator 和 Generative Fill。 也新增了對使用者範圍原則和裝置範圍原則的支援，可更精細地控制 Windows 裝置上的 AI 功能。 如需資訊，請參閱 Windows AI 管理組態。

ChromeOS 功能

行動威脅防護功能

行動威脅防護 (MTD) 保護受管理裝置，防止行動威脅和漏洞影響裝置、網路及應用程式。 有關適用最新版本的 MTD 相關功能，請參閱適用您平台的行動威脅防護 Solution Guide for your platform，位於 Ivanti 產品文件頁面的「行動威脅防護」區段。

> MTD 指南的每個版本包含所有行動威脅防護功能，這些功能曾接受完整測試，而且同時適用於伺服器和用戶端環境。 由於伺服器與用戶端發行版本間的落差，會提供多個新版 MTD 指南，當各項功能均可正常運作時，將提供最終發行版本。

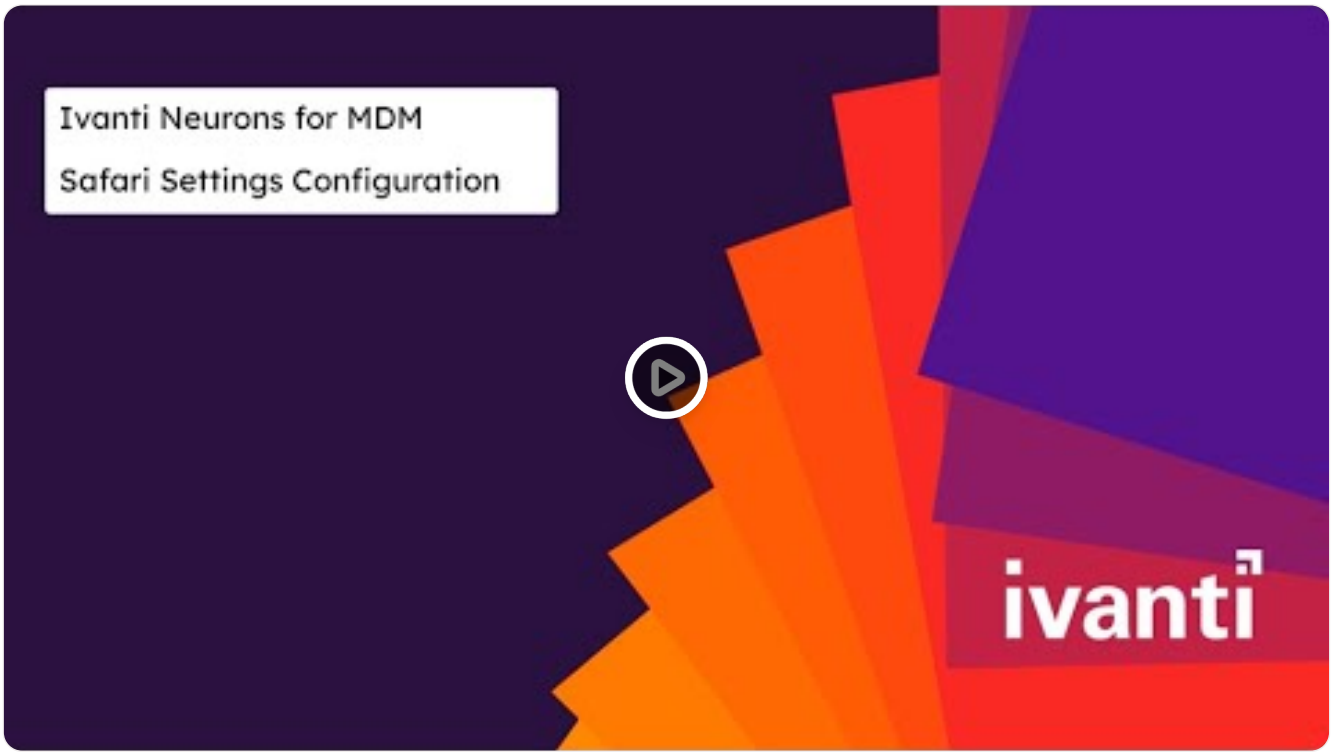
3. 影片

推薦影片


Ivanti N-MDM
Privacy Configuration
ivanti
Copyright © 2025 Ivanti. All rights reserved.


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.



正在尋找 Ivanti Neurons for MDM 中特定特性或功能的視訊？ 在本文件任何頁面的「**這篇文章有用嗎？**」區段中分享您的意見回饋，讓我們知道您的看法。

4. 開始使用

本節提供需要在 Ivanti Neurons for MDM 入口網站上進行互動的功能的設定與使用概覽。 本節包含以下各主題：

- 解決方案概覽
  - 主要特色
  - 架構圖
  - Ivanti Neurons for MDM 應用程式
  - 角色
  - 開始使用
- 在瀏覽器中設定偏好的語言
- Ivanti Neurons for MDM 和 Access 的整合導覽介面
- 管理 Android 裝置的裝置管理 (DA) 模式已棄用

解決方案概覽

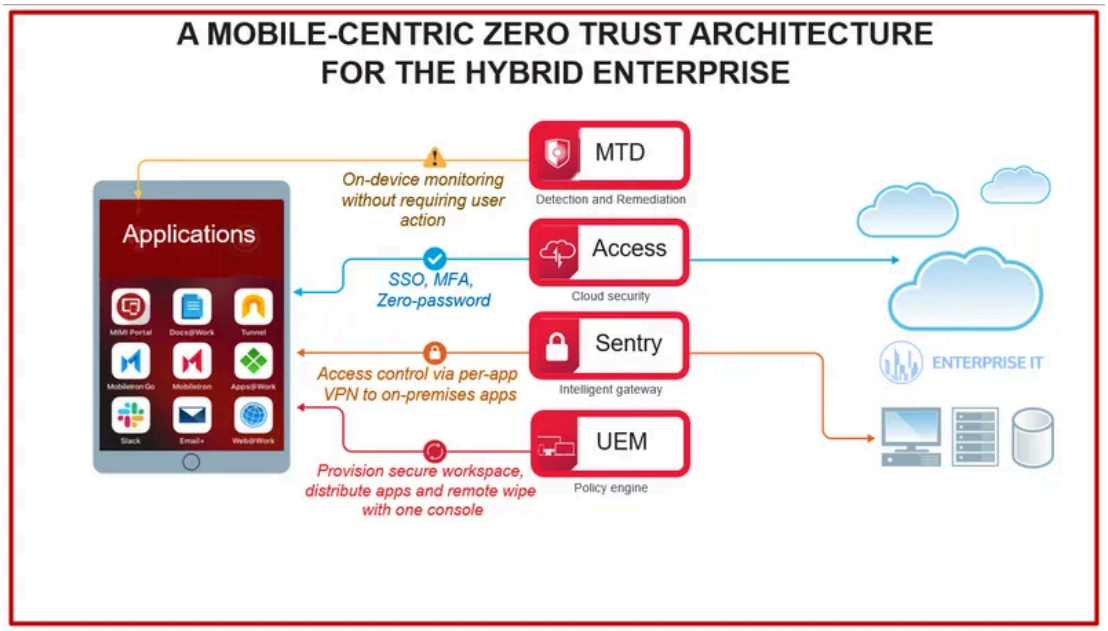
如要在行動裝置和公司網路以外的其他端點上連續存取商業資料，需要專注於安全性。 為跟上最新的安全性需求，企業需要考量他們是否可以：

- 佈建端點 (例如行動電話和筆記型電腦)
- 基於一組命令式資料授予存取權限
- 保護靜態和流動資料
- 視需要強化措施

針對此現代問題的 Ivanti 解決方案可因應所有挑戰。 您可監測端點並觸發自適性原則以補救威脅、隔離裝置並維持合規性。 搭配以下元件可協助您的組織實現行動導向的零信任架構：

- Ivanti Neurons for MDM - 協助您在任何裝置上建立安全的工作空間，基於使用者的角色向其提供應用程式、組態和原則。 使用者可輕鬆安全地存取工作所需的資源
- **Sentry** - 內嵌式智慧型閘道器，可協助您確保內部部署資源
- **Access** – 協助您驗證使用者、裝置、app、網路類型和威脅出現。 調適型存取控制檢查是零信任模型的基礎。 Access 提供雲端單一登入和安全性
- **行動威脅防護** - Ivanti Neurons for MDM 搭配行動威脅防護 (MTD) 可使用最新的加密與威脅監測技術來保護裝置和網路上的資料，並偵測裝置、網路和應用程式層級的攻擊

下圖為解決方案概覽：



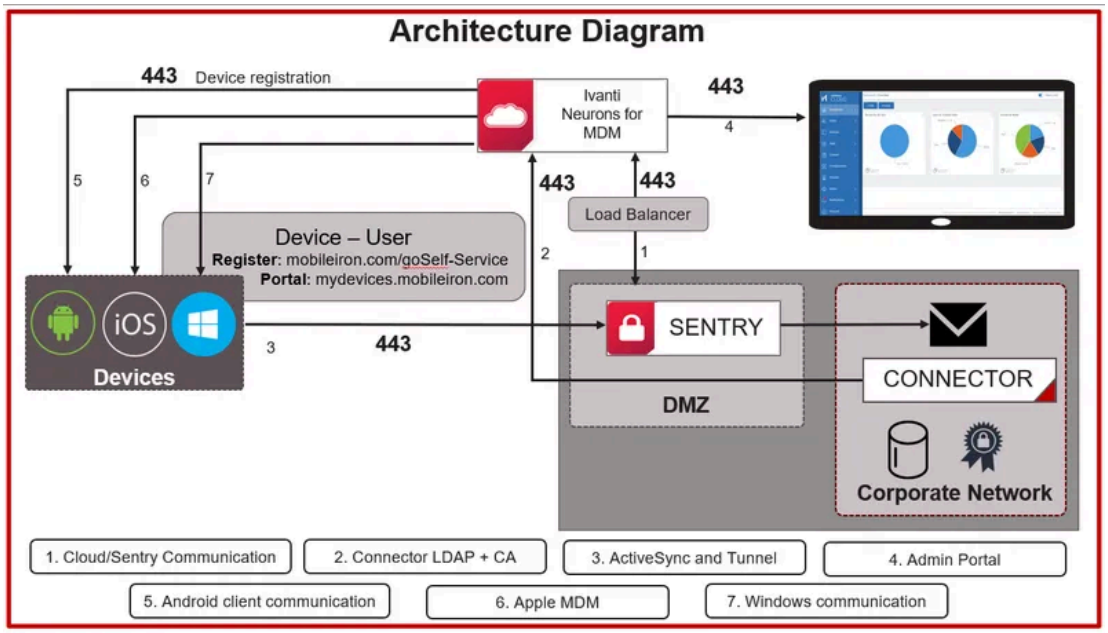
主要特色

Ivanti Neurons for MDM 平台提供基本可見性和 IT 控制，以保護、管理和監測任何可存取關鍵業務資料的公司或員工擁有的行動裝置或桌上型電腦。 Ivanti Neurons for MDM 平台可協助組織確保在組織內使用的各種員工裝置安全無虞，同時還能管理裝置的整個生命週期，包括：

- 原則配置管理與施行
- 應用程式發佈與管理
- 針對桌上型電腦裝置的指令碼管理與發佈
- 裝置動作
- 存取控制與多重要素驗證
- 威脅偵測與補救

架構圖

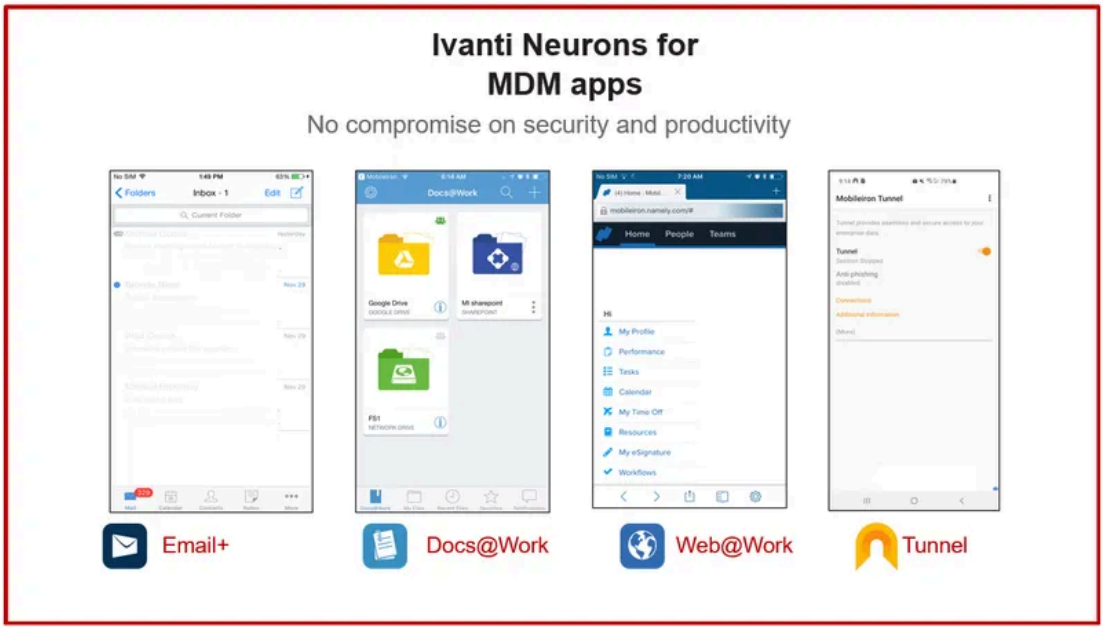
下圖顯示 Ivanti Neurons for MDM UEM 平台的架構概觀：



Ivanti Neurons for MDM 應用程式

- **App Catalog** - App Catalog 是一種可自訂的企業 app 店面。 IT 系統管理員可直接發佈私人或內部開發的 app 至其使用者裝置。 App Catalog 也可以與 Apple 大量採購方案結合，以利在 iOS 裝置上安全發佈行動 app。 此外，Ivanti 可以控管受管理的 iOS app 和 Android Enterprise 的功能。 如此就可在 Ivanti Neurons for MDM UEM 平台中針對兩項進階應用程式安全功能，輕鬆設定應用程式層級設定和安全性原則。
- **Email+** - 可跨平台確保在 iOS 和 Android 上的 PIM 應用程式安全。 Email+ 可藉由與您企業的 ActiveSync 伺服器通訊，在公司擁有的裝置和個人裝置上提供安全的電子郵件、行事曆、通訊錄和工作。
- **Docs@Work** - 讓使用者可以從 Microsoft Share Point 等儲存庫以及 Box 和 Dropbox 等雲服務，安全地存取、建立、編輯、標記和共用內容。 這點很重要，如此使用者即使出門在外也能將生產力提升到最大。
- **Web@Work** - 此安全瀏覽器可讓企業使用者安全地存取公司內部網路上的內容。 使用 Web@Work，您可以限制僅授權的使用者才能存取企業資料。 將 Web@Work 與 App Tunnel 一起部署時，您就可確保行動存取企業資料的安全性。 使用 Web@Work，使用者可快速輕鬆地存取內部網路資源。

下圖顯示 Ivanti Neurons for MDM 應用程式：



角色

系統管理員 - 身為企業系統管理員，您負責以下工作：

- 為企業使用者提供無縫安全存取工作空間的電子郵件、應用程式、配置和連線能力（例如 Wi-Fi 和 VPN）。
- 在員工裝置上分開個人資料與商務資料，如此商務資料就不會外洩至個人 app，而個人資料也不會意外被 IT 人員存取。

使用者 – 身為企業使用者，您可從安全的行動裝置、桌上型電腦和雲端服務無縫存取商務應用程式和個人資料。 關於您作為使用者可以執行的各種工作的更多資訊，請參閱使用者 和角色管理。

開始使用

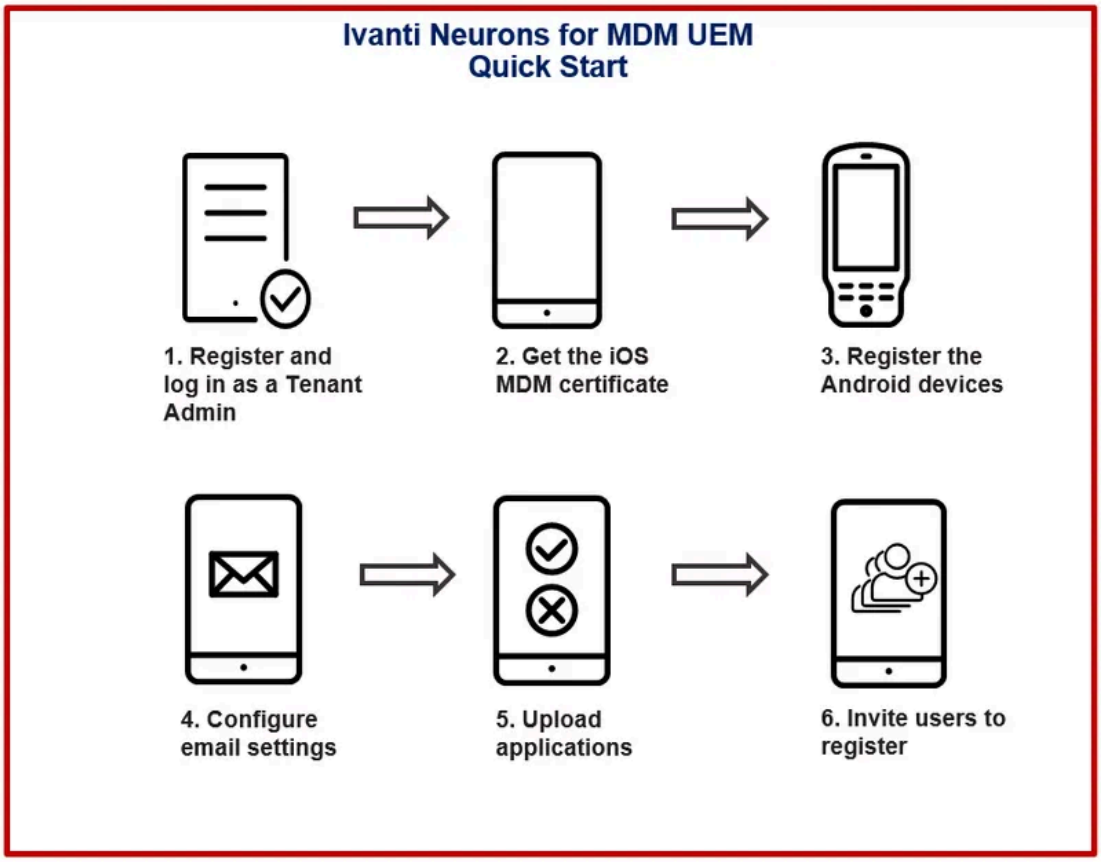
如果您是新註冊的使用者，請依照本節所述的步驟快速上手使用 Ivanti Neurons for MDM 服務。

在訂閱 Ivanti Neurons for MDM 平台後，Ivanti 會為您建立 Ivanti Neurons for MDM 租用戶。 您的註冊電子郵件地址會收到一封電子郵件，信中包含一個 PDF 檔案，提供有關為您企業建立的租戶之以下資訊：

- 有關您購買的軟體套件資訊
- URL 及租戶的超級管理員登入認證
- 如何存取 Ivanti Neurons for MDM 的支援社群和常見問題集
- 如何存取技術說明文件和下載軟體

> Ivanti, Inc 未提供軟體金鑰。 使用超級管理員認證登入 Ivanti Neurons for MDM 租用戶並接受服務條款，即可啟動 Ivanti Neurons for MDM 產品。

下圖描述了開始使用 Ivanti Neurons for MDM 的步驟：



程序

1. 按一下租戶註冊電子郵件中提供的 URL。 出現密碼重設提示。
2. 變更密碼。
3. 使用 ID 和密碼登入租戶帳戶。 歡迎使用精靈出現。
4. 填寫**歡迎使用**表格中的詳細資訊，接受條款與條件，然後按一下**繼續**。
5. 如要安裝 iOS MDM 憑證，請參見**安裝 MDM 憑證**。

> 如果您想稍後再管理您的 iOS 裝置，可以略過 iOS MDM 憑證安裝。 然後精靈會提示您註冊您企業的 Android 裝置。 略過 iOS MDM 憑證安裝代表無法註冊 iOS 裝置。 使用者將會看到一則訊息，指出尚未啟用 iOS 裝置註冊。

6. 如要在 Android Enterprise (AE) 模式中註冊 Android 裝置，請參閱**受管理的 Google Play 帳戶 (Android Enterprise 帳戶)**。 精靈會提示您設定電子郵件帳戶。

> 如果您想稍後再管理您的 Android 裝置，可以略過 Android 受管理的 Google Play 帳戶註冊。 略過受管理的 Google Play 帳戶註冊，您將無法註冊 Android Enterprise 裝置。 Android 裝置仍可透過裝置管理員進行註冊，但主要功能像受管理的 Google Play 和 App 配置將會無法使用。

7. 如要設定電子郵件和 ActiveSync，請參閱 **Exchange 組態**和**電子郵件配置**。
8. 按一下**繼續**。 出現建立密碼提示。
9. 選擇密碼類型，然後按一下**繼續**。
10. 選擇您要上傳的應用程式，然後按一下**繼續**。

11. 指定使用者的電子郵件地址，然後按一下**繼續**。 使用者將會收到一封電子郵件以註冊其行動裝置。 這時會顯示配置的摘要。
12. 按一下**完成**。 顯示「儀表板」頁面。
13. 如要進一步探索，請執行以下步驟：
    - 前往**使用者**。 將會列出所有受邀的使用者。
    - 前往 **App**。 將會列出您已上傳的所有應用程式。
    - 前往**配置**。 將會列出您在註冊期間推送的所有配置。

如需您身為系統管理員可執行的各種工作，請參見管理。

在瀏覽器中設定偏好的語言

如果使用者已將其瀏覽器語言設定為不支援的語言，使用者可以使用 en_US (英文，美國) 做為入口網站的預設語言。

如要設定在 macOS 10.15+ 裝置上執行之 Safari 瀏覽器的語言偏好設定，使用者可依下列方式設定偏好的語言：

1. 在 macOS 裝置上，前往**系統偏好設定**。
2. 前往**語言和地區 > 一般**。
3. 將 **en_US** (或任何其他語言選項) 設定為**偏好語言**。

Ivanti Neurons for MDM 和 Access 的整合導覽介面

針對某些叢集中的新客戶，會透過 Ivanti Neurons for MDM 以整合導覽介面的形式提供 Access。 使用 Ivanti Neurons for MDM 管理員憑證登入。 Access 選項位在左側導覽窗格中的個別索引標籤之下。 請造訪產品文件，然後按一下 Access 以取得有關 Access 和如何設定 Access 的更多資訊。

此整合導覽介面包含以下功能：

- Ivanti Neurons for MDM 和 Access 的整合登入。
- 左側導覽窗格中提供產品選擇器，可在 Ivanti Neurons for MDM 和 Access 產品之間切換。
- 產品選擇記憶：初次登入時，會顯示 Ivanti Neurons for MDM 管理入口網站。 之後再登入時，Ivanti Neurons for MDM 或 Access 會出現，鏡像初次登入時選取的產品。
- Ivanti Neurons for MDM 和 Access 的左側導覽窗格。
- 整合帳號設定窗格，並提供多種選項的連結，例如升級選項、說明文件、支援入口網站、變更密碼和登出。

管理 Android 裝置的裝置管理 (DA) 模式已棄用

自 Ivanti Neurons for MDM 78 起，用於管理 Android 裝置的裝置管理員 (DA) 模式會分階段逐步棄用。

任何在 Ivanti Neurons for MDM 78 上建立新租用戶的新使用者，將無法在 DA 模式下註冊任何裝置 (Android 6 和更新版本)。 任何需要啟用 DA 註冊 Android 6 至 Android 9 裝置的新租戶都必須聯絡 Ivanti 支援中心。

- Android 10 和更新版本的裝置仍將無法註冊為 DA 模式。
- 針對現有的使用者 (不論是否已進行 DA 部署)，在管理現有 DA 裝置 (Android 6 到 Android 11) 方面並無改變。 不過，在升級至 Ivanti Neurons for MDM 78 後，在現有租用戶上執行 Android 10+ 的任何新註冊裝置，將無法在 DA 模式下運作。 此類的現有租戶只能在 DA 模式下註冊 Android 6 到 Android 9 版本裝置。
- 如果使用者打算將 DA 裝置從 Core 執行個體移轉至 Ivanti Neurons for MDM R78，在觸發移轉之前，請確定 Android Enterprise 已啟用，且至少一個系統組態已分發至目標集: PO、DO 或 COPE。 此步驟非常重要，可防止裝置在移轉後淘汰。

DA 註冊類型	現有租戶 (升級至 78 版本)	新租用戶
新 DA 註冊 Android 10 或以上的裝置	不允許	不允許
新 DA 註冊 Android 10 以下的裝置	允許	不允許
Android 10 或以上的現有 DA 裝置	將保持作用	不適用
Android 10 以下的現有 DA 裝置	將保持作用	不適用
Android 10 或以上的移轉 DA 裝置	將淘汰	將淘汰
Android 10 以下的移轉 DA 裝置	將保持作用	將淘汰

4.1. 設定 macOS 裝置

此為概覽性主題，提供常見程序清單與在 Ivanti Neurons for MDM 中設定 macOS 裝置相關的內容。 您可以在Ivanti Neurons for MDM *管理員指南*中存取所有的 macOS 主題。

內容

- 註冊裝置
- 設定使用者邀請範本
- 設定 Zero Sign-on 功能
- 設定適用於 macOS 用戶端的 Mobile@Work
- 設定 macOS shell 指令碼
- 設定 macOS 配置
- 設定 macOS 原則

註冊裝置

大多數的使用者一開始都要先註冊裝置。 您可使用下列任何一種方法開始註冊程序：

- 傳送邀請給一或多位一般使用者 (iReg 註冊)。 如需詳細資訊，請參閱裝置註冊區段中的 *macOS 裝置註冊*主題。
- Device Enrollment 和透過 Apple Business Manager 進行使用者註冊

如需更多資訊，請參閱裝置註冊。

設定使用者邀請範本

您可將一般使用者電子郵件邀請品牌化，讓一般使用者對其外觀更有熟悉感。 如需更多資訊，請參閱將電子郵件範本品牌化。

您可以利用使用者認識的名稱與標誌，來自訂裝置註冊程序。 如需更多資訊，請參閱使用者品牌化。

如需更多資訊，請參閱設定和使用註冊確認電子郵件。

設定 Zero Sign-on 功能

有關零登入相關說明文件，請參閱 *Access 指南*中的「零登入搭配 Access 使用」。

有關零接觸自動化註冊，請參閱使用者設定主題，「設定新裝置註冊的設定」章節，步驟 13。

設定適用於 macOS 用戶端的 Mobile@Work

適用於 macOS 的 Mobile@Work app 提供：

- 指令碼處理 macOS 裝置上的功能
- 適用於使用者的 App Catalog
- 推送通知
- 針對自動化 Device Enrollment 註冊的使用者上架 (歡迎/狀態) 畫面

將 Mobile@Work 推送給一般使用者前，請確保已建立Mobile@Work for macOS Configuration.htm適用於 macOS 的 Mobile@Work，並已將之設為發佈至目標 macOS 裝置。

您可以在自動化 **Device Enrollment** 程序期間，啟用 macOS 裝置上的使用者上架。 當 Device Enrollment 完成時，會將適用於 macOS 的 Mobile@Work 與描述檔、配置和 app 一併推送給裝置。

設定 macOS shell 指令碼

Ivanti Neurons for MDM可讓您建立自己的 macOS 殼層指令碼，然後上傳至 Ivanti Neurons for MDM 並在受管理的 macOS 裝置上執行。 您可以使用適用於 macOS 的 Mobile@Work 指令碼配置來設定指令碼。 適用於 macOS 的 Mobile@Work 會將指令碼執行結果傳回 Ivanti Neurons for MDM，並顯示在裝置日誌中。 您可以在 macOS 裝置上透過裝置詳細資料頁面的**日誌**索引標籤查看裝置日誌。 如需建立、上傳與管理指令碼儲存庫的相關更多資訊，請參閱**所有指令碼**。

在 macOS 裝置上執行殼層指令碼之前，請確定使用者已在其裝置上執行適用於 macOS 的 Mobile@Work app，並已將適用於 macOS 的 Mobile@Work 配置推送至其裝置。 指令碼可執行一次或重複執行。 透過 Ivanti Neurons for MDM 上的指令碼，可以讓管理員從裝置收集資訊，並將之儲存在 Ivanti Neurons for MDM 做為自訂屬性。 例如，如果您需要知道 macOS 裝置上的 Java 版本，您可以收集此資訊並將之儲存在每部裝置上做為自訂裝置屬性。 如需更多資訊，請參閱 **Mobile@Work for macOS** 中的*建立 Mobile@Work for macOS 指令碼組態*。

設定 macOS 配置

配置是指您傳送給裝置的設定集合。 例如，您可以使用會自動設好裝置 VPN 設定和密碼需求的配置。 使用**配置**頁面來選擇、設定與發佈配置。 有很多**組態類型**可用。 在此**頁面**中，您可以檢視可用 macOS 配置清單，包括以下配置：

- **Wi-Fi**
- **密碼**
- **VPN**
- **加密 DNS**
- **FileVault 2**
- **FileVault 復原金鑰**
- **macOS 防火牆**
- **macOS 限制**
- **macOS AppStore 限制**
- **macOS Finder 設定**
- **macOS 核心擴充原則**
- **Active Directory (macOS)**
- **Office 365 自動帳戶建立 (macOS)**

您可使用**自訂配置**匯入並發佈預先定義的配置檔。

設定 macOS 原則

原則用來定義裝置的規範，包括當裝置不符合規範時的處置原則。 每種原則都包含一項規則和相符性動作 (違反規則時的作法)。 使用**原則**頁面來選擇、設定與發佈原則。 停用資料保護/加密和**允許的 app** 為 macOS 相關的原則。 您可使用**自訂原則**依據裝置和指定的使用者屬性、區段準則、值和合規動作，來建立自訂原則。

發佈 macOS app

Ivanti Neurons for MDM 透過 Apple 的 MDM 通訊協定和使用 Mobile@Work 應用程式支援 macOS **應用程式**發佈。 管理員可選擇使用以下一或兩種方式：

- Apple 的 MDM 通訊協定 - 管理員只能上傳特定 PKG 格式 (發佈格式) 為內部開發的 app，也可以從 Mac App Store (包含 Apple 的 Apps and Books 授權支援) 發佈 app。 然而，此方式不允許管理員發佈 DMG 和其他 PKG 格式。
- 適用於 macOS 的 Mobile@Work 應用程式 - 是一種將應用程式散發給使用者的方式，管理員可使用 MobileIron Packager (MIP) 應用程式將任何 PKG、DMG 或 .app 檔案轉換為 MIP 檔案。 將 MIP 檔案上傳至 Ivanti Neurons for MDM 作為內部應用程式。

> 從 MobileIron 軟體下載中，可下載 Ivanti Neurons for MDM Mac Packager 公用程式。

管理員可使用 Mobile@Work 以 DMG、PKG 或 .app 格式發佈內部開發的 app。 針對僅在 Mac App Store 提供的 app，管理員可繼續使用 Apple 原生的 MDM 功能，包括 Apple Apps and Book 授權功能。

4.2. 設定和使用註冊確認電子郵件

管理員可設定和觸發在使用者完成註冊後傳送電子郵件給使用者。 此電子郵件可包含，例如，在使用者成功註冊後提供額外的指示。 管理員可啟用在邀請使用者期間傳送此電子郵件。

此程序：

- **設定功能：**
  - 設定電子郵件範本: 預設英文版電子郵件範本如下所示，但可按照**將電子郵件範本品牌化**中的**自訂電子郵件範本**中的說明進行修改，使其更符合需求。



  - 開啟註冊確認電子郵件。 請參閱**使用者設定**中的**設定使用者註冊確認電子郵件**。
- **使用此功能：**
  - 依照**邀請使用者**中的指示，傳送註冊邀請給使用者。 當使用者註冊成功後，Ivanti Neurons for MDM 將會傳送註冊確認電子郵件給使用者。

4.3. 設定和使用原則遵循通知電子郵件

管理員可編寫原則遵循通知電子郵件範本，自訂和允許的 App 原則之傳送電子郵件動作會傳送電子郵件給違規裝置的使用者。 以下程序說明配置：

- **設定功能：**
  - **設定電子郵件範本**。
    預設英文版電子郵件範本如下所示，但可按照**自訂電子郵件範本**中的**將電子郵件範本品牌化**中的說明進行修改，使其更符合需求:
    
  - **啟動原則遵循通知範本**。 此範本可和您使用自訂和允許的 App 原則之傳送電子郵件動作編寫的訊息一起使用。 Ivanti Neurons for MDM 可將您在這些電子郵件動作中指定的資訊插入原則合規性通知範本。 當您建立或編輯自訂或允許的 App 原則時，您可啟動原則遵循電子郵件範本。 有關針對自訂政策或允許的 App 原則啟用原則遵循通知範本的更多資訊，請個別參閱**新增自訂原則**和**建立允許的應用程式原則**。
- **使用此功能：**
  - 在已啟用原則通知範本後，若裝置不符自訂或允許的應用程式原則，Ivanti Neurons for MDM 會先將電子郵件整合至原則通知範本，再將電子郵件傳送給裝置擁有者。 您與該功能的互動旨在按照上文所述方式對其進行設定，Ivanti Neurons for MDM 會自行使用此功能。

4.4. 隨選即用功能

Ivanti Neurons for MDM 包含一些依預設停用的隨選功能。 這類功能可能會影響效能，而且可能還沒完全準備好進行正式部署。

如果管理員有意協助其租用戶裝置啟用一或多個已依預設停用的隨選即用功能，管理員可以聯絡支援中心。

下表包含記錄的隨選即用功能清單：

功能	描述	平台	授權
Windows 10 功能	適用於 Windows 10 裝置的功能。	Windows 10	• 舊版：Gold • 目前：Secure EUM 請參見套件以取得有關舊版和目前產品的更多資訊。
將 App Catalog URL 複製到剪貼簿	可讓管理員將 App Catalog URL 複製到 app 的剪貼簿。 此 URL 可透過電子郵件發佈給使用者。 如果使用者從註冊的裝置按一下連結，含有該 app 的 App Catalog 將會在瀏覽器中開啟，使用者可從哪裡選擇安裝 app。 管理員要負責限制此 URL 僅發佈給預定使用者。	• iOS • macOS	NA (租戶特定)
將 Web Clip 設為 app	在 App Catalog 中將 **Web Clip** 設為 app，以便透過 App Catalog 提供 Web 應用程式給使用者運用。 Web Clip 可定義為配置，但只有管理員能夠推送配置。 使用者可選擇在其裝置上安裝 Web 應用程式或退出，但使用者無法選擇退出 Web Clip 配置。	iOS	NA (租戶特定)
開啟列入允許清單裝置的註冊	可讓您根據使用者 > **使用者設定** > 預設裝置註冊設定中的「允許列出的」序號註冊裝置。	• iOS • macOS	NA (租戶特定)
憑證型驗證	**憑證型驗證**功能可讓管理員使用數位憑證和租戶特定主機名稱或虛擬主機名稱登入。 此驗證設定可使用**管理**標籤之下的虛擬主機配置進行設定。	此功能不受平台限制。	NA (租戶特定) 只有支援中心啟用時，才能在 NA3 叢集環境中使用此功能。
建立專屬裝置配置 (公司擁有的單一使用，或 COSU)	管理員可用使用「專屬」裝置 (公司所擁有的一次性或 COSU 組態) 的 Android Enterprise 設定可用於特定目的之專屬裝置。將 **COSU 組態**散發至「工作受管理裝置」 (「裝置擁有者」模式)，僅為使用者提供一個在 kiosk 模式下可用的應用程式。	Android Enterprise	銀級
儀表板閒置期間	依預設，儀表板閒置期間會設為 15 天。 此天數可根據租戶需求更新並最多延長至 30 天。 若您需要更長的閒置期，請聯絡**支援**團隊。	此功能不受平台限制。	

4.5. 準備 Android Enterprise 裝置支援

本節說明 Android Enterprise 裝置的最低網路需求。 Android 裝置一般不需要您為了正確運作而開啟防火牆上的傳入連接埠。 不過，管理員在為 Android Enterprise 裝置設定網路環境時，需要注意許多輸出連線。

下表所提供的網路變更清單可能不夠全面，同時也可能變動。 其中涵蓋企業管理 API 與 GMS app 目前和過去版本的已知端點。

> 除了下表中所列出的連接埠外，Android Enterprise 裝置還需要 Ivanti Neurons for MDM 的存取權。

如需 Android Enterprise 裝置的需求相關資訊，請參閱 Android Enterprise 說明中的 **Android Enterprise 網路需求**。

Google 不提供特定 IP，因此您應該允許您的防火牆接受連接至 Google AS 15169 之 IP 封鎖清單當中所有 IP 位址 (列於 **http://bgp.he.net/AS15169#_prefixes**) 的外送連線。

> Google 對等項目和邊緣節點的 IP 不會列在 AS15169 封鎖中。 請參閱 **https://peering.google.com/** 取得 Google 邊緣網路的詳細資訊。

5. 儀表板

儀表板會顯示有關註冊的裝置與使用者的重要統計資料。 儀表板上的每個區段稱為小工具。 您可以為每個小工具定義：

- 要顯示的資料類別 (例如：裝置或使用者)
- 資料分組的方式 (例如：依作業系統組建版本或模型)
- 資料的篩選方式 (例如：僅顯示 iOS 裝置或依作業系統組建版本顯示)
- 資料的顯示方式 (例如：圓餅圖或長條圖)

驗證報告和其他資訊

儀表板會顯示註冊的裝置與使用者的重要統計資料。 儀表板上的每個區段稱為小工具。

您可以驗證其他資訊如下：

- **檢視通知**: 前往**儀表板 > 通知**頁面 (或按一下鈴鐺圖示 (右上方)) 以檢視通知並在必要時採取行動。
- **報告**: 前往**儀表板 > 報告**頁面存取統一端點管理 (UEM) 系統中的資料。
- **稽核追蹤**: 前往**儀表板 > 稽核追蹤**頁面存取按時間順序彙整的一組記錄，其中擷取對 Ivanti Neurons for MDM 中所有項目執行的活動。 如要啟用此功能，移至**管理員 > 基礎架構 > 稽核追蹤**頁面並按一下**啟用稽核追蹤**。
- 應用程式洞察: 前往**儀表板 > 應用程式洞察**頁面以檢視並分析應用程式發佈和其他應用程式詳細資料。

本節包含以下主題:

- 使用小工具
- App 深入解析
- 使用排程報告
- 使用自訂報告

5.1. 使用小工具

本節包含以下各主題：

- 新增小工具
- 排列小工具
- 編輯小工具
- 檢閱通知
- 報告
- 稽核追蹤

儀表板會顯示有關註冊的裝置與使用者的重要統計資料。 儀表板上的每個區段稱為小工具。 您可以為每個小工具定義：

- 要顯示的資料類別 (例如：裝置或使用者)
- 資料分組的方式 (例如：依據作業系統版本或機型)
- 資料的篩選方式 (例如，僅顯示 iOS 裝置)
- 資料的顯示方式 (例如：圓餅圖或長條圖)

新增小工具

1. 按一下**新增** (右上角)。
2. 指派小工具的名稱。
3. 選擇資料類別。
4. 在顯示篩選選項時，完成這些選項。
5. 選擇預設的顯示類型 (圓餅圖、長條圖、曲線圖)。
6. 按一下**完成**。

排列小工具

小工具顯示時都是以三個為一組。 不過，您可以變更小工具的顯示順序：

1. 按一下**排列** (右上角)。
2. 以想呈現小工具的順序來拖放方塊。
3. 按一下**確定**。

編輯小工具

1. 按一下小工具的設定圖示 (右上角)。
2. 選擇**編輯**。
3. 進行變更。
4. 按一下**完成**。

檢閱通知

按一下鈴噹圖示 (右上角) 或前往**儀表板 > 通知**頁面，以檢閱通知並根據下列條件採取必要動作：

- 元件類型
  - 應用程式
  - LDAP
  - Entra ID
  - 裝置允許清單
  - Apps and Books
  - iOS
  - Android
  - macOS
  - visionOS
  - watchOS
  - tvOS
  - 租戶
  - CA
  - 連接器
  - Sentry
  - Device Enrollment 伺服器權杖

通知類型

  - 到期
  - 資料同步
  - 用量限制
  - 管理動作
  - 伺服器身份認證錯誤
  - 驗證錯誤
  - 狀態變更

嚴重性

  - 已清除
  - 資訊
  - 重要
  - 警告

管理員可以選擇應用程式元件，在「通知」頁面上還有鈴鐺通知區段中快速檢閱所有特定應用程式通知。 如果需要接受 Google Play app 的新權限，管理員可按一下通知以接受新權限，無需造訪每個 app 頁面以檢閱與接受權限。

> Ivanti Neurons for MDM 客戶/租戶將收到 Android Go 應用程式核准通知，即使 Android Go 應用程式尚未匯入應用程式目錄。

檢閱使用者的密碼到期日和 ID 變更通知

管理員可以在**通知**頁面中，檢閱即將到來的密碼到期日。 在密碼到期日前兩週到前一天，系統也會傳送通知給管理員，其中包括 CSV 報告檔 (內含對應使用者清單) 的連結。 密碼到期後，將不會再產生通知。

管理員也可以檢視通知，其中列出已偵測到於上次 LDAP 同步期間變更使用者 ID (UID) 的使用者。

清除通知

如有需要，您可從**通知**頁面手動清除任何嚴重性通知。

1. 在**通知**頁面中，針對您想清除的通知，按一下**動作**欄中的圖示。 隨即顯示**確認清除通知**視窗。
2. 按一下**清除通知**。 清除後，**狀態**欄中的通知狀態會變更為**已清除**。

> 清除的通知總數會顯示在**通知**頁面中。

報告

在**儀表板 > 報告**頁面中，您可以存取統合端點管理 (UEM) 系統中的資料。 例如，管理員在建立裝置和封鎖的裝置報告時，可使用對應的篩選選項，將資訊（例如裝置空間名稱和裝置自訂屬性）新增至報告。 如此，這些報告會分別包含裝置空間名稱和裝置自訂屬性欄。 在建立報告時，可在篩選選項之下找到自訂裝置屬性。 管理員可從用於裝置的自訂裝置屬性鍵清單中挑選並選擇可用的運算子。

從 Ivanti Neurons for MDM 76 起，所有報告範本的運算子都包含標準運算子。 在本版本中已標準化以下範本的運算子：

- 儀表板> 報告> 建立報告

下列為報告的工作流程：

1. 選擇 - 從預先定義的報告範本中進行選擇。
2. 定義範圍 - 設定報告資料的時間段。
3. 設定詳細資料 - 命名報告並進行自訂。
4. 執行或排程 - 立即執行報告或建立排程。
5. 共用 - 指定報告的接收對象。

相關主題:

- **儀表板 > 報告 (已排程)**
- **儀表板 > 報告 (自訂)**

快速搜尋：導覽至「報告」標籤。 快速搜尋欄位可讓您從以下欄進行搜尋，即使包含空格或特殊字元，也能搜尋：

- 名稱
- 描述
- 範本名稱

稽核追蹤

稽核追蹤 提供在 Ivanti Neurons for MDM 中執行活動的時序記錄。 這些記錄包括管理員、終端使用者和系統元件執行的動作。

管理員使用**稽核追蹤**來檢閱變更、驗證動作、排解疑難，並支援合規性檢查。 **稽核追蹤**可追蹤動作，例如新增、更新和刪除受管理實體，包括裝置。 如需更多資訊，請參閱**裝置註冊 (iOS、macOS 及 Android)**。

啟用稽核追蹤

您需要啟用**稽核追蹤**選項，才能擷取在 Ivanti Neurons for MDM 中執行的活動。

程序

1. 選擇管理員 > 基礎架構 > 稽核追蹤。
   稽核追蹤窗格隨即出現。
2. 選取並設定**稽核追蹤匯出**切換按鈕為開啟。

> 啟用稽核追蹤功能後無法將其停用。 若要停用，請聯絡 Ivanti 支援。

檢視稽核追蹤

依照步驟檢視有關**稽核追蹤**的更多詳細資訊:

程序

1. 前往**儀表板** > **稽核追蹤**。

稽核追蹤窗格隨即出現。

2. 下表列出顯示在**稽核追蹤**窗格中的詳細資料:

設定	描述
圖示	顯示稽核事件的活動圖示。
活動	顯示發生的動作，例如裝置簽入或管理員登入。
狀態	顯示活動是成功還是失敗。 如果報告失敗，您可以從**報告歷史記錄**重試報告工作。 使用此選項可在不建立新報告排程的情況下重新執行失敗的工作。
執行者	顯示執行活動的管理員或使用者。
執行於	顯示活動發生的日期和時間。
執行時間	顯示受活動影響的裝置、帳戶或物件。
詳細資料	顯示有關活動的其他資訊。
類型	顯示活動類型，例如裝置動作或帳戶。
類別	顯示與活動相關的功能區域，例如裝置管理或管理入口網站存取。

3. 按一下**動作**按鈕以執行下列選項:

- **設定稽核追蹤設定**: 選取此選項，即可在**管理員** > **基礎架構** > **稽核追蹤**中顯示**稽核追蹤**組態。
- **匯出至 CSV**: 選取此選項可匯出和下載**稽核追蹤**。

4. (選用) 您可以使用**篩選器**來檢視特定的**稽核追蹤**。

活動詳細資料檢視

變更 - 之前與之後圖示將出現在**儀表板** > **稽核追蹤** > **詳細資料**欄中。 它可協助管理員比較稽核動作前後的屬性值。 此比較可更輕鬆地識別變更的內容、驗證使用者或系統活動，以及對組態更新進行疑難排解。

按一下圖示，即可在**稽核追蹤變更 - 之前與之後**窗格中檢視稽核追蹤比較詳細資料，並且它會顯示下列詳細資料:

設定	描述
屬性	顯示修改過的屬性的名稱。 例如，`createdAt`。
下列時間之前	顯示執行動作前的屬性值。 以紅色反白顯示。
下列時間之後	顯示執行動作後的屬性值。 以綠色反白顯示。

稽核追蹤的進階搜尋

使用進階搜尋選項，根據規則搜尋稽核追蹤。 定義識別和檢視活動的特定條件。 可以使用以下屬性來執行進階搜尋:

- **活動**
- **類別**
- **建立時間**
- **執行者**
- **執行時間**
- **空間名稱**
- **狀態**
- **類型**

建立稽核追蹤報告

您可以排程**稽核追蹤**報告每 12 小時或 24 小時執行一次，或產生自訂報告。 此外，您可以視需要執行**稽核追蹤**報告。 未排程隨選報告，並包含過去 24 小時的**稽核追蹤**資料。

您可以產生下列格式之一的稽核追蹤報告:

- CSV
- JSON
- CEF

此外，在為**稽核追蹤** > **報告分發**建立報告時，您可以選取 **SFTP 匯出**選項，將所有稽核追蹤資訊匯出並上傳至特定伺服器位置。 稽核追蹤匯出使用安全殼層檔案傳輸通訊協定 (SFTP)。 必須可透過預設連接埠存取伺服器。 您可以設定**稽核追蹤匯出**設定，每天自動將稽核追蹤封存檔上傳到特定位置。 如需更多資訊，請參閱匯出稽核追蹤。

如需建立報告的詳細資訊，請參閱使用排程報告和使用自訂報告。

5.2. App 深入解析

本節包含以下各主題：

- 檢視 app 發佈
- 檢視 app 詳細資料
- 新增單一 app 發佈圖表
- 新增未受管理 iOS app 圖表
- 新增前 10 大已安裝的受管理 App
- 新增前 5 大內部開發的 App

App 深入解析是儀表板的其中一項功能，其可協助您檢視與分析下列 app 發佈：

- 需要進行安裝的內部開發 app 發佈
- 需要進行安裝的公開 app 發佈
- 未受管理 iOS app
- 前 10 大已安裝的受管理 app
- 前 5 大內部開發的 App

分析需要進行安裝的前 5 名 app：這些需要進行安裝的公開 app 已發佈給大量使用者，但安裝比率卻很低。 「未受管理 iOS app」圖表針對裝置上的未受管理 app 提供相關資訊。 您已經能夠查看未受管理 app 清單、它們安裝在哪些裝置上，並採取行動以將 app 轉換為受管理 app。 這些 app 發佈需要管理員注意或行動以改善發佈。 這些圖表呈現已安裝 app 的裝置。 環圈圖提供公開和內部開發 app 的概觀，不僅可協助分析需要進行 app 安裝的裝置數目，還可讓您進一步向下鑽研，藉由點按圖表的特定區域來取得更多的 app 專屬資訊。 此外，您還可新增單一發佈圖，以呈現單一 app 的特定版本發佈。

> 儀表板僅顯示有關最近 15 天登記的裝置之相關資訊。

檢視 app 發佈

在**儀表板**下的 **App** 頁面中，您可檢視下列圖表：

- 需要進行安裝的內部開發 app 發佈
- 需要進行安裝的公開 app 發佈
- 未受管理 iOS app

預設顯示內含 5 個內部開發 app、5 個公開和未受管理 iOS app 的圖表。 圖形由左向右排序，開頭是未安裝率最高的 app。

環圈圖用 2 種顏色來代表安裝狀態。 藍色代表已安裝 app 的裝置數目。 紅色代表需要進行安裝的裝置數目。 當您將游標移到各個顏色區域時，畫面便會顯示裝置計數。

若要刪除圖表，您可以按一下圖表右上角的刪除選項。

檢視 app 詳細資料

環圈圖的中心也會顯示需要進行安裝的裝置數目。 例如：750/1000 表示 1000 個裝置當中的 750 個需要安裝。

環圈圖用 3 種顏色來代表 app 發佈。

- 藍色代表已安裝 app 的裝置數目。 按一下圖表中的藍色區域即可瀏覽至**裝置**頁面。 在**裝置**頁面中，**App 版本**欄位顯示已安裝的 app 版本，以及 app 的安裝日期。

> 還可以從左側面板的 **版本**區段中選取選項，根據已安裝的應用程式版本檢視裝置。

- 紅色代表需要進行 app 安裝的裝置數目。 按一下圖表中的紅色區域即可瀏覽至**裝置**頁面。 您可在**裝置**頁面中，檢視需要安裝 app 的裝置。

圖表中心會顯示 app 圖示。 按一下該圖示，即可瀏覽至 **App > App Catalog** 下的 app 詳細資料頁面。

在此頁面中，按一下**已安裝 App 的裝置**索引標籤，即可檢視已安裝所選 app 的裝置清單。

按一下**未安裝 App 的裝置**索引標籤，即可檢視未安裝所選 app 的裝置清單。

新增單一 app 發佈圖表

您可以在「App」頁面中，針對 app 的特定版本新增單一發佈環圈圖。 紅色代表應安裝 app 的合格裝置清單。 這些圖表透過圖形呈現 app 發佈的下列詳細資料：

- 已安裝 app 特定版本的裝置
- 已安裝 app 其他版本的裝置
- 未安裝 app 的裝置

程序

1. 按一下 **App** 頁面中的 **+新增**。 新增 **App** 圖表視窗隨即顯示。
2. 在**圖表類型**下拉清單中選擇**單一 App 發佈**。
3. 針對您想檢視單一 app 發佈圖表的 app，選擇 app 清單的勾選框。

> 您也可以在「搜尋 App」欄位中輸入 app 名稱，以搜尋特定 app。

4. 按一下**新增圖表**。 單一 app 發佈圖表隨即顯示在 App 頁面中。

> 您可從清單中選擇最多 9 個 app。

圖表中心會顯示已安裝指定 app 版本的裝置數目。

例如：5/10 表示 10 個裝置當中的 5 個已安裝指定的 app 版本。

環圈圖用 3 種顏色來代表 app 發佈。

- 綠色代表已安裝 app 特定版本的裝置數目。 按一下圖表中的綠色區域，即可瀏覽至內含已安裝 app 指定版本之**裝置**清單的裝置頁面。 您也可以從左面板選擇 **App 版本**區段中的選項，以檢視安裝 app 其他版本的裝置。
- 淡綠色代表已安裝 app 其他版本的裝置數目。 按一下圖表中的淡綠色區域，即可瀏覽至內含已安裝 app 其他版本之裝置清單的**裝置**頁面。 您也可以從左面板選擇 **App 版本**區段中的版本選項，以檢視安裝 app 其他版本的裝置。
- 紅色代表未安裝 app 的裝置數目。 當您將游標移到各個顏色區域時，畫面便會顯示裝置計數。 按一下圖表中的紅色區域，即可瀏覽至內含未安裝 app 之裝置的**裝置**頁面。 左面板也會顯示 App Catalog 開始提供 app 的日期。

圖表中心會顯示 app 圖示。 按一下該圖示，即可瀏覽至 **App > App Catalog** 下的 app 詳細資料頁面。 在此頁面中，按一下**已安裝 App 的裝置**索引標籤，即可檢視已安裝所選 app 的裝置清單。 按一下**未安裝 App 的裝置**索引標籤，即可檢視未安裝所選 app 的裝置清單。

若要刪除圖表，您可以按一下圖表右上角的刪除選項。

新增未受管理 iOS app 圖表

您可以透過新增 App 頁面中的未受管理 iOS app 圖表來識別與檢視未受管理 app 清單。 此圖表會於管理員新增未受管理 iOS app 到目錄時自動出現。 管理員可視需要刪除或新增此圖表。

程序

1. 按一下 **App** 頁面中的 **+新增**。 新增 **App** 圖表視窗隨即顯示。
2. 在**圖表類型**下拉清單中選擇**未受管理 iOS App**。
3. 按一下**新增圖表**。 「未受管理 iOS app」圖表隨即顯示在 **App** 頁面中。

圖表顯示 App Catalog 中未受管理 app 的數目。 圖表底部顯示 3 個欄位，其中內含下列詳細資料：

- **內含未受管理 iOS app 的裝置** - 指出未受管理 iOS app 的數目。 在「內含未受管理 iOS app 的裝置」視窗中，按一下連結以檢視內含未受管理 app 的裝置清單。
- **App Catalog 中的 app 總數** - 顯示 App Catalog 中可用的 app 總計數目。
- **未受管理 iOS apps (%)** - 以百分比顯示未受管理 iOS app。

如果已從 iTune App Store 安裝 app，您可以將 app 及其資料轉換為受管理 app。若要將 app 轉換為受管理 app：

1. 按一下**內含未受管理 iOS app 的裝置欄位**中的數字連結。 **未受管理 iOS app** 視窗隨即顯示。
2. 從清單選擇 1 個或更多的未受管理 app，然後按一下「未受管理 iOS app」下的數字連結。 所選 app 將轉換為受管理 app，並在裝置下次登記時更新狀態。

> 可以按一下**匯出至 CSV** 連結，以 CSV 格式匯出未受管理應用程式的相關資料。

新增前 10 大已安裝的受管理 App

您可以使用「App」頁面中的「前 10 大已安裝的受管理 App 圖表」來識別與檢視前 10 大已安裝的受管理 App 清單。 管理員可視需要刪除或新增此圖表。

在 **App** 頁面中，依預設顯示前 10 大已安裝的受管理 App 圖表。 如果該圖表已刪除，管理員可從 **App** 頁面新增它。

程序

1. 按一下 **App** 頁面中的 **+新增**。 新增 **App** 圖表視窗隨即顯示。
2. 在**圖表類型**下拉清單中選擇**前 10 大已安裝的受管理 App**。
3. 按一下**新增圖表**。 「前 10 大已安裝的受管理 App」圖表隨即顯示在 **App** 頁面中。

您可以根據在**顯示**下拉清單中選擇的類別來檢視前 10 大已安裝的受管理 App。 可用類別如下：

- **所有 App** (預設選擇)
- **內部開發的 app**
- **公開 app**

圖表中顯示的每個長條代表各個特定 app，其中也會顯示 app 的名稱。 將游標移到每個長條上，以檢視平台 (Android、iOS 或 Windows) 與已安裝 app 的裝置數目。

按一下代表特定 app 的長條，以導覽至**裝置**頁面，其中顯示已安裝 app 之裝置的詳細資料。 「裝置」頁面中的左面板指出已安裝 app 的裝置數目。 按一下左面板的 X 按鈕可回到儀表板的 **App** 頁面。

若要刪除圖表，您可以按一下圖表右上角的刪除選項。

新增前 5 大內部開發的 App

您可以使用「App」頁面中的「前 5 大內部開發的 App 圖表」來識別與檢視前 5 大內部開發的 App 清單。 管理員可視需要刪除或新增此圖表。

在 **App** 頁面中，依預設顯示前 5 大內部開發的 App 圖表。 如果該圖表已刪除，管理員可從 **App** 頁面新增它。

程序

1. 按一下 **App** 頁面中的 **+新增**。 新增 **App** 圖表視窗隨即顯示。
2. 在**圖表類型**下拉清單中選擇**前 5 大內部開發的 App**。
3. 按一下**新增圖表**。 「前 5 大內部開發的 app 圖表」隨即顯示在 **App** 頁面中。

此圖表透過 App 的標誌來呈現資料，其中還會顯示該 App 的星號評等。 星號評等以星號影像和整數表示法 (最高評等 5 顆星) 呈現。 另外也會顯示給予 App 評等的使用者數目。

> App 的評等數目不限於隸屬該管理員和空間的裝置，而是依據 app 所有使用者的評等。 評等即在註冊裝置上從 Apps@Work 檢視該 app 之不同使用者給予該 app 的所有評等的平均值。

按一下特定 app 可瀏覽至 **App 詳細資料**頁面，其中顯示 app 的特定詳細資料。

若要刪除圖表，您可以按一下圖表右上角的刪除選項。

5.3. 使用排程報告

授權：Silver

「排程報告」功能可讓您使用預先包裝好的現成範本，針對各種測量數據進行排程與產生報告。 您必須具備「系統管理員」或「系統唯讀」角色，才能存取此功能。 您目前最多可建立 40 份報告。

> 如果裝置有多個 Tunnel 執行個體，違反原則報告可能有針對相同裝置的多筆記錄。 這適用於標準報告和自訂報告。

產生報告

您可以排程並產生報告。

程序

1. 前往**儀表板** > **報告**。
2. 按一下**建立報告**，以顯示「選擇報告範本」頁面。
3. 從您已配置的選項，為您的報告選擇範本。
   - **已封鎖裝置**: 報告目前 Sentry 封鎖存取權的裝置。
   - **裝置**: 您系統中所有分割區上裝置的相關報告。
   - **違反原則**: 系統中的違反原則報告。
   - **使用者**: 系統中的使用者報告
   - **使用者密碼到期狀態**: 報告您系統中使用者的密碼到期狀態。
   - **最常安裝的應用程式**: 系統中所有應用程式的相關報告，並會依據每種應用程式的安裝次數來劃分。
   - **未受管理的應用程式**: 系統中未受管理應用程式的相關報告。
   - **所有應用程式**: 您在裝置中管理的全部應用程式的相關報告。
   - 稽核追蹤會記錄在 Ivanti Neurons for MDM 內所有實體上執行的所有活動。
4. 按**下一步**。
   報告詳細資訊頁面隨即顯示。
   - 輸入**報告名稱**。
   - (選填) 輸入報告的**描述**。

從下列選項中選取**事件範圍**:
針對現有報告:

- **所有事件**
- **前一天**
- **上一週**
- **上個月**
- **先前範圍** - 顯示使用先前版本的 Ivanti Neurons for MDM 管理入口網站的範圍滑桿所建立的報告。 如果管理員為報告選定並儲存了上述任何一個選項，則不會顯示「先前範圍」選項。 在「報告摘要」頁面上可看見範圍值。

針對新報告:

- **所有事件**

- **前一天**
- **上一週**
- **上個月**

按**下一步**。 「報告資料」頁面隨即顯示。

6. 按一下**自訂欄**以新增、移除或重新排序**報告欄**區段中的欄。 或是按一下該欄名稱來移除已新增的欄。
7. (選用) 使用**選取所有欄**核取方塊以選取清單中所有顯示的欄。
8. 按一下**還原預設值**可還原成先前產生的欄位。 若要將欄位還原成沒有任何自訂，您可從**選擇報告範本**頁面中選擇其中一種範本。
9. 在**進階篩選器**區段中根據特定規則來建立篩選器。

> 不是所有報告都能使用所有的篩選器選項。 如需有關可用篩選器清單的詳細資訊，請參閱此程序下方的篩選器主題。

> 在建立報告時，下列新硬體屬性適用於 Windows 裝置 - BitLocker 加密、作業系統版本、系統版本、主機板製造商、主機板產品、主機板狀態、BIOS 製造商、BIOS 版本、硬碟分割區、光碟機類型、CPU 名稱，以及 CPU 狀態。

10. (選擇性) 您可以按一下 **+** 圖示以新增其他規則，或按一下**新增群組**圖示以新增其他的規則群組。
11. 按**下一步**。 「報告排程」頁面隨即顯示。
12. 選擇下列其中*一種*格式以下載報告:
    - CSV
    - PDF
    - **CSV 及 PDF**
      若是 PDF 報告檔案，最多允許 10 個欄位。 在「報告圖表」區段中，會顯示將納入 PDF 報告中的兩類圖表。
      所有的應用程式報告僅支援 CSV 格式。

按一下**自動排程**，藉由設定週期性的方式設定要自動定期執行的報告。 或是按一下**手動**以執行一次報告，報告結果將透過電子郵件傳送。

- 選取下列其中*一個***週期性報告**選項:
  - **每天**
  - **每週**
  - **每月**
  - **上一個排程** - 針對現有報告
- 選取**開始日期**與**結束日期** (選用)。

14. 按**下一步**。 「報告發佈」頁面隨即顯示。 選取報告的收件者。
15. (選用) 按一下**新增外部電子郵件**連結以新增外部電子郵件 ID。
16. 按一下**完成**。 **報告發佈摘要**隨即顯示。
17. (選擇性) 按一下**編輯**以修改您的報告。
18. 按一下**儲存**。
19. 按一下下載圖示以選擇報告格式。 傳送一封電子郵件給報告收件者，其中包含可下載報告的**下載報告**按鈕。

篩選器

規則選項	描述
啟用啟用鎖定	根據啟用鎖定的啟用狀況為**是**或**否**來建立規則。 規則範例：「啟用啟用鎖定等於是」
App Tunnel 狀態	根據 App Tunnel 狀態為**鎖定**或**允許**來建立規則。 規則範例：「App Tunnel 狀態等於鎖定」
電力	裝置的電力值。 規則範例：「電力等於 1080」 您輸入的電力值應該以秒為單位。
用戶端上一次登記	根據在時間範圍內的用戶端上一次登記來建立規則。 規則範例：「用戶端上一次登記的範圍為 04/02/2019 上午 06:00:00 到 04/05/2019 17:00:00」。
相符性狀態	根據相符性狀態為**是**或**否**來建立規則。 規則範例：'Compliance State is equal to Yes'。
目前的國家/地區名稱	輸入目前的國家/地區名稱。 規則範例：「相符性狀態等於法國」。
目前 MCC	以目前行動國家代碼 (Mobile Country Code) 為依據的規則。 規則範例：「目前 MCC 等於 410」。
目前 MNC	以目前行動網路代碼 (Mobile Network Code) 為依據的規則。 規則範例：「目前 MNC 等於 06」。
Device Enrollment 已啟用	根據 Device Enrollment 已啟用為**是**或**否**來建立規則。 規則範例：「Device Enrollment 已啟用等於是」
防網路釣魚原生狀態	選取下列任一反網路釣魚本機狀態選項: • 等於 • 不等於 可能的值為: • 未啟用 • 不適用 • 啟用 • 不明
防網路釣魚 VPN 狀態	選取下列任一反網路釣魚 VPN 狀態選項: • 等於 • 不等於 可能的值為: • 未啟用 • 不適用 • 啟用 • 不明

規則選項	描述
已註冊 Device Enrollment	根據已註冊 Device Enrollment 為**是**或**否**來建立規則。 規則範例：「已註冊 Device Enrollment 等於是」
資料保護	指出裝置上是否啟用資料保護。 可能的值為**是**或**否**。 規則範例：「資料保護等於是」。
啟用數據漫遊	根據啟用數據漫遊為**是**或**否**來建立規則。 規則範例：「啟用數據漫遊等於是」
裝置封鎖狀態	以裝置封鎖狀態為依據的規則。 規則範例：「裝置封鎖狀態等於鎖定」
裝置 ID	根據特定裝置 ID 或裝置 ID 範圍來建立規則。 規則範例：「裝置 ID 大於 45」。 x
歸屬 MCC	以歸屬行動國家代碼 (Home Mobile Country Code) 為依據的規則。 規則範例：「歸屬 MCC 等於 310」。
歸屬 MNC	以歸屬行動網路代碼 (Home Mobile Network Code) 為依據的規則。 規則範例：「歸屬 MNC 等於 510」。
IMEI	根據特定 IMEI 值來建立規則。 規則範例：'IMEI begins with 9900'
邀請狀態	選擇下列其中一個「邀請狀態」選項： • 無 • 擱置中 • 已過期 • **已完成** 規則範例：'Invite State is equal to Pending'。
定位服務已啟用	根據啟用定位服務為**是**或**否**來建立規則。 規則範例：「啟用定位服務等於是」
MTD 啟用狀態	根據需要選取以下任一 MTD 啟用狀態選項。 • 等於 • 不等於 可能的值如下： • 不適用 • 錯誤 • 擱置中 • 受保護
隔離狀態	根據啟用定位服務為**是**或**否**來建立規則。 規則範例：「隔離狀態等於是」

規則選項	描述
註冊時間	根據裝置註冊的日期和時間範圍來建立規則。 規則範例：註冊時間範圍為 10/03/2017 09:00:00 到 10/20/2017 17:00:00。
漫遊	根據漫遊為**是**或**否**來建立規則。 規則範例：「漫遊等於是」
狀態	選擇下列其中一個「邀請狀態」選項： • 作用中 • 淘汰擱置中 • 淘汰已傳送 • 已淘汰 • 淘汰已取消 • 抹除擱置中 • 抹除已傳送 • 已抹除 • 抹除已取消 規則範例：「狀態等於淘汰擱置中」。
啟用語音漫遊	根據啟用語音漫遊為**是**或**否**來建立規則。 規則範例：「語音漫遊等於是」
WiFi MAC 位址	輸入特定的 MAC 位址值。 規則範例：'Wifi Mac Address is not equal to 00-14-22-01-23-45'。
啟用 iCloud 備份	根據啟用 iCloud 備份為**是**或**否**來建立規則。 規則範例：「啟用 iCloud 備份等於是」
iTunes Store 帳戶啟用狀態	根據 iTunes Store 帳戶啟用狀態為**是**或**否**來建立規則。 規則範例：「iTunes Store 帳戶啟用狀態等於否」。
平台類型	適用於「所有應用程式」報告。
來源	適用於「所有應用程式」報告。
自訂屬性	適用於「所有應用程式」報告。
受管理	適用於「所有應用程式」和「最常使用的應用程式」報告。
App 識別碼	預設用於「所有應用程式」報告。
Meid	適用於「未受管理應用程式」報告。

從「排程報告」頁面對報告執行動作

您可以從「排程報告」頁面執行各種動作。

程序

1. 前往**儀表板** > **報告**。
2. 在**我的排程報告**頁面中，按一下**動作**下拉式功能表，然後選取下列其中一個選項:

動作選項	已執行的動作
檢視	讓您檢視報告。
編輯	讓您編輯報告。 該報告還可讓您針對在上個版本中選定為「先前範圍」的範圍進行檢視。
立即執行	執行報告。
下載 CSV	下載格式為 CSV 的報告。
下載 PDF	下載格式為 PDF 的報告。
刪除	刪除報告。

檢視報告詳細資料

您可以檢視報告詳細資料，並對建立的報告執行某些動作。

程序

1. 前往**儀表板** > **報告**。
2. 在**我的排程報告**頁面中，按一下報告名稱以檢視報告詳細資料。 報告頁面隨即開啟。
3. 您可在此頁面檢視「報告摘要」和「報告歷程記錄」。

相關主題：

- 若要指派自訂角色給使用者，請參閱**指派角色**。
- 請參閱**使用者角色**以檢視預設角色清單。
- **角色管理**
- **使用自訂報告**

5.4. 使用自訂報告

授權：Gold

自訂報告功能可讓您使用現成範本，針對各種測量數據進行自訂與產生報告。 您必須具備「系統管理員」或「系統唯讀」角色，才能存取此功能。 您目前最多可建立 40 份報告。

本節包含以下各主題：

[產生報告]

[對報告執行動作]

[檢視報告詳細資料]

產生報告

您可以從 Ivanti Neurons for MDM 管理入口網站進行排程並產生報告。

程序

1. 前往**儀表板** > **報告**。
2. 按一下**建立報告**，以顯示「選擇報告範本」頁面。
3. 從您已設定的選項中，為您的報告選擇範本。
   - **已封鎖裝置**: 報告目前 Sentry 封鎖存取權的裝置。
   - **裝置**: 您系統中所有分割區上裝置的相關報告。
   - **違反原則**: 系統中的違反原則報告。
   - **使用者**: 系統中的使用者報告
   - **使用者密碼到期狀態**: 報告您系統中使用者的密碼到期狀態。
   - **最常安裝的應用程式**: 系統中所有應用程式的相關報告，並會依據每種應用程式的安裝次數來劃分。
   - **未受管理的應用程式**: 系統中未受管理應用程式的相關報告。
   - **所有應用程式**: 您在裝置中管理的全部應用程式的相關報告。
   - 稽核追蹤會記錄在 Ivanti Neurons for MDM 內所有實體上執行的所有活動。
4. 按**下一步**。 「報告詳細資訊」頁面隨即顯示。
5. 輸入**報告名稱**。
6. (選填) 輸入報告的**描述**。
7. 從下列選項中選取**事件範圍**:
   針對現有報告:
   - **所有事件**
   - **前一天**
   - **上一週**
   - **上個月**
   - **先前範圍** - 顯示使用先前版本的 Ivanti Neurons for MDM 管理入口網站的範圍滑桿所建立的報告。 如果管理員為報告選定並儲存了上述任何一個選項，則不會顯示「先前範圍」選項。 在「報告摘要」頁面上可看見範圍值。

針對新報告:

- **所有事件**
- **前一天**
- **上一週**
- **上個月**

按**下一步**。 「報告資料」頁面隨即顯示。

9. 按一下**自訂**以產生自訂報告：

> 在**儀表板 > 報告**頁面中，若「範本名稱」欄在括號中顯示「自訂」，即指明該報告已經過自訂。

10. 按一下**自訂欄**以新增、移除或重新排序**報告欄**區段中的欄。 或是按一下該欄名稱來移除已新增的欄。
11. (選用) 使用**選取所有欄**核取方塊以選取清單中所有顯示的欄。
12. 按一下**還原預設值**可還原成先前產生的欄位。 若要將欄還原成無任何自訂的狀態，您可在**選擇報告範本**頁面中選擇其中一種範本。 預設欄會用鎖定圖示來表示。
13. 在**進階篩選器**區段中根據特定規則來建立篩選器。

> 不是所有報告都能使用所有的篩選器選項。 如需有關可用篩選器清單的詳細資訊，請參閱此程序下方的篩選器主題。

> 在建立報告時，下列新硬體屬性適用於 Windows 裝置 - BitLocker 加密、作業系統版本、系統版本、主機板製造商、主機板產品、主機板狀態、BIOS 製造商、BIOS 版本、硬碟分割區、光碟機類型、CPU 名稱，以及 CPU 狀態。

14. (選擇性) 您可以按一下 **+** 圖示以新增其他規則，或按一下**新增群組**圖示以新增其他的規則群組。
15. 按**下一步**。 「報告排程」頁面隨即顯示。
16. 選擇下列其中*一種*格式以下載報告:
    - **CSV**
    - **PDF**
    - **CSV 及 PDF**
      若是 PDF 報告檔案，最多允許 10 個欄位。 在「報告圖表」區段中，會顯示納入 PDF 報告中的兩種圖表。
      所有的應用程式報告僅支援 CSV 格式。

按一下**自動排程**，藉由設定週期性的方式設定要自動定期執行的報告。 或是按一下**手動**以執行一次報告，報告結果將透過電子郵件傳送。

- 選取下列其中*一個***週期性報告**選項:
  - **每天**
  - **每週**
  - **每月**
  - **上一個排程** - 針對現有報告
- 選取**開始日期**與**結束日期** (選用)。

> 「立即執行」選項將會產生一次性報告。 您可使用相同範本來產生排程報告。 在**儀表板 > 報告**頁面中，「頻率」和「下一個排程」等欄位將會顯示這些報告的未排程狀態。

18. 按**下一步**。 「報告發佈」頁面隨即顯示。 選取報告的收件者。
19. (選用) 按一下**新增外部電子郵件**連結以新增外部電子郵件 ID。
20. 按一下**完成**。 **報告發佈摘要**隨即顯示。
21. (選擇性) 按一下**編輯**以修改您的報告。
22. 按一下**儲存**。
23. 按一下下載圖示以選擇報告格式。 傳送一封電子郵件給報告收件者，其中包含可下載報告的**下載報告**按鈕。

篩選器

規則選項	描述
啟用啟用鎖定	根據啟用鎖定的啟用狀況為**是**或**否**來建立規則。 規則範例：「啟用啟用鎖定等於是」
App Tunnel 狀態	根據 App Tunnel 狀態為**鎖定**或**允許**來建立規則。 規則範例：「App Tunnel 狀態等於鎖定」
電力	裝置的電力值。 規則範例：「電力等於 1080」 您輸入的電力值應該以秒為單位。
用戶端上一次登記	根據在時間範圍內的用戶端上一次登記來建立規則。 規則範例：「用戶端上一次登記的範圍為 04/02/2019 上午 06:00:00 到 04/05/2019 17:00:00」。
相符性狀態	根據相符性狀態為**是**或**否**來建立規則。 規則範例：'Compliance State is equal to Yes'。
目前的國家/地區名稱	輸入目前的國家/地區名稱。 規則範例：「相符性狀態等於法國」。
目前 MCC	以目前行動國家代碼 (Mobile Country Code) 為依據的規則。 規則範例：「目前 MCC 等於 410」。
目前 MNC	以目前行動網路代碼 (Mobile Network Code) 為依據的規則。 規則範例：「目前 MNC 等於 06」。
Device Enrollment 已啟用	根據 Device Enrollment 已啟用為**是**或**否**來建立規則。 規則範例：「Device Enrollment 已啟用等於是」
防網路釣魚原生狀態	選取下列任一反網路釣魚本機狀態選項: • 等於 • 不等於 可能的值為: • 未啟用 • 不適用 • 啟用 • 不明
防網路釣魚 VPN 狀態	選取下列任一反網路釣魚 VPN 狀態選項: • 等於 • 不等於 可能的值為: • 未啟用 • 不適用 • 啟用 • 不明

規則選項	描述
已註冊 Device Enrollment	根據已註冊 Device Enrollment 為**是**或**否**來建立規則。 規則範例：「已註冊 Device Enrollment 等於是」
資料保護	指出裝置上是否啟用資料保護。 可能的值為**是**或**否**。 規則範例：「資料保護等於是」。
啟用數據漫遊	根據啟用數據漫遊為**是**或**否**來建立規則。 規則範例：「啟用數據漫遊等於是」
裝置封鎖狀態	以裝置封鎖狀態為依據的規則。 規則範例：「裝置封鎖狀態等於鎖定」
裝置 ID	根據特定裝置 ID 或裝置 ID 範圍來建立規則。 規則範例：「裝置 ID 大於 45」。 x
歸屬 MCC	以歸屬行動國家代碼 (Home Mobile Country Code) 為依據的規則。 規則範例:「Home MCC 等於 310」。
歸屬 MNC	以歸屬行動網路代碼 (Home Mobile Network Code) 為依據的規則。 規則範例：「歸屬 MNC 等於 510」。
IMEI	根據特定 IMEI 值來建立規則。 規則範例：'IMEI begins with 9900'
邀請狀態	選擇下列其中一個「邀請狀態」選項： • 無 • 擱置中 • 已過期 • **已完成** 規則範例：'Invite State is equal to Pending'。
定位服務已啟用	根據啟用定位服務為**是**或**否**來建立規則。 規則範例：「啟用定位服務等於是」
MTD 啟用狀態	根據需要選取以下任一 MTD 啟用狀態選項。 • 等於 • 不等於 可能的值如下： • 不適用 • 錯誤 • 擱置中 • 受保護
隔離狀態	根據啟用定位服務為**是**或**否**來建立規則。 規則範例：「隔離狀態等於是」

規則選項	描述
註冊時間	根據裝置註冊的日期和時間範圍來建立規則。 規則範例：註冊時間範圍為 10/03/2017 09:00:00 到 10/20/2017 17:00:00。
漫遊	根據漫遊為**是**或**否**來建立規則。 規則範例：「漫遊等於是」
狀態	選擇下列其中一個「邀請狀態」選項： • 作用中 • 淘汰擱置中 • 淘汰已傳送 • 已淘汰 • 淘汰已取消 • 抹除擱置中 • 抹除已傳送 • 已抹除 • 抹除已取消 規則範例：「狀態等於淘汰擱置中」。
啟用語音漫遊	根據啟用語音漫遊為**是**或**否**來建立規則。 規則範例：「語音漫遊等於是」
WiFi MAC 位址	輸入特定的 MAC 位址值。 規則範例：'Wifi Mac Address is not equal to 00-14-22-01-23-45'。
啟用 iCloud 備份	根據啟用 iCloud 備份為**是**或**否**來建立規則。 規則範例：「啟用 iCloud 備份等於是」
iTunes Store 帳戶啟用狀態	根據 iTunes Store 帳戶啟用狀態為**是**或**否**來建立規則。 規則範例：「iTunes Store 帳戶啟用狀態等於否」。
平台類型	適用於「所有應用程式」報告。
來源	適用於「所有應用程式」報告。
自訂屬性	適用於「所有應用程式」報告。
受管理	適用於「所有應用程式」和「最常使用的應用程式」報告。
App 識別碼	預設用於「所有應用程式」報告。
Meid	適用於「未受管理應用程式」報告。

對報告執行動作

您可以從「排程報告」頁面執行各種動作。

程序

1. 前往**儀表板** > **報告**。
2. 在**我的排程報告**頁面中，按一下**動作**下拉式功能表，然後選取下列其中一個選項:

動作選項	已執行的動作
檢視	讓您檢視報告。
編輯	讓您編輯報告。
立即執行	執行報告。
下載 CSV	下載格式為 CSV 的報告。
下載 PDF	下載格式為 PDF 的報告。
刪除	刪除報告。

檢視報告詳細資料

您可以檢視報告詳細資料，並對建立的報告執行某些動作。

程序

1. 前往**儀表板** > **報告**。
2. 在**我的排程報告**頁面中，按一下報告名稱以檢視報告詳細資料。 報告頁面隨即開啟。
3. 選取下列其中一個選項

動作選項	已執行的動作
切換	讓您啟用或停用報告。
立即執行	執行報告。
檢視	讓您檢視報告詳細資料。 使用「動作」下拉式功能表以執行以下任何一項工作: • **停用** • **下載最新 CSV/PDF** (依據所選報告的類型，無論是 CSV、PDF 或 CSV 與 PDF，皆會顯示「下載」選項) • **歷程記錄** • **刪除**
刪除	刪除報告。

相關主題:

- 若要指派自訂角色給使用者，請參閱指派角色。
- 請參閱使用者角色以檢視預設角色清單。
- 角色管理
- 使用排程報告

6. 使用者

邀請別人註冊裝置之前，您必須為他們建立使用者項目。 對於將使用 Ivanti Neurons for MDM 來協助管理裝置或發佈內容的人員 (管理者)，您也需要為他們建立使用者。

本節包含以下各主題：

- 使用者群組
- 使用者設定
- 使用者品牌
- 透過 Apple 商務管理進行使用者註冊
- 帳戶導向使用者註冊
- 使用者授權
- 管理使用者

6.1. 新增使用者

本節包含以下各主題：

- 新增使用者
- 新增多位使用者
- 藉由上傳檔案來新增多個使用者
- 新增管理員
- Nobody 使用者
- 檢視裝置註冊 PIN 碼資訊

您可同時新增一名或多名使用者。 新增多名使用者之後，您可以篩選畫面，僅顯示您所需的使用者。

針對使用者，您可在此頁面進行的其他作業包括：

- 指派或移除使用者群組中的使用者
- 傳送訊息
- 邀請註冊
- 指派角色
- 變更密碼
- 刪除
- 產生 PIN

所有的裝置擁有者描述檔都會指派給某個裝置帳號。 指派給裝置帳號的裝置數目沒有任何限制。 (員工擁有的) 工作描述檔會指派給使用者帳號。

新增使用者

程序

1. 前往**使用者**。
2. 按一下 **+新增** (右上角)。
3. 選擇**單一使用者**。
4. 填妥表單的下列使用者資訊：
    - 電子郵件地址 (必要)
    - 名字
    - 姓氏

> 「使用者名稱」欄位會顯示您輸入的電子郵件地址。 在大多數情況下，您都不應編輯這項預設值。 如需更多資訊，請參閱如何編輯使用者名稱

    - 顯示名稱

> 如果您想要變更此使用者的顯示名稱，可編輯**顯示名稱**欄位中的預設文字。

5. 若要指派密碼，請將其輸入**密碼**和**確認密碼**欄位。
    - 如果您要指派密碼，您必須在裝置註冊時告知使用者。
    - 如果您不指派密碼，使用者就必須在裝置註冊期間建立密碼。
6. 從下拉式清單選擇**地區設定**。
7. 輸入**受管理的 Apple ID**。 您可將「appleid」加為受管理的 Apple ID 的子網域，以避免與現有的 Apple ID 發生衝突。 例如，user@appleid.yourdomain.com。 子網域必須為 Apple Business Manager 上的有效驗證的子網域。

> 如果有作用中的使用者註冊裝置使用目前帳戶的受管理的 Apple ID，則無法將帳戶更新為不同的受管理的 Apple ID。

(選用) 指派一或多個使用者群組。 當有裝置的狀態為「作用中」和「淘汰擱置中」，則無法更新受管理的 Apple ID。

10. 如果您想在邀請此使用者之前設定其他功能，可清除**立即傳送此邀請**選項。 不然的話，當您按一下**完成**時就會傳送出邀請電子郵件。
11. 按一下**完成**以新增使用者。

針對 Android 裝置，裝置帳戶專為單一使用的受管理裝置而設計，其中單一本機服務帳戶可用於註冊大量裝置。 建立新使用者時，必須啟用**管理員 > Google > Android Enterprise** 下提供的 Android Enterprise 裝置帳戶。 在預設情況下，會為裝置擁有者管理的 Google Play 帳戶註冊啟用裝置帳戶 (而不是使用者帳戶)。

選取 **Android Enterprise 裝置帳戶**核取方塊，以為附加到此帳戶的 Android Enterprise 工作受控裝置註冊自動指派 Google 裝置帳戶。

編輯 Android 裝置的本機或 LDAP 使用者時，與此使用者關聯的 Android Enterprise 裝置擁有者管理的 Google Play 帳戶裝置，將在下次裝置登入時獲指派裝置帳戶，但須滿足以下條件:

- 已藉由選擇 **Android 企業裝置帳號**勾選框來啟用此功能。
- Android 裝置上的 Go App 版本為 47 及以上版本。

新增多位使用者

程序：

1. 前往**使用者**。
2. 按一下 **+新增** (右上角)。
3. 選擇**多位使用者**。
4. 預設下，您可以**手動**輸入電子郵件地址。 輸入或貼上使用者的電子郵件地址，以逗號區隔。
5. 例如：jdoe@mycompany.com, jsmith@mycompany.com, tjones@mycompany.com
   如果您想在邀請此使用者之前設定其他功能，可清除**立即傳送此邀請**選項。
6. 不然的話，當您按一下**完成**時就會傳送出邀請電子郵件。
   按一下**完成**以新增使用者。

藉由上傳檔案來新增多個使用者

程序：

1. 前往**使用者**。
2. 按一下 **+ 新增** (右上角)。
3. 選擇**多位使用者**。
4. 選擇**上傳 CSV**。

5. 按一下**下載 CSV 範本**。
6. 針對每位使用者，使用下列資訊編輯範本：
   - 使用者 ID (必要)
   - 電子郵件地址 (必要)
   - 密碼
   - 姓氏
   - 名字
   - 顯示名稱
   - 使用者群組
   - 自訂屬性
7. 此為您新增單一使用者時所輸入的相同資訊。 檔案中不能超過 10,000 個項目。
   儲存檔案。
8. 將檔案拖曳到上傳區域，或選擇**上傳 CSV**，即可選擇檔案。
9. 顯示上傳的使用者資訊後，您即可進行必要的編輯。
10. 按**下一步** (右下角)。
11. 如果您不想立即傳送邀請，請選擇**不要傳送邀請**。
12. 按一下**完成**。

新增管理員

程序：

1. 按一下**新增** (右上角)。
2. 選擇**單一使用者**。
3. 填妥表單的下列使用者資訊：
   - 電子郵件地址
   - 名字
   - 姓氏
4. **使用者名稱**欄位會顯示您輸入的電子郵件地址。
   如果您想要變更此使用者的顯示名稱，可編輯**顯示名稱**欄位中的預設文字。
5. 在**密碼**欄位中指派密碼。
6. 在**確認密碼**欄位中，再次輸入密碼。
7. 按一下**完成**以新增使用者。
8. 將密碼告知未來要協助管理裝置的人員。

Nobody 使用者

nobody 使用者是無法刪除的預設使用者。 服務會將此使用者套用至不具備任何相關使用者的裝置，例如淘汰的裝置。

檢視裝置註冊 PIN 碼資訊

新增使用者時，系統會顯示所產生的註冊 PIN 碼資訊給管理員看 (僅限「裝置註冊驗證類型」設為 PIN 碼時)。 此資訊在協助使用者進行裝置註冊時很有用。

- 若是單一使用者，可透過**使用者 > 邀請使用者註冊**動作和「使用者詳細資料」頁面的「PIN 碼資訊」區段等顯示 PIN 碼。
- 若是多位使用者，在「使用者清單」頁面中，除了「PIN 碼狀態」(有效或已過期)、「已發出的 PIN 碼」和「PIN 碼有效日期」等欄位之外，還可顯示「PIN 碼」欄位。

如果您無法在**使用者**頁面上執行工作，可能是您沒有所需的權限。 您需具備下列其中一個**角色**：

- 系統管理
- 使用者管理

6.2. 使用者群組

本節包含以下各主題：

- 動態建立受管理的使用者群組
- 手動建立受管理的使用者群組
- 從其中一個重複的使用者群組建立使用者群組
- 透過上傳 CSV 檔案建立使用者群組

建立使用者群組便可將應用程式和角色指派給多名使用者。 例如，若希望所有部門經理都是應用程式和內容的管理員，則可建立一個「經理」群組。

您可以使用下列其中一個方法來建立要管理的使用者群組：

- **動態管理 (最常用)：**依據特定規則及/或屬性，動態新增/移除群組的本機和 LDAP 使用者。
- **手動管理 (用途有限)：**手動新增/移除群組的使用者。 建議您僅將「手動管理」群組用於需要較少權限的測試用途。

您可在**搜尋**欄位中輸入文字，以顯示所有名稱開頭為所輸入文字的使用者群組清單。

- 搜尋結果會在輸入文字的同時即時顯示可能相符項目清單。
- 從可能相符項目清單選擇所需的使用者群組，以便採取後續動作。
- 搜尋比對區分大小寫。

動態建立受管理的使用者群組

> 以下程序不適用於動態使用者群組。

程序

1. 按一下 **+新增**。
2. 在**名稱**欄位中，輸入使用者群組的名稱。
3. (選用) 按一下**新增描述**，以新增使用者群組的描述。
4. 按一下**動態管理 (最常用)** 選項。
5. 依據您的需求，設定自訂規則及/或屬性。 下列為可用的規則選項：
    - 自訂 LDAP 屬性
        - msExchPoliciesIncluded
        - msExchMailboxGrid
        - mailNickname

    預設 LDAP 屬性

        - samAccountName
        - userPrincipalName

    預設使用者屬性

        - email_address

- distinguished_name
- last_name
- display_name
- first_name
- 使用者群組
- 自訂使用者屬性

使用者群組 DN

- 使用者群組 GUID
- 使用者群組名稱

6. 針對每項規則，選擇本機或 LDAP 使用者。 您可以透過**使用者群組**篩選準則，來包括或排除子群組。
7. 按一下加號字元，以新增更多規則。
   可以針對已新增的規則設定**任何**或**全部**條件式篩選器。
8. 按一下加號旁的階層圖示，以建立規則群組。
9. 在規則選擇選項下方顯示的文字查詢中，檢視使用者群組的規則以及屬性。
10. 在**結果**區段中，檢閱符合設定準則的使用者詳細資料。 新增或修改規則或屬性時，您可以查看顯示的相符使用者 (若有的話)。
11. 按一下**儲存**，以儲存設定好的使用者群組。

手動建立受管理的使用者群組

1. 按一下 **+新增**。
2. 輸入群組名稱。
3. (選用) 按一下**新增描述**以輸入描述。
4. 選擇**手動管理 (用途有限)** 選項。
5. 在**搜尋使用者**欄位中，輸入要包含在群組中的每個使用者的電子郵件地址。
   在您輸入時，系統就會尋找並顯示符合的使用者 (若有的話)。
6. 選擇您想要新增至群組的使用者。 您可以視需要搜尋並新增更多使用者。
7. 按一下**儲存**。

> 您可建立手動管理使用者群組，然後將此群組新增至動態管理使用者群組中。 在這種情況下，編輯手動受管理使用者群組不會破壞動態受管理使用者群組規則。 如果將手動受管理使用者群組新增至動態受管理使用者群組，則您將無法刪除該手動受管理使用者群組。

從其中一個重複的使用者群組建立使用者群組

從 Neurons for MDM 127 開始，在規則建立器中選取了「使用者群組名稱」屬性後，管理入口網站會顯示重複的使用者群組數量及對應的 GUID 數量，以識別重複的群組。 此外，此規則之下的表格會顯示重複使用者群組的清單以及其詳細資訊，例如使用者群組名稱、GUID、來源和可分辨的名稱 (DN)。

程序

1. 登入 Ivanti Neurons for MDM 管理員入口網站。
2. 前往**使用者**，**使用者群組**。
3. 按一下 **+新增**。 建立使用者群組精靈開啟。

1. 在**名稱**欄位中指定名稱。
2. 從規則建置器選擇**使用者群組名稱**，選擇 **is equal to**，然後選擇以下*一個*重複的群組名稱。
3. 按一下 **+** 加號圖示以新增更多規則。
4. 選擇**使用者群組 GUID**，**is equal to**。
5. 從列出重複的使用者群組名稱和 GUID 的表格複製並貼上 GUID。 結果會顯示將會新增至新群組的關聯使用者。
6. 按一下**儲存**。 現在列出的使用者會新增至您建立的新使用者群組。

如果您無法在**使用者群組**頁面上執行工作，可能是您沒有所需的權限。 您需具備下列其中一個**角色**：

- 系統管理
- 使用者管理

透過上傳 CSV 檔案建立使用者群組

這項新加入的功能可讓管理員建立使用者群組，並使用 CSV 檔案將使用者新增至建立的群組。

程序

1. 登入 Ivanti Neurons for MDM 管理員入口網站。
2. 前往**使用者**，**使用者群組**。
3. 按一下 **+新增**。
4. 選取**從 CSV 匯入使用者群組**。 「匯入使用者群組」精靈隨即開啟。
    1. 在「下載 CSV」區段中，按一下**下載 CSV 範本**以下載 CSV 範本。 可使用範本來編輯檔案，以建立使用者群組，並將使用者新增至新的/現有使用者群組。
    2. 編輯並儲存 CSV 檔案後，按一下**選擇檔案**以上傳 CSV 檔案。
    3. 按一下**上傳**。 隨即顯示上傳成功的確認訊息。

屬性	描述
CSV 檔案大小限制	匯入的 CSV 檔案大小上限為 2MB。
CSV 檔案格式要求	CSV 檔案應只包含 2 欄: accountUid 和 groupName。 • accountUid 和 groupName 這兩個值均為必要值。 • 不符合上述條件的記錄將在匯入過程中捨棄。 管理員可以從匯入區段下載範例 CSV 檔案作為參考。
匯入過程中的錯誤處理	如果 CSV 匯入過程中發生錯誤或失敗，將產生錯誤檔案。 • 管理員可以下載此錯誤檔案以檢閱失敗的 CSV 列，並了解失敗的原因。 • 錯誤檔案包含失敗的特定 CSV 列，並提供失敗的解釋。
成功匯入條件	使用者群組必須在本機且為手動管理，才能成功將使用者匯入使用者群組。 • 使用者必須存在於系統中，才能成功匯入。

使用範例 CSV 檔案建立使用者群組和新增使用者的條件

範例 CSV 檔案詳細資訊-

accountUid: test_user_1@org.com

groupName: test_group_1

條件	描述
現有群組	如果群組 test_group_1 已存在，則使用者 test_user_1@org.com 將與該群組建立關聯。
非現有群組	如果群組 test_group_1 不存在，則會建立一個名為 test_group_1 的新群組，並將使用者 test_user_1@org.com 與該群組建立關聯。
非本機群組	如果群組 test_group_1 存在但不是本機群組，則此記錄將包含在錯誤 CSV 檔案中，且原因為「群組不在本機」。
非手動管理群組	如果群組 test_group_1 存在但不是手動管理的群組，則此記錄將包含在錯誤 CSV 檔案中，且原因為「不是手動管理的群組」。
非現有使用者	如果使用者 test_user_1@org.com 不存在，則此記錄將包含在錯誤 CSV 檔案中，原因為「找不到使用者」。
非現有使用者和群組	如果使用者 test_user_1@org.com 和群組 test_group_1 均不存在，則會建立一個名為 test_group_1 的新群組，且此記錄將包含在錯誤 CSV 檔案中，原因為「找不到使用者」。

6.3. 使用者設定

本節包含以下各主題：

- 編輯預設設定
- 新增自訂設定
- 刪除自訂設定
- 針對新的裝置註冊進行設定
- 設定每位使用者的裝置限制
- 設定裝置清除限制
- 使用者設定
- 設定自助式入口網站身分認證
- 設定密碼複雜度
- 定義服務條款
- 設定使用者邀請提醒電子郵件
- 設定使用者註冊確認電子郵件
- 設定使用者工作排程設定
- 設定管理入口網站身份認證設定

使用者設定可定義裝置的註冊選項。 包括如下類型：

- **裝置註冊設定**: 利用密碼和 PIN 碼或兩者設定驗證；Apple 註冊類型以及裝置擁有權。
  - 之前，如果您設定 SAML auth/IdP，SAML 驗證用於裝置註冊和入口網站驗證。
  - **平台裝置註冊設定** - 管理員現在可以透過限制特定 Apple、Android 和 Windows 平台註冊系統，在作業系統層級控制裝置註冊。 此新的 OS 層級限制設定會套用為父註冊控制項，而且在為平台啟用時，該平台的相關註冊限制會自動停用。 這有助於組織強制執行註冊原則，並防止不支援的裝置平台註冊。

裝置限制設定: 設定使用者可註冊的裝置數量。

- **抹除限制設定**: 設定可以一次抹除的裝置數量上限。
- **自助式入口網站身份認證設定：**為自助式入口網站設定密碼身份認證類型。
- **密碼複雜度設定**：針對用於裝置註冊的本機帳戶設定密碼複雜度和原則參數，然後存取管理入口網站與自助式入口網站。
- **服務條款設定**: 設定每次裝置註冊時要顯示給使用者的服務條款。
- **使用者邀請提醒設定：**設定日期與頻率以傳送使用者邀請提醒電子郵件。
- **使用者註冊確認設定：**控制是否要傳送使用者註冊確認電子郵件。 請參閱設定和使用註冊確認電子郵件以瞭解解決方案的概觀，以及下方設定使用者註冊確認電子郵件以瞭解特定使用者設定指示說明。
- **使用者工作排程設定：**控制設定使用者工作排程的功能，在非工作時間內封鎖來自 Sentry 至受管理裝置的所有通訊。 這對具離線權法律的地區很有用。
- **管理入口網站驗證設定：**控制 Ivanti Neurons for MDM 是提示管理員僅輸入密碼，還是提示管理員輸入密碼和 PIN 碼。

您可以編輯**所有使用者**群組，或新增自訂設定，再將其指派給其他使用者群組。

編輯預設設定

按一下含鎖定圖示之設定的**編輯**連結。 您無法刪除預設設定。

新增自訂設定

按一下**新增特定使用者群組的設定**連結。

刪除自訂設定

按一下 X 圖示。

針對新的裝置註冊進行設定

針對新的裝置註冊，您可以設定最低作業系統版本、驗證類型，以及裝置擁有權。 舊版 Ivanti Neurons for MDM 所產生的裝置註冊 URL 將無法在目前版本中使用。 管理員必須重新產生裝置註冊 URL 才能進行裝置註冊。

裝置註冊允許清單

僅在預設使用者設定中才可使用允許清單裝置註冊選項，在自訂使用者設定中則無法使用。 您可使用範本來上傳 CSV 檔案，其中包含序號與用來將一些裝置列入允許清單的自訂裝置屬性。 您可納入一或多個現有的自訂裝置屬性，以建立允許清單。 這可讓您在註冊之後指派屬性給裝置群組或空間。

若要自訂屬性，請前往**管理 > 屬性**。 如果啟用允許清單功能，而且在 CSV 檔案中未提到裝置序號，則不允許 iOS 和 macOS 裝置透過 iReg 註冊。 如果 CSV 檔案包含重複序號，則註冊時將使用 CSV 檔案中的最後一個輸入項目，以及與該輸入項目相關聯的自訂裝置屬性。

如果啟用了**裝置允許清單**選項，則僅允許列入允許清單的裝置註冊 Ivanti Neurons for MDM。 此功能僅適用於透過 Web 註冊程序註冊的裝置。 這並不會影響已註冊 Ivanti Neurons for MDM 的裝置。 在註冊之後，如果裝置序號從 CSV 檔案移除，該裝置不會遭淘汰。 您可選擇是否要在 CSV 檔案中提到使用者，只有在 CSV 檔案中提到使用者，而且是一位有效的使用者時，才會進行指派。

如果您想上傳新的 CSV 檔案，您可以先刪除現有 CSV 檔案，然後才上傳新檔案。 僅 iReg 支援允許清單設定，如果需要 Go 用戶端，請選擇零接觸註冊。 要使 AppConnect 和威脅防護等功能正常運行，應在系統上安裝 Go 用戶端。 我們不支援 app 內部註冊，因此使用者可以先透過 iReg 註冊裝置，稍後再從 App Catalog 推送 Go app。 當使用者接受應用程式安裝時，裝置將成為受控裝置，且所有功能將在註冊後繼續運作。 在 AppConnect 狀態為啟用或停用的裝置上無法使用零接觸配置。 只能在 AppConnect 狀態為「無」時才能使用。 AppConnect 狀態會維持為「無」，直到透過 iReg 註冊後在裝置上啟動 Go 用戶端。

程序

1. 登入 Ivanti Neurons for MDM。
2. 前往**使用者** > **使用者設定**。
3. 在**裝置註冊設定**下，按一下 **+新增特定使用者群組的設定**。
4. 編輯預設的**裝置註冊驗證類型**設定，或新增項目。
5. 在**名稱**欄位中輸入名稱。
6. (選填) 輸入設定的描述。
7. 在**作業系統設定**區段中，定義 iOS、macOS 或 Windows 的最低作業系統版本:
8. 選擇**啟用最低版本**切換按鈕，然後再從下拉式清單中選擇作業系統版本。

> 啟用最低版本設定不適用於 DEP 裝置註冊。

適用於 **Android**：

- 啟用**最低安全性修補程式**選項 (僅限 Android)，並從下列的下拉式清單選項中選擇期間類型以指定期間。

- 天
- 月
- 年

啟用**製造商允許清單/封鎖清單**選項並選擇下列選項之一：

- **建立允許清單** - 以僅允許這些製造商生產的裝置註冊。
- **建立封鎖清單** - 以防止這些製造商生產的裝置註冊。
  若要新增製造商：
  1. 按一下**新增製造商**。
  2. 在**製造商名稱**欄位中，輸入製造商的名稱。
  3. 按一下**儲存**。 表格中隨即顯示新增的製造商名稱。

     > 製造商名稱有區分大小寫。 若要編輯或刪除已新增的製造商名稱，請按一下該製造商的**編輯**或**刪除**選項。

在 Apple 註冊區段，選擇 Apple 註冊類型：

- **裝置註冊**
- **使用者註冊** - 依預設，「使用者註冊」適用於 iOS 和 iPadOS 裝置。
- (選用) **包括 macOS 裝置 (macOS 10.15+)** - 選擇此選項，讓「使用者註冊」也適用於 macOS 裝置。

在**註冊邀請方法 (僅限 iOS 和 Android)**區段中，啟用**僅限 MAM 註冊**。

> 應針對 MAM-Only 裝置註冊啟用此選項，啟用後，會將使用者重新引導至公開的 App Store 下載 AppStation 用戶端 app。

11. 在**裝置註冊驗證類型**區段中，從**選擇註冊類型**下拉式清單中選擇下列註冊類型選項之一。 若使用「裝置註冊」，請確定「裝置註冊」組態符合所選。
    - **僅限密碼**
    - **僅限 PIN 碼** 選擇此選項時，「繞過 IdP 裝置註冊驗證」切換按鈕已鎖定。
    - **密碼和 PIN 碼**

      > 使用者可能仍會收到 PIN 碼，以利完成帳戶啟用。

> 此設定會影響一般註冊和 Device Enrollment 註冊。

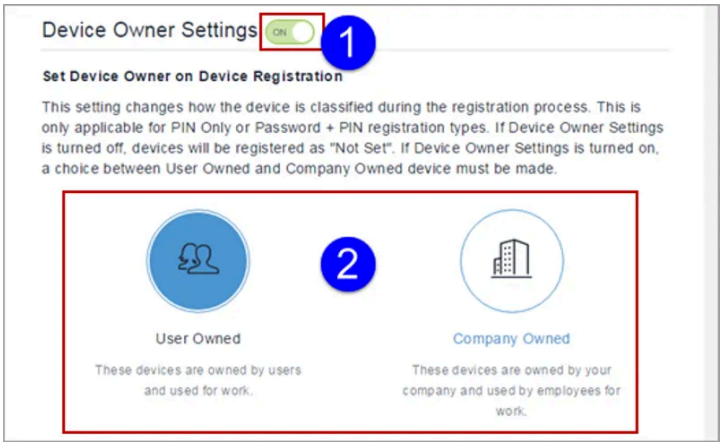
對於 PIN 碼，請指定下列內容。 如有需要，在進行裝置註冊時，使用者可以按一下**重新傳送 PIN 碼**。

- **PIN 碼時效**：PIN 碼保持有效的期間 (1 至 30 天)。
- **PIN 碼長度**：字元數 (4 至 12)。
- **可讓使用者要求新的 PIN 碼**：(忘記或過期時)。

您也可以開啟**裝置擁有者設定**，然後按一下**使用者擁有**或**公司擁有**。 此設定會變更裝置在註冊程序期間的分類方式。

- 如果**裝置擁有者設定**為「開啟」，且管理員已將裝置標示為「使用者擁有」，則在裝置註冊期間與自助式入口網站中，使用者都會看到將裝置標示為「使用者擁有」或「公司擁有」的選項。 針對已註冊使用者註冊裝置，不論管理員所做選擇為何，預設的「裝置擁有者設定」都將為「使用者擁有」。

- 若是受監管的裝置，「裝置擁有者設定」必須設為「公司擁有」。



針對您要發佈設定的目標使用者群組 (至少一個)，按一下 **+新增**。

15. (僅限 iOS 和 macOS 裝置的**隨選即用功能**) 或者，開啟**裝置允許清單**選項，可允許根據允許清單列出的序號註冊裝置。
16. 按**下一步**。 使用者設定發佈頁面開啟。
17. 選擇使用者群組發佈。
18. 按一下**完成**。
19. 傳送邀請給使用者。 如需更多資訊，請參閱**邀請使用者**。

注意以下幾點:

> 若使用「僅限 PIN 碼」選項註冊使用者裝置，則使用者會收到一封註冊確認電子郵件，其中包含用於驗證的 PIN 碼。

- 系統會傳送一個 PIN 碼至使用者的電子郵件 ID。
- 使用者在裝置註冊頁面上輸入 PIN 碼。
- 若 PIN 碼正確，則指導使用者完成註冊程序。

對於透過 SAML 型**身分識別提供者** (IdP) 設定的使用者，Ivanti Neurons for MDM註冊裝置時支援 PIN 碼型身分驗證。 「裝置註冊身分驗證類型」應為 PIN 碼或 PIN 碼和密碼。 PIN 碼和密碼功能具有雙重要素驗證作用，可提高安全性。 因此，當這類使用者嘗試註冊裝置時：

- 系統會傳送一個 PIN 碼至使用者的電子郵件 ID。
- 使用者在裝置註冊頁面上輸入 PIN 碼。
- 如果 PIN 碼正確，使用者會被重新導向至 IdP 的登入頁面，以便使用者輸入 IdP 使用者名稱和密碼。
- 如果 IdP 憑證是正確的，使用者會被重新導向至裝置，以便完成註冊程序。

設定每位使用者的裝置限制

程序

1. 編輯預設的**裝置限制**設定，或新增項目。
2. (選擇性) 按一下 **+ 新增特定使用者群組的設定**，為特定使用者群組設定裝置限制。
3. 編輯或指派可識別該設定的名稱。
4. 針對該設定輸入選填的描述。

5. 從**使用中裝置的數量上限**下拉式清單中，選取作用中 Apple 裝置的限制。
6. 從**與 iPhone 配對的 Apple watchOS 裝置的最大數量**下拉式清單中，選取與 iPhone 配對的作用中 Apple watchOS 裝置限制。
7. (選擇性) 如果已選取 **+ 新增特定使用者群組的設定**，請按一下**下一步**，並選擇至少一個使用者群組來發佈此設定。
8. 按一下**完成**。

設定裝置清除限制

程序

1. 編輯預設的**裝置清除限制**設定。
2. 開啟**為所有使用者 (包括預設角色) 啟用清除限制**選項。
3. 在**使用者每次可清除的裝置數目上限**欄位中，輸入每次可清除的最多裝置數目。 預設值為 1。 您可以將最大值 200 設為裝置清除限制。
4. 按一下**完成**。

設定自助式入口網站身分認證

程序

1. 編輯預設的**自助式入口網站身分認證**設定，或藉由按一下**+ 新增特定使用者群組的設定**來新增一個設定。
2. 編輯或指派可識別該設定的名稱。
3. 針對該設定輸入選填的描述。
4. 從下拉式清單選擇**自助式入口網站身分認證類型**。 可以是下列選項之一：
   - 密碼
   - 認證
5. 按**下一步**。
6. 選擇將發佈此配置至其中的一或多個使用者群組。
7. 按一下**完成**。

設定密碼複雜度

您可以針對用於裝置註冊的本機帳戶設定密碼複雜度和原則參數，然後存取管理入口網站與自助式入口網站。

> 請注意，下面設定的密碼長度、特性和原則將決定密碼的安全性。

這也會決定使用者選擇有效密碼的難度。 如果您使用一般使用者的本機帳戶，但您想要用安全密碼來存取管理入口網站，請考慮使用 PIN 來進行裝置註冊，以確保密碼複雜度不會干擾裝置註冊。 在**使用者設定 > 裝置註冊設定**底下，使用「裝置註冊驗證類型」設定來選取裝置註冊的驗證模式。

程序

1. 編輯預設的**密碼複雜度**設定。
2. 定義下列密碼複雜度設定：

設定	方法
密碼長度下限	移動滑桿以指定密碼的長度下限，以防止使用者建立不安全的短密碼。 數字範圍介於 8 到 32。
需要特性	指定選擇密碼時應符合的密碼特性數目。 應符合的特性數目下限為 3 個 (聯邦客戶為 4 個)。
需要特殊字元 (符號)	指定密碼應包含的非英數字元數目。
需要大寫字元	指定密碼應包含的大寫字母字元數目。
需要小寫字元	指定密碼應包含的小寫字母字元數目。
需要數字字元	指定密碼應包含的數字字元數目。
密碼驗證	
允許的數字序列	選擇序列中重複數字的數目。 例如：123。
允許的重複字元	選擇重複字母字元的數目。 例如：bbc。

3. 設置下列密碼原則設定以自訂行為。

設定	方法
保留的密碼歷程記錄	移動滑桿以選擇使用者帳戶必須要建立多少個新密碼，之後才能重複使用舊密碼。 數字範圍介於 3 到 36。
密碼到期時間	移動滑桿以選擇密碼到期期限 (天)。 數字範圍介於 30 到 365 天。
閒置逾時	移動滑桿以指定使用者閒置多久時間之後，管理入口網站和自助式入口網站的工作階段將逾時。 數字範圍介於 5 到 60 (分鐘)。
登入失敗次數臨界值	移動滑桿以選擇在 5 分鐘帳戶登出生效之前的登入失敗嘗試次數。 數字範圍介於 2 到 5。 當嘗試登入的失敗次數還在臨界值限制內時，系統會向使用者顯示鎖定和稍後再嘗試登入的相關訊息。 當嘗試登入的失敗次數超出臨界值限制時，系統會向使用者顯示鎖定和過了指定時間 (分鐘) 後再嘗試登入的相關訊息。

4. 按一下**完成**。 如果您已變更密碼複雜度預設設定，現有本機帳戶的較舊密碼將保持不變。 到期時，系統將會提示使用者更新密碼。 嘗試登入管理入口網站的管理員可聯絡服務台，他們可提供密碼重設指引。

> 在註冊裝置時，建議的方法是使用僅限 PIN 碼註冊模式。

定義服務條款

程序

1. 建立新的**服務條款**設定。
2. 指派可識別的設定。
3. 針對該設定輸入選填的描述。
4. 選擇**提示使用者...** 選項。
5. 輸入要顯示的標題和文字。
6. 針對您要發佈設定的目標使用者群組 (至少一個)，按一下 **+新增**。
7. 按一下**儲存**。

> 一旦接受以後，就無法刪除服務條款。 不過，可以透過清除**提示使用者...** 關閉新註冊提示。 選項。

設定使用者邀請提醒電子郵件

管理員可以透過使用此設定傳送使用者邀請提醒電子郵件來驅使裝置註冊。

程序

1. 編輯現有的**使用者邀請提醒設定**或新增設定。
2. 編輯或指派可識別該設定的名稱。
3. 針對該設定輸入選填的描述。
4. 確認**使用者邀請提醒**選項已開啟。
5. 在定義開始日期和結束日期區域中，選擇您要開始和停止傳送電子郵件提醒的時間。

> 可傳送之電子郵件的數量上限為 30。 若要重設此限制，管理員應重送邀請。

6. 在定義頻率區域中，選擇您要傳送電子郵件提醒的頻率。
7. 按**下一步**。
8. 選擇此配置的發佈。
9. 按一下**完成**。

設定使用者註冊確認電子郵件

管理員可傳送電子郵件給已完成註冊的新使用者。

程序

1. 編輯現有的**使用者註冊確認設定**或新增設定。
2. 編輯或指派可識別該設定的名稱。
3. 針對該設定輸入選填的描述。
4. 確定**使用者註冊成功時傳送確認電子郵件**選項已開啟。
5. 按**下一步**。
6. 選擇此配置的發佈。
7. 按一下**完成**。

設定使用者工作排程設定

管理員可針對使用者設定使用者工作排程，在非工作時間內封鎖來自 Sentry 至受管理裝置的所有通訊。 這對具離線權法律的地區的使用者很有用。

程序

1. 選擇**使用者**
2. 選擇**使用者設定**。
3. 在**使用者工作排程設定**一節中，選擇 **+新增特定使用者群組的設定**。
4. 提供設定的名稱。
5. 開啟設定。
6. 選擇時區。
7. 設定 Ivanti Neurons for MDM 封鎖 Exchange ActiveSync 通訊協定、啟用 AppConnect 的應用程式和受管理應用程式的小時數。
8. 按**下一步**。
9. 設定發佈，然後按一下**完成**。

> 套用的變更可能需要最長 1 小時 15 分鐘才會在裝置上生效。

設定管理入口網站身份認證設定

管理員可設定身份認證類型以驗證使用者登入。 此設定控制是否要提示使用者「僅限密碼」或「密碼和 PIN 碼」。

程序

1. 編輯現有的**管理入口網站身份認證設定**或新增設定。
2. 編輯或指派可識別該設定的名稱。
3. 針對該設定輸入選填的描述。
4. 在**管理入口網站身份認證類型**中，選擇下列選項之一：

選項	描述
密碼	選擇此選項以僅使用密碼來驗證登入身份。 使用者可能仍會收到 PIN 碼，以利完成帳戶啟用。
密碼和 PIN 碼	選擇此選項以使用密碼和 PIN 碼來驗證登入身份。 當您選擇此選項，隨即顯示下列額外欄位： • **PIN 碼有效期**：從下拉式清單選擇 PIN 碼有效期的分鐘數。 分鐘數應介於 1 到 15 之間。 • **PIN 碼長度**：從下拉式清單選擇 PIN 碼的字元長度。 PIN 碼長度應介於 4 到 12 之間。 此選項僅適用於本機帳戶，不適用於 LDAP 管理帳戶。
可讓使用者要求新的 PIN 碼	選擇此選項可讓使用者請求新的 PIN 碼。

5. 按**下一步**。
6. 選擇此配置的發佈。
7. 按一下**完成**。

對於透過 SAML 型身份識別提供者 (IdP) 設定的使用者，註冊裝置時 Ivanti Neurons for MDM 支援 PIN 碼型身份認證。 「管理入口網站身份認證類型」應為「PIN 碼和密碼」。 此功能用來擔任雙因子身份認證，藉此提高安全性。 因此，當這類使用者嘗試登入入口網站時：

- 系統會傳送一個 PIN 碼至使用者的電子郵件 ID。
- 使用者在管理入口網站登入頁面上輸入 PIN 碼。
- 如果 PIN 碼正確，使用者會被重新導向至 IdP 的登入頁面，以便使用者輸入 IdP 使用者名稱和密碼。
- 如果 IdP 憑證是正確的，使用者會被重新導向至管理入口網站。

登入管理入口網站時，使用者可以按一下**忘記密碼**以重設密碼。 在下一個畫面中，使用者可以輸入新密碼或傳送至使用者電子郵件地址的 PIN 碼 (根據先前的使用者身分認證模式設定來決定是否提示)。 如有需要，您可以按一下**重新傳送 PIN 碼**。 使用者必須在兩次「忘記密碼」要求之間等候 15 分鐘。

> 當此配置發佈到裝置時，使用者使用密碼或 PIN 碼連續嘗試登入失敗 (預設值：5 次) 會導致帳戶鎖定，並會向使用者顯示鎖定相關資訊的訊息。

6.4. 使用者品牌

「使用者品牌」可讓您利用使用者認識的名稱與標誌，來自訂裝置註冊程序。 您可用下列方式自訂向使用者顯示的品牌：

- 為註冊 URL 設定自訂的主機名稱
- 在註冊電子郵件與註冊畫面中顯示您的標誌
- 在註冊活動期間顯示自訂的網頁圖示

> 更新上述設定會變更 **$** 引用的值。

授權：Gold

必要條件：

- 決定您要用於自訂 URL 的主機名稱。 名稱必須符合下列需求：
  - 不含空格
  - 不含特殊字元

取得符合下列需求的標誌檔案：

  - PNG 格式
  - 580 x 80 畫素

取得符合下列需求的網頁圖示檔案：

  - PNG 格式
  - 64 x 64 畫素

程序：

1. 前往**使用者 > 使用者品牌**。
2. 按一下**自訂** (右上角)。
3. 在**主機名稱**欄位中，輸入要做為 URL 主機名稱的簡短名稱。
4. 按一下**檢查可用性**，確認您輸入的主機名稱沒有其他人使用。
5. 如果主機名稱無法使用，請輸入其他名稱。
6. 記下 **URL 預覽**下方產生的註冊 URL。
7. 按**下一步**。
8. 在**標誌**下方，按一下**選擇檔案**，並上傳標誌以用於註冊電子郵件和註冊畫面。
9. 按**下一步**。
10. 在**網頁圖示**下，按一下**選擇檔案**，上傳要在註冊活動期間顯示為 Ivanti Neurons for MDM 網頁圖示的網頁圖示。
11. 按一下**完成**。

6.5. 透過 Apple 商務管理進行使用者註冊

本節包含以下各主題：

- 啟用「使用者註冊」的需求
- 註冊的優先順序
- 標準 MDM 註冊和使用者註冊之間的差異
- 使用者註冊和裝置註冊之間的差異
- 將 Ivanti Neurons for MDM 連線至 Apple 商務管理

適用於：

- iOS 13.0 到 Ivanti Neurons for MDM 支援的最新版本未受監管裝置。
- 使用 macOS 10.15 或支援的更新版本 Ivanti Neurons for MDM 的裝置。

Apple Business Manager 頁面可讓 IT 團隊自動化裝部署、購買和散發內容，以及管理其組織中的角色。 Apple Business Manager 建置使用者註冊 – 此註冊選項適用於實施 BYOD (自攜裝置，Bring Your Own Device) 的公司。 使用者註冊為 MDM 通訊協定的修改版本，更注重使用者隱私權，以企業所需的安全性層級建置。

使用者註冊允許管理員執行以下操作:

- 安裝和移除受管理的應用程式
- 安裝和移除網路組態配置
- 安裝專用於受管理 app 和帳戶的局部 VPN
- 要求使用密碼

啟用「使用者註冊」的需求

以下為啟用使用者註冊的需求。 如果有任一條件未符合，註冊類型將會是裝置註冊。

- iOS 13.0 到 Ivanti Neurons for MDM 支援的最新版本未受監管裝置，或 macOS 10.15 或 Ivanti Neurons for MDM 支援的最新版本裝置。
- Apple 註冊類型欄位的使用者設定應設為「使用者註冊」。
- Apple Business Manager 帳戶。
    - Apple App License 帳戶必須是相同 Apple Business Manager 帳戶的一部分。
    - 在 Apple Business Manager 內，如果您有帳戶列在「地點」中，就必須要有符合相同地點的 Apps and Books。 您可能需要新增地點 (例如，West Coast)。

受管理的 Apple ID - 受管理的 Apple ID 將會與每個註冊的裝置建立關聯。

- 此受管理的 Apple ID 將為 MDM 管理與 app 授權提供身份認證。
- 當 MDM 下推 app 和媒體時，會將必要的 Apple 授權指派至與該裝置關聯的受管理 Apple ID。
- 根據 GDPR 合規性規定，考量到 Apple ID 屬於使用者資料，受管理的 Apple ID 在使用者清單及使用者詳細資料頁面中皆經遮罩處理。
- 受管理的 Apple ID 最初用於 Apple School Manager，現在 Apple Business Manager 則將它運用於使用者註冊。

> 裝置的受管理 Apple ID 和 Apps and Books 地點權杖應來自同一個 Apple Business Manager 帳戶的組織。

如果兩者不同，當 app 的授權配置失敗，將會在 Ivanti Neurons for MDM 管理入口網站顯示通知。

Microsoft Entra ID 已設為同盟驗證，或使用已驗證的網域在 Apple 商務管理中手動建立 Apple ID。

- 有關使用同盟驗證的說明，請參閱 Apple 網站上的 **Apple Business Manager 使用指南**。 需要登入。

會指派一個裝置管理角色給同步至 LDAP 的裝置使用者，並與受管理的 Apple ID 建立關聯。

在**使用者**清單頁面和**裝置**清單頁面中，您可以新增要向所有使用者顯示的「受管理 Apple ID」欄。 在**裝置**清單頁面中，您可以新增「已註冊使用者註冊」欄以顯示使用者註冊裝置的狀態。 此外，使用者和裝置匯出會包括這些欄，並匯出為 CSV 檔案。

註冊的優先順序

- 透過 Go for iOS 用戶端和 iReg 支援使用者註冊。 Apple 不再支援透過 Ivanti Go for iOS 和 iReg 進行使用者註冊。 **帳戶導向使用者註冊**僅適用於裝置的工作或學校帳戶。
- 自動化 Device Enrollment 和 Apple Configurator 註冊一律為裝置註冊。
- 如果套用 MAM 配置至裝置，MAM 註冊會優先於使用者註冊。
- 如果符合 auth-only 和使用者註冊要求，則使用者註冊會取得優先。
- 如果您從 iOS 專用的 Go 用戶端重新註冊裝置，註冊類型將會和裝置註冊期間的類型相同，不論在 Ivanti Neurons for MDM 中的註冊類型如何改變。 例如，如果裝置為使用者註冊，在 Ivanti Neurons for MDM 變更為 Device Enrollment，然後從 Go 用戶端重新註冊裝置，該裝置仍會為使用者註冊，而非裝置註冊。

標準 MDM 註冊和使用者註冊之間的差異

本節說明標準 MDM 註冊和透過 Apple Business Manager 進行使用者註冊之間的差異。

標準 MDM 註冊

以下為 Ivanti Neurons for MDM伺服器在標準 MDM 註冊下可以做，但是在使用者註冊模式下無法做到的事。

MDM 伺服器：

- 無法清除裝置。
- 無法檢視裝置使用者已在裝置上安裝的個人 app。
- 無法將使用者安裝的 app 轉換為 MDM 已受管理的 app。
- 無法清除裝置驗證碼 (即 解除裝置鎖定)。
- 無法設定較長、複雜的裝置密碼要求。
- 無法設定全裝置範圍的 VPN 或 Wi-Fi Proxy，也無法進行任何行動電話功能管理。
- 無法檢視裝置識別碼，例如 UDID、序號或 IMEI。
- 無法套用許多全裝置範圍的限制 (例如限制 app 內容評等)、封鎖 iCloud，以及套用任何受監管的限制。

透過 Apple Business Manager 進行使用者註冊

在使用者註冊中，MDM 伺服器仍可執行管理企業 app、帳戶和資料所需的一切活動。

使用者註冊可以：

- 透過基於使用者的 (Apple) Apps and Books 授權安裝內部開發的 app 或其他 app。
  - 授權採用先到先得方式套用，提供受管理的 Apple ID 使用。
  - 安裝在使用者註冊裝置上的 app 使用的授權與安裝在裝置註冊裝置上的相同 app 使用的授權不同。
  - 在使用者詳細資料頁面中透過「授權用量」索引標籤檢查 Apple Apps and Books 應用程式的授權：「註冊類型」將顯示為使用者註冊或 Device Enrollment。

強制執行密碼裝載設定。 例如：

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

查詢企業管理 app、憑證和描述檔相關資料。

- 設定個別 app VPN，用於 MDM 安裝的 app、郵件、通訊錄和行事曆。
- 強制執行某些限制，例如受管理的 open in、受管理的通訊錄、鎖定畫面上的受管理資料等。

企業資料儲存在個別 Apple File System (APFS) 磁碟區 (在註冊時建立)，並從裝置使用者資料個別加密。 此磁碟區包含受管理 app 儲存的資料、企業 Notes、企業 iCloud Drive 文件、企業 Keychain 項目、受管理郵件附件和內文，以及行事曆附件。 從 MDM 取消註冊會銷毀磁碟區和金鑰。

所有第三方應用程式只能是個人應用程式或透過 Ivanti Neurons for MDM 管理的應用程式。 MDM 服務無法開始管理裝置使用者安裝的 app。 在此情況下，管理員將需要要求裝置使用者先刪除個人 app，然後再透過 MDM 安裝 app。 MDM 服務無法開始管理使用者安裝的 app。 但是，某些系統 app (例如 Notes 和 Files) 將支援工作和個人帳戶。

macOS 裝置的使用者註冊

macOS 10.15 或支援的更新版本 Ivanti Neurons for MDM 裝置可支援「使用者註冊」。

- macOS 已註冊使用者註冊裝置不支援適用於 macOS 的 Mobile@Work。
  - 即使 app 已發佈至 macOS 已註冊使用者註冊裝置，app 也不會從 MDM 推送至裝置。
  - 因此，macOS 已註冊使用者註冊裝置不支援 Mobile@Work 功能，例如封裝工具 (MIP) app 的指令碼管理及 app 管理等。

macOS 已註冊使用者註冊裝置的 app 相依性與行為變更。

  - 在 macOS 已註冊使用者註冊裝置中，app 相依性係按盡最大努力之原則運作，因為 MDM 在發佈主要 app 之前並不知道 (無法確認) 先決條件 app 的安裝狀態。
  - App 和配置可發佈至屬於 macOS 已註冊使用者註冊裝置的使用者和使用者群組。 不過，app 一律會顯示**安裝**按鈕，而非「已安裝」，因為 MDM 無法顯示 macOS 已註冊使用者註冊裝置中 app 的安裝狀態。
  - 已安裝的 app 在**裝置 > App 庫存**中顯示為「要求的 App」，因為 macOS 已註冊使用者註冊裝置並不會在庫存報告中告知 Ivanti Neurons for MDM 伺服器是否已安裝 app。

在 app 的發佈篩選中，可視需要將已註冊使用者註冊和已註冊自動化 Device Enrollment 屬性用於自訂發佈。

- 使用受管理的 Apple ID 來安裝 Apple Apps and Books 應用程式即可支援使用者型授權。 裝置型授權則不受允許。 App Catalog 只會顯示 Apple Apps and Books 應用程式。
- 並非所有配置、原則和動作皆在允許之列。 請查看此程序後面所列的配置與原則完整清單。
  - 如果將不支援的配置發送至 macOS 已註冊使用者註冊裝置，這些配置將不會發送或套用至裝置，而且可能會顯示如下的訊息「Restrictions - this is not a valid request type」(限制 - 這不是有效的要求類型)。

- 同樣地，Ivanti Neurons for MDMUI 中也將收到不支援的管理裝置動作通知。
- Ivanti Neurons for MDM不會傳送不支援的報告。

以下是不支援發送至 macOS 已註冊使用者註冊裝置的配置與原則：

- 密碼
- Tunnel
- Tunnel (隨選)
- VPN 配置
- Office 365 自動帳戶建立
- macOS 核心擴充原則
- 隱私權偏好設定
- macOS 限制
- 軟體更新
- AirPrint
- MI 用戶端隱私權
- FileVault 2
- FileVault 復原金鑰
- 防火牆
- 系統原則規則
- 憑證偏好設定
- 系統原則控制
- 受管理的系統原則
- macOS AppStore 限制
- macOS 燒錄光碟限制
- macOS Finder 設定
- 適用於 macOS 的 Mobile@Work
- 適用於 macOS 的 Mobile@Work 指令碼
- 允許的媒體控制
- 時間伺服器
- 允許的 App 原則

使用者註冊和裝置註冊之間的差異

本節說明使用者註冊和 Device Enrollment 之間的差異。

使用者註冊適用於 iOS 13.0 和 macOS 10.15 到支援的最新版本裝置。 版本低於 iOS 13.0 和 macOS 10.15 的裝置將會被視為「裝置註冊」，不論裝置使用者是否已啟用使用者註冊。

> 適用於 Apple Business Manager 的使用者註冊不允許抹除或解除鎖定。 但是，使用者入口網站仍會提供這些選項 (即使它們沒有作用)。

使用者註冊 vs Device Enrollment			
功能	使用者註冊	MAM	裝置註冊
清除裝置及檢視使用者的個人 app	✗	✗	✓
轉換受管理到未受管理，反之亦然	✗	✗	✓
清除裝置密碼、設定全裝置範圍的 VPN 或 Wi-Fi Proxy，或管理行動電話功能	✗	✗	✓
檢視裝置識別碼，例如序號、IMEI	✗	✗	✓
套用受監管的限制	✗	✗	✓ (僅限受監管裝置)
可安裝和設定 app 和帳戶	✓	✓	✓
可設定個別 app VPN，用於 MDM 安裝的 app、郵件、通訊錄和行事曆。	✓	✗	✓
可強制執行某些限制，例如受管理的 open in、受管理的通訊錄、鎖定畫面上的受管理資料等	✓	✗	✓
可查詢企業管理 app、憑證和描述檔相關資料	✓	✗	✓

將 Ivanti Neurons for MDM 連線至 Apple 商務管理

本節說明如何針對 Apple Business Manager 啟用使用者註冊。

必要條件

- 您必須要有 Apple Business Manager 帳戶。 請參見 https://business.apple.com/。
- 您必須要求並安裝 Apple **MDM 憑證**，以管理 iOS 裝置。

建立本機使用者以啟用使用者註冊

本節說明如何建立本機和 LDAP 使用者，以及針對未受監管的 Apple 裝置設定使用者註冊。 使用者註冊無法用於受監管的裝置或在 Apple 的 Device Enrollment 中註冊的裝置。

手動建立受管理的 (靜態) 使用者群組

此為一次性程序。 如果您已建立此群組，請跳至「為使用者註冊建立使用者」一節。

程序

1. 前往**使用者 >** 使用者群組。
2. 建立手動受管理的 (靜態) 使用者群組 (例如使用者註冊群組)，以新增裝置註冊類型為使用者註冊的使用者。
3. 按一下**儲存**。

建立裝置註冊類型設定

此為一次性程序。 如果您已建立此群組，請跳至「為使用者註冊建立使用者」一節。 針對已註冊使用者註冊裝置，預設的「裝置擁有者設定」將為「使用者擁有」。

程序

1. 前往**使用者** > 使用者設定。
2. 在裝置註冊設定章節中，按一下 **+新增特定使用者群組的設定**。
3. 針對裝置註冊類型為使用者註冊的使用者建立新設定 (例如 UE 註冊)。
4. 在 Apple 註冊區段，選擇**使用者註冊**為 Apple 註冊類型。
5. 按**下一步**。
6. 在使用者設定發佈頁面，選擇剛建立的使用者群組，例如使用者註冊群組。
7. 按一下**完成**。

為使用者註冊建立本機使用者

先決條件是，為使用者註冊建立手動管理的使用者群組和裝置註冊設定。

程序

1. 前往使用者。
2. 按一下 **+新增** > **單一使用者**。
   輸入新使用者資訊並將它新增至剛建立的使用者群組，例如使用者註冊群組。 如需詳細資訊，請參閱使用者主題中的*新增使用者*。

匯入 LDAP 使用者以啟用使用者註冊

必要條件

- 先決條件是，設定 Ivanti Neurons for MDMConnector 以存取 **LDAP** 資源。
- 確保**受控 Apple ID** 設定已設為**模式** (使用者電子郵件地址)。 確定受管理的 Apple ID 的模式是獨一無二的。 否則，如果有另一個帳戶使用相同的受管理 Apple ID，將不會使用該受管理的 Apple ID 更新帳戶。
- (選用) 納入 appleid 子網域，避免與現有 Apple ID 衝突。
- 您可以從 LDAP 匯入使用者並邀請他們加入使用者註冊。 針對匯入的 LDAP 使用者，使用者註冊會要求將受管理的 Apple ID 與 Ivanti Neurons for MDM 同步。

程序

1. 前往**使用者**。
2. 按一下 **+新增 > 邀請來自 LDAP 的使用者**。
3. 按一下 LDAP 伺服器項目中的**選擇使用者**。
4. 在「新增 LDAP 使用者」頁面的搜尋欄位中，輸入使用者、群組或 OU 的名稱。
5. 若要加入新的使用者或群組，請按一下要加入之項目旁的 **+新增**。
6. 按一下**完成**。

匯入 Entra ID 使用者以啟用使用者註冊

先決條件是，將 Ivanti Neurons for MDM 連線至 Microsoft Entra ID (Entra ID)。

您可以邀請 Entra ID 使用者進行使用者註冊。 匯入的 Entra ID 使用者需要將他們的受管理 Apple ID 與 Ivanti Neurons for MDM 同步，這是使用者註冊的要求。

程序

1. 前往**管理員 > Entra ID 使用者來源**。
2. 編輯設定。
3. 選取**啟用此 Entra ID**。
4. 在受控 Apple ID 設定中，選取以下選項之一:
   - **模式**
     - **使用者電子郵件地址** - 確認受控 Apple ID 的模式是唯一的。 否則，如果有另一個帳戶使用相同的受管理 Apple ID，將不會使用該受管理的 Apple ID 更新帳戶。
     - 或選取 **userUPN**。
5. (選用) 納入 appleid 子網域，避免與現有 Apple ID 衝突。
6. 選取**自動邀請從 Entra ID 匯入的使用者**。 從 Entra ID 匯入 Ivanti Neurons for MDM 的使用者將自動受邀透過電子郵件註冊。
7. 按一下**儲存**。

使用使用者註冊進行註冊的裝置使用者說明

本節說明裝置使用者在註冊 Apple 使用者註冊時需要執行的動作。

程序

1. 在您要註冊的 iOS 裝置上，開啟包含連結和文字的邀請電子郵件，引導使用者前往註冊連結，例如 mobileiron.com/go。
2. 在 Safari 中開啟註冊連結。
3. 登入頁顯示。 裝置使用者使用其本機使用者或 LDAP 憑證登入。
   註冊頁面會顯示訊息，指出描述檔已下載。
   輕點設定。 設定頁面顯示。
4. 輕點註冊 [您的公司名稱]。
5. 使用者註冊頁面顯示。
6. 點選註冊我的 [您的裝置]。 。例如，註冊我的 iPhone。
   如果您輕點「取消」和「刪除描述檔」，將會從頭開始註冊程序。
   您將會看到 Apple 或同盟帳戶登入畫面。 輸入您受管理的 Apple ID 的密碼。 (受管理的 Apple ID 將會列在您登入頁面的最上方。)
   您可能會看到保持登入選項，請進行選擇。
   將會出現頁面指出「註冊成功」。

使用裝置記錄進行疑難排解

如要對使用者註冊裝置進行錯誤或問題疑難排解，請先檢視裝置日誌。

程序

1. 前往裝置。
2. 按一下裝置，以顯示裝置詳細資料頁面。 您可以確認已使用者註冊和已註冊受管理的 Apple ID 欄位是否正確。
3. 選擇日誌標籤。

4. 在「篩選」區中，使用篩選功能根據動作名稱 (例如「移出」、「裝置名稱」、「設定啟動程序權杖」、「取得啟動程序權杖」等等)、狀態、開始日期和結束日期等來精簡裝置日誌。
5. 在動作欄中，按一下眼睛圖示，以顯示裝置日誌詳細資料，例如註冊 ID。
6. 按一下**確定**。

6.6. 使用者授權

Ivanti Neurons for MDM 以使用者為基礎的授權定義了您可註冊的使用者數量、針對每個使用者授權允許的裝置數量、可配置並發佈到裝置的內容數量，以及可供使用的功能。 當您達到使用者限制時，「管理」頁面上就會顯示一個紅色的三角形。 當您達到內容限制時，服務就不會再讓您新增更多項目，並會顯示一則訊息，指出您已達到限制。

若要判斷應規劃的使用者授權數量，請考慮下列選項：

- 在 Secure UEM 或 Secure UEM Premium 套件下購買的每個使用者授權最多可註冊五台裝置。
- 只要使用者註冊超過五台裝置，就必須要求其他使用者授權。
- 我們沒有強制限制使用者可以要求的使用者授權數。
- 只要裝置淘汰或清除時，就會釋出授權。

例如，若 User1 一到任就註冊了工作手機，並要求使用者授權。 一個禮拜以後，她使用相同授權註冊了兩台個人手機和平板電腦。 如果她又註冊一台平板電腦，就有五台裝置了，因此必須要求第二個使用者授權。 當她的個人手機遭竊而清除掉該裝置時，就會釋出第二個使用者授權。

檢視使用者的裝置/授權數量

程序：

1. 前往**使用者**。
2. 按一下使用者的連結。

左窗格會列出使用者詳細資料，包括授權用量。

6.7. 管理使用者

本節包含以下各主題：

- 新增用於 Cisco ISE 作業的 API 使用者
- 指派角色至使用者
- 使用者角色
- 搜尋與篩選使用者
- 指派使用者至使用者群組
- 邀請使用者
- 啟用與停用使用者
- 針對多次的管理員登入進行管理
- 變更密碼
- 傳送訊息
- 將使用者從使用者群組中移除
- 刪除使用者
- 匯出使用者
- 指派自訂屬性給使用者
- 移除使用者的自訂屬性
- 變更使用者地區設定
- 編輯使用者名稱
- 退出位置資料收集
- 逾時資訊
- 退出系統使用量分析
- 透過產生 PIN 進行裝置註冊

6.7.1. 新增用於 Cisco ISE 作業的 API 使用者

可以新增角色為「Cisco ISE 作業」的 API 使用者，以便讓 Cisco ISE 與 Ivanti Neurons for MDM 中的 Cisco ISE API 互動。 建立此使用者之後，可以從 Cisco ISE 使用此使用者的憑證來驗證進入 Ivanti Neurons for MDM 的 API 呼叫。 這些 API 可讓 Cisco ISE 取得裝置資訊、對裝置採取動作，例如：完整清除、企業清除、PIN 鎖定，以及傳送訊息給裝置。

> API 使用者將無法登入管理入口網站。 此使用者僅啟用 API 使用。

> 依預設，僅租戶的超級管理員會指派為「Cisco ISE 作業」角色。 超級管理員必須明確選擇系統中必須擁有此角色的其他使用者，並指派此角色給他們。 被指派「Cisco ISE 作業」角色的使用者，也可以指派此角色給系統中其他適合的使用者。

程序

1. 前往**使用者** > **使用者**。
2. 按一下**新增**。
3. 選擇 **API 使用者**。
4. 填妥表單的下列使用者資訊：
    - 電子郵件地址
    - 名字
    - 姓氏

> 「使用者名稱」欄位會顯示您輸入的電子郵件地址。 在大多數情況下，您都不應編輯這項預設值。 請參閱**編輯使用者名稱的時機**。

如果您想要變更此使用者的顯示名稱，可編輯**顯示名稱**欄位中的預設文字。

6. 輸入**密碼**和**確認密碼**欄位，以便指派密碼。
7. 在**指派角色**區段中選擇 **API 管理 Cisco ISE 作業**角色。
8. 按一下**完成**以新增使用者。

如果您無法在**使用者**頁面上執行工作，可能是您沒有所需的權限。 您需具備下列其中一個**角色**：

- 系統管理
- 使用者管理

6.7.2. 指派角色至使用者

可以透過指派角色提供 (Undefined variable: 使用者群組) 資料和功能的存取權給使用者。您可直接指派角色給使用者或使用者群組。 指派角色給{{使用者群組}}會將該角色給予該群組中所有的使用者。

> 預設不會指派使用者唯讀角色給使用者。
> 針對同時有權存取 Ivanti Neurons for UEM 和 Ivanti Neurons for MDM 的租用戶，會對其隱藏「角色」頁面及相關選項。

使用者無法指派他們尚未取得的權限。 未指派給使用者的權限和角色不會顯示為選項。 在這種情況下，將會顯示錯誤訊息。 當 Ivanti Neurons for MDM 管理員或合作夥伴管理員嘗試指派角色給合作夥伴管理員時，Ivanti Neurons for MDM 會顯示訊息，指出合作夥伴管理員必須在服務提供者入口網站上執行此項操作。

如需更多資訊，請參閱角色管理。

程序：

1. 前往：
   - **使用者 > 使用者***或*
   - 使用者 > 使用者群組。

選擇一或多個使用者或使用者群組。

3. 按一下**動作**。
4. 從「使用者」詳細資料頁面或「使用者群組」詳細資料頁面，按一下**指派角色**或
   從「使用者」清單或「使用者群組」清單頁面選擇**附加角色**。
5. 選擇一或多個下列您想指派的角色：
   - 系統管理 | 跨空間
   - 系統唯讀 | 跨空間
   - 使用者管理 | 跨空間
   - 使用者唯讀 | 跨空間
   - LDAP 使用者匯入及邀請 | 跨空間
   - 裝置管理 | 空間專用
   - 裝置唯讀 | 空間專用
   - App 及內容管理 | 空間專用
   - App 及內容唯讀 | 空間專用
   - 裝置動作 | 空間專用
   - Cisco ISE 作業 | 跨空間
   - 排程作業管理 | 跨空間
   - 通用平台服務 (CPS) | 跨空間
   - 低使用者影響移轉管理 | 跨空間
   - 自訂裝置註冊 | 跨空間
   - 編輯 Microsoft Graph | 跨空間
   - 傳送/取消抹除 | 跨空間

- 檢視 Microsoft Graph | 跨空間
- 管理 Access 整合 | 跨空間

按**下一步**。

7. 如果所選角色屬於空間繫結，請選取適用於所有空間繫結角色的空間。

> 如果只有一個空間 (預設空間)，則指派空間綁定角色時將會略過「指定空間」步驟。

摘要頁面中空間綁定的空間名稱會顯示為「預設空間」。
檢閱待指派角色的摘要，然後按一下**完成**。

提供服務台人員基本裝置動作使用權限

一般來說，服務台角色僅可讓員工檢視資料。 不過，有些組織希望將下列基本裝置動作納入權限：

- 強制登記
- 鎖定
- 取消鎖定
- 傳送訊息
- 淘汰
- 抹除

程序

您可以提供權限給上述動作。

1. 前往**使用者 > 使用者**或**使用者 > 使用者群組**。
2. 選擇一或多個使用者或使用者群組。
3. 按一下**動作**。
4. 從「使用者」詳細資料頁面或「使用者群組」詳細資料頁面選擇**指派角色**，*或*
   從「使用者」清單或「使用者群組」清單頁面選擇**附加角色**。
5. 選擇**裝置唯讀**。
6. 選擇**裝置動作**。
7. 按一下**完成**。

> 請您務必先選擇「裝置唯讀」之後才選擇「裝置動作」，以便使用者取得預期的權限。

6.7.3. 使用者角色

使用者角色決定使用者可以在 Ivanti Neurons for MDM 中看到的頁面以及使用者可以執行的操作。 下表顯示您可指派的角色與意義。

角色	描述	空間專用
系統管理	可讓管理員管理租戶層級的設定，如 MDM 憑證、App Catalog 設定等各種項目。	否
系統唯讀	可讓管理員檢視租戶層級的設定，如 MDM 憑證、App Catalog 設定等各種項目。	否
使用者管理	可讓管理員新增和移除使用者、指派角色，以及新增使用者到使用者群組。	否
使用者唯讀	可讓管理員檢視使用者、使用者群組、app 及內容目錄。	否
裝置管理	可讓管理員管理裝置群組、配置和原則，並執行所有的裝置動作。	「是」
裝置唯讀	可讓管理員檢視裝置群組、配置及原則。	「是」
App 及內容管理	可讓管理員新增、發佈和移除 App 及內容。	「是」
App 及內容唯讀	檢視「使用者」、「App」、「內容」中的資料，包括 AppConnect 工作	「是」
裝置動作	可讓管理員起始裝置動作，例如： • 強制登記 • 鎖定 • 取消鎖定 • 傳送訊息 • 淘汰 • 抹除 必須先選擇「裝置唯讀」之後才能選擇「裝置操作」。 否則使用者將無法得到預期的權限。	「是」
LDAP 使用者匯入及邀請	可讓管理員註冊 LDAP 使用者，並傳送註冊裝置的邀請	否
Cisco ISE 作業	可讓管理員叫用必要的 API 以進行 Cisco ISE 整合。	否
排程作業管理	允許管理員建立與管理各種管理作業的排程作業。	否
通用平台服務 (CPS)	可讓管理員使用通用平台服務。	否
低使用者影響移轉管理	可讓管理員管理「低使用者影響移轉」設定。	否
自訂裝置註冊	可讓管理員使用自訂裝置註冊來註冊裝置。	否
編輯 Microsoft Graph	可讓管理員編輯用於 Office 365 App 保護的 Microsoft Graph API 設定。	否
檢視 Microsoft Graph	可讓管理員檢視用於 Office 365 App 保護的 Microsoft Graph API 設定。	否
傳送/取消抹除	可讓管理員傳送抹除命令至裝置，或是在發出的抹除命令執行之前取消它。	否
管理 Access 整合	可讓管理員管理 Access 整合。	否

如需更多資訊，請參閱指派角色。

6.7.4. 搜尋與篩選使用者

本節包含以下各主題：

- 搜尋使用者
- 使用使用者的進階搜尋
- 載入使用者的搜尋查詢
- 篩選使用者

搜尋使用者

若您已新增許多使用者，可使用篩選或搜尋功能以快速找到使用者項目。

程序

1. 前往**使用者**。
2. 在搜尋方塊中輸入字元。

使用使用者的進階搜尋

您可使用進階搜尋選項根據規則來搜尋使用者，以識別和檢視符合特定準則的使用者。 這些規則選項可以用「任何 (或)」或「所有 (及)」選項來建立巢狀結構。 符合規則的使用者會顯示在此區段下方。 您可以使用以下運算子來建構規則:

- 開頭為
- 結尾是
- 包含
- 不包含
- 開頭不是
- 結尾不是
- 小於
- 大於
- 在範圍內
- 等於
- 不等於

從 Neurons for MDM 127 開始，在規則建立器中選取了「使用者群組名稱」屬性後，Ivanti Neurons for MDM 管理入口網站會顯示重複的使用者群組數量及對應的 GUID 數量，以識別重複的群組。 此外，此規則之下的表格會顯示重複使用者群組的清單以及其詳細資訊，例如使用者群組名稱、GUID、來源和可分辨的名稱 (DN)。

程序

1. 從使用者頁面，按一下**進階搜尋**連結。
2. 如果使用者要符合至少一項規則，請按一下**任一**，或如果使用者必須符合所有規則，請按一下**全部**。
3. 建立一個定義搜尋準則的規則，例如使用者群組、自訂使用者屬性和自訂 LDAP 屬性。
4. (選用) 按一下 + 以視需要建立其他規則。
5. (選用) 按一下**儲存**以儲存查詢。

6. 按一下**搜尋**。 符合搜尋準則的使用者清單會顯示在此頁面。

載入使用者的搜尋查詢

程序

1. 從使用者頁面，按一下**進階搜尋**連結。
2. 按一下「資料夾」圖示。 **進階搜尋**視窗顯示。 建立的搜尋查詢清單會顯示在**載入查詢**區段。 此區段會顯示下列詳細資訊：
   - **查詢名稱** - 載入查詢的名稱。
   - **查詢內容** - 顯示定義搜尋查詢的規則內容。
   - **動作** - 選擇要對查詢執行的動作。
3. 按一下**動作**欄中的**載入查詢**，以檢視符合載入查詢中定義準則的使用者清單。
   如要刪除載入查詢，按一下刪除圖示。

篩選使用者

「篩選」側邊導覽列會列出各種區段以協助您在整個使用者清單中搜尋使用者。 「管理篩選」精靈包含所有區段的清單，使您可以選取要顯示在「篩選」導覽列中的區段。

程序

1. 前往**使用者**。
2. 在「管理篩選」精靈中列出的區段中按一下相關核取方塊。 您可以搜尋下列區段:
   - 管理員
   - Google 狀態
   - 邀請狀態
     - 已完成 (已收到邀請並回覆的使用者)
     - 已過期 (使用者未及時回應)
     - 未邀請 (您並未邀請此名使用者)
     - 待處理 (待處理的使用者回應。)

   密碼到期

     - 到期 (密碼到期選項設為有限日期的使用者。)
     - 永不 (密碼到期選項設為永不的使用者。)
   - 使用者群組 (選擇感興趣的{{尋找使用者}}。)
   - 使用者來源
     - LDAP
     - Entra ID
     - 名冊
     - Salesforce
     - 本機
   - 同步
     - 直接同步 - 列出直接與 LDAP 伺服器同步的使用者

- 不同步 - 列出從 LDAP 伺服器移除的使用者
- 間接同步 - 列出間接與 LDAP 伺服器同步的使用者
- 不適用

3. (選用) 按一下**還原預設值**將選取的項目還原為預設篩選。 「篩選」導覽列會顯示選取的區段。 若您清除「管理篩選」精靈中的所有核取方塊，則「篩選」側邊導覽列會顯示所有區段。
4. 按一下「管理篩選」精靈以外的任何位置即可結束精靈。
5. 按一下 x 圖示以關閉「篩選」側邊導覽列，按一下**篩選**則可重新開啟側邊導覽列。

6.7.5. 指派使用者至使用者群組

本節包含以下各主題：

- 從「使用者」頁面指派使用者
- 從「使用者群組」頁面指派使用者

指派使用者至使用者群組，非常有利於將下列重複作業的次數降至最低：

- 發佈 app
- 指派角色

從「使用者」頁面指派使用者

1. 前往**使用者**。
2. 選擇您需要的使用者。
3. 按一下**動作**。
4. 選擇**指派給群組**。
5. 選擇群組或按一下**新建**以開啟新的群組。
6. 按一下**儲存**。

從「使用者群組」頁面指派使用者

1. 前往**使用者 > 使用者群組**。
2. 選擇您需要的使用者群組。
3. 按一下**動作** (右上角)。
4. 選擇**指派使用者**。
5. 輸入每位使用者的電子郵件地址。
6. 按一下**指派使用者**。

6.7.6. 邀請使用者

新增使用者時，您可以邀請使用者註冊裝置。 事實上，預設已選好此選項。 受邀請的使用者會收到一封包含註冊相關資訊的電子郵件訊息。 您也可以從**使用者 > 使用者**頁面邀請 (或重新邀請) 使用者。

程序

1. 前往**使用者**。
2. 選擇您要邀請的使用者。
3. 選擇**動作 > 傳送邀請**。 此時將顯示「邀請預覽」以及用於將裝置擁有權設定為**使用者擁有**或**公司擁有**的選項。

4. 或者，開啟**裝置擁有者設定**。
5. 按一下**使用者擁有**或**公司擁有**。 此設定會變更裝置在註冊程序期間的分類方式。 僅適用於「僅限 PIN 碼」或「密碼 + PIN 碼」註冊類型。 若**裝置擁有者設定**已關閉，裝置將被註冊為「未設定」。對於受監督的裝置，裝置擁有者設定將為「公司擁有」。
6. 按一下**傳送**。 若執行了 PIN 碼型的裝置註冊，則使用者將收到寄至其註冊電子郵件地址的 PIN 碼。 若設定了 QR 碼型註冊，則使用者將收到一個 QR 碼。
7. 按一下**確定**。

> 如果已依照**設定和使用註冊確認電子郵件**中的說明啟用了註冊確認電子郵件功能，您還會看到提醒訊息，指出使用者將會在註冊成功後收到註冊確認電子郵件。 若要收到此電子郵件，使用者必須已列入您在**使用者設定**的**設定使用者註冊確認電子郵件**中所指定的通訊群組清單。

如需更多資訊，請參閱**匯入 LDAP 使用者**。

6.7.7. 啟用與停用使用者

本節包含以下各主題：

- 啟用與停用本機使用者
- 啟用與停用 LDAP 使用者

本機與 LDAP 使用者可以是啟用或停用狀態。 您可根據他們的狀態建立自訂原則，在規則建置器中運用「已啟用使用者」條件並設定條件的動作。 例如，您可以自訂原則規則，以淘汰屬於已停用之本機/LDAP 使用者的裝置。

啟用與停用本機使用者

本機使用者建立好之後，使用者預設為啟用狀態。

程序

1. 前往**使用者**。
2. 按一下本機使用者的顯示名稱。
3. 按一下**編輯**。 **需要身分驗證**視窗隨即顯示。
4. 請輸入您的管理員密碼，然後按一下**驗證**。

> 當輸入多個不正確的密碼時，若超過「密碼複雜度設定」中所設的「登入失敗次數臨界值限制」，帳戶將被鎖定，且您將會從目前的工作階段登出。

5. 選擇或取消選擇**已啟用**選項，以分別啟用或停用本機使用者。
6. 按一下**儲存**。

啟用與停用 LDAP 使用者

您只能啟用或停用 Microsoft Active Directory 的 LDAP 使用者。 在 Microsoft Active Directory 中，當您開啟使用者帳戶的屬性時，請按一下**帳戶**索引標籤，然後選擇或清除**帳戶**選項對話方塊的勾選框，指派數值給 **UserAccountControl** 屬性。 指派給屬性的值告知 Windows 哪些選項已啟用。 在您指派數值給 UserAccountControl 屬性之後，使用者狀態會在 LDAP 與 Ivanti Neurons for MDM 同步後予以反映。

以下是您可能指派的值：

- 512 - 已啟用。
- 514 - 已停用。
- 66048 - 已啟用，密碼永不到期。
- 66050 - 已停用，密碼永不到期。

檢視使用者帳戶

程序

	1.	按一下開始。
	2.	前往程式。

	3.	前往管理工具。

	4.	按一下Active Directory 使用者和電腦。

如需詳細資訊，請參閱 https://support.microsoft.com/en-in/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-pro。

您可使用 Ldp.exe 工具或 Adsiedit.msc 嵌入式管理單元來檢視與編輯屬性。 僅限有經驗的管理員才能使用這些工具來編輯 Active Directory。 在您從原始的 Windows 安裝媒體安裝支援工具之後，即可使用這兩項工具。

6.7.8. 針對多次的管理員登入進行管理

支援多個 Ivanti Neurons for MDM 管理入口網站工作階段，因此管理員可以同時檢視入口網站的不同頁面。 如果您是管理員，可以檢視上一次的登入日期，以掌握多次登入的情況。

檢視最近一次的管理員登入

程序

1. 按一下**帳戶** `
2. 檢視**上一次登入日期**項目。

6.7.9. 變更密碼

本節包含以下各主題：

- 從「使用者」索引標籤變更密碼
- 套用密碼永不到期
- 移除密碼永不到期設定

> 如果使用者擁有系統管理角色，則僅限超級使用者或目前登入的使用者才能看見**變更密碼**選項。

您可以變更 Ivanti Neurons for MDM 密碼。 如果您具備相關權限，亦可變更其他使用者的密碼。

程序

1. 按一下「帳戶」圖示 (右上角)。
2. 
   從下拉式功能表選擇**變更密碼**。
3. 輸入您目前的密碼。
4. 輸入您的新密碼。
5. 再次輸入您的新密碼。
6. 若要將密碼設為不到期，請選擇**將密碼設為永不到期**。

> 將密碼設為永不到期會覆寫在「使用者」>「使用者設定」>「密碼複雜度設定」中所定義的**密碼到期時間**。

7. 按一下**完成**。

> 若要將本機帳戶的密碼重設為會到期，請取消選擇**將密碼設為永不到期**。 取消選擇此選項後，隨即顯示快顯視窗，其中顯示先前對使用者套用的密碼到期日。

從「使用者」索引標籤變更密碼

程序

1. 前往**使用者**。
2. 按一下使用者的顯示名稱。
3. 按一下**編輯** (左上角)。 **需要驗證**視窗隨即開啟。 在編輯使用者之前，管理員 (本機使用者或 LDAP 使用者) 必須輸入管理員密碼以進行驗證。
4. 請輸入您的管理員密碼，然後按一下**驗證**。

> 當輸入多個不正確的密碼時，若超過「密碼複雜度設定」中所設的「登入失敗次數臨界值限制」，帳戶將被鎖定，且您將會從目前的工作階段登出。

5. 在**目前密碼**欄位中，輸入目前密碼。

> 如果您要變更其他使用者的密碼，則不會顯示此欄位。

6. 在**變更密碼**欄位中，輸入新密碼。
7. 確認新密碼。
8. 按一下**儲存** (左上角)。

套用密碼永不到期

1. 前往**使用者**。
2. 選擇一或多位使用者。
3. 按一下**動作**。
4. 選擇**指派密碼永不到期**。 隨即顯示**將本機帳戶密碼設為永不到期**視窗。
5. 按一下**提交**。

移除密碼永不到期設定

1. 前往**使用者**。
2. 選擇一或多位使用者。
3. 按一下**動作**。
4. 選擇**移除密碼永不到期**。 隨即顯示**移除本機帳戶密碼設為永不到期**視窗。
5. 按一下**提交**。 移除此設定後，將會對使用者套用先前的密碼到期日。

6.7.10. 傳送訊息

本節包含以下各主題：

- 傳送訊息給使用者
- 傳送訊息給裝置

您可以向任何已知使用者傳送訊息。 訊息的形式可以是電子郵件或{{推送通知}}。 僅有已註冊裝置的使用者可以收到推送通知。

必要條件

- 對於 iOS 裝置，確保已安裝 Go 用戶端。
- 對於 macOS 裝置，確保已安裝 Mobile@Work 用戶端。

傳送訊息給使用者

1. 前往**使用者 > 使用者**。
2. 選擇您要傳送訊息的使用者。
3. 按一下**動作** (右上角)。
4. 按一下**傳送訊息**。
5. 如果您不想傳送電子郵件，可清除**傳送電子郵件訊息**勾選方塊。
6. 如果要傳送電子郵件，請輸入主旨和訊息文字。
7. 如果要傳送推送通知，請選擇**傳送推送通知**勾選方塊，並輸入訊息文字。
8. 按一下**傳送**。

傳送訊息給裝置

1. 前往**裝置 > 裝置**。
2. 選擇您要傳送訊息的裝置。
3. 按一下**動作** (右上角)。
4. 按一下**傳送訊息**。
5. 或者，按一下裝置名稱連結，以前往「裝置詳細資料」頁面，然後按一下**傳送訊息**  圖示。
6. 如果您不想傳送電子郵件，可清除**傳送電子郵件訊息**勾選方塊。
7. 如果要傳送電子郵件，請輸入主旨和訊息文字。
8. 如果要傳送推送通知，請選擇**傳送推送通知**勾選方塊，並輸入訊息文字。

> 推送通知訊息也可以包括使用者可存取的 URL。

9. 按一下**傳送**。
   收到推送通知時，使用者可在裝置螢幕工具列上看到鈴鐺圖示。 使用者點一下鈴鐺圖示，即可檢視所接收通知的歷程記錄，並且執行動作或刪除通知。

> **裝置**和**使用者**頁面中均可用，管理員可以將特定裝置或使用者屬性插入訊息，然後排入佇列以進行最終使用者傳送。

6.7.11. 將使用者從使用者群組中移除

本節包含以下各主題：

- 從「使用者」頁面移除使用者
- 從「使用者群組」頁面移除使用者

將使用者從使用者群組中移除時，表示：

- 會將任何指派給該群組的角色從該名使用者身上移除
- 任何指派給該群組的 app 將不再顯示於該名使用者的 {{App Catalog}} 中
- 會將之前設定為可移除的 app 從該名使用者的裝置上移除

從「使用者」頁面移除使用者

1. 選擇您需要的使用者。
2. 按一下**動作** (右上角)。
3. 選擇**從群組移除**。
4. 選擇群組。
5. 按一下**移除**。

從「使用者群組」頁面移除使用者

1. 按一下使用者群組以顯示詳細資料。
2. 按一下**編輯** (右上角)。
3. 按一下您要移除之使用者旁的**移除**連結。
4. 按一下**儲存** (右上角)。

6.7.12. 刪除使用者

本節包含以下各主題：

- 刪除本機使用者時，會有什麼結果
- 那 LDAP 使用者呢？

程序

1. 前往**使用者 > 使用者**。
2. 選擇所要的使用者項目。
3. 按一下**動作** (右上角)。
4. 選擇**刪除**。

當 Ivanti Neurons for MDM 管理員或合作夥伴管理員嘗試刪除合作夥伴管理員時，Ivanti Neurons for MDM 會顯示訊息，指出合作夥伴管理員必須在服務提供者入口網站上執行此項操作。

> 若使用者有一些與其帳戶關聯的裝置，則首先必須停用並刪除這些裝置，然後刪除此使用者。 若使用者沒有裝置，則刪除使用者時即可刪除使用者資訊。

刪除本機使用者時，會有什麼結果

- 系統也會將已刪除使用者的所有相關資訊刪除。
- 與此使用者相關聯的裝置會被淘汰。
- 此使用者上傳的內容仍會保留。
- 該使用者帳戶將不能再進行任何裝置註冊。

那 LDAP 使用者呢？

- 如果停用 LDAP 伺服器時，即無法永久刪除 LDAP 使用者。 下一次 LDAP 資料同步即會還原已刪除的 LDAP 使用者。
- 如果已將 LDAP 伺服器或群組刪除，LDAP 使用者即會變成本機使用者，並可將其刪除。
- 當從 LDAP 刪除使用者時，並不會從 Cloud 將其刪除。 同步狀態將切換為「NO_SYNC」，但並不會移除使用者。

6.7.13. 匯出使用者

作為管理員，您可從 Ivanti Neurons for MDM 匯出使用者清單。

> 當使用者的裝置註冊 PIN 匯出至 CSV 檔案時，基於安全理由，PIN 將會標示為「」而非實際的 PIN。

程序

1. 前往**使用者 > 使用者**。
2. 選取清單中的一個或多個使用者。
3. 按一下**匯出至 CSV**。

系統會以彈出訊息提示您，告知報告的匯出需要一些處理時間。 提交要求後，您必須等候完成要求，然後再提交另一項要求。 報告就緒後，系統會以訊息提示您下載或刪除產生好的報告。 您也會收到一封包含報告下載連結的電子郵件。

> **自訂使用者**及 **LDAP** 屬性詳細資訊也可連同其他詳細資訊，一併匯出為 CSV 檔案。

> 用來新增使用者的任何欄位值含有 +、-、= 或 @ 字元時，已匯出 CSV 檔案中的使用者資料就會在該欄位自動加上單引號 (') 前綴，此外，直立線 (|) 符號前則會新增反斜線 (\)。 這樣做是為了防止 Excel 插入弱點。

6.7.14. 指派自訂屬性給使用者

您可指派自訂使用者屬性給一或多位使用者，例如：部門。 每個屬性都有一個對應值，可用於建立組態和使用者群組等任務。 可指派自訂屬性給一個或多個使用者。

程序

1. 必要時，前往**管理員 > 系統 > 屬性**新建自訂屬性。
2. 前往**使用者**。
3. 選擇一或多位使用者。
4. 按一下**動作**。
5. 選擇**指派自訂屬性**。
6. 請選擇下列選項之一：
    - 即使有找到任何既有的值，仍要強制指派 (覆寫) 所有屬性。
    - 僅有當值為空白時才覆寫，並略過具備既有值的屬性。

選擇您想指派的屬性並輸入值 (不允許空白值)。

8. 按一下**指派**。

相關主題：

- 屬性
- 變數

6.7.15. 移除使用者的自訂屬性

您可以移除一個或多個使用者的自訂屬性。

> 請謹慎操作，因為此動作不可還原。

程序

1. 前往**使用者**。
2. 選擇一或多位使用者。
3. 按一下**動作**。
4. 選擇**移除自訂屬性**。
5. 選擇您要移除的屬性。
6. 按一下**移除**。

相關主題：

- 屬性
- 變數

6.7.16. 變更使用者地區設定

依預設，使用者地區設定會設為租用戶地區設定。 您可視需要變更單一使用者的地區設定。

程序

1. 前往**使用者**。
2. 按一下使用者的顯示名稱。
3. 按一下**編輯**。 **需要身分驗證**視窗隨即顯示。
4. 請輸入您的管理員密碼，然後按一下**驗證**。

> 當輸入多個不正確的密碼時，若超過「密碼複雜度設定」中所設的「登入失敗次數臨界值限制」，帳戶將被鎖定，且您將會從目前的工作階段登出。

5. 在「地區設定」欄位下方，按一下**變更**。
6. 在**變更使用者地區設定**視窗的**將使用者地區設定變更為:** 下拉式清單中，選擇所需的地區設定。
7. 按一下**完成**。
8. 按一下**儲存**。

6.7.17. 編輯使用者名稱

新增使用者時，您輸入的電子郵件地址文字也會自動列為使用者名稱。 在大多數情況下，您都應原封不動這項預設使用者名稱，因為：

- 以電子郵件地址為格式的使用者名稱是必要的。
- 使用{{配置}}中的使用者名稱變數很方便，不過也可以使用電子郵件地址。

只有在現有使用者名稱發生衝突的罕見情況下需要編輯使用者名稱，因為在整個裝置管理系統中，使用者名稱必須是唯一的。 這種衝突發生的情況可能是由於組織的兩個部門都註冊了裝置管理系統。

如果發生使用者名稱衝突時

如果因為發生使用者名稱衝突導致您無法新增使用者時，您可使用電子郵件地址的格式來輸入不同的使用者名稱。 這個電子郵件地址可以與實際的電子郵件地址不相符。 例如，您可以變更下列電子郵件地址:

ksmith@mycompany.com

至

ksmith21@mycompany.com

如果您編輯了使用者名稱，則這名使用者之所有以使用者名稱作為變數的配置都將無法運作。 您要改用電子郵件地址變數，來建立其他的配置。

6.7.18. 退出位置資料收集

本節包含以下各主題：

- 若是 iOS 裝置
- 若是 Android 裝置

如果啟用位置資料的收集時已套用隱私權組態，則裝置使用者可覆寫此組態。

若是 iOS 裝置

iOS 裝置使用者可使用以下設定關閉位置服務，以避免將位置資料傳送到裝置管理系統:

設定 > 隱私權 > 定位服務

若是 Android 裝置

Android 裝置使用者可以關閉位置設定，以防止位置資料遭到收集。 此設定的位置依據不同製造商而異。 在要求位置資料時，Android 裝置使用者也會收到接受要求的提示。

6.7.19. 逾時資訊

管理入口網站的閒置逾時為 5 到 60 分鐘，逾時為 24 小時。

程序

1. 前往**使用者 > 使用者設定**。
2. 編輯預設的**密碼複雜度**設定。
3. 在「密碼原則」區段中，移動**閒置逾時**滑桿以指定使用者閒置多久時間之後，管理入口網站和自助式入口網站的工作階段將逾時。 數字範圍介於 5 到 60 (分鐘)。
4. 按一下**完成**。

6.7.20. 退出系統使用量分析

收集匿名產品診斷和使用量資料，以協助產品改善。

如果您想保有使用狀況資料的所有權，您可選擇停止傳送系統使用狀況分析。

程序

1. 在 Ivanti Neurons for MDM 管理入口網站中按一下頁面底部的**使用狀況資料**連結。**使用量資料**視窗隨即顯示。
2. 取消選取**傳送診斷和使用狀況資料**核取方塊。
3. 按一下**儲存**。

6.7.21. 透過產生 PIN 進行裝置註冊

本節包含以下各主題：

- 在使用者登陸頁面中針對單一或多個使用者進行操作
- 在使用者詳細資訊中針對單一使用者進行操作

您可以為使用者產生裝置註冊 PIN，而不需傳送邀請電子郵件，這樣可讓裝置註冊流程更簡單。

在使用者登陸頁面中針對單一或多個使用者進行操作

1. 前往**使用者** > **使用者**。
2. 選取要為其產生註冊 PIN 的使用者。 您可以選取一或多個使用者。
3. 按一下**動作**按鈕。
4. 從下拉式功能表選取**產生 PIN**。
5. 產生的 PIN 將顯示在**註冊 PIN** 欄中。
6. 若要檢視 PIN，請按一下**檢視 PIN**。

在使用者詳細資訊中針對單一使用者進行操作

1. 前往**使用者** > **使用者**。
2. 針對要為其產生註冊 PIN 的使用者，按一下其使用者名稱以開啟使用者詳細資訊。
3. 在「使用者資訊」區段中，按一下**產生 PIN**。
4. 按一下**檢視 PIN**，即可檢視產生的 PIN。

> 請確認您有適當的權限可為使用者產生註冊 PIN。 只能針對裝置註冊狀態為「密碼和 PIN」的使用者啟用「產生 PIN」選項。

7. 裝置

本節包含以下各主題：

- 開始使用裝置
- 裝置群組
- App 庫存
- 管理裝置

7.1. 開始使用裝置

本節包含以下各主題：

- 管理裝置
- 在裝置上執行動作
- 設定裝置的時區
- 依準則列出裝置
- 顯示詳細的裝置資訊
- 針對裝置大量指派或變更使用者和自訂屬性
- 將裝置匯出至 CSV 檔案
- 搜尋裝置日誌

裝置頁面中的每個項目都代表已向 Ivanti Neurons for MDM 註冊的行動裝置，並列出每個裝置的相關重要資訊。 「裝置清單」頁面顯示裝置的相關資訊，例如：

- 名稱
- 電子郵件地址
- 電話號碼
- 作業系統
- 裝置類型
- 狀態
- 最近一次簽入
- 違規計數
- 空間
- 合法擁有者 (iPad 共享)

Wi-Fi IP 位址會回報給 Ivanti Neurons for MDM 伺服器。 每次登記時都會回報 IP 位址的任何變更。 裝置清單頁面和裝置詳細資料頁面中都提供 GDPR 合規性 IP 位址的選項。 此功能需要裝置透過 Go 5.5 for iOS 或更新版本，以及 Ivanti Neurons for MDM 支援的 Go 72 for Android 或更新版本進行註冊。

> 由於 Ivanti Neurons for MDM 版本增加了新的 GDPR 欄位 (例如「IP 位址」和 eSIM ID)，已設定 GDPR 的管理員必須編輯 GDPR 描述檔才能隱藏新欄位。

將裝置清單匯出為試算表 (CSV) 格式時，設備識別碼 (EID) 會顯示為 iOS 屬性。 EID 和行動 EID (MEID) (出現時) 會分別前置於 EID 字串或 MEID 字串。

> 如果相同裝置上有不同的用戶端識別碼，並註冊了各種不同租戶，Ivanti Neurons for MDM 伺服器就無法處理這類裝置。 如果相同裝置上有不同的用戶端識別碼，伺服器只能處理註冊了相同租戶的裝置。

管理裝置

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 前往**裝置**。
3. 選擇一或多台裝置。
4. 從**動作**下拉式清單選取動作。

以下表格會列出「裝置」頁面中的可用動作：

類別	動作
通用	• 新增至群組 • AppConnect 解除鎖定> • 指派自訂屬性 • 指派給使用者 • 裝置合規性狀態同步 • 停用遠端桌面 • 啟用遠端桌面 • 啟用/停用 Bluetooth • 強制登記 • 鎖定 • 移除自訂屬性 • 重新啟動/關閉 • 裝置合規性狀態同步 • 裝置淘汰 • 傳送訊息 • 設定擁有權 • 取消鎖定 • 清除
iOS macOS Android Windows	• 指派給合法擁有者 (僅限 iPad 共享) • 重新安裝 iOS 系統 App • 設定時區 • 設定 macOS 自動管理密碼 • 設定/變更韌體密碼 • 設定/變更復原鎖定 • 進入單一應用模式 • 退出單一應用模式 透過 Ivanti Bridge 的指令碼和動作

在裝置上執行動作

「動作」功能表 (省略符號按鈕) 可讓您在選取的裝置上執行各種動作。

程序

1. 按一下裝置名稱。 「裝置詳細資料」頁面開啟。
2. 按一下動作 (省略符號) 功能表以執行以下其中一個裝置動作：
    - 變更裝置名稱
    - 刪除裝置
    - 編輯群組成員
    - 啟用/停用 Bluetooth
    - 透過 Ivanti Bridge 的指令碼和動作
    - 提取 Ivanti Bridge 記錄檔
    - 放棄擁有權
    - 要求偵錯日誌
    - 重新啟動/關閉裝置
    - 淘汰
    - 設定擁有權
    - 設定/變更復原鎖定
    - 抹除
    - 裝置合規性狀態同步

設定裝置的時區

適用於：iOS 14.0+ 和 tvOS 14.0+ 裝置

此動作不需要定位服務。 時區裝置動作也會顯示在裝置的裝置詳細資料頁。 在裝置中所做的時區變更也會反應在 Ivanti Neurons for MDM 伺服器中。

> 若在 **iOS 限制組態**中啟用了**強制自動的日期與時間**限制，則此裝置操作會觸發錯誤。

程序

1. 選擇一或多台裝置。
2. 對所選裝置按一下**動作** > **設定時區**。
3. 以 Olson 時區 ID 格式，輸入時區字串。 例如，Pacific/Midway。
4. 按一下**設定時區**。

依準則列出裝置

您可以使用「篩選」側邊導覽列來搜尋及檢視整個裝置清單中的特定裝置。 使用「空間」下拉式清單選取所有或特定空間以檢視裝置及其相關資訊。 也可使用顯示版本或套組版本搜尋裝置。 「裝置」面會顯示裝置的套組版本和顯示版本。

> 在「裝置群組」頁面按一下**裝置數量**欄下列出的數字，或是在**應用程式詳細目錄頁面**按一下**安裝數量**欄下列出的數字，會顯示訊息指出頁面中所列裝置的空間名稱。

顯示詳細的裝置資訊

按一下項目的「名稱」欄位，即可顯示「裝置詳細資料」頁面。 「裝置詳細資料」包含多個索引標籤，以整理下列資訊：

- **概觀** - 下表列出「概觀」索引標籤上顯示的所有詳細資料:
- **組態** - 顯示已套用{{組態}}的詳細資訊。如需更多資訊，請參閱使用配置。

區段名稱	描述
一般	• 裝置位置 • 製造商 • Wi-Fi MAC 位址 • Wi-Fi IP 位址 (Android 裝置) • 網路綁定 - (iOS 裝置) • 有電池 - (僅適用於 macOS 13.3+) • IP 位址 • 公用 IP 位址 - 顯示 Android 或 ChromeOS 裝置的 IP 位址。 如果裝置連線到 VPN 或 Proxy 伺服器，則會顯示 Proxy WAN IP 位址。 • 型號 - (macOS 13.3+ 和 iOS 16.4+) • 序號 • 替代序號 (Android 裝置) - 製造商專屬序號適用於處於「裝置管理」或「裝置擁有者」模式的 Samsung 裝置。 • 鎖定 PIN 碼 - 管理員可以遠端鎖定受管理裝置，並產生唯一的 PIN 碼以手動解除鎖定。 選取**檢視**，以針對具有管理員權限的使用者在**裝置詳細資料**頁面上顯示 PIN 碼。 僅適用於 macOS 裝置。 • 儲存空間使用 - 裝置上已用 (Windows 除外) 與可用的內部儲存空間 • 可用的電池 (Android) • 電池狀態 (Android) - 充電中、放電中、已充滿和未充電 • 電池的估計剩餘電力 (Windows) • 電池的估計執行時間 (Windows) • 可用更新 (macOS) • 可用更新名稱 (macOS) • 作業系統版本 • 作業系統組建版本 • 補充建置版本 • 補充作業系統/版本額外資訊 • Apple 矽裝置 • 韌體版本 • 裝置來源 • 合法擁有者 • 多位使用者模式 • 時區 • 上次已知裝置解除鎖定密碼 • 安全鎖定模式 • 系統更新 (Android 裝置) • Zebra 修補程式版本 (Android 裝置)

區段名稱	描述
	• 上一個 Hotfix ID - (Windows 裝置) • 上一個 Hotfix 安裝在 - (Windows 裝置) • MDM 註冊類型 • MDM 返回服務 (iOS 27.0+ 和 visionOS 27.0+)
設定	• 裝置名稱 • 裝置識別碼 • 裝置 GUID • Device Enrollment 裝置 (Apple 裝置) • 已註冊 Device Enrollment (Apple 裝置) • 已啟用自動化 Device Enrollment • 已註冊自動化 Device Enrollment • 已註冊使用者註冊 (Apple 裝置) • 已註冊受管理的 Apple ID (Apple 裝置) • 裝置群組 • 語言 • MDM 裝置識別碼 • 裝置用戶端 ID • 用戶端 App 版本 • 用戶端 App 套件 ID • 已註冊的用戶端 • EAS 裝置識別碼 • 啟用啟用鎖定 • 已啟用 Apple 宣告式管理 • Apple DDM 應用程式已啟用 • 啟用鎖定密碼鎖 • 服務條款 • 擁有權 • iTunes 帳號啟用 • 裝置定位服務已啟用 • 已隔離 • Sentry 已封鎖 • Access 已封鎖 • 合規性動作已封鎖 • 支援 APNS

區段名稱	描述

	• 受監管模式 (iOS 和 macOS 裝置) - 識別受監管的裝置。 裝置會持續由 IT 團隊直接控管。 受監管模式也會啟用其他的裝置功能 (例如：適用於現場服務部署、零售端點銷售裝置)、飯店服務業的借用裝置以及教室實驗室中供學生共用的裝置。
	• 清除 PIN 碼 - 按一下**檢視**以顯示 PIN 碼。
	• 受管理的 macOS 管理使用者 (macOS 裝置)
	• 本機 macOS 管理員密碼 (macOS 裝置) - 選取**檢視**，查看使用自動裝置註冊的註冊和受管理裝置的**管理員密碼**、**上次輪換密碼**、**下次輪換密碼**和**原因**資訊。
	管理員檢視密碼後，密碼可能需要再花一個小時 (下一次登記) 才能從顯示的**下次輪換**時間開始輪換。
	• 裝置加密狀態 (macOS 裝置)
	  ◦ FileVault 加密啟用
	  ◦ 使用個人復原金鑰
	  ◦ 使用機構復原金鑰
	• 可用的啟動程序權杖
	• 已啟用「系統完整性保護」
	• 韌體密碼
	  ◦ 密碼
	  ◦ 變更擱置中
	  ◦ 命令狀態
	  ◦ 允許選用 ROM
	• 復原鎖定
	  ◦ 密碼
	  ◦ 已啟用復原鎖定
	• 適用於 macOS 的採用 Mobile@Work 的指令碼
	• 防火牆設定 (macOS 裝置)
	  ◦ 已啟用防火牆
	  ◦ 封鎖所有連入連線
	  ◦ 隱形模式
	• 應用程式防火牆狀態 (macOS 裝置)
	• 防火牆狀態 (Windows 裝置)
	• 上一次備份至 iCloud 的日期 (iOS 裝置)
	• 密碼鎖定寬限期 (iOS 裝置)
	• Android ID
	• Android 安全性修補程式層級 (Android 裝置)
	• 單一應用模式 (Android 裝置)
	• Android SafetyNet Attestation 類型 (Android 裝置)
	• 可支援 Android 企業 (Android 裝置)

區段名稱	描述
	• 已啟用 Android Work (Android 裝置) • 可支援 Samsung SAFE (Android 裝置) • 已啟用 Android 受工作管理的裝置 (裝置擁有者) • 公司擁有的裝置上的 Android 工作描述檔已啟用 • 防網路釣魚原生狀態 • 防網路釣魚狀態 • 防網路釣魚 VPN 狀態 • 搭配工作描述檔的 Android 受管理裝置 • 公司擁有的裝置上的 Android 工作描述檔鎖定已啟用 • 可使用 Help@Work • 支援 Zebra • 安全 App 狀態 • 安全 App 加密狀態 • 安全的應用程式加密模式 • 已啟用 FCM • MTD 啟用狀態
Windows 資訊保護 (Windows 裝置)	• WIP • App Locker 已設定 • EDP 強制設定
電話	**裝置服務訂閱** • 電話號碼 • 行動電話技術 • IMSI • ICCID • IMEI • IMEI 2 - (僅在配備雙重 SIM 連接埠的 Android 裝置上。 適用於 Android 8.0 或更高版本) • MEID • 裝置位置 • 電信業者 • 歸屬 MCC • 歸屬 MNC • 目前的國家/地區名稱 • 主要國家/地區名稱 • 行動電話技術 • 漫遊

區段名稱	描述
	• 目前的電話公司 • 目前的 MCC • 目前的 MNC • 數據漫遊 • 語音漫遊 • EID - (適用於支援的 Android 裝置) **SIM 服務訂閱** - (適用於支援的 iOS 裝置) 對於支援的 iOS 裝置，系統會顯示多個 eSIM 作用中服務訂閱的這些屬性。 • 電信業者設定版本 • 電信業者設定網路 • 目前 MCC • 目前的 MNC • EID • ICCID • IMEI • 慣用資料 • 慣用語音 • 標籤 • 標籤 ID • 電話號碼 • SIM 卡插槽 • 正在漫遊 • 訂閱者電信業者網路 **SIM 服務訂閱** - (適用於支援的 Android 裝置) 對於支援的 Android 裝置，系統會顯示多個作用中服務訂閱的這些屬性。 • 電信業者設定版本 • 目前的 MCC • 目前的 MNC • ICCID • 慣用資料 • 慣用語音 • 訂閱ID • 電話號碼 • SIM 卡插槽 • 嵌入式 • 是受管理的

區段名稱	描述
Azure 裝置合規性	• Azure 裝置識別碼 • Azure 裝置合規性狀態 • Azure 用戶端狀態代碼 • Azure 裝置相符性報告時間 • Azure Intune 裝置使用者 UPN
Google BeyondCorp 裝置合規性	• 裝置識別碼 • 合規性狀態 • 合規性報告時間 • 使用者
電池資訊	• 電池電力 - 顯示 Android 作業系統報告的目前電池電力 • 電池健全狀況狀態 - 由 Android、Mac、iOS、iPad 裝置報告。 • 電池充電狀態 - Android 作業系統報告的狀態 • 電池健全狀況百分比 (OEM 特定) - 支援之裝置製造商裝置 (例如 Zebra 裝置) 的電池健全狀況百分比 • 電池生產日期 (OEM 特定) - 支援之裝置製造商裝置 (例如 Zebra 裝置) 的電池生產日期 • 電池充電週期 (OEM 特定) - 支援之裝置製造商裝置 (例如 Zebra 裝置) 完成的週期總數
裝置組件健康狀況 (適用於 iOS 27.0+ 和 macOS 27.0+ 受監管裝置)	• **基帶**: 指示裝置的基帶健康狀態。 • **相機**: 指示裝置的相機健康狀態。 • **顯示**: 指示裝置顯示健康狀態。 • **Face ID**: 指示裝置 Face ID 健康狀態。 • **近場**: 指示裝置近場通訊 (NFC) 狀態健康狀態。 • **Touch ID**: 指示裝置 Touch ID 健康狀態。 • **超寬帶**: 指示裝置的超寬頻健康狀態。

- **已安裝的應用程式** - 顯示已安裝在裝置上的應用程式的詳細資訊。 已安裝的應用程式的目前版本安裝日期顯示在**應用程式報告日期**欄下。 搜尋裝置的已安裝應用程式，如下所示:
- App 名稱
- 套組或套件 ID

從隔離區出來的裝置，其 app 安裝日期便是裝置離開隔離區當天的日期。

若是 Android Enterprise 裝置，還可以依日、週、月或年排序方式檢視已安裝的應用程式使用量詳細資料。 若要檢視這些詳細資料，必須已選取**組態設定**區段中的**啟用應用程式使用量資料收集**選項，然後才能選取**應用程式使用量 - 日**、**應用程式使用量 - 週**、**應用程式使用量 - 月**、**應用程式使用量 - 年**選項，以檢視應用程式使用量詳細資料。

- **可用的應用程式** - 顯示裝置可以使用的應用程式的詳細資訊。 搜尋裝置的可用應用程式，如下所示:
- App 名稱

- 套組或套件 ID

在**應用程式組態**欄中，選取**組態名稱**後，系統將導向至應用程式目錄的**應用程式組態**索引標籤，以便檢視應用程式組態選項。 如果需要，可以在**應用程式組態摘要**頁面上修改裝置的應用程式組態。 如需有關設定應用程式的詳細資訊，請參閱**App 配置**。

在**應用程式組態**欄中，當您選取**組態名稱**時，將被導向至應用程式目錄的**應用程式組態**索引標籤，以查看應用程式組態選項。 如果需要，可以在**應用程式組態摘要**頁面上修改裝置的應用程式組態。 如需有關設定應用程式的詳細資訊，請參閱**App 配置**。

> 請務必記住已指派裝置的特定應用程式組態的名稱和類型，這些資訊可以在**應用程式組態**頁面上找到。

> **狀態**欄指示裝置上的應用程式安裝狀態。 只擷取受控應用程式的應用程式安裝狀態。 非受控應用程式的應用程式安裝狀態顯示為「未安裝」。 必須將應用程式轉換成「受控」，才能檢視正確的安裝狀態。

- **AppConnect 應用程式** - 已安裝的 AppConnect 應用程式詳細資料。
- **原則** - 已套用{{原則}}的詳細資料。 針對受威脅的裝置，請在「違規」欄位中查看違規原因。 如果裝置已遭 Root 破解，系統會顯示**違規**欄位所示的原因：

優先順序 (1 = 最高)	違規
1	外掛程式遭破解
2	用戶端遭竄改
3	未知的裝置製造商：未知
4	偵測到可疑的資料夾：[路徑]
5	找到可疑的二進位檔：[路徑]
6	/data 資料夾可供瀏覽，或者，/data/data 資料夾可供瀏覽
7	找到 /system/app/Superuser.apk
8	套件管理員遭破解
9	找到可疑的 app：[套件]

- **憑證** - 已安裝憑證的詳細資訊。
  對於認證使用，請查看「使用類型」欄位。 如果認證為裝置專用，其使用類型將顯示為「裝置」。 如果認證為使用者專用，其使用類型將顯示為「使用者」。
- **Sentry** - Sentry 資訊 (ActiveSync 關聯)
- **屬性** - 自訂屬性與裝置屬性
- **使用者** - 顯示受監管 macOS 裝置的作用中使用者清單。

> **使用者**索引標籤已增強並將受管理的 Apple ID 顯示為超連結，按一下此連結即可重新導向至共享 iPad 裝置中的使用者帳戶詳細資訊頁面。

- **記錄** - 檢視與自訂裝置篩選器。 可以從篩選器執行以下操作:
  - 選擇要根據應用程式操作篩選裝置的操作名稱。

- 選擇狀態。
- 指定開始日期與結束日期。

- **硬體** - 硬體清查詳細資料 (系統、主機板、BIOS、硬碟、CD ROM、處理器和實體記憶體)

針對裝置大量指派或變更使用者和自訂屬性

可以使用「透過上傳進行大量指派」圖示來上傳 CSV 檔案，以針對裝置大量指派或變更使用者和/或自訂屬性。

程序

1. 按一下「裝置」頁面中的**透過上傳進行大量指派**圖示 (在「動作」按鈕旁)。
2. (選擇性) 按**下載範本**，以儲存 CSV 範本檔並編輯與上傳。
3. 準備好 CSV 檔案之後，請按一下**選擇檔案**，以瀏覽至 CSV 檔案位置，或將 CSV 檔案拖曳至「檔案資料」區段。
4. 請選擇下列選項之一：
   - **即使有找到任何現有值，仍要強制指派 (覆寫) 所有屬性**
   - **僅當值為空白時才覆寫，並略過具備現有值的屬性**

按一下**上傳**。

將裝置匯出至 CSV 檔案

您可以使用**裝置**頁面中的**匯出至 CSV** 選項匯出特定裝置的裝置詳細資料。

程序

1. 前往**裝置**。
2. 請選擇所有或多個空間，以檢視特定空間的相關資訊。
3. 按一下裝置計數連結。 隨即顯示與所選空間相關的裝置清單頁面。
4. 按一下**匯出至 CSV** 選項，將裝置清單及相關詳細資料匯出至 CSV 檔案。 隨即顯示快顯訊息，告知報告的匯出需要一些處理時間。 請先等候要求完成，然後再提交另一項要求。 報告就緒後，系統會以訊息提示您下載或刪除報告。
5. 按一下**下載**。 您也會收到一封包含報告下載連結的電子郵件。
6. (選用) 按一下**刪除**以刪除報告。

搜尋裝置日誌

程序

1. 前往**裝置** > **裝置**，按一下項目的**名稱**欄連結。
2. 按一下**日誌**索引標籤。
3. 使用「操作」、「狀態」、「開始日期」和「結束日期」篩選器可縮小顯示的裝置範圍。 可以從篩選器執行以下操作:
   1. 選擇要根據應用程式操作篩選裝置的操作名稱。
   2. 選擇狀態。
   3. 指定開始日期與結束日期。
4. 「裝置詳細資訊」欄會顯示應用程式的狀態，如下所示:
   對於所有裝置，狀態顯示以下詳細資訊:
   - 應用程式名稱、應用程式版本、套組或套件 ID

- 安裝狀態
- 任何錯誤和錯誤原因
  例如 - appOrConfigName=Name:<app name>;Identifier=<bundleid>;iTunesStoreId:<itunesid>;Status:<status or error reason from Apple>version: <app version>

對於 Windows 裝置，狀態顯示以下詳細資訊:

- 包括套組 ID 或套件 ID、狀態和錯誤
  例如 -
- 對於類型 - 應用程式清單和狀態 - 確認 - 顯示 - appType
- 對於類型 - 應用程式清單和狀態 - 傳送中 - 不顯示任何內容
- 對於類型 - 安裝/解除安裝和狀態 - 成功/失敗/傳送中 - 顯示包括套組 ID 或套件 ID、狀態、名稱、版本和錯誤

如果您無法看到**裝置**頁面，可能是您沒有所需的權限。 您需具備下列其中一個角色：

- 裝置管理
- 裝置唯讀

7.2. 裝置群組

本節包含以下各主題：

- 新增裝置群組
- 移除裝置群組
- 將裝置匯出至 CSV 檔案
- 將自訂屬性指派給裝置群組

在**裝置群組**頁面中，您可以建立要以相同方式處理的裝置清單。 您可以定義原則和組態，並將其指派給裝置群組。 下列為 Ivanti Neurons for MDM 所建立的預設裝置群組:

- 所有裝置
- Android 裝置
- Android Enterprise 裝置
- iOS 裝置
- 裝置類型 (Apple)
- tvOS 裝置
- macOS 裝置
- visionOS 裝置
- watchOS 裝置
- Windows 裝置

指派至特定裝置群組的 app 詳細資訊會顯示在該特定裝置群組的 **App** 標籤之下。

新增裝置群組

> 新增不適用於動態使用者群組的裝置群組。

視您所擁有的授權類型而定，您可以根據規則新增裝置群組，以識別符合特定準則的裝置。 符合規則的裝置會顯示在規則建立器區段下方。 這些規則可以用「任何 (或)」或「所有 (及)」選項來建立巢狀結構。 您可以使用以下運算子來建構規則:

- 開頭為
- 結尾是
- 包含
- 不包含
- 開頭不是
- 結尾不是
- 小於
- 大於
- 在範圍內
- 等於
- 不等於

- 不為空
- 為空

在規則建立器中選取「使用者群組名稱」屬性後，Ivanti Neurons for MDM 管理入口網站會顯示重複的使用者群組數量及對應的 GUID 數量，以識別重複的群組。 此外，此規則之下的表格會顯示重複使用者群組的清單以及其詳細資訊，例如使用者群組名稱、GUID、來源和可分辨的名稱 (DN)。

Bronze 授權：

規則可根據下列準則識別裝置

- 裝置類型
- 作業系統 - 作業系統 (預先填入)
- 作業系統版本
- 作業系統及版本
- 使用者群組

Silver 授權：

規則可根據下列準則識別裝置

- 已註冊 Entra ID
- 替代序號 (僅限 Android - 適用於處於「裝置管理」或「裝置擁有者」模式的 Samsung 裝置)
- Android 專用裝置
- 支援 Android Enterprise
- 搭配工作描述檔的 Android 受管理裝置
- Android SafetyNet Attestation 類型
- Android Work 啟用
- Android 安全性修補程式層級 (Android 裝置)
- 已啟用 Android 受工作管理的裝置 (裝置擁有者)
- Android 工作設定檔已啟用
- 公司擁有的裝置上的 Android 工作設定檔已啟用
- 防網路釣魚原生狀態
- 防網路釣魚狀態
- 防網路釣魚 VPN 狀態
- 支援 APNS
- Apple 矽裝置
- 已啟用自動化 Device Enrollment
- 已註冊自動化 Device Enrollment
- Azure 裝置識別碼
- Azure 裝置合規性狀態
- Azure 用戶端狀態代碼
- Azure 裝置相符性報告時間

- 基頻健康狀態
- BitLocker 加密
- Sentry 已封鎖
- Access 已封鎖
- 可用的啟動程序權杖
- 大量佈建的類型 (Apple Configurator 或無)
- 電信業者
- 相機健康狀態
- 用戶端上一次登記
- 已註冊的用戶端
- 相符性
- 合規性動作已封鎖
- 目前的國家/地區名稱 (從下拉式清單中，選取目前的國家/地區名稱)
- 目前的 MCC
- 目前的 MNC
- 自訂裝置屬性
- 自訂 LDAP 屬性
- 自訂使用者屬性
- 數據漫遊
- 裝置名稱
- 裝置已註冊
- 裝置來源
- 裝置類型
- 顯示名稱
- 顯示健康狀態
- 加密已啟用
- Face ID 健康狀態
- 硬碟分割區
- 主要國家/地區名稱 (從下拉式清單中，選取主要國家/地區名稱)
- 歸屬 MCC
- 歸屬 MNC
- IMEI
- IMEI2 (僅適用於具有雙 SIM 卡插槽的 Android 裝置，並且裝置必須為 Android 8.0 或更高版本)
- 機構復原金鑰已啟用
- IP 位址
- 單一應用模式
- 上一次登入

- 僅限 MAM
- 製造商
- MDM 註冊類型
- MDM 返回服務 (iOS 27.0+ 和 visionOS 27.0+)
- 多使用者模式 (iOS 27.0+)
- MTD 啟用狀態
- NFC 健康狀態
- 作業系統
- 作業系統組建版本
- 作業系統版本
- 作業系統版本
- 作業系統及版本
- 擁有權
- 電話號碼
- 公用 IP 位址 (Android 或 ChromeOS 裝置)
- 個人復原金鑰已啟用
- 已隔離
- 已啟用復原鎖定
- 漫遊
- 安全 App 狀態
- 安全鎖定模式
- 序號
- 狀態
- 受監管
- 系統版本
- 裝置總容量
- 總記憶體 MB
- TPM 版本
- Touch ID 健康狀態
- 可用的解除鎖定權杖 (iOS)
- 使用者註冊已啟用
- 使用者群組
- 超寬帶無線電健康狀況
- 語音漫遊
- macOS 個人復原金鑰已委付
- macOS 復原金鑰類型

程序

1. 按一下**新增**。
2. 輸入群組名稱。
3. 為此群組輸入一個選填的描述。
4. 選擇您要建立的裝置群組類型：
   - **動態管理**：使用規則來定義群組中要包含哪些裝置。
     - **從進階搜尋載入**: 選取此選項可開啟已儲存搜尋的庫。 選擇查詢會根據選取的搜尋自動填入裝置群組的名稱和規則條件。

     > 您可以透過導覽至**裝置** > **裝置** > **進階搜尋**來建立和儲存這些查詢。 此處儲存的任何查詢將自動可供在此載入。

   手動管理：逐一輸入群組中要包含之裝置的使用者。
5. 若是動態管理的群組：
   1. 建立一個定義群組的規則。
   2. **例如**：OS is iOS
      按一下 **+** 以視需要建立其他規則。
   3. **例如**：Device is iPhone 5S
      如果裝置要符合至少一項規則，請按一下**任一**。
   4. 如果裝置必須符合所有規則，請按一下**全部**。
6. 若是手動管理的群組：
   1. 輸入您想新增之裝置的使用者名稱。
   2. 從顯示的清單中選擇裝置。
   3. 重複步驟 a 和 b，直到所有裝置都顯示在清單中為止。

按一下**儲存**。

移除裝置群組

程序

1. 前往**裝置** > **裝置群組**。
2. 按一下您要移除之裝置群組的勾選方塊。
3. 按一下**刪除裝置群組**。

將裝置匯出至 CSV 檔案

您可以使用**裝置群組**頁面中的**匯出至 CSV** 選項匯出特定裝置群組的裝置詳細資料。

程序

1. 前往**裝置** > **裝置群組**。
2. 請選擇所有或多個空間，以檢視特定空間的相關資訊。
3. 按一下裝置群組計數連結。 隨即顯示與所選空間相關的裝置清單頁面。
4. 按一下**匯出至 CSV** 選項，將裝置清單及相關詳細資料匯出至 CSV 檔案。 隨即顯示快顯訊息，告知報告的匯出需要一些處理時間。 請先等候要求完成，然後再提交另一項要求。
5. 按一下**下載**。 您將會收到一封包含報告下載連結的電子郵件。

6. (選用) 按一下**刪除**以刪除報告。

如果您無法看到**裝置群組**頁面，可能是您沒有所需的權限。 您需具備下列其中一個**角色**：

- 裝置管理
- 裝置唯讀

將自訂屬性指派給裝置群組

管理員現在可以將自訂屬性直接指派給裝置群組。 成為裝置群組成員的任何裝置會自動繼承設定的自訂屬性值，無需在註冊後手動將屬性指派給個別裝置。 使用裝置群組將自訂屬性值自動指派給成為群組成員的裝置。

程序

1. 前往**裝置** > **裝置群組**。
2. 選取現有群組或建立群組。
3. 在裝置群組詳細資料頁面中，按一下**屬性**。
4. 按一下**新增**。
5. 選擇自訂屬性並指定所需的值。

7.3. 未受管理的裝置

本節包含以下各主題：

- 封鎖裝置
- 取消封鎖裝置
- 從裝置清單清除裝置

授權： Silver

如果您已設定 Sentry 電子郵件存取控制，任何存取您的電子郵件系統但未註冊的裝置就稱為未受管理的裝置。 當您設定 Sentry 時，即可定義是否預設讓未受管理的裝置存取電子郵件。 之後您即可允許或封鎖這些裝置的電子郵件存取權。

> 「未受管理的裝置」頁面每 5 分鐘會更新一次。 因此，管理方面的變更不會立即生效。

封鎖裝置

程序

1. 選擇裝置。
2. 選擇**動作 > 封鎖**。

除非選擇**動作 > 允許**或**動作 > 刪除**，否則裝置會一直處於封鎖狀態。

取消封鎖裝置

程序

1. 選擇裝置。
2. 選擇**動作 > 允許**。

除非選擇**動作 > 封鎖**或**動作 > 刪除**，否則裝置會持續存取電子郵件。

從裝置清單清除裝置

程序

1. 選擇裝置。
2. 選擇**動作 > 刪除**。

裝置下次嘗試存取電子郵件系統時，仍會重新顯示在這份清單中，您必須重複進行之前套用至裝置的所有「封鎖」或「允許」動作。

7.4. App 庫存

本節包含以下各主題：

- 篩選 app 的顯示畫面
- 顯示已安裝某 app 的裝置
- 顯示 app 清單
- 顯示裝置上已安裝的 Win32 或 Win32 市集應用程式
- 建立自訂檢視權限
- 匯出應用程式詳細目錄

應用程式詳細目錄是在已註冊裝置上所偵測到的應用程式清單。 作為管理員，您可使用此頁面取得已註冊裝置上使用的應用程式相關資訊。 您可以掌握下列問題的答案：

- 哪些 app 最受歡迎？
- iOS 裝置的 app 是否都直接來自 App Store？
- 有多少 Android 使用者下載了選擇性的{{內部應用程式}}？
- 有多少裝置使用過時的 app 版本？

篩選 app 的顯示畫面

顯示**裝置 > App 庫存**頁面時，其中會列出所有 app。 若要將此清單縮減為特定 app，請使用篩選 (左窗格)。 例如，若要限縮清單僅顯示來自 Google Play 的私人 app，請選擇**來源**區段中之下的**私人**。

您可從下拉式清單中選擇多個空間，以檢視所有或多個空間裝置上的 app 庫存。 當您將游標移至顯示的 app 上時，會顯示裝置計數。 您可按一下 app 的計數，以顯示包含該 app 的所有裝置。 每個 app 庫存記錄將會依空間分組。

您可以使用應用程式名稱或套組/套件 ID 來搜尋。

若已選取多個空間，則將滑鼠懸停在**已安裝數量**欄中的**總計**值，將顯示每個裝置空間的安裝數。

顯示已安裝某 app 的裝置

按一下**受管理**、**未受管理**或在**已安裝的數量**欄中列出的**總計**數字。

顯示 app 清單

按一下 app 庫存中 app 的**已要求數量**來檢視已要求 app 的裝置。 此動作僅適用於「僅限 MAM」裝置。

顯示裝置上已安裝的 Win32 或 Win32 市集應用程式

若裝置的隱私權組態允許收集該裝置上所有應用程式的資訊，則應用程式詳細目錄便會顯示裝置上的 Win32 或 Win32 市集應用程式。 您可以設定裝置的隱私權政策。

程序

1. 遵循裝置中的指示，判斷所需裝置適用哪類隱私權配置。
2. 前往**配置**。
3. 如需您在步驟 1 中看到的隱私權配置

1. 選擇配置。
2. 按一下「編輯」。
3. 在**收集 App 庫存**下方，選擇**裝置上的所有 App**。
4. 按一下**完成**。

> 在裝置上執行詳細目錄掃描後，Win32AppInventory CSP 會每 24 小時傳回一次裝置上安裝的所有 Win32 與 Win32 市集應用程式的清單。

建立自訂檢視權限

您可針對使用者指定自訂檢視權限。

程序

1. 前往**管理**。
2. 前往**角色管理**。
3. 按一下**新增自訂角色**。
4. 選擇**空間專用角色**選項。
5. 在**名稱**欄位中，輸入使用者名稱。
6. 從**裝置**功能表，按一下 **App 庫存**。
7. 選取**檢視**勾選框。
8. 從**裝置**功能表，按一下**裝置動作**。
9. 按一下**儲存**。
10. 前往主功能表中的**使用者**。
11. 按一下您建立的新使用者。
12. 按一下**指派角色**。
13. 選擇 **app | 空間專用**勾選框，按一下**下一步**。
14. **摘要**頁面顯示指派給您建立的角色的權限。
15. 按一下**完成**。
16. 登入為新使用者。
17. 從主功能表，按一下**裝置**。
18. 按一下 **App 庫存**。
19. **App 庫存**頁面現在僅顯示允許該使用者存取的應用程式。

匯出應用程式詳細目錄

作為管理員，您可使用**匯出至 CSV** 選項要求取得應用程式詳細目錄報告。

程序

1. 前往**裝置 > 應用程式詳細目錄**。
2. 從清單選取詳細目錄。
3. 按一下**匯出至 CSV**。

4. 請選擇下列選項之一：

- **將應用程式匯出為 CSV** 可匯出「應用程式詳細目錄」中的所有應用程式。
- **將裝置匯出為 CSV** 可根據下表匯出特定應用程式:

選項	描述
套組 ID	輸入應用程式的套組/套件 ID。
您是否要匯出	請選擇下列選項之一： • 安裝總計 • 受管理 • 未受管理 • 已要求 (對於僅限 MAM 的裝置)

5. 按一下**匯出**。

系統會以彈出訊息提示管理員，告知報告的匯出需要一些處理時間。 提交要求後，管理員必須等候完成要求，再提交另一項要求。 報告就緒後，系統會以訊息提示管理員下載或刪除產生的報告。 管理員也會收到一封包含報告下載連結的電子郵件。

如果您無法看到 **App 庫存**頁面，可能是您沒有所需的權限。 您需具備下列其中一個**角色**：

- 裝置管理
- 裝置唯讀

7.5. 管理裝置

本節包含以下各主題：

- 部署 Windows 裝置
- 在 macOS 裝置上設定 Apple 遠端桌面
- 裝置註冊 (iOS、macOS 及 Android)
- 裝置註冊（Windows 10+ PC 和 Microsoft HoloLens 2）
- 佈建使用 PIN 碼註冊套件
- 使用 Windows 裝置大量註冊
- 變更密碼設定
- 變更裝置名稱
- 搜尋與篩選裝置
- 使用裝置擁有者
- 搭配工作描述檔的受管理裝置
- 使用 Android 大量註冊
- 使用 CSV 檔案上傳進行大量註冊
- 使用 Samsung Knox Mobile Enrollment
- 註冊 Oculus 裝置
- 在裝置上啟用 Bluetooth
- 排程 iOS 更新
- 重新安裝 iOS 系統 App
- 指派裝置給新使用者
- 重新指派 Android 裝置
- 強制裝置登記
- 定位裝置
- 鎖定裝置
- 管理遺失模式下的 Apple 裝置
- 要求偵錯日誌
- 淘汰裝置
- 放棄裝置擁有權
- 清除裝置
- 刪除裝置
- 解除鎖定裝置
- 重新啟動或關閉裝置
- 清除限制密碼 (僅限 iOS)
- 刪除裝置的 Sentry 關聯
- 指派自訂屬性給裝置

- 移除裝置的自訂屬性
- 同步並擷取 App 回饋
- 設定韌體密碼
- 重新發行新的個人復原金鑰
- 設定或者變更復原鎖定
- Apple 存取權限管理
- 群組原則註冊

7.5.1. 部署 Apple 裝置

Ivanti Neurons for MDM 支援所有 Apple 裝置的管理。 它是一個全面的解決方案，用於佈建、管理、更新和保護您的機群，為一般使用者提供最佳的使用者體驗。

本節包含以下各主題：

- 安裝您的 Apple MDM 憑證
- 註冊 Apple 裝置
- Ivanti Go for iOS 用戶端
- 管理 Apple 裝置的應用程式
- 管理配置
- 管理軟體更新
- 設定 iOS/iPadOS 裝置
- 設定 watchOS 裝置
- watchOS 裝置支援的裝置動作
- 設定 visionOS 裝置
- visionOS 裝置支援的裝置動作
- 設定 macOS 裝置
- 設定 TvOS 裝置
- 支援宣告性裝置管理 (DDM)

安裝您的 Apple MDM 憑證

若要管理 Apple 裝置，首先要申請並安裝 Apple MDM 憑證以管理 iOS 裝置。 每年更新一次 Apple MDM 憑證。 (接近到期日時，用於建立憑證的 Apple 帳戶會收到 Apple 網站發出的通知。) 使用「 MDM 憑證」頁面新增或續訂此憑證。

依照安裝 MDM 憑證中所述的步驟進行操作

註冊 Apple 裝置

您可以選擇以下任何一種方法來註冊裝置:

- 自動化裝置註冊
- Apple School Manager
- Apple Configurator

Ivanti Go for iOS 用戶端

下一步是選取您的公司針對該裝置允許的註冊類型。 Ivanti Neuros for MDM 目前支援:

- 裝置註冊 (iOS、macOS 及 Android)
- 透過 Apple 商務管理進行使用者註冊
- 帳戶導向使用者註冊
- 設定 (Apple)

管理 Apple 裝置的應用程式

Ivanti Neurons for MDM 中的「應用程式目錄」頁面可作為一種介面，以供管理員更有效率地管理其應用程式目錄。 此功能包含一般使用者可用的行動應用程式協調，涵蓋公用應用程式商店和指定為透過 Ivanti Neurons for MDM 發佈的應用程式商店。

支援的應用程式:

「應用程式目錄」頁面彙整了各種類型的應用程式，包括公用 AppStore 應用程式、自訂應用程式、內部開發的應用程式、支援 AppConnect 的應用程式、GoClient for iOS 和 M@W for macOS，簡化了後續組態和發佈的匯入程序。

在僅限行動應用程式管理 (MAM) 組態下執行的裝置上，系統會提示 iOS 使用者在存取應用程式目錄時選取驗證憑證。 若要對於列出的應用程式進行存取保護，同時符合強大的安全做法，則此驗證步驟將至關重要。

> Apple 的 M1 晶片組 MacBook 可針對 [您的軟體產品] 中的 iPhone 和 iPad VPP 應用程式提供專業化支援。 值得注意的是，只有管理員有權推送支援的 iPhone 和 iPad VPP 應用程式，並限制使用者直接從應用程式安裝它們。

如需詳細的實作指示和組態選項，請參閱管理指南中提供的綜合性文件和以下資源:

- 管理應用程式
- 應用程式目錄設定
- 設定 Apple Apps and Books
- Apps@Work 企業應用程式商店
- MacOS AppStore 限制

管理配置

組態是指身為管理員的您傳送給裝置的設定集合。 例如，您可以使用會自動設好裝置 VPN 設定和密碼需求的配置。 您系統的現有組態於「組態」頁列出。 您可從「組態」頁選取多個組態，並一次推送至多部裝置。 這些組態可推送至空間專屬裝置，以及其他仍未受影響空間中的裝置。 組態可以推送至單一空間，或一次推送至多個空間或全部空間。

Ivanti Neurons for MDM 中的大多數組態對於所有平台都是通用的。 有關如何使用組態的詳細資訊，請參閱「使用組態」。

某些組態僅由特定平台支援。 您可以按「組態類型」支援的平台檢閱清單

管理軟體更新

您可以先為 iOS 和 macOS 裝置設定「軟體更新」組態以開始執行。

> 設定軟體更新的排程時段時，作業系統更新命令會每小時推送到裝置一次，以確保更新不會錯過該時段。 根據 Apple 的行為，每次裝置收到作業系統更新命令時，都會顯示快顯視窗以通知使用者進行升級。 使用者最多可以推遲三次。 根據 Apple 的行為，第三次裝置將強制升級。

MacOS 裝置還有一些可套用的特定規則。 查看 macOS 軟體更新規則組態

iOS 的作業系統更新命令

您也可以傳送一次性命令以更新「裝置清單」或「裝置頁面」中的一個或多個裝置。 請參閱排程作業系統更新命令。

設定 iOS/iPadOS 裝置

您的 iOS/iPadOS 支援下列組態:

- iOS/iPadOS 限制
- eSIM 組態
  - 保留數據方案
- 行動網路組態
- 啟用遺失模式
- 設定 iOS MDM 描述檔
- 單一 App 模式
  - 自發的單一應用程式模式
- 共享商務版 iPad
- 教育組態
- iOS 自訂配置
- 鎖定畫面訊息

設定 watchOS 裝置

現在與 iOS 裝置配對時，您可以在 Ivanti N-MDM 中註冊 Apple watchOS 裝置。

此功能目前支援: watchOS 10+。

Procedure程序

1. 您必須註冊 iOS 17+ 受監管裝置。
2. 將 Apple Watch 註冊組態指派給 iOS 裝置。
3. 您現在可以將 Apple Watch 與 iPhone 配對。

> 將 Watch 組態推送到 iPhone 後即可與 Apple Watch 配對。 如果 Apple Watch 與 iPhone 配對後將 Watch 設定推送到 iPhone，則無法為 Apple Watch 啟用遠端管理。

您的 watchOS 裝置支援下列組態:

- Cellular_Configuration
- 憑證配置
- 憑證透明度
- Identity_Certificate_Configuration
- iOS 限制
- Passcode_Settings
- Per-App_VPN_Configuration
- Wi-Fi_Configuration

watchOS 裝置支援的裝置動作

您的 watchOS 裝置支援以下裝置動作:

- 清除密碼
- 鎖定 Apple watch
- 抹除 Apple watch
- 從 Ivanti Neurons for MDM 取消註冊 Apple Watch

> 取消註冊配對的 iOS 裝置將重設手錶並取消與 iOS 裝置的配對。

設定 macOS 裝置

您的 macOS 支援下列組態:

- macOS 限制
- 設定 macOS 裝置
- 使用指令碼和 Mobile@Work 用戶端
- 設定 macOS MDM 設定檔
- 設定韌體密碼
- 啟用 FileVault
  - FileVault 復原金鑰
  - FileVault 選項配置
- 平台和可延伸 SSO
- Active Directory macOS
- 防火牆
- 乙太網路
- Office 365 帳戶建立
- macOS 系統延伸模組
- 媒體磁碟燒錄限制
- 隱私權設定

設定 TvOS 裝置

您的 tvOS 支援下列組態:

- Apple TV 配置
- Apple TV 限制
- 會議室顯示器
- AirPlay 鏡像

設定 visionOS 裝置

現在您可以在 Ivanti Neurons for MDM 中註冊 Apple visionOS 裝置。

此功能目前支援: visionOS 1.1+

您可以使用下列其中一種方法，註冊 visionOS 裝置:

- 帳戶導向裝置註冊
- 帳戶導向使用者註冊
- 裝置註冊

您的 visionOS 裝置支援下列組態:

- CalDAV 配置
- CardDAV 配置
- 憑證配置
- 憑證撤銷檢查配置
- 憑證透明度
- 建立 DNS Proxy 組態
- 加密 DNS
- 電子郵件配置
- Exchange 組態
- Google 配置
- 身份憑證
- iOS 限制
- LDAP 配置
- 受管理的網域
- 網路轉送組態
- 個別 App VPN 組態
- 單一登入配置
- 訂閱的行事曆配置
- VPN 組態
- Web 內容篩選
- Wi-Fi 組態

visionOS 裝置支援的裝置動作

您的 visionOS 裝置支援以下裝置動作:

- 抹除 Apple Vision Pro
- 淘汰 Apple Vision Pro
- 解鎖 Apple Vision Pro

支援宣告性裝置管理 (DDM)

Apple 的宣告性裝置管理是一種現代管理協定，允許受控裝置主動、自主地套用自己的管理設定，減少通訊往返。 在註冊期間或簽入已註冊裝置期間，宣告式裝置管理已在新註冊的裝置上啟用。

宣告式裝置管理會在符合以下條件的裝置上自動啟用:

- 安裝 macOS 13 或更新版本的電腦

- 具有 iOS 16 或 iPadOS 16 或更高版本的裝置
- 透過使用者註冊而註冊的裝置在 iOS 或 iPadOS 15 或更高版本上支援聲明式裝置管理。
- 安裝 tvOS 16 或更新版本的 Apple TV 裝置
- 搭載 watchOS 10 或更新版本的 Apple Watch 裝置
- 搭載 visionOS 1.1 或更新版本的 Apple Vision Pro 裝置

目前支援的宣告式管理功能:

- **狀態通道**:
  - 作業系統版本的變更
  - 密碼合規性
  - 當前的密碼
- **組態**:
  - 宣告式管理組態

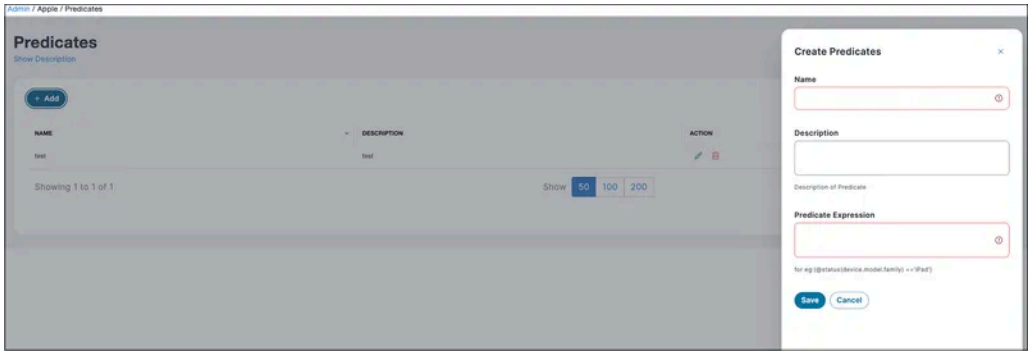
DDM 組態中的述詞

述詞是採用 Cocoa 語言的表達式，可以為裝置組態的啟用提供靈活度和細微性。 表達式位於裝置上，會在滿足此述詞的條件時套用。 我們新增了一項新功能，可讓您建立、儲存述詞，以及對任何 DDM 組態套用述詞。

DDM 組態的「發佈」頁面中會顯示一個用來套用述詞的新選項。 您可在此區段的下拉式清單中找到已建立的述詞。

建立述詞

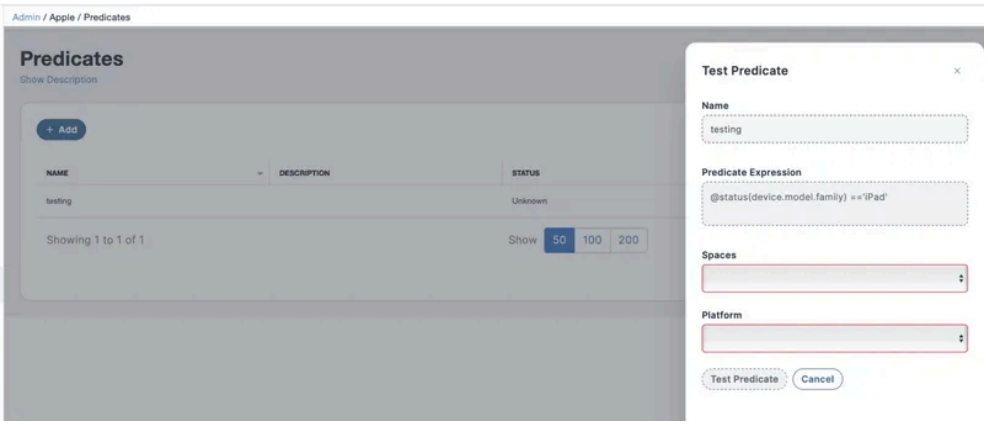
1. 前往**管理員** > **Apple** > **述詞**。
2. 按一下**新增**。 畫面上會顯示**建立述詞**視窗。
3. 輸入下列資訊：
   - **名稱** – 述詞的名稱
   - **說明** – 新增一些相關說明
   - **述詞運算式** – 述詞運算式。 例如 @status(device.model.family) =='iPad'



4. 按一下**儲存**。 畫面上會出現一個對話方塊，確認建立述詞。
5. 透過重新整理頁面並觀察狀態欄位中的值 (值為: **未知**、**進行中**、**有效**、**無效**) 來檢查述詞語法的有效性。
   1. 按一下**測試**。 畫面上會顯示**測試述詞**視窗。
   2. 輸入下列資訊：
      - **名稱** - 預設

- **述詞表達式** – 預設
- **空間** – 預設空間
- **平台** – iOS/macOS
- **裝置名稱** – 與述詞表達式相關。

> 只有從下拉式功能表中選取了**空間**和**平台**欄位詳細資訊後，**裝置名稱**欄位才會出現在**平台**欄位下方。



3. 按一下**測試述詞**。
4. 畫面上會出現一個對話方塊，確認測試述詞發起。
5. 重新整理頁面以尋找述詞語法的狀態。
   - 對於正確的述詞表達式，狀態將依據**未知**> **進行中** > **有效**進行更改。
   - 對於不正確的述詞表達式，狀態將依據**未知** > **進行中** > **無效**進行更改。
6. 如果您想要使用不同的述詞表達式建立多個述詞，請重複此程序。

為 DDM 組態發佈述詞

1. 建立 DDM 支援的組態。
2. 將切換開關「使用述詞啟用」設定為「開」，並使用 + 按鈕以包含述詞 (根據需要)。



若要編輯或刪除述詞，請前往**管理員** > **Apple** > **述詞**。 您可以在此頁面中找到可用述詞的清單。 按一下**編輯**，即可對現有述詞進行任何變更並儲存。 同樣，若要刪除現有述詞，請選取該述詞並按一下**刪除**。

> 如果述詞與任何組態相關聯，則無法將它刪除。

DDM 組態的管理屬性

管理員可以使用以下方式來建立述詞:

- 使用者和裝置變數
- 使用者屬性
- 裝置屬性

在述詞中使用管理屬性的範例 (自訂屬性):

用來檢查使用者的名字是否為 'test' 的述詞: @property(userFirstName)=='test'

更多範例

- 裝置的硬體系列: (Mac、iPhone、iPad 等)
  @status(device.model.family) =='iPad'
  若為 true，則表示裝置上存在密碼。 若為 false，則表示裝置上沒有密碼。
  @status(passcode.is-present)==true
- 在裝置上使用的作業系統系列，例如 macOS 或 iOS。
  @status(device.operating-system.family)=='iPadOS'
- 在裝置上使用的作業系統版本，例如 15.0
  @status(device.operating-system.version)=='18.2'
  @status(device.operating-system.version)<'18.3'
  @status(device.operating-system.version)>='18.2'
- 在裝置上指定 FileVault 已啟用狀態的布林值
  @status(diskmanagement.filevault.enabled)==true
- 管理屬性 (自訂屬性) 的範例:
  檢查使用者的名字是否為 'test' 的述詞
  @property(userFirstName)=='test'

7.5.2. 部署 Windows 裝置

本節包含以下各主題：

- 概覽
- 裝置管理
- Windows 裝置註冊與登錄
- Windows Update 管理
- 應用程式管理與發佈
- 應用程式控制
- Windows 裝置管理組態
- Windows 裝置合規
- Windows 應用程式與硬體詳細目錄

概覽

Ivanti Neurons for MDM 可協助您管理所有 Windows 筆電與桌機，包括 HoloLens 2 端對端裝置生命週期管理：從組態、註冊、佈建、安全保護、應用程式、管理、監控、軟體及作業系統更新直至淘汰。

裝置管理

支援的 Windows 裝置:

- Windows PC 10+
- Microsoft HoleLens 2

如需「裝置管理」及報告功能的詳細資訊，請參閱裝置。

Windows 裝置註冊與登錄

Ivanti Neurons for MDM 支援 Windows 裝置適用的所有標準裝置註冊方法:

- 手動註冊
- 大量註冊
- 透過 SCCM 與 Ivanti EPM
- Windows Autopilot
- Entra ID 註冊

如需註冊方法的詳細資訊，請參閱使用 Microsoft Azure。

如需關於多使用者支援的資訊，請參閱 Windows 裝置的多使用者支援。

Windows Update 管理

- 設定及排定 Windows Update - 若要設定及排定 Windows Update，請使用「組態 - 軟體更新」建立組態。
- Windows 更新管理 - 您可以使用「Windows 更新管理」檢視及核准要更新的 Windows 裝置所回報的更新。 使用此功能可以避免非必要或尚未完成裝置安裝測試的更新。 如需詳細資訊，請參閱 Windows Update 管理。

應用程式管理與發佈

使用者可管理 Windows 應用程式完整的應用程式生命週期 (匯入、組態、排程、發佈、更新與移除)。

支援的應用程式類型:

- 內部
- MSB
- 公開商店

支援的應用程式副檔名:

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

如需管理 Windows應用程式的更多資訊，請參閱**App 配置**。 若要自動進行應用程式更新，請參閱 **Windows app 排程**及**使用配置**。

應用程式控制

App 控制配置可讓您在裝置層級將 app 分類為允許清單或封鎖清單。 已安裝的 app 將無法顯示，也無法啟動。 App 仍可在 App Store 中看到，但無法下載或啟動。 接收應用程式控制組態發佈的任何裝置，將會使用此組態並忽略任何已允許的應用程式原則設定。 應用程式控制組態的優先性，高於在目標裝置上指向相同應用程式的任何應用程式相關原則。

如需詳細資訊，請參閱**App 控制配置：控制每台裝置要安裝哪些 App**。

Windows 裝置管理組態

支援 Windows 10+ PC 及 Microsoft HoloLens 2 並包含下列功能:

- **裝置註冊（Windows 10+ PC 和 Microsoft HoloLens 2）**
- **密碼組態**
- **Exchange 組態**
- **組態**
- **裝置**
- **App**
- **Windows app 排程**
- **App 控制配置：控制每台裝置要安裝哪些 App**
- **Windows Update 管理**
- **從 Ivanti Neurons for MDM 到 Azure 的裝置狀態報告**
- **設定 Windows Autopilot 描述檔**
- **使用自訂組態將 SyncML 推送至裝置**
- **政策**
- Windows 限制

- 身分識別憑證
- Windows Hello for Business
- Wi-Fi 和 VPN 設定檔

> 組態發佈至不受此裝置類型支援的 HoloLens 裝置時，不會將其回報為發佈在「裝置詳細資訊」的「組態」索引標籤下的組態。

Windows 功能 (僅支援 Windows PC):

- **Ivanti Bridge**
- **Windows BIOS 配置**
- **Windows BitLocker**
- **Windows 單一應用配置**
- **Windows 授權配置**
- **EMA 伺服器整合配置**
- **列印設定**
- **移除膨脹配置**
- **ADMX (GPO) 瀏覽器**

Windows 裝置合規

可以透過 Microsoft Azure 來設定 Ivanti Neurons for MDM，以便使用者在執行 Windows 10+ 的 Windows 桌面電腦和平板電腦中進行無縫註冊。 若要設定 Azure 租戶整合，以落實 Windows 裝置合規，請參閱**使用 Microsoft Azure**。

Windows 應用程式與硬體詳細目錄

Windows 應用程式詳細目錄

應用程式詳細目錄是在已註冊裝置上所偵測到的應用程式清單。 您可使用此頁面取得已註冊裝置上使用的 app 相關資訊。 如需更多資訊，請參閱**App 庫存**。

> 若裝置的隱私權組態允許收集該裝置上所有應用程式的資訊，則應用程式詳細目錄便會顯示裝置上的 Win32 或 Win32 市集應用程式。

設定應用程式詳細目錄間隔

您可針對多種應用程式來源類型詳細目錄，設定 Windows 10 應用程式詳細目錄收集間隔。 「隱私組態」設定收集裝置的所有應用程式時，會使用此間隔。

如需更多資訊，請參閱**配置 app 庫存間隔**。

Windows 硬體詳細目錄

您可從 Windows 10+ 裝置啟用硬體資訊收集。 會使用 Bridge 擷取這些詳細資訊。 如需詳細資訊，請參閱**硬體庫存**。

7.5.3. 在 macOS 裝置上設定 Apple 遠端桌面

本節包含以下各主題：

- 在 macOS 裝置上啟用 Apple 遠端桌面
- 在 macOS 裝置上停用 Apple 遠端桌面

在 macOS 裝置上啟用 Apple 遠端桌面

Apple 遠端桌面可提供螢幕畫面分享功能並可讓您遠端管理裝置。 Apple 遠端桌面功能適用於受監管的 macOS 10.14.4+ 裝置。

程序

1. 前往**裝置**，選擇一或多個受監管的 macOS 裝置。
2. 對裝置按一下**動作** > **啟用遠端桌面**動作。
3. 按一下**啟用遠端桌面**以確認。

在 macOS 裝置上停用 Apple 遠端桌面

程序

1. 前往**裝置**，選擇一或多個受監管的 macOS 裝置。
2. 對裝置按一下**動作** > **停用遠端桌面**動作。 螢幕畫面分享功已停用，您無法遠端管理裝置。

7.5.4. 裝置註冊 (iOS、macOS 及 Android)

本節包含以下各主題：

- 手動安裝管理描述檔
- 傳送邀請 (iOS、macOS 及 Android)
- 指導一般使用者下載 app (iOS 和 Android)

大多數的使用者一開始都要先註冊裝置。 您可使用下列任何一種方法開始註冊程序：

- 傳送邀請給一或多位一般使用者 (iReg 註冊)
- 指導一般使用者下載 Go(app 內註冊)

> 如果 iOS 和 macOS 裝置 MDM 註冊失敗且出現 *設定檔安裝失敗，SCEP 伺服器傳回無效回應* 錯誤，裝置使用者必須從頭開始重新啟動裝置註冊程序。 這種情況主要發生在裝置使用者將設定檔下載到裝置以後，完成 iOS 和 macOS 裝置 MDM 註冊程序的時間比預期更久時。 請聯絡 Ivanti 支援團隊，進一步釐清此問題。

Ivanti Neurons for MDM 支援在 macOS 裝置上針對單一使用者 (本機使用者或 Active Directory (AD) 註冊使用者) 進行使用者層次管理。 管理員可以管理使用者的 裝置、套用裝置描述檔和使用者描述檔，並使用 App Store、app 發佈、配置及原則 (包括 Apps@Work、限制、安全)。

若要透過 AD 使用者管理 macOS 裝置，該 AD 使用者必須是註冊時的登入使用者。 任何其他的非註冊使用者無法檢視註冊使用者專屬的描述檔 (例如身份認證、VPN)。 不過，裝置層次配置可供檢視，而且可供任何登入使用者使用。

> 一般使用者必須在 Ivanti Neurons for MDM 中擁有帳戶，才能開始裝置註冊程序。 若是 LDAP 使用者，就必須先設定好 Connector 和 LDAP 伺服器，也必須將使用者從 LDAP 伺服器進行匯入。 若是本機使用者，就必須新增使用者。

> 舊版 Ivanti Neurons for MDM 所產生的裝置註冊 URL 將無法在目前版本中使用。 管理員必須重新產生裝置註冊 URL 才能進行裝置註冊。

手動安裝管理描述檔

適用於：

- iOS 12.2 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- macOS 11.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。

iOS 裝置註冊

在 iOS 裝置上進行 app 內註冊期間：

- 在使用 Go app 註冊裝置期間，會出現包含安裝設定檔說明的頁面。
- 按一下**安裝下載的設定檔**選項，然後再按一下**我了解**。
- 下載的描述檔的有效期僅數分鐘，之後就必須重新註冊。

macOS 裝置註冊

在自助式入口網站中註冊 macOS 裝置時，使用者必須執行下列步驟：

程序

1. 使用其認證登入。
2. 在安裝管理描述檔頁面中，會將描述檔下載至使用者的本機系統。
3. 連按兩下下載的描述檔，使它顯示在使用者的系統偏好設定中。

> 使用者必須在描述檔失效之前進行安裝。

4. 在系統偏好設定中開啟**描述檔**。 將描述檔下載至裝置後，使用者可檢視包含描述檔連結的網頁。 按一下**描述檔**以開啟設定 app。
5. 按一下**安裝**，安裝管理設定檔。
6. 繼續完成安裝程序。 在提示時輸入系統密碼。

傳送邀請 (iOS、macOS 及 Android)

透過傳送邀請開始註冊程序。 Ivanti Neurons for MDM 提供下列方法，讓您傳送註冊裝置的邀請給終端使用者:

- 在**啟動精靈**中
- 當**新增一個或多個使用者**時
- 在「使用者」頁面 (**動作 > 傳送邀請**) 中

> 若一般使用者誤置邀請，可以分享邀請中列出的 URL。 確定在 URL 結尾加上 **/go**。

擁有 Ivanti Neurons for MDM 含密碼帳戶的一般使用者無需邀請即可開始註冊程序。 可將邀請中列出的 URL 傳給他們。

指導一般使用者下載 app (iOS 和 Android)

Go 應用程式適用於 Android 和 iOS 裝置。 可以為一般使用者提供有關如何從公用應用商店下載應用程式並從應用程式啟動註冊過程的說明。 電子郵件邀請包含下列資訊:

- 前往註冊頁面的連結
- 一次性 PIN 碼 (若由管理員設定)
- 後續步驟的基本說明

若您已設定帳戶密碼，則可以將密碼傳送至一般使用者的公司電子郵件地址。 如果您是使用 LDAP 進行驗證，則可通知一般使用者需提供網路憑證。

如果使用者在註冊期間未完成 MDM 設定檔安裝，則 Ivanti Neurons for MDM 會定期傳送推播通知到裝置，提示使用者完成註冊程序。

使用者可以選用「使用者名稱」和「密碼」或者掃描 QR 碼從 Go app 開始裝置註冊。 詳細資訊如下:

- **使用者名稱**: 電子郵件地址
- **密碼**: 若在**使用者設定**中已指定，並由管理員定義了一個臨時密碼
- **QR 碼**: 從 Ivanti Neurons for MDM 自助式入口網站產生 QR 碼。 當您使用**掃描 QR 碼**選項掃描 QR 碼時，畫面上會顯示提示，要求您授予存取裝置相機的權限。 在授予權限之後，相機會掃描 QR 碼並註冊裝置。 Android 9 及更高版本、iOS 14 及更高版本支援此選項。

身為一般使用者，若您在行動裝置上收到註冊電子郵件，則點選連結以啟動註冊程序。 若您在筆記型電腦或桌上型電腦中收到註冊電子郵件，則可在行動裝置上輸入 URL 以開始註冊程序。

若您還沒有為 Ivanti Neurons for MDM 使用者帳戶定義密碼，或者使用者設定需要註冊 PIN 碼，則隨附單次有效的 PIN 碼。 輸入 PIN 碼之後，如果沒有密碼，系統就會提示您設定帳戶密碼。

> Android Enterprise 裝置完成註冊後，任何手動安裝至公司所擁有裝置或工作受管理裝置之工作設定檔的 CA 憑證，都會解除安裝。

重新註冊 iOS 裝置

如果要重新註冊裝置，可以依照下列方式執行此操作:

1. 在您的裝置上啟動 Go 用戶端。
2. 前往**設定** > **疑難排解** > **重新註冊裝置**。 重新註冊程序將啟動，並顯示一些確認提示。
3. 在提示上點選**是**。

> 如果在設定檔安裝程序中點選**取消**，註冊程序將停止，且 Ivanti Neurons for MDM 伺服器將停用裝置 MDM。

要重新啟動重新註冊程序，您必須重新安裝已下載的設定檔。 下載的設定檔僅在幾分鐘內有效，之後您必須從 Go 用戶端執行重新註冊。

重新註冊 Android 裝置

管理員可使用淘汰、抹除或刪除動作來重新註冊裝置，而不需要手動清除現有的作用中項目。 此方法對於重新註冊來說特別有用，因為新項目和現有項目都屬於相同租戶。 「裝置」頁面會在 Ivanti Neurons for MDM 管理入口網站中顯示裝置狀態，如下所示:

- **作用中** - 裝置註冊成功
- **已淘汰** - 將顯示狀態為已重設且已淘汰的裝置
- **已抹除** - 將顯示狀態為已重設且已抹除的裝置
- **已重設** - 裝置已重設且將在伺服器中維持作用中狀態，直到下一次註冊為止

「稽核追蹤」頁面會列出 Android 裝置的裝置註冊、重新註冊和已淘汰狀態。 如需更多資訊，請參閱使用小工具。

> 針對 Android 9.x 和較舊版本，會在重新註冊後顯示單一項目。 若為 Android 10.x 和較新版本，則會顯示多個項目。 不過，只有最新項目才會處於作用中狀態，而較舊的項目將處於已淘汰狀態。

7.5.5. 裝置註冊（Windows 10+ PC 和 Microsoft HoloLens 2）

本節包含以下各主題：

- 手動註冊
  - 傳送邀請
  - 完成一般使用者註冊程序
- Windows Autopilot
- Entra ID 標準註冊

裝置註冊程序有以下幾種類型：

- 手動註冊
  - 邀請
  - 使用者註冊
- Windows Autopilot
- 使用 SCCM 和 Ivanti EPM 並透過「使用 PIN 碼佈建套件註冊」。 請參閱使用 PIN 碼佈建註冊套件。
- 大量註冊

手動註冊

大多數的使用者一開始都要先註冊裝置。 您可使用下列任何一種方法開始註冊程序：

- 電子郵件邀請
- 將使用者導向您實作的 URL
- 一般使用者必須在 Ivanti Neurons for MDM 中擁有帳戶，才能開始裝置註冊程序。 若是 LDAP 使用者，就必須先設定好 **Connector** 和 **LDAP 伺服器**，也必須將使用者從 LDAP 伺服器進行匯入。 若是本機使用者，就必須新增使用者。
- 舊版 Ivanti Neurons for MDM 所產生的裝置註冊 URL 將無法在目前版本中使用。 管理員必須重新產生裝置註冊 URL 才能進行裝置註冊。

傳送邀請

大部分情況下，您都是透過傳送邀請來開始註冊程序。 可透過 Ivanti Neurons for MDM 提供的下列方法，將裝置註冊邀請傳送給終端使用者：

- 透過**啟動精靈**
- 在**新增一或多位使用者**時
- 在「使用者」頁面 (**動作 > 傳送邀請**) 中

如果一般使用者遺失邀請、使用桌上型電腦或筆記型電腦來接收邀請，或基於任何原因沒有收到邀請，您仍可以將邀請中隨附的 URL 傳送給他們。 只要將 **\go** 新增至服務 URL 尾端。

如果一般使用者擁有已設置密碼的 Ivanti Neurons for MDM 帳戶，無需邀請即可開始註冊程序。 您可以將邀請中隨附的 URL 傳送給他們。

完成一般使用者註冊程序

告知您的裝置使用者如何完成註冊程序。 您可將下列說明作為範本，並進行任何必要變更：

程序

1. 在您的 Windows 10+ PC 上開啟瀏覽器。
2. 導覽至 mobileiron.com/go。
   系統會將您重新導向至包含註冊 URL 的新頁面。
3. 將註冊 URL 複製到剪貼簿。
4. 點選**設定**頁面底端的**新增帳戶**。
5. 輸入您收到邀請的相關電子郵件地址。

> 如果使用者的 Ivanti Neurons for MDM 使用者名稱不符合在 Ivanti Neurons for MDM 中所輸入的使用者電子郵件地址，請告知使用者在系統提示輸入電子郵件地址時輸入使用者名稱。

將您複製的 Workplace 伺服器 URL 貼入下一個文字欄位中。

7. 點選**登入**。
8. 在下一個欄位中輸入密碼。
9. 其他欄位保留空白。
10. 點選**登入**。
11. 按一下**已新增帳戶**畫面中的**完成**。
    Workplace 啟動畫面中會顯示帳戶已新增。

Windows Autopilot

Windows Autopilot 是一種 Microsoft 功能，可協助系統管理員設定和預先配置新裝置，以便在工作中使用它們。 Autopilot 功能可幫助快速、可靠且無縫佈建 Windows Desktop 或 HoloLens 2 裝置。 此外，Autopilot 功能可幫助執行以下工作：

- 自動將裝置加入 Entra ID (Entra ID)
- 自動將裝置註冊至 MDM 服務
- 根據裝置描述檔建立和自動指派裝置至配置群組
- 自訂註冊體驗
- 套用配置和原則
- 安裝必要的應用程式

Ivanti 支援各種模式的 Autopilot 描述檔：

- 使用者導向
- 使用者導向預先佈建（之前稱為 White Glove）
- 自我部署模式

如需更多資訊，請參閱**設定 Windows Autopilot 描述檔**。

> 基於安全考量和防止未授權使用裝置，所有 Autopilot Windows 裝置都可使用 TenantLockdown CSP 功能鎖定至特定租戶。 如要使用此功能，必須使用 Autopilot 選項來註冊裝置。 可在裝置層級套用此配置。 請參閱 **TenantLockdown CSP**。

Entra ID 標準註冊

將使用者新增至 Entra ID 租用戶時，他們可以透過工作帳戶直接註冊其裝置。

程序

1. 在 Windows 裝置上，前往**設定 > 帳戶 > 存取公司或學校資源**。
2. 選取新增公司或學校帳戶，然後按一下**連接**。
3. 從您的工作帳戶提供電子郵件地址。

裝置會自動註冊至 Ivanti Neurons for MDM。

7.5.6. 本機管理密碼解決方案 (LAPS)

本機管理密碼解決方案 (LAPS) 將 Windows 裝置密碼的安全管理自動化。 LAPS 強制執行隨機、定期的密碼更改，並將這些密碼安全地儲存在一個目錄中，從而降低了在遭遇破解時發生橫向移動的風險。

現代 LAPS 與 Azure 和最新的 Windows 裝置管理平台整合，透過 Ivanti Neurons for MDM 和 Azure 入口網站實現安全的密碼儲存、擷取和原則組態。 這可確保管理員憑證在舊版和雲端受管理 Windows 端點上保持受保護和可稽核狀態。

> 要將 LAPS 用於 Ivanti Neurons for MDM，Azure 管理員應確保 N-MDM 應用程式以所需的 LAPS 權限 (**DeviceLocalCredential.Read.All**) 新增到其 Azure 租用戶中。

> LAPS 組態可以透過使用原則設定**管理員帳戶名稱**指定它套用於哪個本機管理員帳戶。 如果裝置上不存在設定中指定的帳戶名稱，則無法管理帳戶名稱。 但是，當**管理員帳戶名稱**為空時，原則預設為裝置的內建本機管理員帳戶，此帳戶由其眾所周知的相對識別碼 (RID) 標識。

> 套用 LAPS 組態後，裝置的本機管理員帳戶密碼將由管理員管理，密碼將在 Azure Active Directory 中產生。

LAPS 的其他特性

- Azure 中的密碼儲存 - 本機管理員密碼現在可以安全地儲存在 Azure 裝置物件中。
- 密碼擷取 – 管理員可以直接透過 Azure 入口網站擷取裝置密碼。
- 可配置設定 - 可以在 Ivanti Neurons for MDM 入口網站中管理 LAPS 可配置設定。
- 按需密碼輪換 - 管理員可以從 Ivanti Neurons for MDM 入口網站手動輪換裝置密碼。
- 使用時自動重設密碼 - 一旦存取密碼，就可以自動重設密碼。

建立 LAPS 組態

必要條件

- 必須為您的裝置啟用 LAPS 解決方案。 預設情況下，並非所有人都可以使用此解決方案。 請聯絡技術支援團隊尋求協助。
- 必須在 Azure Device Operations (ADO) 中註冊裝置。

程序

1. 在您的組態管理平台中，啟動 LAPS 組態的建立。
2. **設定所需參數**:
    - **備份目錄** - 選取僅將密碼備份到 Microsoft Entra ID。
    - **本機管理員名稱** - 指定系統上的管理員帳戶名稱 (例如 Admin)。
3. **設定額外的設定** - 根據組織的安全性原則設定這些設定。 如果不指定，則會使用預設值。
    - **PasswordAgeDays** - 自動輪換本機管理員密碼前的天數。
    - **PasswordComplexity** - 指定密碼複雜性要求 (例如，英數字元、特殊字元)。
    - **PasswordLength** - 設定所需的本機管理員密碼長度。
    - **PostAuthenticationActions** - 定義身分驗證後應執行的任何動作。
    - **PostAuthenticationResetDelay** - 設定延遲 (以小時/分鐘為單位) 以在身分驗證後重設密碼。

4. **發佈 LAPS 組態**
    - 將 LAPS 組態描述檔指派給 ADO 註冊的使用者/裝置。
    - 套用組態後，將建立一個隨機的本機管理員密碼，並將其安全地儲存在 Microsoft Entra ID 中：**裝置 → 管理裝置 → 本機管理員密碼復原**。
5. **密碼輪換**
    - 密碼會根據 **PasswordAgeDays** 中設定的值自動輪換。
    - 您可以在裝置記錄中查看密碼輪換狀態。

密碼輪換

要強制立即輪換本機管理員密碼，請執行以下步驟：

1. **導覽至裝置** - 轉到管理控制台中的裝置詳細資料頁面。
2. **啟動密碼輪換**
    - 按一下三點選單 (...)。
    - 選取**輪換本機管理員密碼**。
    - 出現系統提示時，確認動作。 這將提交密碼輪換要求。
3. **登記和確認**
    - 裝置在下次強制登記時處理密碼更改。
    - 重新整理 Microsoft Entra ID 中的頁面，在密碼復原區段檢視更新的密碼。

7.5.7. 佈建使用 PIN 碼註冊套件

管理員可將 SCCM 或 Ivanti Endpoint Manager 管理的裝置註冊到 Ivanti Neurons for MDM。 部署套件工具允許組織簡化 Windows 裝置到 Ivanti Neurons for MDM 現代管理的轉換，無需停機或中斷一般使用者。 從 Ivanti Neurons for MDM 主控台下載特定的部署套件，然後透過現有的管理工具或網域進行部署，以達成順利轉換。 在執行此套件後，它將會以無訊息方式將端點註冊至 Ivanti Neurons for MDM 以繼續進行管理。 此方式可讓管理員先輕鬆地移轉裝置，之後再透過無線方式來配置裝置。 當裝置以無訊息方式註冊至 Ivanti Neurons for MDM 後，就會加入 MDM，由這兩個管理授權單位共同管理。 管理員在 Ivanti Neurons for MDM 中設定所需的 Windows 體驗後，即可停用舊版管理平台，讓 Ivanti Neurons for MDM 成為裝置的唯一管理授權單位。

> 若裝置從 Microsoft Endpoint Manager (MEM) 或先前的 SCCM 轉換，則不適用此規則。 現有的 MEM Client 將以「共存模式」 (相對於共同管理模式) 繼續運作，直到停用 MEM 平台。 啟用共存模式後，MEM Client 將自動停用某些功能，轉而支援提供那些工作負載的 Ivanti Neurons for MDM。 如需更多資訊，請參閱 **Microsoft 的共存說明文件**。

如需在使用 MEM 和其他第三方管理平台時執行更準確的行為，Ivanti 建議先在您的環境中測試 Ivanti Neurons for MDM 部署套件工具。

必要條件

- 必須使用 LDAP、Entra ID (Entra ID)、Local User Upload 或其他身分識別整合，在 Ivanti Neurons for MDM 上匯入使用者帳戶
- 所有裝置都應安裝 **Windows Configuration Designer**。
- 在 Ivanti Neurons for MDM上啟用 PIN 碼型註冊
- 使用者的使用者名稱中不應有空格，這可能會導致使用者裝置轉換失敗。
- 此工具可在不利用 Entra ID 的環境中部署。
- Ivanti Neurons for MDM Modern Windows Management Suite 的主要元素不需要 Entra ID。 共同管理或共存可能需要在無訊息自動註冊時部署某些工作負載/組態，以免在轉換期間發生任何影響。
- 「部署套件」目前僅在 SCCM 和 Ivanti Endpoint Manager 上受支援。

程序

1. 前往**管理員 >Windows >部署套件**。
2. 選擇**使用者**或**使用者群組**以產生 PIN 碼，然後按一下**下載部署套件** (.zip 檔案)。
3. 將部署套件提供給 SCCM / Ivanti Endpoint Manager 管理員，由這些管理員將檔案解壓縮後傳輸到受管理的各個裝置。 若需如何執行此步驟的相關說明，請參閱 **Configuration Manager 的套件與程式**。
4. 傳輸後，管理員遠端觸發裝置上的 setup.ps1 指令碼。 觸發指令碼的相關資訊，請參閱**透過 Configuration Manager 建立與部署指令碼**。
5. 裝置註冊在 Ivanti Neurons for MDM 上。

>

為使用者產生的 PIN 碼僅在 24 小時內有效。 一旦 PIN 碼過期，就必須重新產生新的 PIN 碼。

包含 PIN 碼的檔案會在裝置註冊後刪除。

將 SCCM 裝置註冊到 Ivanti Neurons for MDM

程序

1. 針對所選使用者，從 Ivanti Neurons for MDM 下載所有與部署相關的檔案。

2. 選擇應註冊的帳戶或群組。
3. 使用 SCCM 將套件檔案部署至用戶端裝置:
    1. 驗證 SCCM 中是否存在所需的用戶端。 若用戶端上沒有 Windows Configuration Designer，則管理員應推送 Designer 並將其部署在用戶端上。
    2. 在 SCCM 伺服器上，建立一個資料夾，然後複製部署 zip 檔案，然後解壓縮檔案內容。
    3. 建立一個會複製資料夾內容 .bat 檔案，將資料夾中的檔案解壓縮至用戶端裝置。
    4. 在 SCCM 中，前往**軟體程式庫 > 應用程式管理 > 套件**，然後建立一個套件將資料夾的內容複製到用戶端。 輸入要複製內容的目的地資料夾。
    5. 將套件部署到裝置或裝置位置。
    6. 在「監控」區段下，可以監控部署狀態並確認檔案是否已複製到用戶端目的地資料夾。
4. 執行指令碼註冊裝置:
    1. 前往**軟體程式庫 > 指令碼**，建立指令碼。
    2. 為指令碼輸入一個名稱，然後從解壓縮的資料夾中匯入 PowerShell 指令碼 **setup.ps1**。
    3. 核准指令碼並在目標裝置上執行指令碼。
    4. 選擇**立即啟動**，然後按一下**儲存**。 「已排程」的工作開始執行指令碼。 成功執行後，狀態將變成「綠色」。
5. 若要驗證裝置註冊，前往**設定** > **新增或移除佈建套件** > **詳細資訊**。

將 Ivanti Endpoint Manager 裝置註冊到 Ivanti Neurons for MDM

程序

1. 針對所選使用者，從 Ivanti Neurons for MDM 下載所有與部署相關的檔案。
2. 選擇應註冊的帳戶或群組。
3. **案例 1**: 考慮一個適用於以相同使用者名稱註冊裝置的裝置名稱 - 在這種情況下，電子郵件地址並非有效的使用者電子郵件地址。 帶有串連了 AD 網域的裝置名稱的電子郵件被視為註冊電子郵件地址。 管理員必須將「帳戶」設定為 LocalSystemAccount 並使用 setup.ps1 作為主要檔案以初始化 PowerShell 執行。
   案例 2: 考慮一個適用於註冊裝置的有效電子郵件地址，對修改裝置位置中的檔案沒有限制 - 使用登入的使用者電子郵件地址進行註冊。 若要啟用此註冊，管理員必須將「帳戶」設定為「目前」使用者帳戶並使用 setup.ps1 作為主要檔案以初始化 PowerShell 執行。
   案例 3: 考慮一個適用於註冊裝置的有效電子郵件地址，對修改裝置位置中的檔案有所限制 - 使用登入的使用者電子郵件地址進行註冊。 本案例有兩個子案例:
    - 使用兩個指令碼進行註 - 使用**setupEPMCopyContentsToTempFolderStep1.ps1 建立發佈套件**並以「目前使用者帳戶」身分執行。 將檔案複製到暫存位置。 使用 **setupEPMCopyContentsToTempFolderStep2.ps1 建立另一個發佈套件**並以「本機系統帳戶」身分執行。

      > 如果裝置使用者對包含套件檔案的資料夾的修改設有限制 - 則會複製檔案到暫存資料夾，確認使用者 ID 並建立 PowerShell 套件。 PowerShell 套件是由 **setupEPMCopyContentsToTempFolderStep2.ps1** 指令碼執行。 安裝完成後，便會刪除暫存資料夾。

   停用/啟用 UAC

    1. 更新登錄項目以停用 UAC 控制並重新啟動電腦
    2. 以「目前」使用者的帳戶身分並使用 setup.ps1 執行 PowerShell 套件
    3. 更新登錄項目以啟用 UAC 控制並重新啟動電腦

建立 PowerShell 套件:

1. 驗證 Endpoint Manager 中是否存在所需的用戶端。
2. 將檔案複製到 C:\Program Files\LANDesk\ManagementSuite\LANDesk\files\。 在此資料夾中建立一個子資料夾，然後將檔案解壓縮。
3. 建立套件: **發佈 > 發佈套件 > 新增 > Windows > PowerShell**。

   > 管理員可根據裝置上設定的限制層級將套件散發到不同的裝置。

4. 在「主要檔案」區段中，請輸入套件名稱並從含有所複製檔案的資料夾上傳 setup.ps1
5. 在「其他檔案」區段下，使用**新增**複製其餘檔案 (setup.ps1 script 除外)
6. 在「帳戶」區段下，選擇「目前」使用者的帳戶。
7. 按一下**儲存**。

4. 建立排程工作:
   1. 選擇已建立的套件，按一下滑鼠右鍵，然後選擇**建立排程工作**。 排程工作隨即建立。
   2. 拖曳裝置並將其新增到排程套件區段。
   3. 在排程套件上，按一下滑鼠右鍵，然後選擇**內容**。
   4. 驗證套件。
   5. 在工作類型下，選擇**推送**。
   6. 選擇**立即啟動**，然後按一下**儲存**。 「已排程」的工作開始執行指令碼。 成功執行後，狀態將變成「綠色」。
5. 若要驗證裝置註冊，前往**設定** > **新增或移除佈建套件** > **詳細資訊**。 或者，管理員可以在裝置的「診斷記錄」下驗證裝置註冊。

7.5.8. 使用 Windows 裝置大量註冊

大量註冊功能可讓您快速向 Ivanti Neurons for MDM 註冊多台 Windows 裝置。

必要條件：

- 必須使用 Entra ID (Entra ID) Premium 帳戶，在 Ivanti Neurons for MDM 上匯入使用者帳戶。
- 所有裝置都應安裝 **Windows Configuration Designer**。

程序：

1. 連結 Ivanti Neurons for MDM 和 Entra ID 租用戶。 請參閱**針對 Windows 10 裝置將 Entra ID 連線至 UEM**。
2. 開啟 **Windows 設定設計工具** 應用程式並選取**佈建桌上型電腦裝置**。 新的專案視窗會顯示在畫面中。
3. 輸入下列詳細資料：
    - 名稱 - 您專案的唯一名稱
    - 專案資料夾 - 您要在裝置中儲存專案的位置
    - 說明 - 專案的選用說明

按一下**結束**以關閉新專案視窗並執行一連串步驟。

5. **設定裝置**
   輸入您裝置的唯一名稱。 名稱可包含序號 (%SERIAL%) 或一組隨機字元。
6. 或者，若您正在升級 Windows、設定裝置以進行共用或移除預先安裝的軟體，也可以輸入產品金鑰。
7. **設定網路**
   或者可設定在其第一次啟動時連線的 Wi-Fi 網路裝置。 若未設定網路裝置，則當裝置第一次啟動時會需要有線網路連線。
8. **帳戶管理**
   選取**在 Entra ID 中註冊**，輸入**大量權杖到期**日期，然後按一下**取得大量權杖**。
9. 輸入您的 Entra ID 認證以取得大量權杖。
10. 在**維持登入所有應用程式**頁面中，按一下**否，只登入此應用程式**。
    - 當成功擷取大量權杖並建立套件後，按「下一步」。
    - 已在 Azure 入口網站中建立佈建套件的使用者 - 使用者主體名稱 (例如 package_0ea893a5-1e93-4d21-a6b1-dc788946fd1d@miwinqe.onmicrosoft.com)。 將檔案 (執行時期 ppkg 工具) 複製到儲存裝置。

> 建立大量權杖的 Entra ID 使用者以及套件使用者不應啟用 MFA。 若要驗證，您必須針對該使用者執行 OOBE + Entra ID 聯結。

重新建立或同步處理套件使用者 (在 Azure 中建立) 至 Ivanti Neurons for MDM。

使用包含佈建套件的快閃磁碟機進行裝置的大量註冊。 您也可以在現有裝置上按兩下以執行 OOBE 後體驗。 若套件第一次嘗試安裝時失敗，則第二次嘗試也會失敗。 確認是否已在 Ivanti Neurons for MDM 中建立新裝置且 Entra ID 屬於套件使用者。

7.5.8.1. Ivanti 大量註冊

管理員可以使用前置詞為 **windows-bulkenroll** 的一般使用者 (透過 ppkg) 註冊多部 Windows 裝置，然後再進行使用者指派。

必要條件：

- 在 Ivanti Neurons for MDM 上，建立一個前置詞為 **windows-bulkenroll** 的使用者帳戶。 例如，**windows-bulkenroll**-user1@abc.com、**windows-bulkenroll**-user2@abc.com。

使用 Windows 設定設計工具建立 PPKG 套件

1. 下載並安裝 **Windows 設定設計工具**。
2. 建立新專案。
3. 按一下**佈建桌面**。
4. 輸入專案名稱，然後選取路徑。
5. 在**設定裝置**區段中，輸入裝置名稱。
6. 在**設定網路**區段中，輸入網路名稱 (如果需要，可以設定網路，或可予以停用)。
7. 在**帳戶管理**區段中，選取**以本機管理員身分註冊**。 輸入**使用者名稱**和**密碼**，然後按一下**下一步**。
8. 在**新增應用程式**區段中，按一下**下一步**。
9. 在**新增憑證**區段中，選取**切換到進階編輯器**，然後按一下**繼續** > **是**。
10. 前往 **RuntimeSettings** > **Workplace 註冊**。 輸入 **UPN** (於 Ivanti Neurons for MDM 先決條件區段中建立的同一位使用者)。 選擇下列選項:
    - AuthPolicy: OnPremise
    - DiscoveryServiceFullUrl: https://login.mobileiron.com
    - 選取: 輸入密碼

按一下**檔案** > **儲存**。

12. 按一下**匯出** > **佈建套件**。
13. 在後續畫面上按一下**下一步**，然後按一下**建立**。
    ppkg 檔案儲存在指定位置。

使用 ppkg 在 OOBE 模式下佈建裝置

使用從上一個區段中新建立的 ppkg 套件檔案來佈建裝置。 裝置註冊並簽入成功後，您將在 MDM 伺服器上找到前置詞為 **windows-bulkenroll** 的使用者之裝置項目。

指派裝置給使用者

1. 在「裝置」頁面上，按一下前置詞為 **windows-bulkenroll** 的使用者。
2. 按一下**指派給使用者**。 「指派給使用者」視窗隨即開啟。
3. 從清單中選取或搜尋裝置。
4. 選取所需的裝置。
5. 按一下**指派給使用者**。 系統會將所選裝置指派給使用者。

使用者初次登入裝置時，必須變更密碼。

「指派給使用者」選項僅適用於 Ivanti 大量註冊裝置。

針對在此類別下註冊的裝置，只有裝置範圍組態和應用程式能夠正常運作。 不支援使用者範圍組態和應用程式。

7.5.9. 變更密碼設定

本節包含以下各主題：

- 變更指派的密碼配置
- 指派不同的密碼配置

使用指派給裝置的密碼組態變更密碼設定。 您也可以：

- 變更已指派配置的設定

或者

- 指派其他密碼配置

若您對配置進行變更，將會影響指派了該項配置的所有裝置。

變更指派的密碼配置

程序

1. 前往**裝置**。
2. 找到清單中的裝置項目。
3. 按一下**名稱**欄位中的連結。

> 如果已指派了密碼配置，就會顯示在「配置」索引標籤中。

在「配置」索引標籤中，按一下**密碼配置**連結。

5. 按一下**編輯** (右上角)。
6. 進行所需變更。

指派不同的密碼配置

程序

1. 確認已有人建立了您所需的配置
2. 前往**裝置**。
3. 找到清單中的裝置項目。
4. 按一下**名稱**欄位中的連結。

7.5.10. 變更裝置名稱

管理員可手動變更裝置的名稱 (不使用「編輯裝置名稱」配置)。

適用於：

- iOS 受監管的裝置
- tvOS 受監管的裝置
- macOS 10.10+ 裝置

程序

1. 前往**裝置**。
2. 找到清單中的裝置項目。
3. 執行下列其中一個步驟：
    - 若要新增**裝置名稱**欄位 (如果尚未新增)，請按一下右上角的「設定」齒輪圖示，然後選擇**裝置名稱**。
    - 按一下**名稱**欄位中的連結，以前往裝置詳細資料頁面。
4. 在裝置名稱旁邊，按一下**編輯**鉛筆圖示。
5. 輸入新的裝置名稱，然後按一下勾號圖示。
6. 在「覆寫裝置名稱」顯示方塊中，檢閱注意事項並按一下**確定**。

變更的名稱將在裝置下次簽入時推送到裝置。 此動作無法取消。

> 如果之前已設定「預設裝置名稱」配置，此動作將會覆寫配置中的名稱設定。

7.5.11. 搜尋與篩選裝置

本節包含以下各主題：

- 搜尋裝置
- 篩選裝置
- 使用進階搜尋
- 載入搜尋查詢

搜尋裝置

在規則建立器中選取「使用者群組名稱」屬性後，Ivanti Neurons for MDM 管理入口網站會顯示重複的使用者群組數量及對應的 GUID 數量，以識別重複的群組。 此外，此規則之下的表格會顯示重複使用者群組的清單以及其詳細資訊，例如使用者群組名稱、GUID、來源和可分辨的名稱 (DN)。

程序

1. 前往**裝置**。
2. 在**搜尋**欄位中輸入裝置名稱。 隨即列出包含這些字元的所有裝置。

篩選裝置

「篩選」側邊導覽列會列出各種區段以協助您在整個裝置清單中搜尋裝置。 「管理篩選」精靈包含所有區段的清單，使您可以選取要顯示在「篩選」導覽列中的區段。

程序

1. 前往**裝置**。
2. 在「篩選」側邊導覽列所列出的區段中按一下相關核取方塊。

   範例：
   - 從**已啟用使用者**區段中選擇**是**，以僅顯示使用者處於已啟用狀態的裝置。
   - 如果您已指派自訂屬性給裝置，可以按一下設定 (齒輪) 圖示，藉此根據那些屬性來篩選裝置。
   - 從**狀態**區段中選擇**已淘汰**與 **iOS**，以僅顯示已淘汰的 iOS 裝置。

(選用) 按一下**還原預設值**將選取的項目還原為預設篩選。 「篩選」導覽列會顯示選取的區段。 若您清除「管理篩選」精靈中的所有核取方塊，則「篩選」側邊導覽列會顯示所有區段。

4. 按一下「管理篩選」精靈以外的任何位置即可結束精靈。
5. (選用) 按一下 x 圖示以關閉「篩選」側邊導覽列，按一下**篩選**則可重新開啟側邊導覽列。
   - 若您使用 stopwords.txt 檔案中列出的任何停用字詞 (Apache SOLR 伺服器組態的一部分)，則不會建立該字詞的索引，因此包含這些停用字詞的項目都不會顯示在搜尋結果中。
   - 實體範例如下：裝置、使用者、群組、屬性、應用程式、憑證、稽核追蹤、內容及通知模組。
   - 停用字詞範例如下：a、an、if、be、into 等等。

使用進階搜尋

您可使用進階搜尋選項根據規則來搜尋裝置，以識別和檢視符合特定準則的裝置。 此規則可使用適用的運算子進行建構，包括「開頭是」、「結尾是」、「包含」、「不包含」、「開頭不是」、「結尾不是」、「小於」、「大於」、「範圍」、「等於」及「不等於」運算子。 這些規則選項可以用「任何 (或)」或「所有 (及)」選項來建立巢狀結構。 符合規則的裝置會顯示在此區段下方。

Ivanti Neurons for MDM在規則建立器中選取了「使用者群組名稱」屬性後，管理入口網站會顯示重複的使用者群組數量及對應的 GUID 數量，以識別重複的群組。 此外，此規則之下的表格會顯示重複使用者群組的清單以及其詳細資訊，例如使用者群組名稱、GUID、來源和可分辨的名稱 (DN)。

程序

1. 從「裝置」頁面，按一下**進階搜尋**連結。 「進階搜尋」精靈隨即開啟。
2. 按一下下列其中一個選項：
   - 如果裝置必須符合至少一項規則，請選取**任一**
   - **全部** - 裝置必須符合所有規則時使用

建立一個定義搜尋準則的規則。 **例如**：「支援 APNS」等於「是」。

4. (選用) 按一下 **+** 以建立其他規則。
5. 按一下**搜尋**。 會顯示符合搜尋準則的裝置清單。
   - 在 iOS 14.0+ 裝置上，裝置詳細資料頁面會顯示裝置的 eSIM ID (EID)。 eSIM ID (EID) 可讓電信業者將 SIM 指派給特定裝置。「eSIM ID (EID)」欄位符合 GDPR 的規範。
   - 由於新版本Ivanti Neurons for MDM增加了新的 GDPR 欄位 (例如「IP 位址」和 eSIM ID)，已設定 GDPR 的管理員必須編輯 GDPR 設定檔才能隱藏新欄位。
   - 進階搜尋顯示裝置的復原鎖定狀態。

載入搜尋查詢

可以檢視已儲存的搜尋查詢清單。

程序

1. 按一下「進階搜尋」，然後按一下資料夾圖示。 建立的搜尋查詢清單會顯示在**載入的查詢**區段中，並顯示下列詳細資訊：
   - **查詢名稱** - 載入查詢的名稱。
   - **查詢內容** - 顯示定義搜尋查詢的規則內容。
   - **動作** - 選擇要對查詢執行的動作。
2. 按一下**動作**欄中的**載入查詢**，以檢視符合載入查詢中定義準則的裝置清單。
3. 按一下**刪除**以刪除載入查詢。

7.5.12. 使用裝置擁有者

本節包含以下各主題：

- 使用 QR 代碼或 NFC Bump 佈建 Android Enterprise 裝置
- 使用用戶端權杖佈建 Android Enterprise 裝置

授權：Gold

註冊裝置後，您即可將其指定為「公司擁有」或「員工擁有」。 此指定有助於根據使用者持有的是個人裝置或公司擁有裝置來管理原則。 如果您擁有適當的授權，即可使用擁有權規則來建立裝置群組。

開始使用新裝置或原廠重設裝置，請使用 **Provisioner** app 搭配下列其中一個選項來設置裝置擁有者模式：

- NFC (近場無線通訊) bump
- QR 代碼掃描

NFC bump 方式為透過讓新裝置或原廠重設裝置感應主要裝置或範本裝置，藉此進行佈建。

QR 代碼掃描方式依序為輕觸新裝置或原廠重設裝置的螢幕、設定 Wi-Fi 網路，然後在裝置準備好進行佈建時掃描代碼。

使用 NFC 或 QR 代碼佈建「裝置擁有者」模式時，Provisioner app 接受註冊權杖。 進行註冊時，註冊權杖會傳送到伺服器。 當伺服器上出現註冊權杖，而且裝置已指派給使用者，則裝置即成功註冊。

Go 用戶端會控制進入「裝置擁有者」模式的裝置，並鎖定螢幕畫面直到裝置向 Ivanti Neurons for MDM 註冊為止，以防止使用者離開佈建程序。 裝置擁有者模式也支援單一應用模式。 如需配置資訊，請前往：**鎖定與單一應用配置**。

重要

- 如果您淘汰處於裝置擁有者模式的裝置，裝置將進行原廠重設。
- 裝置擁有者模式中的所有裝置都可選擇是否要啟用所有系統 app。
- 裝置一次只能有一個作用中的裝置擁有者模式。
- 只有支援 Android Enterprise 的裝置才能佈建到裝置擁有者模式。
- 若是處於裝置擁有者模式的 Samsung Knox Standard 裝置，系統會提示使用者啟動 Samsung ELM 授權。 若是處於裝置擁有者模式的 Samsung 裝置，從舊版 Go 用戶端應用程式升級至 Ivanti Neurons for MDM 支援的最新版本時，也會出現這項提示。 啟動之後，「裝置詳細資料」頁面上會顯示序號，並與「裝置 > 設定 > 序號」欄位相符。

使用 QR 代碼或 NFC Bump 佈建 Android Enterprise 裝置

若要使用 QR 代碼或 NFC Bump 佈建 Android Enterprise 裝置，您必須在主裝置上從 Google Play 下載並安裝 Provisioner 應用程式。

相容的元件

Provisioner 版本：1.3.0。

Provisioner 可與下列項目相容或搭配使用：

個項目	版本
Android 作業系統 (在要佈建的裝置上)	• 需要 5.0 - 或支援的更新版本 (如果使用 NFC)。 • 需要 7.0 - 或支援的更新版本 (如果使用 QR 碼)。 裝置必須支援 Android Enterprise。
Android OS (在主要裝置上)	5.1 - 至支援的最新發行版本。 裝置必須具備 NFC 以使用 NFC bump。 若為 QR 代碼則不需要此功能。
UEM 伺服器產品，已啟用 Android Enterprise	下列其中一項： Ivanti Neurons for MDM，或標示允許的 Ivanti Neurons for MDM。
Android 用戶端 app	最新版的用戶端 app 會自動安裝在 Provisioner 所設置的裝置上。

必要條件

若要將 Android Enterprise 裝置佈建為工作受控裝置，您需要:

- 確保已定義所需的 Android Enterprise 相關組態，並將其套用至已註冊的裝置。

> 預設 Android Enterprise: 必須為裝置啟用工作受控裝置組態。

在伺服器上啟用 Android Enterprise。

- 讓具備 NFC 功能，並已安裝 Provisioner app 的 Android 裝置 (僅限如果使用 NFC) 作為主要裝置。
- 佈建支援 Android Enterprise 的裝置。

若要啟用 Android Beam 以使用 NFC bump：

程序

1. 在裝置上前往**設定**。
2. 前往**網路 > 無線網路**。
3. 在**連線區段**中選擇**共用與連線**。
4. 將 **NFC** 的開關滑至**開**。
5. 將 **Android Beam** 的開關滑至**開**。

> 啟用 Android Beam 和 NFC 的步驟可能會隨裝置不同而有差異。

將 Android Enterprise 裝置佈建為工作受控裝置

程序

1. 使用 Android 主要裝置，從 Google Play 下載 Provisioner app 並安裝該 app。
2. 在主要裝置上啟動 Provisioner。
3. 選擇 NFC 或 QR 代碼作為佈建方式。
4. 輕觸 **App for Provisioning**，然後選擇要在進行佈建之裝置上安裝的用戶端 app：

選擇此用戶端 app：	向此 UEM 伺服器註冊：
前往	Ivanti Neurons for MDM
工作中 UEM	(標示允許的) Ivanti Neurons for MDM

5. 填寫 Provisioner app 中剩下的欄位。 如果有支援的 Wi-Fi 類型，部分欄位可能會自動填入。 如果選擇 QR 代碼，則不會顯示 Wi-Fi 欄位。 使用以下準則：

欄位	值
選擇要佈建的 app	Go 或 At Work
時區	輸入要在裝置上設定的時區
地區設定	輸入要在裝置上設定的地區設定
啟用所有系統 App	按一下勾選框以啟用所有系統 app
Wi-Fi 網路 SSID	輸入目標裝置將使用的 Wi-Fi SSID
Wi-Fi 安全性類型	輸入 Wi-Fi 安全性類型
Wi-Fi 密碼	輸入 Wi-Fi 的密碼
大量註冊	大量註冊功能為選用性。 若要使用大量註冊，必須輸入主機名稱。 (選用)，可輸入使用者名稱，並可選擇快速啟動選項。 若要略過大量註冊功能，必須將這些欄位保留空白。

6. 輕觸以**繼續**。
7. 如果您選擇 **NFC**，請輕觸**繼續**。 畫面 **Bump 裝置！**顯示在主要裝置上。 繼續進行以下的 **NFC Bump** 區段。
8. 若選擇了 **QR 碼**，畫面**掃描此 QR 碼！**顯示在主要裝置上。 繼續進行以下的 **QR 代碼**區段。

若為 NFC Bump，請使用以下步驟

確認目標裝置正顯示 Android 歡迎使用畫面。

9. 讓主要裝置與目標裝置的背面互相接觸並按住，以起始 NFC 傳輸。 如果 NFC 傳輸成功，目標裝置會發出聲響，然後繼續下載用戶端 app。 如果無法建立 Wi-Fi 連線，或者如果裝置無法下載用戶端 app，裝置會自動進行原廠重設。
10. 如果您聽到聲響或看到畫面已不是歡迎使用畫面的話，便可以將裝置分開。 這通常需要幾秒鐘的時間。 如果裝置未加密，則在繼續之前會先啟動加密程序。
11. 您可繼續透過將裝置與主要裝置 bump 的動作來佈建其他裝置。 目標裝置必須顯示「歡迎使用」畫面，而主要裝置則必須顯示「Bump 裝置！」畫面。

若為 QR 代碼佈建，請使用以下步驟

確認目標裝置正顯示 Android 歡迎使用畫面。

12. 在目標裝置的 Android 歡迎使用畫面相同位置上連續輕觸 6 次

13. 系統將提示您設定 WiFi 網路，好讓設置精靈可在目標裝置下載 QR 代碼讀取器。
14. 下載 QR 代碼讀取器之後，相機會隨即啟動。
15. 將目標裝置保持在主要裝置上方幾公分的距離，直到 QR 代碼掃描成功為止。 設置精靈隨後將繼續下載用戶端 app。 如果其無法下載用戶端 app，會自動進行原廠重設。
16. 您可繼續透過掃描主要裝置上的 QR 代碼來佈建其他裝置。 目標裝置必須讓相機準備好進行掃描，並且主要裝置必須顯示「掃描此 QR 碼！」畫面。
17. 也可透過輕觸共用圖示將 QR 代碼匯出。 各個裝置提供的匯出選項可能所有差異。

使用用戶端權杖佈建 Android Enterprise 裝置

您可以使用品牌用戶端權杖在裝置擁有者模式下佈建 Android Enterprise 裝置，而非使用 NFC Bump 或 QR 代碼進行佈建。 此方法可讓您使用權杖來登入裝置，這有助於加速 Go 或 At Work 用戶端的自動安裝以及在裝置擁有者模式中進行佈建：

> 在使用 Android 6 或支援的更新版本，並透過受管理的 Google Play 帳戶來進行佈建的裝置支援品牌化用戶端權杖。 如需詳細資料，請參閱 Android UEM 開發人員指南。 https://developers.google.com/android/work/prov-devices#Key_provisioning_differences_across_android_releases.

使用此方法的需求：

- 您必須註冊 Android Enterprise 帳戶。
- 裝置必須支援 Android Enterprise。
- 裝置必須使用 Android 6 至最新發行版本。
- 您必須具有新裝置或原廠重設裝置。

設定 (執行 Android 5.0+ 的裝置)

程序

1. 在 Ivanti Neurons for MDM 入口網站中，前往**配置**。
2. 按一下 **+新增**。
3. 選取**鎖定和 Kiosk: Android Enterprise**。
4. 將顯示**建立鎖定和 Kiosk: Android Enterprise 組態**頁面。

輸入配置名稱與說明。

5. 選擇鎖定類型。

按一下**受工作管理的裝置 (裝置擁有者)**。

6. 隨即顯示裝置擁有者鎖定設定選項。

您可選擇

- 停用 WI-FI 或 WI-FI 設定
- 停用相機
- 停用 Bluetooth
- 不允許 Bluetooth 設定
- 停用螢幕擷取

- 總音量靜音
- 不允許 App 管制
- 不允許憑證
- 不允許緊急廣播
- 不允許行動網路
- 不允許網際網路共用
- 不允許 VPN
- 不允許原廠重設
- 啟用原廠重設保護。

> 您可選擇性指定獲得授權的 Google 帳戶 ID (整數值) 清單，以便在原廠重設或將游標移到「說明」圖示以檢視擷取已授權帳戶 ID 的說明之後設置裝置。

不允許修改帳戶

- 停用 NFC (外送 Beam)
- 不允許撥出電話
- 不允許安全開機
- 不允許共享位置
- 不允許偵錯功能
- 確認驗證 App
- 不允許 SMS
- 不允許取消麥克風靜音
- 停用自動設定時間
- 停用自動時區
- 停用數據漫遊
- 停用 Wi-Fi 休眠
- 限制輸入法
- 限制存取服務
- 停用 USB 檔案傳送
- 停用外部媒體
- 停用 Keyguard (如果已設定 PIN 碼/密碼，則無效)
- 連接電源時保持螢幕開啟
- 不允許建立視窗
- 略過第一次使用提示

在**啟用/停用系統 App** 區段中，您可以選擇啟用以停用下列系統 App：

7. 您可選擇啟用**單一應用模式**。

個項目	版本
預設系統 App	
內建相機	按一下切換按鈕以**開啟**或**關閉**內建相機 app。
內建電話	按一下切換按鈕以**開啟**或**關閉**內建電話 app。
系統 App 套件名稱	若要啟用或停用預設系統 App 以外的任何其他系統 App，請按一下 +(加號) 圖示並新增系統 App 套件名稱。 若要移除系統 app，請按一下 -(減號) 圖示。

隨即顯示下列設定：

- 啟用鎖定作業模式
- 自動輸入單一應用 (僅在初始設置時)
- 停用快速設定
- 允許使用者存取 Wi-Fi 設定
- 允許使用者存取 Bluetooth 設定
- 允許使用者存取位置設定
- 允許使用者延遲應用程式更新
- 允許使用者存取日期與時間設定
- 允許使用者存取行動網路設定
- 允許使用者選擇語言
- 啟用共用裝置 (選擇下列其中一個選項)
  - 啟用登入
  - 啟用登出 (提供逾時設定 - 以小時為單位)

可選擇從下拉式清單選擇預設或自訂品牌選項。

8. 您可選擇建立「單一應用退出 PIN 碼」，以便退出單一應用模式。
9. 您可選擇建立 app 允許清單，以便讓使用者在單一應用模式中使用。

佈建裝置

程序

1. 開啟裝置電源並輸入您的 WI-FI 密碼。 您的裝置可能會提示您使用不同的密碼。
2. 在**驗證您的帳戶**畫面中，輸入您的 Android Enterprise 權杖。 按**下一步**。
3. 在 **Google 服務**畫面中按一下**安裝**。
4. 接受條款與細則。
5. 在設置工作裝置畫面中按**下一步**。 Go 或 At Work 用戶端下載並安裝於裝置上。 裝置現在隨即進入裝置擁有者模式。

相關主題

- 使用 Android 大量註冊
- 裝置群組

7.5.13. 搭配工作描述檔的受管理裝置

「搭配公司擁有裝置上的工作描述檔的受管理裝置」是一種模式，其中 Android Enterprise 裝置是企業擁有的裝置但內含各不相同的個人資料。 此模式支援兩個描述檔，其中您可在受管理描述檔內部部署工作 app，同時讓使用者保有個人空間。 「搭配公司擁有裝置上的工作描述檔的受管理裝置」模式的建立是透過將「搭配工作描述檔的受管理裝置」配置發佈到使用裝置擁有者模式設置的裝置上。

如需「搭配工作描述檔的受管理裝置鎖定設定」的相關詳細資訊，請參閱**鎖定與單一應用：Android Enterprise**。

> 此模式需要 Android 8.0 至支援的最新發行版本。

App 配置、跨描述檔的 app 共享小工具、用戶端憑證別名及 ID 憑證都可以套用到「搭配工作描述檔的受管理裝置」。

下列配置適用於「搭配工作描述檔的受管理裝置」：

- 進階密碼
- 一律開啟 VPN
- 認證
- 身份憑證
- Google 帳戶
- 密碼
- Samsung 手機限制
- 威脅防護
- Wi-Fi
- 預設的 App 執行時期權限
- SafetyNet 證明
- 密碼
- 威脅防護本機動作

7.5.14. 使用 Android 大量註冊

大量註冊功能可讓您快速向 Ivanti Neurons for MDM 註冊多台 Android 裝置。

授權：Silver

在使用大量註冊之前，請執行以下作業：

1. 在用來註冊裝置的電腦上，安裝 Android Debug Bridge (adb) 隨附的 Android SDK。
   有關 Android 偵錯橋接器的詳細資訊，請參閱: http://developer.android.com/tools/help/adb.html。
2. 啟用 USB 偵錯。
   Android 裝置的 USB 功能啟用程序取決於 Android 版本而定。 請參閱：http://developer.android.com/tools/device.html 以取得啟用 USB 偵錯的相關詳細資訊。
3. 在每台裝置上安裝 Go 用戶端。
4. 透過 USB 纜線將裝置連接至要用來註冊裝置的設置電腦。

可使用 Android Debug Bridge (adb) 殼層啟動 Go 並將之註冊至伺服器。 Android Debug Bridge 是一種工具，可從 Windows 的命令列使用，或透過 iOS 的 Terminal 公用程式使用。 該工具可讓您與連接的 Android 裝置通訊。 從 adb 殼層使用的命令格式為：

> 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

> 註冊通訊協定 **(mirp)** 用於將註冊的相關資料編碼。

有效的索引鍵和值為：

金鑰	值
使用者	若使用 iReg，user 即已在使用者名稱欄位中輸入的使用者電子郵件地址。 此為必要項目。
密碼	使用者的密碼
pin	使用者的註冊 PIN 碼
quickStart	**設為 TRUE 時：**登入過程畫面會快速顯示。 在「歡迎使用」畫面中，當微調按鈕變更為「繼續」按鈕時，不需點選「繼續」，畫面也會自動繼續。 此外，此簡化的供應流發生在所有設備： • 對於用戶的私密性和快捷的提示被跳過。 • 在 Zebra 設備，客戶應授予管理權限本身沒有用戶提示。 需要的最低版本 Zebra MX 4.3。 **設為 FALSE 時：**登入過程畫面會照常顯示，且使用者必須在「歡迎使用」畫面中點選「繼續」。 選用項目，預設值為 FALSE。

> 若要使用大量註冊，就必須使用密碼、PIN 碼或權杖。

此範例命令指定了伺服器、使用者、密碼、PIN 碼及快速啟動：

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

大量註冊範例指令碼

設計自己的大量註冊指令碼時，您可以將這個指令碼做為範例來使用。 此範例指令碼可使用相同的使用者和密碼來註冊所有附接至佈建機器的裝置。

```
for i in `adb devices | grep -v devices |
do
  回應「註冊 $i」
  adb -s $i shell "am start -a android.intent.action.MAIN -d \"mirp://<servername?user=user email addresspassword=password
done
```

可能的錯誤訊息

下列為使用大量註冊時可能發生的錯誤訊息:

錯誤	解決方式
找不到 mirp 架構	使用 mirp 架構的範例命令：am start -a android.intent.action.MAIN -d "xxxmirp://?
URL 無效	如果未傳送任何資料字串時會出現此錯誤。 確認 URL 正確。
找不到伺服器資訊	遺漏伺服器資訊或輸入有誤。
找不到使用者資訊	請確認已輸入 user 索引鍵。
找不到密碼/PIN 碼資訊	請確認已輸入 pin 或 password 索引鍵。

當為大量註冊建立多個設定檔時:

- 以原生方式註冊的完全受控 Android Enterprise 裝置會接收使用第一個設定檔建立的自訂屬性。
- 遷移裝置時，如果裝置存在於大量註冊設定檔中，則大量註冊設定檔中為遷移裝置定義的自訂屬性將套用至遷移時的裝置。 對於遷移的完全受控 Android Enterprise 裝置，此行為相同，因為它會接收第一個設定檔的自訂屬性。

此外，為該特定裝置所建立的所有設定檔都會被視為作用中。

7.5.15. 使用 CSV 檔案上傳進行大量註冊

大量註冊可讓您使用裝置識別碼來註冊多個 Android 裝置。 您可以上傳 CSV 檔案以新增大量裝置。

程序

1. 在**裝置**頁面中，按一下**大量註冊**索引標籤。 **大量註冊**頁面隨即顯示。
2. 按一下**新增**。
3. 在**設定檔名稱**文字欄位中輸入設定檔的名稱。 您可選擇按一下 **+新增描述**以提供 CSV 檔案的描述。
4. 在**上傳 CSV** 區段中，按一下**下載 CSV 範本**來下載 CSV 範本。 您可使用現有格式進行檔案編輯以新增裝置。

> 在大量註冊 CSV 檔案中，一次允許最多 200,000 列。

5. 編輯與儲存 CSV 檔之後，按一下**上傳 CSV** 以上傳 CSV 檔。 隨即顯示上傳成功的確認訊息。

> 資訊不足的資料列可能會導致 CSV 上傳失敗。 每筆記錄均應至少包含序號與製造商資訊，或是 IMEI 值。

> 若要移除已新增的 CSV 檔，請按一下「減號」圖示。 若要選擇上傳不同的 CSV 檔，請按一下**選擇不同檔案**連結。

6. 選用：選擇**在無權杖的情況下指派自訂屬性**，以在不產生權杖的情況下，大量註冊所有類型的裝置。 此選項預設為不選取。

當上傳的 CSV 檔中提供 IMEI 或序號以及製造商的組合 (含或不含自訂屬性) 時，也可套用無權杖的大量註冊。 但是裝置的註冊則取決於 CSV 檔中所上傳屬性值的正確性。 下表依據針對大量註冊所輸入的屬性值組合，說明有關所得結果的案例：

案例	輸入的屬性值			裝置註冊狀態
	IMEI	**序號**	**製造商**	
1	正確	不正確	不正確	裝置已註冊
2	不正確	正確	正確	裝置已註冊
3	不正確	不正確	正確	裝置未註冊
4	不正確	正確	不正確	裝置未註冊

> 製造商名稱不區分大小寫。

7. 在**選擇使用者**欄位中，您必須選取一個使用者。
   註冊權杖會顯示在「註冊權杖」欄位中。 若要重新整理註冊權杖，按一下**重新整理**。
   權杖的到期日會顯示在**權杖到期時間**區段中。 若要延長權杖期限，按一下**延長**。 在**最多延長到**欄位中，輸入權杖的延長天數。

> 指定天數應在 7 到 999 的範圍內。 預設權杖在 7 天後到期。
> 如果選取了**在無權杖的情況下指派自訂屬性**選項，將不會顯示此頁面。

8. 按一下**完成**。

完成上傳後，所上傳 CSV 檔案的下列詳細資料將在**大量註冊設定檔**頁面中以表格形式顯示。

設定	描述
設定檔名稱	設定檔的名稱。
描述	關於設定檔的一些描述。
上次修改日期	上次在 CSV 檔案中完成修改的日期。
類型	對於自維護的描述檔 → 自維護
裝置數目	大量註冊中的裝置數目。
關聯使用者	相關使用者的名稱。
使用者名稱	指定與裝置關聯的使用者。 啟用裝置至使用者對應時需要。 使用者必須存在於 Ivanti Neurons for MDM 中。
動作	您可以執行下列其中任何一項動作： **下載現有的詳細目錄** - 按一下此按鈕以下載設定檔中所有裝置的詳細資料。 **檢視** - 按一下此連結可檢視為註冊大量上傳的設定檔詳細資料。 **編輯** - 按一下此按鈕以編輯設定檔詳細資料。 只有在選取單一裝置選項後才能使用此選項。 **刪除** – 按一下此連結可刪除設定檔。 在確認視窗中，按一下**是**可確認刪除所上傳的設定檔。

上傳 CSV 時所產生的權杖應該用於註冊。 若輸入錯誤權杖，系統將重新導向應輸入 ID/密碼的正規 IReg 流程。

動作

當您在「檢視設定檔」詳細資訊區段中檢視「大量註冊」時，可在「檢視設定檔」詳細資訊頁面中顯示的「動作」索引標籤中執行其他工作。

- **新增更多裝置** - 使用此選項將更多裝置新增至設定檔。 您需要提供 **IMEI 號碼**和/或**序號**、**製造商**以及可選的**自訂屬性**資訊，然後按一下**儲存**。
- **修改組態** - 使用此選項來修改現有組態。 您可以新增 **Ivanti 特定金鑰**、對**預先定義的 Android 系統附加功能**或是**自訂的 Android 系統金鑰**進行變更，然後按一下**更新**。
- **產生 QR 碼** - 使用此選項為設定檔的大量註冊產生 QR 碼。
- **重新整理權杖** - 使用此選項以重新整理權杖或延長權杖的有效期間。 有效期限可以設定在 7 到 999 天的範圍內，也可以設定為**永不過期**。
- **更改關聯使用者** - 使用此選項更改關聯使用者。 您需要從**更改關聯使用者**快顯視窗中搜尋並選取使用者，然後按一下**套用**。
- **編輯** - 使用此選項以編輯所選設定檔中的裝置。 您將需要選取裝置並按一下**編輯**按鈕。
- **刪除** - 使用此選項以刪除所選設定檔中的裝置。 在選取裝置並按一下「刪除」按鈕後，畫面上就會顯示一個確認快顯視窗。 按一下**刪除**。

自維護裝置具有不同的裝置狀態。 您可以在使用 Samsung Knox Mobile Enrollment找到更多詳細資訊。

7.5.16. Device_to_User_BulkEnrollment

File not found!

7.5.17. 使用 Samsung Knox Mobile Enrollment

Samsung Knox Mobile Enrollment 使管理員能夠將合格的 Samsung 裝置註冊到 Ivanti Neurons for MDM。 使用 Knox Mobile Enrollment，裝置可以直接從經核准的經銷商運送給終端用戶，Go Android 用戶端將自動下載並預先填充註冊資料。 如需詳細資訊，請參閱**適用於 Android Enterprise 的 Samsung Knox Mobile Enrollment**。

需求

- 依 IMEI 的裝置清單
- CSV 檔，其中包含有 IMEI 或序號的裝置清單，以及選填的使用者名稱和註冊密碼。
- Ivanti Neurons for MDM (目前版本)。
- Samsung Knox 帳戶獲准用於行動裝置註冊
- Samsung 支援裝置。 **此處**提供 Samsung 支援裝置清單。

7.5.18. 註冊 Oculus 裝置

Ivanti Neurons for MDM 現在可以管理 Quest for Business 裝置 (Oculus 裝置)。 目前 Meta 支援在 Oculus for Business (OFB) 和 Quest for Business (QFB) 裝置上使用 MDM。 您需要在 Meta 控制台上執行一些基本工作，讓裝置為使用 MDM 做好準備，然後註冊 Ivanti Neurons for MDM。

您可以在 Meta Workplace 控制台下的「裝置管理員」中註冊 Oculus 裝置機群。 您必須使用註冊電子郵件中共享的認證來登入 Oculus Business Workplace。 在首頁上，所有的裝置資訊將會在「裝置機群」區段下顯示。 「裝置機群」區段提供「裝置管理」底下所有可用裝置的概觀。 這些詳細資料包括「裝置名稱」、「裝置狀態」、「OS (作業系統)」、「型號」等等。

本節包含以下各主題：

- 註冊 Oculus 裝置的必要條件
  - 在裝置管理員內設定 MDM 應用程式
  - 設定 Oculus 裝置

使用 MobileIron Go 註冊 OFB 裝置

  - 在 Ivanti Neurons for MDM 控制台上
  - 在 Go 用戶端上

註冊 Oculus 裝置的必要條件

在裝置管理員內設定 MDM 應用程式

裝置/頭戴式裝置均已佈建且已至少更新到 **Oculus for Business v28** 版本。 在 Meta 控制台上，管理員必須在裝置管理員內設定 MDM，並將 Oculus 裝置對應到此特定 MDM 服務。

程序

1. 在 **Oculus Business Workplace** 首頁上，選取**應用程式**。
2. 在**應用程式庫**內，按一下您要安裝的第三方 MDM 應用程式，接著按一下**更新**。
3. 在**行動裝置管理**下的清單中為應用程式選取適當的 MDM，然後按一下**更新應用程式**。
4. 按一下您想安裝 MDM 的 Oculus 頭戴式裝置。 畫面上將會顯示裝置資訊。
5. 在**關於**索引標籤下，向下捲動至**行動裝置管理員**。
6. 按一下 **MDM 授權單位**選項旁的**編輯**按鈕。

> 依預設，將會選取「Oculus 裝置管理員」選項。 您需要選取 MDM 授權單位應用程式，然後從 MDM 授權單位應用程式清單中選取 **MobileIron Go**。

按一下**儲存**。 裝置會自動重設，接著您需要使用設定應用程式來設定 Oculus 裝置。

設定 Oculus 裝置

您可以使用 Device Setup 應用程式來新增 Oculus Quest 2 頭戴式裝置。 此應用程式必須與需要的使用者分享，以便這些使用者能在其 Android 裝置上下載並安裝該應用程式。

程序

1. 在**裝置機群**區段下，按一下**未設定的裝置**。
2. 按一下**取得設定應用程式**。 畫面上將會出現**傳送下載連結**頁面。
3. 從清單中選取一個或多個團隊成員，或是按一下**新增收件者**以從清單中選取。
4. 按一下**傳送連結**。 選取的使用者將會收到一封電子郵件，其中包含可安裝 **Device Setup** 應用程式的連結。
5. 按一下電子郵件內的**下載 Device Setup 應用程式**連結，將 **Device Setup 應用程式**安裝在您的 Android 裝置上。

> 下載完成後，該應用程式並不會出現在您裝置上的應用程式商店中。 您需要在裝置的「下載」區段中找到該應用程式並進行安裝。

開啟您 Android 裝置上的 **Oculus for Business** 應用程式。

7. 按住電源按鈕 2 秒，啟動 Oculus 裝置電源。
8. 開啟藍牙，並將您的 Android 裝置放置在 Oculus 裝置鄰近處，直到設定完成。
9. 使用您 Android 裝置的藍牙搜尋 Oculus 裝置。
10. 一旦找到需要的 Oculus 裝置，您需要將其連線至 Wi-Fi 網路以完成設定。
11. 按一下**輸入 Wi-Fi 資訊**並提供網路名稱及密碼，然後按一下**儲存**。 現在 Oculus 裝置已連線至 Wi-Fi 網路。
12. 按一下**開始設定**。 畫面上會顯示通知，說明設定正在進行中，而且在設定期間您不應關閉應用程式或操作頭戴式裝置。
    畫面上會出現確認訊息。 您可以使用**尋找更多裝置**按鈕繼續搜尋更多裝置。

使用 MobileIron Go 註冊 OFB 裝置

在 Ivanti Neurons for MDM 控制台上

可使用 MobileIron Go 在 Ivanti Neurons for the MDM 控制台上註冊 OFB 裝置。 不過，必須將工作受控裝置非 GMS 模式 (AOSP) 組態 (在**組態**下) 發佈至這些 OFB 裝置群組。

在 Go 用戶端上

OFB 裝置可以在 MobileIron Go 用戶端上註冊。 您必須執行下列工作才能註冊 OFB 裝置:

- 在使用 OFB 設定應用程式完成設定後，請繼續依照 OFB 頭戴式裝置畫面上的指示，完成裝置設定。
- MobileIron Go 應用程式會自動啟動，而您需要提供登入認證並依照 MDM 指示來完成註冊。

現在裝置已在 DO 模式下完成佈建，並設定為由 MDM 管理。

7.5.19. 在裝置上啟用 Bluetooth

適用於：

- iOS 11.3+
- macOS 10.13.4+

您可以在裝置上啟用或停用 Bluetooth。

程序

1. 在**裝置頁面**中，導覽到裝置。
2. 執行下列其中一個動作：
    - 從清單中選擇裝置。
    - 按一下裝置名稱，以顯示裝置詳細資料頁面。
3. 按一下**動作**功能表，然後按一下**啟用/停用 Bluetooth**。
4. 按一下**確定**。

變更將會在裝置下次進行登記時推送到裝置上。

7.5.20. 排程 iOS 更新

適用於：

- iOS 9.0+ 受監管的 Device Enrollment 裝置
- iOS 10.3+ 受監管的裝置。

將 iOS 裝置更新排程在有最新的 iOS 版本可用時進行更新。 受監管 iOS 裝置的**裝置** > **動作**功能表選項**更新作業系統版本**只會顯示適用於該裝置的 iOS 版本清單。

程序

1. 在**裝置頁面**中，導覽到裝置。
2. 按一下裝置名稱，以顯示裝置詳細資料頁面。
3. 從**動作**功能表，按一下**更新作業系統版本**。
4. 在**更新作業系統版本**精靈中，檢閱 iOS 版本並在**更新至版本**下拉式清單中選取作業系統版本。

> 若您輸入相同或較舊的版本，則會顯示錯誤訊息以指出目標 iOS 版本應高於目前版本。

5. 按一下**更新**。

裝置簽入時，iOS 裝置會排程更新至可用的最新 iOS 版本。 如果裝置設有密碼，在 MDM 傳送更新至裝置後，裝置會排定更新佇列，系統則會提示使用者輸入密碼以開始安裝。 如需更多資訊，請參閱**軟體更新**。

7.5.21. 重新安裝 iOS 系統 App

適用於：

- iOS 11.3+ 裝置。

在 iOS 裝置上重新安裝已刪除的 iOS 系統 app。

程序

1. 導覽至**裝置頁面**。 或者，您可以按一下裝置的名稱，然後從「裝置詳細資料」頁面執行此動作。
2. 選擇一或多台 iOS 裝置。
3. 從**動作**功能表按一下**重新安裝 iOS 系統 App**。
4. 在「重新安裝 iOS 系統 App」顯示方塊中，選擇要在裝置上安裝的一或多個可用系統 app。
5. 按一下**重新安裝 App**。

當裝置簽入時，這些應用程式將安裝在所選且相容的 iOS 裝置上。 以此方式安裝的系統應用程式將不被視為受管理的應用程式。 如果所選擇的裝置中沒有任何相容裝置，您會收到系統 app 將不會安裝在那些裝置上的訊息。

如需更多資訊，請參閱**軟體更新**。

7.5.22. 指派裝置給新使用者

當出現新的使用者，或現有註冊裝置的上一個使用者與公司的關係改變時，都必須重新設置此裝置。 下列步驟有助避免淘汰與重新註冊裝置的程序：

程序：

1. 在**裝置頁面**中，導覽到裝置。
2. 按一下裝置名稱，以顯示裝置詳細資料頁面。
3. 按一下**指派給使用者**  圖示。

> 或者，您可以從**裝置**頁面選取一部裝置，然後從**動作**功能表中按一下**指派給使用者**選項。

在**搜尋使用者...** 中開始輸入使用者名稱 欄位。

5. 選擇所需的使用者。
6. 按一下**指派給使用者**。
   隨即將此裝置設置給該名使用者。

> 您可能會發現，在以使用者為基礎和以授權為基礎的案例中，您可指派裝置給已超出指派裝置限制的使用者。 這是因為裝置限制功能的本意是，在支援自攜裝置 (BYOD) 案例中限制裝置註冊。

而在以裝置為基礎和以使用者為基礎的授權中，強制執行裝置限制是不合邏輯的。 若是以裝置為基礎的授權，客戶成本不會變更，因為系統當中的裝置總數不會變更。 若是以使用者為基礎的授權，缺乏此檢查其實反而對客戶有利。 例如，假設有五位使用者 U1 到 U5，5 個裝置一人一台。 若是以使用者為基礎的授權，這會使用五個授權。 如果將 U4 和 U5 的兩台裝置分別移給 U1 和 U2，這樣授權使用數目反而會從五個「減少」成三個。

7.5.23. 重新指派 Android 裝置

管理員可以將 Android 裝置的擁有權從一個使用者轉讓給其他使用者。 在重新指派程序中，裝置的管理設定檔將在 Android Enterprise 模式中得到重新設定，或從目前使用者重新對應到新使用者。 重新指派可以在除了 Android Management API (AMAPI) 裝置之外的所有 Android Enterprise 裝置上完成，但不能在 Google Domain Android Enterprise 裝置上完成。

> 裝置重新指派只能在處於相同模式的裝置之間完成。 例如，可以將處於工作受控裝置模式的裝置重新指派給同一模式下的其他使用者。

裝置重新指派程序具有以下狀態:

- 已起始
- 成功
- 失敗
- 擱置中

您可以在**裝置詳細資訊**頁面 → **概觀**索引標籤 > **上次重新指派狀態**下方查看裝置上次重新指派的狀態。

程序

1. 前往**裝置**。
2. 從清單中選取一部或多部裝置。
3. 從**動作**清單中，按一下**指派給使用者**。
4. 或者，您可以按一下任何裝置名稱。 此時將開啟**裝置詳細資訊**頁面。 按一下**指派給使用者**圖示進入「指派給使用者」畫面，並選取所需的使用者。
5. 按一下**指派給使用者**。 將驗證所選的選項，以確認是否可以將所選裝置重新指派給所選的使用者。
   成功驗證和重新指派後，螢幕上將顯示確認訊息。

> 如果您選取了上限 10 部裝置，螢幕上會顯示「指派已起始」的訊息。 如果您選取了 11 部或更多部裝置，螢幕上會出現「驗證進行中」的彈出視窗。

> Android 裝置重新指派是一套創新解決方案，專為消除先前註冊使用者遺留的資料而建立，僅在 SUEM-Premium SKU 中提供使用。

7.5.24. 強制裝置登記

裝置需要聯絡 Ivanti Neurons for MDM (簽入) 以提供與接收資訊。 系統會在固定間隔的排程時進行登記。 您也可以提示裝置隨選即用進行登記。 強制裝置登記可加速套用{{配置}}的程序、更新{{原則}}等等。

程序

1. 前往**裝置 > 裝置**。
2. 選擇裝置。
3. 按一下**動作**。
4. 選擇**強制登記**。
5. 或者，按一下裝置名稱連結，以前往「裝置詳細資料」頁面，然後按一下**強制登記**  圖示然後按一下**確定**。

如果在簽入期間處理組態安裝命令時發生裝置故障，在稍後自動簽入時，Ivanti Neurons for MDM 將不會重新嘗試將組態安裝至裝置。 管理員需要從裝置的裝置詳細資料頁面手動重新嘗試安裝配置。 若要執行此動作，請前往「配置」索引標籤，選擇發生錯誤的配置，然後按一下**重試安裝**。

7.5.25. 定位裝置

如果您已啟用裝置的「定位」功能，即可顯示該裝置的上一次已知位置。 您必須編輯**隱私權配置**，啟用位置資料的收集，並將此配置套用到裝置以啟用這項功能。 此外，裝置必須支援這項功能，使用者也必須同意共享他們的位置資料。

程序

1. 在**裝置 頁面中，導覽到裝置**。
2. 按一下**名稱**欄位中的連結。
3. 在**概覽**索引標籤中，按一下**裝置位置**下方的連結。

頁面上隨即顯示下列詳細資料：

欄位名稱	描述
上一次定位時間	顯示裝置上一次定位的日期和時間。
座標	顯示裝置的緯度 (南北緯) 和經度 (東西經)。

您也可以在頁面中找到裝置位置的地圖。

7.5.26. 鎖定裝置

您可以觸發裝置的螢幕鎖定。 不同裝置的鎖定方式也略有不同。

程序

1. 前往**裝置 > 裝置**。
2. 選擇裝置。
3. 按一下**動作**。
4. 選擇**鎖定**。
5. 或是按一下裝置名稱連結，前往「裝置詳細資訊」頁面，接著依序按一下**鎖定**  圖示、**確定**。
6. 對於 AppConnect Android 應用程式，「鎖定」指令會將使用者鎖定在容器之外，也會鎖定裝置。 使用者可以分別使用裝置密碼和 AppConnect 密碼重新登入裝置和 AppConnect 應用程式。
7. 若是 iOS 7 裝置，您可以輸入顯示訊息與電話號碼 (選用)。
   這些選項可提供裝置使用者為何裝置受到鎖定，以及要解除鎖定的聯絡電話號碼等相關資訊。
8. 若是 macOS 裝置，系統會提示使用者輸入 6 位數 PIN 碼以做為存取裝置的密碼。 要繼續進行螢幕鎖定，裝置使用者需要:
   1. 輸入 PIN 碼。
   2. 選擇確認鎖定裝置的核取方塊。
   3. 按一下**是，傳送鎖定命令**。

> 在 macOS，在裝置鎖定密碼設定期間，使用者可以新增選用的鎖定畫面訊息和電話號碼。

9. 針對 ChromeOS 裝置，當您執行鎖定操作時，畫面上會出現快顯視窗，說明「若鎖定裝置，可能會需要使用者輸入密碼才能存取該裝置。」。 按一下**鎖定**，裝置狀態將更新為**已傳送停用**，而更新後的裝置狀態將於定期裝置同步後可見。

鎖定裝置的其他方法：

- 裝置使用者可以透過自助式入口網站來執行鎖定動作。
- 管理員可以透過管理員入口網站來執行鎖定動作。

7.5.27. 管理遺失模式下的 Apple 裝置

本節包含以下各主題：

- 啟用遺失模式
- 執行遺失模式動作
- 停用遺失模式

適用於：iOS 10.3+ 受監管的裝置

可以透過 Ivanti Neurons for MDM 將受監管的裝置設為遺失模式。 這麼做等於向 Apple 伺服器回報裝置遺失，同時可讓您擷取最後一次的裝置記錄位置，並在尋回裝置時停用遺失模式。

啟用遺失模式

您可以將裝置設為遺失模式，以向 Apple 伺服器回報裝置遺失。 將裝置設為遺失模式之後：

- 如果裝置已淘汰，就無法停用遺失模式。
- 如果裝置已抹除，就無法定位或追蹤裝置。

程序

1. 前往**裝置**。
2. 選擇所要裝置的勾選方塊。
3. 選取**動作** > **通用** > **啟用遺失模式**。
4. 或者，透過選取裝置名稱連結，導覽至**裝置詳細資訊**頁面。 按一下裝置的動作圖示，然後選取**啟用遺失模式**。

執行遺失模式動作

啟用遺失模式之後，您即可從「遺失裝置模式」區段中執行下列動作：

- 推播訊息/電話號碼至 iPhone
  - 輸入要顯示在遺失裝置鎖定畫面上的訊息。
  - 輸入要顯示在遺失裝置鎖定畫面上的聯絡人號碼。 如果有人找到裝置，就可以撥打號碼來回報。

鎖定裝置

- **重新整理裝置位置**

> 如果裝置已抹除，就無法定位裝置。

- **播放遺失模式音效**

> 音效會一直播放到裝置從遺失模式移除，或使用者停用裝置的音效為止。

- **重新整理位置**
  重新整理位置選項已新增到**遺失模式**以檢視裝置位置。 顯示下列詳細資訊:
  - **緯度**: 裝置位置的緯度。
  - **時間戳記**: 顯示承載的時間和日期時間戳記。

- **經度**: 裝置位置的經度。

停用遺失模式

如果您擷取到處於遺失模式的裝置，或遺失模式啟用時發生錯誤，即可停用遺失模式。

> 如果遺失裝置已被 Ivanti Neurons for MDM 淘汰，停用遺失模式將不會正常運作。

程序

1. 前往**裝置**。
2. 選擇所要裝置的勾選方塊。
3. 選取**動作** > **通用** > **停用遺失模式**。
4. 或者，選取裝置名稱連結，導覽至**裝置詳細資訊**頁面，然後選取**遺失裝置模式: 已啟用** > **停用遺失模式**。

7.5.28. 管理遺失模式下的 Android 裝置

本節包含以下各主題：

- 啟用遺失模式
- 停用遺失模式

啟用遺失模式

適用於: Android 8+ 裝置

您可以透過 Ivanti Neurons for MDM 同時將多部 Android 裝置設為遺失模式。 這表示，您可以透過將裝置設為遺失模式來向 Ivanti Neurons for MDM 回報遺失的裝置，這樣做可讓您在畫面上顯示自訂訊息、電話號碼和註腳，並且可選擇播放音效。

> 此功能僅支援完全受控裝置，包括非 GMS 裝置在內。

程序

1. 前往**裝置**。
2. 選取裝置的核取方塊。
3. 選取**動作 > 啟用遺失模式**。
4. 或是按一下裝置名稱連結，前往「裝置詳細資訊」頁面，然後按一下 ⋮ 圖示。 選取**啟用遺失模式**。
5. 輸入要在遺失裝置的鎖定畫面上顯示的鎖定畫面訊息或電話號碼，也可以兩者都顯示。 管理員也可以選取註腳和**播放遺失模式音效**選項。若有人找到裝置，可撥打電話號碼來回報。

> 訊息或電話號碼必須分別輸入不同的欄位中，才能啟動**啟用遺失模式**選項。

> 遺失模式音效將持續播放 5 分鐘，除非在這段時間內手機解鎖、按下通話按鈕，或管理員停用遺失模式。 若要重播音效，請在裝置上重新啟用遺失模式。

6. 選取**啟用遺失模式**會將 Android 裝置設為遺失模式。

啟用遺失模式會停用下列動作:

- 取消鎖定
- 進入/結束 Kiosk
- 強制登出共用的 Kiosk
- 指派給使用者
- 傳送訊息
- 設定擁有權

> 在裝置上啟用遺失模式後，會停用伺服器上的遺失模式選項。

停用遺失模式

若找回了處於遺失模式的裝置，或誤啟用遺失模式，您可以停用遺失模式。

如果遺失裝置已被 Ivanti Neurons for MDM 抹除，則無法停用遺失模式。

程序

1. 前往**裝置**。
2. 選取裝置的核取方塊。
3. 選取**動作 > 停用遺失模式**。
4. 或是按一下裝置名稱連結，前往「裝置詳細資訊」頁面，接著選取**遺失裝置模式: 已啟用 > 停用遺失模式**。

在**詳細資訊**區段中，**停用遺失模式**只有在**啟用遺失模式**啟用後才會顯示。 一旦啟用了**停用遺失模式**，包括**停用遺失模式**選項的**遺失裝置模式: 已啟用**欄位就會消失。

停用遺失模式後，先前處於 Kiosk 模式的裝置需要重新進入 Kiosk 模式。

7.5.29. 要求偵錯日誌

您可以傳送要求給受工作管理的 iOS、macOS 和 Android 裝置，以擷取疑難排解裝置問題所需的偵錯日誌。 使用裝置頁面中的「要求偵錯日誌」指令，會在偵錯日誌中擷取動作以及事件成功或失敗。

此功能需要以下用戶端：

- iOS 裝置需要安裝 Go 5.3.0 for iOS 或支援的更新版本。 對於從 Ivanti EPMM 移轉到 Ivanti Neurons for MDM 的裝置，此功能需要 iOS 版 Mobile@Work 12.2.0 或受支援的更新版本。
- macOS 裝置需要安裝 Mobile@Work 1.5 for macOS 或支援的更新版本。
- Android 工作受控裝置需要適用於 Android 的 Go 65 或受支援的更新版本。

程序

1. 前往**裝置 > 裝置**。
2. 選擇裝置並按一下裝置名稱連結，以前往「裝置詳細資料」頁面。
3. 按一下 ⋮ 圖示。
4. 選擇**要求偵錯日誌**，並按一下**確定**。

當已傳送要求且裝置備妥日誌時，就會傳送一則通知給管理員，並將通知顯示在裝置日誌中。 您也可以按一下連結，以下載裝置日誌。

7.5.30. Apple_Enhanced_Logging

File not found!

7.5.31. 淘汰裝置

如果淘汰裝置，則會結束該裝置與 Ivanti Neurons for MDM 的關係。 在下列情況下，您可以淘汰裝置：

- 使用者已離開公司
- 使用者已更換裝置
- 您需要取消已完成的管理作業 (重頭開始)

程序

1. 前往**裝置 > 裝置**。
2. 選擇裝置。
3. 按一下**動作** (右上角)。
4. 選擇**淘汰**。
5. 或者，按一下裝置名稱連結，以前往「裝置詳細資料」頁面，然後按一下 ⋮ 圖示。
6. 選擇**淘汰**，然後按一下**確定**。

> 在處於「使用中」狀態的裝置上執行停用操作時，該裝置將立即停用。

7.5.32. 放棄裝置擁有權

適用於在公司擁有的裝置上的工作描述檔模式中的 Android 裝置。

在「公司擁有裝置上的工作設定檔」模式下放棄裝置擁有權會移除工作設定檔，並從 Ivanti Neurons for MDM 淘汰該裝置，但不會影響個人應用程式和資料。 然後使用者就可將該裝置當成個人裝置使用，可完整存取所有裝置控制和設定。

> 需要從 Google Zero Touch 或 Knox 行動註冊入口網站將裝置移除。

在以下情況中，您可以透過放棄裝置擁有權:

- 使用者已離開公司
- 使用者已更換裝置

程序

1. 前往**裝置 > 裝置**。
2. 選擇裝置。
3. 按一下**裝置詳細資料頁面**，然後按一下 ⋮ 圖示。
4. 選取、**放棄擁有權**。

7.5.33. 清除裝置

清除裝置將會移除所有資料，並將裝置回復為原廠預設值。

程序

1. 前往**裝置 > 裝置**。
2. 選擇裝置。
3. 按一下**動作** (右上角)。
4. 選擇**抹除**。
5. 或者，按在一下裝置名稱連結，以前往「裝置詳細資料」頁面，然後按一下 ⋮ 圖示。 選擇**清除**，然後按一下**確定**。
6. 依預設，會選取**保留資料方案**選項。
   (選用，適用於 iOS 11.3+ 裝置) 選擇**略過近接設定**選項。
7. 選取**返回服務**選項可在擦除資料後自動重新註冊，這樣您就不必在擦除後手動重新註冊裝置。 僅適用於在 DEP 模式下註冊的 iOS 17+ 裝置。
   1. 從下拉選單選取 **Wi-Fi 組態**。 使用者需要停用所有啟用鎖定。 僅適用於在 DEP 模式下註冊的 iOS 17+ 裝置。
   2. (選用) 如果您希望裝置在保留現有應用程式的情況下恢復服務，請選取**保留應用程式**選項。 只有使用 Ivanti N-MDM 安裝的具有高優先順序的應用程式才會被保留。 僅適用於 iOS 26+ 裝置。
8. 若是 macOS 裝置，您可以傳送 6 位數 PIN 碼至裝置以做為密碼。 使用者會在裝置上，收到輸入 PIN 碼以存取裝置的提示。 若要繼續清除動作，裝置使用者必須：
   1. 輸入 PIN 碼。
   2. 選擇核取方塊以確認裝置抹除動作。
   3. 按一下**是，清除此裝置**。
9. 針對 ChromeOS 裝置，當您從**裝置詳細資訊**或**裝置列出**頁面執行抹除操作時，畫面上會出現快顯視窗，說明「抹除裝置將使裝置回到原廠設定，這樣會造成裝置上的資料遺失。 抹除動作會依平台而有所不同」。
   1. 選取「本人瞭解抹除操作無法復原」核取方塊以確認裝置抹除動作。
   2. 按一下**抹除**以抹除裝置。

裝置狀態會變更為「**已傳送抹除**」。更新後的裝置狀態將於定期裝置同步後可見。

在 Android Enterprise 裝置上，即使在裝置重新開機並維持鎖定後，仍可執行**抹除**裝置操作。

您可以使用**裝置詳細資訊**頁面中的**刪除裝置**選項來刪除處於**抹除擱置**狀態的 Android 裝置。 在刪除裝置後，它會失去與伺服器的連線而變成不合規狀態。 因此使用者在執行原廠重設後必須重新註冊裝置。

7.5.34. 刪除裝置

淘汰裝置之後，您即可將其刪除。 刪除裝置後，即會將其從所有頁面中移除。 您只能刪除狀態為「已淘汰」、「待淘汰」、「已抹除」或「待抹除」的裝置。

程序

1. 前往**裝置 > 裝置**。 畫面上將會顯示裝置清單。
2. 選取您要刪除的裝置。
3. 按一下**動作**。
4. 在**通用**區段下，選取**刪除裝置**選項。 畫面上將會出現一個快顯視窗。
5. 選取「本人瞭解刪除操作無法復原」選項，然後按一下**刪除裝置**。
6. 或者，您可以遵循下列步驟，刪除裝置:
   - 前往**裝置** > **裝置**。
   - 按一下**使用者顯示名稱**欄下的任何連結。 畫面上將會出現**裝置詳細資訊**頁面。 按一下**裝置詳細資訊**。 畫面上將會出現一個快顯視窗，如果您確認此警告並按一下**確定**，特定裝置將遭到刪除。

刪除多部裝置

您可以選取您要刪除的所有裝置來刪除多部裝置。

程序

1. 前往**裝置 > 裝置**。
2. 從可用裝置清單中選取裝置。
3. 按一下**動作**索引標籤，然後在**通用**標題下選取**刪除裝置**選項。
4. 在**刪除裝置**視窗:
   1. 選取**本人瞭解刪除操作無法復原**核取方塊。
   2. 按一下**刪除有效的裝置**以刪除選取的裝置。

7.5.35. 解除鎖定裝置

本節包含以下各主題：

- 解除鎖定 Android 裝置
- 解鎖 AppConnect for Android app
- 解除鎖定 iOS 裝置
- 解除鎖定 ChromeOS 裝置

若要解除鎖定裝置：

您可以清除裝置的螢幕鎖定。 不同裝置的解除鎖定方式也略有不同。

程序

1. 前往**裝置 > 裝置**。
2. 選擇裝置。
3. 按一下**動作**。
4. 選擇**取消鎖定**。
5. 或是按一下裝置名稱連結，前往「裝置詳細資訊」頁面，接著依序按一下**解除鎖定**  圖示、**確定**。

解除鎖定 Android 裝置

收到解鎖指令時，Android 應用程式會嘗試重設密碼。 在「裝置管理員」和「裝置擁有者」模式下，解鎖代碼會重設，而在「設定檔擁有者」和「公司擁有個人啟用」模式下，工作設定檔解鎖代碼會重設。

解鎖指令為管理員提供一個選項，可以使用字母數字字元的組合來設定解鎖代碼。 預設選項會將解鎖代碼設定為「0000」，可以在多個裝置上執行。 不過，新選項「Android 的自訂解鎖代碼」一次只能在一台裝置上執行。 字元數量最少應為 6，最多應為 8。 此選項位於**操作**索引標籤下方，以及**裝置詳細資訊**頁面中。 當您從**動作**索引標籤或**裝置詳細資訊**頁面選取「解鎖」選項時，可以看到下面兩個選項。

- 預設
- (僅限 Android) 提供解鎖代碼 - 可以在此區段中提供解鎖代碼，然後按一下**解鎖**。
    - 略過裝置上的密碼重設提示 - 如果已將密碼組態推送至裝置，則選取此項以略過密碼重設。

設定解鎖代碼後，管理員可以在**稽核追蹤**頁面和**裝置記錄**頁面中找到解鎖代碼。

> 直接啟動解鎖僅適用於預設解鎖選項，即「0000」解鎖代碼。 不支援用於直接啟動的自訂解鎖代碼。

解鎖 AppConnect for Android app

若是 AppConnect app，**AppConnect Unlock** 指令可協助解除鎖定因使用者多次使用不正確密碼嘗試登入而遭鎖定的容器。 此解鎖無法解鎖裝置。

解除鎖定 iOS 裝置

收到「解除鎖定」命令時，iOS app 會移除裝置的密碼。 如果密碼配置指明需要新密碼，系統就會提示裝置使用者設定符合密碼配置中所定義之規則的新密碼。 使用者必須在 60 分鐘內完成變更，否則 app 就會強制使用者設定新密碼。

解除鎖定 ChromeOS 裝置

當選取 ChromeOS 裝置並按一下**解除鎖定**選項時，畫面上會出現快顯視窗，說明「解除鎖定可能會清除現有密碼，讓使用者能夠存取該裝置。解除鎖定會依平台而有所不同」。按一下**解除鎖定**，裝置狀態將更新為「已傳送解除鎖定」，而更新後的狀態將於定期裝置同步後可見。

7.5.36. 重新啟動或關閉裝置

本節包含以下各主題：

- 重新啟動裝置
- 關閉裝置

適用於: Android 7.0+ (受管理裝置)、iOS 10.3+ 受監管、tvOS 10.3+ 受監管、macOS 10.13+ 以及 Windows 10+ 裝置。

管理員可以從裝置詳細資訊頁面單獨或從裝置清單頁面批量重啓或關閉 iOS 受監管裝置。

重新啟動裝置

程序

1. 前往**裝置**。
2. 導覽至裝置。
3. 按一下**名稱**欄位中的連結。
4. 按一下**動作**按鈕。
5. 按一下**重新啟動/關閉裝置**。

> 您無法重新啟動不受支援的裝置。

6. 讀取顯示的警告。
7. (選擇性) 選擇此選項，以在重新啟動裝置時清除裝置的密碼。 如果未清除密碼，重新啟動裝置之後，就必須提供密碼，且不會連接 Wi-Fi。
8. 選擇**重新啟動裝置** (如果尚未選擇的話)。
9. 如果您仍想重新啟動裝置，請按一下**傳送至裝置**。 否則，請按一下**取消**。

> 對於 Android 裝置，管理員可在「裝置詳細資訊」頁面的**運作時間**下檢視裝置重新啟動時間的相關資訊。

您可以透過**裝置清單**頁面，重新啟動多台受支援的裝置。 若要進行此作業，請選擇裝置，按一下**動作 > 重新啟動/關閉裝置**，然後遵循畫面上的指示。

關閉裝置

程序

1. 前往**裝置**。
2. 導覽至裝置。
3. 按一下**名稱**欄位中的連結。
4. 按一下**動作**按鈕。
5. 按一下**重新啟動/關閉裝置**。

> 您無法重新啟動不受支援的裝置。

6. 讀取顯示的警告。
7. 選擇**關閉裝置**。
8. 如果您仍想關閉裝置，請按一下**傳送至裝置**。 否則，請按一下**取消**。

您可以透過**裝置清單**頁面，關閉多台受支援的裝置。 若要進行此作業，請選擇裝置，按一下**動作 > 重新啟動/關閉裝置**，然後遵循畫面上的指示。

7.5.37. 清除限制密碼 (僅限 iOS)

您可清除使用者在受監管 iOS 8 裝置上所設的限制密碼。 此動作僅適用於作用中的裝置。

程序

1. 前往「裝置」>「裝置」。
2. 選擇所要的裝置項目。
3. 前往「動作」>「清除限制密碼」。
4. 出現系統提示時，確認動作。

7.5.38. 刪除裝置的 Sentry 關聯

為了使用支援 App Tunneling 或 ActiveSync 的電子郵件系統，來控制裝置的電子郵件存取，需建立裝置的 Sentry 關聯。 如果任何裝置已與 Sentry 建立關聯，您可以依下列方式移除其關聯 (若要必要的話)：

程序

1. 前往**裝置**。
2. 在**名稱**欄位中，按一下要刪除其 Sentry 關聯之裝置的裝置連結。
3. 按一下 **Sentry** 索引標籤。
4. 在**動作**欄上，按一下**刪除**。

7.5.39. 指派自訂屬性給裝置

您可指派自訂裝置屬性給一或多台裝置，例如：內部 ID。 每個屬性都有對應值，在建立配置與建立裝置群組等作業時，可使用這些值。 建立自訂屬性後，即可將其指派給裝置。 如需關於管理屬性的詳細資訊，請參閱**屬性**。

程序

1. 登入管理入口網站。
2. 前往**裝置**。
3. 選擇一或多台裝置。
4. 按一下**動作**。
5. 選擇**指派自訂屬性**。
6. 選取下列其中*一個*選項:
    - 即使有找到任何既有的值，仍要強制指派 (覆寫) 所有屬性。
    - 僅限值為空白時才覆寫，並略過具備現有值的屬性。

選擇您想指派的屬性並輸入值 (不允許空白值)。

8. 按一下**指派**。

> **自訂裝置屬性**及其值可從**裝置詳細資訊**頁匯出為 CSV 格式。

7.5.40. 移除裝置的自訂屬性

請謹慎操作，因為此動不可回復。 若要移除一或多台裝置的自訂屬性：

程序

1. 前往**裝置**。
2. 選擇一或多台裝置。
3. 按一下**動作**。
4. 選擇**移除自訂屬性**。
5. 選擇您要移除的屬性。
6. 按一下**移除**。

7.5.41. 同步並擷取 App 回饋

您可以傳送要求給安裝在 Android 裝置上的 app，以取得 app 其目前 app 配置狀態的詳細資料。 傳送要求後，您會收到裝置的 app 配置回饋報告。

程序

1. 前往**裝置**。
2. 按一下您想傳送要求至其中的裝置。
3. 按一下**動作**。
4. 選擇**同步並擷取 App 回饋**。系統便會傳送要求以同步並擷取 app 配置回饋。 「用戶端上一次登記」欄位旁的「App 回饋上一次同步」欄位將會獲得更新。
5. 在**已安裝的應用程式**索引標籤中，按一下**應用程式意見回應**欄中應用程式的**檢視詳細資料**連結。 **應用程式意見回應**視窗隨即顯示。
   機碼 - 根據從應用程式收到的回饋提供詳細資訊，並提供所報告設定的佈置 (在應用程式的受管理應用程式組態中)。
   時間戳記 - 金鑰的時間和日期。
   嚴重性 - 指定事件的嚴重性。 範例：'Info'、'Error'。
   訊息 - 從 app 配置回饋收到的訊息類型。 範例： 'Failure'。
   資料 - 從 app 配置回饋收到的資料其詳細資料。

從 App Catalog 檢視 app 配置回饋

您可以從 App Catalog 檢視特定 app 的 app 配置回饋。

程序

1. 前往 **App > 應用程式目錄**。
2. 選擇您想要檢視詳細資料的 app。
3. 按一下 **App 配置回饋**索引標籤。 **裝置計數**欄顯示 app 配置回饋報告其每個金鑰的裝置數目 (超鏈結)。
4. 按一下裝置數目超鏈結以檢視裝置的詳細資料。 例如，按一下超鏈結 5，便會顯示 5 個裝置的詳細資料。 系統會針對「金鑰」與「嚴重性」組合顯示下列詳細資料 (顯示於表格上方)：
   電子郵件地址 - 指定使用者名稱。 按一下使用者連結，以導覽至**裝置 > 裝置詳細資料**下的**已安裝的 App** 索引標籤。
   裝置類型 - 指定裝置機型。
   OS - Android OS 版號。
   序號 - 裝置的序號。
   時間戳記 - 上一次進行更新的時間和日期。
   訊息 - 從 app 配置回饋收到的訊息類型。 範例： 'Failure'。
   資料 - 從 app 配置回饋收到的資料其詳細資料。

您可以按一下鈴鐺圖示 (右上角) 或**儀表板 > 通知**頁面，以檢視 Android 裝置的 App 配置回饋錯誤通知。 按一下通知連結導覽至 **App 配置回饋**索引標籤，並檢視 App 回饋報告。

> 當裝置被清除或淘汰時，將會移除並且不會顯示 App 配置回饋報告。 每 24 小時會執行背景工作，清除 7 天之前的資料。

7.5.42. 設定韌體密碼

適用於：macOS 10.13 或支援的更新版本。

管理員可設定或更新 macOS 裝置的韌體 (EFI) 密碼。 韌體密碼可防止 macOS·裝置從裝置使用者選定之啟動磁碟以外的外部或內部儲存裝置開機。 因此，它還能封鎖使用大部分的啟動金鑰組合。

程序：

1. 前往**裝置**。
2. 若要設定或變更單一裝置的韌體密碼。
    1. 按一下裝置的相關聯使用者名稱，以檢視裝置的詳細資料頁面。
    2. 在「一般」區段中，展開**韌體密碼**，然後從裝置「動作」功能表按一下**設定密碼**或按一下**設定/變更韌體密碼**。
    3. 此區段會顯示下列資訊：
        1. **密碼：**密碼或可能密碼清單。

            > 當管理員設定密碼時，命令會傳送到裝置。 如果裝置未及時回應，密碼會暫存並顯示在此欄位中。 在從裝置收到確認且裝置重新啟動之前，新密碼不會生效。 屆時，將會顯示所有的可能密碼。 在裝置重新啟動且密碼變更獲得確認之後，將會清除所有不需要的密碼。

        2. **變更擱置中 -** 指出密碼變更是否為擱置狀態。
        3. **指令狀態 -** 指出密碼變更成功或失敗。
        4. **允許 OptionROM -** 指出是否啟用 OptionROM。 預設為「否」。

若要設定或變更多重裝置的韌體密碼：

1. 選擇裝置。
2. 從「動作」功能表按一下**設定/變更韌體密碼**。

輸入目前的密碼和新密碼。

如果是首次輸入，目前的密碼可以空白。

若要重設密碼，新密碼欄位可以空白。

5. 按一下**儲存**。

> 只有執行受支援 macOS 版本的裝置才會更新為新密碼。 不支援的裝置將會略過。

7.5.43. 重新發行新的個人復原金鑰

適用於：適用於 macOS 1.66 或支援之更新版本的 Mobile@Work 的 macOS 裝置。

從其他 MDM 解決方案移轉至 Ivanti Neurons for MDM 時，如果在註冊之前曾發行過 PRK，管理員可要求作業系統在註冊時重新發行新的個人復原金鑰 (PRK)。 這可讓金鑰儲存在 Ivanti Neurons for MDM。

您可檢視稽核追蹤記錄項目，以查看 PRK 活動如下：

1. 前往**儀表板 > 稽核追蹤**。
2. 在類型篩選器中，選擇**個人修復金鑰**。PRK 項目將顯示在「裝置管理」類別和活動中，例如「已檢視個人修復金鑰」。

必要條件

在執行此程序之前，先將以下配置發佈至裝置：

- 適用於 macOS 的 Mobile@Work 配置。
- FileVault 復原金鑰配置。

程序

1. 聯絡支援中心以要求指令碼在裝置上產生新的 PRK。
2. 以指令碼中使用的名稱「deviceprk」來建立裝置自訂屬性。
3. 將指令碼上傳到**管理 > 指令碼和檔案 > 所有指令碼**中的儲存庫。 在這麼做時，選擇「deviceprk」自訂屬性。
4. 針對未從舊有 MDM 解決方案擷取 PRK 的裝置建立動態的裝置群組。 選擇裝置群組規則如下：「**Platform=macOS**、**Encryption Enabled 等於 Yes**、**macOS Personal Recovery Key escrowed 等於 No** 且 **macOS Recovery Key Type 等於 Personal**」。
5. 建立適用於 macOS 的 Mobile@Work 指令碼配置，您可在其中從儲存庫選擇 PRK 指令碼。 發佈配置至新的裝置群組。
6. 排程指令碼每天執行一次或視需要執行。 此指令碼在每次執行時將會要求輸入使用者密碼。 依預設，指令碼執行的逾時期間為 60 秒。 建議透過將**最大運行時間**欄位設為 300 秒，來延長 macOS 版 Mobile@Work 組態中的逾時期限。

- 您可從裝置的裝置詳細資料頁面中的「裝置加密狀態」區段取得解密金鑰。 按一下「FileVault 加密已啟用」欄位旁邊的**檢視**。
- 取得 PRK 後，裝置會移出裝置群組。 因此，該指令碼配置將不再適用，並將會從裝置刪除。
- 在 MDM 使用指令碼擷取裝置的復原金鑰後，將會從裝置解除安裝此指令碼。

相關主題：

- 屬性
- 所有指令碼
- 裝置群組
- 適用於 macOS 的 Mobile@Work
- FileVault 復原金鑰

7.5.44. 設定或者變更復原鎖定

適用於：macOS 11.5+

系統管理員可針對 Apple 矽 macOS 裝置設定或變更裝置重新開機復原鎖定。 復原鎖定可防止 macOS 裝置在復原模式下啟動，除非已輸入密碼。

程序：

1. 前往**裝置**。
2. 如要設定或變更重新開機復原鎖定：
    1. 按一下裝置顯示名稱的相關聯使用者名稱，以檢視裝置的詳細資料頁面。 執行下列其中一個步驟：
    2. 在**概覽**區段中，展開**復原鎖定**，然後按一下**設定密碼**或按一下**變更密碼**。 或按一下**動作**省略符號，然後按一下**設定/變更復原鎖定**。
    3. 在**設定/變更恢復鎖定**對話方塊中，執行以下操作:
        1. **目前密碼**：在此輸入目前的密碼。 如果您是初次進行設定，請保留空白。
        2. **密碼**：輸入您要設定的密碼。
        3. **確認密碼**：重新輸入您要設定的密碼。

按一下**設定/變更復原鎖定**。

> 在「概覽」中，**已啟用復原鎖定**會顯示復原鎖定密碼的狀態。

> 系統管理員也可以清除密碼，只需移除現有的密碼，然後按一下**設定/變更復原鎖定**即可。

7.5.45. Apple 存取權限管理

先決條件:

- 在 Apple Business Manager 或 Apple School Manager 上驗證並鎖定此網域。
- 從 Apple Business Manager 或 Apple School Manager 組織中設定至少一個 MDM 收發器，其中受管理 Apple ID 存在於 Ivanti Neurons for MDM 中。

登入受管理 Apple ID 允許組織控制使用者可以存取哪些 Apple 服務和功能。

在 Apple Business Manager 或 Apple School Manager 中，**允許受管理 Apple 帳戶的位置**設定控制使用者可以在什麼地方使用其受管理 Apple ID 登入。 管理員可以配置此設定以限制登入受管理或受監管裝置，或允許在任何裝置上登入。

- **任何裝置** (預設): 使用者可以在任何裝置上使用他們的受管理 Apple ID 登入，無論此裝置是否由 MDM 解決方案管理。
- **僅限受管理裝置**: 使用者只能登入由支援取得權杖端點的 MDM 解決方案管理的裝置。
- **僅限受監管裝置**: 使用者只能登入由支援取得權杖端點的 MDM 解決方案監管 (管理) 的裝置。

這些設定是 Apple Business Manager 和 Apple School Manager 中 Apple 服務更廣泛「存取管理」的一部分。

> 透過增強安全性，限制登入受管理或受監管裝置，進而可以透過確保與工作相關的資料只能在受控裝置上存取來提高資料安全性。

如果**裝置註冊**索引標籤中存在零個或多個裝置註冊 MDM 伺服器組織，並且管理員在 Apple Business Manager 或 Apple School Manager 中將**訪問管理** > **Apple服務**下的**允許受管理 Apple 帳戶的位置**設定為「僅限受監管裝置」或「僅限受管理裝置」，則受管理 Apple 帳戶登入將失敗。

> 如果 Ivanti Neurons for MDM 裝置註冊 MDM 伺服器中不存在**受管理 Apple 帳戶**，則裝置將無法登入。

7.5.46. 群組原則註冊

使用群組原則可在 Ivanti Neurons for MDM 中註冊 Windows 10/11 裝置。 建立群組原則將自動註冊所有混合式加入 Azure AD 的裝置。

Procedure使用群組原則註冊裝置

	1. 確保您的裝置已混合式加入 Azure AD。 有關詳細資訊，請參閱 Microsoft 文件: 混合式加入 Azure AD 的裝置。
	2. 建立群組原則物件。 有關詳細資訊，請參閱 Microsoft 文件: 設定裝置群組的自動註冊。
	3. 建立一個包含要註冊的裝置的安全群組。 有關詳細資訊，請參閱 Microsoft 文件: Active Directory 安全群組。
	4. 將群組原則物件連結至安全群組。 有關詳細資訊，請參閱 Microsoft 文件: 將 GPO 連結至網域。

使用者體驗

當使用者使用 Azure AD 中的憑證登入裝置時，Microsoft 會找到屬於其組織的基於 Azure AD 的 MDM 組態。 裝置已在 Ivanti Neurons for MDM 註冊，並且可以接收原則和指令。

8. App

本節包含以下各主題：

- 「App Catalog「
- Apps@Work
- iOS Apps@Work AppStore 功能
- 檢視 App 詳細資料
- App 配置
- 將自訂屬性指派給應用程式
- Android 受管理的配置
- 管理 Google Play app
- 從 App Catalog 刪除 App
- 升級內部開發的 App
- 搜尋 Android App 的套件名稱
- 類別
- 發佈篩選
- 排除或分發應用程式
- 評論
- Apple Apps and Books
- 目錄設定
- 部署 app 相依性
- 使用 Android Enterprise 部署 Divide Productivity
- 設定 Provisioner app
- 管理 Windows 應用程式
- Ivanti Bridge

8.1. 「App Catalog「

本節包含以下各主題：

- App 功能的授權
- 切換清單檢視和方格檢視
- 新增適用於 Android Enterprise 的 Google Play Store app
- 從公開的商店新增 app
- 新增內部應用程式
- 委派裝置權限以取得 Android Enterprise 內部開發的 app
- 顯示內部開發 app 的設置描述檔狀態
- 更新 iOS 內部開發 app 的佈建描述檔
- 將內部開發 app 部署至 Google Play
- 為 Android Enterprise 裝置新增 Web app
- 新增適用於 iOS 裝置的 Web app
- 使用進階搜尋
- 將應用程式匯出至 CSV 檔案

使用「應用程式目錄」頁面可管理應用程式目錄。 App Catalog 會列出您提供給使用者的行動電話 app。 這些包括使用者可從公用應用程式商店下載的應用程式，以及您打算使用 Ivanti Neurons for MDM 發佈的應用程式 (內部應用程式)。 已啟用 AppConnect 的應用程式、適用於 iOS 的 GoClient，以及適用於 macOS 的 M@W 也會以商業應用程式的形式出現在應用程式目錄頁面中，藉此簡化將其匯入以供組態和發佈的流程。 當 iOS 使用者開啟 App Catalog 時，MAM-Only 裝置會提示他們選擇憑證，以驗證這些 app 的存取權。

Apple MacBook 的 M1 晶片組支援 iPhone 和 iPad VPP app。 僅管理員才能推送支援的 iPhone 和 iPad VPP app。 此選項不適用於從 App Catalog 安裝的使用者。

針對使用 Android 裝置的 Ivanti Neurons for MDM 租用戶，如果在 2021 年 3 月底之前未啟用 Android Enterprise，管理員將無法使用名稱搜尋應用程式。 當存取 App Catalog 頁面時，將會以橫幅訊息顯示此變更。 此橫幅訊息將繼續顯示，直到在這些租用戶上啟用 Android Enterprise，且未選取「不再顯示此內容」核取方塊選項。

- 無訊息 App 安裝方法不適用於公用 macOS app。 使用 Apple Apps and Books 與裝置型授權時，系統會在註冊時以「無訊息 App 安裝」方法部署 macOS app。
- 將 Ivanti Go 應用程式上傳到 Ivanti Neurons for MDM 伺服器時，如果您需要選擇**轉換成受管理應用程式**選項，您還需要啟用**在裝置上安裝**選項。
- Sonim XP5s 裝置不支援 App Catalog 及 app 安裝。
- 針對含有作用中管理權限的 app，Android 不允許使用者將其解除安裝。 若要解除安裝這類 app，請前往**「裝置設定 > 安全性 > 裝置管理員」**，然後停用「裝置管理員」權限。 然後，即可解除安裝 app。
- 如果在裝置上使用 Android Enterprise Play Store 手動安裝 Android Enterprise 應用程式，而且如果管理員稍後取消分發應用程式，則也必須手動解除安裝應用程式。
- 經過壓縮或混淆處理的內部開發 Android app 將無法上傳。
- 共享 iPad 上不支援公用應用程式。
- 由於 Apple 的限制，對於應用程式目錄中可用的企業對企業 (B2B) iOS 應用程式，**詳細資訊**索引標籤中不提供這些應用程式的說明和螢幕擷取畫面。

- 當您在應用程式目錄或管理入口網站內搜尋應用程式時，系統會根據**應用程式名稱**、**註解**、**說明**、**顯示版本**以及**新功能**顯示搜尋結果。 若搜尋到的應用程式資料與這些欄位中的任何一項相符，系統便會顯示該資料作為搜尋結果。

App 功能的授權

下列「應用程式目錄」功能需要額外的授權：

- 無訊息 app 自動安裝/解除安裝：Silver 授權
- 個別 App 配置：Gold 授權
- AppConnect 自訂配置：Gold 授權
- **Android Enterprise** 自訂組態: Silver 授權

如果是採單一應用模式的 Android 裝置：

當裝置是在單一應用模式中時，僅可以安裝內部開發的 app。 您可以安裝公用 app，但裝置先必須退出單一應用模式才能安裝這些 app。 此外，您可以將單一應用模式裝置上的可用 app，限制為僅限公司核准或設為允許清單的 app。 在使用 Android 4.1 的裝置上，如果核准的 app 啟動某個允許清單不含的 app，該 app 仍會啟動，但會快速最小化。 在使用 Android 5.0 的裝置上，由設為允許清單單的 app 啟動的未核准 app 仍可使用。

切換清單檢視和方格檢視

按一下「App 目錄」畫面右側的清單或方格圖示。

新增適用於 Android Enterprise 的 Google Play Store app

- 您可將 Google Play 商店中的應用程式新增至應用程式目錄，以供使用者運用。 若要從 Android Enterprise 中的 Google Play Store 新增 app，需要核准將 app 納入 App Catalog。
- Android Enterprise 裝置的 Google Play 商店版面針對從 Core 管理的移轉裝置提供首頁和 Ivanti Neurons for MDM 的快速連結，以顯示從 Ivanti Neurons for MDM 管理的所有應用程式。 當您將 Android Enterprise 裝置從 Core 移轉至 Ivanti Neurons for MDM 時，裝置的工作設定檔 Google Play 商店僅會列出 Core 和 Ivanti Neurons for MDM 應用程式目錄之間共同的應用程式。 您可按一下 Ivanti Neurons for MDM 按鈕以檢視從 Ivanti Neurons for MDM 應用程式目錄提供的所有應用程式清單。

Android Enterprise 裝置的 Google Play 商店版面針對從 Core 管理的移轉裝置提供首頁和 Ivanti Neurons for MDM 的快速連結，以顯示從 Ivanti Neurons for MDM 管理的所有應用程式。 當您將 Android Enterprise 裝置從 Core 移轉至 Ivanti Neurons for MDM 時，裝置的工作設定檔 Google Play 商店僅會列出 Core 和 Ivanti Neurons for MDM 應用程式目錄之間共同的應用程式。 您可以按一下 Ivanti Neurons for MDM 按鈕以檢視可在 Ivanti Neurons for MDM 應用程式目錄中使用的所有應用程式。

必要條件

- 您必須啟用 Android Enterprise 才能存取並新增 Google Play Store 應用程式至 App Catalog。

Procedure程序

1. 前往 **App > 應用程式目錄**。
2. 按一下**新增** (左上角)。

> 從下拉式清單選擇 Google Play，以搜尋 Google Play Store 中的 app。 Google Play iFrame 會在註冊 Android Enterprise 時顯示。

3. 在「搜尋」欄位中搜尋 app，然後按一下該 app。
4. 按一下**完成**。

已核准的應用程式以後可透過按一下**未核准**來取消核准。

選項	描述
核准設定	
在 app 要求新權限時保持核准	允許使用者安裝已更新的應用程式
在此 app 要求新權限時移除 app 核准	**將 app 從商店移除直到其獲得重新核准。**
核准設定	
新增訂閱者	當您已核准的 app 要求新權限時，請輸入電子郵件地址以將訂閱者新增至電子郵件通知。

從公開的商店新增 app

您可從從公開的商店將 app 新增到 App Catalog 中，以供使用者運用。

程序

1. 前往 **App > 應用程式目錄**。
2. 按一下**新增**。
3. 選擇您要的 app：
4. 選擇公開的 App Store。
5. 輸入 app 的名稱。
6. 從清單中選擇 app。
7. 按**下一步**。
8. 為使用者描述 app：
9. 新增或移除類別。
10. 輸入選填的描述。
11. 按**下一步**。
12. 定義 app 發佈：
13. 選擇發佈選項。
14. 展開**進階選項與應用程式組態**區段。
15. 請使用下列方針來完成選項：

設定	方法
安裝到裝置上	選擇此選項，以在註冊後立即啟動安裝。 除了下列情況例外，系統皆會提示使用者確認安裝 app： • 針對全新 app 安裝和 app 更新方面，裝置為受監管 iOS 裝置。 • 針對 app 更新方面，裝置為 iOS 非受監管裝置。 • 已註冊 Apps and Books 方案的使用者。 • 裝置為 Samsung Knox 裝置，並已選擇下方的無訊息自動安裝選項。 若是 iOS 公開 app，當首次在裝置上安裝時，App Catalog 會顯示「重新安裝」按鈕，以方便使用者再次安裝 app。 如果在裝置上執行的 app 版本與 iOS App Store 上的版本不同，將執行重新安裝。
App Catalog 不會顯示 app 給使用者	如果您不想讓使用者看到裝置 App Catalog 中的 app，可選擇此選項。
設定 App 安裝優先性	在使用者上架期間，選擇「高」、「中」或「低」以設定 app 安裝的優先順序。 在使用者上架期間，僅會安裝高優先性的 app。
在達到一定的嘗試失敗次數後，暫停 app 重新推送 (僅限 iOS)	請將切換開關切到「開啟」，以使用下列設定，在達到一定的重新推送嘗試失敗次數後，暫停 app 重新推送： **在以下次數之後停止重新推送：**輸入重新推送嘗試失敗次數，在達到此次數後便應停止重新推送。 輸入的值應在 **1** 到 **999** 的範圍內。 **次嘗試後並在以下時數之後重試：**輸入重新推送失敗後到再次執行重新推送前需經過的時數。 輸入的值應在 **3** 到 **48** 小時的範圍內。
(僅限 Android) 無訊息自動安裝到 Samsung Knox 裝置上	此選項不適用於公用 app。
(僅限 iOS 和 macOS) 啟用此 app 的 Per-App VPN	選擇此選項，以搭配使用個別 App VPN 配置與此 app。 從下拉清單中選擇要使用的個別 App VPN 配置。 若是 macOS，請僅選擇 Tunnel Per App VPN 配置。
(僅限 iOS) 防止備份至 iCloud 和 iTunes	選擇此選項可防止將此 app 的相關資料備份至 iCloud 和 iTunes。
(僅限 iOS) 移除取消註冊的 app	選擇此選項，以便在裝置不再受 Ivanti Neurons for MDM 管理時移除此應用程式。
(僅限 iOS) AppConnect 自訂配置	若是 AppConnect app，請輸入可指定您的自訂配置偏好設定的索引鍵和值。 請參閱 app 的說明文件，以瞭解可用的索引鍵。
iOS 7+ 受管理的 App 設定	輸入將此 app 定義為 iOS 7+ 受管理之 app 的索引鍵和值。 請參閱 app 的說明文件，以取得受支援索引鍵的詳細資訊。

> Android Enterprise 應用程式將提供不同的選項。

按**下一步**。

4. 選擇推廣選項：
5. 按一下 **+新增描述**以輸入配置的簡短描述。

- 不推薦

- 推薦清單
- 特色橫幅
- 如果選取「特色橫幅」，請指定以下詳細資訊:
    1. **標題** - 指定應用程式標題
    2. **說明** - 指定應用程式詳細資訊
    3. **橫幅樣式** - 選取橫幅顏色
6. 您可以選擇變更配置的發佈。
7. 按一下**完成**以儲存 app 配置。
8. 按一下**完成**。

> 當您在應用程式目錄中搜尋 Windows 應用程式時，您可以在下拉式清單中使用**應用程式名稱**或 **AppStore ID** 選項以搜尋最相符的應用程式:

- **應用程式名稱** - 選取此選項並提供應用程式名稱
- **AppStore ID** - 選取此選項並提供 AppStore ID

Windows 市集應用程式搜尋支援 Win32 市集應用程式。

確認裝置上有可用的 Winget 工具，可用於管理 Win32 市集應用程式。

新增內部應用程式

您可以使用下列檔案格式，將內部開發的 app 上傳至 App Catalog。 大型檔案可能需花幾分鐘時間上傳。 內部開發應用程式的版本數上限為 100。 如果超過數量上限，Ivanti Neurons for MDM 系統會清除最舊版本的應用程式。 可在「稽核追蹤」頁面檢視應用程式上傳和清除狀態。

Mobile@Work 傳回某些 app 的 MIP app 庫存可能不正確。 Mobile@Work 可能無法偵測到未安裝在預設位置的 app 的安裝狀態。 針對此類 app，新增偵測指令碼將有助於識別裝置上 app 的正確狀態。 如果偵測指令碼的結束代碼為 0，Mobile@Work 會判定 app 已存在。 如果為其他結束代碼，將會判定 app 為未安裝。 根據偵測到的 app，Mobile@Work 會準備裝置的庫存報告。

- IPA (iOS)
- MIP (Packager macOS app)
- PKG (macOS)
- APK (Android)
- APPX、APPXBUNDLE、EXE 和 MSI (Windows)

> 適用的應用程式包括具有指令碼的 PKG 或具有 PKG 與指令碼的 DMG，適用於 macOS 的 Mobile@Work 只能偵測成功的安裝要求。 如果 app 已刪除或已安裝的指令碼遭移除，它將不會報告。 因此，Ivanti Neurons for MDM 伺服器將無法重新傳送安裝指令。 如果連線在下載 app 時中斷，請藉由執行登記來重試 app 安裝。 若是 MIP app，在使用含指令碼的 PKG 或其中具有含指令碼的 PKG 的 DMG 進行安裝的裝置上，即使已移除 app，如果用戶端裝置的回條資料夾中存在 PKG 的項目，則 Mobile@Work 將不會安裝 MIP app。

程序

1. 前往 **App > 應用程式目錄**。
2. 按一下**新增** (左上角)。
3. 在**選取要上傳檔案的平台**下，選擇您的平台類別 (例如 **Apple 應用程式**) 並選取特定作業系統 (例如 Apple 應用程式下拉式清單中的 iOS 或 macOS)。

> 如果使用者選取平台，並嘗試上傳衝突的檔案類型 (例如選取 Apple 但上傳 .apk)，系統將觸發「無效檔案格式」錯誤。

4. 將 app 檔案拖曳到虛線方塊中，或按一下**選擇檔案**，從檔案系統中進行選擇，然後按一下**確認**。
5. 按**下一步** (右下角)。
6. 描述使用者適用的 app，並設定必要條件 app：
7. 新增類別。
8. 新增 macOS 套件時，如果套件包含一個以上的 app (例如：Microsoft Office 和 Cisco AnyConnect 套件)，則系統會使用所選擇的主要 app 來識別套件是否已安裝。 Per-app VPN (若設定) 將套用到這些 app。
9. 輸入選填的描述。
10. **MSI 產品代碼**：上傳 MSI app 時，MSI app 的產品代碼會自動填入此欄位。

> 您必須選取「我已檢查 MSI 產品代碼」選項，以確保填寫正確的 GUID。

覆寫 URL：輸入選用的 App 來源 URL 覆寫，以允許從不同來源下載 App，或允許從本機網路 (HTTP 和 HTTPS) 取得大型檔案 (例如 Microsoft Office 安裝媒體)。 此選項需要存取安全內部網路，並與儲存 app 的備用伺服器進行手動同步。 除非您已建立必要的基礎架構，否則請勿輸入值。 編輯特定 app 的 app 設定時，您可編輯此值。

- 如果是 iOS 應用程式，應用程式覆寫 URL 必須使用 HTTP 或 HTTPS 格式。
- 如果是 Android 和 macOS 應用程式，則應用程式覆寫 URL 僅能使用 HTTPS 格式。
- 如果是 macOS 應用程式，則 URL 的副檔名應為 .pkg。

6. **命令列** (僅限 Windows 32 位元 MSI app)：輸入選用的命令列切換，以指定其他不屬於套件但會用來部署 MSI 檔案的資訊。 例如，若要將安裝日誌寫至輸出檔，您可以在此欄位中輸入 "/log output.txt"。 如此一來，即會在 C:\Windows\System32 資料夾中建立 output.txt 檔。 預設下，在上傳 MSI app 期間，會自動填入用於無訊息自動安裝的命令列選項 /qn。

> 要上傳的 MSI app 封裝名稱不應新增為命令列引數的一部分。 如果已新增，將會限制上傳，直到 app 的封裝名稱從命令列引數移除。 將會在額外的連結之下提供所有支援的命令列選項清單。 在 app 的檢視和編輯模式中將可看到此連結。

適用於 Win32 的 .EXE: 已使用 Admin PowerShell 模式透過 Bridge 安裝。 Bridge 功能可用時，系統會自動使用此功能。

- 更新版本以維護**顯示版本**與**套組版本**之間的一致性
- 安裝程式 (.EXE) 位置
- 安裝程式命令列參數: 無訊息執行檔案引數 (例如，/SILENT 或 /VERY SILENT) 為必填
- 以使用者身分執行安裝程式: 若要使用使用者認證進行安裝，請選取「以使用者身分執行」選項

適用於 Win32 市集應用程式: 已使用 Admin PowerShell 模式透過 Bridge 安裝。

9. 若是封裝工具 macOS app，請設定必要條件 app (選用)。 如需必要條件 app 功能的概覽，請參閱瞭解封裝工具內部開發 macOS app。
10. **啟動 URL**：輸入用來啟動 AppStation 當中 app 的 URL。 僅在為了透過 AppStation 在「僅限 MAM」部署中發佈而新增非 AppConnect app 時才需要，而且僅適用於 iOS app。
11. 設定 app 委派。

> 一旦您委派必要條件 app，而它成為非預設空間當中 app 的必要條件 app 時，您無法解除安裝該 app，除非您先移除必要條件關係。

按**下一步**。

13. 按**下一步**。
14. (選用) 新增 app 的畫面擷取。
15. (選用) 新增或更換應用程式的圖示 (iOS，MacOS 和 Windows 應用程式)。
16. 按**下一步**。
17. 針對封裝工具 macOS app，定義或選擇在 app 安裝之前及/或之後要執行的安裝指令碼。 在搜尋方塊中輸入或按一下連結以查看指令碼清單，選擇以下一或兩個指令碼。 按**下一步**。
18. 您可以在**管理 > 指令碼和檔案 > 所有指令碼**頁面中建立指令碼。 如果您升級 app，您可以選擇從舊版 app 複製指令碼，並執行升級的 app 的指令碼。 如果您略過此區段，您之後可透過編輯方式配置指令碼。

- **預先安裝指令碼** - 輸入指令碼名稱以選擇在 app 安裝之前要執行的指令碼。 將會執行或重試預先安裝指令碼，直到用戶端收到指令碼執行成功狀態。 只有在此之後，會傳送 app 安裝指令。 您可在**記錄**標籤中的裝置詳細資料查看指令碼執行狀態。
- **安裝後指令碼** - 輸入指令碼名稱以選擇在 app 安裝之後要執行的指令碼。
- **解除安裝指令碼**：輸入當伺服器偵測到有 app 不再發佈至裝置時，伺服器要傳送至裝置的指令碼名稱。
- **偵測指令碼** - 輸入伺服器要傳送至裝置的指令碼名稱，用來偵測 app。 App 的偵測指令碼結果會覆寫裝置上 app 的預設庫存結果。 不論 App 是否已發送至裝置，所有 app 的偵測指令碼將會傳送至裝置，以評估裝置上的 app 是否存在。
  範例偵測指令碼如下：

```
#!/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
```

定義 app 發佈：

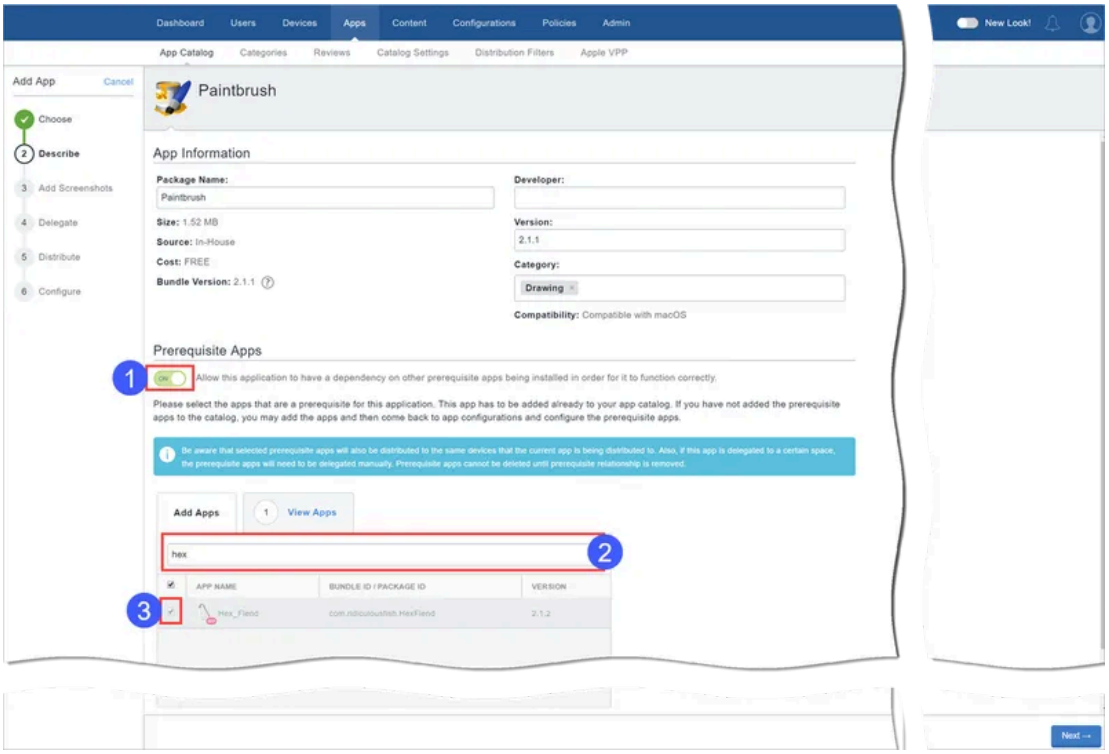
12. 選擇推廣選項：
13. 選擇發佈選項。
14. 展開**進階選項與應用程式組態**區段。
15. 請使用下列方針來完成選項：
16. 按**下一步**。

設定	方法
安裝到裝置上	選擇此選項，以在註冊後立即啟動安裝。 除了下列情況例外，系統皆會提示使用者確認安裝 app： • 裝置為受監管的 iOS 裝置。 • 裝置為 Samsung Knox 裝置，並已選擇下方的無訊息自動安裝選項。
App Catalog 不會顯示 app 給使用者	如果您不想讓使用者看到裝置 App Catalog 中的 app，可選擇此選項。
設定 App 安裝優先性	在使用者上架期間，選擇「高」、「中」或「低」以設定 app 安裝的優先順序。 使用者上線期間僅安裝高優先順序的應用程式。
在達到一定的嘗試失敗次數後，暫停 app 重新推送 (僅限 iOS)	請將切換開關切到「開啟」，以使用下列設定，在達到一定的重新推送嘗試失敗次數後，暫停 app 重新推送： **在以下次數之後停止重新推送：**輸入重新推送嘗試失敗次數，在達到此次數後便應停止重新推送。 輸入的值應在 **1** 到 **999** 的範圍內。 **次嘗試後並在以下時數之後重試：**輸入重新推送失敗後到再次執行重新推送前需經過的時數。 輸入的值應在 **3** 到 **48** 小時的範圍內。
(僅限 Android) 無訊息自動安裝到 Samsung Knox 裝置上	如果您不想讓系統提示使用者確認 Samsung Knox 裝置上進行的安裝，可選擇此選項。
(僅限 iOS 和 macOS) 啟用此 app 的 Per-App VPN	選擇此選項，以搭配使用個別 App VPN 配置與此 app。 從下拉清單中選擇要使用的個別 App VPN 配置。 若是 macOS，請僅選擇 Tunnel Per App VPN 配置。
(僅限 iOS) 防止備份至 iCloud 和 iTunes	選擇此選項可防止將此 app 的相關資料備份至 iCloud 和 iTunes。
(僅限 iOS) 移除取消註冊的 app	選擇此選項，以便在裝置不再受 Ivanti Neurons for MDM 管理時移除此應用程式。
(僅限 iOS) AppConnect 自訂配置	若是 AppConnect app，請輸入可指定您的自訂配置偏好設定的索引鍵和值。 請參閱 app 的說明文件，以瞭解可用的索引鍵。
iOS 7+ 受管理的 App 設定	輸入將此 app 定義為 iOS 7+ 受管理之 app 的索引鍵和值。 請參閱 app 的說明文件，以取得受支援索引鍵的詳細資訊。

17. 按一下**完成**。
    - 不推薦
    - 推薦清單
    - 橫幅

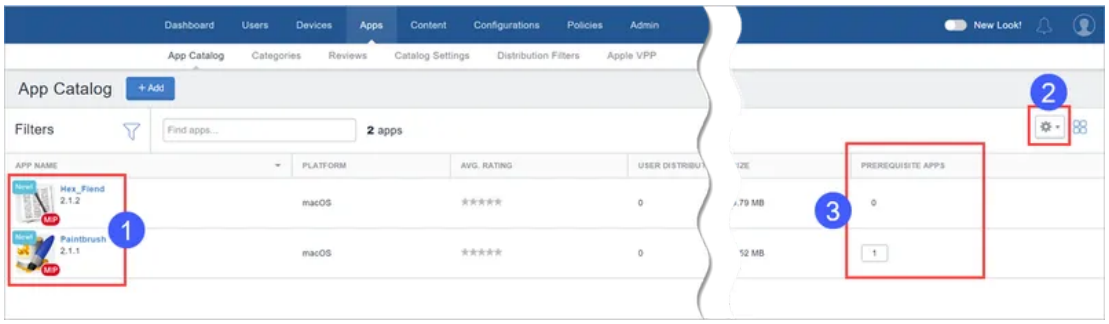
瞭解封裝工具內部開發 macOS app

匯入封裝工具內部開發的 macOS app 時，管理員可以啟用 1 要搜尋的必要條件 App 功能 2，並選擇 3 用戶端上必須安裝的必要條件 app，之後才能安裝管理員匯入的 app。



完成匯入後，封裝工具 macOS 內部開發的 app 將顯示在 App Catalog 中，而且下方會顯示 MIP 1。 接著您可以使用欄位設定 (2) 來新增必要條件 APP 欄位 (3)，以概覽具有相依項目的 app (即具有必要條件 app)。

- 您可以搜尋並選擇 MIP、非 MIP 及公開 app (Apps and Books 和 macOS App Store 公開 app) 做為必要條件 app。
- 使用者需要接受 Apps and Books 必要條件 app 的 Apps and Books 授權，才能會以無訊息方式自動安裝。
- 若是非 Apps and Books 公開必要條件 app，管理員需要明確發佈公開 app，而使用者必須安裝公開 app。 公開 app (Apps and Books 和非 Apps and Books app) 必須匯入 App Catalog 中，這樣才能顯示在必要條件 app 清單中。 「來源」欄位指出必要條件 app 的類型。
- 安裝非 MIP 自行開發的 app (含有非 MIP 必要條件 app) 時，必須使用 MDM 登記。
- 使用者需要手動安裝公開非 Apps and Books 必要條件 app。
- 如果 Apps and Books 權杖遭到移除或授權已用完，則選擇做為必要條件 app 的 Apps and Books App 和主要 app 將不會安裝。 如果 Apps and Books app 出現任何上述狀況，管理員必須遵循最佳作法，事先通知使用者。



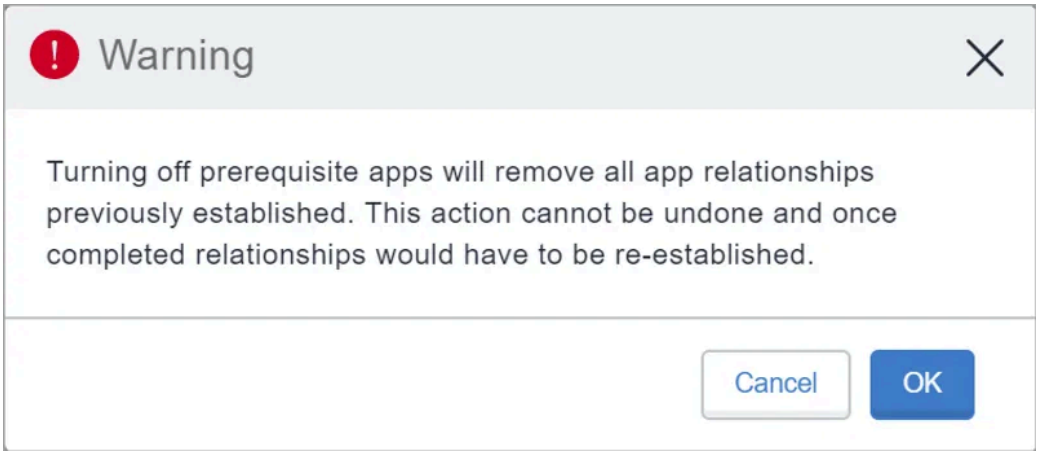
當必要條件 app 已明確發佈時，它們就成為可供使用者下載的獨立 app。 如果使用者試圖解除安裝必要條件 app：

- 務必在下次裝置簽入時，再次安裝必備應用程式。
- 如果相同裝置未安裝相依的主要 app，必要條件 app 將會解除安裝。

- 假如必要條件 app 未明確發佈，必要條件 app 將連同主要 app 一併解除安裝。
- 倘若必要條件 app 已明確發佈，則必要條件 app 將會留在裝置上。
- 若是必要條件 app 具有相依 app，則必要條件 app 將會留在裝置上。

關閉必要條件 App 功能

與具有相依項目和必要條件 app 的 app 互動時，例如更新、刪除或委派上述 app，您將看到系統提示指導您 app 的相依項目或必要條件狀態可能會如何影響您有意執行的動作。 例如，當您嘗試關閉 app 的必要條件 App 功能，將會顯示下列提示：



- 如果您關閉 app 的必要條件 App 功能，系統會清除必要條件 app 的詳細資料。 這包括自動委派和解除委派子空間的必要條件 app。
- 在 Apps@Work 中，如果相依 app 的必要條件 apps 尚未安裝在裝載用戶端上，就不會顯示相依 app 的安裝按鈕。
- 在使用者裝置上，當使用者試圖安裝具有相依項目的內部開發 app 時，將會最先安裝必要條件 app (若尚未安裝)，接著安裝主要 app，這會耗時幾分鐘。 使用者將會看到此相依 app 清單，以及它們的安裝狀態。

委派和解除委派空間的必要條件 app

- 將主要 app 委派給子空間時，系統會自動委派與該 app (主要 app) 綁定的必要條件 app。
- 如果您解除委派子空間的主要 app，在未明確發佈必要條件 app 的情況下，系統也會解除委派必要條件 app。 不過，如果必要條件 app 已綁定多個主要 app，則系統不會將其解除委派。
- 如果您已明確委派必要條件 app，系統即不會自動將其解除委派。

委派裝置權限以取得 Android Enterprise 內部開發的 app

可以將委派權限指派給可套用至 Android Enterprise 受控裝置和 AMA 裝置的內部應用程式。

程序

1. 前往 **App > 應用程式目錄**。
2. 在 **App Catalog** 中，選擇您想委派裝置權限的 app。
3. 按一下 **App 配置**索引標籤。
4. 在委派權限 (內部 Android Enterprise 應用程式) 中，選取應用程式所需的權限:

> 僅 COSU 部署會使用 AMAPI。 請參閱 AMAPI 區段以取得更多資訊。

   - **設定第三方 app 執行時期權限**

- **隱藏與暫停第三方 app**
- **管理憑證**
- **管理 app 配置**
- **管理封鎖 app 解除安裝**
- **管理啟用系統 app**
- **管理認證選擇** (在 AMAPI 模式中不支援)
- **管理解除安裝 app 保留** (在 AMAPI 模式中不支援)
- **管理網路記錄收集** (一次僅支援一個應用程式)
- **管理安全記錄收集** (一次僅支援一個應用程式)
- **管理現有 app 的安裝** (在 AMAPI 模式中不支援)
- **安裝與移除套件** (在 AMAPI 模式中不支援)

在所有支援的「Android 裝置擁有者」模式裝置 (7.0 或更新版本) 上，都可以使用安裝和移除套件選項。 其他的委派權限僅適用於 Android 8.0 或更新版本。
選擇**有此 App 的每個人**、**沒有人**或**自訂**，以設定發佈選項。

6. 按一下**儲存**。

顯示內部開發 app 的設置描述檔狀態

在 App Catalog 頁面上，iOS 內部開發 app 的佈建描述檔狀態。 描述檔名稱旁的工具提示會顯示描述檔的到期天數。 此狀態可用來檢查內部開發 app 的設置描述檔何時到期。

此狀態有助您針對因描述檔過期而未能安裝的 app 進行疑難排解。 如果沒有適當的設置描述檔，app 或許可以安裝但可能無法開啟或啟動。

程序

1. 前往 **App > 應用程式目錄**。
2. 按一下右上角的齒輪圖示以顯示欄位。
3. 在 App Catalog 頁面上，選擇**設置描述檔**以顯示 app 清單的欄位。

設置描述檔詳細資料也會顯示在 app 詳細資料的「設置描述檔設定」區段下。

更新 iOS 內部開發 app 的佈建描述檔

設置描述檔已套用至特定 iOS 內部開發 app。 App 的佈建描述檔詳細資訊會列在 app 詳細頁面。 若要在裝置上啟動 iOS 內部開發 app，其中的設置描述檔需為未過期。 如果過期，您可以在 app 詳細資料頁面中上傳描述檔，藉此更新設置描述檔。

程序

1. 前往 **App > 應用程式目錄**。
2. 按一下需要設置描述檔更新的 app。 隨即顯示 app 詳細資料頁面。
3. 按一下**編輯**。
4. 在**設置描述檔**區段中，按一下**選擇檔案**。
5. 選擇要上傳的設置描述檔檔案 (副檔名為 .mobileprovision)，然後按一下**儲存**。

將內部開發 app 部署至 Google Play

將您的內部應用程式上傳到 Google Play 專用頻道，並將其匯入 Ivanti Neurons for MDM，以便部署到支援 Android Enterprise 的裝置。

程序

1. 登入 Google 私人 app 控制台：https://play.google.com/apps/publish。
2. 按一下功能表中的**所有應用程式**。
3. 按一下**建立新的應用程式**，然後輸入應用程式的名稱。
4. 按一下**上傳 APK** 以上傳您產生的 .apk 檔案。
5. 按一下**商店清單**：
   - 輸入簡短描述和完整描述。
   - 上傳所有索引標籤的畫面擷取。
   - 上傳高解析度圖示。
   - 上傳功能圖形圖示。
   - 輸入分類、詳細聯絡資訊和隱私權政策等必填資訊。
   - 完成 app 評等問卷。
6. 按一下**價格與發佈**。
   當所有必填資訊都已經輸入，頁面頂端會顯示「準備發佈」。
7. 前往 Ivanti Neurons for MDM 中的「應用程式」索引標籤。
8. 按一下**重新整理可用目錄**以同步您的私人 app。

> 發佈 app 可能需要數小時的時間。

為 Android Enterprise 裝置新增 Web app

Web App 是某個網站的連結，以捷徑形式安裝在裝置上。 Web App 的行為類似於其他 app，這表示 Web App 的發佈準則可以與任何 app 相同。 Web 應用程式可以出現在 App Catalog 中，也可以由使用者安裝，如同任何其他 app。 不過 Web App 只能有單一版本，而且不支援無訊息自動安裝。 Web App 使用 Web Clip，以配置形式安裝在裝置上，但行為模式則如同 app。

在 App Catalog 中將 Web Clip 設為 app，以便透過 App Catalog 提供 Web App 給使用者運用。 Web Clip 可定義為配置，但只有管理員能夠發佈配置。 使用者可選擇在其裝置上安裝 Web App 或退出，但使用者無法選擇退出 Web Clip 配置。

在 Android Enterprise 中，網頁應用程式是一種嵌入式的網頁應用程式，可在工作設定檔中的 Google Chrome 上執行。 它可以與 Android Enterprise 中的 VPN 或 SSO 解決方案合併使用。 在建立 Web app 後，app 的運作方式和任何其他 Android app 相同，您可視需要發佈。 必須在公司擁有裝置上的工作描述檔中安裝 Chrome，才能執行 Web app。

> 如果使用此功能時發生任何問題，管理員可聯絡支援中心。

程序

1. 前往 **App > 應用程式目錄**。
2. 按一下 **+新增**。
3. 從下拉式清單選擇 **Google Play**，以搜尋 Google Play Store 中的 app。 如果註冊了 Android Enterprise，則會顯示 Google Play iFrame。
4. 按一下 **Web 應用程式**。
5. 為使用者描述 app：

1. App 標題或名稱。
2. App URL。
3. 顯示 Web App 類型。
4. 上傳圖示，可以是 512px 正方形 PNG 或 JPEG 影像。

按一下**建立**。 等待將 app 發佈至 iFrame。 可能需要幾分鐘。 您可以關閉它，之後再回來。

7. 在 Web App 發佈後，將 app 匯入 App Catalog 以便發佈。 按一下 Web App 圖示。
8. 向下捲動，然後按一下**選擇**。
9. 新增類別和選填的描述。
10. 按**下一步**。
11. 選擇下列其中一個 App 委派選項：
    - 委派此 app 給所有空間。
    - 請勿委派此 app 給所有空間。

按**下一步**。

13. 選擇應用程式的發佈選項。
14. 按一下 **完成**。

新增 Web App 後，如有需要您可以編輯 Web App。 操作方式：

1. 在 **App Catalog** 頁面中，按一下現有 Web App 的名稱。
2. 按一下**編輯**以編輯 Web App 欄位。

新增適用於 iOS 裝置的 Web app

Web App 是某個網站的連結，以捷徑形式安裝在裝置上。 Web App 的行為類似於其他 app，這表示 Web App 的發佈準則可以與任何 app 相同。 Web 應用程式可以出現在 App Catalog 中，也可以由使用者安裝，如同任何其他 app。 不過 Web App 只能有單一版本，而且不支援無訊息自動安裝。 Web App 使用 Web Clip，以配置形式安裝在裝置上，但行為模式則如同 app。

將 Web 剪輯設定為應用程式目錄中的應用程式，以便使用者可以在應用程式目錄中使用 Web 應用程式。 Web Clip 可定義為配置，但只有管理員能夠發佈配置。 使用者可選擇在其裝置上安裝 Web App 或退出，但使用者無法選擇退出 Web Clip 配置。

> 如果使用此功能時發生任何問題，管理員可聯絡支援中心。

程序

1. 前往 **App > 應用程式目錄**。
2. 按一下 **+ 新增** (左上角)。
3. 按一下 **Web App**。
4. 為使用者描述 app：
    1. App 名稱。
    2. App URL。
    3. 平台類型。
    4. App 圖示。

5. 新增或移除類別。
6. 全螢幕 - 選擇此選項可將 Web App 顯示為全螢幕應用程式。
7. 可移除 - 選擇此選項可將 Web App 變成可移除。
8. 按**下一步**。

選擇下列其中一個 App 委派選項：

- 委派此 app 給所有空間。
- 請勿委派此 app 給所有空間。

按**下一步**。

7. 選擇應用程式的發佈選項。
8. 按一下 **完成**。

編輯 Web 應用程式

新增 Web App 後，如有需要您可以編輯 Web App。

程序

1. 在 **App Catalog** 頁面中，按一下現有 Web App 的名稱。
2. 按一下**編輯**以編輯 Web App 欄位。

慢速推出發佈

慢速推出發佈設定可讓管理員自動為裝置逐步推出新版本的應用程式。 當您要推出應用程式的後續版本時，可使用此「使用慢速推出發佈方法」選項。 即使慢速推出已暫停，Ivanti Neurons for MDM 管理入口網站仍然允許編輯應用程式。

為某個版本設定慢速推出後，其後續版本可套用上次設定的相同百分比。 若發佈設定為 100%，則可暫停發佈應用程式。 不過，如果您將發佈目標設為 100%，就必須為下個版本手動設定發佈目標百分比，因為此 UI 會將百分比重設為 0%。

程序

	1. 前往 App Catalog > App，選擇其中一個發佈模式選項。
	2. 選擇自訂在選擇摘要中的裝置 % (慢速推出) 選項。
	3. 從慢速推出設定，拖曳指定發佈目標 % 的滑桿。
4. 按一下確認，然後按一下完成。 最新應用程式版本的狀態隨即顯示。 「應用程式目錄」頁面在表格中指出「慢速推出」狀態。	

如果您無法在 **App Catalog** 頁面上執行工作，可能是您沒有所需的權限。 需要「應用程式與內容管理」角色。

使用進階搜尋

您可使用進階搜尋選項根據規則來搜尋應用程式，以識別和檢視符合特定準則的應用程式。 這些規則可使用適用的運算子進行建構，包括「等於」、「小於」、「大於」及「不等於」運算子。 這些規則選項可以用「任何 (或)」或「所有 (及)」選項來建立巢狀結構。 符合規則的應用程

式會顯示在此區段下方。

> 在搜尋中使用的自訂屬性值區分大小寫。

程序

1. 從「應用程式目錄」頁面，按一下**進階搜尋**連結。 「進階搜尋」精靈隨即開啟。
2. 按一下下列其中一個選項：
   - **任一** - 應用程式必須符合至少一項規則時使用
   - **全部** - 應用程式必須符合所有規則時使用

若要建立定義搜尋條件的規則，選取下列其中一個選項，並選取適當的相關動作:

- AppConnect 已啟用
- 平均評分
- 套組 ID
- 類別
- 成本
- 自訂屬性
- 新增至 AppCatalog 的日期
- 修改日期
- 裝置發佈
- 裝置群組發佈
- 裝置類型
- 群組發佈
- 最低作業系統版本
- 名稱
- 作業系統平台
- 佈建設定檔
- 大小
- 來源
- 使用者發佈
- 使用者群組名稱
- 版本

4. (選用) 按一下 **+** 以建立其他規則。
5. 按一下**搜尋**。 會顯示符合搜尋準則的應用程式清單。

載入搜尋查詢

可以檢視已儲存的搜尋查詢清單。

程序

1. 按一下「進階搜尋」，然後按一下資料夾圖示。 建立的搜尋查詢清單會顯示在**載入的查詢**區段中，並顯示下列詳細資訊：
    - **查詢名稱** - 載入查詢的名稱。
    - **查詢內容** - 顯示定義搜尋查詢的規則內容。
    - **動作** - 選擇要對查詢執行的動作。
2. 按一下**動作**欄中的**載入查詢**，以檢視與載入查詢中定義的準則相符的應用程式清單。
3. 按一下**刪除**以刪除載入查詢。

將應用程式匯出至 CSV 檔案

您可以使用「應用程式目錄」頁面中的「匯出至 CSV」選項匯出應用程式。

程序

1. 前往**應用程式** > **應用程式目錄**。
2. 按一下**匯出至 CSV**，將應用程式清單及相關詳細資訊匯出至 CSV 檔案。

> 僅包含所選空間中列出的應用程式，所有分頁結果都會編譯到單一檔案中。

> 使用篩選或搜尋結果將僅匯出相關的應用程式。

3. 隨即顯示一則含有**繼續**和**取消**按鈕的快顯訊息，指出匯出程序已開始，並且很快就會提供報告。
4. 按一下**繼續**，請先等候要求完成，然後再提交另一項要求。
5. 隨即顯示一則訊息，指出**應用程式目錄 - CSV 報告已完成**，其中包含**下載**和**刪除**按鈕。
6. 按一下**下載**即可下載報告。
7. (選用) 按一下**刪除**以刪除報告。

> **匯出至 CSV** 選項僅在選取**下載**或**刪除**選項後才會重新啟用。

> 如果應用程式有多個版本，則每個應用程式版本只會顯示一個項目。

相關主題

- 使用者角色
- 從 App Catalog 刪除 App
- 部署 app 相依性

8.2. 宣告式裝置管理 (DDM) 應用程式管理

概覽

聲明式裝置管理 (DDM) 應用程式管理引入了對 Apple 聲明式管理架構的支援，該架構用於 iOS 和 iPadOS 裝置上的應用程式部署和生命週期管理。 DDM 不依賴連續命令傳遞和定期拉取，而是使裝置能夠在本機套用聲明，並主動報告狀態變更。

使用 DDM 時，伺服器僅向裝置傳送聲明一次。 裝置接著會套用組態、監視其狀態，並將狀態變更回報給伺服器。 這種以裝置為導向的方法可減少伺服器通訊、改善擴充性，並為應用程式部署提供更及時的狀態更新。

DDM 應用程式管理目前專注於支援 Apple 裝置的核心應用程式管理功能。

DDM 應用程式管理工作流程

在 DDM 工作流程中，伺服器會將所需的狀態傳送至裝置，裝置將負責維護和報告該狀態。

將應用程式指派給已啟用 DDM 裝置時:

1. 伺服器傳送應用程式聲明至裝置。
2. 裝置會在本機處理聲明
3. 裝置會根據指派的設定安裝、更新或維護應用程式。
4. 裝置會持續監控應用程式狀態。
5. 任何安裝狀態或狀態變更都會立即回報給伺服器。

此聲明模型提供應用程式部署進度的近乎即時可見性，不需要定期狀態拉取。

啟用 DDM 應用程式管理

DDM 應用程式管理可透過使用者設定啟用，並指派給特定使用者群組。

若要啟用 DDM 應用程式管理:

1. 前往**使用者** > **使用者設定**。
2. 在 **Apple DDM 設定**下，按一下特定使用者群組的 **+新增** 設定。 **Apple DDM 設定**頁面隨即開啟。
3. 輸入名稱並切換**啟用 DDM 應用程式管理**滑桿。
4. 按**下一步**。 **使用者設定發佈**頁面開啟。
5. 選取將使用 DDM 應用程式管理的使用者群組。
6. 按一下**完成**。

為使用者群組啟用 DDM 後，指派給該群組使用者的所有受支援應用程式都會透過 DDM 應用程式管理 進行處理。 DDM 組態是租用戶通用組態，但是透過使用者群組指派套用，讓組織能夠逐步將 DDM 推出至選取的使用者或群組。

支援的註冊方法

DDM 應用程式管理支援使用下列方式註冊的 iOS / iPadOS 裝置:

- iReg/ 受管理 Ivanti Go 用戶端
- 裝置註冊描述檔 (DEP)
- 帳戶驅動的裝置註冊

支援的應用程式類型

DDM 應用程式管理支援下列應用程式類型:

- 公用應用程式
- VPP 應用程式 (僅適用於裝置註冊)
- 內部開發的應用程式

應用程式指派和部署工作流程與傳統的 N-MDM 部署大致上保持不變。 現有的應用程式發佈程序繼續運作，同時受益於 DDM 增強狀態報告功能。

8.2.1. DDM 應用程式管理設定

一般而言，應用程式管理包含下列設定:

- 防止備份到 iCloud
- 請勿在新註冊的裝置上安裝應用程式
- 行動 5G
- DNS 代理
- 受管理的應用程式組態
- 商務應用程式 – Apps@Work、Email+ 等。
- 個別應用程式 VPN
- 網路繼電器
- Webcontent 篩選器
- 允許 Appstore 更新

除了上述設定之外，DDM 應用程式管理還引入了一些功能，僅適用於 DDM 管理的裝置。

應用程式版本釘選

應用程式版本釘選可讓管理員在 DDM 管理的裝置之間部署和維護特定應用程式版本。

啟用版本釘選時:

- 裝置安裝指定的應用程式版本。
- 無法自動升級至較新版本。
- 應用程式會保留在指派的版本上，直到管理員明確選取新版本為止。

利用此功能可更緊密地控制應用程式版本一致性和階段式升級部署。

程序

1. 前往**應用程式** > **應用程式目錄**。
2. 從顯示的清單中按一下應用程式。 **應用程式詳細資料**頁面隨即開啟。
3. 在**應用程式組態**索引標籤下，按一下 **Apple 應用程式設定**。
4. 按一下列出的任何現有設定。
5. 按一下**編輯**。
6. 在**將應用程式版本釘選到裝置**區段下，選取**釘選應用程式版本**選項。
7. 從**選取應用程式版本**清單中，選取所需的應用程式版本。

> 如果裝置有現有的應用程式版本，則無法將其取代為舊版。

8. 按一下**更新**。

自動 App Store 更新控制項 (自動應用程式更新)

管理員可以設定如何為受管理應用程式處理 App Store 更新。 此功能可更好地控制應用程式更新行為，並幫助組織使更新與內部驗證和推出流程保持一致。

允許透過行動電話網路下載

DDM 引入專用設定，透過行動電話網路控制應用程式下載和更新。

程序

1. 前往**應用程式** > **應用程式目錄**。
2. 從顯示的清單中按一下應用程式。 **應用程式詳細資料**頁面隨即開啟。
3. 在**應用程式組態**索引標籤下，按一下**安裝到裝置上**。
4. 按一下列出的任何現有設定。
5. 按一下**編輯**。
6. 在**允許透過行動電話下載**區段下，選取下列其中一個選項:
    - **儲存設定** – 預設選項。 裝置在下載應用程式時使用對應商店的設定。
    - **一律開啟** – 即使裝置沒有 Wi-Fi 連線，也可以下載應用程式。
    - **一律關閉** – 如果裝置沒有 Wi-Fi 連線，則不允許下載應用程式。
7. 按一下**更新**。

應用程式安裝工作流程

分發應用程式的程序仍然與傳統的 N-MDM 應用程式管理類似。

管理員可以:

- 指派應用程式
- 分發應用程式
- 安裝應用程式

但是，DDM 會變更部署狀態的通訊方式。 裝置報告應用程式狀態並非依賴伺服器提取，而是在動作完成後立即變更。 這可提供關於安裝進度和部署結果的更準確和及時的資訊。

狀態報告與監控

DDM 應用程式管理的主要優點之一是主動狀態報告。

對於 DDM:

- 裝置在本機監視應用程式狀態。
- 立即偵測到安裝和更新事件。
- 狀態變更會自動報告給伺服器。
- 部署資訊隨即可用，無需等待排程的輪詢間隔。

這可讓管理員更快速地瞭解:

- 應用程式安裝進度
- 成功安裝

- 應用程式更新完成
- 應用程式狀態變更
- 部署失敗

即時報告可改善疑難排解，並提供反應更靈敏的應用程式管理體驗。

需求

DDM 應用程式管理僅支援:

- iOS 26 或更新版本
- iPadOS 26 或更新版本
- 受管理的 Ivanti Go 用戶端 126 或更新版本

不符合這些要求的裝置繼續使用傳統的 N-MDM 應用程式管理。

> 一旦透過 DDM 應用程式管理處理裝置，停用或更新此原則發佈不會將裝置復原為 MDM 應用程式管理。 若要將裝置返回 MDM 應用程式管理，請移除原則指派並重新註冊裝置。

8.3. Apps@Work (iOS、Android、Windows 和 macOS)

Apps@Work 是一個企業應用程式店面，可輔助安全發佈軟體和應用程式。 Apps@work 適用於 iOS、Android、Windows 和 macOS 裝置。 Apps@Work 企業應用程式商店已整合到 Ivanti Go app 和 Mobile@Work 用戶端中，適用於 iOS、Android 和 macOS。 對於 Windows 裝置而言，Apps@Work 是一個原生獨立應用程式。 本節包含以下各主題：

- iOS Apps@Work
- Android Apps@Work
- macOS Apps@Work
- Windows Apps@Work

iOS Apps@Work

透過 Go 用戶端自動部署 Apps@work 原生應用程式商店。 管理員無需執行任何操作。 Apps@work 索引標籤會顯示在 Go 用戶端工作列上。 一般使用者可以前往此索引標籤檢視和安裝所屬公司核准的應用程式。 如需更多資訊，請參閱 iOS Apps@Work AppStore 功能。

iOS Apps@Work 的一般使用者應用程式更新通知預設為啟用。 若您要變更設定，請參閱目錄設定中的**通知**主題。

使用 iOS Apps@Work Webclip 的現有客戶

依預設，部署了舊版 iOS Apps@Work webclip 的客戶不會獲得原生整合 AppCatalog。 若想要轉換為 iOS Apps@Work 原生目錄並從裝置中刪除 Apps@work webclip，請執行以下步驟:

推送組態

管理員必須將「原生用戶端應用程式目錄」組態推送到裝置，使 Apps@Work 可用於 Go 用戶端應用程式的「原生應用程式商店」體驗。 如需更多資訊，請參閱使用配置。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 前往**組態** > 篩選器，然後選擇**用戶端服務**。 所有用戶端組態全部列出。
3. 選取**原生用戶端應用程式目錄**。 「原生用戶端應用程式目錄」組態頁面隨即開啟。
4. 按一下**編輯發佈**圖示。 「編輯發佈」頁面隨即開啟。
5. 請選擇下列選項之一：
    - **所有裝置**
    - **無裝置** - 若不想散發到任何裝置，可選取此項
    - **自訂** - 可讓您選擇裝置、裝置群組、使用者、使用者群組
6. 散發組態之後，使用者必須將 Go 用戶端版本升級到 83 或更高版本。 Apps@Work 索引標籤現在出現在 Go app 用戶端中。

> 無法為使用 iReg 註冊的裝置推送組態，因為 Go 用戶端在裝置上無法使用。 必須安裝 Go app 用戶端才能取得原生應用程式目錄。 如需更多資訊，請參閱裝置註冊 (iOS、macOS 及 Android)。

移除 iOS Apps@Work Webclip

對於已將 Apps@Work Webclip 散發到其裝置並已移轉到 Apps@Work 原生體驗的客戶，他們可以移除 iOS Apps@Work webclip。

程序

1. 前往**配置**。
2. 篩選組態 – **Apple 應用程式目錄**。
3. 按一下**編輯**。
4. 從**發佈**中選擇**不發佈到任何裝置**。
5. 按一下**儲存**。

Android Apps@Work

透過 MI Go 用戶端自動部署 Apps@work 原生應用程式商店。 管理員無需執行任何操作。 Apps@work 索引標籤會顯示在 Mi Go 用戶端工作列上。 一般使用者可以前往此索引標籤檢視和安裝所屬公司核准的應用程式。 如需更多資訊，請參閱**管理 - Android Enterprise**。

macOS Apps@Work

macOs Apps@work 已整合到 macOS Mobile@Work 用戶端。 裝置註冊到 Ivanti Neurons for MDM 後，用戶端將會切換並顯示為 Apps@Work。 對於新建租戶，Apple App Catalog Webclip 組態不會推送到 macOS 裝置。 必要時，管理員可以將 Apps@work Webclip 組態散發到 macOS 裝置。 如需更多資訊，請參閱**設定 macOS 裝置**。

發佈 macOS app

- Ivanti 透過 Apple MDM 通訊協定和使用 Mobile@Work 應用程式支援 macOS 應用程式發佈。 管理員可選擇使用以下一或兩種方式：
  - Apple 的 MDM 通訊協定 - 管理員只能上傳特定 PKG 格式 (發佈格式) 為內部開發的 app，也可以從 Mac App Store (包含 Apple 的 Apps and Books 授權支援) 發佈 app。 然而，此方式不允許管理員發佈 DMG 和其他 PKG 格式。
  - 適用於 macOS 的 Mobile@Work 應用程式 - 是一種將應用程式散發給使用者的方式，管理員可使用 MobileIron Packager (MIP) 應用程式將任何 PKG、DMG 或 .app 檔案轉換為 MIP 檔案。 將 MIP 檔案上傳至 Ivanti Neurons for MDM 作為內部應用程式

您可以從**軟體下載網站**下載公用程式。

- 管理員可使用 Mobile@Work 以 DMG、PKG 或 .app 格式發佈內部開發的 app。 針對僅在 Mac App Store 提供的應用程式，管理員可繼續使用 Apple 的原生 MDM 功能，包括 Apple Apps and Book 授權功能。 如需更多資訊，請參閱**設定 macOS 裝置**。

Windows Apps@Work

Apps@Work 是一個獨立的原生應用程式，可以從 Microsoft Store 下載，也可以直接從 Ivanti Neurons for MDM 推送。 Apps@Work 可讓您使用 Ivanti Neurons for MDM 中 Windows 10+ 裝置上的 Windows 公用和內部應用程式。 Apps@Work 以無訊息方式自動安裝在支援的 Windows 10+ 裝置上。

如需更多資訊，請參閱**App 配置**。

使用 Windows Apps@Work

Apps@Work 可讓您使用 Ivanti Neurons for MDM 中 Windows 10 裝置上的 Windows 公用和內部應用程式。 Apps@Work 以無訊息方式自動安裝在支援的 Windows 10 裝置上。

Apps@Work 憑證驗證

若要透過 Windows Apps@Work 使用憑證驗證:

1. 前往**管理 > Windows > Apps@Work 憑證驗證**。
2. 將設定切換到**開啟**。

> 將設定切換到**關閉**以強制使用該使用者名稱和密碼。

> Apps@Work for Windows 不支援 SAML。

若要針對 Apps@Work 設定 app：

1. 選擇 Windows 應用程式。
2. 按一下 **App 配置**索引標籤。
3. 按一下**安裝在裝置上**。
   Windows 內部開發的 app 配置可設成無訊息自動安裝旗標或使用 Apps@Work 安裝。 無法將公用應用程式設定為無訊息自動安裝。
4. 或者，選擇在 Apps@Work 目錄中顯示或隱藏應用程式。
   此選項僅適用於內部開發的應用程式。
5. 按一下**推廣**索引標籤。

> Apps@Work 目前不支援橫幅推廣，因此可用選項為**精選**和**非精選**。
>
> **推廣**選項僅針對公用 app 顯示。

8.4. iOS Apps@Work AppStore 功能

Apps@Work 索引標籤具有下列功能:

- 從 Go 應用程式存取 Apps@Work 索引標籤
- 搜尋
- 安裝應用程式 - 按鈕狀態
- 精選應用程式和橫幅
- 應用程式更新通知
- 設定 – 我的裝置

從 Go 應用程式存取 Apps@Work 索引標籤

程序

1. 從 iOS 裝置登入 Go app。
2. 點選 **Apps@Work** 圖示。 兩個預設索引標籤可用 -「所有應用程式」和「類別」。

3. 點選**所有應用程式**索引標籤。 所有應用程式索引標籤按字母順序列出所有應用程式。
4. 點選**類別**索引標籤。 類別索引標籤如下僅顯示其中含有任何應用程式的類別:
    - 每個類別都顯示其中存在的應用程式數量。
    - 「類別」索引標籤下的 MyApps 列是清單項目，其中包含所有已安裝的應用程式。 MyApps 列將始終屬於第一個類別，其餘類別按字母順序列出。
    - 未安裝應用程式時，MyApps 列表顯示「無」。
    - 按一下某個類別後，就會列出專屬該類別的所有應用程式及「安裝」選項。 按一下**安裝**個別安裝每個應用程式，也可以按一下**全部安裝**安裝該類別中的所有應用程式。 系統將詢問是否允許安裝每個應用程式。

搜尋

程序

1. 從 iOS 裝置登入 Go app。
2. 點選 **Apps@Work** 圖示。
3. 點擊搜尋 (透鏡) 圖示搜尋以下內容:
    - **新版本** - 搜尋列中未鍵入任何文字時顯示新發佈的應用程式清單

    - 鍵入任何文字，搜尋欄位將動態預測並顯示相符的應用程式。
    - 搜尋結果計數顯示為子標題
    - 可以點擊**安裝**按鈕安裝應用程式，無需瀏覽至詳細資訊頁面。


安裝應用程式 - 按鈕狀態

由於應用程式安裝需要伺服器處理要求並將應用程式推送到裝置，因此安裝按鈕不會即時顯示進度。 安裝按鈕將依序按「安裝」>「已要求」>「已安裝」變更狀態。

程序

1. 從 iOS 裝置登入 Go app。
2. 點選 **Apps@Work** 圖示。
3. 點選**安裝**，狀態通知顯示如下:
   - 警示訊息第一次出現，表示已要求安裝。
   - 點選「已要求」按鈕。 出現警示訊息。

     > 已安裝狀態並非按鈕。



精選應用程式和橫幅

「精選」索引標籤根據管理員推送的組態顯示。 「精選」索引標籤是無可用更新時的預設登陸頁面。



程序

1. 從 iOS 裝置登入 Go app。
2. 點選 **Apps@Work** 圖示。
3. 點選**精選**索引標籤。
   - 「精選應用程式橫幅」在橫幅中顯示一個應用程式。
   - 「精選應用程式」包含所有精選應用程式的清單。



應用程式更新通知

有任何應用程式更新可用時，一般使用者會在裝置上收到通知。 通知包含有可用更新的應用程式數量。 使用者按一下通知後，Apps@Work 隨即開啟。

程序

1. 從 iOS 裝置登入 Go app。 Apps@Work 圖示顯示有擱置中更新的應用程式計數。
2. 點擊應用程式更新通知，您將被重新導向至 Apps@Work 中的「所有應用程式」索引標籤。 下列指示隨即顯示:
   - 「所有應用程式」索引標籤下的「可用更新」子區段顯示可更新應用程式的計數。
   - 需要更新的每個應用程式都顯示一個紅點圖示。



設定 – 我的裝置

程序

1. 從 iOS 裝置登入 Go app。
2. 點選**設定**圖示。

- 在「設定」下可找到「我的裝置」索引標籤。
- 「我的裝置」現在被列為「身分驗證」下的條項。

8.5. iOS Go 進階功能

機碼值對 (KVP) 是由機碼 (設定名稱) 和值 (您要套用的組態) 組成的簡單應用程式設定。 在 Ivanti Go for iOS 中，組織使用 KVP 來啟用或停用功能並調整應用程式行為，而不需要更新應用程式。

當 Ivanti Go 在組織管理的 iPhone 或 iPad 上執行時，它會在啟動或簽入時讀取這些 KVP 設定。 應用程式會立即套用更新，確保快速、一致地將組態變更傳遞給正確的使用者。

在 Ivanti Go 應用程式組態中使用 KVP

Ivanti Go 應用程式支援用於自訂違規訊息的 KVP。 您可以在 Ivanti Go 應用程式設定中設定 KVP 以自訂應用程式。

程序

1. 在 AppCatalog 中開啟 **Ivanti Go** 應用程式。
2. 選擇**配置**。
3. 按一下**新增**以建立新的 **Apple 應用程式組態**。
4. 手動新增您的 KVP：
    - 在**機碼**欄中，輸入要自訂的組態機碼。
    - 在**值**欄中，輸入要在裝置上強制執行的值。
5. (選用) 上傳包含要套用的預先定義 KVP 的現有 *.plist* 檔案。
6. **儲存**組態。
7. 更新的 KVP 將在下次簽入時套用於裝置。

新增 plist 至特定 iOS 應用程式 (適用於多個機碼值對)

管理員可以使用應用程式序號、套件識別碼、版本詳細資料或其他中繼資料，為 iOS 應用程式設定多個機碼值對 (KVP)。 您可以透過經由 Ivanti Neurons for MDM 控制台上傳 .plist 檔案，有效率地完成此操作。

程序

1. 前往 **App**。
2. 開啟**應用程式目錄**。
3. 選取並開啟您要設定的**特定 iOS 應用程式**。
4. 前往應用程式組態索引標籤。
5. 選取 **Apple 受管理應用程式組態**。
6. 按一下**新增按鈕**。
7. 輸入組態的**名稱**。
8. 按一下**使用 .plist**。
9. 選取**選擇其中一個選項**。
10. 瀏覽到您的 plist 檔案，選取此檔案，然後按一下**開啟**。 系統將自動將 plist 中機碼值對填入組態表。
11. 選擇應接收組態的使用者群組或裝置群組。
12. 按一下**散發此應用程式組態**。

13. 按一下**儲存**以完成程序。

> 上傳的檔案必須具有副檔名 .plist。 如果您手動建立檔案 (例如，在文字編輯器中)，請確保在上傳前將副檔名從 *.txt* 變更為 *.plist*。

在註冊期間以單一應用程式模式啟動 Ivanti Go

此功能可讓管理員在裝置註冊期間使用機碼值對，以在單一應用程式模式 (SAM) 中自動啟動 Ivanti Go for iOS。 裝置開始註冊時，設定的機碼值對會觸發 Ivanti Go，使其立即開啟。 在此程序期間，會對使用者呈現以下訊息：

正在設定您的裝置，請稍候。

若要啟動此行為，在註冊工作流程之前或期間必須安裝單一應用程式模式組態，並明確針對 Ivanti Go for iOS。 註冊成功完成後，會自動結束單一應用程式模式。 然後裝置會釋出給終端使用者進行正常操作，確保安全設定，而不會限制註冊後使用。

此功能支援 Ivanti Mobile@Work 環境，為受監督的 iOS 裝置提供安全註冊流程。

設定 Zero Touch 啟用

若要啟用 Zero Touch Activation for Ivanti Go，請完成下列步驟：

1. 設定僅包含 *Client Registered = No* 的裝置之群組。
2. 為 Ivanti Go 應用程式建立單一應用程式模式 (SAM) 組態。 僅將此組態指派給在*步驟 1*中建立裝置群組。
3. 將 zero_touch_activation 機碼值對 (KVP) 新增至 Ivanti Go 應用程式組態。 鎖定先前步驟中使用的相同裝置群組。

KVP 組態

金鑰	值	類型	描述
zero_touch_activation	True	布林值	當值設為 true 時，Ivanti Go 應用程式會識別其是透過 SAM 組態在單一應用程式模式 (SAM) 中執行。 SAM 組態會啟動 Ivanti Go 應用程式，而此值則作為其他設定，可讓應用程式在 SAM 模式中正確運作。 註冊成功後，裝置會結束單一應用程式模式，並可供一般使用者正常使用。

在 Ivanti Go 中啟用恢復服務按鈕 (iOS 18+)

恢復服務功能可讓裝置在資料清除後自動重新註冊，減少在清除後手動重新註冊裝置的需求。

管理員可以使用可設定的機碼值對 (KVP) 啟用或停用恢復服務按鈕。 在將 KVP 部署到 Ivanti Go 做為應用程式組態的一部分時：

- 終端使用者可以看到恢復服務選項。
- 使用者可以直接從 Ivanti Go 啟動重設處理序。
- 裝置執行 Apple 管理的恢復服務重設。
- 管理設定檔和所需的應用程式保持不變。
- 裝置完成重新佈建流程，並準備重複使用。

Ivanti Go for iOS、iOS 18 及註冊 DEP 模式的更新裝置支援此功能。

KVP 組態

將下列 KVP 新增至 Ivanti Neurons for MDM 中 Ivanti Go 管理的應用程式組態：

金鑰	值	描述
ReturnToServiceEnabled	true	在 Ivanti Go 中啟用**恢復服務**按鈕。 設定為 false 或省略時，功能會保持隱藏狀態。

在 SAML 驗證畫面上停用螢幕擷取畫面保護

Ivanti Go for iOS 內建螢幕擷取畫面保護功能，可在裝置註冊期間增強安全性。 預設情況下，使用 SAML 驗證註冊的畫面會封鎖：

- 螢幕擷取畫面
- 畫面錄製
- 畫面共用

此保護可確保敏感驗證資料 - 例如使用者姓名、密碼和基於 SAML 的登入內容，在未經授權的情況下無法擷取或共用。

管理員可以使用 KVP 組態停用受管理裝置上的螢幕擷取畫面保護。 套用此組態後，Ivanti Go 應用程式將僅允許在 SAML 驗證畫面上進行螢幕擷取畫面和錄製，同時在整個應用程式維持所有其他安全性機制。

KVP 組態

若要停用 SAML 驗證畫面的螢幕擷取畫面保護，請將下列 KVP 套用至 MDM 中的 Ivanti Go 應用程式組態：

金鑰	值	描述
SCREENSHOT_PROTECTION_DISABLED	True	停用 SAML 驗證畫面上的螢幕擷取畫面、畫面錄製和畫面共用保護。 省略或設定為 False 時，保護預設為啟用。

用於自訂原則違規訊息的 KVP

這些 KVP 可讓管理員自訂在偵測到原則違規時傳送給終端使用者的訊息。

這些用於自訂的 KVP 描述了管理員可用於自訂 Ivanti Go for iOS 應用程式行為的 KVP 和違規類型。 這些 KVP 會定義應用程式行為，例如向裝置使用者提供詳細通知，以及從 Ivanti Go for iOS 匯出聯絡人。

違規類型不是相互排斥的。 如果有一組違規，則 Ivanti Go for iOS 中會顯示訊息清單。

機碼值對 (KVP)	預設訊息
compliance.message.COMPROMISED	• 您的裝置已被破解，因此它已遭入侵。 請以正確方式將您的裝置恢復為非越獄狀態，或聯絡您的管理員以尋求解決此問題的協助。
compliance.message.DATA_PROTECTION_DISABLED	• 已停用公司存取權以保護資料。 如需協助您解決此問題，請聯絡您的管理員。
compliance.message.OUT_OF_CONTACT	• 您的 iOS 裝置失去聯絡。 如需協助您解決此問題，請聯絡您的管理員。
compliance.message.APPS	• 您的裝置缺少需要的應用程式，和/或存在不允許的應用程式。 請新增/移除必要的應用程式，或聯絡您的管理員以協助解決此問題。
compliance.message.MDM_DISABLED	• 由於 MDM 功能已停用，因此裝置不符合要求。 請重新註冊您的裝置，或聯絡您的管理員以協助您解決此問題。
compliance.message.ROAMING	
compliance.message.generic	• 公司存取權因未明確的原因已停用。 如需協助您解決此問題，請聯絡您的管理員。
compliance.message.header	由於以下原因，您的裝置不合規： 當違規類型為 CUSTOM 或 CUSTOM_NOTIFY_ONLY 時，系統會顯示不含標題的獨立訊息。
compliance.message.CUSTOM	您的裝置可能需要執行動作。 如有需要，請聯絡您的管理員。
compliance.message.CUSTOM_NOTIFY_ONLY	您的裝置不合規，已傳送通知。 如需詳細資訊，請參閱通知索引標籤或您的電子郵件。

如果違規類型清單未包含任何與對應訊息相符的違規，但包含至少一個沒有對應訊息的違規，則顯示預設訊息：

- 公司存取權因未明確的原因已停用。 如需協助您解決此問題，請聯絡您的管理員。

如果訊息清單包含至少一個違規訊息，請在清單上方顯示下列標題：
由於以下原因，您的裝置不合規：

如果您不想變更預設訊息，請不要對其加入機碼值對 (KVP)。 僅定義您要修改的訊息的 KVP。

使用受管理的應用程式組態設定預設瀏覽器和電子郵件用戶端

鍵值對 (KVP) 可讓管理員設定 **Ivanti Go** 在開啟 web 連結時所使用的瀏覽器和電子郵件用戶端，並透過受管理應用程式組態撰寫電子郵件。

身為管理員，您可以使用受管理應用程式組態 KVP 來控制在**支援**索引標籤中處理連結的方式:

金鑰	值	類型	描述
default_browser	safari, edge, chrome, firefox, brave, opera, webatwork, duckduckgo	字串	瀏覽器 Ivanti Go 用於在支援索引標籤中開啟 web 連結。 http/https 連結已重新導向至設定的瀏覽器方案。 **若未設定，則預設為**系統預設瀏覽器。
Allow_browser_fallback	true、false	布林值	**未安裝預設瀏覽器時的行為**: **True**: 回到預設系統瀏覽器。 **False**: 連結未開啟，使用者看到「<Browser> 未安裝」警示。 **若未設定，則預設為**: True
restrict_log_sharing_to_email	true、false	布林值	記錄/支援共用是否僅限於電子郵件 (使用預設電子郵件)。 自動附加記錄適用於 Email+ 和原生郵件 適用於 **allow_email_fallback**。 **True**: 僅分享到電子郵件。 **False**: 標準共用選項可用。 **如果未設定，則為預設**: false。
default_email	nativemail, outlook, gmail, yahoo, citrixmail.emailplus, spark, protonmail	字串	電子郵件用戶端 Ivanti Go 用於從支援索引標籤中的 mailto 連結編寫郵件。 mailto 已轉換為用戶端撰寫 URL **如果未設定則為預設**: 預設郵件應用程式。 未安裝預設電子郵件用戶端時，連結解析和記錄共用中的雙重角色。
Allow_email_fallback	True、False	布林值	**未安裝預設電子郵件時的行為**。 **正確**: 如果未安裝設定的電子郵件用戶端，電子郵件撰寫會回到預設電子郵件應用程式，而且記錄共用可以使用替代的傳送方式。 **錯誤**: 如果設定的電子郵件用戶端不可用，電子郵件撰寫被封鎖，使用者看到「**未安裝**」警示。 會強制執行記錄共用限制，不會有回退選項。 **如果未設定，則預設為**: true。 (已啟用回退行為)

8.6. 檢視 App 詳細資料

您可以從 App Catalog 向下鑽研至目錄中任何 app 的 app 詳細資料。 在 app 詳細資料頁面中，將會顯示關於 app 的詳細資料，例如顯示版本 (如 1.5.0)、套件版本 (如 1.5.0.42) 和需要的最低作業系統版本 (如 Android 5.0)。

不符合「需要的最低作業系統版本」欄位中指定的版本之 app 不會顯示在 Apps@Work 類別。 因此，您無法將此類 app 發佈至裝置。 「需要的最低作業系統版本」欄位也會顯示在 app 的稽核追蹤中。

程序

1. 按一下 **App**。
2. 按一下 **應用程式目錄**。
3. 選擇 app。

「應用程式詳細資料」視窗隨即出現。

對於 iOS 內部應用程式，可以在應用程式詳細資料頁面上查看**佈建設定檔到期日期**。

應用程式資訊顯示**允許發佈時在 M1 裝置上安裝應用程式**選項，該選項適用於所有 iOS 和 iPadOS VPP 應用程式。 管理員必須僅針對可安裝在 M1 macOS 裝置上的 iOS 或 iPad VPP 應用程式啟用**允許發佈時在 M1 裝置上安裝 App** 選項。 在啟用此選項後，管理員就可在應用程式安裝期間看到 M1 macOS 裝置。 已在 M1 Mac 裝置中支援 iOS VPP 應用程式的受管理應用程式組態。

對於 iOS 和 macOS App Store 應用程式，包括企業對企業，**同步新版本**檢查並從 App Store 同步應用程式更新。 根據應用程式同步排程，更新的應用程式版本會在 12 至 24 小時內顯示。

在裝置詳細資料中會新增一個用於**必要條件 App** 的切換按鈕。 管理員可選擇此選項，並將多個 app 新增為主要 app 的必要條件。

將應用程式發佈到不同裝置後，可以在**裝置摘要**索引標籤下檢視應用程式發佈狀態。 「裝置摘要」索引標籤亦包含有關符合條件裝置數量、已安裝應用程式的裝置數量、待安裝應用程式的裝置數量以及應用程式安裝失敗的裝置數量的資訊。 這些方塊中的裝置計數是根據具有必需應用程式安裝的裝置，因此管理員可以追蹤必要應用程式的初始部署情況。

對於一般應用程式計數 (包括使用者已安裝的應用程式)，請使用「應用程式詳細目錄」搜尋。

從裝置中排除的應用程式具有「待發佈」狀態。

下表列出 iOS / OSX 應用程式安裝失敗的原因:

原因	描述
AppAlreadyInstalled	「已安裝應用程式。」
AppStoreDisabled	「已停用應用程式商店。」
CouldNotVerifyAppID	「無法驗證應用程式 ID。」
失敗	「應用程式安裝失敗，出現不明錯誤。」
ManagedButUninstalled	「此應用程式受控，但使用者已將其刪除。 再次安裝應用程式時 (即使由使用者安裝)，其將再次受控。」
ManagementRejected	「使用者拒絕將非受控應用程式轉換為受控應用程式。」
NotAnApp	「由於無效的應用程式識別碼解析為資產而非應用程式，InstallApplication 指令被拒絕。」
NotSupported	「不支援應用程式。」
Other	「新增錯誤的原因。」
PurchaseMethodNotSupported	「對於 iOS 7 及更高版本，由於購買方式無效 (僅適用於 VPP 應用程式) 而無法安裝應用程式。」
UserInstalledApp	「使用者已在受控應用程式能夠安裝之前安裝應用程式。」
UserRejected	「使用者拒絕了安裝應用程式的提議。」
UpdateRejected	「使用者拒絕了更新應用程式的提議。」

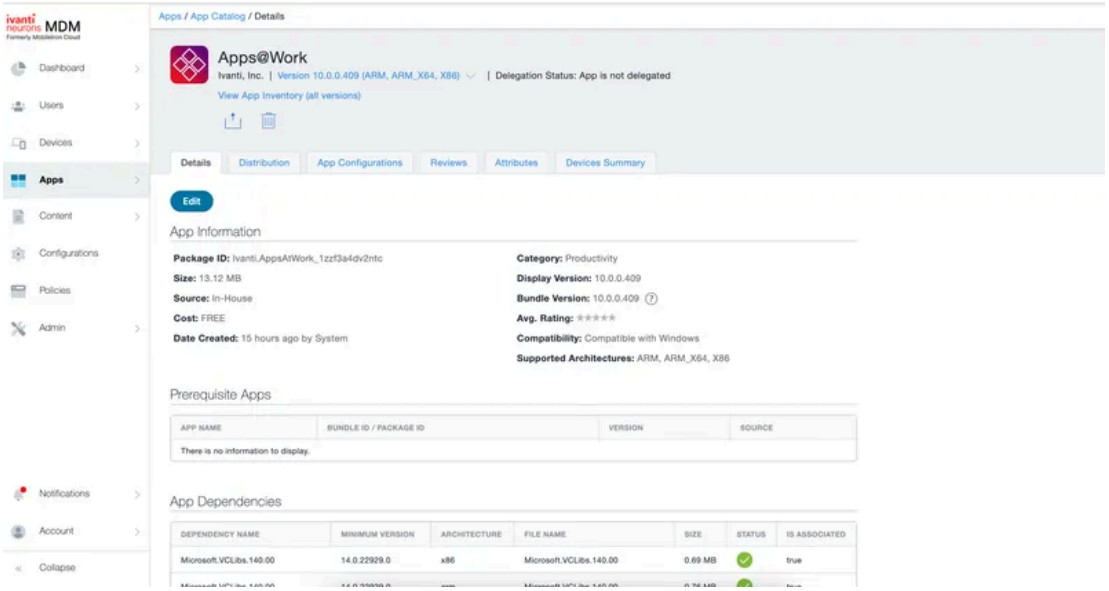
下表列出 Android 應用程式安裝失敗的原因:

原因	描述
USER_INSTALLED	「已安裝在裝置上 (不屬於 MDM)。」
UNSUPPORTED	「不受支援」
USER_REJECTED_INSTALL	「使用者拒絕安裝應用程式。」
ERROR_INSTALL	「嘗試安裝時偵測到錯誤；安裝失敗。」
UNRECOGNIZED	「找不到項目或不再追蹤項目 (例如，錯誤/從裝置中解除安裝並從追蹤中刪除)。」
UNSUPPORTED_INSTALL	「已針對 3.0 Android 用戶端/22.0.0 伺服器進行更新: 必須提供特定狀態以追蹤安裝與解除安裝。」
HIDDEN	「在隔離期間，將傳送 HIDDEN/UNINSTALLED 狀態。 取消隔離應該將其恢復到已安裝狀態。」
OTHER	「新增錯誤的原因。」

對於 Windows 裝置，若應用程式在應用程式組態中設定為無訊息安裝，則「裝置摘要」會顯示此應用程式的符合條件裝置、已安裝裝置、待定裝置或失敗裝置的數量。

從應用程式詳細資訊頁檢視應用程式詳細目錄資訊

若要檢視應用程式詳細目錄資訊，請按一下**檢視應用程式詳細目錄 (所有版本)**，以在**裝置 > 應用程式詳細目錄**中檢視依照該應用程式套組 ID 篩選的清單。



8.7. App 配置

本節包含以下各主題：

- App 功能的授權
- 配置步驟通用於多種 app
- 隱藏和暫止應用程式 (僅限 Android)
- 設定網路轉送
- 設定行動數據 5G 分段
- 使用 Web 內容篩選器組態分發應用程式
- 使用 DNS Proxy 分發應用程式
- 清除 Android Enterprise 裝置的應用程式快取

App 配置可以讓您針對部署於使用者裝置上的應用程式，自訂安裝、推廣與發佈。 此處的應用程式可以是您自己的內部應用程式、來自公開商店的應用程式，或者是 Ivanti Neurons for MDM 應用程式。 您可以彈性部署 app 至許多不同的使用者和群組，並針對每一位接收者指定專屬的唯一名稱和配置。 內部開發應用程式的版本數上限為 100。 如果超過數量上限，Ivanti Neurons for MDM 系統會清除最舊版本的應用程式。 可在「稽核追蹤」頁面檢視應用程式上傳和清除狀態。

> 當您針對 App Catalog 或受管理 app 配置描述檔中的 app 變更其 app 配置時，需要進行一或兩次的裝置登入，裝置才會接收新的配置值。

App 功能的授權

> 下列功能需要額外的授權：

- 無訊息 app 自動安裝/解除安裝：Silver 授權
- 個別 App 配置：Gold 授權
- AppConnect 自訂配置：Gold 授權

多個應用程式套件需要良好的群組管理，因為 Windows 作業系統不會定義未來的裝置類型。 在這種情況下，安裝適當版本 app 的唯一方式就是，管理員使用正確群組搭配正確應用程式。

配置步驟通用於多種 app

先執行這些步驟，然後針對您想要部署的每一個 app 執行其配置步驟。 您可以針對同個 app 設定多種配置，然後為每種配置指定唯一名稱。 每種配置都可以有自己的發佈和推廣層級，以符合您的部署策略。 內部開發應用程式的版本數上限為 100。 如果超過數量上限，Ivanti Neurons for MDM 系統會清除最舊版本的應用程式。 可在「稽核追蹤」頁面檢視應用程式上傳和清除狀態。 一次最多可將應用程式部署到 100 個使用者、使用者群組、裝置或裝置群組。 可以選擇要新增到應用程式目錄的應用程式。 Ivanti Neurons for MDM 具有 iOS 應用程式「傳送安裝/更新要求」命令的非同步程序。 當您使用「傳送安裝/更新要求」命令時，Ivanti Neurons for MDM 管理入口網站會顯示訊息以指示:

- 處理序將繼續在背景中執行
- 處理序完成
- 處理序成功或發生任何錯誤的狀態

程序

1. 前往 **App > App Catalog**，然後按一下 **+新增**。
2. 使用下拉式功能表來選擇 App Store、Google Play 或您內部的 app 商店，然後選擇要新增至目錄的 app。
   視您的授權協議而定，您可能還可以選擇在您的目錄中新增 app。
3. 您可以選擇編輯 app 的類別。
4. 您可以選擇在**描述**欄位中新增 app 的簡短描述。
5. 按**下一步**。
6. 選擇 app 配置的發佈層級：
   - **給所有使用者** - app 將新增至所有的使用者相容裝置。
   - **不給任何使用者** - app 將暫置以供日後發佈。
   - **自訂發佈** - 請選擇下列任一選項：
     - **使用者/使用者群組** - App 將僅發佈給您選擇的使用者或使用者群組。
       按一下**使用者**索引標籤，以選擇使用者。
       按一下**使用者群組**索引標籤，以選擇使用者群組。
     - **裝置/裝置群組** - App 將僅發佈給您選擇的裝置或裝置群組。
       按一下**裝置**索引標籤，以選擇裝置。
       按一下**裝置群組**索引標籤，以選擇裝置群組。
7. 按**下一步**。

設定安裝選項

可以選擇安裝組態選項。

程序

1. 按一下**安裝應用程式配置設定**，或按一下 **+** 圖示，即可新增其他配置以檢視**配置設定**頁面。
2. 在**名稱**欄位中，輸入配置的名稱。
3. 您可以選擇在**描述**欄位中新增安裝配置的簡短描述。
4. 選取**裝置安裝組態**選項。
5. 請選擇下列選項之一：
   - **需要在裝置上安裝**
   - **只在裝置註冊時安裝一次**
6. 選取**不需特定應用程式版本**選項，以免將已安裝的應用程式降級至較低版本。 此選項僅適用於現代化應用程式。
7. 選擇下列選項：
   - **在 Samsung Knox 工作區及 Zebra 裝置上以無訊息方式安裝** (僅限 Android)
   - **在一般使用者的 App 目錄中不顯示 app**。
   - **請勿在新註冊的裝置上安裝應用程式**: 現有裝置將不會受影響，並且仍會在裝置應用程式目錄中顯示該應用程式。
     - 對於此發佈中任何新註冊的裝置，將不會列出或推送該應用程式。
     - 如果管理員觸發傳送安裝/更新命令，則會將該命令傳送到裝置。
   - **延遲應用程式更新時間**: 您可以使用此選項延遲新的應用程式版本安裝。 此設定會根據設定的持續時間，延遲自動安裝新的應用程式版本。

- **應用程式更新模式** (也支援 AMAPI 裝置)。 (僅限 Android)
  使用此選項，利用以下其中一種模式將 app 更新至最新版本：
  - **預設**：在選擇「應用程式更新模式」選項時，會選取此模式。 在此模式中，從有可用的 app 更新起的 24 小時內進行更新。
  - **延遲 90 天**：如果選擇此更新模式，可以將應用程式更新延遲 90 天。 在 90 天後，會根據在受管理的 Google Play 配置中的其他設定自動更新 app。
  - **高優先順序**：如果選擇此更新模式且使用者裝置已連線，則在 Google Play 商店中有可用更新時，會立即更新應用程式。
- **設定應用程式安裝優先順序** - 如需更多詳細資訊，請參閱「設定應用程式優先順序」主題

> 在 Android 裝置上，即使不選擇「無訊息自動安裝」選項，也可以使用「自動更新」選項來更新應用程式。 對於非強制性應用程式或是使用者自行安裝的應用程式，管理員可以控制這些應用程式的更新。

- **應用程式使用中時不更新**: 選取此選項，以防止應用程式在使用者主動使用應用程式時更新。 啟用此選項時:
  - 應用程式在前景中執行時，應用程式更新會延遲。
  - 使用者可以繼續使用應用程式，不會中斷。
  - 應用程式關閉或移至背景時，將自動安裝擱置中更新。

移除發佈時移除應用程式 (Android)
對於受管理的 Google Play 應用程式，當應用程式不再指派給裝置時，Ivanti Neurons for MDM 會自動從 Android 裝置移除應用程式。
在下列情境中，會移除應用程式:

- 應用程式發佈對象變更為「不指派給任何人」。
- 應用程式將從應用程式目錄中刪除。
- 裝置已從應用程式發佈中排除。

依據您所選擇的 app 而定，可能會顯示額外的配置選項。 這些選項可能包含新增多組金鑰和值配對的功能。 在這種情況下，請按一下 **+ 新增**，以輸入金鑰和值對。 如需更多資訊，請參閱「App Catalog「中的**從公開商店新增應用程式**。

9. (macOS 11+) 選擇選項以安裝並將 app 設為受管理的 app：
   - **安裝為受管理的 App**
   - **轉換為受管理的 App**

     > 在 macOS 12.0+，於使用者註冊的裝置上提供受管理的 App 支援。

隱藏和暫止應用程式 (僅限 Android)

對於處於以下模式的 Android 裝置、**工作設定檔**、**完全受管理裝置**、**具有工作設定檔的完全受管理裝置**以及**公司所有裝置上的工作設定檔**，您現在可以在安裝後隱藏或暫止應用程式。

程序

1.	**在要套用「隱藏」或「暫止」動作的裝置上安裝一個或多個應用程式。**
2.	**建立 App Control 組態，並將受管理應用程式新增到隱藏或暫止清單中。**

	3.	**將更改套用至裝置。**

> 如果某個應用程式同時出現在「隱藏」和「暫止」清單中，則該應用程式將被隱藏，因為「隱藏」清單將被優先處理。

設定 app 優先順序

您可定義初次註冊裝置時，會接收到哪些 app (尤其是在註冊日期與時間後前 20 分內) 以及必須推送要安裝的 app。 您可排列 app 下載的優先順序。 例如，將下載 Tunnel 和 Email app 設為優先於其他不重要的 app。 此功能適用於公用與私人 app。 先推送必要條件 app 再推送相依性 app。

iOS (AppStation for iOS 除外)、Android (Android for Enterprise 除外)、macOS (內部 PKG 應用程式以及 Apple 應用程式和 Books 應用程式) 和 Windows 裝置支援此功能。

> 此功能適用於新註冊的裝置。 依預設，所有應用程式均設定為中優先順序。 在此程序中，儘管應用程式將爭奪安裝所需資源，並且可能排在高優先順序應用程式之前，使用者也可以選取手動安裝目錄中的任何應用程式。

> 若是 Windows 應用程式，則 Bridge 應用程式的優先順序高於其他應用程式。

請參閱上節「設定安裝選項」，以瞭解使用**設定 App 安裝優先性**選項設定 app 優先性的程序。 您可以為應用程式設定高、中或低優先順序。 相同優先性的 app 無特定的安裝順序。 當使用者安裝該 app 時，在 app 更新期間，不會使用 app 優先性。

選取 Apple 應用程式管理組態設定

這些設定僅會套用至此 app，並會覆寫在 **App > 目錄設定**中所選的任何全域設定。 選擇 **Apple 應用程式管理**設定。

程序

1. 按一下 **Apple App 設定**，或按一下 **+** 圖示，即可新增其他配置以檢視**配置設定**頁面。
2. 在**名稱**欄位中，輸入配置的名稱。
3. 在**發佈**欄位中，輸入配置的簡短描述。
4. 在 **Apple 管理設定**中選取或取消選取下列其中一個或多個選項:
   - **防止備份至 iCloud 和 iTunes**
   - **移除取消註冊的 App**
   - (iOS 14.0+) **允許移除和卸載此應用程式** - 可取消選取此選項，以防止使用者移除和卸載受管理應用程式。
   - (選用) 新增 **Apple 受管理應用程式組態**
5. 按一下**更新**。

選擇 App 推廣層級

可以為該應用設定推廣層級。

程序

1. 按一下**推廣發佈配置設定**，或按一下 **+** 圖示，即可新增其他配置以檢視**推廣配置**頁面。
2. 按一下**編輯**。
3. 在**名稱**欄位中，輸入推廣發佈配置設定。

4. 您可以選擇在**描述**欄位中新增配置的簡短描述。
5. 選擇您希望 app 接收的推廣層級：**不推薦**、**推薦清單**，或使用**推薦橫幅**。 如果選取**不推薦**，此 app 將不會列出。
6. 如果選取「特色橫幅」，請指定以下詳細資訊:
    1. **標題** - 指定應用程式標題
    2. **說明** - 指定應用程式詳細資訊
    3. **橫幅樣式** - 選取橫幅顏色
7. 按一下 **+新增描述**以輸入配置的簡短描述。
8. 您可以選擇變更配置的發佈。
9. 按一下**完成**以儲存 app 配置。

設定 AppTunnel 流量規則

使用 AppTunnel 配置來定義流量規則以允許使用 Sentry 存取變更為服務。

有關新增 AppTunnel 組態的資訊，請參閱*適用於 Ivanti Neurons for MDM 的 AppConnect 指南* 中的「新增 AppTunnel 組態」。

設定受管理的 App

程序

1. 按一下 **+** 圖示以開啟配置頁面。
2. 按一下 **+新增描述**以輸入配置的簡短描述。
3. 按一下 **+新增**以輸入鍵和值。
4. 選擇發佈層級。
5. 按**下一步**。

使用 Per App VPN 來設定每個 app 的 VPN

程序

1. 按一下 **+** 圖示以開啟配置頁面。
2. 在**名稱**欄位中，輸入此 app 的 VPN 名稱。
3. 按一下 **+新增描述**以輸入配置的簡短描述。
4. 按一下**啟用此 app 的個別 App VPN** 選項，然後選擇一個可用的個別 App VPN 配置。
5. (選用) 針對 macOS app，以 identifier「%s」格式輸入**指定要求**字串。 例如，identifier "com.google.Chrome"。 使用此欄位讓多套件 macOS app 使用個別 App VPN，例如 Tunnel。
6. 選擇如何**發佈此 App 配置**。
7. 按**下一步**。

使用 Apple 受管理 App 配置

使用「Apple 受管理 App 配置」，已安裝的受管理 app 即可設定特定設定。 應用程式可能包含一些由開發人員實作或限制的參數。 對於有此類限制的應用程式，組態選項可能會受到限制。 可以設定 Apple 受管理的應用程式。

程序

1. 前往 **App > 應用程式目錄**。
2. 選取 app。
3. 按一下 **App 配置**索引標籤。
4. 按一下 **Apple 受管理 App 配置**，或按一下 **+** 按鈕。
   在「Apple 受管理 App 配置」中，已有一些預設的配置設定。
5. 按一下**新增**，即可視需要新增其他配置。 您也可以選擇性地按一下配置的名稱，以編輯該配置。
6. 在**配置來源**下方，選擇任一**來源類型**選項

- **AppConfig 社群** - 此選項僅可用於在社群儲存庫中提供 app 配置規格的 app。 如果可用，此選項將預設為已選擇。
- **使用 .xml 規格** - 選擇此選項可上傳 app 的架構檔案，以推送 app 配置的特定版本。 按一下**選擇檔案**來上傳 .xml 檔案。 請確認 .xml 檔案中包含套件 ID 和版本。 如果檔案中的套件 ID 與 app 的套件 ID 不致，將會顯示錯誤訊息。
- **無** - 如果您不想套用 app 的任何架構檔案，請選擇此選項。 如果 **AppConfig 社群**選項無法使用，此選項將預設為已選擇。
  已上傳的 .xml 檔案會顯示在**配置來源**區段中。 按一下刪除圖示即可刪除已上傳的 .xml 檔案。

7. 在 **Apple 受管理 App 設定**中，您可以設定配置選項以輸入索引鍵/值組。

- 按一下**新增**將機碼值組新增到受控應用程式組態，以便在 iReg 或 Apple 裝置註冊期間透過 Go 用戶端擷取註冊名稱識別碼。
  您可以選擇索引鍵/值組的資料類型 (字串、整數、布林值、長浮點數、雙精度浮點數、日期、字串陣列、整數陣列、雙精度浮點數陣列、浮點數陣列、長陣列)。

新增以下索引鍵/值組至受管理 app 配置，以擷取 iReg 或 Apple Device Enrollment 程序期間 Go 用戶端的註冊名稱身份識別。

索引鍵	值	類型
registration.username	$	字串
registration.token	$	STRING
registration.token.expirationSeconds	$	字串
registration.url	$	字串

將以下機碼值組新增到受控應用程式組態，以便在 iReg 或 Apple 裝置註冊期間，透過 Mac 代理程式 (Mobile@Work) 擷取註冊名稱身分識別:

索引鍵	值	類型
用戶端註冊 URL	$	字串
權杖	$	字串
權杖到期時間	$	字串

如果一般使用者終止 Ivanti Go 應用程式，請按一下**編輯**將應用程式設定為執行以下操作之一:

金鑰	值	類型
要顯示預設通知，請使用以下值:		
enableAppTerminationNotification	True/False 或 1/0	布林值或字串
若要顯示自訂通知，請使用以下值:		
appTerminationNotificationMessage	自訂通知	字串
enableAppTerminationNotification	True/False 或 1/0	布林值或字串

- **使用 .plist** - .plist 檔案包含要大量上傳的多個索引鍵/值組。 請按一下**選擇檔案**來上傳 .plist 檔案。 已驗證的 plist 資料將會顯示在 **Apple 受管理 App 設定**表格中。

> 具有巢狀字典的 plist 無效。

8. 按一下**更新**以儲存您的項目。

設定網路轉送

讓您的應用程式網路流量更加私密和安全，且無需連線 VPN。 如需詳細資訊，請參閱**網路轉送組態**。

1. 按一下**網路轉送 + 圖示**以開啟組態頁面。
2. 在名稱欄位中，輸入此應用程式的**網路轉送**名稱。
3. 按一下 + **新增說明**以輸入組態的簡短說明。
4. 按一下此應用程式的**啟用網路轉送**選項，然後選取一個可用的**網路轉送組態**。
5. 選擇如何**發佈**此應用程式組態。
6. 按**下一步**。

設定行動數據 5G 分段

行動數據 5G 網路分段支援可將個別受管理的應用程式 (針對所有 iOS 應用程式) 指派至能提供特定網路功能及特性的網路分段，從而最佳化應用程式體驗。 指派作業使用 MDM 應用程式安裝命令或宣告式應用程式組態中的新 **CellularSliceUUID** 應用程式屬性完成。 要放入金鑰的網路分段字串值需要由支援的行動網路業者來提供。

> 如果特定應用程式或整個裝置設定為使用 VPN，則不會使用 5G 網路分段。

Procedure程序

1. 前往**應用程式 > 應用程式目錄 > 應用程式組態 > 行動數據 5G 分段**，然後按一下**新增**。
2. 在**組態設定**區段下，更新下列欄位:
   - 名稱
   - 選取**啟用 5G 網路分段**選項
   - 選擇 **DNN** 或**應用程式類別** (取決於網路供應商)
3. 選擇 app 配置的發佈層級：
4. 按一下**儲存**。

使用 Web 內容篩選器組態分發應用程式

可以使用 Web 內容篩選器組態來分發應用程式，而不使用 DNS Proxy 伺服器。 建立 Web 內容篩選器組態後，可以將此組態新增到應用程式以進行分發。 關於 Web 內容篩選器組態的更多資訊，請參閱 **Web 內容篩選**。

程序

1. 前往**應用程式** > **應用程式目錄**。
2. 選取 app。
3. 按一下**下一步**。
4. 選取委派選項，然後按一下**下一步**。
5. 選取分發選項，然後按一下**下一步**。
6. 選擇 **Web 內容篩選器組態**，然後按一下 **+** 圖示。
7. 指定**名稱**。
8. 選取**對此應用程式啟用 Web 內容篩選器**核取方塊。
9. 從下拉式功能表中選取 Web 內容篩選器。
10. 選擇 app 配置的發佈層級：
    1. **給所有使用者** - app 將新增至所有的使用者相容裝置。
    2. **不給任何使用者** - app 將暫置以供日後發佈。
    3. **自訂發佈** - 請選擇下列任一選項：
        - **使用者/使用者群組** - App 將僅發佈給您選擇的使用者或使用者群組。
          按一下**使用者**索引標籤，以選擇使用者。
          按一下**使用者群組**索引標籤，以選擇使用者群組。
        - **裝置/裝置群組** - 應用程式僅分發到您選擇的裝置或裝置群組。
          按一下**裝置**索引標籤，以選擇裝置。
          按一下**裝置群組**索引標籤，以選擇裝置群組。
11. 按**下一步**。
12. 按一下**完成**。 選取的應用程式會透過 Web 內容篩選器組態，分發給特定使用者。

使用 DNS Proxy 分發應用程式

可以使用 DNS Proxy 組態來分發應用程式。 建立 DNS Proxy 組態後，可以將該組態新增到應用程式以進行分發。 如需關於 DNS Proxy 組態的更多資訊，請參閱**建立 DNS Proxy 組態**。

程序

1. 前往**應用程式** > **應用程式目錄**。
2. 選取 app。
3. 按一下**下一步**。
4. 選取委派選項，然後按一下**下一步**。
5. 選取分發選項，然後按一下**下一步**。
6. 選擇 **DNS Proxy 組態**，然後按一下 **+** 圖示。
7. 指定**名稱**。

8. 選取**對此應用程式啟用 DNS Proxy** 核取方塊。
9. 從下拉式功能表中選取 DNS Proxy。
10. 選擇 app 配置的發佈層級：
    1. **給所有使用者** - app 將新增至所有的使用者相容裝置。
    2. **不給任何使用者** - app 將暫置以供日後發佈。
    3. **自訂發佈** - 請選擇下列任一選項：
        - **使用者/使用者群組** - App 將僅發佈給您選擇的使用者或使用者群組。
          按一下**使用者**索引標籤，以選擇使用者。
          按一下**使用者群組**索引標籤，以選擇使用者群組。
        - **裝置/裝置群組** - 應用程式僅分發到您選擇的裝置或裝置群組。
          按一下**裝置**索引標籤，以選擇裝置。
          按一下**裝置群組**索引標籤，以選擇裝置群組。
11. 按**下一步**。
12. 按一下**完成**。 選取的應用程式會透過 DNS Proxy 組態，分發給特定使用者。

複製應用程式組態設定

可以複製受管理應用程式的組態設定，相同的設定便可套用在其他裝置上。 甚至可以重新命名並對複製的設定做一些變更。

Android

可以複製 Android 裝置上的「組態設定」。

程序

1. 前往 **App > 應用程式目錄**。
2. 選擇要從中複製組態設定的應用程式。
3. 按一下 **App 配置**。
4. 在**應用程式組態摘要**章節下，可找到適用於 Android 裝置的組態清單 (**適用於 Android 的受管理組態**、**安裝在裝置上**、**推廣**、**已委派裝置權限**，以及**Google Play 版本**)。
5. 在任何一個可用的組態上按一下。
6. 在**動作**下，按一下**複製**，開始複製流程。
7. 在預設情況下，複製的組態名稱會是 <Copy of the Cloned Configuration name>。 不過，可以透過在**名稱**方塊中輸入所選擇的名稱來修改名稱。
8. (選填) 在**描述**方塊中輸入關於所複製設定的一些文字。
9. 按一下**繼續**。

出現一個確認視窗，指出複製該應用程式組態設定已完成。 可以在「應用程式組態摘要」下及所複製的應用程式內查看複製版本。

iOS

可以複製 iOS 裝置上的「受管理應用程式組態設定」。

程序

1. 前往 **App > 應用程式目錄**。
2. 選擇要從中複製組態設定的應用程式。

3. 按一下 **App 配置**。
4. 在**應用程式組態摘要**章節下，可以找到適用於 iOS 裝置的組態清單 (**安裝在裝置上**、**Apple 應用程式設定**、**推廣**、**AppConnect 自訂組態**、**App Tunnel**、**Apple 受管理應用程式組態**，以及 **Per App VPN**)。
5. 在想要複製的所需組態上按一下。
6. 在**動作**下，按一下**複製**，開始複製流程。
7. 在預設情況下，複製的組態名稱會是 <Copy of the Cloned Configuration name>。 不過，可以透過在**名稱**方塊中輸入所選擇的名稱來修改名稱。
8. (選填) 在**描述**方塊中輸入關於所複製設定的一些文字。
9. 從**來源類型**清單中選擇一個組態來源。
10. 在 **Apple 受管理應用程式設定**區段下，輸入**金鑰**、**值**，然後從清單中選擇**類型**。
    有關**金鑰**、**值**及**類型**的資訊，請參閱**使用 Apple 受管理應用程式組態**。
11. 按一下**繼續**。
    出現一個確認視窗，指出複製該應用程式組態設定已完成。 可以在 **Apple 受管理應用程式組態**章節中查看複製版本。

Windows

可以複製在 Windows 裝置上的「應用程式組態設定」：

程序

1. 前往 **App > 應用程式目錄**。
2. 選擇要從中複製組態設定的應用程式。
3. 按一下 **App 配置**。
4. 在**應用程式組態摘要**章節下，可以找到**安裝在裝置上**及**推廣**組態。
5. 在想要複製的所需組態上按一下。
6. 在**動作**下，按一下**複製**，開始複製流程。
7. 在預設情況下，複製的組態名稱會是 <Copy of the Cloned Configuration name>。 不過，可以透過在**名稱**方塊中輸入所選擇的名稱來修改名稱。
8. (選填) 在**描述**方塊中輸入關於所複製設定的一些文字。
9. 按一下**繼續**。

出現一個確認視窗，指出複製該應用程式組態設定已完成。 可以在「應用程式組態摘要」下及所複製的應用程式內查看複製版本。

為您的內部開發目錄選擇 Windows 10 app

選擇要新增至內部開發目錄的 app 內部、Microsoft Store 以及 Microsoft for Business 應用程式支援 Windows 10 。 Windows 10 會根據您允許或不允許 app 的選擇，直接在裝置上強制執行相符性功能。

> Windows 10 的登記間隔預設為每 60 分鐘一次。 您可能想執行強制裝置登記，以進行裝置更新並掌握 app 的狀態。

系統支援下列動作：

- 上傳新的 app
- 無訊息自動安裝
- 從 Apps@Work 手動安裝

- 加入新版本的 app
- 刪除 app

系統支援下列格式：

- APPX
- APPXBUNDLE
- MSI 封裝的 Win32 - 預先配套的 Win32 app
- MSIX (RS5 和上述 Windows 10 裝置可支援)
- .EXE (使用橋接)

> 針對 **Windows** 裝置，**Ivanti Neurons 代理程式**應用程式於**應用程式目錄**提供。 管理員可將 **Ivanti Neurons 代理程式**應用程式部署為內部應用程式，並在 Windows 裝置上據此發佈該應用程式。

設定 Windows 10 應用程式

程序

1. 按一下主導覽列上的**裝置**。
2. 選擇已在 Ivanti Neurons for MDM 中註冊的 Windows 10 裝置。
3. 按一下**應用程式 > 應用程式目錄**。
4. 選取 app。
5. 使用**動作**下拉式功能表，在目錄中新增或刪除應用程式。
   您也可以選擇加入新版的 app。
   - 按一下**動作**下拉式功能表。
   - 選擇**新增版本**。
   - 前往目錄並選擇新版的 app。
   - 按一下**更新並儲存**，檢視應用程式資訊畫面。
6. 使用**版本**下拉式功能表，選擇要使用的版本。
7. 按一下**編輯**開始更改詳細資料。
   - 必要時編輯**類別**。
   - 必要時輸入**說明**。
   - 視需要新增螢幕擷取。
8. 按一下**儲存**。
9. 按一下**發佈**索引標籤，然後按一下**編輯**開始更改發佈層級。
10. 按一下**儲存**。
11. 按一下**應用程式組態**索引標籤，檢視目前組態的摘要。
12. 視需要輸入 app 的描述。
13. 按一下「應用程式組態」摘要頁面中的**安裝在裝置上** 。
    預設為無訊息自動安裝，且無法變更。
14. 按一下左側導覽窗格中的**推廣**，然後再按一下**推廣發佈組態設定**，更改推廣層級。

- 按一下**編輯**，更改推廣層級設定。
- 輸入配置的名稱。
- 輸入配置的描述。
- 選擇發佈層級。
- 按一下**更新**以儲存您的變更。

15. 按一下**評論**索引標籤，檢視有關評論的資訊。
    視需要將評論資料匯出至試算表。

編輯 Windows 10 app 配置設定

程序

1. 按一下**原則 > 組態**。
2. 按一下**+新增**。
3. 選擇 **Windows 應用程式控制**，檢視**建立 Windows 應用程式控制組態**畫面。
4. 輸入組態的**名稱**和**描述**。
5. 將 app 類型定義為：
   - 允許 (列入允許清單) - 僅允許這些 app。 如果裝置上未具備這些 app，則會以無訊息方式自動安裝。
   - 不允許 (列入封鎖清單) - 如果裝置上有此設定，啟動這些 app 時會將其封鎖。
6. 針對「App 類型」和「App 識別碼」，指定「規則」定義。
7. 按一下**查詢應用程式**，檢視**搜尋 Windows 10 應用程式**畫面。
8. 輸入 app 的名稱以在 Windows 市集中進行搜尋。
9. 從顯示的選項中選擇 app，並將其新增至「App 識別碼」。
10. 您也可以使用「App 類型」下拉式功能表，在「App 識別碼」中設定允許或不允許使用特定路徑的 app 路徑定義，或封鎖所有在該路徑中安裝的所有 app。
    應用程式類型**發行者/PFN 等於**套用於 Windows 10+ 裝置，且支援 PFN。 **EXE/Win32 等於**。
11. 按一下**下一步**。
12. 選擇發佈層級。
    - **所有裝置**。
    - **沒有裝置**。
    - **自訂** - 輸入要接收 app 的使用者或群組。
13. 按一下**完成**。
14. 您可以編輯「規則」定義，以選擇「App 類型」並指定「App 識別碼」。
    - 按一下**動作**下拉式功能表。
    - 選擇**新增版本**。
    - 選擇新版本的 app。
    - 按一下**更新並儲存**，檢視**應用程式資訊**畫面。

設定 Windows 的「安裝後重新啟動裝置」選項

您可以使用**安裝後重新啟動裝置**選項，設定裝置在應用程式安裝完成後重新啟動。

程序

1. 前往 **App > 應用程式目錄**。
2. 從清單中選取 Windows 特定應用程式。
3. 前往**應用程式組態 > 在裝置上安裝 > 安裝應用程式組態設定**。
4. 按一下**編輯**並將**安裝後重新啟動裝置**設為「開啟」。
5. 選擇下列要重新啟動之裝置的排程選項之一:

設定	方法
安裝後立即	選擇此選項可在安裝應用程式後立即重新啟動裝置。
在一天中的特定時間	選擇此選項可在安裝應用程式後，在一天中的特定時間重新啟動裝置。
幾分鐘後	選擇此選項可在安裝應用程式的 **15**、**30**、**60** 或 **120** 分鐘後重新啟動裝置。

6. 按一下**更新**。

裝置將會在排程時間重新啟動。

> 如果是公用應用程式與商務用 Microsoft Store (MSB) 應用程式，您需要在**應用程式組態**區段中開啟**無訊息自動安裝在 Windows 裝置上**設定。

若要使用 Apps@Work 安裝 app

若要使用 Apps@Work 安裝 app：

1. 按一下 **Apps@Work** 應用程式。
   您的管理員電子郵件地址和伺服器 URL 會預先填入 Apps@Work 登入對話方塊中。
2. 輸入您的密碼，然後按一下「登入」，以顯示 app 頁面。
3. 選擇要安裝的 app。 您將無法安裝與必要條件 app 具有相依關係的 app (如果必要條件 app 尚未安裝在用戶端上)。
   若是適用於 iOS 裝置的 Apps@Work，您可選擇性按一下**全部安裝**按鈕以安裝所有的 app。 在**新版本**、**精選 App** 及**類別**等畫面中可使用此選項。

> 如果之前未接受 Apps and Books app 授權，將不會安裝 Apps and Books app。

4. 按一下**更新並儲存**，檢視**應用程式資訊**畫面。

Android Enterprise 裝置的應用程式安裝和更新

管理員可以將應用程式發佈到目錄以進行常規存取，同時將其部署到特定裝置以供立即使用。 這允許使用者直接接收應用程式，同時它也可以在目錄中供其他人根據需要安裝。

安裝應用程式和更新

1. 瀏覽至**應用程式 > 應用程式目錄**。
2. 選擇您要的應用程式:
3. 按一下**詳細資訊**螢幕上的**動作**。 **傳送安裝/更新要求**顯示。

4. 按一下傳送安裝/更新要求。 **傳送安裝/更新要求**對話方塊顯示。
5. 在**向此應用程式的裝置傳送安裝和更新通知**下執行以下操作:
    - 選取**發送新應用程式要求 (適用於尚未安裝該應用程式的裝置)** 核取方塊以安裝新應用程式。
    - 選取**傳送更新要求 (適用於已安裝應用程式但有更新可用的裝置)** 核取方塊以更新已安裝的應用程式。
6. 在**選擇要發送要求的使用者**下執行以下操作:
    - 按一下**所有人**可將組態發佈給所有相容使用者。 應用程式出現在它們的應用程式目錄中。
    - 按一下**自訂**以定義在應用程式目錄中看到應用程式的使用者群組或使用者。

> **傳送安裝/更新要求**發佈是應用程式發佈過程的一部分。 您在**發佈**螢幕上選擇的設定決定了哪些裝置將接收該應用程式。

出現一個確認視窗，指出應用程式的安裝已完成。

源自新安裝或更新的更改顯示在**儀表板** > **稽核追蹤**中。

> 對於公用和私用應用程式，已禁用**傳送更新要求 (適用於已安裝應用程式但有更新可用的裝置)**。 只允許**傳送新應用程式要求**。

相關主題：

- 「App Catalog」

清除 Android Enterprise 裝置的應用程式快取

清除應用程式快取請求可讓管理員遠端清除使用 Ivanti Neurons for MDM 安裝在 Android Enterprise 裝置上的所選應用程式的快取資料。 此動作有助於解決常見的應用程式問題，例如效能緩慢、意外錯誤或過期的暫存資料，而無需解除安裝或重新安裝應用程式。 請求僅清除應用程式快取並保留使用者資料、應用程式設定和組態。 管理員使用此功能可快速恢復正常應用程式行為，同時將對一般使用者的干擾降至最低。

程序

1. 瀏覽至**應用程式** > **應用程式目錄**。
2. 選取並開啟應用程式。
   應用程式**詳細資料**頁面隨即顯示。
3. 按一下應用程式**詳細資料**上的動作功能表 (⋮)。
4. 選取**清除應用程式快取請求**選項。
   清除應用程式快取請求窗格隨即出現。
5. 在**選取要傳送請求的使用者**區段中執行下列其中一個動作，以發佈應用程式快取清除請求:
    - 選取**每個人**，將請求傳送至已安裝應用程式的所有相容裝置。
    - 選取**自訂**將請求傳送至特定使用者、使用者群組、裝置或裝置群組。
6. (選用) 在**其他分發篩選選項**下搜尋現有的分發清單。
7. (選用) 選取 **+ 新增分發篩選**，以在**建立分發篩選**窗格中建立分發篩選。

> 使用此選項可將**清除應用程式快取請求**傳送至特定裝置集，例如 DO 或 EPO 模式裝置。

8. 按一下**傳送**。
9. 按一下**清除應用程式快取**確認對話方塊中的**確定**。
   Ivanti Neurons for MDM 會顯示通知，列出接收**清除應用程式快取請求**的裝置數量。

完成**清除應用程式快取**請求後，所有應用程式詳細資料 (版本、名稱、platformAppId、displayVersion 和 bundleVersion) 都會記錄在**稽核追蹤**頁面。

8.8. 將自訂屬性指派給應用程式

建立自訂屬性後，即可將其指派給一個或多個應用程式。 每個屬性都有一個對應值，可用於建立應用程式群組等任務。 如需關於管理屬性的詳細資訊，請參閱**屬性**。

為個別應用程式建立和指派自訂屬性

您可以將自訂屬性指派給單一應用程式。

程序

1. 登入管理入口網站。
2. 瀏覽至**應用程式** > **應用程式目錄**。
3. 選取一個應用程式，然後按一下**屬性**。
4. 按一下 **+新增**從**屬性名稱**下拉式功能表中選取一個值。
5. 在**值**欄位中指定屬性值。
6. 按一下**儲存**。 自訂屬性即新增至應用程式中。

將自訂屬性指派給多個應用程式

您可以將自訂屬性指派給一個或多個應用程式。 選取多個應用程式時，自訂屬性將套用於應用程式的每個版本。 您可以選取特定的應用程式，前往「屬性」索引標籤，然後為特定的應用程式版本變更自訂屬性詳細資料。

程序

1. 登入管理入口網站。
2. 瀏覽至**應用程式** > **應用程式目錄**。
3. 選取一個或多個應用程式的核取方塊。
4. 按一下**動作**。
5. 選取**指派自訂屬性**。 「將自訂屬性指派給應用程式」精靈隨即出現。
6. 選取下列其中*一個*選項:
   - 即使有找到任何既有的值，仍要強制指派 (覆寫) 所有屬性。
   - 僅限值為空白時才覆寫，並略過具備現有值的屬性。
7. 選取一個或多個屬性的核取方塊。
8. 在「值」欄位中指定值 (不允許空白值)。
9. 按一下**指派**。 自訂屬性將指派給所選應用程式的所有版本。
10. (選填) 若要變更單一應用程式版本的自訂屬性，請從版本下拉式清單中選取應用程式版本，然後按一下「編輯」。

> **自訂應用程式屬性**及其值可用於從**裝置詳細資料**頁面建立報告，並匯出為 CSV 格式。

8.9. Android 受管理的配置

本節包含以下各主題：

- 使用 Android Enterprise 受管理配置
- 適用於內部應用程式的應用程式限制與權限
- 使用 Android Enterprise 設定 Gmail

如果 Ivanti Neurons for MDM 已啟用 Android Enterprise，即可針對個別應用程式使用 Android Enterprise 組態。

使用 Android Enterprise 受管理配置

1. 按一下 **App**。
2. 按一下 **應用程式目錄**。
3. 選擇要設定 Android Enterprise 配置的 app。
4. 按一下 **App 配置**。
5. 按一下 **Android 受管理的配置**。
6. 提供配置的名稱。
7. 您可以選擇性地提供描述。
8. 使用「受管理的配置」欄位來設定受管理的配置行為：
9. 使用**通道組態設定**將通道應用程式直接與適用於 Android 裝置的 Ivanti Go 應用程式整合。 選取**啟用通道組態**選項以套用此設定。 透過此增強功能，管理員可以透過 Ivanti Go 啟用通道功能，並使用現有的通道組態設定安全連線。 功能適用於新註冊的 Android 裝置。 為確保無縫轉換，將繼續支援獨立通道應用程式。 不過，安裝獨立通道應用程式的裝置不會在 Ivanti Go 中顯示整合的通道體驗。 移除獨立通道應用程式後，Go 應用程式將可使用整合的通道功能。 一次只能將一個通道組態套用至裝置。

設定	描述
讓 app 無法跨描述檔共用小工具	啟用時，可封鎖 app 使其不能跨描述檔共享小工具 (僅有當 app 不是無訊息自動安裝的情況除外)。 保持停用時，可讓部署於 Android Enterprise 描述檔中的受信任 app 在主畫面上顯示小工具，以便使用者不需登入即可存取資訊。
使用者無法解除安裝 app	啟用此功能可阻止使用者在 Ivanti Neurons for MDM 靜默安裝應用程式後卸載應用程式 (公用、私人或內部)。
最低版本代碼	設定 app 覆寫預設更新行為所需的最低版本代碼。 如果目前安裝在裝置上的 app 版本代碼低於最低版本代碼，會將 app 立即更新至最新版本。
安裝時自動啟動	如果您要在安裝後自動啟動 app，請選擇此選項。 此功能僅適用於剛安裝在裝置上的 app，而非版本更新的 app。 針對工作描述檔和公司擁有裝置上的工作描述檔，Go app 應已啟用並在前景執行。 受到 Android 10+ 的限制，針對工作描述檔和公司擁有裝置上的工作描述檔，如果使用者推送多個 app，僅會自動啟動一個 app。

10. 管理員可控制可傳送至裝置或不應傳送的應用程式組態欄位。 一般來說，將組態推送至不同裝置時會設定預設值。 在「受管理組態」區段的**推送至裝置**設定中，選取**推送全部設定**或**僅推送已定義值的設定**。

受管理的組態

每個 Android Enterprise app 配置都會針對每個文字欄位顯示憑證功能按鈕，按一下按鈕時，文字欄位會被下拉憑證清單取代。 進行設定時，這些認證會無訊息自動套用，不會有任何使用者互動。

按一下欄位旁的相同按鈕，即可將現有的憑證型欄位變更為文字型。 對於已變更為憑證型欄位的文字型欄位，按一下相同按鈕即可變回文字型欄位。 (預設的下拉欄位無法變回文字型欄位)。

> 如果租戶未設定任何 ID 憑證，使用憑證功能按鈕從文字切換到下拉時，下拉清單中只會顯示「無」選項。

按一下**管理權限**，以選取並設定針對 API 23 (或更新版本) 及 Android 6.0+ 所建立之應用程式的執行時期權限。

其中僅列出會對特定應用程式造成危險的權限，供您選擇。
https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups 上列出了危險權限的完整清單 (例如讀取聯絡人、尋找裝置上的帳戶、寫入通話記錄等等)。

11. 您可以指派給每個權限的權利包括：
    - 僅有當應用程式要求權限時，才會套用這些權限。
    - 如果使用者之前已接受或拒絕權限，就不會套用這些權限。
    - 自動授與
    - 自動拒絕 (請小心使用此選項)
    - 預設/全域

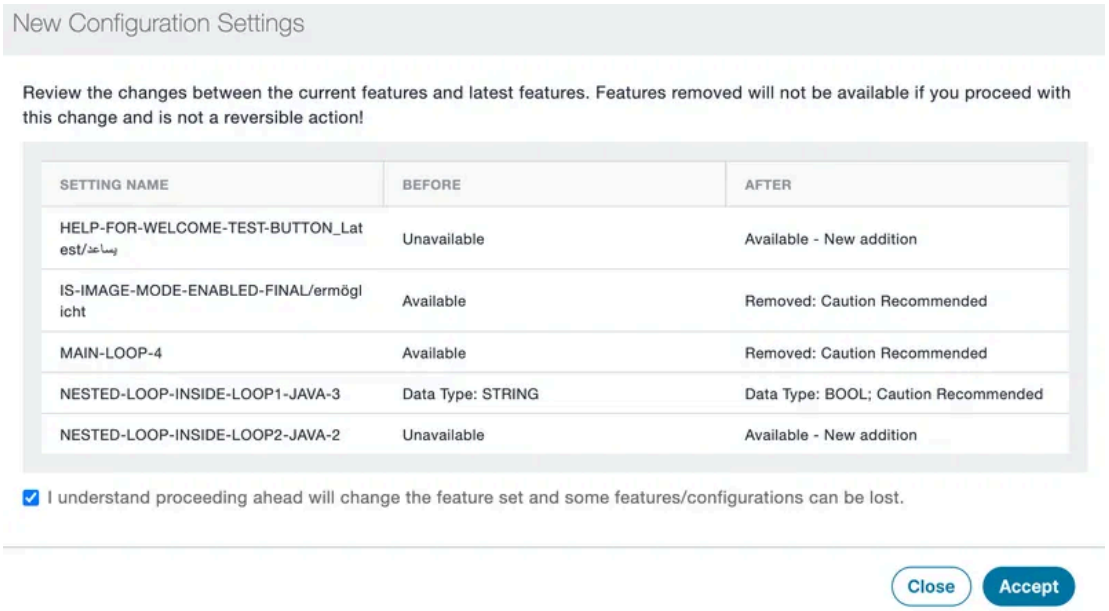
選擇**有此 App 的每個人**、**沒有人**或**自訂**，以設定發佈選項。

12. 按一下**儲存**。

新組態設定

當應用程式版本更新或現有組態發生任何變更時，**更新至最新功能**按鈕會在編輯「組態詳細資料」頁面之後出現。

1. 按一下**更新至最新功能**。
   螢幕上會出現警告訊息，指出切換為最新功能會讓使用者無法存取舊版應用程式。 警告訊息會建議順暢整合最新版應用程式的步驟。
2. 按**下一步**。
3. 畫面上會出現**新組態設定**視窗。



新組態設定視窗會列出組態中現有的不同設定，以及更新後每個設定的狀態。 「新組態設定」視窗會列出資料庫中的所有限制，Google 結構描述將列出以下狀態:

- 已新增
- 已移除
- 已修改

選取核取方塊，然後按一下**接受**以繼續進行更新。
螢幕上會出現確認訊息，指出組態已成功更新且包含最新功能。 現在您可以發佈並儲存組態，以便讓變更生效。

適用於內部應用程式的應用程式限制與權限

管理員可以針對內部應用程式設定某些應用程式限制，以及限制內部應用程式的權限或向其授予權限。 此功能原本僅適用於公用應用程式， 但現在該功能已擴展到適用於內部應用程式。

> 管理員必須重新上傳內部應用程式，使**應用程式限制**與**權限**功能在其應用程式上變為可用。 建議您在上傳新版本前，先刪除現有的應用程式。

程序

1. 前往**應用程式** > **應用程式目錄**。
2. 從清單選取**內部**應用程式。
3. 按一下 **App 配置**。
4. 按一下**適用於 Android 的受管理組態**。
5. 按一下**新增**。
6. 畫面上將會出現**應用程式限制**區段。
   輸入可用限制所需的值。
7. 選取**管理權限**。

8. 畫面上將會出現**選取權限**視窗。
   從清單中選取所需的權限，然後按一下**選取**。
9. 在**執行階段權限**區段下，設定所選權限的值。
10. 在**發佈此應用程式組態**區段底下，選擇下列其中一個**應用程式發佈**選項:
    - **有此 App 的每個人**
    - **沒有人**
    - **自訂**
11. 按一下**儲存**。
    所選限制與權限將會套用在內部應用程式上。

使用 Android Enterprise 設定 Gmail

如果您已為 Android Enterprise 設定 Ivanti Neurons for MDM，就可將 Gmail 部署至 Android Enterprise 裝置。 使用 Android Enterprise 設定 Gmail

1. 前往 **App > 應用程式目錄**。
2. 選擇要設定 Android Enterprise 配置的 Gmail app。 這時會顯示「配置設定」區段。
3. 提供配置的名稱。
4. 您可以選擇性地提供描述。
5. 使用**受管理的配置**欄位來設定受管理的配置行為：

> **全部展開**和**全部摺疊**選項僅適用於巢狀或階層限制。

設定	描述
推送至裝置	推送所有設定 - 選取此選項以啟用所有切換，包括無任何值的切換 僅推送已定義值的設定 - 選取此選項以啟用所有已定義值的切換，並針對不含任何值的設定停用切換 在大部分的情況中預設設定已經可用。 不過，管理員可選取必要的應用程式組態設定或編輯必須傳送至裝置的變數。
電子郵件地址	輸入替換變數以定義電子郵件地址。 通常，您輸入 $emailaddress$。 UEM 可使用此欄位從 Active Directory 提取使用者憑證。
主機名稱或主機	輸入 Active Sync 伺服器的主機名稱，例如主機名稱.公司.com:443/路徑。
使用者名稱	利用使用者的 Active Directory 使用者名稱的變數，它可指定為直接使用者名稱 (janedoe) 或範本化值 ($username$)。
驗證類型	選擇包含允許驗證類型的字串清單。
需使用 SSL	選取後，會啟用 SSL 並要求在與主機名稱一起使用的連接埠號上使用它。
信任所有憑證	僅當您想讓應用程式自動接受不受信任的認證時，才選擇此選項。 只有在測試環境中工作時，才使用此選項進行偵錯或開發。
登入憑證別名	輸入用於驗證 ActiveSync 伺服器的登入憑證別名。
允許未受管理的帳戶	選擇此選項，可讓使用者新增或移除在此受管理的組態中指定的帳戶以外之任何 Exchange 帳戶。
預設電子郵件簽名	輸入包含預設電子郵件簽名的字串，此簽名會附加至所有外寄電子郵件文字的最下方。
預設同步視窗	輸入 0-5 之間的值，代表與 EAS (Exchange Active Sync) 同步的時間間隔。

按**下一步**。

7. 選擇**有此 App 的每個人**、**沒有人**或**自訂**，以設定發佈選項。
8. 按一下**儲存**。

8.10. 管理 Google Play app

您可定義應為特定群組或個人部署 Google Play app 的哪個二進位檔。此部署適用於 Android enterprise部署。 App 開發人員還必須將您的組織列入允許清單，這樣才能部署 Alpha 或 Beta 通道 app。

1. 按一下 **App**。
2. 在 **App Catalog** 中，選擇要為其設定 Google Play 發行版本配置的 app。
3. 按一下 **App 配置**索引標籤。
4. 按一下 **Google Play 發行版本**。

> Google 發行版本配置僅適用於 Android Enterprise app。 如果未針對新增的 app 選擇 Google 發行版本配置，將預設使用「生產」選項。

按一下**新增**。

6. 提供配置的名稱。
7. 您可以選擇性地提供描述。
8. 從下拉式清單選擇選項，以挑選提供給接收此 app 之使用者與裝置使用的二進位檔。 選項包括：
   - 生產
   - Alpha
   - Beta

   > 對於已推送到裝置的 app，預設套用生產選項。
9. 選擇**有此 App 的每個人**、**沒有人**或**自訂**，以設定發佈選項。
10. **自訂**會在使用者群組中發佈 app 並進行裝置篩選。
    按一下**儲存**。

優先排序多個發行版本配置

若新增多個 Google 發行版本配置，您可以安排 Google 發行版本配置的優先套用順序。

1. 在 **App 配置**中，按一下**優先排序配置**。

> 只有在出現多個配置時才會顯示此按鈕。

從列出的配置中，拖放清單中應最優先套用的配置。

3. 按一下**更新**。

> 當最優先的配置遭到刪除，這時次優先的配置就變成最優先。

8.11. 從 App Catalog 刪除 App

您可以從應用程式目錄中刪除公用 app 與內部開發的 app。 您無法刪除必要條件 app。 在刪除這類 app 之前，您需要先編輯 app 以移除必要條件關係。 如果裝置上已安裝 app，下次這些裝置登記時就會將此 app 從裝置上移除。 「裝置管理員」模式下的 Samsung 和 Zebra 裝置或「裝置擁有者」模式下的所有裝置，支援無訊息的應用程式自動安裝/解除安裝。

若是內部應用程式，則螢幕上出現一個確認視窗。 需要選取繼續執行「刪除」操作的確認，然後按一下**刪除應用程式**。 嘗試刪除多個應用程式但無法刪除其中的某些應用程式時，螢幕上將出現一個視窗，其中包含無法刪除的應用程式及其原因的相關資訊。

嘗試從應用程式目錄中刪除一個或多個應用程式時，以下條件適用:

- 若無法刪除內部應用程式的某一個版本，則無法刪除該應用程式的任何版本。
- 若內部應用程式的某一個版本是必備應用程式，則無法刪除該應用程式，也無法刪除該應用程式的任何版本。
- 選取全部或部分內部應用程式欲將其從應用程式目錄中刪除時，所選取內部應用程式的所有版本都將被刪除。
- 無法刪除從「空間」委派的內部應用程式。

程序

1. 前往 **App > 應用程式目錄**。
2. 按一下 app 的連結。
3. 選擇**動作 > 從目錄中刪除**。
4. 詳細閱讀刪除 app 的後果警告。
5. 此警告說明 Apps and Books 授權 (iOS) 和 App 評論 (所有作業系統) 也會一併刪除。
   選取「我瞭解刪除應用程式的後果」核取方塊，以繼續執行刪除操作。
6. 按一下**刪除 App**。

8.12. 升級內部開發的 App

使用以下程序來更新內部開發的 app：

1. 前往 **App > 應用程式目錄**。
2. 選擇要升級的 app。
3. 選擇**動作 > 新增版本**。
4. 將 app 拖曳至**上傳 App** 區域，或按一下**選擇檔案**，從檔案系統中進行選擇。
5. 依據您想對舊版 app 執行哪個動作，選擇下列其中一個選項：
   - **讓描述、畫面擷取、發佈、app 必要條件及 app 配置保持一致：**在 App Catalog 中取代舊版。
   - **變更描述、畫面擷取、發佈、app 必要條件或 app 配置**：在 App Catalog 中存在兩種版本。
6. 在**新功能**下方，輸入文字以向使用者說明新版有何不同。
7. 當使用者選擇安裝 app 時，裝置上即會顯示這段文字。
   如果您選擇要變更描述、畫面擷取和發佈選項，請完成相關變更。
8. 按一下**完成**。

如果您選擇要保留目錄中的舊版 app，**App > 應用程式目錄**下方僅會顯示一個項目。 最左側窗格會依據項目指出 app 的數量。 如果您之後決定要刪除新版，已安裝裝置上就會自動將新版取代為舊版。

顯示 app 版本清單

允許管理員上傳版本相同但架構不同的 app。

Procedure程序

1. 按一下 **App > App Catalog** 下的 app 連結。
2. 按一下**版本**索引標籤。
   如果目錄中的 app 有多個版本，下拉式清單中就會顯示版本。 如果上傳多個版本相同但架構不同的 app，下拉式清單中會針對支援的架構顯示詳細資料。 在 **App 資訊**下也會針對 app 顯示支援的架構。

8.13. 搜尋 Android App 的套件名稱

若是可在 Google Play 商店取得的公用 app：

1. 使用 Web 瀏覽器找到 Google Play 商店中的 app。
2. 選擇 app。
3. 檢查瀏覽器中顯示的 URL。

URL 中 id= 後方的項目即為套件名稱，如下所示：

https://play.google.com/store/apps/details?id=<package name>

若是內部開發 app 及 Play Store 不提供的其他 app，請嘗試下載 Google Play 商店中的**套件名稱檢視器**，或其他類似 app。

8.14. 類別

本節包含以下各主題：

- 新增類別
- 移除類別

類別描述應用程式的類型，有助於在使用者瀏覽應用程式目錄時將應用程式分門別類。 每個 app 都必須至少指派一個類別。 當您開始使用 Ivanti Neurons for MDM 時，會有通用應用程式類別清單可用。 您可使用此頁面來管理 app 類別。

新增類別

您可於此處新增類別，或將 app 新增至應用程式目錄。

1. 按一下**新增** (左下角)。
2. 輸入類別名稱。
3. 類別不區分大小寫，因此 MINE 和 Mine 完全相同。
   按一下**儲存**。

移除類別

- 按一下類別旁邊的 X。

如果您無法在 **App 類別**頁面上執行工作，可能是您沒有所需的權限。 您需具備下列其中一個角色：

- App 及內容管理

8.15. 發佈篩選

本節包含以下各主題：

- 設定發佈篩選
- 設定委派管理員的發佈篩選

使用「發佈篩選」來限制可供安裝的 app。 「發佈篩選」可讓您在 app 目錄中僅顯示適用於該裝置的 app。

授權：Silver

依預設可使用下列篩選：

- **支援 Android 企業的 App** - 將 app 發佈限制為僅限支援 Android 企業的裝置。
- **僅限 iPad App** - 限制 app 只能發佈至 iPad 裝置。
- **僅限 iPhone App** - 限制 app 只能發佈至 iPhone 裝置。

設定發佈篩選

1. 前往 **App > 發佈篩選**。
   這裡列出預設的 app 篩選和所有已建立的 app 篩選。
2. 按一下**+新增**以存取**建立發佈篩選**對話方塊。
3. 在適當欄位中輸入名稱和描述。
4. 選擇規則定義。這些規則包括使用適當的運算子來建構，包括「包含」、「小於」、「大於」、「範圍」、「等於」及「不等於」運算子。 這些規則可以用「任何 (或)」或「所有 (及)」選項來建立巢狀結構。 依照下列方式套用發佈篩選器:
   - Access 已封鎖
   - 支援 APNS
   - 搭配工作描述檔的 Android 受管理裝置
   - Android Work 啟用
   - Android 安全性修補程式層級 (Android 裝置)
   - 已啟用 Android 受工作管理的裝置 (裝置擁有者)
   - 公司擁有的裝置上的 Android 工作描述檔已啟用
   - 用戶端上一次登記
   - 已註冊的用戶端
   - 相符性
   - 合規性動作已封鎖
   - 目前的國家/地區名稱
   - 目前的 MCC
   - 目前的 MNC
   - 自訂裝置屬性
   - 自訂 LDAP 屬性
   - 自訂使用者屬性
   - 自訂 IDP 屬性

- 裝置類型
- 主要國家/地區名稱
- 歸屬 MCC
- 歸屬 MNC
- IMEI
- IMEI2 (僅適用於具有雙 SIM 卡插槽的 Android 裝置，並且裝置必須為 Android 8.0 或更高版本)
- 單一應用模式
- 製造商
- 作業系統版本
- 擁有權
- 電話號碼
- 漫遊
- 安全 App 狀態
- 受監管
- Sentry 已封鎖
- 已使用者註冊
- 已註冊自動化 Device Enrollment
- 已啟用自動化 Device Enrollment

5. 按一下**建立發佈篩選**。
6. 視需要選擇要更新的自訂篩選。
    1. 按一下**編輯**以顯示**更新發佈篩選**頁面。
    2. 在適當欄位中輸入名稱和描述。
    3. 使用下拉式功能表來定義篩選的規則。
    4. 按一下**更新發佈篩選**。
7. 選取 app。
8. 在「App 詳細資料」頁面中選擇**發佈**索引標籤。
9. 按一下**編輯**。
10. 選擇 App 發佈選項：
    - **每個人**
    - **沒有人**
    - **自訂**

    > 選擇**每個人**或**自訂**發佈選項後才會顯示「發佈篩選器」區段。

11. 選擇發佈篩選選項：
    1. 在**搜尋現有發佈篩選器...** 中輸入篩選器名稱... 欄位中輸入篩選名稱，以尋找已建立的篩選。
    2. 按一下**+新增發佈篩選**以新增篩選。

在將 app 新增至目錄之前，可建立或指派發佈篩選至 app。 對發佈篩選進行的變更，將會影響正在使用該篩選之 app 的發佈 (在所有空間中)。

當已設定篩選時，如果**允許發佈時在 M1 裝置上安裝 app** 已啟用，結果會填入 macOS M1 裝置。 如果**允許發佈時在 M1 裝置上安裝 app** 已啟用，且發佈篩選為**每個人**或**自訂**，則所有 mac 裝置都可使用 iOS VPP app。 iOS app 不支援 macOS 相關屬性的發佈篩選。

設定委派管理員的發佈篩選

委派管理員可在委派空間的發佈程序期間，管理與編輯已新增至個別 app 的已建立篩選。 不過，委派管理員無法在任何其他空間中使用已在預設空間中建立的發佈篩選，但可在委派 app 中使用它們。

委派管理員可在他們有權存取的特定空間中建立、管理與編輯發佈篩選。 發佈篩選只能在用來建立它們的空間中使用。 App 發佈篩選無法進行委派。

當具備 App 與系統管理角色的委派管理員使用發佈篩選在委派空間中新增 app 時，可查看自身空間內含裝置以及其他空間內含裝置的裝置詳細資料。

具有系統管理或系統唯讀角色的使用者，無法在任何空間中建立、更新或刪除發佈篩選。

具有 App 與內容管理員角色的委派管理員，可能不具備發佈篩選的存取權。 有鑑於此，您無法：

- 使用發佈篩選建立 app。 當您以委派管理員身分登入並新增 app 時，便會發生此種狀況。
- 具備只有系統唯讀角色或更高層級的委派管理員，可以使用發佈篩選新增 app。 不具備系統管理角色的委派管理員可以新增 app，但無法使用發佈篩選來新增。

委派管理員可在 App catalog 中藉由選擇下列選項來篩選委派狀態：

- 已委派
- 未委派

8.16. 排除或分發應用程式

從裝置中排除或分發受控應用程式，而無需變更 iOS、macOS 和 Windows 裝置上的內部和公用應用程式的應用程式分發組態。 對於所有受控應用程式，可以在所有裝置的**可用應用程式**區段的**操作**欄中，找到這些選項。

權限

若要從裝置排除應用程式，或是將應用程式分發到裝置，您需要擁有以下授權:

- 存取空間中的裝置 (分割區)
- 存取裝置的可用應用程式。

排除

所選取應用程式的排除選項會從裝置解除與刪除相關資料。 依照工作流程排除必備應用程式。 彈出式確認訊息會指明您正在排除必備應用程式，並導致從裝置中排除主應用程式。

如果您排除具有多個版本的內部應用程式，則會從裝置中排除所有未分發的應用程式版本。 如果您從裝置中排除某個應用程式，此應用程式會從 Apps@Work 和 Ivanti Go 中刪除。 如果從應用程式目錄中排除與刪除某個應用程式，後來又再次新增，則在該裝置上此應用程式不再會保持排除狀態。 如果從裝置中排除受控應用程式，則此應用程式應顯示在**裝置** > **裝置** > **可用應用程式**清單中，以便管理員在排除該應用程式後對其進行分發。

發佈

當管理員從應用程式觸發**傳送安裝**指令時，在管理員決定從裝置的**可用應用程式**分發應用程式之前，不會安裝該應用程式。 對於沒有取得該應用程式的裝置，會顯示新的排除訊息。 當管理員分發可用的應用程式時，下次同步會在裝置上安裝分發的應用程式。

8.17. 評論

本節包含以下各主題：

- 檢視評等與評論
- 停用評等與評論
- 刪除評論
- 將評論匯出至 CSV 檔案

評論是指使用者針對應用程式目錄中的應用程式提供的評語和評分 (星等)。 對您和考慮安裝 app 的使用者來說，評論可提供寶貴的資訊。 使用**評論**頁面，即可檢視或刪除評等及評論。 如果評論或評等已過時或不恰當，您可以將其刪除。

- 僅有裝置使用者可以建立與編輯 app 評等和評論。
- 裝置使用者可以編輯自己提供的評等和評論，但無法將其刪除。
- 僅有管理員可以刪除 app 評論。
- App 的評等是無法刪除的。 提供給 app 的評等 (星等) 會一直保留在 **App > App Catalog** 頁面中，即使您之後停用使用者的評等和評論功能亦同。

檢視評等與評論

- 前往 **App > 評論**，即可讀取關於您所發佈之 app 的完整使用者評論和評等 (星等)。
- 前往 **App > App Catalog**，並查看**平均評等**欄位，即可取得總評論數和平均評等。
- 前往 **App > 應用程式目錄**，按一下 **App 名稱**，並查看**評論**索引標籤，即可取得特定 app 的評等和評論。

停用評等與評論

1. 前往 **App > 目錄設定**。
2. 取消勾選**在一般使用者的應用程式目錄中啟用評等與評論**。
3. 按一下**儲存**。

刪除評論

1. 前往 **App > 評論**。
2. 選擇評論。
3. 按一下頁面右上方的**動作**按鈕。
4. 選擇**刪除**。
5. 按一下**刪除評論**確認對話方塊中的**是**。

如果您無法在**評論**頁面上執行工作，可能是您沒有所需的權限。 您需具備下列其中一個角色：

- App 及內容管理

將評論匯出至 CSV 檔案

可以使用**評論**頁面中的**匯出至 CSV** 選項匯出應用程式評論。

程序

1. 前往 **App > 評論**。
2. 按一下**匯出至 CSV** 選項，將評論清單及相關詳細資訊匯出至 CSV 檔案。
3. 隨即顯示一則含有**繼續**和**取消**按鈕的快顯訊息，指出匯出程序已開始，並且很快就會提供報告。
4. 按一下**繼續**，請先等候要求完成，然後再提交另一項要求。
5. 隨即顯示一則訊息，指出**應用程式評論 - CSV 報告已完成**，其中包含**下載**和**刪除**按鈕。
6. 按一下**下載**即可下載報告。
7. (選用) 按一下**刪除**以刪除報告。

8.18. Apple Apps and Books

本節包含以下各主題：

- 在空間中於多個 Apple Apps and Books 帳戶間的 App 授權發佈
- 裝置型授權和使用者型授權發佈
- 使用裝置型授權選項
- 使用使用者型授權
- 將 Apps and Books app 新增至目錄
- 新增 Apps and Books 帳戶
- 更新 Apps and Books 安全權杖
- 更新 Apps and Books 帳戶的優先順序
- 刪除 Apps and Books 安全權杖
- 發佈目錄中 Apps and Books app 的授權
- 檢視每位使用者的 app 授權
- Apps and Books 授權用量通知
- 檢視 Apps and Books 授權用量
- 撤銷 app 的 Apps and Books 授權
- 適用於 macOS 和 iOS 裝置的 Apps and Books 行為
- 當裝置移至其他空間時的 Apps and Books 授權權利

授權：Silver

只有當您在您的 App Catalog 設定中設定 Apple Apps and Books 時，才可使用 **Apple Apps and Books** 畫面。此畫面會顯示透過 Apps and Books 為 Apple 裝置購買的 app 授權，以及已使用的數量。 您可使用此畫面來進行下列作業：

- 選擇要在目錄中包含的 Apps and Books App
- 發佈 Apps and Books App 授權

有關使用 Apps and Books 發佈應用程式的詳細資訊，請參閱 Ivanti 社群文章 Ivanti Neurons for MDM：如何使用 VPP 發佈應用程序。

> Apple Books 並不一定適用於所有國家/地區。 若要透過 Apple 的 Apps and Books 發佈 App 授權，您必須輸入 Apple 提供的 sToken。

在空間中於多個 Apple Apps and Books 帳戶間的 App 授權發佈

- 如果多個 Apps and Books 帳號中具有相同的 App，則系統會依據帳號的優先順序從帳號發佈授權。
- 如果多個 Apps and Books 帳號中具有相同的 App，但優先順序較高之 Apps and Books 帳號的 App 授權已用盡，則系統會從下一個優先順序帳號發佈授權給 App (僅有當下一個優先順序帳號的發佈清單中具有使用者或裝置的情況下)。
- 即使變更 Apps and Books 帳號的優先順序，也不會撤銷或重新指派授權。 系統會從第一個帳戶發佈授權給 app。 如果第一個帳戶的授權已用盡，則系統會從下一個優先順序帳戶發佈授權給 app，以此類推。
- 使用者可以透過 App Catalog 頁面，選擇撤銷 app 的所有授權。 此動作會從所有可用的 Apps and Books 帳號撤銷該 App 的授權。
- 保留授權的優先順序高於 Apps and Books 帳號的優先順序。

裝置型授權和使用者型授權發佈

app 的授權為裝置型或是使用者型，取決於您的指派方式而定。 當您將 app 授權指派給裝置時，就是裝置型授權。 當您將 app 授權指派給使用者時，就是使用者型授權。

將 Apps and Books 應用程式安裝到裝置後，或者為該應用程式核發權杖後，會散發使用權。 如果 app 沒有可用的授權，使用者可以自行付費安裝此 app。 如果已將所要求之 Apps and Books App 的使用者型授權指派給使用者，安裝 App 時就會使用現有的使用者型授權，而不是 Apps and Books 授權。

> 如為共享 iPad，不論是否已選取裝置型授權，都會根據裝置型授權安裝 Apps and Books。

使用裝置型授權選項

搭配裝置型授權時，使用者不需要註冊 Apps and Books。 系統會自動安裝必要的 app。 企業監管的裝置不需要使用 IT 擁有的 Apple ID。

在裝置登記期間，會由序號來識別裝置，如果有可用的授權，即會自動安裝必要的 app。 如果沒有可用的授權，就不會安裝 app。 如果有保留 app 的授權，在 app 安裝期間就不會指派以裝置為基礎的授權。

> 使用以裝置為基礎的 Apps and Books 授權來部署的 app 更新，由管理員負責控制。

若要控制 app 的更新方式，在 **App > App Catalog** 中導覽至 **App 配置/在裝置上安裝**索引標籤。 您可以選擇在下一次裝置登記時執行立即更新，或選擇在新版本推出時自動更新 app。

重要事項：在指派裝置型授權給企業對企業 (B2B) 或生產力 app 之前，請先向 app 開發者確認 app 符合裝置型授權資格。

使用使用者型授權

當使用者更換裝置 (例如裝置遺失、遭竊，或使用者升級至新裝置) 時，該使用者具備的使用者型授權仍然有效。 使用者必須先註冊 Apple Apps and Books 才能使用使用者型授權。 註冊是一項手動的動作，一般使用者必須在 App Catalog 中完成。 必須等到使用者註冊 Apps and Books 後，才會在裝置上安裝所需的 Apps and Books App。

如果 App 是必要的 Apps and Books App，且授權發佈為使用者型：

- 如果使用者未在大量採購方案內註冊，就不會安裝必要的 App。
- 如果使用者有在大量採購方案內註冊，並具有可用的授權，即會安裝必要的 Apps and Books。
- 如果使用者已在 Apps and Books 註冊，但不具有可用的授權，就不會安裝 App。

將 Apps and Books app 新增至目錄

程序

1. 前往 **App > 應用程式目錄**。
2. 選擇 app 並按一下**新增至目錄**。 按**下一步**。
3. 您也可以選擇性地新增 app 的描述。 按**下一步**。
4. 選擇發佈選項。 按**下一步**。
5. 按一下 **App 配置**索引標籤。
6. 您也可以選擇性地選擇**在裝置上安裝**。 此配置選項會在不提示受監管 iOS 裝置使用者的狀態下安裝 app。
7. 視需要選擇其他選項。

在 Apps and Books 安全權杖資訊頁面中，將顯示下列權杖詳細資料：

- 建立日期
- 位置 (如果權杖包含此資訊)
- 到期日期

新增 Apps and Books 帳戶

Ivanti Neurons for MDM 可將多個 Apps and Books 安全權杖新增至單一空間，以新增多個 Apps and Books 帳號。

執行下列步驟以在空間中新增 Apps and Books 安全權杖：

1. 前往 **Apps > Apple Apps and Books**。
2. 按一下 **+ 新增 Apps and Books sToken**。
3. 輸入名稱並選擇權杖檔案。
4. 您也可以取消選擇**自動將 Apps and Books App 發佈給所有使用者**選項。 預設會選擇這個選項，因此會使用「所有使用者」群組來發佈 FCFS 授權。
5. 您也可以選擇**清除之前 Apps and Books 授權的所有資料**選項，移除與此權杖相關聯的所有 App 授權。
6. 按一下**儲存**。

新增帳號之後，表格即會顯示所有新增的 Apps and Books 帳號清單。

更新 Apps and Books 安全權杖

程序

1. 前往 **Apps > Apple Apps and Books**。
2. 按一下 Apps and Books 帳號名稱。
3. 在「權杖」索引標籤中，按一下**更新 sToken** (.stoken 檔案)。
4. 輸入權杖名稱並選擇權杖檔案。
5. 您也可以取消選擇**自動將 Apps and Books App 發佈給所有使用者**選項。 預設會選擇這個選項，因此會使用「所有使用者」群組來發佈 FCFS 授權。
6. 您也可以選擇**清除之前 Apps and Books 授權的所有資料**選項，移除與此權杖相關聯的所有 App 授權。
7. 按一下**更新**。

在「權杖」索引標籤中，按一下**重新同步 Apps and Books 授權用量資訊**，以透過 Apple Apps and Books 服務執行所有 App 和授權資訊的完整同步。 僅有當 Ivanti Neurons for MDM 中的授權配置資訊不精確時，才需要此動作。 此種不精確可能導致 Apple 的 Apps and Books API 內容不一致。

更新 Apps and Books 帳戶的優先順序

管理員可以依據要使用授權的帳號，來指派空間中每個 Apps and Books 帳號的優先順序。 Apps and Books 帳號優先順序的使用目的是為了達成可預測的授權發佈系統，並解決當使用者或裝置可從多個 Apps and Books 帳號接收相同 App 授權時的衝突。

程序

1. 前往 **Apps > Apple Apps and Books**。
2. 對所需的 Apps and Books 帳號名稱按一下**編輯優先順序**。

3. 在「編輯優先順序」視窗中，選擇新的優先順序。
4. 按一下**儲存**。

刪除 Apps and Books 安全權杖

移除 Apps and Books 安全權杖是一種無法復原且具有破壞性的動作。 當權杖移除時：

- 保留權杖的 app 將會移除其權杖。
- 已付費的 App 將留在目錄中，而且使用者可以自己付費。
- 針對一般使用者透過此公司 Apps and Books 帳號安裝的 App，如果使用者想要使用這類 App，則必須將其轉移到個人帳號。 使用者可在 30 天的寬限期內進行上述作業。

程序

1. 前往 **Apps > Apple Apps and Books**。
2. 按一下 Apps and Books 帳號名稱。
3. 在「權杖」索引標籤中，按一下**刪除**。
4. 在「刪除 Apps and Books 安全權杖」視窗中，按一下**是，刪除 Apps and Books 安全權杖**選項以確認。
5. 按一下**刪除**。

發佈目錄中 Apps and Books app 的授權

1. 從主功能表選擇 **Apps > Apple Apps and Books**。
2. 顯示 Apps and Books 帳號清單。 每個帳號下方會顯示透過 Apps and Books 方案購買的 App 清單。
   選擇 app 並按一下**發佈授權**。
3. 在 Apps and Books 授權區段的下列發佈選項中進行選擇：**先到先得**、**保留**或**不允許**。

檢視每位使用者的 app 授權

您可以使用「授權用量」索引標籤，檢視使用者的授權喜好設定。

1. 按一下**使用者**索引標籤。
2. 選擇使用者。
3. 按一下**授權用量**索引標籤。
   隨即顯示 App 清單與其 Apps and Books 授權類型和授權指派詳細資料。

若要檢視每位使用者的每個 app 授權用量：

1. 在 Ivanti Neurons for MDM 主功能表中，前往**使用者**。
2. 選擇使用者。
3. 預設會顯示**裝置**索引標籤。
   按一下**授權用量**索引標籤。
   隨即顯示使用者裝置上已安裝的所有 app 清單，包括授權狀態。 若是裝置型授權，裝置序號會提列在「Apps and Books 授權類型」欄位中。
   - App 名稱
   - app 版本
   - app 成本

- 指派 app 的時間
- Apps and Books 授權類型
- 動作 (授權狀態)
- 授權詳細資訊的平台資訊。

您也可以檢視每個 App 的 Apps and Books 授權用量：

1. 在 Ivanti Neurons for MDM 主功能表中，前往 **應用程式 > 應用程式目錄**。
2. 選取 app。
3. 按一下 **Apps and Books Licenses** 索引標籤 (如果出現的話)。
4. 按一下帳戶名稱。 此索引標籤只會顯示透過 Apps and Books 方案購買的 App。

隨即顯示每個 Apps and Books 授權類型的個別索引標籤。

授權類型和日誌	描述
先到先得 (FCFS) - 您可以選擇哪個使用者群組會收到此類授權。	• 使用者要求的 App - 使用者選擇要安裝的 App。 預設為使用者型授權。 • 必要的 App - 需具備的 app，並由「管理」配置透過**安裝到裝置上**設定來進行安裝。 這些 app 預設會使用裝置型授權。
保留	保留授權的優先順序高於 FCFS 授權。 您可在此處選擇要使用 app 保留授權的使用者或裝置。
不允許	輸入不允許擁有此 app 授權的使用者。 使用者可在購買後安裝 app。
活動日誌	顯示使用者、指派給使用者的 Apps and Books 授權類型、指派日期，以及針對授權執行的最後一個動作。

若要檢視每台裝置的每個 app 詳細授權用量：

1. 在 Ivanti Neurons for MDM 主功能表中，前往**裝置**。
2. 選擇裝置。
3. 按一下**已安裝的 App** 索引標籤。
4. 隨即顯示所選裝置上已安裝的所有受管理 app 清單，包括授權狀態。
   - App 名稱
   - app 版本
   - 支援的平台
   - app 來源
   - app 大小
   - Apps and Books 授權類型
   - iOS app 的 app 報告(安裝) 日期

搜尋裝置的已安裝應用程式，如下所示:

- App 名稱
- 套組或套件 ID

Apps and Books 授權用量通知

Apps and Books 通知可協助您追蹤 Apps and Books 授權用量。 通知的臨界值定義如下：

- 當授權使用量超過 50% 時，會發出資訊通知。
- 當授權使用量達 70-80% 時，會發出警告通知。
- 當授權使用量達 90-100% 時，會發出重要通知。
- 當用量回落到 50% 以下時，就會清除通知。

若要檢視每個 app 的授權資訊：

1. 按一下 **Apps > Apple Apps and Books**。
2. 隨即顯示下列授權資訊：
    - app 名稱。
    - 授權成本。
    - 可用的授權數量。
    - 已兌換的授權數量。

前往**儀表板 > 通知**，以檢視授權通知的詳細資料。

3. 隨即顯示「通知」頁面。
   按一下通知標題，即可查看詳細資料。 有關可用的通知，請參閱儀表板。

Apps and Books 授權用量通知

觸發	嚴重性	通知類型	元件類型
50% 已兌換	資訊	授權用量	Apps and Books
70% 已兌換	警告	授權用量	Apps and Books
80% 已兌換	警告	授權用量	Apps and Books
90% 已兌換	警報	授權用量	Apps and Books
100% 已兌換	警報	授權用量	Apps and Books

檢視 Apps and Books 授權用量

特定使用者的授權用量詳細資料會顯示在授權欄位的授權用量表中。

1. 按一下某個 app。
2. 按一下**授權用量**索引標籤。
3. 在搜尋欄位中輸入使用者名稱。

撤銷 app 的 Apps and Books 授權

在以下情況中會撤銷 Apps and Books 授權：

- 裝置已停用 (遭淘汰或清除)。

- Apps and Books App 被刪除。
- 裝置淘汰時已撤銷裝置型授權。
- Apps and Books 權杖被刪除。

如要撤銷 App 的 Apps and Books 授權：

1. 選擇 **App >應用程式目錄**下的 app。
2. 按一下 **Apple Apps and Books 授權**索引標籤 (如果出現的話)。
3. 執行下列其中一項作業：
    1. 按一下**撤銷所有授權**，撤銷所有使用者或裝置的所有授權。
    2. 按一下**活動日誌**標籤。 使用**動作**欄位，逐一撤銷使用者或裝置的個別授權。
- 若是 iOS 裝置，在 Apps and Books 授權撤銷後，Apple 允許 Apps and Books App 有 30 天的寬限期。 因此，您仍可安裝 Apps and Books App。
- 若是 macOS 裝置，在 Apps and Books 授權撤銷後，app 仍會保留在裝置上。

如要撤銷使用者的 Apps and Books 授權：

1. 按一下某個 app。
2. 按一下**授權用量**索引標籤。
3. 針對要移除其授權的使用者，按一下**撤銷授權**連結。

> 如果將使用者刪除，或使用者移除裝置的 MDM 描述檔時，Apps and Books 授權就會自動撤銷。

Apps and Books 身份認證錯誤通知

使用 Apple Apps and Books 服務時可能會發生某些身份認證錯誤。 這些 Apps and Books 身份認證錯誤通知包括：

錯誤通知	動作
無效的身份認證權杖	上傳有效的 Apps and Books sToken
過期的權杖	使用您公司的帳號在線上產生新的權杖
sToken 已遭到撤銷	上傳有效的 Apps and Books
需要登入	登入 Apps and Books 服務

適用於 macOS 和 iOS 裝置的 Apps and Books 行為

適用於 iOS 的 Apps and Books

動作	裝置型授權	使用者型授權
針對使用者將 Apps and Books App 從發佈中移除	使用者的裝置會解除安裝 app	使用者的裝置會解除安裝 app
取消委派 Apps and Books App	非預設空間中的所有裝置都會解除安裝 app	非預設空間中的所有裝置都會解除安裝 app
從預設或自訂空間刪除 Apps and Books App	所有裝置都會解除安裝 app	所有裝置都會解除安裝 app

適用於 macOS 的 Apps and Books

動作遊戲	裝置型授權	使用者型授權
針對使用者將 Apps and Books App 從發佈中移除	使用者的裝置並不會解除安裝 app	不適用
取消委派 Apps and Books App	非預設空間中的所有裝置不會解除安裝 app	不適用
從預設或自訂空間刪除 Apps and Books App	不會從所有裝置解除安裝 app	不適用

當裝置移至其他空間時的 Apps and Books 授權權利

當裝置移到新空間時，將撤銷指派給裝置或裝置擁有者的 Apps and Books 授權。 新 Apps and Books 授權的指派取決於新空間的可用情況。

以下為 Apps and Books 授權權利案例：

案例	授權
Apps and Books 授權指派給來源空間中的裝置或裝置擁有者，而相同 App 的 Apps and Books 授權可用於目的地空間。	指派目的地空間中來自 Apps and Books 權杖的授權。
Apps and Books 授權指派給來源空間中的裝置或裝置擁有者，但相同 App 的任何 Apps and Books 授權都無法用於目的地空間。	撤銷來源空間中來自 Apps and Books 權杖的授權。
Apps and Books 授權不會指派給來源空間中的裝置或裝置擁有者，但任何已安裝的 Apps and Books App 的 Apps and Books 授權可用於目的地空間。	指派目的地空間中來自 Apps and Books 權杖的授權。

如果您無法在 **App 類別**頁面上執行工作，可能是您沒有所需的權限。 您需具備下列其中一個角色：

- App 及內容管理

8.19. 目錄設定

本節包含以下各主題：

- 變更 Apple App 管理設定
- 設定預設 App Store 地區
- 啟用/停用 iOS app 更新
- 啟用/停用應用程式評等與評論
- 上傳或更新 iOS/macOS Apps and Books sToken (授權：Gold)
- 從 Ivanti Neurons for MDM 服務移除 iOS/macOS Apps and Books sToken

在**應用程式** > **目錄設定**頁面中，設定要套用至應用程式目錄中所有應用程式的偏好設定。 您可執行下列動作:

- 在裝置登記期間包括 app 更新
- 阻止備份至 iCloud 和 iTunes (僅限 iOS)
- 設定預設 App Store 地區 (Apple和 Microsoft)
- 當裝置取消註冊時移除 iOS app
- 啟用 Ivanti Neurons for MDM「評等與評論」
- 上傳 iOS 與 macOS Apps and Books 權杖 (需要 Gold 授權)

變更 Apple App 管理設定

若沒有建立個別 app 的 app 管理配置，則這些設定會套用至所有 app。

1. 選擇或清除下列一或多個勾選框：
    - **於裝置登記期間更新 App** (預設為選擇)
    - **防止備份至 iCloud 和 iTunes**
    - **移除取消註冊的 App**

按一下**儲存**。

通知

1. 按一下**當 Apple App Store 和 Google Play 商店中提供新的應用程式版本時，產生系統通知**底下的下拉式清單，然後選取下列其中一個選項:
    - **一週一次**
    - **一天一次**

按一下**針對應用程式目錄中可用的新應用程式更新產生一般使用者通知**底下的下拉式清單，然後選取其中一個選項:

- **一週一次**
- **一天一次**

設定預設 App Store 地區

在 App Catalog 設定中，設定 Apple 和 Microsoft App Store 的預設地區。

1. 在預設 App Store 地區區段：
    - 選擇 **Apple App Store 地區**。
    - 選擇 **Microsoft App Store 地區**。
2. 選擇或清除此選項，將每個管理員上次選取的 App Store 地區設為預設地區。 如果此選項已選取，那麼 App Store 地區將會設為每個管理員上次選取的地區，它將會覆寫之前的設定。 如果這是管理員第一次使用此功能，則預設 App Store 地區將會設為此程序中之前的選擇。
3. 按一下**儲存**。

啟用/停用 iOS app 更新

1. 選取或清除**裝置登記期間更新應用程式。**
    - 預設會選擇這個選項。
    - 清除此選項時，任何裝置登記 (包括管理員的強制登記) 都不會包括 app 更新。
    - 不過，使用者可以按一下裝置 App Catalog 上的「強制登記」動作以手動更新 app。
    - 裝置登記期間，即會針對新的 app 安裝和所有其他配置與設定進行更新。

按一下**儲存**。

若是受管理的 App，管理員可以按一下 App 詳細資料頁面上的**更新**按鈕，手動將 App 更新為 App Store 的最新版本。

使用者可以在其裝置的 App Catalog 功能表上，按一下**強制登記**按鈕，即可登記裝置，並在其他配置和更新作業進行時一併更新 App。

下列設定可讓使用者選擇更新 app 的時間：

- 請等到連接 Wi-Fi 時再進行，以免產生行動數據費。
- 避免在更新 app 時，不巧受到封鎖。

啟用/停用應用程式評等與評論

這可讓使用者評等並評論此應用程式，以供其他使用者閱讀這些評論。

1. 選擇或清除**在一般使用者的應用程式目錄中啟用評等與評論**。
2. 按一下**儲存**。

> Apps and Books sToken 的格式已變更。 現在它是儲存在 vpptoken 檔案格式之文字檔案中的字元字串，而不是舊版的字元字串。 請直接將這個檔案上傳至管理員控制台以進行處理。 Apps and Books 帳號頁面已更新，以顯示 Apps and Books 組織名稱和有效日期。

上傳或更新 iOS/macOS Apps and Books sToken (授權：Gold)

1. 選擇**新增 Apps and Books sToken**。
2. 在**別名名稱**欄位中，輸入 sToken 檔案的名稱。
3. 將 sToken 檔案拖曳到指定區域，或按一下**選擇檔案**，並瀏覽至 sToken 檔案。
4. 按一下**儲存**，或者，如果您要更新現有的 sToken 檔案，請按一下**更新**。
5. 前往 Apple Apps and Books 頁面，即可檢視與此權杖相關聯的 app。

> 若在 Ivanti Neurons for MDM 的之前版本中已為個人使用者保留了 Apps and Books 權杖，則必須驗證權杖是否仍保留給那些使用者，並視需要再次保留那些權杖。

從 Ivanti Neurons for MDM 服務移除 iOS/macOS Apps and Books sToken

您可將使用者不再需要的 app 撤銷，並於需要時再重新指派。 如果 App 是以 iOS/macOS 適用的 MDM 部署為受管理的 App，您就可以立即移除 App 與所有資料。

1. 選擇要移除的 app。
2. 按一下**刪除**。
   隨即出現警告對話方塊。
3. 您可以選擇性地提供使用者 30 天的寬限期，以便他們可以：
   - 儲存資料。
   - 購買 app 的個人複本。
   - 將他們透過此 Apps and Books 帳戶安裝的 App 傳輸至個人帳戶以持續使用。

如果您無法在**目錄設定**頁面上執行工作，可能是您沒有所需的權限。 您需要以下角色:

- App 及內容管理

8.20. 部署 app 相依性

當您上傳內部應用程式套件時，Ivanti Neurons for MDM 會掃描應用程式以識別相依性。 如果找到任何相依性，將會在「新增 App 精靈」的第三步中列出它們。 對於任何應用程式相依性，管理員可選擇上傳相依性檔案。 不過，如果未上傳相依性檔案，有些應用程式可能無法安裝。

管理員可以選擇在安裝特定應用程式時設定應用程式相依性。 在這種情況下，可以藉由主應用程式標記一個或多個應用程式。 當使用者嘗試安裝主應用程式時，系統將通知使用者相依應用程式將會與主應用程式一起安裝。

> 此功能僅在 iOS、Android、Windows 及 macOS 裝置上受支援。

請注意以下有關應用程式相依性和必要條件的事項：

- 管理員可設定在裝置上安裝應用程式的必要條件相依應用程式。 內部、公用、私人 (Android) 或 VPP 應用程式都屬於必備應用程式。
- 現已在 App Catalog 頁面的「必要條件 App」欄中顯示必要應用程式的計數。 您可將滑鼠移至此數字上，以檢視必要條件應用程式的清單。
- 一旦觸發安裝主要應用程式，就會直接下載必要條件應用程式。
- 如果主要應用程式已委派，就會自動委派關聯的必要條件應用程式。
- 必須等到必要條件關係移除後，才能將必要條件應用程式從 App Catalog 刪除。
- 不同版本的應用程式可能會有不同的必要條件應用程式。
- 「稽核追蹤」頁面記錄 iOS、Android 及 macOS 必備應用程式的新增、移除及自動委派。
- 如果管理員或使用者安裝的應用程式有必要條件應用程式，則會先安裝必要條件應用程式，然後才會安裝主要應用程式。 如果是在安裝必要條件應用程式後才登記裝置，則將會解除安裝這些必要條件應用程式。

> 雖然應用程式需要相依性檔案，但 Ivanti Neurons for MDM 不需要您為了部署應用程式而上傳任何檔案。

> 對於 Samsung 裝置，管理員應將必備應用程式新增至「kiosk 模式允許的應用程式」清單。 已新增至「允許的」應用程式清單的必備應用程式不會被新增至「黑名單」應用程式清單。

> 對於非 Samsung 裝置，若主應用程式已新增至「kiosk 模式允許的應用程式」清單，則必備應用程式應以無訊息方式自動在背景執行。 若管理員在 kiosk 模式中設定必備應用程式，則您只能在 kiosk 模式中檢視此應用程式。

> **Windows 裝置** - 若 Bridge 應用程式是尚未發佈的必要條件應用程式，且主要應用程式是以無訊息方式發佈的 .exe。 當移除相依項目後，Bridge 應用程式將會解除安裝，但 .exe 會在此步驟後失敗。 管理員應確認 Bridge 應用程式並未依預設取消發佈。

> **Windows 裝置** - 當主要應用程式並非以無訊息方式發佈且主要 應用程式具有未發佈的必要條件應用程式，則必要條件應用程式會先成功安裝。 不過，若主要應用程式安裝失敗，則必要條件應用程式會立即解除安裝。 只有當使用者觸發安裝要求後才會重試失敗的主要應用程式。

新增內部開發的應用程式

1. 前往 **App > 應用程式目錄**。
2. 按一下**新增**。

3. 將 app 檔案拖曳到虛線方塊中，或按一下**選擇檔案**，從檔案系統中進行選擇，然後按一下**確認**。
4. 按**下一步** (右下角)。 Ivanti Neurons for MDM 會掃描應用程式以取得相依性檔案，並在**應用程式相依性**表格中列出它們。
5. 檢閱 app 資訊，並確認您已選擇正確的 app。
6. 按一下**動作**欄中的上傳圖示。 **上傳相依性**視窗隨即顯示。
7. 按一下**選擇檔案**以瀏覽並搜尋檔案的本機副本，然後按一下**上傳**。
8. Ivanti Neurons for MDM 會掃描選用套件以查找應用程式，並在「選用套件」表格中列出它們。 如果已列出，按一下「動作」欄中的上傳圖示。 顯示「上傳選用的封裝」視窗。
9. 檢視 app 資訊，並確認您已選擇正確的 app。
10. 按一下**選擇檔案**以瀏覽並搜尋檔案的本機副本，然後按一下上傳。
11. 按**下一步**。
12. (選用) 新增 app 的螢幕擷取，然後按**下一步**。
13. 如果應用程式需要其他必要條件應用程式。
    1. 從**必要條件 App** 區段選擇**開啟**選項。
    2. 在**新增 App** 索引標籤之下搜尋必要條件應用程式。
    3. 選擇應用程式。
    4. 按一下**儲存**。
14. 定義 app 發佈，然後按**下一步**。
15. 定義「應用程式組態」區段，然而按一下**完成**。當裝置下次與 Ivanti Neurons for MDM 進行同步時，系統將會一起部署應用程式與相依性檔案。

> 您可以按一下「新增相依性」按鈕，藉此新增額外的相依性。 完成上傳後，這些額外的相依性也會列在「App 相依性」表格中。 管理員也可以手動新增僅內容類型的選用封裝。 此封裝類型不受版本影響。

新增必要條件 App

您可新增必要條件應用程式至主要應用程式。 您可為不同版本的主要應用程式新增不同的必要條件。 App Catalog 頁面可讓您選擇是否將描述、指令碼、畫面擷取、發佈、app 必要條件，以及 app 配置維持和現有應用程式版本相同，或是變更關聯的必要應用程式。 您必須移除必要條件應用程式與主要應用程式的關聯後，才能將之刪除。

稽核追蹤頁面現在可在以下特定欄位中顯示支援的必要條件應用程式：

「稽核追蹤」頁面中的支援 iOS、 Android 及 macOS 應用程式的「必備應用程式」區段顯示以下欄位:

appVersionId

名稱

platformAppId

自動委派或取消委派的必要條件應用程式包含以下欄位會顯示：

dmPartitionDistributionType

dmPartitionDistributionReason

程序

1. 從 **App Catalog** 選擇應用程式。
2. 按一下**編輯**。
3. 向下捲動至 **App 委派**，然後選擇**委派此 app 給所有空間**選項。
4. 按一下**儲存**。

> 如果您委派多個應用程式，然後從主要應用程式選擇移除委派，並不會自動將必要條件應用程式從委派移除。

8.21. 使用 Android Enterprise 部署 Divide Productivity

Divide Productivity 是一款可部署至 Android Enterprise 裝置的 PIM 應用程式。

1. 前往 **App > 應用程式目錄**。
2. 按一下**商業 App** 下方的 **Divide Productivity**。
3. 輸入其他類別或描述。
4. 按**下一步**。
5. 接受顯示的權限。
6. 按**下一步**。
7. 選擇發佈選項。
8. 展開**進階選項與 App 配置**。
9. 請使用下列方針來啟用選項：
10. 選擇推廣選項。

設定	方法
使用者無法解除安裝 app	選擇防止使用者解除安裝已無訊息自動安裝的 app。
郵件地址	使用變數定義與 app 相關聯的電子郵件地址。
密碼	使用變數定義與電子郵件帳戶相關聯的密碼。 如果您將此欄位保持空白，即會提示使用者輸入密碼。
主機	輸入要使用之郵件伺服器的主機名稱。 輸入 ActiveSync 伺服器的完整網域名稱。 如果您是使用 Standalone Sentry，則輸入 Sentry 的完整網域名稱 (FQDN)。 例如： mySentry.mycompany.com
伺服器類型	選擇郵件伺服器的類型。
使用者名稱	使用變數定義電子郵件帳戶的使用者名稱。
需要 SSL	如果您想使用 https 與您在「主機」欄位中指定的伺服器進行安全的通訊，可選擇此選項。
信任所有憑證	僅有當您想讓 app 自動接受不受信任的認證時才選擇此選項。 一般來說，只有在測試環境中作業時才會選擇此選項。
預設電子郵件簽名	輸入所有電子郵件的預設電子郵件簽名。 使用者可以隨時變更此項目。 一旦裝置使用者變更以後，之後對此欄位進行的變更都將無效。
電子郵件附件上限	輸入允許的附加檔案大小上限。
啟用作業	選擇同步處理作業。
登入認證別名	輸入登入憑證的別名。
Smime 簽署認證別名	目前不支援。
Smime 加密認證別名	目前不支援。
進階選項	
安裝到裝置上	選擇提示使用者安裝 app。
無訊息自動安裝到 Samsung Knox 裝置上	選擇在 Samsung Knox 裝置上自動安裝 app。
App Catalog 不會顯示 app 給使用者	如果您不想在裝置的應用程式目錄中顯示 app，可選擇此選項。

11. 按一下**完成**。

8.22. 設定 Provisioner app

本節包含以下各主題：

- 佈建需求
- 啟用 Android Beam 以使用 NFC Bump
- 佈建企業擁有的裝置
- 註冊裝置
- 確認裝置註冊狀態

Provisioner 是一款 Ivanti Neurons for MDM 應用程式，用於佈建公司擁有的裝置，以便將其註冊為工作受管理裝置並置於「裝置擁有者」模式下。

受公司管理的裝置只有企業描述檔，沒有個人描述檔。 管理員可在裝置上設定 20 種以上的鎖定，以限制裝置的功能運作，例如相機、撥接電話、SMS、上網等等。

將要使用 NFC Bump 初始化 Android Enterprise 目標裝置組態的裝置需要 Provisioner 應用程式。 如要佈建企業擁有的裝置，請在主要裝置上安裝 Provisioner app，然後使用 NFC (近場無線通訊) bump 來佈建新裝置。 bump 讓兩個裝置相互感應。 佈建裝置時可使用下列其中一種用戶端 app：

- Go 搭配 Ivanti Neurons for MDM 使用
- At Work UEM (無品牌用戶端應用程式) 可搭配 Ivanti Neurons for MDM 一起使用。

佈建需求

若要將公司擁有的 Android Enterprise 裝置佈建為工作受管理裝置:

- 佈建之前，公司擁有的原生支援 Android Enterprise 裝置必須恢復出廠預設值。
- 必須定義 Android Enterprise 組態，並將其套用於 Android 裝置群組。
- 具有 NFC 功能的 Android 裝置指定做為主要裝置或範本，其中安裝 Provisioner app。
- 要佈建的 Android Enterprise 裝置。
- Provisioner 應用程式
  從 Google Play 下載適用於 Android 的 Provisioner app。

啟用 Android Beam 以使用 NFC Bump

程序

1. 在裝置上前往**設定**。
2. 前往**無線與網路**，然後按一下**更多**。
3. 選取 **NFC** 勾選框。
4. 按一下 **Android Beam**，然後滑動以切換至**開啟**。

> 您裝置上的確切操作步驟可能略有不同。

佈建企業擁有的裝置

程序

1. 在用來做為 Android 主要裝置的裝置上安裝 Provisioner app。
2. 在主要裝置上啟動 Provisioner。
3. 從下拉式功能表選取 app。
4. 按 Provisioner app 的要求輸入資訊。 如果有支援的 Wi-Fi 類型，部分欄位可能會自動填入。 使用以下準則：

欄位	值
選擇要佈建的 app	Go (選取以搭配 Ivanti Neurons for MDM 使用) At Work UEM (無品牌用戶端應用程式，可選擇將其與 Ivanti Neurons for MDM 一起使用)。
Wi-Fi 網路 SSID	輸入主要裝置將使用的 Wi-Fi SSID。
Wi-Fi 安全性類型	輸入 Wi-Fi 安全性類型
Wi-Fi 密碼	輸入 Wi-Fi 的密碼
時區	輸入本地現行時區
地區設定	輸入地區

5. 按一下**繼續**。
   Bump 裝置畫面隨即顯示在主要裝置上。
6. 當目標裝置開機並顯示 Android 歡迎使用畫面時，讓主要裝置與目標裝置背對背靠近，以啟動 NFC 傳輸。
   如果 NFC 傳輸成功，目標裝置可能會發出聲音，然後繼續下載所選擇的用戶端 app。 如果裝置未加密，則在繼續之前會先啟動加密程序。
7. 繼續藉由 bump 裝置來佈建其他裝置。 目標裝置必須顯示「歡迎使用」畫面，而主要裝置必須顯示 **Bump 裝置**畫面。

註冊裝置

使用 NFC Bump 佈建企業擁有的裝置之後，其中將會安裝所選擇的用戶端 app。 啟動用戶端 app，然後註冊裝置。

確認裝置註冊狀態

程序

1. 前往**裝置 > 裝置**。
2. 按一下裝置連結，即可檢視詳細資料。
3. 裝置的狀態列在左窗格中。

8.23. 管理 Windows 應用程式

使用者可以管理 (匯入、設定、排程、發佈、更新和移除) Windows 應用程式的完整應用程式生命週期。 透過 MDM 控制台支援應用程式發佈和應用程式更新程序。 如需有關管理 Windows 應用程式及其他應用程式的更多詳細資訊，請參閱**App 配置**、**App 深入解析**及**「App Catalog」**。

支援的應用程式類型

- 內部 (從**「App Catalog」**區段選取**新增內部應用程式**中的選項)
- MSB (商務用 Microsoft Store 整合)
- 公開商店 (透過原生 Microsoft Store 整合) 可以在「應用程式」>「目錄設定」中設定 Microsoft Store 地區。 如需詳細資訊，請參閱**「App Catalog」**章節中的**從公開商店新增應用程式**。

支援的應用程式副檔名

- MSI
- MSIX
- APPX
- APPX 套組
- EXE (透過 **Ivanti Bridge**)

應用程式控制

「應用程式控制組態」可以控制每個裝置的應用程式安裝。 如需詳細資訊，請參閱**App 控制配置：控制每台裝置要安裝哪些 App**。

套件和相依性

可以使用下列的不同功能:

1. 可以將 Windows 應用程式設定為所有類型應用程式的先決條件。 如需有關如何設定應用程式先決條件的資訊，請參閱**部署 app 相依性**。
2. APPX 和 APPX 套組應用程式相依性及其他套件相依性。 在**檢視 App 詳細資料**頁面中，檢閱**應用程式相依性和其他套件**章節。
3. Win32 應用程式支援選擇正確的產品代碼 (MSI) 以及命令列和變數。 可以在**這裡**找到常用命令列選項的清單。

指令碼

透過 Ivanti Bridge 用戶端支援指令碼。 如需有關設定指令碼的資訊，請參閱 **Ivanti Bridge**

在裝置上安裝 Ivanti Bridge 後，即可發佈指令碼，步驟如下:

- 在裝置層級使用透過 Ivanti Bridge 動作的指令碼和動作
- 透過 Ivanti Bridge 組態 (前往**組態** > **Bridge**)

檢查裝置上的現有版本核取方塊，在內部 MSI 和 EXE 應用程式的**指令碼和檔案** 索引標籤中可用，它控制應用程式在 Windows 裝置上安裝的方式。 當您啟用此選項時，裝置會執行簽入，以驗證是否已安裝應用程式並識別其版本。 只有在應用程式不存在或已安裝版本比所需版本舊時，Ivanti Neurons for MDM 才會安裝或升級應用程式。 如果存在相同或較新的版本，則略過安裝。 此選項要求在啟用應用程式之前，至少在一台裝置上安裝應用程式。

安裝前和安裝後指令碼和檔案

針對 .exe 檔案和 .MSI 檔案

您可以配置安裝前和安裝後 PowerShell 指令碼和檔案、登錄機碼指令碼和 Windows 可執行檔 (.exe)，並在應用程式詳細資訊層級下載 Windows 應用程式的其他類型檔案。

在新增安裝前或安裝後指令碼和檔案時，Ivanti Bridge 畫面隨即出現。 您可以附加指令碼或檔案、新增指令碼引數，也可以提供檔案的目標位置。 必須在裝置上成功執行安裝前指令碼後，才能將應用程式安裝指令傳送到裝置。 系統會以與上傳至控制台相同的順序來執行/安裝這些安裝前和安裝後指令碼和檔案。 若安裝前指令碼下載或安裝失敗，則無法繼續執行應用程式安裝。

若安裝後指令碼失敗，您可以在「裝置記錄」區段之下的「裝置詳細資訊」頁面中檢視錯誤。 此外，當安裝後動作失敗時，您無法回復安裝前指令碼/已下載的檔案和已安裝的 .exe 檔案。

您可以使用「排列指令碼和檔案的優先順序」選項，重新排序安裝前或安裝後的指令碼和檔案。 唯有至少有兩個或更多指令碼或檔案可用時，才可使用此選項。 使用此選項，即可將檔案或指令碼拖放到各自的安裝前或安裝後區段中，而不是從一個區段拖放到另一個區段。

安裝行為和組態

Windows 應用程式支援以下功能:

- 無提示安裝
- **Windows app 排程**
- 重新啟動選項

如需有關安裝行為選項的更多詳細資訊，請參閱**App 配置**。

> MSI 應用程式和 EXE 應用程式 (已使用 Bridge 安裝) 支援使用無使用者 MDM 工作階段進行安裝。

例如，在以下情況下:

- 裝置已重新啟動，尚無使用者登入
- 使用者已從 Windows 工作階段登出
- 裝置已在 Autopilot 無使用者 (自行部署或預先佈建) 模式下註冊
- 在裝置層級安裝應用程式

> 允許以更有效率的方式安裝 MSI 應用程式，例如，在 Auto-pilot 註冊期間或無人使用 Windows 裝置的夜間。 對 MSI 中的 EXE 使用簡單重新封裝時，即可進行安裝操作，但不能進行升級或刪除。 實際的 MSI 套件與 CSP 有連線。 將在使用者登入後安裝其他應用程式類型。

Tunnel for Windows (個別應用程式 VPN)

Tunnel 是一個獨立的原生 Windows 應用程式。 目前在 Microsoft Store 提供，可發佈到裝置。 建立個別應用程式 VPN 組態。 需要部署 Sentry。 若要設定 Tunnel 應用程式，請前往**組態** > **+新增** > 搜尋 Tunnel (選擇支援 Windows 裝置的組態)。 選取 Sentry 設定檔並進行設定，以開始透過 Sentry 為應用程式建立通道。 若要設定 Sentry 伺服器，請前往**管理員** > **基礎架構** > **Sentry**。

App 庫存

可以在兩個層級追蹤安裝在 Windows 裝置機群中的應用程式和軟體清單:

- 若要檢查裝置中安裝的應用程式，請前往**裝置** > **應用程式詳細目錄**
- 若要檢查裝置層級的詳細目錄，請前往「裝置」> 選擇一個裝置 > 按一下「已安裝的應用程式」

管理員可以設定 Windows 應用程式詳細目錄收集間隔。 前往「管理員」>「Windows」>「應用程式詳細目錄間隔」。設定隱私權組態收集裝置中的所有應用程式時，會使用此間隔。 若要設定隱私權組態，請前往「組態」>「+新增」> 搜尋「隱私權」 > 選擇「收集裝置上所有應用程式的應用程式詳細目錄」。 選取要收集的應用程式類型。

公司應用程式目錄 (Apps@Work)

客戶可以使用 Apps@Work 啟用 Windows 裝置上的公司目錄。 Apps@Work 可在 Neurons for UEM 中使用，並透過其中的應用程式目錄進行部署。 如需詳細資訊，請參閱**Apps@Work (iOS、Android、Windows 和 macOS)**。

8.24. Ivanti Bridge

本節包含以下各主題：

- Bridge 支援的檔案類型
- Bridge 設定
- Bridge 日誌
- Bridge 上次簽入
- 橋接服務失敗修復

Ivanti Bridge 使用單一控制台和通訊通道整合 Windows 10 的行動裝置和桌上型裝置作業。 它延伸 UEM 功能以管理 PC 並允許組織充分利用大幅縮減成本與提高效率的優點，同時確保 PC 和行動裝置之間的一致安全性。 企業使用 Ivanti Bridge，即可如同針對支援的 Windows 行動裝置一樣，將單一協定用於 Windows 10 桌上型裝置，以便將資訊傳送到作業系統上的舊版應用程式。

Ivanti Bridge 可讓 IT 部門將 UEM 上的 Windows 作業現代化時，同時保留所有關鍵功能。 IT 可以套用既有的原則與指令碼，而不需系統映像、多個裝置通訊通道，也不需加入網域。

組織使用 Ivanti Bridge，現在可以:

- 透過 UEM 完整控制 PC
- 透過無線遠端管理 PC
- 減少為桌上型電腦製作映像檔的需要
- 使用 GPO 型指令與 UEM 所部署的 PowerShell 指令碼
- 輕鬆編輯與管理登錄檔
- 輕鬆部署非 MSI 封包的 Win32 應用程式和 Win32 市集應用程式
- 獲得檔案系統的可見性

> Windows 11+ 裝置和 ARM 處理器支援 Ivanti Bridge。 Ivanti Bridge 不支援 Windows 10 家用版桌上型裝置。

Bridge 支援的檔案類型

Ivanti Bridge 包括對下列檔案類型的支援:

- PowerShell
  使用橋接推送至裝置的 PowerShell 指令碼，可支援具名引數。
  64 位元的 Windows 10 Desktop 裝置可支援 64 位元 PowerShell 指令碼。

> 傳送 PowerShell 指令碼至裝置後，伺服器端等待結果的 Bridge 逾時約為 20 分鐘。 逾時會記錄為「失敗」。 但是，裝置上的指令碼會繼續運作。

> 等待 PowerShell 指令碼執行程序的 Bridge 逾時約為 60 分鐘。 60 分鐘後，程序就會終止，不會儲存來自指令碼的輸出，並將新的「失敗」記錄傳送至伺服器。

> 伺服器端及裝置端逾時都會記錄為「失敗」。 如果經過第二次逾時且指令碼產生一些輸出，伺服器端不會記錄輸出。

登錄檔

- VB 指令碼
- 適用於 Win32 應用程式部署的 .EXE
- Win32 市集應用程式使用 WinGet 工具來安裝與解除安裝應用程式。

> 如果管理員需要推送 Win32 (.EXE) 檔案到裝置 (例如做為 Windows 內部 app)，則會自動使用 Bridge (如果有)。 一定要輸入引數才能無訊息自動安裝檔案 (例如 /SILENT 或 /VERYSILENT)。
> 使用 Admin PowerShell 模式透過 Bridge 安裝 .EXE app。 對於 Windows 裝置，若要使用使用者認證進行安裝，請選擇「以使用者身份執行」選項。

> 管理員應在**應用程式安裝程式 - 設定**中選取**以使用者身分執行安裝程式**核取方塊，來為使用者安裝應用程式。 如果您想要在系統層級安裝應用程式，請勿選取此核取方塊。

使用 Ivanti Bridge 的裝置可在以下關鍵區域得到增強。

- **登錄檔：**讀取、寫入與更新登錄值。
- **檔案：**驗證、讀取與更新檔案的內容。
- **應用程式部署：**新增將 .EXE 型應用程式安裝到桌上型裝置的能力。 這些應用程式可位於 Ivanti Neurons for MDM 伺服器或 Cloud 的內容傳遞網路 (CDN) 中。

Bridge 設定

設定 Ivanti Bridge 需要管理員按下列順序完成以下步驟:

1. 啟動橋接授權
2. 安裝 Bridge 應用程式
3. 上傳指令碼到裝置以供裝置永久或一次性使用。

啟動橋接授權

Ivanti Bridge 是舊版 Gold 套件和目前安全 UEM 套件的一部分。

安裝 Bridge 應用程式

啟動「Ivanti Bridge」授權後，即可安裝 Bridge 行動裝置應用程式，步驟如下:

1. 前往 **App > 應用程式目錄**。
2. 按一下 **+新增**。
3. 按一下商務版應用程式區段中的 **Ivanti Bridge**。
4. 新增詳細資料、按照所採購的授權，自訂與發佈 Bridge 行動應用程式到所需裝置上。
   若啟用了**無訊息自動安裝在 Windows 裝置上**選項，系統將會無訊息自動安裝橋接行動應用程式，並且橋接服務將在裝置上開始執行。

> Bridge app 預設新增至 App Catalog，而且也預設發佈至所有裝置。

> 將最新版本的 Ivanti Bridge 匯入租用戶目錄後，管理員可以檢視新調整的應用程式版本。

上傳指令碼到裝置

管理員可建立新的 Bridge 配置，藉此上傳指令碼到裝置以供永久使用：

1. 前往**組態 > +新增**。
2. 選取**適用於 Windows 指令碼和動作的 Ivanti Bridge 組態組**。
3. 輸入配置的名稱。
4. 輸入描述。
5. 在設定 Ivanti Bridge 區段中，使用以下兩個選項之一上傳指令碼:
   - 從指令碼程式庫中選取指令碼 - 從清單中選取其中一個可用的指令碼。
   - 或者
     上傳指令碼 - 按照步驟 7 下的表格所述指定設定。
     - 輸入**指令檔**類別設定，指定要在裝置上推送或執行的安裝指令碼。
     - (選填) 進入**復原指令檔**類別設定，指定要在裝置上推送或執行的解除安裝指令碼。 這在裝置汰換或配置刪除等情況下很有用。
     - (選用) 選擇**設定 Outlook** 選項，以使用 Bridge 在裝置上設定 Microsoft Outlook。

       > 僅支援 Outlook 2010 和 2013。

按一下**下一步**。

7. 選擇此配置的發佈。
   針對這些裝置動作自動完成強制登記。

類別	設定	方法
	名稱	輸入可識別此配置的名稱。
	描述	輸入可說明此配置用途的描述。
指令碼檔案	**所有版本 (Windows 10+ Desktop)** 指令碼檔案	選擇有效的指令碼或可執行檔 (.ps1、.reg、.exe)。 • 指定的指令碼檔案或可執行檔 (.ps1、.reg、.exe) 將會自動執行。 • 其他檔案類型只會複製到目標資料夾。
	指令碼引數	指定指令碼檔案的引數清單。 • 若是 Win32 (.exe) 檔案，請輸入引數以無訊息自動執行檔案 (例如 /SILENT 或 /VERYSILENT)。 這是強制作業。
復原指令碼檔案	目標資料夾 **所有版本 (Windows 10+ Desktop)** 指令碼檔案	指定指令碼檔案的目標資料夾。 • 如果未指定目標資料夾，則將使用 %TEMP% 系統環境變數的值做為目標資料夾。 選擇有效的指令碼或可執行檔 (.ps1、.reg、.exe)。 • 指定的指令碼檔案或可執行檔 (.ps1、.reg、.exe) 將會自動執行。 • 其他檔案類型只會複製到目標資料夾。
	指令碼引數 目標資料夾	指定指令碼檔案的引數清單。 • 若是 Win32 (.exe) 檔案，請輸入引數以無訊息自動執行檔案 (例如 /SILENT 或 /VERYSILENT)。 這是強制作業。 指定指令碼檔案的目標資料夾。 • 如果未指定目標資料夾，則將預設使用 %TEMP% 系統環境變數的值。

上傳指令碼到裝置以供一次性使用

管理員可上傳指令碼到裝置以供一次性 (臨時) 使用。

1. 前往**裝置 > 裝置**。
2. 按一下裝置名稱連結，以前往「裝置詳細資料」頁面。 這是將推送至其中/在其中執行一次性指令碼的 Windows 10 Desktop。
3. 按一下 ⋮ 圖示，然後按一下**透過 Ivanti Bridge 的指令碼和動作**。
4. 輸入名稱。
5. 在「指令碼檔案」區段中，指定要推送到裝置或在裝置上執行的指令碼，如前面表格所述。
6. 按一下**套用**。
   指令碼執行將會排入佇列，可能需要一些時間來完成。 前往「日誌」索引標籤，以檢查與檢視狀態 (輸出或故障訊息)。 針對這些裝置動作自動完成強制登記。

Bridge 日誌

此功能可讓您提取個別裝置的 Ivanti Bridge 記錄檔，進行應用程式的疑難排解和診斷。 日誌會裝置下次登記時送出。 您可等待下一次排程的同步，或執行強制裝置簽入以快速取得記錄。

若要從裝置提取日誌：

1. 前往**裝置 > 裝置**。
2. 按一下裝置名稱連結，以前往「裝置詳細資料」頁面。 這是將推送至其中/在其中執行一次性指令碼的 Windows 10 Desktop。
3. 按一下 ⋮ 圖示，然後按一下**提取 Ivanti Bridge 記錄檔**。 隨即顯示**提取 Ivanti Bridge 記錄檔**視窗。
4. 請選擇下列選項之一：
   單一日誌 – 要求 Ivanti Neurons for MDM 提取裝置上最近的 Bridge 日誌。
   全部日誌 – 要求 Ivanti Neurons for MDM 提取裝置上的所有日誌 (最多 30 天)。
5. 按一下**提取日誌**。 在裝置將日誌傳送到 Ivanti Neurons for MDM 之後，您可以從「裝置詳細資料」頁面上的「日誌」索引標籤檢視 Bridge 日誌。

> 只有使用**所有記錄**選項傳送的記錄只能以 zip 檔案的形式下載。

Bridge 上次簽入

在「裝置」頁上，「Bridge 上次簽入」欄會列出 Bridge 服務上次簽入的日期與時間。 可使用「自訂欄」選項將此欄新增至「裝置」頁面，依預設不會看見此欄。

若要看見此欄，請選取**裝置** > **自訂欄** > 選取 **Bridge 簽入**。

> 匯出的資料也會依適用狀況，盡量提供 Bridge 上次簽入詳細資訊。

橋接服務失敗修復

已在 Bridge 2.1.14 版本中引入「Bridge 服務失敗修復」。 依預設，此版本已對所有使用者匯入了應用程式目錄。 在某些罕見情況下，橋接服務可能以不明原因失敗。 在這種情況下，Bridge 2.1.14 及更新版本可提供支援。

9. 內容

請使用「內容」頁面來發佈由外部來源託管的內容。 內容可能包括使用者可以下載的檔案，例如業務簡報、影像、試算表與文件。

本節包含以下各主題：

- 管理內容
- 類別

9.1. 管理內容

本節包含以下各主題：

- 發佈託管的內容
- 刪除內容

託管的內容支援使用外部 URL 發佈可下載內容。 外部 URL 應僅會導向可下載的 PDF 或 EPUB 或 IBOOK 檔案，且外部 URL 必須包含這些副檔名。

不支援發佈 VPP Book 授權，因此不支援基於 iTunes Store ID 發佈 Apple Books。

在裝置上使用 Books 或 Pages 應用程式，從 Ivanti Neurons for MDM 存取推送內容。 您可在媒體庫區段中存取內容。

iBook 和 EPUB 內容可發佈至 iOS 8+ iPad 裝置 (Gold 授權)。 這些格式僅限於 iPad，因為 Apple 僅支援這些格式的 iPad 內部發佈。 此限制不適用於 iOS 9 裝置。

> 這些格式皆不提供內容預覽。

若是 **PDF** 內容，您可選擇將內容推送至 iOS 8+ 裝置上的 iBook app。

發佈託管的內容

雖然您無法將新文件上傳至 Ivanti Neurons for MDM，您可以提供內容託管所在的路徑 (URL)，並將它發佈至裝置群組。

程序

1. 前往**內容 > 託管內容**。
2. 按一下 **+新增**。
3. 輸入下列資訊：
   - 職稱
   - 作者
   - 類別
   - (選用) 描述
4. 在**託管內容路徑**欄位中，輸入您要上傳的檔案的 URL。
5. 按**下一步**。
6. 進行所需的發佈變更。
7. 按一下**完成**。

如要修改託管內容，必須刪除之前的內容，並且新增與發佈新的託管內容。

若要修改 URL 以外的設定：

1. 前往**內容 > 託管內容**。
2. 按一下**名稱**欄位中的文件連結。
3. 按一下「編輯」圖示。
4. 進行必要變更。

5. 按**下一步**。
6. 進行所需的發佈變更。
7. 按一下**完成**。

刪除內容

1. 按一下**名稱**欄位中的文件連結。
2. 選擇**動作 > 刪除此文件**。
3. 按一下勾選方塊確認。
4. 按一下**刪除文件**。

刪除文件時：

- 會將文件從系統中移除。
- 內容目錄中將不再提供此文件。
- 該文件也會從之前下載過的裝置上移除。

如果您無法在**內容**頁面上執行工作，可能是您沒有所需的權限。 您需要以下**角色**:

- App 及內容管理

9.2. 類別

本節包含以下各主題：

- 新增類別
- 移除類別

> 根據 2017 年 4 月 15 日公告的「結束內容支援」，已停用內容新增功能。 目前已上傳的內容仍可發佈至 Apple iBooks app 與進行使用。

類別說明{{內容類別}}中的{{內容}}類型。 類別可用來將內容分門別類，以讓使用者輕鬆找到所需的項目。 新增到內容目錄的每個項目都必須至少指派一個類別。

新增類別

程序

1. 按一下**新增** (左下角)。
2. 輸入類別名稱。 類別不區分大小寫。
3. 按一下**儲存**。

移除類別

您可以按一下類別旁邊的 X 以移除類別。

如果您無法在**內容（內容）**頁面上執行工作，可能是您沒有所需的權限。 您需要以下角色:

- App 及內容管理

10. 組態

配置是指您傳送給裝置的設定集合。 例如，您可以使用會自動設好裝置 VPN 設定和密碼需求的配置。 系統的現有配置會提列在「配置」頁面中。

本節包含以下各主題：

- 使用配置
- 建立使用者自助式入口網站配置
- 自訂配置
- 使用自訂組態將 SyncML 推送至裝置
- 首頁畫面版面配置
- App 控制配置：控制每台裝置要安裝哪些 App
- App 通知配置
- 滙出配置
- 優先排序配置
- 管理配置

10.1. 使用配置

本節包含以下各主題：

- 篩選配置的顯示
- 新增配置
- 發佈配置
- 慢速推出發佈組態
- 推送配置至多個裝置
- 排除配置
- 推送排除的配置
- 匯出配置
- 正在匯入組態
- 編輯組態
- 刪除配置
- 排程內部開發的應用程式更新
- 需要作用中使用者工作階段的 Windows 組態

組態是指身為管理員的您傳送給裝置的設定集合。 例如，您可以使用會自動設好裝置 VPN 設定和密碼需求的配置。 您系統的現有組態於「組態」頁列出。 您可從「組態」頁選取多個組態，並一次推送至多部裝置。 這些組態可推送至空間專屬裝置，以及其他仍未受影響空間中的裝置。 組態可以推送至單一空間，或一次推送至多個空間或全部空間。

有很多組態類型可用。 這些配置類型以下列基本類別來劃分：

- 安全性
- 使用者資源
- 企業網路存取
- 行動電話網路
- 其他 (其他配置)

您可針對大多數配置執行下列動作：

- 新增
- 編輯
- 複製
- 刪除
- 從特定裝置上排除一或多項配置
- 將一或多項已排除的配置推送至特定裝置

特定配置僅支援有限的動作：

- 您無法新增或複製某些配置，「iOS 啟用鎖定」就是這類配置之一。 因此，當您新增配置時，這類配置不會顯示在提列的動態磚當中，而僅會顯示在「配置」頁面。
- 您無法編輯或刪除系統定義的配置，「iOS 註冊適用的 SCEP」就是這類配置之一。

- 您可將某些配置標示為不可從裝置刪除或不可重新安裝。 這些配置即無法排除或推送至裝置。

篩選配置的顯示

顯示**配置**頁面時，其中會列出所有的配置。 若要將此清單限縮至特定配置，請使用作業系統和配置類型之下的篩選 (左側窗格)。 例如，若要限縮清單僅顯示 macOS 配置，請選擇**作業系統**區段中之下的 **macOS**。

您可從下拉式清單中選擇多個空間，以檢視所有或多個空間裝置上的配置。 當您將滑鼠游標移至顯示的配置上時，會出現快顯視窗，其中包含空間清單。 您可按一下空間，以顯示配置詳細資料頁面。

在 **Apple DDM** 下套用**支援的**篩選器，以輕鬆識別與 DDM 相關的組態，並更好地區分組態類型。

如要依名稱搜尋現有的配置，在**搜尋**欄位中輸入配置名稱。

從 Ivanti Neurons for MDM 版本 81 開始，全域管理員可以委派空間管理員，針對所有裝置和自訂發佈選項編輯動態產生的身分憑證。

新增配置

只有在下拉式清單中選取單一空間時，才會啟用此選項。

> 您一次可發佈最多 100 個配置檔案。

程序

1. 按一下**新增**。
2. 選擇您要建立的配置類型。
3. 按**下一步**。
4. 如果您不想立即啟用這項配置，可清除**啟用此配置**選項。
5. 選擇此配置的發佈層級：
    - **所有裝置** - 發佈配置到所有可用的裝置。 如要在多個空間委派配置，請選擇以下其中一個選項：
        - **請勿套用至其他空間**。
        - 若要跨不同空間委派配置，請選擇**發佈摘要** > **套用至其他裝置空間中的裝置**。
            - 選擇**允許空間管理員編輯發佈**勾選方塊以允許委派的空間管理員編輯發佈特定空間。
    - **無裝置** - 選擇此配置以便之後進行發佈。
    - **自訂** - 定義將會收到此配置的特定裝置組。 如要在多個空間委派配置，請選擇以下其中一個選項：
        - **請勿套用至其他空間**。
        - **發佈摘要** > **套用至其他空間中的裝置**。
            - 選擇**允許空間管理員編輯發佈**勾選方塊以允許委派的空間管理員編輯發佈特定空間。

      > 管理員可使用「自訂發佈」選項，將自訂配置發佈至裝置、裝置群組、使用者和使用者群組。 以下配置不適用於指派或發佈配置至使用者或使用者群組：

        - Android Enterprise: 工作設定檔 (Android for Work)
        - Android Enterprise: 工作受管理裝置 (Android for Work)
        - Android Enterprise: 具有工作設定檔的受管理裝置/公司擁有的裝置上的工作設定檔
        - 適用於工作受控裝置非 GMS 模式 (AOSP) 裝置的 Android 工作受控裝置 (裝置擁有者)

6. 如果您的服務已定義空間，您就必須指定配置是否要套用至其他空間以及優先順序為何。
7. 按一下**完成**。

> 如果配置會將命令發到裝置，而不會在裝置上安裝描述檔，則配置詳細資料中就不會將該配置提列為已套用至任何裝置。

發佈配置

全域管理員可委派空間管理員，以針對所有裝置和自訂分發選項編輯動態產生的身分憑證。 如需動態產生的憑證，您可以選擇**允許在所有空間中使用此配置**選項。 此選項提供動態產生的身份憑證給所有空間，而且可在 Exchange、Wi-Fi、VPN 及任何其他應用配置中使用，包括受管理的 app 配置。 此選項可用於以下情況：動態產生的身分認證只需要伴隨關聯配置發佈到裝置 (在非預設空間中)，不需要做為個別配置進行發佈。

程序

1. 如適用時，使用表中為個別組態指定的資訊來指定設定欄位。
2. 按**下一步**。
3. 選擇**啟用此配置**選項。
4. (選用) 選擇**允許在所有空間中使用此配置**。
5. 請選擇下列發佈選項之一：
   - **所有裝置**。 請選擇下列選項之一：
     - **請勿套用至其他空間**。
     - **套用至其他空間中的裝置**。
     - **以最高優先順序套用於其他裝置空間中的所有裝置**。 (這僅適用於 Wi-Fi 組態。)
     - **以最低優先順序套用於其他裝置空間中的所有裝置**。 (這僅適用於 Wi-Fi 組態。)
       - 選擇**允許空間管理員編輯發佈**勾選方塊以允許委派的空間管理員編輯發佈特定空間。
   - **沒有裝置** (預設)
   - **自訂**選擇下列其中一個選項:
     - **請勿套用至其他空間**。
     - **套用至其他空間中的裝置**。
     - **以最高優先順序套用於其他裝置空間中的所有裝置**。 (這僅適用於 Wi-Fi 組態。)
     - **以最低優先順序套用於其他裝置空間中的所有裝置**。 (這僅適用於 Wi-Fi 組態。)
       - 選擇**允許空間管理員編輯發佈**勾選方塊以允許委派的空間管理員編輯發佈特定空間。

> 身份憑證與空間無關，動態產生的身份憑證可配置給所有空間、發佈給所有裝置，以及套用到其他裝置空間中的所有裝置。

6. 按一下**完成**。

慢速推出發佈組態

使用**自訂**選項分發組態時，您可以使用慢速推出程序分發組態，以便及時推出組態。 您可以手動或排程方式排程緩慢推出發佈。

> 慢速推出發佈目前僅支援 VPN 和 Wi-Fi 組態。

程序

1. 前往**組態** > **新增**。
2. 搜尋所需的組態。
3. 輸入詳細資料，例如**名稱**、**說明**等。 根據組態，然後按一下**下一步**。
4. 選取**自訂**作為發佈選項。 **慢速推出發佈**區段會出現在畫面上。
5. 選取**使用慢速推出發佈方法**。 **手動推出**和**排程推出**選項會出現在畫面上。
   - **手動推出** - 使用此選項，您可以手動設定發佈目標的百分比。 只會完成指定的發佈百分比。 或者，您也可以選取**選擇摘要中的所有裝置**，將組態發佈到所有裝置。
   - **排程發佈** - 使用此選項以四個階段推出發佈。 對於每個階段，您可以指定推出百分比，確保每個後續階段的百分比都比上一個階段高。 階段之間的持續時間必須至少為一天，且不得超過 30 天。 最近儲存的組態會自動預先載入為可編輯範本，以供未來組態使用。
6. 選取組態必須分發到的所需群組。
7. 按一下**完成**。

您可以從**組態** > 新建立的組態 > **詳細資訊**來檢視詳細資訊。 在詳細資料頁面中，您可以暫停和繼續推出。

> 當您使用排程推出建立新的組態時，您在建立現有組態時所提供的百分比會轉送到新的組態。 您可以編輯詳細資訊，或以相同的百分比繼續。

推送配置至裝置

如果您想要將任何已排除的配置重新安裝到裝置上，您可以推送配置。

程序

1. 前往**裝置** > **裝置**。
2. 按一下裝置名稱，以檢視詳細資料頁面。
3. 前往**配置**。
4. 選擇勾選方塊以選擇要推送至裝置的特定配置。
5. 按一下**推送描述檔**。
6. 若要推送單一配置，請按一下**動作**欄位下方的**推送**。

推送配置至多個裝置

您可從「配置」頁面選擇多個配置，然後一次將它們推送至多部裝置。

程序

1. 登入 Ivanti Neurons for MDM 管理員入口網站。
2. 前往**配置**。
3. 選擇勾選方塊以選擇特定配置。
4. 按一下**動作**，選擇**推送選取的配置**至裝置。 推送配置精靈開啟，並顯示所有配置及其推送狀態。
5. 按一下**推送有效的配置**。 將大量配置推送至所有裝置。 將不會推送從**裝置** > **配置**標籤針對特定裝置排除的配置。

排除配置

您可排除某些之前已發佈的配置，從裝置將其手動移除。

程序

1. 前往**裝置** > **裝置**。
2. 按一下裝置名稱，以檢視詳細資料頁面。
3. 前往**配置**。
4. 選擇勾選方塊以選擇特定配置。
5. 按一下**排除描述檔**。

若要排除單一配置，請按一下**動作**欄位下方的**排除**。 所選的配置現已列在「排除的配置」標籤之下。

推送排除的配置

程序

1. 前往**裝置** > **裝置**。
2. 按一下裝置名稱，以檢視詳細資料頁面。
3. 前往**配置** > **排除的配置**。
4. 選擇一或多項要推送至裝置的配置。
5. 按一下**推送描述檔**。
6. 若要推送單一配置，請按一下**動作**欄位下方的**推送**。

匯出配置

您可將所選配置或所有配置的詳細資料從選取的空間匯出至個別檔案。

程序

1. 前往**配置**。
2. 選擇勾選方塊以選擇特定配置。
3. 按一下**動作** > **匯出選取的配置與詳細資料**。 如果您要匯出所有配置，請選擇**匯出所有配置與詳細資料**。
   一組 YAML 檔案會包含在 .ZIP 檔中。 此報告包含所選空間中所有現有配置的詳細資料。

匯出所有組態

匯出配置檔案，以傳送給支援中心用於診斷輔助。 您可以將單一組態檔案匯出為 Yaml 格式檔案，或將所有組態匯出成 .zip 檔案。 依據您要匯出的配置而定，您可以從「配置」頁面的不同區域匯出檔案。

程序

1. 前往**配置**。
2. 選擇勾選方塊以選擇特定配置。
3. 按一下**動作** > **匯出選取的配置與詳細資料**。 如果您要匯出所有配置，請選擇**匯出所有配置與詳細資料**。
   一組 YAML 檔案會包含在 .ZIP 檔中。 此報告包含所選空間中所有現有配置的詳細資料。

正在匯出自訂組態

程序

1. 前往**配置**。
2. 按一下 **+新增**以選擇配置。
3. 遵循下列步驟以自訂配置。
4. 按**下一步**。
5. 選擇發佈層級。
6. 按一下**完成**。
7. 從**配置**頁面清單中，選擇您剛建立的配置。
8. 按一下**動作**下拉式功能表，然後按一下 **「匯出」**。

。含有配置名稱與時間戳記 _yyyymmdd.yaml 的檔案會下載至您的裝置。

正在匯出現有組態

程序

1. 前往**配置**。
2. 選擇現有的配置。
3. 按一下**動作**下拉式功能表，然後按一下**匯出**。
   含有配置名稱與時間戳記 _yyyymmdd.yaml 的檔案會下載至您的裝置。

正在匯入組態

您可匯入含有組態詳細資訊的 YAML 檔案。 若要編輯組態，您可在 YAML 檔案中編輯詳細資訊，選取組態並匯入檔案，組態中就會顯示更新後的值。 如果選取超過一個組態或空間，「匯入」按鈕會停用。 如果選取的檔案類型不正確，會顯示錯誤訊息。 如果您選取的 YAML 檔案包含的詳細資訊與組態要求不同，會顯示錯誤訊息。

程序

1. 前往**配置**。
2. 選取組態，按一下**匯入**，按一下**選擇檔案**，選取 YAML 檔案，然後點選**匯入**。 含有組態詳細資訊的 YAML 檔案就會匯入。

支援的允許清單中的組態

- 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
- 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

使用 YAML 檔案建立組態

您可以從 YAML 檔案建立組態。 發佈相關規格不屬於 YAML 檔案。 發佈的預設設定是「無裝置」。

程序

1. 前往**配置**。
2. 按一下**匯入**，按一下**選擇檔案**，選取 YAML 檔案，然後點選**匯入**。 含有組態詳細資訊的 YAML 檔案就會匯入。 「建立組態」頁隨即開啟，並顯示 YAML 檔案中新增的所有詳細資訊。
3. 選取發佈類型之一:
   - **所有裝置**
   - **沒有裝置**

- **自訂**

4. 確認組態的詳細資訊，然後選取下列其中*一個*「發佈摘要」選項:

> 發佈摘要無法提供所有組態使用。

- **不套用至其他空間**
- **套用至其他空間中的裝置**

5. 如果組態的新名稱符合現有組態名稱，會顯示錯誤訊息。按一下**確定**，按一下**返回**，然後編輯組態名稱。
6. 按一下**下一步**，然後按一下**完成**。

編輯組態

您可以開啟組態並直接編輯組態的詳細資訊，或者匯入包含所有必要詳細資訊的 YAML 檔案。 如果選取超過一個組態或空間，「匯入」按鈕會停用。

程序

1. 前往**配置**。
2. 選取並開啟組態，按一下編輯 (鉛筆) 圖示，然後編輯組態。
3. 或者從編輯組態頁按一下**匯入**圖示，選取 YAML 檔案，然後點選**匯入**。 「編輯組態」頁隨即開啟，並顯示 YAML 檔案中新增的所有詳細資訊。
4. 確認組態的詳細資訊，然後選取下列其中一個「發佈摘要」選項:

> 發佈摘要無法提供所有組態使用。

- **請勿套用至其他空間**。
- **套用至其他空間中的裝置**

  > 發佈預設為「無裝置」。

5. 按一下**完成**。

刪除配置

您可刪除選取的配置。

程序

1. 選擇勾選方塊以選擇特定配置。
2. 按一下**動作** > **刪除**。

排程內部開發的應用程式更新

當裝置簽入時，Ivanti Neurons for MDM 會自動更新內部應用程式。 管理員現在可以根據伺服器時區安排內部應用程式更新時間。 只有當裝置在排程時間內登記，應用程式才能更新。 根據預設，應用程式更新排程會停用。

> 此組態僅適用於更新，並不適用於全新安裝。 您可使用傳送安裝/更新指令，以覆寫 iOS 應用程式的自動更新排程。 如果是在應用程式級別或目錄級別啟用自動更新，其將優先於排程的應用程式組態，並且應用程式會在簽入時立即更新。

此組態僅適用於下列應用程式類型:

- iOS 內部開發的應用程式。
- 僅在 DO 模式下的 Android 內部開發的應用程式。
- 格式為 .pkg 和 .MIP 的 macOS 應用程式。
- Windows 應用程式。

必要條件

請確認以下的必要條件符合配置，才能如預期般運作：

- 應用程式必須針對 iOS 和 Android 加以管理。 針對 macOS，應用程式可以處於受管理或不受管理狀態。
- 請確定在「應用程式配置」之下的「在裝置上安裝」選項已啟用。
- 必須在排程時間內登記裝置。

程序

1. 登入 Ivanti Neurons for MDM 管理員入口網站。
2. 前往**配置**。
3. 按一下**新增**。 「新增配置」頁面開啟。
4. 搜尋 **App 自動更新**。 「建立 App 自動更新配置」頁面開啟。
5. 在**名稱**欄位中指定名稱。
6. 從**配置設置**區段，從下拉清單中選擇**時區**。
7. 從下拉清單中選擇**開始時間**，然後從下拉清單中選擇**期間**。
8. 按**下一步**。
9. 選擇所需的使用者和裝置群組，然後按一下**啟用此配置**勾選框。
10. 按一下**完成**。 套用配置，應用程式現在只會在指定排程進行更新。

如果您無法看到「配置」頁面，可能是您沒有所需的權限。 您需具備下列其中一個角色：

- 裝置管理
- 裝置唯讀

相關主題：

- 空間
- 優先排序配置

需要作用中使用者工作階段的 Windows 組態

某些 Windows 組態需要作用中的使用者工作階段 (即有使用者已登入裝置) 才能進行佈建。 如果沒有使用者登入，這些組態會在 MDM 使用者登入裝置後套用。

下列組態需要作用中的使用者工作階段:

- 密碼
- 使用者憑證 (使用者範圍的身分識別憑證)
- Windows 防火牆
- Exchange
- VPN
- Windows 授權
- Microsoft Defender for Endpoint
- Windows 設定 (使用者範圍)
- Bridge 服務相依組態
- 現代/UWP 應用程式

Bridge 服務相依組態

只有在有作用中的使用者工作階段時，才會佈建需要 Ivanti Bridge 服務的組態。 範例包括 Windows 桌面限制、瀏覽器設定、開始功能表、資訊站、BIOS、Windows 指令碼、GPO 和其他 Bridge 服務相依組態。

例外: 下列預設的 Bridge 指令碼不需要使用中的使用者工作階段，並且會傳送到裝置，無論 MDM 使用者是否已登入:

- get-device-data.ps1
- get-bitlocker-status.ps1
- device-hardware.ps1

現代/UWP 應用程式

只有當使用中使用者工作階段可用時，才會佈建現代/UWP 應用程式。 這包括:

- 封裝為 .appx 或 .appxbundle 的內部應用程式
- Microsoft Store/UWP 應用程式

傳統 MSI 和 EXE 應用程式不受此要求約束。

> 如果設定排程部署時無法使用所需的使用者工作階段，則組態會在 MDM 使用者登入裝置後自動佈建。

10.2. 建立使用者自助式入口網站配置

身為企業使用者，您可使用自助式入口網站來管理您的裝置和憑證。 「我的裝置」標籤會顯示您已註冊的裝置。

您可從「我的裝置」標籤執行以下工作：

- 鎖定
- 取消鎖定
- 淘汰
- 重設安全應用程式密碼

您可從「我的憑證」標籤執行以下工作：

- 上傳認證

> 您一次可發佈最多 100 個配置檔案。

程序

1. 登入 Ivanti Neurons for MDM 管理員入口網站。
2. 按一下**新增**。
3. 搜尋**建立使用者自助式入口網站配置**。
4. 按**下一步**。
5. 如果您不想立即啟用這項配置，可清除**啟用此配置**選項。
6. 選擇此配置的發佈層級：
    - **所有裝置** - 發佈配置到所有可用的裝置。 如要在多個空間委派配置，請選擇以下其中一個選項：
        - **請勿套用至其他空間**。
        - 若要跨不同空間委派配置，請選擇**發佈摘要** > **套用至其他裝置空間中的裝置**。
            - 選擇**允許空間管理員編輯發佈**勾選方塊以允許委派的空間管理員編輯發佈特定空間。
    - **無裝置** - 選擇此配置以便之後進行發佈。
    - **自訂** - 定義將會收到此配置的特定裝置組。 如要在多個空間委派配置，請選擇以下其中一個選項：
        - **請勿套用至其他空間**。
        - **發佈摘要** > **套用至其他空間中的裝置**。
            - 選擇**允許空間管理員編輯發佈**勾選方塊以允許委派的空間管理員編輯發佈特定空間。
7. 如果您的服務已定義空間，您就必須指定配置是否要套用至其他空間以及優先順序為何。
8. 按一下**完成**。

> 如果配置會將命令發到裝置，而不會在裝置上安裝描述檔，則配置詳細資料中就不會將該配置提列為已套用至任何裝置。

10.3. 自訂配置

本節包含以下各主題：

- 定義自訂配置
- 自訂配置設定

授權：Silver

適用於: iOS、macOS、tvOS、Android 和 Windows

描述

可讓您匯入並發佈預先定義的配置檔案。

有效的配置檔案格式如下所述：

作業系統	有效的配置檔案格式
iOS 和 tvOS	• .plist • .mobileconfig • .xml
macOS	• .plist • .mobileconfig
Android	.xml。 目前，此功能僅支援適用於 Zebra 裝置的 .xml 配置。
Windows	SyncML

定義自訂配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入「自訂」，然後按一下**自訂**配置。
   隨即顯示「自訂配置」詳細資料頁面。
4. 在此頁面上進行設定。 請參閱自訂配置設定一節中的表格，以取得 相關值說明。
5. 按**下一步**，確認發佈設定。
6. (macOS 裝置) 針對這項配置，依據您所需的行為，在**此配置的套用目標**設定中，選擇其他選項：
   - 整個裝置 (最常使用)。
   - 特定使用者 (目前註冊的使用者)。

按一下**完成**。

自訂配置設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
選擇作業系統	按一下作業系統圖示，以上傳所選圖示的相對應配置檔案。
選擇檔案	此選項會在您選擇作業系統之後顯示。 將配置檔案拖曳至拖放方塊，或按一下**選擇檔案**按鈕以選擇配置檔案。

自訂 CSP 組態 (僅限 Windows)

只能在 Windows 裝置上建立自訂 CSP 組態。 當您從「選擇作業系統」區段中選取「Windows 作業系統」時，將獲得兩個選項:

選項 1 - CSP XML 檔案 - 選取此選項並按照與**選取檔案**設定相同的所述程序操作。

選項 2 - 自訂 CSP OMA-URI 結構描述節點

程序

1. 從清單中選取「自訂 CSP OMA-URI 結構描述節點」選項。 螢幕上出現「自訂 CSP 組態」區段。
2. 在**動作**下，按一下 + 按鍵，開始建立包含不同 OMA-URI 欄位的組態。
3. **新增列**快顯示窗出現在螢幕上，包含以下欄位:
    - 描述 - 輸入關於設定的任何一般資訊
    - OMA-URI - 輸入要用作設定的 OMA-URI
    - 資料類型 - 選取要用於此設定的資料類型 - DATE、FLOAT、BASE64、NODE、XML、BINARY、CHARACTER、TIME、BOOLEAN、INTEGER
    - 值 - 輸入與所選取資料類型關聯的值
    - 存取類型 - 新增、刪除、執行、取代、取得

按一下**儲存並關閉**，關閉含有已提供詳細資料的視窗。 按一下**儲存並新增**，另外建立新的一列。

5. 按**下一步**。
6. 選取發佈模式，然後按一下**完成**。

相關主題

- 使用自訂配置將 SyncML 推送至裝置
- 如何建立配置

10.4. 使用自訂組態將 SyncML 推送至裝置

您可以建立自己的同步標記語言 (SyncML) 配置檔案，或從第三方來源取得，以藉由在自訂配置中新增該檔案來實作自訂功能。

支援的平台：

- Windows

支援的裝置:

- Windows 10+
- Microsoft HoloLens 2

程序

1. 前往**配置**。
2. 按一下 **+新增**。
3. 按一下**自訂配置**以顯示**建立自訂配置**頁面。
4. 輸入配置的名稱。
5. 按一下 Windows 作業系統圖示。
6. 將 SyncML 檔案拖放至介面中，或按一下**選擇檔案**來導覽檔案，以選擇要上傳到裝置的檔案。

> Ivanti Neurons for MDM 不會對檔案中的程式碼執行任何驗證檢查。

7. 按**下一步**。

自訂 SyncML 記錄

可在「裝置記錄」索引標籤下查看傳送給 Windows 裝置的 SyncML 命令，以及裝置對這些命令的 SyncML 回應。 此記錄資訊將在傳送 **Windows 自訂 SyncML** 組態後可用。 當系統傳送自訂 SyncML 組態時，無論 SyncML 的回應為何，其在裝置上「組態」索引標籤中的組態將一律為「已安裝」狀態。

10.5. 首頁畫面版面配置

主畫面版面配置組態會定義主畫面上應用程式、資料夾和 Web 剪輯的版面配置。

本節包含以下各主題：

- 定義首頁畫面版面配置
- 首頁畫面版面配置設定

授權：Silver

符合條件的裝置:

- 僅限 iOS 9.3+ 受監管
- 僅限 tvOS 受監管

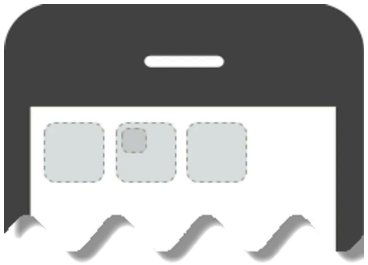
定義首頁畫面版面配置

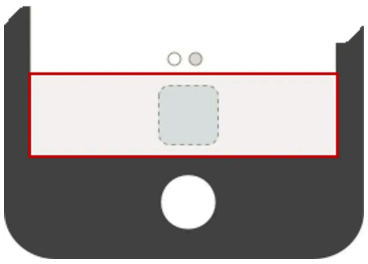
程序

1. 前往**組態** > 按一下 **+新增**。
2. 在搜尋欄位中輸入「首頁」，然後按一下**首頁畫面版面**組態。 「首頁畫面版面組態」詳細資料頁面隨即開啟。
3. 在此頁面上進行設定。 請參閱 Home_Screen_Layout_Configuration_Settings 一節，以取得相關值說明。
4. 按一下**下一步**以設定發佈設定。 針對共享 iPad 裝置，請選取**裝置**通道或**使用者**通道。 如需更多資訊，請參閱使用配置。
5. 按一下**完成**。

首頁畫面版面配置設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
固定	按一下 + 圖示將應用程式或 Web 剪輯新增到主畫面的停駐位置 (此處強調顯示)，然後按照後續螢幕上的說明操作: 您可輸入 Apple 套件 ID (開頭為「com.apple」) 以手動新增系統應用程式。 例如，輸入 'com.apple.DocumentsApp' 以新增「檔案」app。
第 1 頁	按一下 ⊕ 以將 app 或 Webclip 新增至首頁畫面的頁面區域中，在這裡以醒目提示的方式顯示，然後遵循畫面上的指示： 您可以按一下「新增頁面」，將另一頁面新增到電話顯示。







10.6. App 控制配置：控制每台裝置要安裝哪些 App

App 控制配置可讓您在裝置層級將 app 分類為允許清單或封鎖清單。 已安裝的 app 將無法顯示，也無法啟動。 App 仍可在 App Store 中看到，但無法下載或啟動。 將這項配置發佈給任何裝置時，這些裝置就會使用此配置而忽略「允許的 App 原則」設定。 此配置會取代參考目標裝置上相同應用程式的任何 app 相關原則。

此配置會取代參考目標裝置上相同應用程式的任何 app 相關原則。 若是 Windows 10 裝置，則必須在裝置層級進行限制，因此要強制執行 app 規則時只能透過配置來進行。

App 控制配置可讓您建立：

- **允許清單：**僅允許明確新增至此清單的 app。 裝置上將無法安裝任何其他的 app。
- **封鎖清單：**不允許裝置上安裝特定的 app。

支援裝置

您可使用 App 控制配置在以下裝置上將不同的 app 列入封鎖清單或允許清單：

- 公司擁有的裝置上的 Android 工作描述檔
- 僅限 iOS 9.3+ 受監管
- tvOS 11+
- Windows

建立 App 控制配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在顯示的**選擇配置**欄位中，輸入 **App 控制**，然後選擇 **App 控制**配置。
4. 輸入配置的名稱與描述。
5. 選擇作業系統，然後繼續下方的區段以將其套用至您的作業系統。

公司擁有的裝置上的 Android 工作描述檔

使用者可新增最多 50 個應用程式 ID 至允許清單或封鎖清單群組。

程序

1. 選擇**建立個人 App 的允許清單**或**建立個人 App 的封鎖清單**，以新增適合應用程式的允許清單或封鎖清單。
2. 輸入應用程式 ID (com.example.com) 然後按一下新增。
3. 按**下一步**，然後選擇發佈選項。
4. 按一下**完成**。

iOS 9.3 受監管的裝置

程序

1. 選擇要建立允許清單或封鎖清單。

2. 按一下**新增 App**。
3. 按一下下列其中一個或兩個索引標籤，藉此選擇允許清單或封鎖清單的 app：
    - 按一下**藉由查閱來新增**，從 App Store 或 App Catalog 搜尋並選擇 app。
    - 按一下**手動新增**，藉由輸入 Apple 系統 app 的 Apple 套件 ID (開頭為 com.apple) 來選擇 app。

按一下**允許清單**或**封鎖清單**索引標籤，以檢閱獲選進入允許清單或封鎖清單的 app 清單。

5. (選用) 選擇**隨附所有 Webclip** 選項。
6. 按**下一步**，然後選擇發佈選項。
7. 按一下**完成**。

Windows 裝置

程序

1. 選擇**允許**或**不允許**將適合的應用程式清單新增至允許清單或封鎖清單。
2. 在**規則定義**區段之下，從清單中選擇 **App 類型**。
3. 在 **App 識別碼**方塊中輸入識別碼名稱，以搜尋特定 app。 您也可以使用**查閱 App** 連結以開啟新對話方塊，並搜尋 Windows 特定 app 識別碼。
4. (選用) 在 **App 描述**方塊中輸入 app 的一些描述。
5. 使用 **+新增**連結，以新增更多規則定義至允許清單或封鎖清單 app。
6. 按**下一步**，然後選擇發佈選項。
7. 按一下**完成**。

10.7. App 通知配置

選擇使用者要以何種方式接收所選 app 的通知。

適用於： iOS 9.3+ 受監管裝置。

建立 App 通知配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入通知，然後按一下 **App 通知**配置： 隨即顯示「App 通知配置設定」頁面。
4. 命名配置，並加以描述。
5. 若要新增 App，您可以查閱 App Store 或手動使用套件 ID。
6. 選擇要套用此 app 通知設定的 app。
7. 設定通知設定。 此處為您可選擇的通知。
    - 允許通知
        - 顯示於通知中心
        - 音效
        - 標記 App 圖示
        - 顯示於鎖定畫面
        - (iOS 12.0+ 受監管) 使用 CarPlay 時顯示重要警示
        - (iOS 12.0+ 受監管) 允許啟用重要警示 (忽略「請勿打擾」)
    - 解除鎖定警報樣式
        - 橫幅
        - 強制回應警報
        - 無
    - (iOS 12.0+ 受監管) 群組類型
        - 自動
        - 依據 app
        - 關閉
    - (iOS 14.0+) 通知預覽類型 - 選擇要在裝置通知訊息預覽中顯示的預覽類型。
        - 受使用者控制 - 依裝置上的 app 使用者設定顯示訊息預覽。
        - 永遠 - 顯示訊息預覽。
        - 當解除鎖定時 - 只有在裝置解除鎖定時才顯示訊息預覽。
        - 從不 - 防止 app 在通知中顯示訊息預覽。
8. 按**下一步**，確認發佈設定。
9. 按一下**完成**。

如需更多資訊，請參閱[如何建立配置]。

10.8. 滙出配置

匯出配置檔案，以傳送給支援中心用於診斷輔助。 您可以將單一配置檔匯出為 Yaml 格式檔案，或將所有配置匯出為 .zip 檔案。

程序

匯出配置

依據您要匯出的配置而定，您可以從「配置」頁面的不同區域匯出檔案。

匯出所有配置：

1. 前往**配置**。
2. 選擇勾選方塊以選擇特定配置。
3. 按一下**動作** > **匯出選取的配置與詳細資料**。 如果您要匯出所有配置，請選擇**匯出所有配置與詳細資料**。
   一組 YAML 檔案會包含在 .ZIP 檔中。 此報告包含所選空間中所有現有配置的詳細資料。

匯出自訂配置：

1. 前往**配置**。
2. 按一下 **+新增**以選擇配置。
3. 遵循下列步驟以自訂配置。
4. 按**下一步**。
5. 選擇發佈層級。
6. 按一下**完成**。
7. 從**配置**頁面清單中，選擇您剛建立的配置。
8. 按一下**動作**下拉式功能表，然後按一下 **「匯出」**。

。含有配置名稱與時間戳記 _yyyymmdd.yaml 的檔案會下載至您的裝置。

匯出現有的配置：

1. 前往**配置**。
2. 選擇現有的配置。
3. 按一下**動作**下拉式功能表，然後按一下**匯出**。
   含有配置名稱與時間戳記 _yyyymmdd.yaml 的檔案會下載至您的裝置。

10.9. 優先排序配置

如果您針對配置選擇多個裝置群組，則可能會將相同類型的多個配置指派給特定裝置。當同類配置套用到相同裝置時，會由定義的優先順序來判斷要套用哪項配置。 最高優先順序的配置其編號最小。 例如，優先順序為 1001 的配置會比優先順序為 1002 的配置有更高的優先權。 服務會自動指派編號。

> 無法將 Wi-Fi 優先順序套用至裝置，它已從優先順序豁免。

只有當頁面包含兩個或以上的同類配置，且在下拉式清單中選取單一空間時，才能使用此選項。 您可變更配置的優先順序。

程序

1. 前往**配置**。
2. 在尚未選擇任何配置時，選擇**動作 > 優先排序配置**。
   如果沒有顯示**動作**，就表示沒有需要優先排序之類型的多個配置。
3. 請使用方向箭頭移動配置，將最高優先順序的配置移到最頂端。

> 鎖定圖示表示您必須編輯配置內的「所有裝置」發佈設定，才能變更配置的優先順序。

按一下**儲存**。

> 優先排序可處理多達 400 個配置。

如果您無法看到「配置」頁面，可能是您沒有所需的權限。 您需具備下列其中一個角色：

- DeviceManagement
- DeviceReadOnly

10.10. 管理配置

本節包含以下各主題：

- AppConnect 組態
- 安全性配置
- 使用者資源配置
- 企業網路存取配置
- 行動數據
- 其他配置

10.10.1. 配置類型

本節包含以下各主題：

- 搜尋組態
- 安全性
- 使用者資源
- 企業網路存取
- 行動電話通訊網路
- 更多配置
- 裝置同步配置

搜尋組態

使用**選擇組態**頁面上的搜尋和篩選器功能尋找要套用的組態。

程序

1. 選擇**配置**。
2. 選擇所列的其中一項配置，或按一下 **+新增**按鈕。
3. 這時會顯示**選擇配置**頁面。
   按一下所列的其中一項配置，或者：
   - 在搜尋方塊中輸入配置名稱
   - 按一下搜尋方塊右側的篩選圖示，即可顯示與平台相容的配置類型。

按一下配置按鈕，以存取配置設定選項。

如需更多資訊，請參閱使用配置。

安全性

類型	用途	適用裝置	所需授權
Android Enterprise	指定 Android Enterprise 選項	Android Enterprise	銀級
AppConnect 裝置	指定裝置上已啟用 AppConnect 的應用程式的安全性設定	• Android • iOS	金級
Apple 金輪證明	在 Apple 裝置上為特定金鑰啟用 WebAuthn 企業證明。	• macOS	
Entra ID (Azure 租用戶)	透過將 Ivanti Neurons for MDM 連線至 Entra ID，您可以使用受管理裝置的裝置合規性狀態，條件式存取 Microsoft 365 應用程式。	• iOS • Android	• 針對新的客戶：Secure UEM Premium • 針對現有的客戶：Platinum
認證	與伺服器建立信任	• Android • iOS • macOS • watchOS • visionOS • tvOS	
憑證透明度	控制憑證透明度強制執行 (只在裝置設定檔中顯示)。	• iOS • macOS • tvOS • watchOS • visionOS	
裝置記錄	從裝置擷取額外記錄，例如網路與安全性記錄。	• Android Enterprise	
磁碟管理組態	定義管理外部和網路儲存裝置的原則。	• 受監督的 macOS 15.0+	
Android 加密	提示使用者開始加密。	Android	
加密 DNS	可讓您增強安全性，無需設定 VPN。	• iOS • macOS • visionOS	金級
外部智慧設定	允許外部智慧整合	• iOS 26.4+	

類型	用途	適用裝置	所需授權
		• macOS 26.4+ • visionOS 26.4+	
行動威脅防護	可保護受管理裝置，防止行動威脅和漏洞影響裝置、網路及應用程式。	• Android • iOS	
威脅防護本機動作	建立並發佈內容如下的裝置配置：定義當支援威脅防護的用戶端偵測到威脅時，要在受支援 Android 裝置上採取的本機動作。	Android	
FileVault 2	提供可在磁碟區內容上執行完整 XTS-AES 128 磁碟加密的功能。	macOS	金級
FileVault 復原金鑰	決定將 FileVault 修復金鑰重新導向至企業伺服器的設定。	macOS	金級
身份憑證	• 可進行伺服器與裝置的驗證。 • 可進行網路資源與裝置的驗證。	• Android • iOS • macOS • watchOS • visionOS	
iOS 啟用鎖定	啟用受監管裝置上的 Apple「啟用鎖定」功能。	iOS	銀級
iOS 自訂配置	發佈不同 app 所建立的 iOS 配置描述檔。	iOS	
iOS 限制	• 鎖定裝置的功能。 • 啟用裝置的功能。	• iOS • watchOS • visionOS	
智慧設定	允許 Apple Intelligence 整合。	• iOS 26.4+ • macOS 26.4+ • visionOS 26.4+	
會議室顯示器	在 Apple TV 上啟動會議室顯示器模式。	tvOS 10.2+	
鍵盤設定	允許裝置管理鍵盤行為、輸入選項和相關的使用者體驗設定。	• iOS 26.4+ • macOS 26.4+	
鎖定與單一應用：Android	• 鎖定裝置的功能。 • 重新啟用裝置的功能。	Android	

類型	用途	適用裝置	所需授權
	• 套用單一應用功能。		
鎖定與單一應用：Android Enterprise	• 定義在 Android 企業裝置上限制使用的功能與 app。 • 套用單一應用功能。	Android 5.0 +	
鎖定與單一應用：Samsung Knox Standard	• 定義在 Samsung Knox Standard 裝置上限制使用的功能與 app。 • 套用單一應用功能。	Samsung Knox	
本機管理員密碼解決方案組態	允許管理員以設定的時間間隔在受管理的 macOS 裝置上自動重新產生本機管理員密碼	macOS	
macOS 防火牆	管理 macOS 裝置上可透過「安全性喜好設定」窗格存取的「應用程式防火牆」設定。 管理員可以將裝置指定為不受 Ping 命令的探索，以啟用隱形模式。	macOS 10.12+	金級
macOS 限制	決定已在 macOS 裝置上啟用的限制。	macOS	金級
macOS AppStore 限制	定義要在 macOS AppStore 中啟用哪些限制。	macOS	金級
macOS 燒錄光碟限制	管理 macOS 中的磁碟燒錄限制。	macOS	金級
適用於 macOS 的 Mobile@Work	為適用於 macOS 的 Mobile@Work 建立與發佈執行規則。	macOS	金級
適用於 macOS 的 Mobile@Work 指令碼	建立用於發佈至 Mobile@Work for macOS 的指令碼。	macOS	金級
身分偏好設定	識別使用者鑰匙圈中的「身份偏好設定」項目，此鑰匙圈會參照相同描述檔中所附的身份裝載。	macOS	金級
憑證偏好設定	識別使用者鑰匙圈中的「憑證偏好設定」項目，此鑰匙圈會參照相同描述檔中所附的憑證裝載。	• macOS	金級
允許的媒體控制	設定實體媒體的裝載、卸載和退出選項。	macOS	金級
macOS Finder 設定	管理 macOS 中的 Finder 應用程式設定。	macOS	金級
macOS 核心擴充原則	控制載入「使用者核准的核心擴充」的限制與設定。	macOS	金級
Active Directory (macOS)	設定進階選項以綁定 macOS 裝置與 Active Directory (AD) 網域，藉此存取依賴 AD 提供身份認證與安全性的軟體服務。	macOS	金級

類型	用途	適用裝置	所需授權
Office 365 自動帳戶建立 (macOS)	設定使用者資訊與選項，以便為所有的 Microsoft Office 365 應用程式設置初始配置。	macOS	金級
Apple 應用程式目錄	管理透過網頁剪輯存取 Apple 應用程式目錄。	• iOS • macOS	
受管理的網域	指定信任的電子郵件及網頁網域。	• iOS 8+ • visionOS 1.1+	銀級
密碼	• 將密碼設為必要。 • 指定密碼長度與內容。 • 變更密碼需求。	• Android • iOS • macOS • watchOS	
隱私權偏好設定 (macOS)	設定允許哪些應用程式取得系統服務、系統檔案及系統資源的存取權。	macOS	金級
驗證	提供雲端服務和/或桌面登入無密碼驗證。	• macOS • Windows	
隱私權配置	指定是否收集位置資料。	• iOS • Android • Windows	
用戶端隱私權聲明資訊	向 Go 用戶端使用者顯示隱私權政策。	• Android • Android Enterprise • iOS	
Ivanti Go Client 設定	用於設定透過 MixPanel 收集資料，包括進行疑難排解與提供最高品質服務所需的裝置及使用情況資訊。	• iOS • macOS	
Safari 擴充功能設定組態	管理來自不同網域的 Safari 瀏覽器擴充功能。	• 受監督的 iOS 18.0+ • 受監督的 macOS 15.0+	
Siri 設定	允許裝置存取和使用 Siri 設定。	• iOS 26.4+ • macOS 26.4+	

類型	用途	適用裝置	所需授權
		• watchOS 26.4+ • visionOS 26.4+	
服務組態檔案組態	管理員可以集中管理和部署各種系統服務的組態檔案。	macOS	
軟體更新	針對作業系統更新建立和發佈規則。	• iOS • macOS • Windows	
軟體更新設定組態	建立和更新「軟體更新強制執行」設定。	• 受監督的 iOS 18.0+ • 受監督的 macOS 15.0+	
時間伺服器	可讓裝置連接自訂的時間伺服器。	macOS	金級
Web 內容篩選	可控制 Safari 的內容。	• 受監督的 iOS 7 • visionOS 1.1+	Silver
Windows_Firewall	Windows 防火牆組態有各種防火牆限制。 根據管理員套用的防火牆限制，防火牆狀態會導致 Windows 裝置上的「安全性喜好設定」窗格中出現下列其中一種防火牆狀態: • 防火牆已開啟且正在監控。 • 防火牆已停用。 • 防火牆並未監控所有網路，或是部分規則已關閉。 • 防火牆暫時未監控所有網路。 • 不適用。	Windows 10+	
Windows 資訊保護	定義 Windows 資訊保護 (WIP) 設定以保護企業資料。	Windows 10+	金級
Windows 限制	決定哪些功能可在 Windows 10+ 裝置上使用。	Windows 10+	
Windows AI 管理組態	可讓您管理 Windows AI 設定和組態。	Windows 10+	

使用者資源

類型	用途	適用裝置	所需授權
CalDAV	• 設定 CalDAV 伺服器 (如 Google 行事曆) 的存取權	• iOS • visionOS	
CardDAV	• 可設定 CardDAV 伺服器 (如 Google 聯絡人) 的存取權	• iOS • visionOS	
電子郵件	• 可設定 POP/IMAP 電子郵件 (如 Gmail) 的存取權	• iOS • visionOS	
Exchange	• 可為 Android 和 iOS 行動裝置設定 ActiveSync 電子郵件 (如 Outlook) • 可為 macOS 裝置設定 Exchange Web 服務 (EWS) 電子郵件 • 定義要與裝置同步到何種程度 • 定義電子郵件的安全性	• Android • iOS • macOS • visionOS	• macOS 不支援透過 Sentry 使用 Exchange • 「要同步處理的電子郵件經過天數」旗幟不適用於 macOS
Google	• 建立 Google 帳戶配置，以便讓 iOS 9.3.2+ 裝置連接 Google 帳戶。 • 指定要用哪個 app 來與 Google 系統中的聯絡人進行音訊通話。	• iOS • visionOS	
字型	• 可安裝非標準字型以便正確顯示文件	• iOS	
訂閱的行事曆	• 可設定網際網路行事曆的訂閱	• iOS • visionOS	
Web Clip	• 顯示網頁的捷徑 (圖示)	• iOS • macOS	
內容快取	• 提供內容快取服務，以啟用 App Store 軟體的本機複本，並 • 啟用連線用戶端，以提高軟體和 app 下載速度。	• macOS	

企業網路存取

類型	用途	適用裝置	所需授權
AirPlay	• 可設定其他裝置的存取權，以便顯示媒體	• iOS • macOS	Silver
AirPrint	• 可設定無線列印	• iOS • macOS	Silver
一律開啟 VPN	• 可設定不需使用者互動的 VPN 伺服器存取權	• Android 7.0+ • iOS 8+	• Gole 適用於 Android 企業 • Silver 適用於 iOS
預設的 App 執行時期權限	• 可針對部署至 Android 企業裝置的 app，設定執行時期權限配置。	• 針對 Android API 23+ 所建立的 App，以及在 Android 企業裝置上執行 Android 6.0+ 的 App。	
教育	• 設定領導者和成員的「Apple 教育方案」內容及「課堂」app。	• supervised iOS 9.3+	金級
全域 Proxy	• 可設定裝置將 HTTP 流量轉送至 Proxy 伺服器	• 受監管的 iOS 7 • 受監管的 tvOS	Silver
LDAP	• 可設定公司目錄的存取權	• iOS • visionOS	
Tunnel	• 使用 Tunnel 定義用戶端與 Sentry 之間的每個應用程式 VPN 連線。	• iOS 7+ • macOS 10.13+ • Windows 10+ • Android	
橋接	• 允許 IT 在更新 UEM 上的 Windows 作業時，保留所有關鍵功能	• Windows 10+ Desktop	Bridge 授權
macOS 伺服器	• 使用已配置的帳號類型和相關設定來定義 macOS Server 帳號。 允許使用者啟用伺服器上的檔案共用。	• iOS 10+	
Per-App VPN	• 可設定特定 app 和 VPN 伺服器之間的連線	• iOS • watchOS • visionOS • tvOS	Silver
網路轉送組態	• 新增組態以定義網路轉送的設定	• iOS • macOS • visionOS	

類型	用途	適用裝置	所需授權
單一登入	• 針對特定的受管理 app 設定單一登入	• iOS • macOS • visionOS	
多位使用者安全登入	• 通过Web剪辑设置安全多用户登录	• iOS	
VPN	• 可設定 VPN 伺服器的存取權	• Android • Windows • iOS • macOS • visionOS • tvOS	
隨選即用 VPN	• 可依據網域、主機名稱等項目來設定 VPN 伺服器的存取權	• iOS	
Wi-Fi	• 可設定無線網路的存取權	• Android • Windows • iOS • macOS • watchOS • visionOS • tvOS	

行動電話通訊網路

類型	用途	適用裝置	所需授權
APN	• 可為裝置設定行動電話的存取點名稱	• iOS	
行動電話	• 可設定行動電話網路存取	• iOS • watchOS	
行動數據私人網路組態	• 設定承載以提供有關私人網路部署上的裝置資訊	• iOS	
iOS 電信商預設配置	• 可設定漫遊限制的預設值 • 可設定個人熱點限制的預設值	• iOS	

更多配置

類型	用途	適用裝置	所需授權
Apple TV	• 定義 Apple TV 的語言和地區設定	• 受監管的 iOS 7	Silver
預設裝置名稱	• 可使用變數定義預設裝置名稱	• 受監管的 iOS 8	Silver
iOS 桌布	• 安裝首頁並鎖定畫面背景	• 受監管的 iOS 7	Silver
macOS 桌布	• 在裝置上安裝首頁畫面和鎖定畫面桌布。 使用者可以變更桌布，但桌布一發佈裝置就無法加以移除。		不需要
移轉助手設定	協助管理員和使用者在裝置設定或移轉期間傳輸資料、應用程式和設定。	• macOS 26.4+	
單一 App 模式	• 限制裝置使用特定的 app	• 受監管的 iOS 7 • 受監管的 tvOS	Silver
相關聯網域組態	• 相關聯網域組態是將應用程式對應到其相關聯網域的字典。 • 相關聯網域可與可延伸 AppSSO、通用連結及密碼自動填寫等功能搭配使用。	• macOS 10.15+	Gold
螢幕共用主機設定組態	• 使管理員能夠跨受管理裝置安全地控制 macOS 熒幕共用功能。	• macOS 14+	

裝置同步配置

裝置同步設定提供您可在裝置上監控的資料點清單。 裝置同步配置無法編輯。 您可以查看已檢查完畢的設定清單。

程序

1. 前往**配置**。
2. 按一下**裝置同步組態**，會顯示**裝置同步組態**頁的「詳細資訊」索引標籤，並提供已勾選項目清單。

設定	讀取時間間隔 (分鐘)
憑證清單	
裝置資訊	60
已安裝的 App 清單	60
受管理的 App 清單	60
描述檔清單	60
設置描述檔清單	60
限制	60
安全性資訊	60
iOS 9+	
檢查更新	1440

相關主題

- 變數
- 使用配置

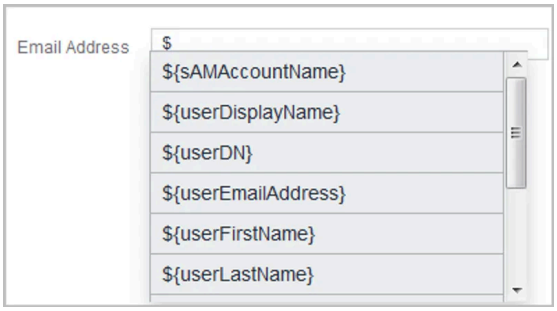
10.10.2. 變數

您可以使用特定配置欄位中的變數，來代表給定使用者專屬的值。 若在支援變數的任何欄位中鍵入 $，則相應欄位會顯示受支援變數的清單。本節包含以下各主題：

- 支援的使用者帳戶變數
- 支援的裝置變數

支援的使用者帳戶變數

使用者變數

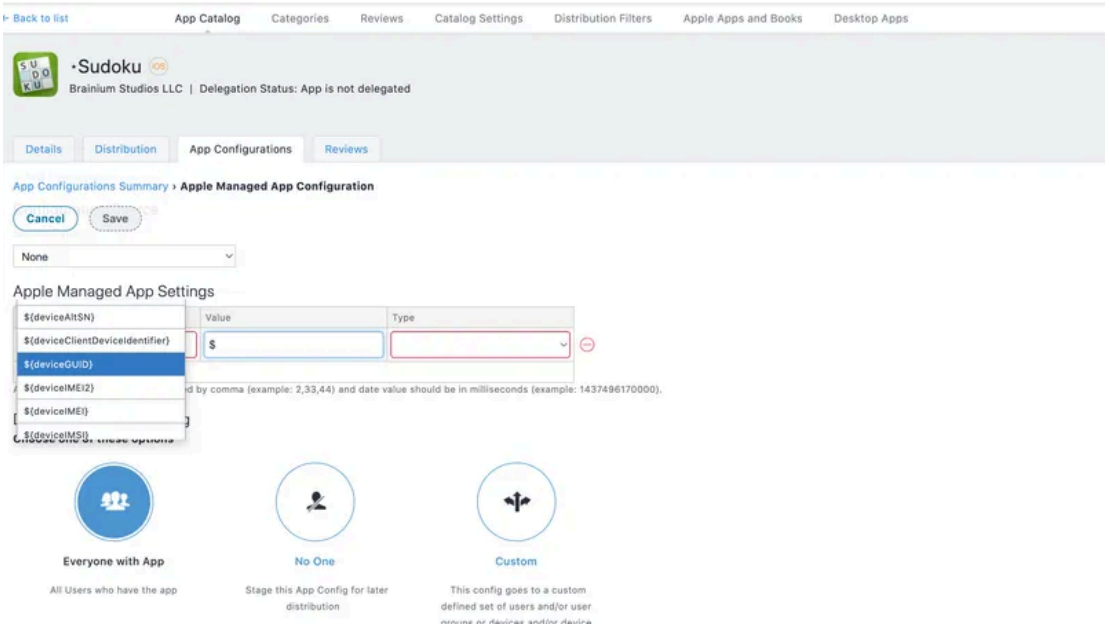


變數金鑰	值說明
$	部門屬性 (需要 Entra ID)
$	電子資料交換 - 個人識別碼
$	使用者的受管理 Apple ID
$	sAMAccountName 屬性 (需要 Active Directory)
$	從辨別名稱中擷取的一般名稱 (CN) 屬性 (需要 LDAP)
$	顯示名稱
$	辨別名稱 (需要 LDAP)
$	電子郵件地址的網域部分 (「@」之後的部分)
$>	電子郵件地址的本機部分 (「@」之前的部分)
$	電子郵件地址
$	名字
$	姓氏
$	地區設定
$	從辨別名稱中擷取的組織單位 (OU) 屬性 (需要 LDAP)
$	Kerberos 領域資訊 (需要 Active Directory)
$	登入 ID 的網域部分 (「@」之後的部分)
$	登入 ID 的本機部分 (「@」之前的部分)
$	登入 ID (電子郵件地址格式)
$	userPrincipalName 屬性 (需要 Active Directory)

支援的裝置變數

利用裝置變數指定行動裝置相關資訊。

裝置變數


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

變數金鑰	值說明
$	用戶端上次簽入日期 (最近簽入 - MDM 或用戶端)
$	替代序號
$	用戶端應用程式使用的識別碼
$	全域唯一裝置識別碼
$	ICCID
$	IMEI2
$	IMEI
$	IMSI
$	裝置上次簽入日期 (最近簽入 - MDM 或用戶端)
$	內部裝置識別碼
$	用於 MDM 的識別碼
$	MEID
$	模型
$	裝置名稱
$	裝置電話號碼
$	叢集唯一裝置識別碼
$	序號
$	iOS UDID
$	Wi-Fi MAC 位址

佈建範本變數

變數金鑰	值說明
$	電子郵件正文
$	電子郵件主旨

時間戳記變數

變數金鑰	值說明
$	目前時間戳記 (自該時期起以毫秒計)

原則範本變數

變數金鑰	值說明
$	原則名稱已違規
$	傳送訊息後要採取的「下一個階層式合規行動」 (不同於等待和淘汰)
$	裝置處於不符合規範狀態的天數
$	首次觸發違反原則的時間戳記 (UTC DD-MM-YYYY 格式)
$	規則定義 (查詢字串現在顯示的方式)

相關主題：

- 屬性

10.10.3. AppConnect 組態

本節包含以下各主題：

- AppConnect 概覽
- AppConnect 密碼

10.10.3.1. AppConnect 概覽

AppConnect 是一項功能，內含多種 app 可用來保護 iOS 和 Android 裝置上的資料。 每個 AppConnect app 變成安全容器，其中的資料經過加密並受到保護，可防範未經授權存取與移除。 每個使用者都有多個商業 app，因此每個 app 容器也會連線至其他的安全 app 容器。 此連線可讓 AppConnect app 共享資料，例如文件。 Ivanti Neurons for MDM 使用原則來管理已啟用 AppConnect 的應用程式。

有關 AppConnect 以及如何配置和部署 AppConnect 應用程式的更多資訊，請參閱*適用於 Ivanti Neurons for MDM 的 AppConnect 指南*。

安全應用程式的狀態

從**裝置 > 裝置**頁面按一下要檢視**概覽**頁面的裝置。 在此頁面中，使用者可檢查安全應用程式的狀態與下列資訊：

- **安全 app 狀態** - 指出 AppConnect 目前啟用或停用。
- **安全 app 加密狀態** - 指出 AppConnect 密碼目前啟用或停用。
- **安全 app 加密模式** - 指出加密模式 (例如 AES 256)。

此外，這些欄位可用來：

- 做為篩選 (左窗格) 以縮小使用者嘗試搜尋/篩選裝置時的裝置項目顯示範圍。
- 做為規則，同時建立動態管理的裝置群組。
- 做為發佈篩選，以進一步調整要依據定義之規則發佈 app 至其中的裝置。

管理員可以針對每個安全應用程式，在裝置詳細資訊頁面的**組態**索引標籤中，檢閱容器原則和組態狀態 (已安裝、已套用、已傳送或安裝擱置中)。

10.10.3.2. AppConnect 密碼

本節包含以下各主題：

- 變更/重設密碼
- 產生一次性 PIN 碼，以重設 iOS 裝置的安全應用程式密碼

您可要求 AppConnect 密碼 (也稱為安全 app 密碼)。 裝置使用者可利用 AppConnect 單一登入密碼來存取所有的安全 app。 在管理入口網站中，您可設定 AppConnect 密碼的規則。 AppConnect 密碼與用來解除鎖定裝置的密碼不同。

變更/重設密碼

使用者可在 Secure Apps Manager app (Android 裝置) 和 Go app (iOS) 中變更或重設安全應用程式密碼，前提是已在 AppConnect 配置中允許它。 若是 iOS 裝置：

程序

1. 開啟 Go app (iOS)。
2. 按一下**安全 App**。
3. 按一下**身份認證**。
4. 按一下**變更安全 App 密碼**，然後遵循密碼變更/重設指示。

若是 Android 裝置：

1. 開啟 Secure Apps Manager app。
2. 按一下選項功能表中的**變更密碼**。
3. 按一下**忘記密碼**以重設密碼。

產生一次性 PIN 碼，以重設 iOS 裝置的安全應用程式密碼

管理員可設定 Ivanti Neurons for MDM，以允許 iOS 裝置使用者在忘記其安全應用程式 (AppConnect) 密碼時重設密碼。 在您設定此選項後，已使用使用者名稱和密碼向 Ivanti Neurons for MDM 註冊的裝置使用者可在 Go 3.1.0 for iOS 或支援的較新版本中輸入這些憑證進行身分驗證，然後重設他們的安全應用程式密碼。 不過，忘記密碼和 PIN 碼的裝置使用者需要不同的身分認證機制。

程序

1. 在 Ivanti Neurons for MDM 中，管理員可開啟「預設 iOS AppConnect 組態」(或任何其他的 iOS AppConnect 組態) 中的**安全應用程式密碼**選項。
2. 使用者可在自助式入口網站中，按一下**重設安全 App 密碼**選項並遵循指示，藉此產生特定 iOS 裝置的一次性 PIN 碼。 一次性 PIN 碼的有效期為 30 分鐘。
3. 使用者可在裝置的 Go for iOS 中，遵循忘記安全應用程式密碼的重設指示。
4. 當系統提示提供使用者憑證時，使用者可輸入其使用者名稱與 PIN 碼以取代一般密碼。
5. 使用者重設其 Secure App 密碼。

10.10.4. 安全性配置

本節包含以下各主題：

- Android Enterprise
- 編輯 Android Enterprise 預設組態
- 設定 Android Enterprise
- Android 工作挑戰
- 憑證配置
- 憑證透明度
- 憑證撤銷檢查配置
- 建立自發的單一應用程式模式組態
- 建立 DNS Proxy 組態
- 裝置記錄組態
- 磁碟管理組態
- Android 加密
- 加密 DNS
- 外部智慧設定
- 威脅防護
- FileVault 2
- FileVault 復原金鑰
- FileVault 選項配置
- 身份憑證
- Apple 啟用鎖定配置
- iOS 自訂配置
- 智慧設定
- 鍵盤設定
- iOS 限制
- 會議室顯示器
- 鎖定與單一應用：Android 裝置管理模式
- 設定 Android 的單一應用模式
- 設定 Android 共用裝置單一應用
- 鎖定與單一應用：Android Enterprise
- 鎖定與單一應用：Samsung Knox Standard
- macOS 防火牆
- macOS 限制
- macOS AppStore 限制
- macOS 燒錄光碟限制

- 允許的媒體控制 (已棄用)
- macOS Finder 設定
- macOS 核心擴充原則
- 適用於 macOS 的 Mobile@Work
- macOS 軟體更新規則配置
- 憑證偏好設定
- Active Directory (macOS)
- 身分偏好設定
- Office 365 自動帳戶建立 (macOS)
- 驗證
- Apple 應用程式目錄
- 受管理的網域
- 密碼組態
- 隱私權偏好設定 (macOS)
- Ivanti Go Client 設定
- 隱私權配置
- 用戶端隱私權聲明資訊
- Safari 擴充功能設定組態
- 軟體更新
- 軟體更新設定組態
- 安全性喜好設定配置
- Siri 設定
- 時間伺服器
- Web 內容篩選
- Windows 防火牆
- Windows 資訊保護
- Windows 限制
- Windows Desktop 的限制
- Windows 10 的桌面設定
- Windows Hello 企業版配置
- Windows AI 管理組態
- Play Integrity (前身為 SafetyNet Attestation)
- 進階 Android 密碼與鎖定畫面
- Microsoft Defender for Endpoint
- 憑證型驗證

10.10.4.1. Android Enterprise

授權：Silver

Android Enterprise 組態可定義所支援裝置啟用的 **Android Enterprise** 選項。 您可為不同裝置群組建立其他配置，或直接編輯預設配置。 如需支援 Android Enterprise 的裝置清單，請參閱 **Android** 官方頁面。

Android Enterprise 設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
啟用螢幕擷取 (Android 5.0 +)	選取此選項可防止裝置使用本機螢幕擷取功能。
停用應用程式控制 (Android 5.0 +)	選取此選項可防止使用者在「設定」或「啟動器」中修改應用程式。
不允許設定認證 (Android 5.0 +)	選擇以防止使用者設定使用者憑證。
不允許跨設定檔複製/貼上 (Android 5.0 +)	選取此選項可防止裝置複製和貼上到其他 Android Enterprise 工作設定檔。
不允許修改帳戶 (Android 5.0 +)	選取此選項可防止使用者新增和移除帳戶。
不允許外送 Beam (Android 5.0 +)	選取此選項可防止使用者使用 NFC 傳輸應用程式資料。
不允許共用位置 (Android 5.0 +)	選擇以防止網站和 app 提示裝置使用者共用裝置位置。
限制輸入法 (Android 5.0+)	選取此選項可透過指定允許的套件名稱清單來限制輸入法。 未列入允許清單的套件，則只允許系統輸入法。 輸入法不僅限於工作應用程式，還限於整個裝置。
限制協助工具服務 (Android 5.0 +)	選取此選項可透過指定允許的套件名稱清單來限制輸入法。 未列入允許清單的套件，則只允許系統輔助功能服務。 輸入法不僅限於工作應用程式，還限於整個裝置。
停用來電者 ID (Android 6.0 +)	設定傳入呼叫時，是否於裝置顯示工作設定檔中的呼叫者 ID 資訊。

相關主題

- **設定 Android Enterprise**

10.10.4.2. Apple 金輪證明

使用金鑰證明組態將裝置配置為允許對某些金鑰進行 WebAuthn 企業證明。

當使用者使用金鑰對其裝置進行身分驗證和註冊時，Apple 金輪認證組態使用企業管理憑據，透過企業憑證證明金鑰。 支援的憑證包括 SCEP、ACME 和身分憑證。

金輪證明支援以下項:

- 支援的最低作業系統版本: macOS 14
- 支援的註冊方式: 裝置註冊
- 需要受管理 Apple 帳戶來控制金鑰的同步。
- 可以與 ABM 的存取管理結合使用。

> Mac 上的金鑰有效負載失敗。

建立金鑰組態時，您必須首先建立身分證書組態，並將其連結到金鑰組態。 此外，請在「安全金鑰證明組態」區段提供以下詳細資訊:

欄位	描述
名稱	金輪的名稱。
描述	有關組態的任何資訊。
證明身分資產參考 • 證明身分金鑰是可擷取的	提供您建立的資產參考身分識別，以連結到金鑰組態。 選取此選項以確認身分識別金鑰是否可選取。
依賴者	輸入經過身分驗證的網域的詳細資訊。

10.10.4.3. 應用程式隱私權預設值

使用**應用程式隱私權預設值**定義受監管裝置上應用程式的預設隱私權限。 管理員可以識別應用程式使用的隱私元件、在組態中列出應用程式及其元件，並設定隱私預設值。 使用者啟動應用程式時，應用程式會檢查設定的隱私預設值，並提示使用者授予權限，同時允許使用者延遲或稍後在裝置設定中管理權限。

適用於：

- 受監管的 iOS 27.0+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監管的 iPad 27.0+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監管的 macOS 27.0+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取**應用程式隱私權預設值**組態。
3. 在**名稱**欄位中，輸入可識別組態的文字。
4. 在**描述**欄位中，輸入描述以闡明此組態的目的。
5. 在**組態設定**窗格中，選取**藉由查閱來新增**。
6. 透過選取下列其中一個選項，輸入您要設定**應用程式隱私權預設值**的應用程式名稱:

- iOS Store
- 「App Catalog「
- visionOS 商店
- OS X Store (macOS)

> 您可以選取多個應用程式。

7. (選用) 選取手動**新增**以選取應用程式。
8. (選用) 輸入應用程式**套件名稱**。
9. (選用) 按一下**新增應用程式**。
10. 選取**檢視應用程式**。

檢視應用程式窗格會列出所有選取的應用程式。

11. 按一下每個應用程式上的**新增預設值**，以個別設定應用程式隱私權預設值。

新增預設值窗格隨即顯示。

12. 依照下表選取**預設值**和**限制**:

預設值	限制
相機	請選擇下列選項之一： • 允許 • 無
藍牙	請選擇下列選項之一： • 允許 • 無
協助工具	請選擇下列選項之一： • 允許 • 無
聽寫	請選擇下列選項之一： • 允許 • 無
麥克風	請選擇下列選項之一： • 允許 • 無
定位	請選擇下列選項之一： • 使用時 • 無 • 一律
位置準確性	請選擇下列選項之一： • 大約 • 精確 • 無
本機網路	請選擇下列選項之一： • 允許 • 無
組織理由	**組織說明**提示可能會顯示組織名稱、應用程式名稱、管理員提供的理由，以及具有建議隱私預設值的每個元件的詳細資訊。 如果使用者選取**允許**，系統會套用到建議的隱私預設值。 如果使用者選取**現在不要**，則在應用程式存取使用者裝置中指定的元件時，同意提示會出現。

13. 按一下**儲存**。
14. 按**下一步**，確認發佈設定。
15. 選取其中一個發佈選項以設定**應用程式隱私權預設值**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
16. 按一下**完成**。

10.10.4.4. 編輯 Android Enterprise 預設組態

全域管理員可允許空間管理員在自訂空間中，編輯任何下列 Android Enterprise 預設組態的發佈。

- Android Enterprise: 公司所擁有裝置上的工作設定檔 (Android for Work)
- Android Enterprise: 工作受管理裝置 (Android for Work)
- Android Enterprise: 具有工作設定檔的受管理裝置
- Android Enterprise: AOSP

如要編輯上述任一配置的發佈

程序

1. 在「配置」標籤中，選擇要編輯的配置。
2. 按一下「編輯」圖示。
3. 按**下一步**。
4. 在發佈頁面中選取下列任意發佈層級以進行編輯和設定:
    - **所有裝置**:選取下列其中一個選項，將組態發佈至所有相容裝置:
        1. 不套用至其他空間
        2. 套用至其他空間中的裝置。
    - **沒有裝置** (預設)
    - **自訂**: 選取下列其中一個選項，對所有相容裝置或使用者發佈組態:
        1. **使用者/使用者群組**: 選取使用者或使用者群組旁的核取方塊。 或者，您也可以鍵入並搜尋使用者或使用者群組。
        2. **裝置/裝置群組**: 選取裝置或裝置群組旁的核取方塊。 或者，您也可以鍵入並搜尋裝置或裝置群組。
           在**發佈摘要**中，選取以下其中一個選項以啟用或停用多個空間的組態:
            - 請勿套用至其他空間。
            - 套用至其他空間中的裝置。

            > 如果選取**套用至其他空間的裝置**選項，則會出現**允許空間管理員編輯發佈**核取方塊，且其允許委派的空間管理員編輯特定空間的發佈。

> 如果您編輯發佈選項，則必須選取核取方塊「**我了解，如果從現有裝置中移除組態，則變更 Android Enterprise 裝置模式組態的發佈可能會導致裝置淘汰或抹除**」。

5. 按一下**完成**。

當此配置套用至空間時，空間管理員將可透過按一下自訂空間中的發佈圖示來編輯發佈。

10.10.4.5. 設定 Android Enterprise

本節包含以下各主題：

- 支援裝置
- 連接 Ivanti Neurons for MDM 與 Android Enterprise
- 取得 Android Enterprise 認證
- 將 Android Enterprise MDM 權杖新增至 Ivanti Neurons for MDM
- 在 Ivanti Neurons for MDM 與 Google 之間同步使用者
- Active Directory/LDAP 使用者
- 本機使用者
- 將 Android Enterprise 部署到支援的裝置
- 淘汰已註冊的裝置
- 部署裝置
- 確認部署
- 部署 Android Enterprise App
- 設定商業 App

授權：Silver

Android Enterprise 是 Google 提供的一個程式，使行動管理員能:

- 將工作及個人資料區隔開來
- 保護企業 app 的安全並加以管理
- 控制系統 app (例如相機及相片集)
- 在 Android Enterprise 容器中集中佈建和設定應用程式
- 防止資料遺失 (螢幕擷取)

可將 Ivanti Neurons for MDM 設定為管理 Android Enterprise 的 UEM 伺服器。 Android Enterprise 的最低需求為 Android 3.0。 Android Enterprise 有兩個支援的組態，裝置擁有者和受管理設定檔 – 員工擁有。

支援裝置

Ivanti Neurons for MDM 目前僅在執行 Android 5.0 並由製造商啟用 Android Enterprise 的裝置上支援 Android Enterprise。 Android Enterprise 是執行 Android 5.0 的裝置上使用 kiosk 模式所必需的。

必要條件

如果您尚未向 Google 註冊網域，則必須先前往 Google 網站進行註冊：

https://admin.google.com.

程序期間，您將進行下列作業：

- 宣告網域 (必須與使用者電子郵件地址的網域相符)
- 接收權杖
- 下載 JSON 用戶端 ID

在 Ivanti Neurons for MDM 上設定 Android Enterprise 時，兩個項目均為必需。

程序完成後，您即會收到一封電子郵件，說明如何驗證您之前所要求的網域為您所有。

若公司已經使用公司的網域名稱註冊 Google Apps for Work，請參閱 https://support.google.com/work/android/answer/6174062，了解啟用 Android Enterprise 的相關資訊。

連接 Ivanti Neurons for MDM 與 Android Enterprise

註冊 Android Enterprise 後，請將 Ivanti Neurons for MDM 設定為 UEM 伺服器。

取得 Android Enterprise 認證

程序

1. 前往**管理員 > Android Enterprise**。
2. 按一下 **Google 開發人員控制台**。
3. 按一下第一個顯示的連結，前往 Google 開發人員控制台。
4. 從下拉式功能表中選擇**建立專案**。
5. 輸入專案的名稱。
6. 接受服務條款。
7. 按一下**建立**。
8. 按一下 **API**。
9. 選擇 **API**。
10. 在搜尋欄位中，輸入 **emm** 以尋找 Google Play EMM
11. 按一下 **Google Play EMM API** 連結。
12. 按一下**啟用 API**。
13. 按一下**認證**。
14. 選擇**服務帳戶**。
15. 按一下**建立**以儲存 JSON 檔。

將 Android Enterprise MDM 權杖新增至 Ivanti Neurons for MDM

程序

1. 登入 https://admin.google.com。
2. 按一下**安全性**。
3. 若沒看見 Android Enterprise 設定，請按一下**顯示更多**。
4. 選擇**Android Enterprise 設定**。
5. 在**管理企業行動力管理提供者**下，複製 MDM 權杖。
6. 返回 Ivanti Neurons for MDM 入口網站。
7. 按一下**完成**。
8. 在方塊 2 中，貼入您剛複製的 MDM 權杖。
9. 在**網域**欄位中，輸入已向 Google 宣告的網域。

10. 按一下**選擇檔案**，上傳所下載的 JSON 檔案。
11. 按一下**連線**。
    連線成功後，會顯示**已連接至 Google** 的訊息。
12. 在方塊 3 中按一下**授權**，即表示您想讓 Ivanti Neurons for MDM 存取 Google 使用者資料。
13. 按一下**接受**。
    在 Ivanti Neurons for MDM 入口網站中顯示**已連線至使用者**訊息。

在 Ivanti Neurons for MDM 與 Google 之間同步使用者

將 Android Enterprise 部署到 Ivanti Neurons for MDMIvanti Neurons for MDM 所管理的 Android 使用者之前，每個使用者都必須在 Google 管理入口網站上擁有對應的記錄。 在Ivanti Neurons for MDM 和 Google 管理入口網站之間同步使用者資訊的必要步驟，取決於您是否已設定與組織目錄服務 (AD/LDAP) 的整合。

Active Directory/LDAP 使用者

如果您已設定 AD/LDAP 與 Ivanti Neurons for MDM 的整合，就必須使用 Google Apps Directory Sync 來設定 AD/LDAP 與 Google 管理入口網站的整合。 如需詳細資訊，請參閱 https://support.google.com/a/answer/106368?hl=en。

本機使用者

如果您只在 Ivanti Neurons for MDM 中建立本機使用者，而不想將其與目錄服務整合，則可完成下列步驟，以與 Google 管理入口網站同步這些使用者:

程序

1. 登入 Google 管理入口網站，網址為 https://admin.google.com。
2. 按一下**使用者**。
3. 按一下右下角的**新增使用者**或**新增多名使用者**圖示。
4. 對於將使用 Android Enterprise 的每個 Ivanti Neurons for MDM 使用者，請新增一個使用者名稱和電子郵件地址與 Ivanti Neurons for MDM 使用者相同的 Google 使用者。
5. 在 Ivanti Neurons for MDM 入口網站中，針對每個已新增至 Google 管理入口網站的 Ivanti Neurons for MDM 使用者:
   a. 按一下「使用者」索引標籤中的使用者名稱連結，顯示使用者的詳細資料。
   b. 選擇**將使用者與 Google 使用者目錄同步**。
   c. 按一下**與 Google 使用者目錄同步**。
   d. 確認 Google 狀態列為「已啟用」。

將 Android Enterprise 部署到支援的裝置

部署 Android Enterprise 需要兩個組態:

- Android Enterprise: 公司所擁有裝置組態上的工作設定檔支援 Android Enterprise。
- 鎖定與 kiosk 組態定義要套用的 Android Enterprise 限制。

淘汰已註冊的裝置

在 BYOD 情節中，在公司所擁有的裝置上從「裝置管理員」移到「 Android Enterprise 工作設定檔」不需要淘汰與重新註冊裝置。 只有從裝置管理移至裝置擁有者模式時才需要裝置清除或淘汰。

選擇已在「裝置擁有者」/「增強型設定檔擁有者」/「公司擁有個人啟用」模式下註冊的裝置執行「淘汰」動作時，螢幕上會出現一個快顯視窗，顯示「組織擁有的裝置不支援淘汰命令」。

部署裝置

程序

1. 在 Ivanti Neurons for MDM 入口網站中，前往**組態**。
2. 按一下 **Android Enterprise: 工作設定檔**。
3. 按一下**編輯**。
4. 按一下**下一步**。
5. 選擇**所有裝置**或**自訂**。
6. 若選擇了**自訂**，請搜尋並選擇應接收 Android for Work 設定的裝置群組。
7. 按一下**完成**。
8. 按一下**返回清單** (左上角)。
9. 按一下**+新增**。
10. 按一下**鎖定與 kiosk: Android Enterprise**。
11. 在**名稱**欄位中，輸入可識別組態的文字。
12. 在**選擇鎖定類型**下，選擇**工作設定檔**。
13. 選擇您要套用至目標裝置的鎖定設定。
14. 按一下**下一步**。
15. 選擇**所有裝置**或**自訂**。
16. 如果您選擇「自訂」，請搜尋並選擇應接收 Android Enterprise 設定的裝置群組。
17. 按一下**完成**。

> 部署之後，您就無法再針對產生的描述檔進行變更。 您必須改為建立新的 Android Enterprise 組態並進行部署。

確認部署

您可透過下列方式確認是否已部署 Android Enterprise:

- 在**使用者 > 使用者**下方，找到使用者的項目，然後確認 **Google 狀態**為**已啟用**。
- 在**裝置 > 裝置**下，按一下裝置的連結，然後確認 **Android Enterprise** 的狀態是否為**已啟用**。

使用者的 **Google 狀態**應列為**已啟用**。 如果不是「啟用」，使用者就無法註冊裝置。

> 針對未擁有 GSuite 訂閱者身分的企業，受管理的 Google Play 帳戶方法允許使用者註冊 Android Enterprise。 如果之前已將 Android Enterprise 設定為受管理的 Google Play 帳戶，則只有在註冊 Android Enterprise 裝置之後，使用者才會顯示為 **Google 狀態: 已啟用**。請參閱**受管理的 Google Play 帳戶**，以進一步瞭解受管理的 Google Play 帳戶。

部署 Android Enterprise App

為 Android Enterprise 開發的任何應用程式都可能包含可透過 Ivanti Neurons for MDM 設定的選項。

程序

1. 在 Ivanti Neurons for MDM 入口網站中，前往**應用程式 > 應用程式目錄**。
2. 在 Google Play 商店中尋找 app。
3. 按一下 app 項目。
4. 代表 Android Enterprise 使用者接受權限。
5. 按**下一步**。
6. 選擇發佈選項。
7. 展開**進階選項與 App 配置**。
8. 請使用下列方針來完成選項：
9. 按**下一步**。

設定	描述
安裝到裝置上	選擇此選項，以在註冊後立即啟動安裝。 系統將會提示使用者確認安裝 app，但當裝置為 Samsung Knox 裝置，且已選擇下方的無訊息自動安裝選項時除外。
在一般使用者的 App Catalog 中不顯示 app	如果您不想讓使用者看到裝置 App Catalog 中的 app，可選擇此選項。
無訊息自動安裝到 Samsung Knox 裝置上	如果您不想讓系統提示使用者確認 Samsung Knox 裝置上進行的安裝，可選擇此選項。
設定 App 安裝優先性	針對 Android Enterprise 應用程式，您可將特定應用程式的下載順序設為優先於其他應用程式。 例如，您可以將下載 Tunnel 和電子郵件 app 設為優先於其他不重要的 app。 以下是可用的優先等級選項： • **高** • 中 (預設選擇選項) • **低** 此設定適用於內部、公用、私人與 Web 應用程式。 內部開發 app 是透過用戶端安裝，而公用和私人 app 則是透過 Google 安裝。 app 優先性僅會套用至透過相同通道安裝的 app。
僅在連線至 Wi-Fi 時安裝	選擇此選項，以便只在裝置連線至 Wi-Fi 時安裝 app。
僅在充電時安裝	選擇此選項，以便只在裝置正在充電時安裝 app。
僅在閒置時安裝	選擇此選項，以便只在裝置閒置 (使用者並未正在使用) 時安裝 app。
安裝時自動啟動	選擇此選項，在安裝後自動啟動 app。 此功能僅適用於剛安裝在裝置上的 app，而非版本更新的 app。

10. 選擇推廣選項。
11. 按一下**完成**。

設定商業 App

您可在應用程式目錄的「商務應用程式」區段中找到 Android Enterprise 應用程式，其中包括下列應用程式:

- Divide Productivity

- Email+
- Tunnel
- Gmail

10.10.4.6. Android Enterprise: 工作受控裝置非 GMS 模式 (AOSP)

Ivanti Neurons for MDM 支援「工作受控裝置非 GMS 模式」(AOSP) 裝置的裝置擁有者註冊，無需使用 Google 行動服務 (GMS)。 它是一種系統配置，管理員無法新增該配置。 管理員可發佈或取消發佈它。

程序

1. 使用使用者認證登入 Ivanti Neurons for MDM。
2. Android Enterprise 的搜尋組態: 工作受控裝置非 GMS 模式 (AOSP)。
3. 編輯配置並將它發佈至適合的裝置群組。 例如：Android 裝置。
4. 按一下**完成**。

10.10.4.7. Android 工作挑戰

本節包含以下各主題：

- 建立 Android 工作挑戰配置：
- 配置設定

授權：Silver

「Android 工作挑戰 (Work Challenge)」配置可定義安全的密碼，以供使用者存取 Work Profile 資料和 app。 需要 Android Enterprise 工作設定檔。

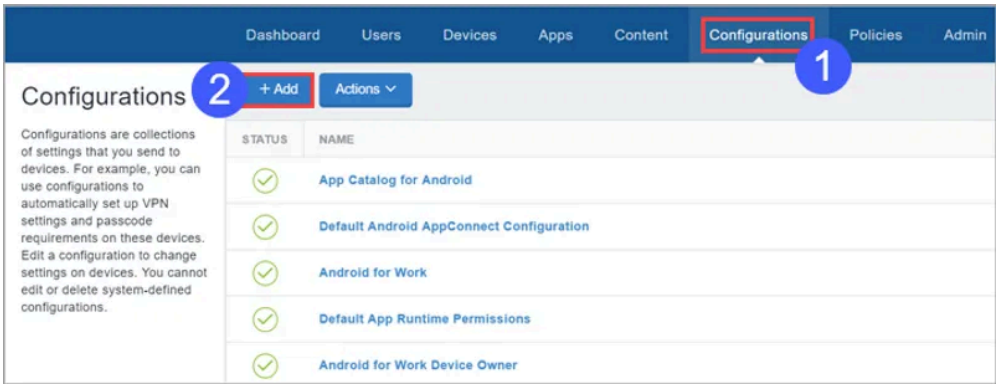
實作注意事項：

- 管理員可以個別套用裝置密碼原則，以及工作描述檔密碼原則。
- Ivanti Neurons for MDM 不會將此組態傳送給早於 Android 7.0 的用戶端，因為該類裝置不支援這項功能。
  Ivanti Neurons for MDM 只會將此組態傳送給含有 Android Enterprise 工作設定檔的裝置。

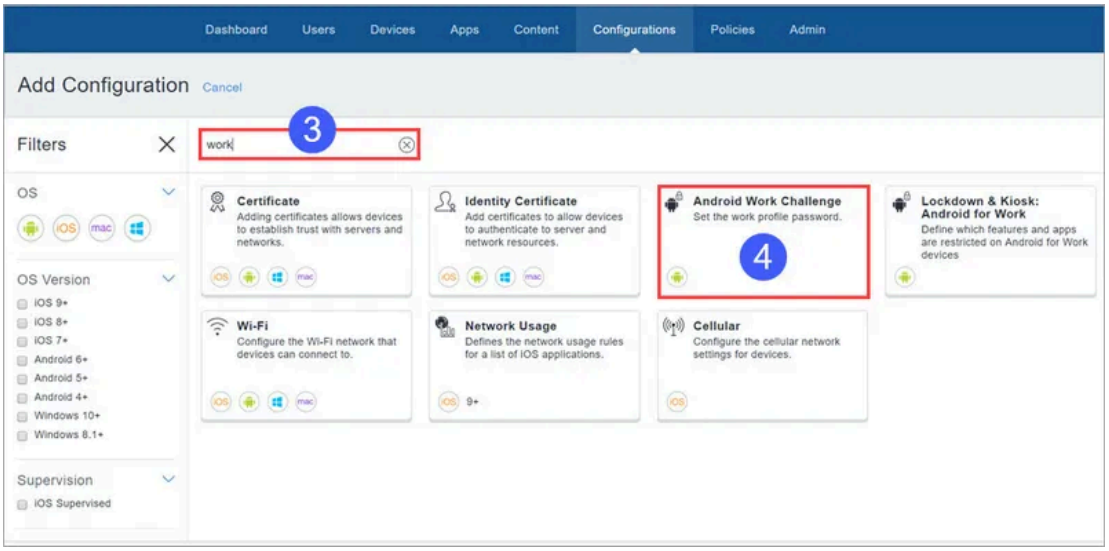
建立 Android 工作挑戰配置：

程序

1. 按一下**配置**。

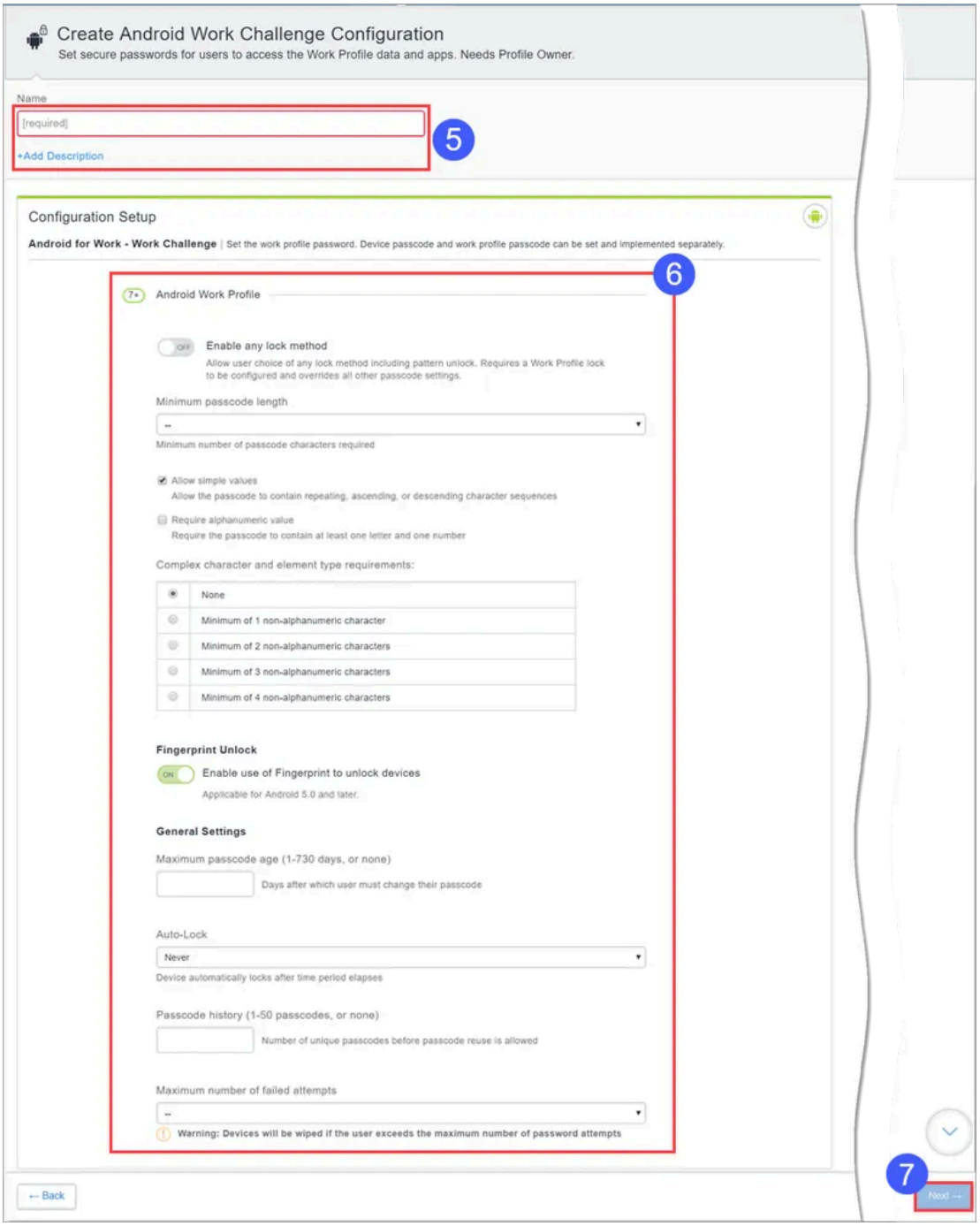


按一下 **+新增**。



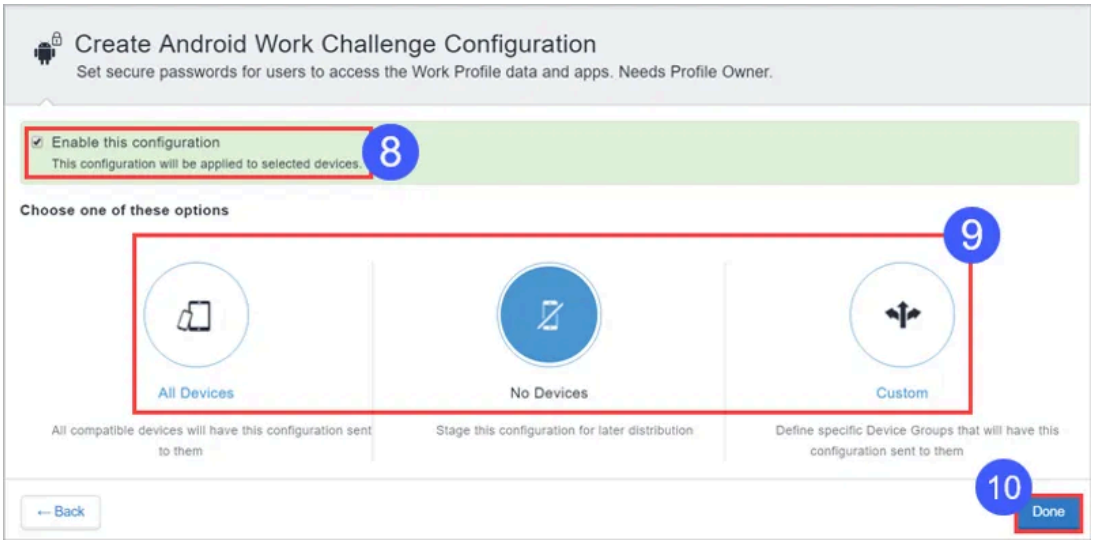
在搜尋欄位中，輸入「工作」(work)。

4. 選擇 **Android 工作挑戰 (Work Challenge)** 配置。



輸入配置名稱，並選擇性輸入描述。

6. 使用「配置設定」欄位，以建立配置。 請參閱**配置設定**以取得設定的詳細資料。
7. 按**下一步 →**。



視需要啟用配置。

9. 將發佈設定對象設為所有裝置、沒有任何裝置或自訂的一組裝置。
10. 按一下**完成**。

配置設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
啟用任意鎖定方法	允許使用者選擇任意鎖定方法，包括模式解鎖。 會覆寫所有其他密碼設定。
最小密碼長度	選擇最小密碼長度 (4 到 16 個字元之間)。
允許簡易值	啟用以允許密碼包含重複、遞增或遞減的字元順序。
必須為英數值	啟用以要求密碼必須至少包含一個字母與一個數字。
複雜字元和項目類型特性	設定複雜字元和項目類型特性需求，範圍如下： • 無 • 至少 1 個非英數字元 • 至少 2 個非英數字元 • 至少 3 個非英數字元 • 至少 4 個非英數字元
指紋解除鎖定	啟用以允許使用者利用指紋來解鎖裝置。
最大的密碼有效期	設定密碼有效期上限，範圍從「無」到「730 天」。
自動鎖定	選擇裝置要在多久時間間隔之後自動鎖定。 時間範圍從「永不」到「十五分鐘」。
密碼歷程記錄	指定需使用幾組唯一密碼之後，才能重複使用密碼，範圍從「無」到「50 組密碼」。
嘗試失敗次數上限	選擇失敗嘗試次數的上限。 **警告: 如果使用者的密碼嘗試次數超過上限，則 Ivanti Neurons for MDM 會抹除相應的裝置！**

10.10.4.8. 憑證配置

認證配置可識別要發佈給使用者的認證。 憑證可讓裝置建立與伺服器和網路資源間的信任關係。 從 76 版起，我們僅支援 v3 憑證。

身為管理員，您現在可以為智慧卡登入和自訂物件 ID (OID) 產生 Ivanti Neurons for MDM 憑證。 您可以從以下驗證選項產生憑證：

- 用戶端驗證 - 預設為啟用
- IPSEC - 選用，管理員可啟用
- 智慧卡登入 - 選用，管理員可啟用
- 自訂 OID - 選填，管理員可啟用

此功能僅適用於以下認證授權中心 (CA)：

- 本機憑證授權中心
- 中繼憑證授權中心
- 外部憑證授權中心 - 在 NDES 伺服器中設定 CA 範本的套用規則，以支援 IPSEC、智慧卡登入和自訂 OID
- 內部部署 SCEP 憑證授權中心

發佈配置

從 Ivanti Neurons for MDM 版本 91 開始，全域管理員可委派空間管理員編輯「所有裝置」和「自訂」發佈選項的「憑證組態」。 對於憑證組態，您可以依需要選取「允許在所有空間中提供此組態」選項。 此選項使憑證組態可用於所有空間，並可用於 Exchange、Wi-Fi、VPN、個別應用程式 VPN 和任何其他適用的組態。 此選項可用於以下情況: 憑證組態只需作為關聯組態的一部分發佈到裝置 (在非預設空間中)，而不是作為個體組態發佈。

程序

1. 在名稱欄位中輸入名稱。
2. 上傳憑證檔案。
3. 按**下一步**。
4. 選擇**啟用此配置**選項。
5. 請選擇下列發佈選項之一：
    - **所有裝置**。 請選擇下列選項之一：
        - **請勿套用至其他空間**。
        - **套用至其他空間中的裝置**。
            - 選擇**允許空間管理員編輯發佈**勾選方塊以允許委派的空間管理員編輯發佈特定空間。
    - **沒有裝置** (預設)
    - **自訂**選擇下列其中一個選項:
        - **請勿套用至其他空間**。
        - **套用至其他空間中的裝置**。
            - 選擇**允許空間管理員編輯發佈**勾選方塊以允許委派的空間管理員編輯發佈特定空間。

無論空間多少，憑證組態均可設定到所有空間、發佈到所有裝置，並套用於其他裝置空間中的所有裝置。

6. 按一下**完成**。

認證設定

身為系統管理員，您可設定內部部署非 SCEP 憑證授權中心。

程序

1. 登入 Ivanti Neurons for MDM 管理員入口網站。
2. 前往**管理** > **基礎架構** > **憑證管理** > **憑證授權中心**。
3. 按一下 **+新增**。 已列出以下選項：

- **建立 Ivanti Neurons for MDM 提供的本機憑證授權單位**
- **使用您現有的 CA 來簽署 Ivanti Neurons for MDM 的本機 CA**。
- **連線至公開信任的 Cloud 憑證授權中心**。
- **連線內部部署的 SCEP 憑證授權中心**。
- **連線內部部署非 SCEP 憑證授權單位**。

4. 完成以下欄位（如相關）：
5. 按一下**完成**。

設定	方法
名稱	輸入可識別此配置的名稱。
網址 (URL)	系統管理員必須從 OpenTrust 採購的 OpenTrust CA URL。
密碼	輸入驗證憑證的密碼
驗證憑證	接受 OpenTrust/IDnomic 提供的 .p12 檔案格式。
TLS CA 憑證鏈	接受 OpenTrust/IDnomic 提供的 PEM 檔案格式。

在您設定內部部署非 SCEP 憑證授權中心後，您必須建立身份憑證。 根據描述檔 ID 描述檔，填寫所有必填欄位以完成設定。

當 SCEP CA 憑證的產生因以下兩項原因而失敗，且已達到階段 2 逾時，便會產生通知:

1. Connector 無法連線
2. CA 伺服器無法連線

10.10.4.9. 憑證透明度

適用於: iOS 12.1.1、macOS 10.14.2、tvOS 12.1.1、watchOS 10.0+、visionOS 1.1+ 以及支援的較新版本。

控制憑證透明度施行只能出現在裝置描述檔中。 您可以納入多個憑證，並視需要停用網域。

建立「憑證透明度」配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入**憑證**，然後按一下**憑證透明度**配置。
4. 輸入配置的名稱和描述。
5. 指定**要停用的網域**。 按一下 **+ 新增網域**，以新增多個網域。 您可以使用前置句號來比對子網域，不過，網域比對規則不得比對頂層網域中的所有網域。 例如，您可以使用 ".example.com" 和 ".example.co.uk"，但不能使用 ".com" 和 ".co.uk"。 不支援萬用字元網域。
6. 請在選取演算法 (SHA 256) 之後，指定**憑證雜湊**。 按一下 **+新增**，以新增多個憑證雜湊。
7. 按**下一步**，確認發佈設定。
8. 按一下**完成**。

若要在 subjectPublicKeyInfo 目錄中產生雜湊金鑰指定的資料，請針對 PEM 編碼的憑證使用下列命令：

```
openssl x509 -pubkey -in example_certificate.pem -inform pem | openssl pkey -pubin -outform der | openssl dgst -sha256 -binary | base64
```

如果您的憑證是 DER 編碼，請使用下列命令：

```
openssl x509 -pubkey -in example_certificate.der -inform der | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

如需更多資訊，請參閱如何建立配置。

10.10.4.10. 憑證撤銷檢查配置

此配置可讓管理員檢查從裝置撤銷的一組憑證。 管理員可指定認證授權中心 (CA)，讓配置啟用對所有連結至該 CA 的憑證的撤銷檢查。

適用於: iOS 14.2+ 和 visionOS 1.1+

程序

1. 前往配置 > +新增。
2. 在搜尋欄位中輸入憑證，然後按一下憑證撤銷檢查配置。
3. 輸入配置的名稱和描述。
4. 選擇演算法為 SHA 256 然後輸入根憑證的雜湊。

> 在雜湊中，您必須輸入憑證的公開金鑰之 Base64 編碼（二進位）SHA-256 雜湊。 請參閱 **Apple 說明文件**，瞭解可用於 Apple 作業系統的受信任根憑證。 您可在此配置中新增多個根憑證。

5. 按下一步。
6. 選擇啟用此配置選項。
7. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂。
8. 按一下完成。

10.10.4.11. 建立自發的單一應用程式模式組態

自發的單一應用程式模式組態讓您確保只有特定應用程式在裝置上執行。 即便使用者嘗試啟動不同的應用程式，組態也只啟動特定的應用程式。

程序

1. 前往**組態** > **新增** > **自發的單一應用程式模式**。
2. 使用下列準則來定義 app 及相關設定。
3. 按**下一步**。

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
配置設置	**套組識別碼** - (必填) 唯一套組識別碼。 若兩個字典包含相同的 BundleIdentifier 值但卻包含不同的 TeamIdentifier 值，則此狀況將被視為錯誤，也不會安裝設定檔。 **團隊識別碼** - (必填) 開發人員的團隊識別碼，用於簽署應用程式。

4. 在**發佈**畫面，選取要接收此組態的群組。
5. 按一下**完成**。

10.10.4.12. 建立 DNS Proxy 組態

作為 Ivanti Neurons for MDM 管理員，您可以使用 iPhone 和 iPad 裝置使用者的 DNS Proxy 組態來配置 DNS Proxy 設定。 您可以使用 DNS Proxy 承載指定提供 DNS Proxy 網路擴充功能和其他廠商特定值的應用程式。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 前往**組態**
3. 在搜尋欄位中輸入 **DNS**，然後按一下 **DNS Proxy 組態**。
4. 輸入配置的名稱和描述。
5. 輸入下列 DNS Proxy 組態設定:
    - 應用程式套件識別碼 (必填)。
    - 提供者套件識別碼。
    - 提供者組態 (鍵值)。
6. 按**下一步**。
7. 選擇**啟用此配置**選項。
8. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂

按一下**完成**。

10.10.4.13. 裝置記錄組態

裝置記錄組態可讓您啟用 Android 裝置的網路與安全性記錄。

建立裝置記錄組態

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中，輸入**裝置記錄**並選取組態。
4. 輸入配置的名稱和描述。
5. 在**組態設定**區段下，選取其中一個或兩個選項:
    - 啟用網路記錄
    - 啟用安全性記錄

> 如需支援的 Android 版本安全性與網路記錄的相關資訊，請參閱下面位於**安全性記錄列表**下的表格。

按**下一步**，確認發佈設定。

7. 按一下**完成**。

安全性記錄列表

裝置類型	支援的 Android 版本
工作受控裝置與工作受控裝置非 GMS 模式 (AOSP)	7、8、9、10、11、12、13
具有工作設定檔的受管理裝置	8、9、10
工作描述檔	不適用
公司擁有裝置上的工作設定檔	11、12、13

網路記錄列表

裝置類型	支援的 Android 版本
工作受控裝置與工作受控裝置非 GMS 模式 (AOSP)	8、9、10、11、12、13
具有工作設定檔的受管理裝置	8、9、10
工作描述檔	12、13
公司擁有裝置上的工作設定檔	12、13

將裝置記錄組態安裝在裝置上後，使用者會收到一則通知，當中有關於裝置管理與網路記錄的資訊。 按一下**確定**以確認通知。

要求偵錯記錄

程序

1. 登入 Ivanti Neurons for MDM。
2. 前往**裝置** > **裝置詳細資料**。
3. 在**概觀**區段中，按一下**強制簽入**按鈕旁的垂直三個點按鈕。
4. 選取**要求偵錯記錄**。
5. 從下列兩個選項中選取一個:
   - 排除錯誤報告 - 當選取此選項並按一下「下一步」時，畫面上會出現確認視窗。 按一下**要求偵錯記錄**。 使用者無需為此選項提供同意意向，而且這些記錄將排除所選 Android 裝置的錯誤報告。
   - 包含錯誤報告 - 當選取此選項並按一下「下一步」時，畫面上會出現確認視窗。 按一下**要求偵錯記錄**。 使用者必須提供同意意向才能分享錯誤報告。 如果是 Android 裝置，系統將提示使用者提交裝置記錄，包含錯誤報告。

10.10.4.14. 磁碟管理組態

Ivanti Neurons for MDM 磁碟管理組態設定用於定義有效管理外部和網路儲存裝置中資料的原則。

適用於: 受監督的 macOS 15.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取**磁碟管理**組態。
3. 依下表設定**磁碟管理**設定:

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
磁碟管理	
外部儲存裝置	從下拉式清單中選取以下其中一個值: • **允許**: 允許讀取和寫入儲存裝置。 • **唯讀**: 允許讀取儲存裝置。 • **不允許**: 不允許存取儲存裝置。
網路儲存空間	從下拉式清單中選取以下其中一個值: • **允許**: 允許讀取和寫入儲存裝置。 • **唯讀**: 允許讀取儲存裝置。 • **不允許**: 不允許存取儲存裝置。

4. 按**下一步**，確認發佈設定。
5. 選取其中一個發佈選項以設定**磁碟管理**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
6. 按一下**完成**。

10.10.4.15. Android 加密

加密配置可定義「裝置管理」模式中 Android 裝置的加密需求。 裝置加密可確保企業的機密資料不受已知的破解或 root 存取。 加密會以無法存取的方式來儲存裝置的資料，當裝置遭竊時，竊賊也無法存取資料。

啟用加密後，會提示裝置使用者加密裝置，同時需要設定裝置密碼。 密碼是用來解密資料，以便您讀取。 在 Android 企業 (工作描述檔或受管理裝置) 或 iOS 裝置上設定密碼後，將自動啟用加密。 正在加密裝置時，無法使用裝置。 開啟加密後，若要關閉則要進行裝置的原廠重設。

加密設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
啟用裝置加密	選擇此設定，以開啟所有具備加密功能並可接收此配置之 Android 裝置的加密功能。

> 針對在 Android 11 上使用裝置管理員模式的 Samsung 裝置，已經棄用 Android 加密組態。 在已設定裝置密碼的情況下，Android Enterprise 裝置預設支援此種加密方式。

如需更多資訊，請參閱**如何建立配置**。

10.10.4.16. 加密 DNS

授權：Gold

適用於：

- iOS 14.0 或支援的更新版本。
- macOS 11.0 或支援的更新版本。
- visionOS 1.1 或支援的更新版本。

配置加密 DNS 可讓您增強安全性，無需配置 VPN。

本節包含以下各主題：

- 加密 DNS 配置
- 加密 DNS 配置設定

加密 DNS 配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入 **DNS**，然後按一下**加密 DNS** 配置。
4. 輸入配置的名稱和描述。
5. 輸入加密 DNS 配置設定。
6. 按**下一步**。
7. 選擇**啟用此配置**選項。
8. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂
9. 按一下**完成**。

加密 DNS 配置設定

使用以下表格中的設定，以設定加密 DNS。 有關這些設定中的更多資訊，請參閱 **Apple 說明文件**。

設定	描述
DNS 設定	此字典定義加密 DNS 伺服器的配置。
DNS 通訊協定	指定用於與 DNS 伺服器通訊的加密傳輸通訊協定。 選擇下列其中一項通訊協定： • HTTPS • TLS
伺服器 URL	DNS-over-HTTPS 伺服器的 URI 範本，如 RFC 8484 中定義。 此 URL 必須使用 https:// 架構，且 URL 中的主機名稱或位址將會用於驗證伺服器憑證。 如果未提供伺服器位址，URL 中的主機名稱或位址將會用於決定伺服器位址。 只有當 DNS 通訊協定為 HTTPS 時才必須提供此金鑰。
伺服器位址	DNS 伺服器 IP 位址字串的未排序清單。 這些 IP 位址可以混合 IPv4 和 IPv6 位址。 按一下**新增**以新增一或多個伺服器位址。
增補相符網域	使用網域字串清單來判斷哪些 DNS 查詢將使用 DNS 伺服器。 如果未提供此清單，所有網域將會使用 DNS 伺服器。 按一下**新增**以新增一或多個網域。
禁止使用者停用 DNS 設定	禁止使用者停用 DNS 設定。 此金鑰僅適用於受監管的裝置。
需求規則	定義 DNS 設定的一組規則。 如果沒有規則，系統會一律套用 DNS 設定。 按一下 **+新增需求規則**以新增一或多組需求規則。
網路	如果此字典符合目前的網路時要採取的行動。 選擇下列其中一項動作： • **連線：**當字典符合時套用 DNS 設定。 • **中斷連線：**當字典符合時不套用 DNS 設定。 • **評估連線：**當字典符合時使用每個網域例外套用 DNS 設定。

評估連線	此網路選項具有以下設定：
	• **網域動作** - 指定網域的 DNS 設定行為。 選擇下列其中一項動作：
	  ◦ **從不連線** - 不針對指定的網域使用 DNS 設定。
	  ◦ **視需要連線** - 允許針對指定的網域使用 DNS 設定。
	• **網域** - 此評估套用的網域。 按一下 **+新增**以新增一或多個網域。

規則	按一下 **+新增**以新增一或多個規則，將以下參數與對應的指定值配對。
DNS 網域相符	一組網域名稱。 如果在指定清單中有任何網域名稱符合裝置搜尋網域清單中的任何網域，則符合此規則。
DNS 伺服器位址相符	一組 IP 位址。 如果有任何網路指定的 DNS 伺服器符合陣列中的任何項目，則符合此規則。
SSID 相符	一組 SSID 符合目前的網路。 如果網路不是 Wi-Fi 網路或如果 SSID 未出現在此陣列中，則不符合。 省略此金鑰和對應陣列以符合任何 SSID。
介面類型相符	一種介面類型。 如已指定，只有當主要網路介面硬體符合指定類型，則符合此規則。 選擇下列其中一個類型： • 乙太網路

設定	描述
	• Wi-Fi • 行動數據
URL 字串探查	要探查的 URL。 如果已成功擷取此 URL (傳回 200 HTTP 狀態代碼) 而不重新導向，則符合此規則。

如需更多資訊，請參閱**如何建立配置**。

10.10.4.17. 外部智慧設定

使用**外部智慧設定**在受監管裝置上設定外部智慧整合。 此組態可協助管理員套用一致的原則式設定，此類設定可控制裝置連線及使用支援的外部智慧服務的方式。

適用於：

- 受監管的 iOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監管的 macOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監管的 visionOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取**外部智慧設定**組態。
3. 按照下表設定**外部智慧設定**組態:

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
允許外部情報整合	選取核取方塊以啟用外部智慧整合。 切換**推播至裝置**按鈕，在受監管的裝置上啟用外部智慧整合。
允許外部智慧整合登入	選取核取方塊以啟用外部智慧整合登入。 切換**推播至裝置**按鈕，以啟用受監管裝置上的外部智慧整合登入。
允許的外部智慧工作區 ID	輸入 Workspace ID 以啟用外部智慧。 切換**推播至裝置**按鈕，為受監管裝置上輸入的工作區 ID 啟用外部智慧。

4. 按**下一步**，確認發佈設定。
5. 選取其中一個發佈選項以設定**外部智慧設定**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
6. 按一下**完成**。

10.10.4.18. 威脅防護

適用於：

- 適用於 iOS 用戶端 3.2.0 版或支援的更新版本的 Go。
- 適用於 Android 用戶端 52 版或支援的更新版本的 Go。

Ivanti Neurons for MDM 能夠發佈啟用權杖，以便啟用已整合在 Go for Android 和 iOS 用戶端中的威脅防護技術。 Threat Defense 可保護受管理裝置，防止行動威脅和漏洞影響裝置、網路及應用程式。

只要在 Ivanti Neurons for MDM 中啟用此組態並套用到裝置，便會在 Go 用戶端上啟用威脅防護程式庫。 若要停用威脅防護服務，請移除授權權杖並將授權配置重新傳送到用戶端。

威脅防護可監控：

- 裝置層級：系統參數、配置、韌體及程式庫，以識別可疑或惡意活動。
- 網路層級：網路流量與往返行動裝置的可疑連線。
- App 層級：外洩 app (可能使得企業資料面臨危險) 和惡意 app，透過風險評量與程式碼分析。

最新文件

如需最新的威脅防護說明，請造訪產品說明文件網站，並參閱 **Ivanti Neurons for MDM 產品說明文件**中的 *Ivanti Neurons for MDM 威脅防護解決方案指南*。

10.10.4.19. FileVault 2

授權：Gold

FileVault 2 提供可在磁碟區內容上執行完整 XTS-AES 128 磁碟加密的功能。

啟用 FileVault 2 時，您可進行下列設定：

類別	設定
FileVault 使用者設定	• 在 SetupAssist 期間啟用 FileVault **預設值**: False • 若為 True，並且在安裝小幫手中註冊 Ivanti Neurons for MDM 後安裝承載，則會要求安裝小幫手在設定時啟用 FileVault。 此外，系統會忽略此承載中的所有其他金鑰，但 ShowRecoveryKey 除外。 **先決條件**:- 在安裝小幫手中啟用 FileVault 之前，請確保在裝置註冊組態設定檔中啟用**在裝置註冊設定期間等待裝置組態**。 • 延遲啟用 FileVault 直到指派的使用者登出為止 ◦ 一律提示使用者啟用 FileVault ◦ 使用者可略過啟用 FileVault 的次數上限 不要在使用者登出時要求啟用 FileVault
輸出路徑	輸入儲存復原金鑰及電腦資訊 plist 位置的路徑。
個人復原金鑰	• 建立個人復原金鑰 • 在 FileVault 啟用後，顯示使用者的個人復原金鑰 只有當**建立個人復原金鑰**啟用時才會顯示此選項。 預設會停用此選項。 • 啟用機構復原金鑰：使用鑰匙圈 - 如果在此裝載中未提供任何憑證資訊，將使用 /Library/Keychains/FileVaultMaster.keychain 上已建立的鑰匙圈。 請選擇下列選項之一： ◦ 上傳認證 ◦ 認證 ◦ 在使用者系統上使用 Keychain
__ 天後輪換 FileVault 金鑰	管理員可以為 macOS 裝置設定 FileVault 金鑰定期輪換，以減輕已部署裝置的安全風險。 管理員可以以天為單位設定輪換間隔。 僅輪換個人復原金鑰。

10.10.4.20. FileVault 復原金鑰

授權：Gold

「FileVault 復原金鑰配置」可決定將 FileVault 復原金鑰重新導向並委付至企業伺服器。

> 已停用「FileVault 復原金鑰」配置的「排除」和「重新推送」，因為 macOS 裝置在重新推送配置時會停止傳送復原金鑰。

您可以設定下列選項：

設定	描述
名稱	輸入可識別此配置的名稱。
描述	(選用) 輸入可說明此配置用途的描述。
適用於 macOS <10.13 的配置設定	
將復原金鑰儲存至 Ivanti Neurons for MDM 租戶	選擇此選項可讓 Ivanti Neurons for MDM 將金鑰儲存在租用戶上。 如有需要，可透過「裝置詳細資料」頁面解密這些金鑰。
限制伺服器的 URL	輸入下列設定： • 輸入應傳送 FDE 復原金鑰至其中 (而不是 Apple) 的**重新導向 URL**。 URL 開頭必須為 https://。 • 從下拉式清單中選擇憑證。 僅支援 PKCS1 格式的憑證。
適用於 macOS 10.13+ 的配置設定	
定位	(必填) 針對將委付復原金鑰的位置，輸入簡短的說明。 此文字將會插入使用者在啟用 FileVault 時所看到的訊息中。
裝置金鑰	(選用) 輸入要納入說明文字中的字串 (若使用者似乎忘記密碼)。

10.10.4.21. FileVault 選項配置

此配置可讓管理員啟用或停用 FileVault，並在系統進入待命時銷毀 FileVault 金鑰。

適用於：macOS 10.7+

程序

1. 前往**組態** > **+新增**。
2. 在搜尋欄位中輸入 FileVault，然後按一下 FileVault 選項配置。
3. 輸入配置的名稱和描述。
4. 在配置設置中，選擇所需的選項：
    - 當系統在待命模式下銷毀 FileVault 金鑰
    - 不允許停用完整磁碟加密
    - 不允許啟用完整磁碟加密
5. 按下一步。
6. 選擇啟用此配置選項。
7. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂。
8. 按一下完成。

10.10.4.22. 身份憑證

本節包含以下各主題：

- 身份憑證設定
- 發佈配置

身分認證配置可定義行動電話裝置的認證驗證機制。 身分認證為 X.509 認證 (.p12 或 .pfx)。 此外，可以使用憑證授權單位作為來源動態產生身分憑證。 開始之前，您應該計劃好要如何將認證發佈至行動電話裝置。 您也應該配置好任何必要的憑證授權中心。

> 從版本 91 開始，Apple 裝置的裝置識別憑證將在到期的 30 天內自動更新。 iOS 裝置將從 Ivanti Neurons for MDM 接收更新後的 MDM 憑證，這是常規裝置簽入流程的一部分。 但是，iOS 裝置若離線的時間過長，導致 MDM 憑證在簽入之前過期而未在過期之前完成更新，就需要重新註冊 Ivanti Neurons for MDM。

- 建立身分憑證時，SHA-1 憑證已被取代。 您可以選擇其他演算法。 更新憑證時，如果舊版憑證使用 SHA-1，即可使用相同的 SHA-1 演算法。 如果舊版憑證使用 SHA-1 以上的演算法，就不允許切換至 SHA-1。
- 在設定身分憑證之後，您可以按一下**測試配置並繼續**，以發出測試憑證並驗證其有效性。 如果主體名稱和本機憑證授權中心相同，針對動態產生的全新或現有身分憑證配置執行此測試時，可能會顯示錯誤。 出現此錯誤訊息時，您應修改身份憑證主體名稱，使其與本機憑證授權中心主體名稱不同。 當現有身分憑證配置隨主體名稱修改時，系統會重新發出憑證，並重新推送配置。
  如果您將建立配置但不發出測試憑證的選項設成**動態產生**憑證發佈，請按一下**繼續**。
- 憑證將以隱含方式重新核發。
- 當身分認證指派給 Android app 時，使用者的 app 會取得身分認證，而且系統不會提示使用者授予使用此認證的權限 (而非 app)。 其中包括所有 app，例如 Email+、Gmail 等等。
- Email+ 可以配置使用者所提供的身份憑證，然後推送並指定為 Android Enterprise 裝置的 app 配置。 這僅適用於「公司擁有裝置上的工作描述檔」和「裝置擁有者」模式。

身份憑證設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。

憑證發佈	選擇要設定的認證發佈類型：
	• **單一檔案**：上傳現有的認證以發佈給裝置。
	• **動態產生**：使用本機或外部認證授權中心，依據要求建立認證。
	• **使用者提供**：建立使用者所要上傳之憑證類型的標籤。 建立後，使用者將可在自助式入口網站中查看建立的標籤 (選項)，並上傳對應這些標籤的憑證。
	• **衍生的憑證：**指定下列其中一種衍生憑證使用方式：
	  ◦ 憑證
	  ◦ 加密
	  ◦ 簽署
	  ◦ 解密
	• **SCEP 組態**: 指定如何從 SCEP 伺服器申請憑證。 選擇下列其中一項配置：
	  ◦ Apple 組態
	  ◦ Windows 配置
	  您的選擇決定了其餘表單中會顯示哪些選項。

允許所有 App 存取私密金鑰 (macOS 10.10+)	**適用於:** 單一檔案身分識別憑證、動態產生的身分識別憑證、使用者提供的身分識別憑證及 SCEP Apple 組態身分識別憑證。 (選用) 對於 PKCS#12 憑證，請啟用**允許所有應用程式存取私密金鑰**選項，以允許所有應用程式存取私密金鑰。 例如，如果要求使用者必須輸入密碼才允許存取用於 VPN 的憑證，便可使用此金鑰。
單一檔案	
身分憑證資料	將認證檔案拖曳到虛線方塊中，或按一下**選擇檔案**，從檔案系統中進行選擇。
密碼	輸入保護 PKCS#12 憑證檔案的密碼。 此密碼可用來進行不予提示的安裝。
動態產生	
來源	從下拉清單中選擇本機憑證授權中心。 您應已在**管理 >** 憑證管理下方建立此 CA。
建立配置但不發出測試憑證	選擇勾選方塊以建立配置但不發出測試憑證。
僅限 Windows - 目標憑證存放區	管理員現在可以選擇 Windows 裝置上的目標憑證存放區。
使用者提供	
憑證顯示名稱	輸入憑證的名稱。 此憑證名稱對於租戶而言是唯一的，而使用者在上傳憑證時，將可在自助式入口網站中查看該名稱。
刪除私密金鑰	選擇此選項可在 *n* (1-30) 天之後刪除憑證的私密金鑰。 您也可以使用 Ivanti Neurons for MDM 提供的 API 來處理這些作業。 請參閱 Ivanti Neurons for MDM

設定	方法
	API 指南，以取得更多 API 相關資訊。 如果您嘗試在任何配置 (例如驗證應用程式，或者推送 Wi-Fi 或 VPN 配置) 中使用已刪除私密金鑰的憑證，作業將會失敗。 請務必在刪除私密金鑰之前執行作業。
在以下天數之後刪除私密金鑰	選擇要在多久後清除憑證私密金鑰的天數 (1-30)。 預設值為 2 天。
衍生的憑證	
衍生的認證使用狀況	請選擇下列任何選項： • **驗證** - 指定用於驗證的衍生認證。 • **加密** - 指定衍生認證的用途是加密。 • **簽署** - 指定衍生認證是用於簽署。 • **解密** - 指定衍生憑證的用途是解密。
品牌	請從下列選項選擇您使用的衍生憑證提供者： • **Entrust** • **Intercede** • **Purebred** 如要新增您使用的自訂衍生憑證提供者，請參閱衍生的憑證提供者。
ACME 組態 - 僅適用於 iOS/iPadOS16+ /macOS14+	
用戶端識別碼	識別特定裝置的唯一字串
目錄 URL	(必要) ACME 伺服器的目錄 URL。 URL 必須使用 https 配置。
擴充金鑰使用方式	值為字串的陣列。 每個字串都是點分表示法中的 OID。 例如，["1.3.6.1.5.5.7.3.2", "1.3.6.1.5.5.7.3.4"] 表示用戶端驗證和電子郵件保護。 裝置會要求 ACME 伺服器核發之憑證的此欄位。 ACME 伺服器可能會覆蓋或忽略自身所核發之憑證中的此欄位。
金鑰大小	(必要) KeySize 的有效值會視 KeyType 和 HardwareBound 的值而定。 有關具體需求，請參閱那些金鑰。
金鑰類型	(必要) 要產生的金鑰配對類型。
主旨	(必填) 輸入以逗號分隔之 OID 和值組呈現的 X.500 名稱。 一般來說，主旨會設為使用者的完整網域名稱。 例如：C=US,DC=com,DC=MobileIron,OU=InfoTech 或 CN=www.mobileiron.com。 您也可以將變數附加至 OID，以自訂主旨。 例如，CN=www.mobileiron.com-$。 為便於配置，您還可以使用 $ 變數，將使用者的 FQDN 填入主旨。 請勿在主旨名稱中使用反斜線字元 (\)。
主體替代名稱	裝置會要求 ACME 伺服器核發之憑證的主體替代名稱。 ACME 伺服器可能會覆蓋或忽略自身所核發之憑證中的此欄位。

設定	方法
金鑰使用方式	此值為位元欄位。 位元 0x01 表示數位簽名。 位元 0x10 表示金鑰協定。 裝置會要求 ACME 伺服器核發之憑證的此金鑰。 ACME 伺服器可能會覆蓋或忽略自身所核發之憑證中的此欄位。
硬體繫結	若硬體繫結設為 true，則私密金鑰會繫結至裝置，而且此時金鑰類型必須為 ECSECPrimeRandom，金鑰大小必須為 256 或 384。
證明	若為 true，裝置會提供描述裝置和產生之金鑰的證明給 ACME 伺服器。 當證明為 true 時，硬體繫結也必須為 true。
SCEP 組態 - Apple 組態	
身分憑證 (SCEP)	選擇指定 SCEP 伺服器。
本機憑證授權中心	選擇以指定您於**管理 >** 憑證管理下方所建立的本機憑證授權中心。 選擇此選項時，請從顯示的下拉清單中選擇本機認證授權中心。
網址 (URL)	輸入 SCEP 伺服器的 URL。
CA 識別碼	輸入憑證授權中心提供的識別碼。
主旨	輸入 X.500 名稱 (以逗號分隔之 OID 和值組呈現)。 一般來說，主旨會設為使用者的完整網域名稱。 例如：C=US,DC=com,DC=MobileIron,OU=InfoTech 或 CN=www.mobileiron.com。 您也可以將變數附加至 OID，以自訂主旨。 例如，CN=www.mobileiron.com-$DEVICE_CLIENT_ID$。 若要更輕鬆配置，您也可以使用 $USER_DN$ 變數，將使用者的 FQDN 填入主旨。 主旨名稱不使用反斜線字元 (\)。
主旨別名類型	依據憑證範本的屬性，選擇「RFC 822 名稱」、「DNS 名稱」、「統一資源識別碼」或「無」。
主旨別名值	輸入對應類型的值。 如果您輸入 $ 做為第一個字元，將會顯示下拉式清單，其中包含可能的自訂 LDAP 和 Entra ID 屬性。 從清單中選擇適當的自訂屬性。 如果使用 Entra ID 值，則僅支援 onPremisesImmutableId。 輸入 fn:base64tohex($)
NT 主體名稱	輸入適用於 Microsoft 環境的主旨別名。 此項目在配置時通常會包括使用者的 UPN (使用者主體名稱)。
挑戰	(選用) 做為自動註冊的預先共用密碼。
重試次數	從清單中選擇數字，以設定第一次傳回「擱置中」狀態之後要嘗試的驗證次數。
重試延遲	從清單中選擇數字，以設定重試前要等待的秒數。
金鑰大小	選擇 1024、2048 或 4096 位元。
用來作為數位簽署	選擇憑證是否可用於簽署。
用來作為金鑰加密	選擇憑證是否可用於加密。
CA 指紋	如果您的憑證授權中心使用 HTTP，請輸入十六進位字串做為 CA 憑證的指紋。 支援 MD5 指紋。 您也可以使用認證來建立指紋。 您可直接將認證拖曳到指定的區域，或按一下**從認證來建立**，以從檔案系

設定	方法
	統中選擇認證。
SCEP 配置 - Windows 配置	
CA (憑證授權中心)	選擇以指定您已在**管理 >** 憑證管理下方建立的憑證授權中心。 選擇此選項時，請從顯示的下拉清單中選擇憑證授權中心。
主旨	輸入 X.500 名稱 (以逗號分隔之 OID 和值組呈現)。 一般來說，主旨會設為使用者的完整網域名稱。 例如：C=US,DC=com,DC=MobileIron,OU=InfoTech 或 CN=www.mobileiron.com。 您也可以將變數附加至 OID，以自訂主旨。 例如，CN=www.mobileiron.com-$DEVICE_CLIENT_ID$。 若要更輕鬆配置，您也可以使用 $USER_DN$ 變數，將使用者的 FQDN 填入主旨。 主旨名稱不使用反斜線字元 (\)。
主旨別名類型	按一下 **+新增**，依據憑證範本的屬性，選擇「RFC 822 名稱」、「DNS 名稱」、「統一資源識別碼」或「無」。
重試次數	從清單中選擇數字，以設定第一次傳回「擱置中」狀態之後要嘗試的驗證次數。
重試延遲	從清單中選擇數字，以設定重試前要等待的秒數。
金鑰長度	選擇 1024、2048 或 4096 位元的金鑰大小。
選擇用途	選擇至少一個選項： • 用於數位簽署 - 選擇憑證是否可用於簽署。 • 用於金鑰加密 - 選擇憑證是否可用於加密。
有效性	選擇有效天數、月數或年數。
CA 指紋	如果您的憑證授權中心使用 HTTP，請輸入十六進位字串做為 CA 憑證的指紋。 支援 MD5 指紋。 您也可以使用認證來建立指紋。 您可直接將認證拖曳到指定的區域，或按一下**從認證來建立**，以從檔案系統中選擇認證。
雜湊演算法系列	選擇 SHA-2 或 SHA-3 演算法。

在未設定工作挑戰 (Work Challenge) 密碼的裝置上，若要將身分憑證套用至工作描述檔，裝置會提示輸入裝置密碼而非工作挑戰密碼。

如需更多資訊，請參閱使用配置。

10.10.4.23. Apple 啟用鎖定配置

授權：Silver

本節包含以下各主題：

- 啟用 iOS 啟用鎖定
- 啟用受監管裝置上的「iOS 啟用鎖定」功能
- 啟用 macOS 啟用鎖定
- 啟用受監管裝置上的「macOS 啟用鎖定」功能
- 使用 iOS 啟用鎖定省略碼
- 清除 iOS 啟用鎖定省略碼

「啟用鎖定」是 Apple 產品的一項功能，專為防止他人冒用遺失或遭竊的裝置而設計。 在啟用「尋找我的」之後，就 iCloud 帳戶與這台裝置的硬體識別碼的對應儲存到 Apple 的啟用伺服器中。 從這時候起，只要沒有輸入既有的 Apple ID 和密碼，就不能關閉「尋找我的」、清除裝置或重新啟用裝置。 如果使用者以外的人想要清除裝置或嘗試重新啟用裝置，「設定小幫手」就會顯示輸入 Apple ID 和密碼的提示。

如果一般使用者已啟用「尋找我的裝置」，則停用「啟用鎖定」並不會停用受監管裝置上的此項功能。 「設定小幫手」會提示使用者在重設或遠端抹除裝置時該採取的動作。

「啟用鎖定」也提供管理員更多選項，以防範受監管的裝置遭竊。 不過，大多數的企業管理員可能會停用「啟用鎖定」，因為這主要是消費型功能。 下表摘要用於公司的部署選項：

裝置類型	結果
用於公司且受監管	• 受監管裝置的「啟用鎖定」預設為停用。 • 裝置使用者無法開啟「啟用鎖定」。
用於公司且未受監管	• 只要一般使用者利用 Apple ID 登入 iCloud，並開啟「尋找我的 iPhone」，即會啟用「啟用鎖定」。 • MDM 伺服器 (包括 Ivanti Neurons for MDM) 無法控制未受監管裝置上的啟用鎖定。 裝置使用者可以用自己的個人憑證來鎖定啟用，日後離職時將可不留任何資源給公司。

啟用 iOS 啟用鎖定

適用於：iOS 7+ 受監管的裝置

此項配置適用於已啟用**尋找我的**功能的受監管裝置 (iOS 7 及更新版本)。 如果管理員或其他使用者嘗試「抹除」、「啟動」或停用裝置上的「尋找我的裝置」，即會顯示 Apple 的「啟用鎖定」畫面。 若要繼續，則必須輸入 iTunes 認證或密碼鎖。

啟用時，系統會儲存受監管裝置的密碼鎖，並可在裝置詳細資料中檢視。 您可使用受監管裝置的「清除啟用鎖定」命令，遠端傳送密碼鎖。 不過，如果重新啟動裝置或關閉「尋找我的裝置」功能時，就必須手動輸入密碼鎖。

> 您僅可針對所有空間，建立一個「啟用鎖定」配置。

啟用受監管裝置上的「iOS 啟用鎖定」功能

程序

1. 在您的裝置上啟用**尋找我的**功能。

2. 前往**配置**。
3. 從既有的配置清單中，選擇 **Apple 啟用鎖定**配置。
4. 按一下**編輯**。
5. 在「iOS 7+ 受監管」區段中，按一下**啟用「啟用鎖定」**。
6. 按一下**完成**。
7. 註冊裝置。

啟用 macOS 啟用鎖定

適用於：macOS 10.15+ 受監管的裝置

此配置會套用至 macOS 10.15 和更新版本的受監管裝置。 macOS 的「啟用鎖定」僅會套用至搭載 Apple T2 安全晶片的 Mac。 在受監管裝置 (不論升級或新安裝) 以及升級的目前註冊裝置中，「啟用鎖定」皆預設為關閉。 啟用「尋找我的裝置」時，並不會自動啟用這些裝置的「啟用鎖定」

如果管理員或其他使用者嘗試「清除」、「啟動」或停用裝置上的「尋找我的」功能，即會顯示 Apple 的「啟用鎖定」畫面。 若要繼續，則必須輸入 iTunes 憑證或密碼鎖。 啟用時，系統會儲存受監管裝置的密碼鎖，並可在裝置詳細資料中檢視。 您可使用受監管裝置的「清除啟用鎖定」命令，遠端傳送密碼鎖。 不過，如果重新啟動裝置或關閉「尋找我的」功能時，就必須手動輸入密碼鎖。

> 您僅可針對所有空間，建立一個「啟用鎖定」配置。

啟用受監管裝置上的「macOS 啟用鎖定」功能

程序

1. 在您的裝置上啟用「尋找我的」功能。
2. 前往**配置**。
3. 從既有的配置清單中，選擇 **Apple 啟用鎖定**配置。
4. 按一下**編輯**。
5. 在「macOS 10.15+ 受監管」區段中，按一下**啟用「啟用鎖定」**。
6. 按一下**完成**。
7. 註冊裝置。

使用 iOS 啟用鎖定省略碼

當啟用 iOS 啟用鎖定的裝置被清除時，略過碼會保留在 Apple 啟用伺服器與 Ivanti Neurons for MDM 管理介面中。

程序

1. 前往**裝置**。
2. 選擇裝置。
3. 按一下**動作 > 清除**。 可能需要幾分鐘時間，裝置才會重新啟動。
4. 當裝置提示您輸入 Apple ID 與密碼時，請將 **Apple ID** 保留空白。
5. 在**密碼**欄位中輸入省略碼。
6. 按**下一步**。

7. 繼續設定。

清除 iOS 啟用鎖定省略碼

在 Ivanti Neurons for MDM 管理介面中清除 iOS 啟用鎖定時，系統會從 Apple 啟用伺服器移除略過碼，但略過碼仍會出現在 Ivanti Neurons for MDM 管理介面的裝置詳細資料中。

程序

1. 前往**裝置**。
2. 選擇裝置。
3. 選擇**配置**。
4. 選擇 **Apple 啟用鎖定**。
5. 按一下**編輯**。
6. 在「iOS 7+ 受監管」區段中，停用**啟用「啟用鎖定」**。
7. 按一下**完成**。
8. 前往**裝置**。
9. 選擇裝置。
10. 按一下**動作 > 清除**。 可能需要幾分鐘時間，裝置才會重新啟動。 您現在即可使用新的 Apple ID 與密碼來設置裝置。
11. 繼續設定。

「清除 iOS 啟動鎖定」狀態會顯示在介面上如下所示：

狀態	結果
擱置中	• 伺服器正傳送「清除啟動鎖定」碼給 Apple。
已傳送	• Apple 確認收到「清除啟動鎖定」碼。
失敗	• 伺服器無法將此碼傳送給 Apple。 • Apple 已對此錯誤提出報告。

10.10.4.24. iOS 自訂配置

iOS 自訂配置可讓您上傳並發佈不同 app (例如 Apple 的 iPhone 配置公用程式) 建立的 iOS 配置描述檔。

iOS 自訂設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
檔案資料	拖曳配置檔案，或按一下**選擇檔案**，從檔案系統中進行選擇。

如需更多資訊，請參閱**如何建立配置**。

10.10.4.25. 智慧設定

使用智慧設定在受監管的裝置上設定 Apple Intelligence 設定。 此聲明可協助管理員套用一致的原則型控制項，以管理裝置存取和使用 Apple Intelligence 功能的方式。

適用於：

- 受監管的 iOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監管的 macOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監管的 visionOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取 **Intelligence 設定**組態。
3. 依下表設定各項**智慧設定**:

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
允許 Apple Intelligence 報告	選取核取方塊以啟用 Apple Intelligence 報告。 切換**推播至裝置**按鈕，在受監管的裝置上啟用 Apple Intelligence 報告。
允許 Genmoji	選取核取方塊以啟用 Genmoji。 切換**推播至裝置**按鈕，在受監管的裝置上啟用 Genmoji。
允許 Image Playground	選取核取方塊以啟用影像播放區。 切換**推播至裝置**按鈕，在受監管的裝置上啟用影像播放區。
允許 Image Wand	選取核取方塊以啟用影像操作棒。 切換**推播至裝置**按鈕，在受監管的裝置上啟用影像操作棒。 此設定不適用於 macOS 裝置。
允許個人化手寫結果操作棒	選取核取方塊以啟用個人化手寫結果操作棒。 切換**推播至裝置**按鈕，在受監管的裝置上啟用個人化手寫結果操作棒。 此設定不適用於 macOS 和 visionOS 裝置。
允許視覺智慧摘要	選取核取方塊以啟用視覺智慧摘要。 切換**推播至裝置**按鈕，以在受監管的裝置上啟用視覺智慧摘要。 此設定不適用於 macOS 和 visionOS 裝置。
允許書寫工具	選取核取方塊以啟用寫入工具。 切換**推播至裝置**按鈕，在受監管的裝置上啟用寫入工具。
強制僅裝置聽寫	選取核取方塊以啟用僅裝置聽寫。 切換**推播至裝置**按鈕，在受監管的裝置上啟用僅裝置聽寫。
強制僅裝置翻譯	選取核取方塊以啟用僅裝置翻譯。 切換**推播至裝置**按鈕，以在受監管裝置上啟用僅裝置翻譯。 此設定不適用於 macOS 和 visionOS 裝置。
App	
行事曆	
允許自然語言編輯	選取核取方塊以啟用行事曆和提醒中的自然語言編輯。 切換**推送到裝置**按鈕，在受監管裝置上啟用行事曆和提醒中的自然語言編輯。
郵件	
允許智慧回應	選取核取方塊以啟用智慧回應。 切換**推播至裝置**按鈕，在受監管裝置上啟用智慧回應。
允許摘要	選取核取方塊以啟用摘要。 切換**推播至裝置**按鈕，以啟用受監管裝置的摘要。

設定	方法
備註	
允許轉譯	選取核取方塊以啟用轉譯。 切換**推播至裝置**按鈕，在受監管裝置上啟用轉譯。 此設定不適用於 visionOS 裝置。
允許轉錄檔摘要	選取核取方塊以啟用轉譯摘要。 切換**推播至裝置**按鈕，以在受監管裝置上啟用轉譯摘要。 此設定不適用於 visionOS 裝置。
Safari	
允許摘要	選取核取方塊以啟用摘要。 切換**推播至裝置**按鈕，以啟用受監管裝置的摘要。

4. 按**下一步**，確認發佈設定。
5. 選取其中一個發佈選項以設定**智慧設定**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
6. 按一下**完成**。

10.10.4.26. iOS 限制

iOS 限制是一些設定，幫助裝置的主要使用者進行控制，確定允許其他使用者使用 iOS、watchOS 和 visionOS 裝置執行的操作。 這些設定是由 Apple 定義並受 Ivanti Neurons for 管理。

將此配置發佈至**共享 iPad** 期間，您可以選擇透過裝置通道或使用者通道。 在發佈個別的配置並強制僅套用限制至裝置或使用者通道時，此功能很有用。

全域管理員可以委派空間管理員，以編輯**所有裝置和自訂發佈**選項的組態。 對於 iOS 限制設定，您可以依需要選取**允許在所有空間中提供此組態**選項。

> 發佈變更僅適用於特定空間。 所有其他空間會繼承預設空間發佈設定。

iOS 限制設定

類別	設定	方法
裝置功能	名稱 描述 **iOS 所有版本**	輸入可識別此配置的名稱。 輸入可說明此配置用途的描述。 **啟用裝置功能使用。**
	允許畫面擷取和畫面錄製	選擇允許裝置使用者利用內建 iOS 螢幕擷取功能來擷取畫面。
	允許遠端螢幕觀察 (iOS 9.3 以及更新版本) 允許強制不出現提示的受管理課程螢幕觀察 (僅限受監管 - iOS 10.3+) 允許漫遊時自動同步	選擇允許使用者觀察遠端螢幕。 (僅適用於 iPad) 選擇此選項，可在受監管的 iPad 已設好受管理的課程時，允許在螢幕不出現提示訊息的情況下自動執行。 選擇允許當裝置不在原本的國家/地區時同步處理郵件帳戶。
	允許 Siri	選擇允許在支援裝置上使用個人助理 app。
	裝置鎖定時允許使用 Siri	選擇在裝置鎖定時允許個人助理 app 執行作業。
	啟用 Siri 不雅內容篩選 (僅限受監管)	選擇啟用 Siri profanity 不雅內容篩選。
	允許語音撥號	選擇允許使用者透過裝置語音撥通聯絡人或號碼。
	允許 App 內購買項目	選擇允許使用者透過裝置上執行的 app 進行加購。
	裝置鎖定時允許使用 Passbook 允許螢幕鎖定「控制中心」 允許螢幕鎖定「通知」檢視	選擇允許裝置鎖定時顯示 Passbook 通知。 選擇允許從鎖定畫面存取「控制中心」。 選擇允許鎖定畫面顯示「通知」檢視
	允許螢幕鎖定「本日」檢視	選擇允許從鎖定畫面存取「今日」檢視。
	允許從受管理 app 至未受管理 app 使用「Open In」	**需要 Gold 授權**。 選擇允許在未受管理的 app 和帳戶中開啟受管理 app 和帳戶中的文件。 停用此選項可防止文件在受管理與未受管理的 app 及帳戶之間進行交換。 例如，您可能不希望企業文件被私人 app 開啟。 您也可以搭配使用「停用」選項和受管理的網域配置，以確保從受管理網域下載的資料只能在受管理的 app 中開啟。

類別	設定	方法
	允許從未受管理 app 至受管理 app 使用「Open In」	**需要 Gold 授權**。 選擇允許在受管理的 app 和帳戶中開啟未受管理 app 和帳戶中的文件。 停用此選項可防止文件在未受管理與受管理的 app 及帳戶之間進行交換。 例如，您可能不希望使用者利用公司電子郵件來傳送私人文件。 您也可以搭配使用「關閉」選項和受管理的網域配置，以確保從受管理網域下載的資料只能在受管理的 app 中開啟。
	第一次 AirPlay 配對時需提供密碼	選擇要求 Apple TV 顯示使用者要在 iOS 裝置上輸入的密碼，以授權裝置的初始配對。
	對 AirPlay 內送要求強制使用密碼 (tvOS 截至 10.1)	選擇要求使用者輸入內送 AirPlay 要求的密碼。 預設：取消選擇
	iOS 26+	
	豁免評等限制的應用程式 (適用於 iOS 26.1+)	僅當套組 ID 包含在多個有效載荷和家長控制應用程式 (如 ScreenTime) 的所有豁免清單的交集中時，才輸入您想要豁免的基於年齡的評級限制的應用程式清單。 預設: 已選取
	iOS 所有受監管版本	
	允許 Apple Books	選擇允許存取 Apple Books app。
	允許 iBooks Store 中的完整色情內容 (iOS 和 tvOS 11.3 以及更新版本)	選擇允許使用者下載標記為情色內容的 iBookstore 內容。
	允許帳戶修改	選擇允許使用受監管 iOS 7 裝置的使用者新增電子郵件帳戶，並變更電子郵件帳戶中已設定的項目。
	允許修改 app 行動數據	選擇允許使用者修改 app 行動數據設定。
	允許修改「尋找好友」	選擇允許使用者變更「尋找好友」的 app 設定。
	允許與非 Configurator 的主機配對	選擇允許主機配對以同步處理 iTunes。 事實上，啟用此選項可讓受監管裝置與 Mac 上的 iTunes 同步，而不只是與監管主機同步。 若停用此選項，則會停用監管主機之外的所有主機配對。 如果沒有設定任何監管主機認證，就會停用所有配對。
	允許 AirDrop	選擇允許裝置使用 AirDrop。 AirDrop 是 Apple 的臨時 Wi-Fi 系統，可讓附近的使用者共用檔案。限制此功能可保障機密文件不會洩漏給未獲授權或不安全的裝置。
	允許使用 Touch ID/Face ID 來解鎖裝置	選擇允許使用 Touch ID / Face ID 來解鎖裝置。
	允許 Spotlight 搜尋傳回網際網路搜尋結果	選擇允許 Spotlight 搜尋傳回網際網路搜尋結果。
	允許 app 進入單一 app 模式	針對可在 iOS 受監督裝置上自動進入單一應用程式模式的應用程式，輸入以逗號分隔的組合 ID 清單。 例如，您可為學生指定自訂的考試 app。 只要學生啟動 app，app 就會進入單一 app 模式，

類別	設定	方法
		這可確保學生在考試時不能使用其他資源。 此功能適用於針對獨立單一 app 模式所開發的 app。監管是透過 Apple Configurator 建立。
	iOS 8+	
	允許備份 Enterprise 書籍	選擇允許個人備份已使用 MDM 發佈到裝置的 iBooks、ePub 與 PDF 文件。
	允許同步處理 Enterprise 書籍的註記和醒目提示	選擇允許新增至企業書籍的註記和醒目提示與 iTunes 同步處理。
	強制執行 Apple Watch 手腕偵測	選擇隱藏畫面上的通知，除非使用者有配戴 Apple Watch 例外。
	iOS 8+ 受監管	
	允許預測鍵盤	選擇允許使用者啟用 iOS 的預測字詞功能，讓使用者可點選三種預測之一來完成字詞。
	允許鍵盤自動修正	選擇允許在搭配 Bluetooth 鍵盤時使用自動校正。
	允許鍵盤拼字檢查	選擇允許在搭配 Bluetooth 鍵盤時使用拼字檢查。
	允許鍵盤定義查閱	選擇允許在搭配 Bluetooth 鍵盤時使用定義查詢。
	允許修改 Touch ID 指紋/Face ID 面孔	選擇允許變更 Touch ID 或 Face ID 設定。
	iOS 9+ 受監管	
	允許 iPad 上的鍵盤快速鍵	選擇允許 iPad 的鍵盤快速鍵。
	允許修改桌布	選擇允許使用者變更桌布影像。
	允許與 Apple Watch 配對	選擇允許將 iPhone 與 Apple Watch 配對。
	允許修改裝置名稱	選擇允許使用者變更裝置名稱。
	允許修改企業 app 信任設定	選擇允許使用者變更企業 app 信任設定。
	iOS 9.3+ 受監管	
	允許修改通知設定	選擇允許使用者變更通知設定。
	iOS 9.3.2+ 受監管	
	允許診斷提交修改	選擇允許使用者變更提交診斷資料給 Apple 的相關設定。
	iOS 10+ 受監管	
	允許 Bluetooth 修改	選擇允許使用者修改受監管裝置上的 Bluetooth 設定。 這非常適用於需要 Bluetooth 才能執行 app 的情況，例如在共用 iPad 執行教育用的課堂 app。

類別	設定	方法
	iOS 10.3+ 受監管	
	允許聽寫	選擇允許使用者採用 iPhone 或 iPad 聽寫功能，而不需打字。
	iOS 11+ 受監管	
	允許 AirPrint	選擇允許 AirPrint 功能以供無線列印。
	允許 AirPrint Credential Storage	選擇允許 AirPrint 之使用者名稱與密碼的 Keychain 儲存。
	允許 AirPrint iBeacon Discovery	選擇允許使用者設定 AirPrint 印表機的 iBeacon 探索。
	允許新增 VPN 配置	選擇允許使用者建立 VPN 配置
	強制 AirPrint Trusted TLS 需求	選擇允許 TLS 列印通訊使用受信任的憑證。 預設：取消選擇
	允許移除系統 App	選擇允許移除系統 App。
	允許修改行動方案設定	選擇允許使用者修改行動方案設定。
	允許設定新的附近裝置	選擇允許使用者設定新的附近裝置。
	自動加入課堂班級，沒有提示	選擇允許使用者自動加入「課堂」班級，沒有提示。 預設：取消選擇
	允許課堂鎖定 app 與鎖定裝置，沒有提示	選擇允許「課堂」鎖定 app 與鎖定裝置，不提示使用者。 預設：取消選擇
	強制使用者執行驗證動作後，才能在 Safari 和應用程式中自動填寫密碼或信用卡資訊	裝置擁有者必須執行驗證動作後，才能在 Safari 瀏覽器和應用程式中自動填入密碼或信用卡資訊。 預設：False
	iOS 11.3+	
	允許與 Remote app 配對 (tvOS 11.3 和更新版本)	選擇允許將裝置與 Remote app 配對。
	允許內送 AirPlay 要求 (tvOS 11.3 和更新版本)	選擇允許內送 AirPlay 要求。
	iOS 11.3+ 受監管	
	允許限制 USB 模式	選擇允許使用者取用限制 USB 模式。
	將軟體更新延後 30 天 (適用於 iOS 11.3、tvOS 12.2	選擇後可輸入您想要延後軟體更新的天數。 預設 30 天，最長 90 天。 預設：取消選擇

類別	設定	方法
	以及更新版本，而且僅限受監管裝置)	
	需要教師權限才能離開未受「課堂」管理的班級 iOS 12+ 受監管	選擇允許使用者取得必要的教師權限才能離開未受「課堂」管理的班級。
	強制執行自動的日期與時間 (iOS 12.0 & tvOS 12.2 (iOS 12.0 和更新版本))	選擇開啟日期與時間「自動設定」功能。 使用者無法關閉它。 預設：False
	允許修改 eSIM 設定 (iPhone XS、iPhone XS Max 與 iPhone XR - iOS 12.1 和更新版本) **iOS 12.2+ 受監管**	選擇以允許使用者修改受支援裝置上的 eSim 設定。 此選項還可以防止使用者新增或移除裝置上「設定」中的行動方案。 預設值：True
	允許修改個人熱點設定	選擇允許使用者修改個人熱點設定。 預設值：True
	iOS 13.0+	
	允許檔案網路磁碟機存取	選擇允許使用者在「檔案」app 中連接網路磁碟機。 預設值：True
	允許檔案 USB 磁碟機存取 **iOS 13.0+ 受監管**	選擇允許使用者在「檔案」app 中連接任何已連接的 USB 裝置。 預設值：True
	允許連續路徑鍵盤	選擇以啟用連續路徑鍵盤 (滑動或追蹤輸入)。 預設值：True
	允許裝置睡眠	選擇以啟用裝置睡眠。 預設值：True
	允許尋找裝置	選擇以在「尋找」app 中啟用「尋找我的裝置」。 預設值：True
	允許尋找我的好友	選擇以在「尋找」app 中啟用「尋找我的朋友」。 預設值：True
	強制 Wi-Fi 啟動 **iOS 13.4+**	選擇以啟用 Wifi 電源開啟。 預設：False

類別	設定	方法
	允許訪客工作階段用於 iPad 共享 **iOS 14.0+**	如為 false，共享 iPad 上便無暫存工作階段可用。 預設值：True
	允許 Apple 個人化廣告	如為 false，限制 Apple 個人化廣告。 這會阻止 Apple 將使用者資訊用於投放廣告。 這可能不會降低接收到的廣告數，但是廣告與使用者的相關性會較低。 預設值：True
	iOS 14.0+ 受監管	
	允許 App Clip **iOS 14.2+ 受監管**	如為 False，則會阻止使用者新增任何 App Clip，並移除裝置上任何現有的 App Clip。 預設值：True
	允許 NFC **iOS 14.5+**	如為 false，停用 NFC。 需要受監管的裝置。 適用於 iOS 14.2 和更新版本。 預設值：True
	允許自動解鎖	管理員可使用現有的 allowAutoUnlock 限制來管理此功能。 如為 false，停用自動解鎖。 適用於 macOS 10.12 和更新版本，以及 iOS 14.5 和更新版本。 預設值：true
	強制裝置僅聽寫 **iOS 14.5+ 受監管**	如為 true，即會告知停用 Siri 伺服器連線以便進行聽寫。 預設：false
	允許未配對的外部開機以復原	如為 true，允許未配對的裝置對裝置開機以復原。 預設：false
	強制僅能 Wi-Fi 連線至允許的網路	如為 true，透過配置描述檔限制裝置僅加入 Wi-Fi 網路設定。 預設：false 如果**強制僅能 Wi-Fi 連線至允許的網路**已啟用，且 Wi-Fi 配置未發佈至裝置，Wi-Fi 連線會中斷。
	iOS 15+	
	強制裝置僅翻譯	如為 true，裝置不會連線至 Siri 伺服器進行翻譯。 預設：false
	需要受管理的剪貼板 **iOS 15.2+**	如為 true，複製並貼上對應的 allowOpenFromManagedToUnmanaged 和 allowOpenFromUnmanagedToManaged 限制。 預設：false
	允許郵件隱私權保護	若為 False，則停用裝置上的郵件隱私權保護。 適用於 iOS 15.2 和更新版本。 若已從 Ivanti Neurons for MDM 管理入口網站安裝及啟用「允許郵件隱私權保護」組態，則可在

類別	設定	方法
		裝置上啟用「保護郵件活動」切換，並顯示下列選項: • **隱藏 IP 位址** - 電子郵件傳送者無法將電子郵件連結到您的線上活動或判斷您的位置 • **封鎖所有遠端內容** - 防止電子郵件傳送者看見您的電子郵件活動 預設值：True
	iOS 15.4+ 允許 Apple TV 的自動螢幕保護程式 (tvOS 15.4 及更新版本)	若為 False，則停用 Apple TV 的自動螢幕保護程式。 適用於 tvOS 15.4 和更新版本。 預設值：True
	iOS 16.0 至 26.0	
	允許安裝背景安全性改進	停用回應。 使用者無法安裝背景安全性改進。
	允許移除背景安全性改進	禁止使用者取消回應。 使用者無法移除背景安全性改進。
	執行 iOS 17.0 以上版本的受監管裝置 允許在 Mac 裝置上顯示 iPhone 小組件 **執行 iOS 17.2 以上版本的受監管裝置**	選取此項可允許 iPhone 小組件顯示在 Mac 裝置上，前提是 Mac 裝置對 iCloud 使用兩種裝置都適用的同一 iPhone AppleID。
	允許即時語音信箱	選取此項可在裝置上啟用即時語音信箱。
	抹除時強制保留 ESIM	選取此項後，可在系統因為密碼嘗試失敗次數過多或因為**設定** > **一般** > **重設**中的「抹除所有內容和設定」選項而抹除裝置時保留 eSIM。 若**尋找我的**啟動並因此清除裝置，則系統不會保留 eSIM。
	執行 iOS 17.4 以上版本的受監管裝置 允許 Marketplace 應用程式安裝	選取此項可允許使用者從其他市場下載應用程式。 當此限制設定為 false 時，使用者將無法安裝新的替代市集應用程式以及從這些市集安裝的應用程式。
	允許自動變暗	選取此項可允許在配備 OLED 顯示器的 iPad 上使用自動調暗選項。
	執行 iOS 17.5 以上版本的受監管裝置	
	允許安裝 Web 發佈應用程式 **執行 iOS 18.0 以上版本的受監管裝置**	這項 **allowWebdistributionAppInstallation** 限制設為 false 時，將防止使用者直接從其他新網站安裝應用程式。 僅適用於受監管裝置。

類別	設定	方法
	允許 eSIM 傳出傳輸	選取此項可允許將 eSIM 從設定了限制的裝置傳輸到其他裝置。
	允許 Genmoji	選取此項可允許建立 Genmoji。
	允許 Image Playground	選取此項可允許使用映像生成。
	允許 Image Wand	選取此項可允許使用 Image Wand。
	允許 iPhone 鏡像	選取此項可允許 iPhone 在 macOS 裝置中進行鏡像。
	允許個人化手寫結果	選取此項可允許系統利用使用者的手寫生成文字。
	允許書寫工具	選取此項可啟用 Apple Intelligence 書寫工具。
	允許隱藏應用程式	選取可允許隱藏應用程式。
	允許鎖定應用程式	選取可允許鎖定應用程式。
	執行 iOS 18.1 以上版本的受監管裝置	
	允許通話錄音	選取可允許通話錄音。 預設值：True
	允許郵件摘要	選取可允許手動建立電子郵件訊息摘要。 預設值：True
	允許 RCS 訊息傳送	選取可允許 RCS 訊息傳送。 預設值：True 在 iOS 26 裝置和具有 iPadOS 26 的行動數據 iPad 型號上，RCS 訊息的使用可能會在行動數據計劃與 ICCID 關聯的裝置上受到限制。
	執行 iOS 18.2 以上版本的受監管裝置	
	允許外部情報整合	選取可允許搭配 Siri 使用外部雲端式情報服務。
	允許外部情報整合登入	選取可允許外部情報提供者進入匿名模式。 如果使用者已經登入外部情報提供者，套用此限制將導致他們遭到登出。
	允許修改預設瀏覽器	選取可允許修改預設瀏覽器喜好設定。 Ivanti Neurons for MDM 設定可讓您設定預設網頁瀏覽器。
應用程式	**iOS 所有版本**	在裝置上啟用應用程式存取。
	允許安裝 app	選擇允許使用者安裝來自 Apple App Store 的應用程式。 取消選擇可停用 App Store 並從主畫面移除其圖示。

類別	設定	方法
	允許使用相機	選擇允許使用者操作相機。 取消選擇可停用相機並從主畫面移除其圖示。 在 iOS 26+ 裝置中，如果將應用程式新增到例外清單中，則不會套用「允許相機」限制。
	允許使用 Safari	選擇允許使用 Safari Web 瀏覽器。 取消選擇可停用 Safari 網頁瀏覽器，並從主畫面移除其圖示，以防止使用者開啟 Web Clip。
	啟用自動填入	選擇針對 Safari 中顯示的欄位開啟自動填入功能。
	強制詐騙警告	選擇提示 Safari 以防止使用者造訪識別為詐騙或受威脅的網站。
	啟用 JavaScript	選擇開啟 Safari 的 Javascript 支援。
	封鎖蹦現視窗	選擇封鎖 Safari 的蹦現視窗。
Safari	**僅限受監管 - 版本 26+**	
	允許清除 Safari 歷史記錄	選取此項可允許使用者清除瀏覽歷程記錄。
	允許 Safari 私人瀏覽	選取此項可允許使用私人瀏覽。
	iOS 所有受監管版本	
	允許移除 app	選擇允許使用者移除裝置的 app。
	允許使用 Game Center	選擇允許存取 Game Center。
	允許新增 Game Center 的好友	選擇允許使用者新增好友至 Game Center。
	允許多人遊戲	選擇允許使用者與其他使用者一起參與遊戲。
	允許 iMessage	選擇允許使用 iMessage。 在 iOS 26 裝置和具有 iPadOS 26 的行動數據 iPad 型號上，如果裝置被新增到拒絕清單中，iMessage 的使用可能會受到限制。
	接受 Cookie	選擇「絕不」、「總是」或「來自造訪過的網站」。
	允許 FaceTime	選擇啟用相機時允許使用者執行 FaceTime。 在 iOS 26 裝置和具有 iPadOS 26 的行動數據 iPad 型號上，如果裝置被新增到拒絕清單中，Face Time 的使用可能會受到限制。
	iOS 8+	
	允許受管理的應用程式使用雲端同步	選擇允許受管理的應用程式使用雲端同步。
	允許動作連續	選擇允許在支援 Handoff 的 app 中進行連續動作。
	iOS 8+ 受監管	

類別	設定	方法
	允許使用 Podcast	選擇允許使用 Podcast。
	iOS 9+	
	允許信任新的企業 app 作者	選擇允許使用者存取新的企業 app。
	iOS 9+ 受監管	
	允許 App Store	選擇允許使用者存取 Apple App Store。
	允許自動 app 下載	選擇允許 app 在提示使用者後下載檔案、資料與更新。
	允許新聞 app	選擇允許使用新聞 app。
	iOS 9.3+ 受監管	
	允許 iTunes Radio	選擇允許使用 iTunes Radio。
	允許 Apple Music	選擇允許使用 Apple Music。
	允許列出 App 套件 ID	選擇此選項以僅允許陣列中列出的套件 ID 顯示或可啟動。 加入 com.apple.webapp 值以允許所有 webclip。
	已封鎖 App 套件 ID	選擇此選項以防止陣列中列出的套件 ID 顯示或可啟動。 加入 com.apple.webapp 值以限制所有 webclip。
	iOS 13.0+ 受監管	
	允許使用 iTunes Store	選擇允許使用 iTunes Music Store。 取消選擇可停用 iTunes Music store 並從主畫面移除其圖示。

類別	設定	方法
iCloud	iOS 所有版本	允許存取 iCloud 服務。
	允許備份	選擇允許裝置透過 Apple iCloud 服務備份資料。
	允許文件同步	選擇允許透過 Apple iCloud 服務同步文件。
	允許照片串流	選擇允許透過 Apple iCloud 將照片同步至其他 iOS 裝置。
	允許共享照片串流 (若不允許可能會造成資料遺失)	選擇允許同步共享照片。 取消選取此選項可能導致照片遺失。
	允許 Keychain 同步 **iOS 9+**	選擇允許同步您的 keychain。
	允許 iCloud 照片程式庫 **iOS 15+ 受監管**	選擇允許存取 iCloud 相片資料庫。
	允許 iCloud Private Relay	如為 False，停用 iCloud Private Relay。 預設值：true

類別	設定	方法
安全性和隱私權	**iOS 所有版本**	啟用安全性和隱私權原則。
	允許 over-the-air 憑證更新	選擇允許根認證進行 over-the-air 更新。
	強制限制廣告追蹤	選擇必須使用限制廣告追蹤功能。
	iOS 所有受監管版本	
	允許安裝配置描述檔	選擇允許使用者交替安裝配置描述檔與認證。
	允許助理使用者產生的內容	選擇允許 Siri 從 Web 上查詢使用者產生的內容。
	iOS 8+ 受監管	
	允許使用者清除「重設 UI」中的所有內容和設定	選擇啟用裝置 iOS「重設 UI」中的「清除所有內容和設定」選項。
	允許螢幕時間	選擇允許螢幕時間 (設定 > 螢幕時間)。
	允許診斷資料傳送至 Apple	選擇允許自動提交診斷資料給 Apple。
	允許使用者存取不受信任的 TLS 憑證	選擇允許使用者接受不受信任的 HTTPS 認證。 如果未選擇此選項，裝置就會自動拒絕不受信任的 HTTPS 認證且不會提示裝置使用者。
	強制加密的備份	選擇 iTunes 必須進行加密備份。 由於 SCEP 需求，此為自動選擇的選項。
	強制使用者輸入 iTunes Store 密碼進行所有交易	選擇強制裝置使用者輸入 iTunes 密碼，以進行每項 App Store 的交易。 如果未選擇此選項，裝置使用者就可憑一次驗證就進行多次交易。
	iOS 9+	
	視 AirDrop 為未受管理目的地	選擇允許使用者 AirDrop 檔案共享。 預設：False
	iOS 9+ 受監管	
	允許修改裝置密碼	選擇允許使用者變更裝置密碼。
	iOS 12+	
	允許受管理 app 將聯絡人寫入未受管理的聯絡人帳戶	允許受管理 app 將聯絡人寫入未受管理的聯絡人帳戶。 預設：False
	iOS 12+ 受監管	
	允許自動填入密碼	選擇允許使用者使用 iOS 上的自動填入密碼功能，並在 Safari 或 app 中提示使用已儲存的密碼。
	允許附近裝置共享密碼要求	選擇允許使用的裝置向附近裝置要求提供密碼。
	允許密碼共享	選擇允許使用者透過 Airdrop 密碼功能。

類別	設定	方法
	允許未受管理 app 從受管理的聯絡人帳戶讀取聯絡人 iOS 18.3	選擇允許未受管理 app 從受管理的聯絡人帳戶讀取聯絡人。 預設：False
	允許外部情報工作區 ID	輸入允許的外部情報工作區 ID。
	允許筆記轉錄檔摘要	選取此選項可從轉錄建立摘要。 預設值：True
	允許視覺智慧摘要	選取此選項可使用影像或視覺內容從 Apple 的 Visual Intelligence 建立摘要。 預設值：True

類別	設定	方法
內容評等	允許播放完整音樂、Podcast 與 iTunes U media (僅限受監管 iOS 13+ 和 tvOS 11.3 以及更新版本) 評等區域	控制 app 與媒體的存取。 透過 iTunes Store 販售時，內容提供者會將完整內容進行標示，例如記錄標籤等。 從下拉清單中選擇區域，即可針對應用程式、電視劇和電影的評等選項變更相關區域。
	電影	選擇裝置上儲存之電影的評等限制： • 不允許電影 • G • PG • PG-13 • R • NC-17 • 允許所有電影
	電視劇 App	選擇裝置上儲存之電視劇的評等限制： • 不允許電視劇 • TV-Y • TV-Y7 • TV-G • TV-PG • TV-14 • TV-MA • 允許所有電視劇 選擇裝置上儲存之應用程式的評等限制： • 不允許 App • 4+ • 9+ • 12+ • 17+ • 允許所有 App

如需更多資訊，請參閱**如何建立配置**

10.10.4.27. 會議室顯示器

適用於：tvOS 10.2 及支援的更新版本。

此配置將會在 Apple TV 上啟動會議室顯示器模式。 會議室顯示器模式會將 Apple TV 鎖定在該模式，以防止其他使用類型。

從 tvOS 10.2 開始，您可將受監管的 Apple TV 裝置設為會議室顯示器模式。 會議室顯示器會將範圍內的 Apple TV 裝置鎖在黑色桌布畫面，並下載預設的螢幕保護程式，除非在 Apple TV 裝置設定中手動定義背景影像和螢幕保護程式。 此模式也會在會議室顯示器配置中設定的訊息。

當裝置在此模式中，可自動部署會議室顯示器配置並安裝 app。 設為會議室顯示器模式的裝置重新開機後，將會自動繼續鎖定畫面而不會先顯示首頁畫面。

> 如果 Apple TV 裝置在單一 App 模式，或如果在單一 App 模式之下部署會議室顯示器，會議室顯示器將會取代單一 App 模式。 此外，如果 Apple TV 裝置已透過乙太網路連線至網路，會議室顯示器將不會自動顯示要加入的 Wi-Fi 網路以分享 AirPlay。 可使用會議室顯示器配置的「自訂訊息」欄位，在螢幕上顯示此指示說明。

建立會議室顯示器配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入 **conference**，然後按一下**會議室顯示器**配置。
4. 輸入配置的名稱和描述。
5. 指定**自訂訊息**。 在會議室顯示器模式中，螢幕上會顯示此自訂訊息。
6. 按**下一步**，確認發佈設定。
7. 按一下**完成**。

如需更多資訊，請參閱如何建立配置。

10.10.4.28. 鍵盤設定

使用**鍵盤設定**在受監管的裝置上設定鍵盤設定。 此聲明可協助管理員套用一致的原則型控制項，以管理鍵盤行為、輸入選項和相關的使用者體驗設定。

適用於：

- 受監管的 iOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監管的 macOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取**鍵盤設定**組態。
3. 依下表設定各項**鍵盤設定**:

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
允許自動更正	選取核取方塊以啟用自動更正。 切換**推播至裝置**按鈕，在受監管的裝置上啟用自動更正。 此設定不適用於 macOS 裝置。
允許定義查詢	選取核取方塊以啟用定義查詢。 切換**推播至裝置**按鈕，在受監管裝置上啟用定義查詢。
允許聽寫	選取核取方塊以啟用聽寫。 切換**推播至裝置**按鈕，在受監管的裝置上啟用聽寫。
允許數學鍵盤建議	選取核取方塊以啟用數學鍵盤建議。 切換**推播至裝置**按鈕，在受監管的裝置上啟用數學鍵盤建議。
允許預測文字	選取核取方塊以啟用預測文字。 切換**推播至裝置**按鈕，在受監管的裝置上啟用預測文字。 此設定不適用於 macOS 裝置。
允許滑動輸入	選取核取方塊以啟用「允許滑動輸入」。 切換**推播至裝置**按鈕，以在受監管的裝置上啟用允許滑動輸入。 此設定不適用於 macOS 裝置。
允許拼字檢查	選取核取方塊以啟用拼字檢查。 切換**推播至裝置**按鈕，在受監管的裝置上啟用拼字檢查。 此設定不適用於 macOS 裝置。
允許文字取代	選取核取方塊以啟用文字取代。 切換**推播至裝置**按鈕，在受監管的裝置上啟用文字取代。 此設定不適用於 macOS 裝置。

4. 按**下一步**，確認發佈設定。
5. 選取其中一個發佈選項以設定**鍵盤設定**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
6. 按一下**完成**。

10.10.4.29. 鎖定與單一應用：Android 裝置管理模式

鎖定與 Kiosk: Android 裝置管理員模式組態會停用 Android 裝置的特定功能，並建立一份應用程式允許清單，以供使用者在 Kiosk 模式中使用。

> 針對使用 Android 8 及更新版本的裝置，其已不再支援且已棄用 Android 裝置管理員模式組態。 建議在 Android 8 及更新版本上將 Android Enterprise 鎖定作為 Kiosk 鎖定使用。

您可以限制在 Android 裝置處於單一應用模式時選擇修改設定或 app。

- 在「建立鎖定與單一應用：Android 裝置管理」配置頁面中，新增 app 並選擇設定。
- 在單一應用模式中，即可選擇用設定圖示變更設定。
- 選取 app 但不選擇任何設定配置選項，則在單一應用模式中將會顯示設定圖示。
- 如果您選擇不要在配置中維入任何 app，則將會顯示設定圖示。

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
鎖定設定：停用所有 Android 裝置的功能。	
停用 Wi-Fi	選擇關閉存取無線 LAN。
停用相機	選擇關閉存取相機。
停用 Bluetooth	選擇關閉 Bluetooth 功能。 請小心使用此選項。 由於免持 Bluetooth 存取已停用，因此 Ivanti 建議您停用音訊。 因為駕駛使用日益普遍，因此須遵循免持使用裝置的法規需求。
單一應用模式設定：讓裝置在單一應用模式中使用，並只提供部分特定 App 的作業。 單一應用模式設定不會套用到執行 Android 8.0 及更新版本的裝置。 對於這類裝置，裝置詳細資料頁面中的單一應用狀態會回報為 UNSUPPORTED_ON_DEVICE。	
啟用單一應用模式	選擇設定 Android 裝置上的單一應用模式。
停用快速設定	選擇停用單一應用模式中的快速設定。
允許使用者存取 WiFi 設定	選擇允許使用者變更 Wi-Fi 設定與存取偏好的無線網路。
允許使用者存取 Bluetooth 設定	選擇允許使用者變更 Bluetooth 設定並配對其他 Bluetooth 裝置。
允許使用者存取位置設定	選擇允許使用者存取位置設定。
允許使用者延遲應用程式更新	選擇允許使用者延遲應用程式更新。
單一應用退出 PIN 碼	輸入一般使用者必須輸入才能退出單一應用模式的四位數密碼。
建立 app 允許清單：將 app 新增至允許的 app 清單，以供使用者在單一應用模式中使用這些 app。 拖放 app，並依照單一應用模式啟動程式中要顯示的順序加以排列。 將應用程式新增至允許的 app 清單並不會在裝置上安裝該 app。 因此，請務必將每項 app 發佈給 App Catalog 中的適當使用者和使用者群組。	
內建 App	按一下「+新增」，納入單一應用模式允許之 app 群組中提列的原生 app。 如果您停用上述「鎖定」設定中的「Dialer」或「相機」，就無法將其新增至「允許的 App」清單中。

設定	方法
「App Catalog「	按一下「+新增」，以將 App Catalog 提列的 app 納入單一應用模式允許的 app 群組中。
其他 App	按一下「+新增」，以納入 Google Play 商店不提供之 App 的套件名稱。
單一應用模式允許的 App	按一下 X，即可從單一應用模式允許之 app 群組中移除 app。拖曳以變更 app 在單一應用裝置上的顯示順序。

> 若是 Samsung 裝置搭配 Knox Standard 4.0 或更新版本，在單一應用模式中會自動鎖定多重使用者功能。

對於非 Samsung 裝置，在 Android 8.0 或更新版本上不支援單一應用模式。 Ivanti 建議在 Android 8.0 或更新版本上使用 Android Enterprise 來取代單一應用模式。

相關主題：

- 設定 Android 的單一應用模式
- 如何建立配置

10.10.4.30. 設定 Android 的單一應用模式

本節包含以下各主題：

- 從遠端啟動單一應用模式
- 退出單一應用模式

授權：Silver

Android 裝置的單一應用模式可讓您限制裝置僅使用特定的 app。 您可使用單一應用模式來設定員工的裝置，以讓員工僅使用工作相關的 app。

準備 Android 裝置以用於單一應用模式或裝置擁有者與單一應用模式時，您需要**建立 app 允許清單**，以供使用者在單一應用模式中使用。 若是使用裝置擁有者模式的裝置，您可以新增 App 至允許的 App 清單，方法是在配置 App 時進行拖放，以 App 在單一應用模式啟動程式中應有的出現順序排列它們。 請參閱**鎖定與單一應用配置**以取得更多資訊。

必要條件

在您設定 Android 裝置的單一應用模式之前，請務必先執行下列作業：

- 將 Go 安裝在裝置上。
- 在應用程式目錄中，設定好單一應用配置所需的 app。
- 將應用程式目錄發佈到將以單一應用模式執行的裝置上。

> SonimXP5S 裝置不支援單一應用模式。

- 安裝好單一應用配置所需的 app。
- （選用）設定 **Android 單一應用品牌化**。

> kiosk 模式支援 Android 5.1 和 6.0。 非 Samsung Knox 必須置於裝置擁有者模式，以防止使用不需要的應用程式。

重要事項：有些裝置的功能可能會導致裝置跳出畫面或跳出單一應用模式。 Samsung Galaxy S6 Edge 的「People Edge」功能就是一例。 建議管理員先關閉這類功能後再部署裝置。

程序

1. 前往**配置**。
2. 按一下 **+新增**。
3. 按一下**鎖定與單一應用：Android 裝置管理模式**。
4. 在**建立設定**畫面中，至少完成**單一應用模式設定**區段。
5. 在**發佈**畫面中，選擇要接收此項配置的裝置群組。
6. 按一下**完成**。
7. 若是 Samsung 以外的裝置，請繼續下列步驟：
    1. 前往**裝置** > **裝置**。
    2. 選擇要啟用單一應用模式的裝置。
    3. 選擇**動作強制簽入**。
    4. 在裝置上，點選**單一應用模式**按鈕。

5. 按裝置上的**首頁**按鈕。
6. 如果出現**選擇啟動程式**對話方塊，請點選 **Go 單一應用啟動程式**，並選擇**總是**。 為確保這項功能使用正確的啟動程式，此為必要的步驟。 否則，系統就會提示使用者選擇啟動程式。

從遠端啟動單一應用模式

程序

1. 前往**裝置 > 裝置**。
2. 新增單一應用模式欄位至顯示畫面。
3. 選擇已啟用單一應用模式但目前不在此模式中的裝置。
4. 選擇**動作 > 進入單一應用模式**。

退出單一應用模式

如果您在配置中設定了 PIN 碼，即可退出裝置的單一應用模式。

程序

1. 點選**設定**圖示。
2. 選擇**退出單一應用模式**。
3. 在畫面提示時，點選**單一應用 PIN 碼**欄位。
4. 輸入單一應用 PIN 碼。

您可以透過入口網站，退出特定裝置的單一應用模式：

程序

1. 前往**裝置 > 裝置**。
2. 顯示裝置的詳細資料。
3. 選擇**動作 > 退出單一應用模式**。

您也可以使用下列方法退出單一應用模式：

- 刪除配置
- 停用配置
- 從配置中移除裝置群組

10.10.4.31. 設定 Android 共用裝置單一應用

若是 Task Worker 部署，公司可能會提供針對特定使用者自訂的專用 Android 裝置。 視使用者的描述檔而定，裝置上可能會出現不同的 app 和配置。 例如，擁有技術角色的使用者可能會有 app 集合可供使用，而擁有維護角色的使用者則可能可以存取不同的 app 集合。

Android 共用裝置 Kiosk 模式可作為共用裝置之不同使用者群組的應用程式篩選器。 登入共用裝置單一應用的使用者只能檢視其角色適用的 app。 共用裝置單一應用的主要優點之一是，您可以允許不同的使用者群組從相同裝置存取不同的 app 集合。 當使用者登出 Android 共用裝置 Kiosk 模式時，其應用程式和使用者資料 (包括歷程記錄) 均會被清除，不會對登入裝置的下一個使用者顯示這些內容 (如果已將應用程式標示為重新安裝)。 共同裝置單一應用可用於搭配受管理 Google Play 帳戶使用的 Android 企業。

共同裝置單一應用需要兩種類型的使用者：暫存使用者與共用使用者，以及至少兩個與這些使用者相對應的原則。 暫存使用者用來提示要出現在共用裝置上的登入畫面。 此外，暫存使用者是一種特殊的管理使用者，其可允許其他使用者登入實際的單一應用裝置。 在共用裝置單一應用使用者成功登入後，暫存使用者就會被共用單一應用原則所取代。 單一應用使用者可根據指派給他們的原則，存取在裝置上安裝的 app。 雖然您可以建立多重共用單一應用原則，但在單一應用裝置上一次只有一個單一應用原則會作用。 當單一應用使用者登出共用單一應用，裝置會還原到暫存使用者，以及隨之而來的暫存原則。

暫存使用者只能存取登入頁面。 因此，您需要建立此使用者專用的暫存原則。 相對的，共用裝置單一應用使用者能夠存取您在 app 原則中所定義的 app 集合。 (當然，還需要在共用裝置 kiosk 裝置上安裝許可的應用程式。)共用裝置 kiosk 原則可讓您從以前安裝的所有應用程式中建立許可的應用程式篩選器。 您無法將 app 直接上傳到 Android 共用單一應用原則。 您常會想要為某種共用單一應用使用者或使用者群組 (取決於您的組織) 建立專用的共用單一應用原則。 例如，公司可能會有日班和夜班員工，他們擔任不同角色而且需要存取各自的 app 集合。 在此情況下，您需要建立日班原則和夜班原則。

如需啟用共用裝置單一應用的更多資訊，請參閱**鎖定與單一應用：Android Enterprise**

10.10.4.32. 鎖定與單一應用：Android Enterprise

鎖定與 Kiosk: Android Enterprise 組態會停用 Android Enterprise 裝置的特定功能，並建立一份應用程式允許清單，以供使用者在 Kiosk 模式中使用。

本節包含以下各主題：

- 鎖定設定
- 工作描述檔
- 受工作管理的裝置 (裝置擁有者和單一應用模式設定)
- 搭配工作描述檔的受管理裝置/公司擁有裝置上的工作描述檔鎖定設定

鎖定設定

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
選擇鎖定類型	選擇您要配置的鎖定設定類型： • 工作描述檔 • 受工作管理的裝置 (裝置擁有者和單一應用模式設定) • 搭配工作描述檔的受管理裝置/公司擁有裝置上的工作描述檔鎖定設定 「公司擁有裝置上的工作描述檔鎖定設定」僅適用於 Android 11+ 裝置。 每種配置只允許一種類型。 系統會依據您選擇的類型顯示選項。 如果是受工作管理的裝置 (裝置擁有者) 和「搭配公司擁有裝置上的工作描述檔的受管理裝置」配置已發佈到相同裝置，則「搭配工作描述檔的受管理裝置」將取得優先。

工作描述檔

停用 Android Enterprise 裝置上的特定功能。

設定	方法	適用裝置
停用螢幕擷取	選擇關閉裝置的內建螢幕擷取功能。	• Android 5.0 +
不允許 App 管制	選擇以防止使用者修改「設定」中的應用程式或啟動程式。	• Android 5.0 +
不允許配置認證	選擇以防止使用者配置使用者憑證。	• Android 5.0 +
不允許描述檔間複製貼上	選擇以防止描述檔之間進行資訊的複製/貼上作業。	• Android 5.0 +
不允許修改帳戶	選擇以防止使用者新增或移除帳戶。	• Android 5.0 +
不允許外送 Beam	選擇以防止使用者利用 NFC 來傳輸 app 的資料。	• Android 5.1+
不允許共享位置	選擇以防止使用者允許 app 取得裝置的位置。	• Android 5.0 +
不允許偵錯功能	選擇停用裝置上的偵錯功能。 此選項預設為開啟。	• Android 5.0 +
確認驗證 App	選擇允許使用裝置上的應用程式驗證功能。 此選項預設為開啟。 如果關閉此選項，裝置就會回到預設的行為，而且可能每台裝置的行為都不同。	• Android 5.0 +
停用裝置上的未知來源	選擇以避免裝置從不明來源安裝 app。 此設定是否會在裝置上生效，取決於預期的 Google Play 更新是否啟用此功能。	• Android 5.0 +
限制輸入法	選擇要透過**套件名稱**欄位指定允許的套件名稱清單，藉此限制列入允許清單的 IME 套件名稱。 裝置將可使用列入允許清單套件的輸入法和預設系統輸入法。 使用者可在預設系統輸入法和列入允許清單套件的輸入法之間切換。 針對 Android 10+，允許清單僅適用於工作描述檔端的 IME app。 針對舊版 Android，允許清單適用於所有 IME app 裝置 (工作描述檔內部和外部)。	• Android 5.0 +
限制存取服務	選擇要透過**套件名稱**欄位指定允許的套件名稱清單，藉此限制工作 app 的協助工具服務。 如果沒有允許的套件，則僅允許系統協助工具服務。	• Android 5.0 +
在工作描述檔內停用未知來源	選擇以不允許從工作描述檔內的未知來源下載。	• Android 5.0 +
啟用/停用系統 App	選擇啟用和停用要部署的系統應用程式 (方法為透過**系統 App 套件 名稱**欄位，分別指定兩份套件名稱清單)。 如果系統應用程式未發佈至 Google Play，您可以使用此功能來管理這些系統應用程式的存取權。 不支援將 app 新增至 App Catalog 和系統 app 清單。	• Android 5.0 +
停用來電者 ID	設定是否要在接聽來電的裝置上顯示工作描述檔中的來電者 ID 資訊。	• Android

設定	方法	適用裝置
		6.0+
停用透過 Bluetooth 共享聯絡人	選擇不允許裝置透過 Bluetooth 與其他裝置共享聯絡人。	• Android 6.0+
停用透過搜尋共享聯絡人	選擇不允許使用者透過私人電話撥號程式搜尋工作聯絡人。	• Android 7.0 +
不允許自動填寫	選擇不允許自動填寫	• Android 8.0+
個人描述檔中不允許工作 app 通知	選擇限制工作描述檔通知。	• Android 8.0+
不允許列印	選擇限制所有 app 的列印。	• Android 9.0 +
不允許描述檔內的共用	選擇以防止使用者在裝置上的工作描述檔中共用個人描述檔的資料。	• Android 9.0 +
允許存取工作描述檔行事曆	選擇下列任一選項以允許所有 app，或在個人端選擇一組 app 以存取工作描述檔中包含的行事曆資訊： • **個人描述檔中的所有 App** - 允許所有 app 存取工作描述檔中包含的行事曆資訊 • **僅個人描述檔中的以下 App** - 在下面的文字欄位中，輸入 app 的 ID，並以逗號分隔。 只有在個人端選擇的這些 app 才能存取工作描述檔中包含的行事曆資訊。 個人端的 app 應實作特定 API，才能存取共用行事曆。	• Android 10.0+
啟用 App 的描述檔間允許清單	選擇勾選框讓使用者將工作描述檔內的特定 app 資訊分享至裝置的個人端。 在**允許清單 App** 欄位中，輸入要列入允許清單的 app 之封裝 ID，以逗號分隔。 預設會停用此選項。	• Android 11.0 +
啟用 5G 網路切片	選擇此項可在公司所擁有裝置的工作設定檔上提供 5G 網路分段選項。 預設會停用此選項。	• Android 12.0+
不允許分享管理員設定的 Wi-Fi	選取此選項可防止使用者分享管理員設定的 Wi-Fi 組態。	• Android 13.0+
停用 AI 助理	選取以禁止使用者使用「AI 助理」功能。 預設會停用此選項。	• Android 15.0+

受工作管理的裝置 (裝置擁有者和單一應用模式設定)

停用 Android 5.0+ 受工作管理的裝置 (裝置擁有者) 上的特定功能。

設定	描述
停用 Wi-Fi	選擇關閉存取無線 LAN。
停用 Wi-Fi 設定	選擇關閉存取無線設定。
停用相機	選擇關閉存取相機。
停用 Bluetooth (Android 8.0+)	選擇關閉 Bluetooth 功能。 請小心使用此選項。 由於免持 Bluetooth 存取已停用，因此 Ivanti 建議您停用音訊。 因為駕駛使用日益普遍，因此須遵循免持使用裝置的法規需求。
不允許 Bluetooth 設定 (Android 8.0+)	選擇關閉存取 Bluetooth 設定。
停用螢幕擷取	選擇關閉裝置的內建螢幕擷取功能。
停用網路重設	選取此項可防止重設網路。 (適用於 Android 7.0+ 裝置，「公司擁有裝置上的工作設定檔」模式不支援)。
總音量靜音	選擇總音量靜音。
不允許 App 管制	選擇以防止使用者修改「設定」中的應用程式或啟動程式。
不允許憑證	選擇以防止使用者配置使用者憑證。
不允許緊急廣播	選擇以防止緊急廣播。
不允許行動網路	選擇以關閉存取行動網路。 若停用 Wi-Fi，則無法停用此項功能。
不允許網際網路共用	選擇關閉網際網路共享選項，以防止其他裝置使用某台裝置的網際網路連線來存取網路網路。
不允許 VPN	選擇關閉 VPN 連線。
不允許原廠重設	選擇以防止使用者將裝置還原為原廠預設值。
啟用原廠重設保護	選擇以允許使用者將裝置還原為原廠預設值。 您可選擇性指定獲得授權的 Google 帳戶 ID (整數值) 清單，以便在原廠重設或將游標移到「說明」圖示以檢視擷取已授權帳戶 ID 的說明之後設置裝置。
不允許修改帳戶	選擇以防止使用者新增或移除帳戶。
不允許 NFC (外送 Beam)	選擇以防止使用者利用 NFC 來傳輸 app 的資料。
不允許撥出電話	選取以防止使用者撥出電話。
不允許安全開機 (Android 6.0+)	選擇以防止使用者將裝置重新開機進入安全開機模式。
不允許共享位置	選擇以防止使用者允許 app 取得裝置的位置。
不允許偵錯功能	選擇停用裝置上的偵錯功能。 此選項預設為開啟。

設定	描述
確認驗證 App	選擇允許使用裝置上的應用程式驗證功能。 此選項預設為開啟。 如果關閉此選項，裝置就會回到預設的行為，而且可能每台裝置的行為都不同。
不允許 SMS	選擇以防止使用者收發 SMS 訊息。
不允許取消麥克風靜音	選取以防止使用者取消裝置麥克風靜音。
不允許自動時間	選取以防止使用者啟用自動時間變更。
不允許自動時區	選擇以防止使用者啟用裝置自動隨時區變更而調整時間的功能。
與伺服器（Android 9.0+）同步時間	選擇此選項以允許第一次註冊時 (以及之後每次簽入後每隔 24 小時) 與 Ivanti Neurons for MDM 伺服器同步時間。 此選項僅適用於當**停用自動設定時間**已選取。
設定時區（Android 9.0+）	以 Olson 時區 ID 格式，指定時區字串 (例如，Pacific/Midway)。
停用數據漫遊	選擇在裝置漫遊時關閉資料交換。
停用 Wi-Fi 休眠	選取以在裝置進入睡眠模式時保持開啟 Wi-Fi。
限制輸入法	選擇要透過**套件名稱**欄位指定允許的套件名稱清單，藉此限制列入允許清單的 IME 套件名稱。 裝置將可使用列入允許清單套件的輸入法和預設系統輸入法。 使用者可在預設系統輸入法和列入允許清單套件的輸入法之間切換。 針對 Android 10+，允許清單僅適用於裝置端的 IME app。 針對舊版 Android，允許清單適用於所有 IME app 裝置。
限制存取服務	選擇要透過**套件名稱**欄位指定允許的套件名稱清單，藉此限制工作 app 的協助工具服務。 如果沒有允許的套件，則僅允許系統協助工具服務。
停用 USB 檔案傳送	選擇以停用 USB 檔案傳送。
停用外部媒體	選擇以停用外部媒體。
停用 Keyguard (如果已設定 PIN 碼/密碼，則無效)	選擇以停用 Keyguard。 如果目前已設定密碼、PIN 碼或圖案，則此選項無效。 如果密碼、PIN 或圖案是在 Keyguard 停用後設定的，則將停止停用 Keyguard。
連接電源時保持螢幕開啟。	選擇以在連接電源時保持螢幕開啟。 當裝置連接電源時，螢幕可能會變暗但不會關閉。 此設定只有在密碼配置中未使用自動鎖定或閒置逾時來設定逾時才會生效。
不允許建立視窗	選擇以防止 app 顯示特定類型的重疊視窗，例如警報和快顯通知。
略過第一次使用提示	選擇以啟用 app 的系統建議，以在首次啟動時略過使用者指導教學和其他介紹提示。
不允許裝置上的未知來源	選擇不允許使用者從不明來源安裝 app。
設定鎖定畫面訊息 (Android 7.0+)	選擇將鎖定畫面訊息設為在裝置上顯示。 在文字欄位中輸入鎖定畫面訊息 (不超過 256 個字元)。 啟用此選項，使用者無法在「設定」中設定訊息，而使用者會看到管理員設定的訊息。

設定	描述
	如果管理員在啟用「設定鎖定畫面訊息」後未輸入任何鎖定畫面訊息，使用者無法在「設定」中設定訊息，也不會看到任何訊息。
設定螢幕亮度	選取以設定裝置的螢幕亮度。 • 手動 - 選取以手動輸入數字 (0 到 255) • 適應性 - 選取以允許裝置設定亮度 在設定裝置的螢幕亮度之前，建議您啟用「不允許設定亮度」選項。
設定螢幕逾時	選取以設定螢幕逾時持續時間 (秒)。 在設定裝置的螢幕亮度之前，建議您啟用「不允許設定螢幕逾時」選項。
設定螢幕方向	選取以設定螢幕方向。 您可以在下拉式清單中將螢幕方向設定至 0、90、180 或 270 度。 預設不會選取此選項。 針對 Go 應用程式 89 及後續版本，您必須選取此選項並將值設為 0，以便在 Kiosk 中維持裝置的縱向模式。
啟用/停用系統 App	選擇啟用和停用要部署的系統應用程式 (方法為透過**系統 App 套件名稱**欄位，分別指定兩份套件名稱清單)。 如果系統應用程式未發佈至 Google Play，您可以使用此功能來管理這些系統應用程式的存取權。 不支援將應用程式新增至應用程式目錄和系統應用程式清單。
Android 8.0+	
不允許自動填寫	選擇不允許使用者使用自動填寫服務。
不允許 Bluetooth 分享	選擇不允許使用者共享裝置上的外送 Bluetooth。
關閉備份服務	選擇停用備份服務。
Android 9.0 +	
不允許列印	選擇不允許使用者列印。
不允許飛機模式	選擇在整個裝置上停用飛機模式。
不允許背景顯示	選擇不允許使用背景顯示。
不允許配置亮度	選擇不允許使用者設定亮度。 在選取此選項之前，建議您先定義「設定螢幕亮度模式」。
不允許配置日期時間	選擇不允許日期、時間及時區配置。
不允許配置地點	選擇不允許使用者停用位置提供工具。
不允許配置螢幕超時	選擇不允許使用者變更螢幕關閉逾時。 在選取此選項之前，建議您先定義「設定螢幕逾時」值。
Android 12.0+	
啟用 USB 僅用於充電	選擇即可啟用 USB 連接埠僅用於充電。

設定	描述
Android 13.0+	
設定要求的最低 Wi-Fi 安全性	使用此選項以設定要求的最低 Wi-Fi 安全性: • 未要求最低安全性 – 若未要求最低安全性則選取此選項 • 個人網路型安全性 – 選取此選項以封鎖個人 Wi-Fi 網路，例如 WEP、WPA/WPA2/WPA3 等等。 • 企業 EAP 網路型安全性 – 選取此選項以封鎖 EAP 通訊協定型 Wi-Fi 網路 • 企業 192 網路型安全性 – 選取此選項以封鎖 EAP 公司型 Wi-Fi 網路 不符合最低標準的所有現有裝置將被中斷連線。 裝置詳細資訊將在**一般 > Wi-Fi 安全性層級**下方顯示要求的最低 Wi-Fi 安全性層級 (如果有)。
不允許分享管理員設定的 Wi-Fi	選取以禁止使用者共用管理員設定的 Wi-Fi 組態。
Android 15.0+	
停用 AI 助理	選取以禁止使用者使用「AI 助理」功能。 預設會停用此選項。
單一應用模式設定：單一應用模式會對裝置套用額外的限制，包括透過自訂啟動程式限制 app 的存取權。	
啟用單一應用模式	選擇以在 Android 裝置上設定單一應用模式。 • 當使用者登入共用單一應用模式再登出時，該使用者名稱仍會留在 Go 用戶端以供日後登入使用。 在共用單一應用模式下，Go 用戶端會保留最近 7 個使用者名稱。 • 共用單一應用模式現已支援 IDP 驗證。 因此，若同時配置 Ivanti Neurons for MDM 和 IDP，共用 Kiosk 模式就可與 IDP 驗證一起使用。
啟用鎖定作業模式	選擇以在 Android 裝置上啟用鎖定作業模式。 啟用時，裝置可顯示 Keyguard、狀態列及安全模式。 此選項預設為停用。 當 Android 9 或支援的更新版本已啟用鎖定作業模式時，會顯示以下額外的設定： **設定圖示** - 允許應用程式存取系統功能 (取決於「裝置設定」應用程式)。 允許裝置設定協助在例如從 app 進行 Bluetooth 配對等情況下，避免違反鎖定作業模式。 建議對特定 app 保持啟用此設定。 **系統資訊** - 在狀態列上顯示日期/時間、連線功能、電池和震動模式。 此選項預設為停用。 **Keyguard**（預設為啟用）- 在鎖定作業模式期間啟用 Keyguard。 **全域動作**（預設為啟用）- 當使用者長按電源按鈕時啟用顯示的功能表。 如果此選項停用，使用者可能無法將裝置關機。 **主畫面按鈕** - 啟用主畫面按鈕。 此選項預設為停用。 啟用時，會顯示以下子選項： • **概覽按鈕**（預設為停用）- 在鎖定作業模式期間啟用概覽按鈕和概覽畫面

設定	描述
	• **通知**（預設為停用）- 在鎖定作業模式期間啟用通知。 這包括狀態列上的通知圖示，提醒通知，以及可展開的通知欄。 如果主畫面按鈕選項未啟用，使用者將無法使用多視窗功能。
自動輸入單一應用 (僅在初始設置時)	選擇以在套用配置時自動允許單一應用模式。
在原則更新後維護 Kiosk 模式	選取此選項，可在套用鎖定原則更新後自動讓裝置返回 Kiosk 模式。 此設定有助於維持 Kiosk 不間斷運作，並減少原則變更後的手動介入需求。 之前，更新鎖定原則可能會導致裝置退出 Kiosk 模式。 啟用後，裝置會在處理更新後的原則後自動重新進入 Kiosk 模式。
停用 Android 5 裝置的快速設定	針對 Android 5 裝置，選擇停用單一應用模式中的快速設定。
停用 Android 6+ 和所有 Samsung 裝置的快速設定	針對從第 6 版到支援的最新發行版本之 Android Enterprise 裝置和所有 Samsung 裝置，選擇停用單一應用模式中的快速設定。 停用此設定不會封鎖裝置上的通知圖示和音效。
允許使用者存取 WiFi 設定	選擇允許使用者變更 Wi-Fi 設定與存取偏好的無線網路。
允許使用者存取 Bluetooth 設定	選擇允許使用者變更 Bluetooth 設定並配對其他 Bluetooth 裝置。
允許使用者存取位置設定	選擇允許使用者存取位置設定。
允許使用者延遲應用程式更新	選擇允許使用者延遲應用程式更新。
允許使用者存取日期與時間設定	選擇以允許使用者存取日期與時間設定。
允許使用者存取行動網路設定	選擇以允許使用者存取行動網路設定。
允許使用者選擇語言	選擇以允許使用者存取語言設定。
啟用共用裝置	在共用裝置單一應用中，多位一般使用者可共用裝置。此選項可讓大家共用裝置，同時讓裝置保持處於單一應用模式： • **啟用登入**：此選項適用於單一應用管理使用者。 當裝置設定此選項，系統將會顯示使用者登入畫面，以供一般使用者登入共用裝置單一應用。 唯有在使用者建立為 Android Enterprise 裝置帳戶使用者 (暫存使用者) 時，才會看到「啟用登入」選項。 選擇使用網域替代並輸入適合的網域。 此選項會檢查使用者名稱中有無網域尾碼。 如果缺少網域尾碼，系統自動將網域尾碼加至使用者名稱。 • **啟用登出**：當裝置設定此選項，登入的使用者將有權存取列入允許清單的 app。 此使用者可看見登出選項，但無法退出單一應用。 當使用者登出共用裝置單一應用，另一位使用者即可登入共用裝置單一應用，並檢視管理員所設定的 app。 • App 出現回收圖示，表示在每次登入時強制重新安裝 app。 此選項可用於已在本機快取資料的那些 app。 若管理員提供退出單一應用 PIN 碼，使用者即可退出單一應用模式。

設定	描述
	• **逾時**：指定逾時期間，單位為小時。 例如，當逾時期間設為 2 小時且一般使用者未登出共用裝置單一應用，則 2 小時後將會在裝置上自動執行登出動作。 **逾時**欄位只會在已選擇**啟用登出**選項時顯示，且為選填欄位。 您也可以按一下裝置詳細資料頁面中的**登出 Android enterprise 單一應用**選項，藉此將一般使用者登出共用單一應用模式。
允許 FIDO 驗證 (裝置上需要 Google Chrome 應用程式)	選取此選項，在使用共用 Kiosk 時對使用者使用 FIDO 驗證。 允許使用者使用 FIDO 金鑰登入裝置。 Google Chrome 是唯一支援的瀏覽器，而且必須在裝置上可用，這樣才能在共用 Kiosk 中使用 FIDO 驗證。
允許使用者配置亮度和自動旋轉	選擇允許使用者設定亮度和自動旋轉。
啟用多重視窗	選擇以允許使用 Samsung 裝置（裝置擁有者單一應用）同時顯示多個 app。 如要在鎖定作業模式中允許多視窗，也應啟用下列鎖定作業模式選項： • **主畫面按鈕** • **概覽按鈕**
啟用閒置保護	選取以啟用 Kiosk 模式中的閒置保護。 如果選取，則預設值為 30 秒，在此之前 Kiosk 畫面將保持活動狀態。 您可以設定 30 到 3600 之間的任意值。
單一應用品牌化	從下拉式清單選擇預設或自訂品牌選項。
單一應用退出 PIN 碼	輸入 6 位數 PIN 碼，使用者必須輸入它才能退出單一應用模式。 此 PIN 碼長度應至少 6 位數，最長 10 位數。 此 PIN 碼適用於單一應用模式下的所有裝置。 之前，單一應用 PIN 碼長度為 4 位數。 從先前版本升級至 Ivanti Neurons for MDM 82 後，使用者仍可繼續使用 4 位數 PIN 碼。 不過，如有任何配置改變，PIN 碼長度必須依新的要求設定（即，最少 6 位數，最多 10 位數）。 Go app 將會保護裝置不受暴力密碼破解攻擊。 如需更多資訊，請參閱適用於 Android 的 Go 說明文件。
啟用單一應用程式啟動器 Kiosk	選取此項以使用 Kiosk 模式將應用程式保留在 GMS 和非 GMS 裝置的前景中。 您需要從應用程式目錄中選取一個應用程式或輸入套件 ID。
允許使用者存取 Ivanti 代理程式設定	選取以在裝置維持**單一應用程式 Kiosk 模式**時存取 **Ivanti Agent** 設定。 在此之前，管理員必須退出 Kiosk 模式才能存取代理程式設定。 啟用設定並發佈至裝置後，使用者可同時按住音量調高和音量調低按鈕，開啟 Ivanti 代理程式設定頁面。 功能僅支援已註冊工作受管理裝置模式的 Android 裝置。
啟用駕駛員安全模式	對於「單一應用模式允許的應用程式」區段中的所有應用程式，選取此選項可啟用「駕駛員安全」圖示 。 如果速度超過限制，按一下「駕駛員安全」圖示以停用應用程式。
建立 app 允許清單：將 app 新增至允許的 app 清單，以供使用者在單一應用模式中使用這些 app。 拖放 app，並依照單一應用模式啟動程式中要顯示的順序加以排列。 將應用程式新增至允許的 app 清單並不會在裝置	

設定	描述
上安裝該 app。 因此，請務必將每項 app 發佈給 App Catalog 中的適當使用者和使用者群組。	
內建 App	按一下「+新增」，納入單一應用模式允許之 app 群組中提列的原生 app。 在「單一應用模式允許的 App」的設定之下，可用選項如下： • **清除 app 使用者資料**：啟用此選項，當使用者登出單一應用時會自動清除所有應用程式資料，不會顯示任何提示。 在單一應用模式設定中選擇啟用共用裝置，可讓此選項在多個應用程式中都可使用。 ◦ 即使用已啟用清除 app 使用者資料並將 Google Chrome 和 webview 套件加入 app 允許清單，仍不會清除它們的 app 資料。 這是因為如果清除這 2 個套件的 app 資料，單一應用可能會當機。 ◦ 不會針對沒有 app 啟動程式的系統 app 清除 app 資料（內部和外部單一應用皆然）。 • **隱藏**：啟用此選項可讓其他 app 存取此應用程式，但是在單一應用啟動程式中不會顯示它。 如果您停用上述「鎖定」設定中的「Dialer」或「相機」，就無法將其新增至「允許的 App」清單中。
「App Catalog「	按一下「+新增」，以將 App Catalog 提列的 app 納入單一應用模式允許的 app 群組中。
其他 App	按一下「+新增」，以納入 Google Play 商店不提供之 App 的套件名稱。 針對 Samsung 裝置，管理員應將下列撥號程式/系統套件列入允許清單，讓它們在單一應用模式下正常運作，在單一應用模式下啟用撥號程式功能。 • 通話 - com.samsung.android.incallui • Phone – com.samsung.android.dialer（應列入允許清單，管理員應對此套件選擇隱藏選項，以避免使用者遇到兩個撥號程式選項的問題） • 通話 - com.sec.phone • 通話設定 - com.samsung.android.app.telephonyui • 輔助撥號 - com.sec.providers.assisteddialing • Call Log Backup/Restore – com.android.calllogbackup • 撥號程式存放區 - com.android.providers.telephony • 電話 - com.android.server.telecom • 電話 - com.android.phone • 智慧通話 - com.samsung.android.smartcallprovider • Wi-Fi Calling – com.sec.unifiedwfc

設定	描述
單一應用模式允許的 App	按一下 X，即可從單一應用模式允許的 app 群組中移除 app。 拖曳以變更 app 在單一應用裝置上的顯示順序。 **新增資料夾** - 您可以使用此選項在此區段下建立資料夾，並將一個或多個應用程式移動到此資料夾。 您最多可以建立兩個級別的資料夾。 已複製到一個資料夾的應用程式無法再複製到另一個資料夾。 一個資料夾中僅支援 25 個應用程式。
建立 app 允許清單：將 app 新增至允許的 app 清單，以供使用者在單一應用模式中使用這些 app。 拖放 app，並依照單一應用模式啟動程式中要顯示的順序加以排列。 將應用程式新增至允許的 app 清單並不會在裝置上安裝該 app。 因此，請務必將每項 app 發佈給 App Catalog 中的適當使用者和使用者群組。 內建 App	按一下「+新增」，納入單一應用模式允許之 app 群組中提列的原生 app。 在「單一應用模式允許的 App」的設定之下，可用選項如下： • **清除 app 使用者資料**：啟用此選項，當使用者登出單一應用時會自動清除所有應用程式資料，不會顯示任何提示。 在單一應用模式設定中選擇啟用共用裝置，可讓此選項在多個應用程式中都可使用。 ◦ 即使用已啟用清除 app 使用者資料並將 Google Chrome 和 webview 套件加入 app 允許清單，仍不會清除它們的 app 資料。 這是因為如果清除這 2 個套件的 app 資料，單一應用可能會當機。 ◦ 不會針對沒有 app 啟動程式的系統 app 清除 app 資料（內部和外部單一應用皆然）。 • **隱藏**：啟用此選項可讓其他 app 存取此應用程式，但是在單一應用啟動程式中不會顯示它。 如果您停用上述「鎖定」設定中的「Dialer」或「相機」，就無法將其新增至「允許的 App」清單中。
「App Catalog「	按一下「+新增」，以將 App Catalog 提列的 app 納入單一應用模式允許的 app 群組中。
其他 App	按一下「+新增」，以納入 Google Play 商店不提供之 App 的套件名稱。 針對 Samsung 裝置，管理員應將下列撥號程式/系統套件列入允許清單，讓它們在單一應用模式下正常運作，在單一應用模式下啟用撥號程式功能。 • 通話 - com.samsung.android.incallui • Phone – com.samsung.android.dialer（應列入允許清單，管理員應對此套件選擇隱藏選項，以避免使用者遇到兩個撥號程式選項的問題） • 通話 - com.sec.phone • 通話設定 - com.samsung.android.app.telephonyui • 輔助撥號 - com.sec.providers.assisteddialing • Call Log Backup/Restore – com.android.calllogbackup

設定	描述
	• 撥號程式存放區 - com.android.providers.telephony • 電話 - com.android.server.telecom • 電話 - com.android.phone • 智慧通話 - com.samsung.android.smartcallprovider • Wi-Fi Calling – com.sec.unifiedwfc
單一應用模式允許的 App	按一下 X，即可從單一應用模式允許的 app 群組中移除 app。 拖曳以變更 app 在單一應用裝置上的顯示順序。 **新增資料夾** - 您可以使用此選項在此區段下建立資料夾，並將一個或多個應用程式移動到此資料夾。 您最多可以建立兩個級別的資料夾。 已複製到一個資料夾的應用程式無法再複製到另一個資料夾。 一個資料夾中僅支援 25 個應用程式。
啟用單一應用程式啟動器 Kiosk	選取此項以使用 Kiosk 模式將應用程式保留在 GMS 和非 GMS 裝置的前景中。 您需要從應用程式目錄中選取一個應用程式或輸入套件 ID。
建立 app 允許清單：將 app 新增至允許的 app 清單，以供使用者在單一應用模式中使用這些 app。 拖放 app，並依照單一應用模式啟動程式中要顯示的順序加以排列。 將應用程式新增至允許的 app 清單並不會在裝置上安裝該 app。 因此，請務必將每項 app 發佈給 App Catalog 中的適當使用者和使用者群組。 內建 App	按一下「+新增」，納入單一應用模式允許之 app 群組中提列的原生 app。 在「單一應用模式允許的 App」的設定之下，可用選項如下： • **清除 app 使用者資料**：啟用此選項，當使用者登出單一應用時會自動清除所有應用程式資料，不會顯示任何提示。 在單一應用模式設定中選擇啟用共用裝置，可讓此選項在多個應用程式中都可使用。 ◦ 即使用已啟用清除 app 使用者資料並將 Google Chrome 和 webview 套件加入 app 允許清單，仍不會清除它們的 app 資料。 這是因為如果清除這 2 個套件的 app 資料，單一應用可能會當機。 ◦ 不會針對沒有 app 啟動程式的系統 app 清除 app 資料（內部和外部單一應用皆然）。 • **隱藏**：啟用此選項可讓其他 app 存取此應用程式，但是在單一應用啟動程式中不會顯示它。 如果您停用上述「鎖定」設定中的「Dialer」或「相機」，就無法將其新增至「允許的 App」清單中。
「App Catalog「	按一下「+新增」，以將 App Catalog 提列的 app 納入單一應用模式允許的 app 群組中。
其他 App	按一下「+新增」，以納入 Google Play 商店不提供之 App 的套件名稱。 針對 Samsung 裝置，管理員應將下列撥號程式/系統套件列入允許清單，讓它們在單一應用模式下正常運作，在單一應用模式下啟用撥號程式功能。

設定	描述
	• 通話 - com.samsung.android.incallui • Phone – com.samsung.android.dialer（應列入允許清單，管理員應對此套件選擇隱藏選項，以避免使用者遇到兩個撥號程式選項的問題） • 通話 - com.sec.phone • 通話設定 - com.samsung.android.app.telephonyui • 輔助撥號 - com.sec.providers.assisteddialing • Call Log Backup/Restore – com.android.calllogbackup • 撥號程式存放區 - com.android.providers.telephony • 電話 - com.android.server.telecom • 電話 - com.android.phone • 智慧通話 - com.samsung.android.smartcallprovider • Wi-Fi Calling – com.sec.unifiedwfc
單一應用模式允許的 App	按一下 X，即可從單一應用模式允許的 app 群組中移除 app。 拖曳以變更 app 在單一應用裝置上的顯示順序。 **新增資料夾** - 您可以使用此選項在此區段下建立資料夾，並將一個或多個應用程式移動到此資料夾。 您最多可以建立兩個級別的資料夾。 已複製到一個資料夾的應用程式無法再複製到另一個資料夾。 一個資料夾中僅支援 25 個應用程式。
啟用單一應用程式啟動器 Kiosk **建立 app 允許清單**：將 app 新增至允許的 app 清單，以供使用者在單一應用模式中使用這些 app。 拖放 app，並依照單一應用模式啟動程式中要顯示的順序加以排列。 將應用程式新增至允許的 app 清單並不會在裝置上安裝該 app。 因此，請務必將每項 app 發佈給 App Catalog 中的適當使用者和使用者群組。 內建 App	選取此項以使用 Kiosk 模式將應用程式保留在 GMS 和非 GMS 裝置的前景中。 您需要從應用程式目錄中選取一個應用程式或輸入套件 ID。 按一下「+新增」，納入單一應用模式允許之 app 群組中提列的原生 app。 在「單一應用模式允許的 App」的設定之下，可用選項如下： • **清除 app 使用者資料**：啟用此選項，當使用者登出單一應用時會自動清除所有應用程式資料，不會顯示任何提示。 在單一應用模式設定中選擇啟用共用裝置，可讓此選項在多個應用程式中都可使用。 ◦ 即使用已啟用清除 app 使用者資料並將 Google Chrome 和 webview 套件加入 app 允許清單，仍不會清除它們的 app 資料。 這是因為如果清除這 2 個套件的 app 資料，單一應用可能會當機。 ◦ 不會針對沒有 app 啟動程式的系統 app 清除 app 資料（內部和外部單一應用皆然）。 • **隱藏**：啟用此選項可讓其他 app 存取此應用程式，但是在單一應用啟動程式中不會顯示它。

設定	描述
	如果您停用上述「鎖定」設定中的「Dialer」或「相機」，就無法將其新增至「允許的 App」清單中。
「App Catalog「	按一下「+新增」，以將 App Catalog 提列的 app 納入單一應用模式允許的 app 群組中。
其他 App	按一下「+新增」，以納入 Google Play 商店不提供之 App 的套件名稱。 針對 Samsung 裝置，管理員應將下列撥號程式/系統套件列入允許清單，讓它們在單一應用模式下正常運作，在單一應用模式下啟用撥號程式功能。 • 通話 - com.samsung.android.incallui • Phone – com.samsung.android.dialer（應列入允許清單，管理員應對此套件選擇隱藏選項，以避免使用者遇到兩個撥號程式選項的問題） • 通話 - com.sec.phone • 通話設定 - com.samsung.android.app.telephonyui • 輔助撥號 - com.sec.providers.assisteddialing • Call Log Backup/Restore – com.android.calllogbackup • 撥號程式存放區 - com.android.providers.telephony • 電話 - com.android.server.telecom • 電話 - com.android.phone • 智慧通話 - com.samsung.android.smartcallprovider • Wi-Fi Calling – com.sec.unifiedwfc
單一應用模式允許的 App	按一下 X，即可從單一應用模式允許的 app 群組中移除 app。 拖曳以變更 app 在單一應用裝置上的顯示順序。 **新增資料夾** - 您可以使用此選項在此區段下建立資料夾，並將一個或多個應用程式移動到此資料夾。 您最多可以建立兩個級別的資料夾。 已複製到一個資料夾的應用程式無法再複製到另一個資料夾。 一個資料夾中僅支援 25 個應用程式。

若是 Samsung 裝置搭配 Knox Standard 4.0 或更新版本，在單一應用模式中會自動鎖定多重使用者功能。

具有工作設定檔的受管理裝置

在搭配工作描述檔的受管理裝置上停用 Android 8.0+ 的特定功能。

可以針對公司擁有裝置上的工作描述檔停用特定功能 (適用於 Android 11+ 裝置)。

設定	描述
受管理裝置鎖定設定	
停用 Wi-Fi	選擇以關閉無線 LAN 存取。(不適用於 Android 11+ 裝置)
停用 Wi-Fi 設定	選擇關閉存取無線設定。
停用相機	選擇關閉存取相機。
停用 Bluetooth	選擇關閉 Bluetooth 功能。 請小心使用此選項。 由於免持 Bluetooth 存取已停用，因此 Ivanti 建議您停用音訊。 因為駕駛使用日益普遍，因此須遵循免持使用裝置的法規需求。
不允許 Bluetooth 設定	選擇關閉存取 Bluetooth 設定。
停用網路重設	選取此項可防止重設網路 (適用於 Android 7.0 及以上版本的裝置)。
總音量靜音	選擇總音量靜音。 (不適用於 Android 11+ 裝置)
不允許緊急廣播	選擇以防止緊急廣播。
不允許行動網路	選擇以關閉存取行動網路。 若停用 Wi-Fi，則無法停用此項功能。
不允許網際網路共用	選擇關閉網際網路共享選項，以防止其他裝置使用某台裝置的網際網路連線來存取網路網路。
不允許 VPN	選擇關閉 VPN 連線。 (不適用於 Android 11+ 裝置)
停用原廠重設	選擇以防止使用者將裝置還原為原廠預設值。 (不適用於 Android 11+ 裝置)
啟用原廠重設保護	選擇以允許使用者將裝置還原為原廠預設值。 您可選擇性指定獲得授權的 Google 帳戶 ID (整數值) 清單，以便在原廠重設或將游標移到「說明」圖示以檢視擷取已授權帳戶 ID 的說明之後設置裝置。
不允許撥出電話	選取以防止使用者撥出電話。
不允許安全開機 (Android 6.0+)	選擇以防止使用者將裝置重新開機進入安全開機模式。
不允許偵錯功能	選擇停用裝置上的偵錯功能。 此選項預設為開啟。
確認驗證 App	選擇允許使用裝置上的應用程式驗證功能。 此選項預設為開啟。 如果關閉此選項，裝置就會回到預設的行為，而且可能每台裝置的行為都不同。
不允許 SMS	選擇以防止使用者收發 SMS 訊息。
不允許取消麥克風靜音	選取以防止使用者取消裝置麥克風靜音。
不允許自動時間	選取以防止使用者啟用自動時間變更。
不允許自動時區	選擇以防止使用者啟用裝置自動隨時區變更而調整時間的功能。
停用數據漫遊	選擇在裝置漫遊時關閉資料交換。

設定	描述
與伺服器（Android 9.0+）同步時間	選擇此選項以允許第一次註冊時 (以及之後每次簽入後每隔 24 小時) 與 Ivanti Neurons for MDM 伺服器同步時間。 此選項僅適用於當**停用自動設定時間**已選取。
設定時區（Android 9.0+）	以 Olson 時區 ID 格式，指定時區字串 (例如，Pacific/Midway)。
停用 Wi-Fi 休眠	選取以在裝置進入睡眠模式時保持開啟 Wi-Fi。 (不適用於 Android 11+ 裝置)
限制輸入法	選擇以透過**套件名稱**欄位指定允許的套件名稱清單，藉此限制工作應用程式的輸入法。(不適用於 Android 11+ 裝置) 裝置將可使用列入允許清單套件的輸入法和預設系統輸入法。 使用者可在預設系統輸入法和列入允許清單套件的輸入法之間切換。 在 Android 10+，輸入方法僅適用於裝置端，否則會限於適用整個裝置。
限制存取服務	選擇要透過**套件名稱**欄位指定允許的套件名稱清單，藉此限制工作 app 的協助工具服務。 如果沒有允許的套件，則僅允許系統協助工具服務。 在 Android 10+，輸入方法僅限於工作 App，否則會限於適用整個裝置。
停用 USB 檔案傳送	選擇以停用 USB 檔案傳送。
停用外部媒體	選擇以停用外部媒體。
不允許裝置上的未知來源	選擇以避免裝置從不明來源安裝 app。 此設定是否會在裝置上生效，取決於預期的 Google Play 更新是否啟用此功能。
設定鎖定畫面訊息 (Android 7.0+)	選擇將鎖定畫面訊息設為在裝置上顯示。 在文字欄位中輸入鎖定畫面訊息 (不超過 256 個字元)。 啟用此選項，使用者無法在「設定」中設定訊息，而使用者會看到管理員設定的訊息。 如果管理員在啟用「設定鎖定畫面訊息」後未輸入任何鎖定畫面訊息，使用者無法在「設定」中設定訊息，也不會看到任何訊息。
設定螢幕亮度	選取以設定裝置的螢幕亮度。 • 手動 - 選取以手動輸入數字 (0 到 255) • 適應性 - 選取以允許裝置設定亮度 在設定裝置的螢幕亮度之前，建議您啟用「不允許設定亮度」選項。 若允許使用者進行變更，則這些設定將會在下次簽入時重設為管理員定義的設定。 針對「公司擁有的裝置上的工作設定檔」模式，在 Android 11 及更新版本的裝置上不支援此設定。
設定螢幕逾時	選取以設定螢幕逾時持續時間 (秒)。 在設定裝置的螢幕亮度之前，建議您啟用「不允許設定螢幕逾時」選項。 若允許使用者進行變更，則這些設定將會在下次簽入時重設為管理員定義的設定。 針對「公司擁有的裝置上的工作設定檔」模式，在 Android 11 及更新版本的裝置上不支援此設定。
設定螢幕方向	選取以設定螢幕方向。 您可以在下拉式清單中將螢幕方向設定至 0、90、180 或 270 度。 針對「公司擁有的裝置上的工作設定檔」模式，在 Android 11 及更新版本的裝置上不支援此設定。
不允許自動填寫 (Android 8.0+)	選擇不允許自動填寫。 (不適用於 Android 11+ 裝置)
不允許 Bluetooth 分享 (Android 8.0+)	選擇不允許使用者共享裝置上的外送 Bluetooth。

設定	描述
停用備份服務 (Android 8.0+)	選擇停用備份服務。 (不適用於 Android 11+ 裝置)
不允許列印 (Android 9.0+)	選擇以限制所有應用程式的列印。(不適用於 Android 11+ 裝置)
不允許飛航模式 (Android 9.0+)	選擇在整個裝置上停用飛機模式。
不允許主動顯示 (Android 9.0+)	選擇不允許為使用者主動顯示。 (不適用於 Android 11+ 裝置)
不允許配置亮度 (Android 9.0+)	選擇以禁止使用者設定亮度 (不適用於 Android 11+ 裝置)。 在選取此選項之前，建議您先定義「設定螢幕亮度模式」。
不允許配置日期時間 (Android 9.0+)	選擇不允許日期、時間及時區配置。
不允許配置地點 (Android 9.0+)	選擇不允許使用者停用位置提供工具。
不允許配置螢幕逾時 (Android 9.0+)	選擇以禁止使用者變更螢幕關閉逾時。 (不適用於 Android 11+ 裝置) 在選取此選項之前，建議您先設定「設定螢幕逾時」值。
不允許系統錯誤對話方塊 (Android 9.0+)	選擇以禁止系統錯誤對話方塊。(不適用於 Android 11+ 裝置)
停用螢幕擷取 (Android 11.0+)	選擇關閉裝置的內建螢幕擷取功能。 選取時，在裝置的個人端會停用螢幕擷取。
Android 12.0+	
啟用 USB 僅用於充電	選擇即可啟用 USB 連接埠僅用於充電。
Android 13.0+	
設定要求的最低 Wi-Fi 安全性	使用此選項以設定要求的最低 Wi-Fi 安全性: • 未要求最低安全性 – 若未要求最低安全性則選取此選項 • 個人網路型安全性 – 選取此選項以封鎖個人 Wi-Fi 網路，例如 WEP、WPA/WPA2/WPA3 等等。 • 企業 EAP 網路型安全性 – 選取此選項以封鎖 EAP 通訊協定型 Wi-Fi 網路 • 企業 192 網路型安全性 – 選取此選項以封鎖 EAP 公司型 Wi-Fi 網路 不符合最低標準的所有現有裝置將被中斷連線。 裝置詳細資訊將在**一般 > Wi-Fi 安全性層級**下方顯示要求的最低 Wi-Fi 安全性層級 (如果有)。
不允許分享管理員設定的 Wi-Fi	選取此選項可防止使用者分享管理員設定的 Wi-Fi 組態。
工作描述檔鎖定設定	
停用螢幕擷取	選擇關閉裝置的內建螢幕擷取功能。

設定	描述
不允許 App 管制	選擇以防止使用者修改「設定」中的應用程式或啟動程式。
不允許配置認證	選擇以防止使用者配置使用者憑證。
不允許描述檔間複製貼上	選擇以防止描述檔之間進行資訊的複製/貼上作業。
不允許修改帳戶	選擇以防止使用者新增或移除帳戶。
不允許 NFC (外送 Beam) (Android 5.1 +)	選擇以防止使用者利用 NFC 來傳輸 app 的資料。
不允許共享位置	選擇以防止網站和 app 提示裝置使用者共用裝置位置。
不允許偵錯功能	選擇停用裝置上的偵錯功能。 此選項預設為開啟。
確認驗證 App	選擇允許使用裝置上的應用程式驗證功能。 此選項預設為開啟。 如果關閉此選項，裝置就會回到預設的行為，而且可能每台裝置的行為都不同。
在工作描述檔內停用未知來源	選擇以不允許從工作描述檔內的未知來源下載。
啟用/停用系統 App	選擇啟用和停用要部署的系統應用程式 (方法為透過**系統 App 套件 名稱**欄位，分別指定兩份套件名稱清單)。 如果系統應用程式未發佈至 Google Play，您可以使用此功能來管理這些系統應用程式的存取權。 不支援將 app 新增至 App Catalog 和系統 app 清單。
停用來電者 ID (Android 6.0 +)	設定是否要在接聽來電的裝置上顯示工作描述檔中的來電者 ID 資訊。
停用透過 Bluetooth 共享聯絡人 (Android 6.0+)	選擇不允許裝置透過 Bluetooth 與其他裝置共享聯絡人。
停用透過搜尋共享聯絡人 (Android 7.0+)	選擇不允許使用者透過私人電話撥號程式搜尋工作聯絡人。
不允許自動填寫 (Android 8.0+)	選擇不允許自動填寫。 (不適用於 Android 11+ 裝置)
不允許在個人描述檔中顯示工作 app 通知 (Android 8.0+)	選擇限制工作描述檔通知。
不允許列印 (Android 9.0+)	選擇限制所有 app 的列印。 (不適用於 Android 11+ 裝置)
不允許描述檔內的共用 (Android 9.0+)	選擇以防止使用者在裝置上的工作描述檔中共用個人描述檔的資料。
限制輸入法 (Android 10.0 +)	選擇要透過**套件名稱**欄位指定允許的套件名稱清單，藉此限制允許清單 IME 套件名稱（不適用於 Android 11+ 裝置）。 裝置將可使用列入允許清單套件的輸入法和預設系統輸入法。 使用者可在預設系統輸入法和列入允許清單套件的輸入法之間切換。

設定	描述
	輸入法將適用於安裝在工作描述檔端的 IME app。 即使安裝在裝置端的 app 已列入此鎖定允許清單，app 在工作描述檔端上仍將無法用它們。
允許存取工作描述檔行事曆 (Android 10.0+)	選擇下列任一選項以允許所有 app，或在個人端選擇一組 app 以存取工作描述檔中包含的行事曆資訊： • **個人描述檔中的所有 App** - 允許所有 app 存取工作描述檔中包含的行事曆資訊 • **僅個人描述檔中的以下 App** - 在下面的文字欄位中，輸入 app 的 ID，並以逗號分隔。 只有在個人端選擇的這些 app 才能存取工作描述檔中包含的行事曆資訊。 個人端的 app 應實作特定 API，才能存取共用行事曆。
啟用 App 的描述檔間允許清單 (Android 11.0+)	選擇勾選框讓使用者將工作描述檔內的特定 app 資訊分享至裝置的個人端。 在**允許清單 App** 欄位中，輸入要列入允許清單的 app 之封裝 ID，以逗號分隔。 預設會停用此選項。
啟用最大描述檔逾時 (Android 11.0+)	選擇此選項以設定在 Ivanti Neurons for MDM 暫停裝置上的個人應用程式之前，可關閉工作設定檔的最大時間間隔。 您可將時間設定在 72 到 8760 個小時之間。 8760 個小時為一年。 如果選取此選項，預設值設為 72 個小時。 裝置使用者會看到訊息提示開啟工作描述檔，以啟用暫停的 app。 在公司擁有的裝置上的工作描述檔中，可用 Android 11+ 裝置。 如果設定檔關閉的時間較長，個人應用程式將在裝置上暫止。
啟用 5G 網路分段 (Android 12.0+)	選擇此項可在公司所擁有裝置的工作設定檔上提供 5G 網路分段選項。 預設會停用此選項。
停用 AI 助理 (Android 15.0+)	選取以禁止使用者使用「AI 助理」功能。 預設會停用此選項。

如需更多資訊，請參閱[如何建立配置]

10.10.4.33. 鎖定與單一應用：Samsung Knox Standard

鎖定與單一應用：Samsung Knox Standard 配置會停用 Samsung Knox Standard 裝置的特定功能，並建立一份 app 允許清單，以供使用者在單一應用模式中使用。

> 在使用 Android 9 及更新版本的裝置上，已不再支援且已棄用 Samsung KNOX 標準組態。

鎖定設定

設定

方法

名稱

輸入可識別此配置的名稱。

描述

輸入可說明此配置用途的描述。

Samsung Knox 鎖定設定：僅停用 Samsung Knox 裝置上的特定功能。

停用 Wi-Fi

選擇關閉存取無線 LAN。

停用相機

選擇關閉存取相機。

停用 Bluetooth

選擇關閉 Bluetooth 功能。

僅允許 Bluetooth 音訊

選擇僅開啟 Bluetooth 音訊功能。

停用行動數據

選擇當裝置碰觸到其他裝置時關閉資料交換。

若停用 Wi-Fi，則無法停用此項功能。

停用 GPS

選擇關閉 GPS。

停用 Phone Dialer

選擇關閉電話 app。

停用 SD 卡

選取以關閉 SD 卡存取。

停用 Google 備份

選擇關閉 Google 伺服器的備份。

停用複製/貼上

選擇關閉存取複製/貼上功能。

停用 NFC

選擇當裝置碰觸到其他裝置時關閉 NFC (近場無線通訊) 資料交換。

停用麥克風

選擇關閉存取裝置麥克風的 app。

停用螢幕擷取

選擇關閉裝置的內建螢幕擷取功能。 開啟此選項時，即不允許進行 Go 的螢幕擷取。 這類螢幕擷取作業是不允許的。

停用 Bluetooth 網路共享

選擇關閉 Bluetooth 網路共享，因為使用某裝置的網際網路連線選項即可透過網路網路存取其他裝置。

停用 USB 偵錯

選擇關閉 USB 偵錯功能。

停用 USB 網路共用

選擇關閉 USB 網路共享，因為使用某裝置的網際網路連線選項即可透過網路網路存取其他裝置。

停用 Wi-Fi 網路共用

選擇關閉 Wi-Fi 網路共享，因為使用某裝置的網際網路連線選項即可透過網路網路存取其他裝置。

停用本地瀏覽器

選擇以防止使用者存取 Android 瀏覽器。

停用 YouTube

選擇以防止使用者存取 YouTube。

停用原廠重設

選擇以防止使用者將裝置還原為原廠預設值。

停用 OTA 升級

選擇關閉裝置韌體的 over-the-air 升級。

警告：如果啟用 **OTA 升級**，請不要選擇**停用設定變更**。 如果在啟用 **OTA 升級**時選擇**停用設定變更**，可能會導致裝置無法運作，因為升級一定需要設定變更。

停用語音漫遊

選擇在裝置漫遊時關閉存取語音通話。

停用 USB 媒體播放器

選擇關閉 USB 媒體播放器。

停用 Google Play

選擇關閉存取 Google Play。

停用數據漫遊

選擇在裝置漫遊時關閉資料交換。

停用未知來源

選擇僅安裝來自 Google Play Store 的 app (Go app 除外)。

停用裝置管理權限移除

選擇禁止使用者關閉 Go 的裝置管理權限。

停用設定變更

選擇關閉存取裝置設定 app。

警告：如果啟用 **OTA 升級**，請不要選擇**停用設定變更**。 如果在啟用 **OTA 升級**時選擇**停用設定變更**，可能會導致裝置無法運作，因為升級一定需要設定變更。

單一應用模式設定：單一應用模式會對裝置套用額外的限制，包括透過自訂啟動程式限制 App 的存取權。

適用於最高 8.1 的 Android 版本。 對於 Android 版本 9.0，請使用 Android Enterprise 受管理裝置 kiosk 組態。

啟用單一應用模式

選擇設定 Android 裝置上的**單一應用模式**。

允許使用者存取 WiFi 設定

選擇允許使用者變更 Wi-Fi 設定與存取偏好的無線網路。

允許使用者存取 Bluetooth 設定

選擇允許使用者變更 Bluetooth 設定並配對其他 Bluetooth 裝置。

允許使用者延遲應用程式更新

選擇允許使用者延遲應用程式更新。

GPS 位置設定

選擇以下 GPS 位置設定之一：

- 停用位置
- 啟用位置
- 允許使用者選擇

單一應用退出 PIN 碼

輸入一般使用者必須輸入才能退出單一應用模式的四位數密碼。

建立 app 允許清單：將 app 新增至允許的 app 清單，以供使用者在單一應用模式中使用這些 app。 拖放 app，並依照單一應用模式啟動程式中要顯示的順序加以排列。

將應用程式新增至允許的 app 清單並不會在裝置上安裝該 app。 因此，請務必將每項 app 發佈給 App Catalog 中的適當使用者和使用者群組。

內建 App

按一下「+新增」，納入單一應用模式允許之 app 群組中提列的原生 app。

如果您停用上述「鎖定」設定中的「Dialer」或「相機」，就無法將其新增至「允許的 App」清單中。

「App Catalog「

按一下「+新增」，以將 App Catalog 提列的 app 納入單一應用模式允許的 app 群組中。

其他 App

按一下「+新增」，以納入 Google Play 商店不提供之 App 的**套件名稱**。

單一應用模式允許的 App

按一下 X，即可從單一應用模式允許之 app 群組中移除 app。 拖曳以變更 app 在單一應用裝置上的顯示順序。

> 在 Android 4.4 或支援的最新發行版本中使用單一應用模式時，支援多位使用者的 Samsung 裝置會自動在單一應用模式中鎖定多位使用者功能。

如需更多資訊，請參閱**如何建立配置**

10.10.4.34. 本機管理員密碼解決方案組態

本機管理員密碼解決方案 (LAPS) 組態設定使 Ivanti Neurons for MDM 管理員能夠以設定的時間間隔在受管理的 macOS 裝置上自動重新生成本地管理員密碼。 有關 LAPS 的更多資訊，請參閱**本機管理密碼解決方案 (LAPS)**。

適用於: 使用自動自動化 裝置註冊進行註冊和管理的 macOS 裝置。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取**本機管理員密碼解決方案 (LAPS)** 組態。
3. 依下表配置 **LAPS** 設定:

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
平台	從下拉清單選取 macOS。
輪換間隔	從下拉清單中選取以下選項之一，以定義密碼的自動輪換: • 無輪換 (**預設**) • 15 天 • 30 天 • 60 天 • 90 天 • 120 天 • 180 天
在檢視間隔之後輪換	從下拉清單中選取以下選項之一，以便在從**裝置詳細資訊**頁面檢視密碼後自動輪換密碼: • 1 至 24 小時 • 36 小時 • 48 小時 預設值設定為 **2** 小時。

4. 按**下一步**，確認發佈設定。
5. 選取其中一個發佈選項以設定**本機管理員密碼解決方案 (LAPS)** 組態。 如需有關設定發佈選項的詳細資訊，請參閱**使用配置**。
6. 按一下**完成**。

10.10.4.35. macOS 防火牆

授權：Gold

「macOS 防火牆」用來管理 macOS 裝置上透過「安全性喜好設定」窗格存取的「應用程式防火牆」設定。

適用於：macOS 12.3+

- **允許內建的軟體接收傳入連線** - 若為 True，則允許內建的軟體接收傳入連線。
- **允許下載的已簽署軟體接收傳入連線** - 若為 True，則允許下載的已簽署軟體接收傳入連線。

適用於：macOS 12.0+

- **啟用記錄** - 若為 True，則啟用記錄
- **指定記錄類型**
  - **節流**
  - **摘要**
  - **詳細資訊**

適用於： macOS 10.12+

按一下**啟用防火牆**後，可以選擇下列一或多個選項：

- **封鎖所有傳入連線** - 選取此選項可阻止所有共用服務 (例如螢幕共用或檔案共用) 接收 macOS 裝置上的傳入連線。 以下系統服務可能仍會接收傳入連線:
  - configd，用於實作 DHCP 與其他網路組態服務
  - mDNSResponder，用於實作 Bonjour
  - racoon，用於實作 IPSec
- **啟用隱形模式** - 選取此選項可阻止 macOS 裝置回應探測請求。 受管理 macOS 裝置仍會回應授權應用程式的傳入請求，同時忽略意外請求，例如 ICMP (ping)。
- **應用程式** - 連線由防火牆控制的應用程式的清單。 選取您想要在 macOS 裝置上為之接收傳入連線的特定應用程式。

選取**新增+** 以將列新增至應用程式清單中。 選取**套組 ID** 下面的儲存格，以選取您想要明確允許其傳入連線的應用程式。 選取**允許連線**儲存格中的核取方塊，以允許來自選定應用程式的傳入連線。

> 配置必須具有系統範圍的描述檔。 如果多個設定檔包含此組態，則將使用最嚴格的設定聯合。

> 不支援**自動允許已簽署的下載軟體**及**自動允許內建軟體**選項。 不過，當此配置可供使用時，系統會將這兩個選項強制設為「開啟」。

> 管理員可以將裝置指定為不受 Ping 命令的探索，以啟用隱形模式。

10.10.4.36. macOS 限制

授權：Gold

「macOS 限制」可決定 macOS 裝置上要啟用的限制。

您可在 macOS 裝置上設定要啟用或停用下列功能：

macOS 版本	功能
macOS 10.11+	
	• 允許相機 • 允許 iCloud 文件同步 **僅限受監管：** • 允許 Spotlight 網際網路結果
macOS 10.11.2+	
	• 允許定義查詢
macOS 10.12+	
	• 允許 iCloud 鑰匙圈同步 • 允許返回我的 Mac • 允許尋找我的 Mac • 允許分享至備忘錄、提醒事項或 LinkedIn • 允許書籤同步 • 允許 macOS iCloud 郵件服務 • 允許 macOS iCloud 行事曆服務 • 允許 macOS iCloud 通訊錄服務 • 允許 iCloud 提醒事項服務 • 允許自動解鎖 **僅限受監管：** • 允許 Apple Music
macOS 10.12.4+	
	• 允許指紋解鎖
macOS 10.13+	
	• 允許 iTunes 檔案共用 • 允許內容快取 • 允許修改桌布 **僅限受監管：** • 允許 AirPrint • 允許 AirPrint iBeacon Discovery • 強制 AirPrint Trusted TLS 需求

macOS 版本	功能
	• 允許 AirDrop • 允許 Game Center
macOS 10.13.4+	
	僅限受監管： 延遲軟體更新的天數範圍 (30 到 90 天) 預設：30 天。
macOS 10.14+	
	僅限受監管： 允許附近裝置共享密碼要求
macOS 10.14.4+	
	• 允許螢幕截圖 • 允許遠端螢幕觀察 **僅限受監管：** • 允許自動加入課堂 • 允許課堂請求離開課堂的授權 • 允許課堂鎖定 app 與鎖定裝置，沒有提示 • 允許強制自動執行受管理課堂螢幕觀察
macOS 11.0+	
	僅限受監管： 允許強制延遲應用程式軟體更新
macOS 11.3+	
	強制執行指紋逾時 預設: 48 小時 先決條件: 須在裝置上設定 Touch ID
macOS 11.3+	
	僅限受監管： • 強制延遲重大作業系統軟體更新延後安裝 • 強制延遲作業系統軟體小更新延後安裝 • 強制延遲非作業軟體更新延後安裝 • 強制延遲重大軟體更新
macOS 12+	

macOS 版本	功能
macOS 13.0 至 26.0	• allowCloudPrivateRelay: 如果您在 macOS 裝置上將 Private Relay 設為「開啟」，網路流量就會加密，確保際網路活動為私人且安全。 此限制需要受監督的裝置。 • 允許 iCloud 照片程式庫 **僅限受監管裝置**: • 允許清除內容和設定

macOS 14.0+	• 允許安裝背景安全性改進：停用回應。 使用者無法安裝背景安全性改進。
	• 允許移除背景安全性改進：阻止使用者復原回應。 使用者無法移除背景安全性改進。
	• 允許通用控制:
	  ◦ 若為 **True**，則該組態讓您可以使用主要裝置的輸入裝置控制次要顯示裝置。
	  ◦ 若為 **False**，則可以新增次要顯示裝置，但無法使用主要輸入裝置控制次要顯示裝置。
	僅限受監管裝置:
	• 允許 UI 組態設定檔安裝: 若為 False，則該組態不允許在 macOS 裝置上安裝設定檔、組態或憑證。
	• 允許 USB 限制模式: 若為 True，該組態會鎖住裝置，使其無法使用遠端連線的輸入裝置。 裝置上的「允許配件連線」選項會呈灰色狀態。
	• 允許修改 ARD 遠端管理
	  ◦ 若為 False，則阻止在系統設定中修改遠端管理共用設定。
	  ◦ 預設值：true
	• 允許修改藍牙共用
	  ◦ 若為 False，則阻止在系統設定中修改藍牙設定。
	  ◦ 預設值：true
	• 允許雲端無邊記
	  ◦ 若為 False，則不允許 iCloud 無邊記服務。
	  ◦ 預設值：true
	• 允許修改檔案共用
	  ◦ 若為 False，則阻止在系統設定中修改檔案共用設定。
	  ◦ 預設值：true
	• 允許修改網際網路共用
	  ◦ 若為 False，則阻止在系統設定中修改網際網路共用設定。
	  ◦ 預設值：true
	• 允許建立本機使用者
	  ◦ 若為 False，則阻止在系統設定中建立新使用者。
	  ◦ 預設值：true

macOS 版本	功能

	• 允許修改印表機共用
	  ◦ 若為 False，則阻止在系統設定中修改印表機共用設定。
	  ◦ 預設值：true
	• 允許修改遠端 Apple 事件
	  ◦ 若為 False，則阻止在系統設定中修改遠端 Apple 事件共用設定。
	  ◦ 預設值：true
	• 允許 Siri
	  ◦ 預設值：true
	• 允許修改啟動磁碟
	  ◦ 若為 False，則阻止在系統設定中修改啟動磁碟設定。
	  ◦ 預設值：true
	• 允許「時光機」備份
	  ◦ 若為 False，則阻止在系統設定中修改「時光機」設定。
	  ◦ 預設值：true
	僅限受監管裝置:
	• 允許帳戶修改
	  ◦ 若為 false，則防止修改帳戶。
	  ◦ 預設值：true
	• 允許修改裝置名稱
	  ◦ 若為 false，則防止變更裝置名稱。
	  ◦ 預設值：true
	• 允許修改 TouchID 指紋
	  ◦ 若為 false，則防止修改 Touch ID 指紋。
	  ◦ 預設值：true

macOS 15.0+	**僅限受監管裝置**:
	• 允許 Genmoji
	  ◦ 選取此項可允許建立 Genmoji。
	  ◦ 預設值：true
	• 允許 Image Playground
	  ◦ 選取此項可允許使用映像生成。
	  ◦ 預設值：true
	• 允許 iPhone 鏡像
	  ◦ 選取此項可允許 iPhone 在 macOS 裝置中進行鏡像。
	  ◦ 預設值：true

macOS 版本	功能

	• 允許書寫工具
	  ◦ 選取此項可啟用 Apple Intelligence 書寫工具。
	  ◦ 預設值：true

macOS 15.1+	

	僅限受監管裝置:
	• 允許郵件摘要
	  ◦ 選取可允許手動建立電子郵件訊息摘要。
	  ◦ 預設值：true
	• 允許修改媒體共用
	  ◦ 選取可允許修改媒體共用設定。
	  ◦ 預設值：true

macOS 15.2+	

	僅限受監管裝置:
	• 允許外部情報整合
	  ◦ 選取可允許搭配 Siri 使用外部雲端式情報服務。
	  ◦ 預設值：true
	• 允許外部情報整合登入
	  ◦ 選取可允許修改預設瀏覽器喜好設定。 套用此項後，用於設定預設瀏覽器喜好設定的 Ivanti Neurons for MDM 設定命令仍然有效。
	  ◦ 預設值：true

macOS 15.3	

	安全和隱私權:
	• 允許外部情報工作區 ID
	  ◦ 輸入允許的「外部情報工作區 ID」
	• 允許筆記轉錄檔摘要
	  ◦ 選取此選項可從轉錄建立摘要。
	  ◦ 預設值: True

10.10.4.37. macOS AppStore 限制

授權：Gold

「macOS AppStore 限制」用來定義要在 macOS AppStore 中啟用哪些限制。

您可以設定下列選項：

設定	**方法**
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
配置設置	
macOS 版本	**功能**
10.9+	App 安裝僅限管理使用者。
10.10+	• App 安裝僅限軟體更新。 • 停用使用者採用 app。 • 停用軟體更新通知。
10.11+	App 安裝僅限 MDM 安裝的 app 和軟體更新。

發佈配置

程序

1. 使用先前的表格設定選項。
2. 按**下一步**。
3. 選擇**啟用此配置**選項。
4. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂

按一下**完成**。

10.10.4.38. macOS 燒錄光碟限制

授權：Gold

「macOS 燒錄光碟限制」用來管理 macOS 中的燒錄光碟。 您可設置 **macOS Finder 設定**，以便從 macOS 的 Finder app 啟用或停用燒錄光碟選項。

您可以設定下列選項：

設定	**方法**
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
配置設置	
設定	**方法**
允許燒錄光碟	• 開 • 關 • 需要身份認證

發佈配置

程序

1. 使用先前的表格設定選項。
2. 按**下一步**。
3. 選擇**啟用此配置**選項。
4. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂

按一下**完成**。

10.10.4.39. 允許的媒體控制 (已棄用)

授權：Gold

「允許的媒體控制」配置用來管理 macOS 中各種實體媒體的裝載、卸載與登出時退出。

您可以設定下列選項：

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
配置設置	
媒體類型的裝載控制	
開啟每種媒體類型的裝載控制，並設置裝載設定。 如果您關閉裝載控制，則會套用作業系統預設設定。	
媒體類型	**裝載設定**
• CD • DVD • BD	• 唯讀與身份認證 • 拒絕裝載 • 退出媒體
• 空白 CD • 空白DVD • 空白 BD • DVD-RAM • 磁碟映像檔 • 內建硬碟 • 外接硬碟 • 網路磁碟	• 唯讀 • 拒絕裝載 • 退出媒體 • 驗證
• 外接硬碟包括 USB 硬碟、USB 隨身碟和 SD 卡。 • 唯讀媒體 (例如：CD、DVD 及 BD) 依預設裝載為唯讀。	
媒體類型的卸載控制	
開啟每種媒體類型的卸載控制，並設置卸載設定。 如果您關閉卸載控制，則會套用作業系統預設設定。 設定媒體類型的「拒絕卸載」設定時請小心。	
媒體類型	**裝載設定**
• CD • DVD • BD • 空白 CD • 空白DVD • 空白 BD • DVD-RAM • 磁碟映像檔	• 拒絕卸載 • 驗證

設定	方法
• 內建硬碟 • 外接硬碟 • 網路磁碟	
登出時退出設定	
在使用者登出時自動退出的媒體類型。	
媒體類型	
• CD • DVD • BD • 空白 CD • 空白DVD • 空白 BD • DVD-RAM • 磁碟映像檔 • 外接硬碟 • 網路磁碟	

發佈配置

程序

1. 使用先前的表格設定選項。
2. 按**下一步**。
3. 選擇**啟用此配置**選項。
4. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂

按一下**完成**。

10.10.4.40. macOS Finder 設定

授權：Gold

「macOS Finder 設定」用來管理 macOS 中 Finder app 的設定。

您可以設定下列選項：

設定	**方法**
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
配置設置	
設定	**方法**
停用 Finder 中的燒錄光碟支援	• 開啟 • 關閉

發佈配置

程序

1. 使用先前的表格設定選項。
2. 按**下一步**。
3. 選擇**啟用此配置**選項。
4. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂

按一下**完成**。

10.10.4.41. macOS 核心擴充原則

適用於：macOS 10.13.2 或支援的更新版本。

控制載入「使用者核准的核心擴充」的限制與設定。

建立 macOS 核心擴充原則配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入**核心**，然後按一下 **macOS 核心擴充**配置。
4. 命名配置，並加以描述。
5. 選擇**允許使用者覆寫**選項，以允許使用者核准下列配置 未明確允許的新增核心擴允。
6. 在「允許的團隊識別碼與核心擴充」區段中，按一下 **+新增**，以新增允許的團隊識別碼與核心擴充。 核心擴充即套件的套件識別碼。 對於每個團隊識別碼，您可在蹦現視窗中新增數個有效簽署的核擴充名稱。
7. 按一下**新增**。
8. 按**下一步**，確認發佈設定。
9. 按一下**完成**。

如需更多資訊，請參閱如何建立配置

10.10.4.42. 適用於 macOS 的 Mobile@Work

本節包含以下各主題：

- 適用於 macOS 的 Mobile@Work 配置和指令碼執行工作流程
- 建立適用於 macOS 的 Mobile@Work 配置
- 啟用 macOS 裝置上的使用者上架
- 建立適用於 macOS 的 Mobile@Work 指令碼配置
- 執行完整解除安裝適用於 macOS 的 Mobile@Work
- 透過 macOS Mobile@Work 套用指令碼

Ivanti Neurons for MDM 可讓您建立自己的 macOS 殼層指令碼，然後上傳至 Ivanti Neurons for MDM 並在受管理 macOS 裝置上執行。 如需建立、上傳與管理指令碼儲存庫的相關資訊，請參閱所有指令碼。

macOS device 使用者可使用適用於 macOS 1.1 或更新版本的 Mobile@Work 來啟動裝置淘汰。 從「關於 Mobile@Work」畫面，按一下**解除安裝**即可使用淘汰選項。 在 Ivanti Neurons for MDM 中，您可透過**裝置**頁面和裝置詳細資料頁面驗證裝置狀態。

適用於 macOS 1.5 或更新版本的 Mobile@Work 會在註冊後立即開啟 Apps@Work，而不會等待 MDM 註冊完成。

在適用於 macOS 的 Mobile@Work 中，按一下應用程式磚以顯示該應用程式的「App 詳細資料」頁面。 此頁面包含 app 的描述、畫面擷取、評等和評論。

適用於 macOS 的 Mobile@Work 會在庫存報告中告知 Ivanti Neurons for MDM 伺服器是否已安裝封裝工具內部開發 macOS app。

必要條件

在 App Catalog 中，適用於 macOS 的 Mobile@Work 用戶端是以商務 app 的形式提供。 可在 macOS 裝置上執行殼層指令碼之前，請先指示使用者使用適用於 macOS 的 Mobile@Work 註冊其含有 Ivanti Neurons for MDM 的裝置 。

程序

1. 請下載適用於 macOS 的 Mobile@Work 應用程式。 在 https://support.mobileiron.com/support/CDL.html 上可提供 PKG 檔案。 請參閱這篇 Ivanti 客戶論壇文章，瞭解有關取得下載網站認證的資訊。
2. 將適用於 macOS 的 Mobile@Work 應用程式 PKG 檔案上傳至安全的伺服器。 此伺服器必須可供裝置使用者存取。
3. 透過電子郵件或訊息，與裝置使用者分享適用於 macOS 的 Mobile@Work 應用程式安裝檔案的 URL
4. 指示使用者：
    1. 在其裝置上下載並安裝適用於 macOS 的 Mobile@Work。
    2. 使用適用於 macOS 的 Mobile@Work 註冊含有 Ivanti Neurons for MDM 的裝置。

適用於 macOS 的 Mobile@Work 配置和指令碼執行工作流程

程序

1. 設定與發佈適用於 macOS 的 Mobile@Work 配置。
2. 設定並發佈適用於 macOS 的 Mobile@Work 指令碼組態，以將指令碼上傳至 Ivanti Neurons for MDM。 指令碼透過對每個租戶來說不重複的已簽署認證進行加密與簽署。 指令碼的解密金鑰會隨經過加密與簽署的指令碼下載 URL 一起傳送。
3. Ivanti Neurons for MDM 會在 macOS 裝置上使用適用於 macOS 的 Mobile@Work 來執行指令碼。 適用於 macOS 的 Mobile@Work 會定期輪詢 Ivanti Neurons for MDM，以檢查是否有任何指令碼正在等待執行。 如果有任何指令碼佇列中，Mobile@Work 會在 macOS 裝置上下載並根據您在 Ivanti Neurons for MDM 中定義的設定來執行指令碼。

4. 適用於 macOS 的 Mobile@Work 會將指令碼執行結果傳回 Ivanti Neurons for MDM，並顯示在裝置日誌中。 您可以在 macOS 裝置上透過裝置詳細資料頁面的 **日誌**索引標籤查看裝置日誌。

建立適用於 macOS 的 Mobile@Work 配置

您可使用適用於 macOS 的 Mobile@Work 配置的預設系統配置。 不過，它不會預設發佈至所有裝置。

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入 **work**，然後按一下**適用於 macOS 的 Mobile@Work** 配置。
4. 命名配置，並加以描述。
5. 輸入**執行時間上限** (秒)，以指定指令碼可以執行多久。 預設值為 60 秒鐘。
6. 輸入**回應大小上限** (Kb)，以指定要傳回 Ivanti Neurons for MDM 的指令碼輸出其回應大小限制的上限。 這是執行指令碼時傳回的 StdOut 和 StdErr 資料。 預設值為 1 KB。
7. 輸入**登記頻率** (分鐘)，以指定適用於 macOS 的 Mobile@Work app 每隔多久就必須向 Ivanti Neurons for MDM 登記。 預設值為 15 分鐘。
8. (選用) 您可使用**啟用 macOS 裝置上的使用者上架**區段，以啟用 macOS 裝置上的使用者上架。
9. 按一下**下一步**以設定發佈設定。
    1. 選擇發佈層級:
    2. **給所有使用者** - app 將新增至所有的使用者相容裝置。
    3. **不給任何使用者** - app 將暫置以供日後發佈。
    4. **自訂發佈** - 請選擇下列任一選項：
        - **使用者/使用者群組** - App 將僅發佈給您選擇的使用者或使用者群組。
          按一下**使用者**索引標籤，以選擇使用者。
          按一下**使用者群組**索引標籤，以選擇使用者群組。
        - **裝置/裝置群組** - App 將僅發佈給您選擇的裝置或裝置群組。
          按一下**裝置**索引標籤，以選擇裝置。
          按一下**裝置群組**索引標籤，以選擇裝置群組。
10. 按一下**完成**。

啟用 macOS 裝置上的使用者上架

您可以在自動化 Device Enrollment 程序期間，啟用 macOS 裝置上的使用者上架如下：

- 當 Device Enrollment 完成時，會將適用於 macOS 的 Mobile@Work (1.68 版或更新版本) 和描述檔、配置和 app 一併推送給裝置。
- 只有在以下情況中，才會將適用於 macOS 用戶端的 Mobile@Work 和其他 app 推送至裝置：
    - app 是內部開發 PKG app 或 Apple Apps and Books 公開 app。
    - App 的無訊息自動安裝設定設為 true。 此設定位於 **App** > **App 詳細資料** > **App 配置** > **在裝置上安裝**頁面中。
    - **App 優先順序**設為「高」。 依預設，適用於 macOS 的 Mobile@Work 用戶端應用程式的優先順序會設為高 (且無法修改)，**否則使用者上線程序可能會失敗**。
    - 已將 app 設為發佈至裝置、使用者群組或裝置。

- 在適用於 macOS 的 Mobile@Work 已安裝並註冊後，macOS 裝置會進入單一應用模式 (使用者無法控制裝置)，直到剩下的描述檔、配置和 app 都已配置並安裝。 以步驟顯示進度。

針對適用於 macOS 1.73 或 Ivanti Neurons for MDM 支援之更新版本的 Mobile@Work，支援以下其他功能：

- 在完成裝置的 Device Enrollment 之後不久，使用者上架程序就會完成。 在觸發使用者上架時窗 (通常在裝置註冊後 20 分鐘) 過期後，即使管理員在 Mobile@Work 配置中啟用使用者上架，使用者上架程序也不會開始。 這可防止當正常使用裝置時，讓裝置進入使用者上架單一應用模式。
- 在適用於 macOS 用戶端的 Mobile@Work 中，以步驟顯示使用者上架程序。 第一個步驟中將會安裝配置。
- 將會開始安裝高優先順序的 app。 每安裝一個高優先順序 app 將會計為一個步驟。 封裝工具 app 不會列入步驟計算。
- 即使在使用者上架完成後，剩下的 app 仍將會繼續在背景執行安裝。 在裝置上開始進行安裝或已實際安裝在裝置上的應用程式將會標示為已安裝。
- 在使用者上架後，您可移至裝置詳細資料，確認配置和 app 已推送至每部裝置。 如需更多資訊，請參見日誌。

程序

1. 使用建立適用於 macOS 的 Mobile@Work 配置建立適用於 macOS 的 Mobile@Work 配置。
2. 選取**啟用使用者上線**選項。
3. 輸入下列詳細資料：
   - **使用者上架逾時值** - 輸入在初始裝置設定期間，裝置大概需要多少時間來安裝 app 和配置。 依預設，使用者在 macOS 裝置上的上架程序會在 120 秒後逾時，您可以視需要修改。
   - **使用者登陸頁面 URL** - 提供要在上架完成後向使用者顯示的登陸頁面 URL。
4. 按**下一步**，確認發佈設定。
5. 按一下**完成**。

建立適用於 macOS 的 Mobile@Work 指令碼配置

您可以建立多個適用於 macOS 的 Mobile@Work 指令碼配置並發佈至裝置。 使用此組態，您可以從儲存庫中選擇一個指令碼 (**管理> 指令碼和檔案 > 所有指令碼**) 發佈到適用於 macOS 的 Mobile@Work。

如果裝置安裝了適用於 macOS 的 Mobile@Work 1.66 或更新版，您可以在該裝置上排程指令碼執行。 如果裝置安裝的是適用於 macOS 用戶端的 Mobile@Work 1.66 版之前版本，當您在該裝置上排程指令碼執行，指令碼只會執行一次。 如果適用於 macOS 用戶端的 Mobile@Work 從 1.4 升級到 1.66，則所有的 macOS 用戶端配置將會發佈至該裝置。

必要條件

- 前往**管理 > 指令碼和檔案 > 所有指令碼**，上傳和管理可用於此組態並發佈到裝置的指令碼。
- 在裝置上設定與發佈適用於 macOS 的 Mobile@Work 配置。 否則，適用於 macOS 的 Mobile@Work 指令碼配置將會處於「錯誤」狀態。

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入 **work**，然後按一下**適用於 macOS 的 Mobile@Work 指令碼** 配置。
4. 命名配置，並加以描述。
5. 在**選擇指令碼**欄位中輸入指令碼的名稱，以從下拉式清單尋找與選擇指令碼。

6. 在「指令碼輸入」區段中，將會顯示與指令碼相關聯的指令碼輸入標籤和指令碼變數。 如果您需要將其覆寫，請輸入替代的指令碼變數 (例如，{$userWorkEmailAddress}) 及其替代預設值 (例如，john.doe@company.com)。
7. 在「指令碼執行」區段中，選擇其中一個排程選項：
    - 在部署上執行一次
    - 重複執行
8. 如果您選擇「重複執行」，請指定下列詳細資料：
    - 使用的時區 - 選擇裝置的當地時間或 UTC 時間。 指令碼將會在透過此欄位選擇的時間執行。
    - 開始執行時間 - 選擇開始日期。
    - 結束執行時間 - 選擇結束日期 (晚於或等於開始日期)。
    - 執行指令碼 - 選擇「每日」或「每週」，並視情況輸入時數 (24 小時制)、分鐘數或天數。
9. 按**下一步**，確認發佈設定。
10. 按一下**完成**。

執行完整解除安裝適用於 macOS 的 Mobile@Work

在安裝 Mobile@Work for macOS 期間，如果您已啟用**在取消註冊時移除應用程式**選項 **(僅適用於受管理的應用程式)**，或如果您從 Ivanti Neurons for MDM 管理入口網站啟動要淘汰的裝置，則只會從裝置刪除 Mobile@Work for macOS 應用程式和解除安裝指令碼。 如要避免從後端執行程序和指令碼，請確定在新使用者註冊裝置或現有使用者淘汰裝置期間，從 Ivanti Neurons for MDM 管理入口網站取消選取下列選項，以確定解除安裝指令碼執行，並從後端刪除相關的程序和指令碼。

程序

1. 登入 Ivanti Neurons for MDM 管理員入口網站。
2. 前往 **App** > **Mobile@Work** > **App 配置** > **App 配置摘要清單** > **Apple App 設定** > **Apple 應用程式管理配置設定**。
3. 從**配置設置**頁面，取消選取下列選項：
    - **移除取消註冊的 app (僅適用於受管理的 app)**。

透過 macOS Mobile@Work 套用指令碼

採用 macOS Mobile@Work 的指令碼可讓管理員進行遠端部署和在受管理的 macOS 裝置上執行 shell 指令碼。 這有助於自動化工作、套用修復、強制執行原則和簡化組態，而無需使用者干預，確保大規模的一致且高效的裝置管理。

先決條件:

- 裝置必須正在執行 macOS。
- Mobile@Work for macOS 必須已安裝在裝置上。
- 確定 Mobile@Work for macOS 組態已正確建立、分發和指派。 如需詳細資訊，請參閱**建立 Mobile@Work for macOS 組態**。

> 如果裝置未安裝並設定 Mobile@Work 用戶端，或者裝置平台支援指令碼執行，則無法透過 macOS Mobile@Work 套用指令碼。 確保 macOS 用戶端處於作用中狀態，且您僅選取支援的 macOS 裝置。

程序

1. 登入 Ivanti Neurons for MDM 管理員入口網站。
2. 前往**裝置**，並選取要為之執行指令碼的 macOS 裝置清單。

3. 在**裝置**頁面中，導覽至**動作** > **macOS** > **採用 macOS Mobile@Work 的指令碼**。
   採用 macOS Mobile@Work 的指令碼窗格將會出現。
4. 若要套用指令碼，請在**選取指令碼**欄位中，輸入並選取指令碼名稱。
   如需建立指令碼的更多資訊，請參閱**所有指令碼**。
5. 選取**確定**以在裝置上執行指令碼。

相關主題：

- 裝置**管理員 > 指令碼和檔案 > 所有指令碼**
- **如何建立配置**

10.10.4.43. macOS 軟體更新規則配置

管理員可以定義 **macOS 軟體更新規則**，以設定裝置的軟體更新規則。

適用於：macOS 10.7 至 26.0。

1. 前往配置 > +新增。
2. 在搜尋欄位中輸入macOS，然後按一下 macOS 軟體更新設定配置。
3. 輸入配置的名稱和描述。
4. 從 **macOS 軟體更新規則**選擇所需的配置。
5. 按下一步。
6. 選擇啟用此配置選項。
7. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂。
8. 按一下完成。

macOS 軟體更新規則

管理員可從規則清單中選擇如下：

> 當裝置套用這些規則時，使用者無法變更這些設定。

- 允許發行前版本軟體安裝。
- 自動：
    - 檢查更新
    - 有可用更新時，自動下載新更新
    - 安裝 macOS 更新
    - 從 App Store 安裝 app 更新
    - 安裝系統資料檔案和安全更新。
- App 安裝僅限管理使用者。
- 新增軟體更新目錄的 URL 的選項（macOS 11+ 上不支援）。

10.10.4.44. 憑證偏好設定

適用於：

- macOS 10.12 到 Ivanti Neurons for MDM 所支援的最新發行版本。

識別使用者鑰匙圈中的「憑證偏好設定」項目，此鑰匙圈會參照相同描述檔中所附的憑證裝載。

此配置用來將憑證與電子郵件地址或 URL 綁定。 將憑證與電子郵件地址綁定後，郵件 app 將會針對該電子郵件帳戶使用它。 如果網站的 SSL 憑證不受信任，新增「憑證偏好設定」可避免瀏覽器在您存取網站時提示警告訊息。

> 管理員必須持有憑證。 如需新增和發佈憑證的詳細資訊，請參閱憑證配置。

建立「憑證偏好設定」配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入**偏好設定**，然後按一下**憑證偏好設定**配置。
4. 命名配置，並加以描述。
5. 在「配置設定」區段的**名稱**欄位中，輸入為其要求偏好憑證的電子郵件 ID 或名稱。
6. 在**憑證 UUID** 欄位中選擇憑證。
7. 按**下一步**，確認發佈設定。
8. 按一下**完成**。

相關主題：

- 身分偏好設定
- 憑證配置
- 如何建立配置

10.10.4.45. Active Directory (macOS)

適用於：macOS 10.9 或支援的更新版本。

設定進階選項以綁定 macOS 裝置與 Active Directory (AD) 網域，藉此存取依賴 AD 提供身份認證與安全性的軟體服務。

本節包含以下各主題：

- 建立 Active Directory 配置
- Active Directory 設定

建立 Active Directory 配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入**隱私權**，然後按一下 **Active Directory** 配置。
4. 命名配置，並加以描述。
5. 輸入如下列 Active Directory 設定表格所述的設定。
6. 按**下一步**，確認發佈設定。
7. 按一下**完成**。

Active Directory 設定

設定	方法
Active Directory 設定 - 基本	
主機名稱	(必填) 輸入主機名稱，Active Directory 要加入的網域。
使用者名稱	針對用來加入網域的帳戶，輸入其使用者名稱。
密碼	針對用來加入網域的帳戶，輸入其密碼。
AD 組織單位	輸入要新增加入電腦物件的組織單位 (OU)。
AD 裝載樣式	請選擇下列選項之一，以指出要使用的網路主通訊協定： • AFP • SMB
Active Directory 設定 - 進階	
啟用 ADCreateMobileAccountAtLogin 鍵	啟用或停用 ADCreateMobileAccountAtLogin 鍵。 其他選項：在登入時建立 行動帳戶。
啟用 ADWarnUserBeforeCreatingMA 鍵	啟用或停用 ADWarnUserBeforeCreatingMA 鍵。 其他選項：在建立行動帳戶之前警告使用者。
啟用 ADForceHomeLocal 鍵	啟用或停用 ADForceHomeLocal 鍵。 其他選項：強制本機主目錄。
啟用 ADUseWindowsUNCPath 鍵	啟用或停用 ADUseWindowsUNCPath 鍵。 其他選項：使用 AD 的 UNC 路徑來衍生網路主位置。
啟用 ADAllowMultiDomainAuth 鍵	啟用或停用 ADAllowMultiDomainAuth 鍵。 其他選項：允許樹系中任何網域的身分認證
預設的使用者 Shell	輸入預設的使用者 Shell，例如 /bin/bash。
將使用者 UID 對應至屬性	選擇將使用者 UID 對應至指定屬性。
將使用者 GID 對應至屬性	選擇將使用者 GID 對應至指定屬性。
將群組 GID 對應至屬性	選擇將群組 GID 對應至指定屬性。
偏好的網域伺服器	偏好此網域伺服器。
名稱空間慣例	請選擇下列使用者帳戶命名慣例之一： • 網域 (預設) • 樹系
封包簽署	請選擇下列封包簽署選項之一： • 允許 (預設) • 停用 • 必需

設定	方法
封包加密	請選擇下列封包加密選項之一： • 允許 (預設) • 停用 • 必需 • SSL
允許由指定的 Active Directory 群組管理	允許由指定的 Active Directory 群組管理。 按一下**新增**以新增一或多個群組。
限制動態 DNS	選擇限制動態 DNS 更新至指定介面 (例如 en0、en1 等等)。 按一下**新增**以新增一或多個介面名稱。
變更密碼間隔	指定所需的電腦信任帳戶變更頻率 (天)。 零值已停用。

如需更多資訊，請參閱**如何建立配置**

10.10.4.46. 身分偏好設定

適用於：macOS 10.12 或支援的更新版本。

識別使用者鑰匙圈中的「身份偏好設定」項目，此鑰匙圈會參照相同描述檔中所附的身份裝載。

macOS 的「身份偏好設定」可讓您選擇要在網站使用的身份 (鍵值配對)。 將「身份偏好設定」(包含 URL 和身份) 推送至裝置之後，其應會顯示在**鑰匙圈存取 → 所有項目**中 (「種類」為「身份偏好設定」)。 下次，當您嘗試從 Safari 連接至該 URL 時，裝置就會顯示已設好的憑證。

Ivanti Neurons for MDM 建立了預設系統身份偏好設定配置，其中包含 AppStore URL 裝載和可用憑證。

在 macOS 10.12 和更新版本上使用 Safari 來存取 macOS App Catalog 時，使用者會收到輸入密碼以快取身份認證的系統提示。 使用者需要在首次使用時選取「一律允許」，以免在存取 macOS App Catalog 時一直出現提示。

從 macOS 裝置上新的瀏覽器工作階段存取 macOS App Catalog 時，Safari (macOS 版本低於 10.12) 和其他瀏覽器將會顯示憑證和系統密碼提示。

建立「身份偏好設定」配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入**偏好設定**，然後按一下**身份偏好設定**配置。
4. 命名配置，並加以描述。
5. 在「配置設定」區段的**名稱**欄位中，輸入電子郵件 ID、DNS 主機名稱或服務的唯一識別名稱。
6. 在**憑證 UUID** 欄位中選擇憑證。
7. 按**下一步**，確認發佈設定。
8. 按一下**完成**。

相關主題：

- 憑證偏好設定
- 如何建立配置

10.10.4.47. Office 365 自動帳戶建立 (macOS)

適用於：

- 支援的 macOS 裝置。
- 建議的 Microsoft Office 365 app 版本為 16.13 或更新版本。

設定使用者資訊與選項，以便為所有的 Microsoft Office 365 應用程式設置初始配置。

本節包含以下各主題：

- 建立「Office 365 自動帳戶建立」配置
- 「Office 365 自動帳戶建立」設定

建立「Office 365 自動帳戶建立」配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入 **office**，然後按一下 **Office 365 自動帳戶建立**配置。
4. 命名配置，並加以描述。
5. 輸入下列「Office 365 自動帳戶建立」設定表格當中所述的設定。
6. 按**下一步**，確認發佈設定。
7. 按一下**完成**。

「Office 365 自動帳戶建立」設定

設定	方法
Office 啟動電子郵件地址	輸入使用者電子郵件地址。
Office 自動登入	選擇以壓抑初次執行視窗。 僅提示使用者輸入必要資訊，例如 O365 身分認證。
預設為本機開啟/儲存	選擇以強制開啟/儲存面板至「我的 Mac 上」而不是「線上位置」。
在啟動時顯示新功能	選擇以在啟動時顯示新功能資訊。
Visual Basic 巨集執行狀態	請選擇下列選項之一： • 停用並帶有警告 • 停用但無警告 • 啟用且無警告
停用 Visual Basic External Dylibs	選擇以停用 Visual Basic 外部相依項目。
允許 Visual Basic 綁定系統	選擇以允許巨集使用 DECLARE 來綁定 system() OS API。 此 API 允許巨集執行任意外部處理程序，然後在命令列傳送任意資料給它們。
停用 Visual Basic 綁定 Popen	選擇以允許巨集使用 DECLARE 來綁定 popen() OS API。 此 API 允許巨集執行任意外部處理程序，然後在命令列傳送任意資料給它們。
停用 Visual Basic Mac 指令碼	選擇以允許巨集呼叫 Apple Script Visual Basic API。

如需更多資訊，請參閱[如何建立配置]

10.10.4.48. 驗證

適用於：

- macOS 10.13 和支援的更新版本。
- Windows 10 和支援的更新版本。

使用身份認證配置，為雲端服務及/或桌面登入提供無密碼身份認證。 每部裝置只有一個身份認證配置。

必要條件

- 需要 Zero Sign-On 授權。
- Ivanti Neurons for MDM 應向 Access (應設定 Access 描述檔) 註冊。
- 在設定身份認證配置後，您無法取消註冊 Access 描述檔，因為身份認證配置將會參照該 Access 描述檔。
- 如果 Access 描述檔有任何變更，請重新發佈身份認證配置至 macOS 裝置。 針對 Windows 裝置，請在新的 app 中複製和使用新的 CLI 值。

建立身份認證配置

Procedure

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入 **auth**，然後按一下**身份認證**配置。
4. 命名配置，並加以描述。
5. 從下拉式清單選擇**桌面身份憑證**。
6. 請選擇下列作業系統選項中的一個或兩個都選：
    - macOS
    - Windows
7. 針對 macOS：
    1. 在自訂資料區中，按一下 **+新增**以新增要推送至裝置的自訂資料鍵和字串值。
    2. 按**下一步**，確認發佈設定。
    3. 按一下**完成**。
8. 針對 Windows 10 裝置，此配置有助於為 Windows 版 Authenticator MSI app 產生命令列引數如下：
    1. 按一下**完成**以完成身份認證配置。
    2. 從**配置**頁面，檢視身份認證配置以複製顯示的命令列文字。 當針對 Windows 裝置發佈身份認證 app 時需要此文字。

> 當身份認證配置套用至 Windows 裝置時，配置會維持「擱置中安裝」狀態。 您可忽略它，因為這對功能沒有影響。

如需更多資訊，請參閱如何建立配置

10.10.4.49. Apple 應用程式目錄

適用於：iOS 和 macOS

Apple App Catalog 配置可管理透過 Web Clip 存取 Apple App Catalog 的行為。 從 Ivanti Neurons for MDM 版本 83 開始，可以從 Go 應用程式轉換為 Apps@Work 原生體驗。 對於新建租戶，依預設不將 Apps@work Webclip 組態散發給透過 iReg 或用戶端安裝的 iOS 裝置。 管理員必須手動將 webclip 組態散發給透過 iReg 或用戶端註冊的裝置。

> Apps@Work Webclip 搜尋結果在 iOS 和 iPad 裝置上僅顯示 10 個應用程式，即使搜尋請求的列參數超過 10 個也一樣。

程序

管理員可依如下所述的方式，編輯發佈這項系統定義的配置：

1. 前往**配置**。
2. 按一下 **Apple App Catalog**。
3. 按一下**編輯發佈**。
4. 請選擇下列發佈選項之一：
    - 所有裝置 - 此配置將傳送給所有相容裝置
    - 沒有裝置 - 停用存取 Apple App Catalog 或將這項配置排到稍後發佈。
    - 自訂 - 定義將會收到此配置的特定「裝置群組」

按一下**儲存**。

10.10.4.50. 受管理的網域

授權：Silver

受管理網域組態可讓您指定 iOS 8+ 和 visionOS 1.1+ 裝置上的 Mail 和 Safari 信任哪些網域。 在裝置套用此項配置之後，裝置上的 Mail 和 Safari 就會將配置中未指定的網域醒目提示出來。 您可搭配使用此配置與**限制配置**，來控制 Safari 中允許的資料下載項目。

受管理的網域設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
受管理的電子郵件網域	按一下 **+新增**並輸入網域，例如 mycompany.com。
受管理的 Web 網域	按一下 **+新增**並輸入網域，例如 mycompany.com。

如需更多資訊，請參閱**如何建立配置**

10.10.4.51. 密碼組態

使用啟動精靈時，您會在 Ivanti Neurons for MDM 中優先設定的項目之一是密碼配置。 此配置可定義裝置上螢幕鎖定功能的設定。

密碼設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
允許簡易值	限制 PIN 碼或密碼包含循序字元或數字。 **針對 iOS、macOS、watchOS 和 Android:** 選取此項以允許較低安全性 PIN 或密碼 (因為它們包含重複或以升序或降序排列的字元序列)。 例如：1111、1234、abcd。 如果將 Android 裝置的這個選項刪除，則會強制執行含複雜 PIN 碼的密碼。 例如，使用者即不得設定重複、遞增或遞減的字元順序。 **針對 Windows 10+**: 選取此項以允許安全性較低的密碼 (其中包含重複或遞增的數字序列)。 例如：1111, 1234
必須為英數值	密碼必須至少包含一個字母與一個數字 **針對 iOS 及 Android**: 選取此項以確認密碼包含字母和數字。 **針對 Windows 10+** : 選取此項以確保使用基於 Microsoft 標準的強式密碼。
最小密碼長度	從清單中選擇數字，以設定最小密碼長度。 **若是 Windows 10 Desktop**：本機帳戶會強制執行最小密碼長度 6。
最小複雜字元數	**針對 iOS 及 Android**: 從清單中選取數字，以設定非數字或字母的最小字元數。 **對於 Windows 10+**: 本機帳戶將強制使用 3 個複雜字元。
最大的密碼有效期	輸入裝置使用者在多少天數之後必須重設密碼。 如果您不想設定密碼有效期，可將此欄位保持空白。
自動鎖定	從清單中選擇間隔，以定義裝置閒置多久後就會自動設定螢幕鎖定。
任意鎖定方法	**僅限 Android**。 允許使用者選擇任何鎖定方法，包括模式解鎖。 上述的密碼設定不會套用至這台裝置。
密碼歷程記錄	輸入數字，以設定使用者必須輸入多少次唯一密碼數後才能重複使用密碼。 例如，如果您將此欄位設為 4，使用者就必須設定 4 次密碼後才能重複使用第一個密碼。
裝置鎖定的寬限期	從清單中選擇間隔，以設定鎖定畫面出現多久後使用者必須輸入密碼才能解鎖裝置。
嘗試失敗次數上限	從清單中選擇數字，以設定裝置使用者連續輸入多少次錯誤密碼後裝置就會遭到重設與清除。 **警告：**如果使用者的密碼嘗試次數超過上限，就會清除裝置 請小心使用此選項。
(僅限 macOS) 啟用密碼規則運算式 (macOS 14+)	指定與密碼相符的運算式字串，以確定其是否與原則相符。
(僅限 macOS) 語言	指定說明的語言。
(僅限 macOS) 描述	描述密碼複雜度。 例如，數字、特殊字元、字串等。

設定	方法
(僅限 macOS) 在下次登入時強制執行密碼	選擇啟用 macOS 提示使用者變更密碼，以使密碼在下次使用者登入時符合密碼原則。 預設為不選擇這個選項。 適用於 macOS 10.13 與更新版本。
(僅限 macOS) 登入失敗重設前的分鐘數	指定達到登入失敗嘗試次數上限後重設登入前的分鐘數。 請確保已設定失敗嘗試次數上限以啟用此欄位。 適用於 macOS 10.10 及以上版本。
SmartLock	**適用於 Android 5.0 裝置 (在 Android 企業描述檔中除外)：** **適用於 Android 6.0 或更新版本：** 允許或不允許使用者選擇 SmartLock 功能以解鎖裝置。 當使用者在裝置附近、裝置位於某個地點，或者，當裝置和受信任的裝置配對等特定情況下，SmartLock 功能會自動解鎖裝置。
指紋解除鎖定	**適用於 Android 5.0 裝置 (在 Android 企業描述檔中除外)：** **適用於 Android 6.0 或更新版本：** 允許或不允許使用者選擇「指紋」解鎖裝置。
鎖定畫面通知 (僅適用於 Android Enterprise)	**啟用「受工作管理的裝置」(裝置擁有者) 的通知** 允許或不允許在受工作管理的裝置的鎖定畫面上發出通知 **啟用工作描述檔的未經修訂通知** **適用於 Android 6.0 或更新版本：** 允許或不允許在工作描述檔裝置的鎖定畫面上發出未經修訂通知。 啟用此設定後，您將會收到通知，但內容顯示為「根據原則隱藏內容」。您只能從 app 檢視內容 (郵件/推送通知)。

如需更多資訊，請參閱[如何建立配置]

10.10.4.52. 隱私權偏好設定 (macOS)

適用於：macOS 10.14 或支援的更新版本。

設定允許哪些應用程式可以存取系統服務、系統檔案及系統資源。 此配置控制 macOS 裝置上「系統偏好設定」>「安全性和隱私權」>「隱私權」。

建立「隱私權偏好設定」配置

Procedure

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入**隱私權**，然後按一下 **隱私權偏好設定** 配置。
4. 命名配置，並加以描述。
5. 導覽至頁面上列出的應用程式之一。 如需相關資訊，請參閱 **Apple 說明文件**。
    1. 針對 macOS 10.14+，可供配置使用的應用程式和設定包括：
        - 協助工具 - 透過協助工具子系統指定 app 的原則。
        - 通訊錄 - 指定通訊錄 app 的聯絡人資訊管理原則。
        - Apple 事件 - 指定限制 AppleEvents 傳送 app 至其他程序的原則。
        - 行事曆 - 指定行事曆 app 的行事曆資訊管理原則。
        - 相機 - 系統相機。 在描述檔中不提供相機存取權限；只能拒絕存取。
        - 麥克風 - 系統麥克風。 在描述檔中不提供麥克風存取權限；只能拒絕存取。
        - 照片 - 照片 app 在 ~/Pictures/.photoslibrary 中管理的照片。
        - 張貼事件 - 指定應用程式使用 CoreGraphics API 傳送 CGEvent 至系統事件資料流。
        - 提醒 - 指定提醒 app 管理提醒資訊的原則。
        - 系統原則 (所有檔案) - 允許應用程式存取所有受保護的檔案，包括系統管理檔案。
        - 系統原則 (管理檔案) - 允許應用程式存取系統管理中使用的某些檔案。
    2. 針對 macOS 10.15+，可供配置使用的應用程式和設定包括：
        - 檔案使用狀況 - 允許 File Provider 應用程式知道何時有使用者使用 File Provider 管理的檔案。
        - 從所有處理程序接聽事件 - 允許應用程式使用 CoreGraphic 和 HID API 接聽 (接收) 來自所有程序的 CGEvent 和 HID 事件。 在描述檔中不提供事件存取權限；只能拒絕存取。 取消勾選「允許」選項。
        - 存取媒體櫃 – 允許應用程式存取 Apple Music、音樂和影音活動以及媒體櫃。
        - 系統顯示器的螢幕擷取 - 允許應用程式擷取 (讀取) 系統顯示器的內容。 在描述檔中不提供內容存取權限；只能拒絕存取。 取消勾選「允許」選項。
        - 辨識並傳送語音資料到 Apple - 允許應用程式使用系統語音辨識裝置並傳送語音資料到 Apple。
        - 存取使用者的桌面資料夾中檔案 – 允許應用程式存取使用者桌面資料夾中的檔案。
        - 存取使用者的文件資料夾中的檔案 - 允許應用程式存取使用者的文件資料夾中的檔案。
        - 存取使用者的下載資料夾中的檔案 - 允許應用程式存取使用者的下載資料夾中的檔案。
        - 存取網路磁碟區中的檔案 - 允許應用程式存取網路磁碟區中的檔案。

    - 存取可移除磁碟區中的檔案 - 允許應用程式存取可移除磁碟區中的檔案。

6. 對您想設定的每個應用程式，按一下**動作 > 新增**。
7. 輸入下列身份字典鍵的值：
    - 識別碼 - 設定的名稱。 例如：「us.zoom.ZoomPresence」。
    - 識別碼類型 - 選擇「套件 ID」或「路徑」。 例如：「套件 ID」。
    - 代碼要求 - 指定「套件 ID」或「路徑」的值。 例如：「identifier "us.zoom.ZoomPresence" and anchor apple generic」。
    - 靜態代碼 (True 或 False)
    - 允許 (True 或 False)
    - 評論
8. 按一下**儲存**。
9. (選擇性) 在任何應用程式下，按一下**動作 > 刪除**，以移除現有的隱私權偏好設定。
10. 按**下一步**，確認發佈設定。
11. 按一下**完成**。

如需更多資訊，請參閱[如何建立配置]

10.10.4.53. 隱私權配置

隱私組態定義是否:

- 在裝置上收集位置資料，然後傳送到裝置管理系統
- 是否允許管理員清除裝置
- app 庫存要收集所有 app 或僅收集應用程式目錄中顯示的 app

隱私權設定

> 裝置抹除動作和收集裝置上的所有 app 庫存不適用於使用者註冊裝置。

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
收集位置資料	選擇啟用位置資料收集。 您可在**裝置**頁面中檢視裝置位置。 • 若是 iOS 裝置，裝置定位顯示僅以網路位置為準。 • 對 於 Android 裝置，則根據網路位置和 GPS 位置 (若可用) 定位。 • 若是 Windows 裝置，定位會以裝置簽入時取得的經緯度值為準。 如果裝置啟用了位置收集功能，就會每 4 小時更新一次目前位置。 如果裝置遭淘汰或隱私權配置遭停用/移除，就會將位置資料從裝置管理系統中移除。 裝置使用者可**關閉裝置上的位置資料收集**。
停用裝置清除動作	選擇以防止管理員清除裝置。 如果是使用者擁有 (員工擁有) 的裝置，請考慮選擇此選項。
提示使用者啟用定位服務	選取此項以允許使用者選擇性啟用允許或不允許使用位置服務的功能，包括根據需要定位裝置、Wi-Fi 和 MTD。 針對完全受管理裝置的情況，如果管理員選擇停用該選項，可自動授予此權限。
收集 App 庫存 **Android Enterprise 裝置 (7.0+) 的設定** 請配置下方設定，以進行 Android Enterprise 裝置的隱私權政策設	選擇**收集 App 庫存**，可收集裝置上安裝之所有 app 的相關資訊，不論 app 是否列在 App Catalog 中皆然。 選擇位於**應用程式目錄**中的**針對裝置上的應用程式**，可僅收集關於安裝在裝置上並存在於「應用程式目錄」中的那些應用程式的資訊。 選擇**裝置 App** 可收集裝置上所有 app 的相關資訊。 此選項適用於 Windows 10+ 裝置。 預設會顯示並選擇下列 app 來源類型庫存。 • **啟用非 App Store 庫存** - 適用於透過 MDM 推送或由一般使用者手動解壓縮 app 並直接本機安裝於裝置的內部開發 app (通用 app)。 • **啟用 App Store 庫存** - 適用於從 Microsoft Store 手動安裝或透過 Apps@work 店面安裝的 app。 • **啟用系統庫存** - 適用於報告為由 Microsoft 隨 Windows 10 OS 預先安裝的 app。 • **啟用 Win32 詳細目錄** - 適用於基於 System32 的應用程式，例如 MSI、EXE、Win32 市集應用程式等應用程式，這些應用程式透過 MDM 推送安裝，或由最終使用者直接安裝在裝置上。 您可以只選擇這些 app 來源類型庫存，收集可選 app 的相關資訊。 即使您沒有選擇非 App Store 或 Win32 應用程式詳細目錄，MDM 安裝的應用程式也會顯示在應用程式詳細目錄中。 當隱私權組態使用預設組態僅為 AppCatalog 收集應用程式詳細目錄時，同時也會收集 .EXE 詳細目錄。 當僅為 AppCatalog 應用程式收集時，必須一致地收集所有應用程式的詳細目錄。 應用程式目錄中可用的現代化、MSI 和 EXE 應用程式的詳細目錄；只有在分發至少一個屬於這些變體的應用程式時，才會被提取。

設定	方法
定。	
組織名稱	輸入管理裝置的組織名稱。
組織色彩	選擇使用者畫面背景應顯示的組織色彩。
簡短訊息	輸入當使用者嘗試使用管理員鎖定的功能時應顯示的簡短訊息。
完整訊息	輸入當使用者按一下簡短訊息時應顯示的完整訊息。 此訊息可提供使用者所受限制的相關詳細資料。
讓 Go 應用程式螢幕維持隱藏	從清單中選取 True 或 False。 • **True** - 在遠端分享期間，將隱藏 Ivanti Go 應用程式螢幕。 • **False** - 在遠端分享期間，將顯示 Ivanti Go 應用程式螢幕，用於提供故障排除方面的任何協助以及檢視說明文件。

如需更多資訊，請參閱如何建立配置

10.10.4.54. 用戶端隱私權聲明資訊

適用於： Android、Android Enterprise 和 iOS 裝置或支援的更新版本。

此配置可將隱私權聲明資訊發佈給 Go 用戶端中的使用者。 這是一項系統定義的配置；您僅可編輯發佈設定。

使用者可以查看的資訊包括與下列配置一起設定的詳細資料：

- 隱私權
  - 收集位置資料
  - 收集 app 庫存
  - Android 7.0+：
    - 組織名稱
    - 組織顏色
    - 短訊息
    - 長訊息
- 用戶端隱私權
  - SLC - 重大位置改變（Significant Location Change）以定期喚醒裝置
  - 依據喚醒定位的最短間隔
  - 啟用 MixPanel 狀態
- 行動裝置管理 - MDM 存取權 (不適用於使用者註冊的裝置)
  - 裝置鎖定與密碼移除
  - 裝置消除
  - 網路資訊 (電話/SIM 編號、MAC 位址)

10.10.4.55. Ivanti Go Client 設定

設定匿名終端使用者資料的收集，包括設備和使用資訊，以幫助識別產品問題並確保高服務品質。 此設定還可啟用支持連絡人配置選項。

建立 Ivanti Go 用戶端設定配寘

適用於：

- Mobile@Work macOS 1.67 或支援的更新版本。
- 適用於 iOS 3.5.0 或支援的更新版本的 Go。
- Mobile@Work for Android 12.9.0.0 或支援的較新版本。
- Go for Android 124 或支援的更新版本。

程序

1. 前往**組態** > **新增組態** > **Ivanti Go 用戶端設定**。 **建立 Ivanti Go 用戶端設定配寘**頁面出現。
2. 在**名稱**方格中輸入組態的名稱。
3. 輸入組態的**說明**。
4. 在**依據定位喚醒**下，選取**啟用 SLC** 選項。 顯著變更定位服務提供更強大的電力友善替代方案，它只會在使用者的位置顯著變更達 15 分鐘 (預設間隔) 以上時，才會提供定位更新給 Go for iOS app。 若啟用此服務，則發生位置變更時，Go app 會在背景中喚醒與登記。
5. 在**透過用戶端分析收集資料**下，選取**啟用分析**選項 (如果已禁用)。 預設啟用此選項。
6. 按**下一步**，確認發佈設定。
7. 按一下**完成**。

配置"支援"索引標籤的設定

適用於：

- Mobile@Work macOS 1.67 或支援的更新版本。
- 適用於 iOS 3.5.0 或支援的更新版本的 Go。
- Mobile@Work for Android 12.9.0.0 或支援的較新版本。
- Go for Android 124 或支援的更新版本。

程序

1. 前往**組態** > **新增組態** > **Ivanti Go 用戶端設定**。 **建立 Ivanti Go 用戶端設定配寘**頁面出現。
2. 在**名稱**方格中輸入組態的名稱。
3. 輸入組態的**說明**。
4. 在**平台**選項下，選擇相應平台。
5. 在**配置支援索引標籤設定**部分，按一下**"啟用支持選項卡"**。

> **啟用支援索引標籤**欄位僅適用於 iOS 裝置。

> 您可以啟用**支援索引標籤**，可啟用該索引標籤的 Go for iOS 版本為 118.0.0 或以上，Android 版本為 124 或以上。 早期版本的裝置將不會顯示或支援此功能。

在**支援連絡人設定**區段下，提供下列欄位:

- **索引標籤名稱** - 輸入 Ivanti 應用程式瀏覽中顯示的索引標籤的名稱。 預設值為「支援」。 (長度上限: 10 個字元)
- **終端使用者說明** - 輸入有關如何使用支持連絡人的說明。 (長度上限: 40 個字元)
- **新增聯絡人** - 按一下 **+新增**以新增聯絡人。 (最大聯絡人數: 5)
  - **名稱** - 輸入聯絡人姓名。 (長度上限: 20 個字元)
  - **電話號碼** - 輸入有效的電話號碼。 (帶國家/地區通話代碼)
- **新增 URL** - 按一下 **+新增**來新增 URL。 (最大 URL 數: 5)
  - **URL 名稱** - 輸入 URL 名稱。 (長度上限: 20 個字元)
  - **URL** - 輸入有效 URL。
- **附加訊息** - 在此處輸入要顯示的其他任何與支援相關的訊息。 (長度上限: 120 個字元)
- **電子郵件地址** - 輸入您可以傳送電子郵件尋求支持的電子郵件地址。 (長度上限: 40 個字元)

  > 您必須以格式 alias@domainname.com 輸入有效的電子郵件地址。

- **支援工單系統 URL** - 新增「**提交支援工單**」按鈕至 **Ivanti Go for iOS** 和 **Ivanti Go for Android** 應用程式中的**支援**索引標籤。 啟用切換以在支援索引標籤上顯示按鈕，並在提供的欄位中輸入適當的 URL，將使用者重新導向至您的支援系統。

  > 此 URL 用於 Ivanti Go **支援**索引標籤，將使用者重新導向至指定的支援系統。 為了提高安全性，建議使用以 *https://* 開頭的 URL，而非 *http://*。

按**下一步**，確認發佈設定。

8. 按一下**完成**。

有關更多資訊，請參閱組態。

10.10.4.56. Siri 設定

使用 **Siri 設定**在受監管的裝置上設定 Siri 設定。 此組態可協助管理員套用一致的原則型控制項，以管理裝置存取和使用 Siri 功能的方式。

適用於：

- 受監管的 iOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監管的 macOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監管的 watchOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監管的 visionOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監管的 tvOS 27+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取 **Siri 設定**組態。
3. 依下表設定各項 **Safari 設定**:

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
啟用	選取核取方塊以啟用 Siri。 切換**推播至裝置**按鈕，在受監管的裝置上啟用 Siri。
允許 Siri AI	選取核取方塊以啟用 **Siri AI** 特定功能。 切換**推送至裝置**按鈕，在受監管裝置上啟用 **Siri AI** 特定功能。
允許使用者產生的內容	選取核取方塊以啟用使用者產生的內容。 切換**推播至裝置**按鈕，以啟用受監管裝置上的使用者產生的內容。 此設定不適用於 macOS 和 visionOS 裝置。
允許「鎖定時」	選取核取方塊以啟用「鎖定時」。 切換**推播至裝置**按鈕，以在受監管裝置上啟用「鎖定時」。 此設定不適用於 macOS 和 visionOS 裝置。
強制粗俗內容篩選器	選取核取方塊以啟用強制粗俗內容篩選器。 切換**推播至裝置**按鈕，在受監管的裝置上啟用強制粗俗內容篩選器。 此設定不適用於 visionOS 裝置。
強制減少敏感內容	選取核取方塊可強制 Siri 減少敏感內容。 切換**推送至裝置**按鈕，強制 Siri 減少受監管裝置上的敏感內容。

4. 按**下一步**，確認發佈設定。
5. 選取其中一個發佈選項以設定 **Safari 設定**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
6. 按一下**完成**。

10.10.4.57. 服務組態檔案組態

復位組態檔案組態管理員用於為註冊的裝置上的各種系統服務集中管理和部署組態檔案。 此外，管理員可以透過在防篡改環境中將檔案傳遞到安全的、特定於服務的目錄來確保服務設定保持一致，並防止未經授權的修改。

適用於: macOS 裝置

在您開始之前:

- 您可以用 *ZIP* 檔案格式上傳各種組態。 有關新增檔案的更多資訊，請參見檔案。
- 擴展存檔中的所有檔案都設定為 *-r-r-r- unix* 檔案權限。 封存中的任何連結都將限於引用服務特定位置內的檔案。
- zip 封存中的檔案需要反映服務期望從檔案系統根目錄開始出現的資料夾結構和組態檔。 該服務僅使用聲明提供的檔案，而忽略其預設目錄中的檔案。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取**服務組態檔案**組態。
3. 依下表配置**服務組態檔案**設定:

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
選取檔案	輸入檔案名稱。
選擇服務類型	從下拉式清單中選取一個**服務類型**: • SSHD • SUDO • PAM • CUPS • HTTP_D • BASH • ZSH

4. 按**下一步**，確認發佈設定。
5. 選取其中一個發佈選項以設定**服務組態檔案**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
6. 按一下**完成**。

10.10.4.58. 軟體更新

適用於：

- iOS 10.3 至 26.0 以及 tvOS 12.0 至 26.0 受監管裝置
- macOS 裝置
- Windows 10+ 裝置

建立並發佈作業系統更新的規則。

本節包含以下各主題：

- 設定 iOS/tvOS 裝置的軟體更新
- 設定非 DEP macOS 裝置和 DEP macOS 裝置的軟體更新
- 設定 Windows 裝置的軟體更新
- 使用宣告式裝置管理進行軟體更新強制執行

設定 iOS/tvOS 裝置的軟體更新

程序

若要允許將 OS 更新傳送給處於受監管模式的 iOS/tvOS 裝置：

1. 前往**配置**。
2. 按一下 **+新增**。
3. 按一下**軟體更新**。
4. 按一下 **iOS/tvOS** 以檢視「配置設定」區段。
5. 選擇**允許在受監管裝置上自動安裝作業系統更新**選項。
6. 請選擇下列選項之一：
    - 更新至最新版本
    - 更新至指定版本 - 例如，輸入 11.3.0 做為 iOS 版號。
7. 選擇下列其中一項安裝動作：
    - 預設
    - 僅下載
    - 儘快安裝
8. 選擇下列更新時間選項：
    - 開始時間
    - 結束時間
    - 時區
9. 按**下一步**。
10. 選擇**啟用此配置**選項。
11. 請選擇下列發佈選項之一：
    - 所有裝置

- 沒有裝置 (預設)
- 自訂

12. 按一下**完成**。

- 為 iOS 裝置安裝特定作業系統更新版本時，您必須選擇適用此裝置的版本。 如果您選擇無效或不適用的版本，將會忽略裝置的軟體更新。
- 如果裝置有密碼，在 MDM 傳送更新至裝置後，裝置會佇列更新，並提示使用者輸入密碼以開始安裝。
- 啟用 **iOS 限制**中的 `enforcedSoftwareUpdateDelay` ，可確保在裝置上手動掃描軟體更新時不會刪除此組態所下載的特定版本。

設定非 DEP macOS 裝置和 DEP macOS 裝置的軟體更新

「裝置註冊」設定檔屬於 Apple Business Manager 的一部分，可讓客戶大量購買裝置，並於啟動期間在 MDM 中自動註冊裝置。 如需詳細資訊，請參閱**裝置註冊**。

以下程序可協助您將作業系統更新傳送至非 DEP macOS 和 DEP macOS 裝置。

程序

1. 前往**配置**。
2. 按一下 **+新增**。
3. 按一下**軟體更新**。
4. 按一下 **macOS** 以檢視「配置設置」區段。
5. 選擇**啟用 macOS 軟體更新**選項。
6. 選擇裝置的更新類型。 對於每一種更新，您還可選擇無需重新啟動的更新。
   - 作業系統更新
   - 重要更新
   - 設定資料更新
   - 韌體更新
   - 非重要更新

     > 管理員可啟用**啟用非重要更新**，以管理 (安裝/排程) 非重要 macOS 更新。 針對現有的租戶此選項預設為停用，如有需要，必須由管理員在明確升級後啟用。

     > 在**作業系統更新**中，管理員可將裝置更新至特定 macOS 版本。

     > 所有 macOS 更新都可使用以下動作設定：

     - 預設
     - 僅通知
     - 稍後安裝
     - 安裝強制重新啟動
     - 僅下載
     - 儘快安裝
   -

可能的值 - 低、高

預設 - 低

優先順序

- 使用者延遲上限
  可能的值 - 整數
  只有選取「稍後安裝」選項時才支援。

7. 選擇下列更新時間選項：
   - 開始時間
   - 結束時間
   - 時區
8. 按**下一步**。
9. 選擇**啟用此配置**選項。
10. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂
11. 按一下**完成**。

設定 Windows 裝置的軟體更新

程序

若要設定您的 Windows 安裝更新排程：

1. 前往**配置**。
2. 按一下 **+新增**。
3. 按一下**軟體更新**。
4. 按一下 **Windows** 以檢視「配置設置」區段。
5. 依據您的 Windows 裝置版本，輸入下列選項。
6. 按**下一步**。
7. 選擇**啟用此配置**選項。
8. 請選擇下列發佈選項之一：
   - 所有裝置
   - 沒有裝置 (預設)
   - 自訂

按一下**完成**。

Windows 10+ 裝置的軟體更新

- 更新來源 - 選擇下列其中一個來源：
  - 企業 WSUS

- Microsoft Update 及/或 Enterprise WSUS

驅動程式更新來源

- 功能更新來源
- 其他更新來源
- 品質更新來源
- 企業 WSUS 伺服器的 URL
- 替代的內部網路 Microsoft 更新伺服器
- 允許來自「信任的發行者」的更新 - 將更新來源限制為僅限信任的發行者。
- 自動更新策略 - 從下拉式清單選擇下列其中一個選項。
- 排程安裝日期 - 設定更新的頻率。
- 排程安裝時間 - 選擇更新的安裝時間。
- 允許計量付費連線下載更新 - 啟用或停用此選項。
- 不允許更新延遲原則引發 Windows Update 掃描 - 啟用或停用此選項。
- 預約的重新啟動期限 - 選擇重新啟動期限的天數。
- 延遲預約的重新啟動期限 - 選擇延遲預約的重新啟動期限天數。
- 預約的重新啟動轉換排程 - 選擇重新啟動轉換排程的天數。
- 更新/填滿空白的內容 URL。
- MO App 下載限制 - 請選擇下列選項之一：
  - 不要忽略 app 及其更新的 MO 下載限制
  - 忽略 app 及其更新的 MO 下載限制 (允許無限下載)
- MO 更新下載限制 - 請選擇下列選項之一：
  - 不要忽略作業系統更新的 MO 下載限制
  - 忽略作業系統更新的 MO 下載限制 (允許無限下載)
- 管理預覽組建版本 - 請選擇下列選項之一：
  - 停用預覽組建版本
  - 在下一個發行版本戈開時停用預覽組建版本
  - 啟用預覽組建版本
- 自動重新啟動更新的警告通知排程 - 選擇自動重新啟動警告通知前的等待分鐘數。
- 重新啟動警告提醒 - 選擇要設定重新啟動警告提醒的小時數。
- 自動更新排程 - 選擇自動更新的頻率。
- 自動啟動更新通知 - 開啟自動啟動更新通知。
- 產品版本 - 輸入 Windows 更新版本頁面 (URL: aka.ms/WindowsTargetVersioninfo) 上所列的產品版本。 例如，「Windows 11」或「11」或「Windows 10」。
- 目標發行版本 - 在 Windows 更新版本頁面上輸入目標發行版本。
- 活動時間開始 – 如果啟用此選項，則在活動時間期間更新後，將不會自動重新啟動電腦。 在活動時間之外，電腦將嘗試重新啟動。
- 活動時間結束 – 如果啟用此選項，則在活動時間期間更新後，將不會自動重新啟動電腦。 在活動時間之外，電腦將嘗試重新啟動。
- 活動時間最大範圍 – 啟用此選項可指示從開始時間起使用者可設定其活動時間的時數上限。

- 活動時間內沒有更新通知 – 更新通知選項見下文。
  - 預設 Windows Update 通知
  - 關閉所有通知，不包括重新啟動警告
  - 關閉所有通知，包括重新啟動警告
- 停用驅動程式更新 – 啟用此選項可排除具有 Windows 品質更新的驅動程式。 如果停用或不設定此選項，Windows Update 將包含具有驅動程式分類的更新。
- 品質更新截止日期 – 在裝置上自動安裝品質更新前的天數，與活動時間無關。
- 品質更新截止日期寬限期 – 從更新安裝到品質更新自動重新啟動的天數下限。
- 功能更新截止日期寬限期 – 功能更新自動部署到裝置前的天數，與活動時間無關。
- 功能更新截止日期寬限期 – 功能更新自動部署到裝置前的天數下限，與活動時間無關。
- 在寬限期結束之前不要自動重新啟動 - 啟用後，即使更新已準備好重新啟動，裝置也不會在截止日期之前和寬限期過後，在活動時間之外自動重新啟動。 停用後，如果更新可在截止日期之前重新啟動，則可以在活動時間之外嘗試自動重新啟動。

Windows 10.0.14393 之前版本裝置的軟體更新

如果裝置已停用「遙測限制」，以下設定就沒有作用：

- 暫停升級/更新 - 開啟此選項以將變更延遲至稍後的日期
- 延後更新 - 選擇延遲至最長 4 週
- 延後升級 - 開啟此選項以延後升級
- 延後升級 - 選擇延遲至最長 8 個月

Windows 10.0.14393+ 裝置的軟體更新

- 從中安裝更新的分支 - 允許 IT 管理員設定裝置從哪個分支接收更新。 「從中安裝更新的分支」欄位包含以下選項:
  - Windows Insider 組建版本 – 快速
  - Windows Insider 組建版本 – 慢速
  - 發佈 Windows Insider 組建版本
  - 半年通道 (目標)
  - 半年通道
  - 僅發佈品質更新預覽版
  - Canary Channel

功能更新 (升級) - 僅在 Windows Professional、Windows Enterprise 和 Windows Education 中受支援。

  - 暫停更新
  - 延後 - 選擇延遲至最長 180 天。

品質更新 (更新) - 僅在 Windows Professional、Windows Enterprise 和 Windows Education 中受支援。

  - 暫停更新
  - 延後 - 選擇延遲至最長 30 天。

Windows 10.0.17083+ 裝置的軟體更新

- 功能更新：
  - 功能更新解除安裝期限 - 選擇解除安裝功能更新前的等待天數。

Windows 10.0.17763+ 裝置的軟體更新

- 停用使用者的「暫停更新」存取權
- 停用使用者的 UXWU 存取權 (Windows Update 掃描、下載及安裝)
- 管理通知等級 - 請選擇下列選項之一：
  - 使用預設 Windows Update 通知
  - 關閉所有通知，不包括重新啟動警告
  - 關閉所有通知，包括重新啟動警告
- 功能更新：
  - 自動重新啟動安裝更新前的等待期限 - 選擇自動重新啟動安裝更新的等待期限天數。
  - 預約的重新啟動期限 - 選擇預約的重新啟動期限天數。
  - 延遲預約的重新啟動期限 - 選擇延遲預約的重新啟動期限天數。
  - 預約的重新啟動轉換排程 - 選擇重新啟動轉換排程的天數。

使用 DDM 進行軟體更新強制執行

管理員可以使用 DDM，在 iOS、macOS 和 iPadOS 裝置上強制安裝軟體更新。

支援:

- iOS 17+
- iPadOS 17+
- macOS 14+

程序

1. 從「組態」區段建立**軟體更新強制執行**組態。
2. 執行強制簽入以確保裝置上已安裝「軟體更新強制執行」組態。

當您開啟裝置時，您應該會看到有關所需軟體更新的通知，其中包含版本號碼、所需日期等詳細資訊。

> 如果您不想要強制執行軟體更新，則需要將組態發佈選項設為**無**。

針對軟體更新強制執行組態發佈述詞

1. 建立「軟體更新強制執行」組態。
2. 將切換開關「使用述詞啟用」設定為「開」，並使用 + 按鈕以包含述詞 (根據需要)。



若要編輯或刪除述詞，請前往**管理員** > **Apple** > **述詞**。 您可以在此頁面中找到可用述詞的清單。 按一下**編輯**，即可對現有述詞進行任何變更並儲存。 同樣，若要刪除現有述詞，請選取該述詞並按一下**刪除**。

> 如果述詞與任何組態相關聯，則無法將它刪除。

10.10.4.59. 軟體更新設定組態

Ivanti Neurons for MDM 可讓您建立「軟體更新強制執行設定」，並定義對一般使用者的更新行為以掌控步調和延遲。

適用於：

- 受監督的 iOS 18.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監督的 macOS 15.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取**軟體更新設定**組態。
3. 依下表設定**軟體更新設定**的各項設定:

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
iOS 18+ 受監督和 **macOS15+**	
測試版註冊 程式註冊 (可選)	請選擇下列選項之一： • **允許**: 使用者可以註冊與其登入的 Apple 帳戶相關的任何適用的測試版程式。 • **一律開啟**: 使用此組織指定的測試版程式，使用者無法使用登入的 Apple 帳戶註冊測試版程式。 **提供程式** - 使用「提供程式」，您可以強制執行所需的程式。 強制執行時，您可以設定 iOS 與 macOS 裝置所需的版本。 **需要程式** - 裝置會自動註冊此測試版程式。 • **一律關閉**: 裝置不允許註冊任何測試版程式。 如果已註冊，系統會從任何測試版程式中刪除裝置。
iOS 18+ 受監督和 **macOS15+ 受監督**	
通知 自動動作 下載 安裝作業系統更新	選取**通知**核取方塊和**顯示所有軟體更新強制執行通知**核取方塊，以在使用者裝置中顯示所有軟體更新強制執行通知。 如果您僅勾選**通知**核取方塊，裝置將在強制執行截止日期前一小時顯示單一強制執行通知。 如果您未選取任何核取方塊，裝置會顯示觸發的通知，以顯示使用者裝置中所有軟體更新強制執行通知。 請選擇下列選項之一： • **允許**: 使用者可以「開啟」或「關閉」自動下載。 • **一律開啟**: 使用者的自動下載一律為「開啟」。 • **一律關閉**: 使用者的自動下載一律為「關閉」。 請選擇下列選項之一： • **允許**: 使用者可以「開啟」或「關閉」自動安裝作業系統更新。 • **一律開啟**: 使用者的自動安裝作業系統更新一律為「開啟」。 • **一律關閉**: 使用者的自動安裝作業系統更新一律為「關閉」。
背景安全性改進	
背景安全性改進	選取**背景安全性改進**核取方塊以控制更新的安裝和復原。 選擇下列選項： • **啟用**：如果選取此選項，會為使用者提供**背景安全性改進**安裝。 • **啟用復原**：如果選取，會向使用者提供**背景安全性改進**復原。
執行 iOS 18 以上版本的受監管裝置 建議的步調	 若有多個可用的更新，請選取下列其中一個選項來對使用者顯示軟體更新:

設定	描述
	• **全部**: 顯示所有軟體更新版本。 • **最舊**: 僅顯示最舊 (編號較低) 的軟體更新版本。 • **最新**: 僅顯示最新 (編號最高) 的軟體更新版本。
延遲	您可以選擇延後所有受監督裝置的軟體更新。 您無法延遲**背景安全性改進**。
合併週期 (以天為單位) **執行 macOS 15 以上版本的受監管裝置**	設定延後裝置上主要或次要系統更新的天數。 設定完成後，主要或次要軟體更新將在發行後經過此指定天數時顯示。 您可以設定 1 到 90 天之間的任意值。
允許標準使用者作業系統更新	選取**允許標準使用者作業系統更新**核取方塊，以允許使用者執行作業系統更新。 選取**允許標準使用者執行主要和次要軟體更新**核取方塊，以允許標準使用者執行次要和主要軟體更新。 如果您未選取此核取方塊，則只有管理員能夠執行次要和主要軟體更新。
延遲 主要更新週期 (以天為單位)	設定延後裝置上主要作業系統軟體更新的天數。 設定完成後，主要軟體更新將在發行後經過此指定天數時顯示。 您可以設定 1 到 90 天之間的任意值。
次要更新週期 (以天為單位)	設定延後裝置上的次要作業系統軟體更新的天數。 設定完成後，主要軟體更新將在發行後經過此指定天數時顯示。 您可以設定 1 到 90 天之間的任意值。
系統更新週期 (以天為單位) 自動動作 安裝安全性更新	設定延後裝置上系統作業系統更新的天數。 設定完成後，主要軟體更新將在發行後經過此指定天數時顯示。 您可以設定 1 到 90 天之間的任意值。 請選擇下列選項之一： • **允許**: 使用者可以「開啟」或「關閉」安全更新的安裝。 • **一律開啟**: 使用者的安全更新安裝一律為「開啟」。 • **一律關閉**: 使用者的安全更新安裝一律為「關閉」。

4. 按**下一步**，確認發佈設定。
5. 選取其中一個發佈選項以設定**軟體更新設定**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
6. 按一下**完成**。

10.10.4.60. 安全性喜好設定配置

管理員可透過安全性喜好設定配置，來管理和控制使用者對裝置的防火牆設定、鎖定訊息和密碼進行變更。

適用於：macOS 10.10+

Procedure

1. 前往配置 > +新增。
2. 在搜尋欄位中安全性，然後按一下安全性偏好設定配置。
3. 輸入配置的名稱和描述。
4. 選擇所需的配置：
    - 停用對防火牆設定進行變更
    - 停用對鎖定訊息進行變更
    - 停用對密碼進行變更
5. 按下一步。
6. 選擇啟用此配置選項。
7. 選擇以下一個要套用配置的通道選項：
    - 裝置通道 (最常用)
    - 使用者通道 (目前註冊的使用者)
8. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂。
9. 按一下完成。

10.10.4.61. 時間伺服器

適用於：macOS 10.12.4 和支援的更新版本。

建立「時間伺服器」配置，以讓裝置連接自訂的時間伺服器。

建立「時間伺服器」配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入**時間**，然後按一下**時間伺服器**配置。
4. 輸入配置的名稱和描述。
5. 指定 **NTP 伺服器**。
6. 以 Olson 時區 ID 格式，指定**時區**字串 (例如，Pacific/Midway)。 若要取得 Olson 時區格式，請在管理員的 macOS 裝置上執行 `"/usr/sbin/systemsetup -listtimezones` " 命令。
7. 按**下一步**，確認發佈設定。
8. 按一下**完成**。

如需更多資訊，請參閱如何建立配置

10.10.4.62. Web 內容篩選

授權：Silver

Web 內容篩選器組態限制了 iOS 7+、macOS 10.15+ 和 visionOS 1.1+ 裝置的網路存取。

Web 內容篩選設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
允許的網站	**限制成人內容**：如果您要依據 iOS 自動篩選來封鎖網站，請選擇此選項。 這些篩選會嘗試以高度精準的方式來封鎖含有不當內容的網站。 **僅限特定網站**：如果您想手動提列可存取的網站，請選擇此選項。 **外掛程式 (僅限 iOS8 受監管版本和 macOS 10.15+):** 選取此選項以使用第三方外掛程式。
允許的 URL   <

設定	方法
組織	僅有當您選擇「外掛程式」時才可使用此選項。 選用：輸入外掛程式所需的任何組織字串。 請參閱外掛程式的文件，以決定是否需要使用此值。
使用者名稱	僅有當您選擇「外掛程式」時才可使用此選項。 選用：輸入外掛程式服務所需的任何使用者名稱。 請參閱外掛程式的文件，以決定是否需要使用此值。
密碼	僅有當您選擇「外掛程式」時才可使用此選項。 選用：輸入外掛程式服務所需的任何密碼。 請參閱外掛程式的文件，以決定是否需要使用此值。
認證	僅有當您選擇「外掛程式」時才可使用此選項。 選用：輸入外掛程式服務用來驗證使用者所需的任何認證。 請參閱外掛程式的文件，以決定是否需要使用此值。
篩選 Webkit 流量	僅有當您選擇「外掛程式」時才可使用此選項。 選擇在篩選中包括 Webkit 流量。
篩選 Socket 流量	僅有當您選擇「外掛程式」時才可使用此選項。 選擇在篩選中包括 Socket 流量。
自訂資料	僅有當您選擇「外掛程式」時才可使用此選項。 選用：新增外掛程式服務所需的任何金鑰/值配對。 請參閱外掛程式的文件，以決定是否需要使用此值。

如需更多資訊，請參閱**如何建立配置**。

10.10.4.63. Windows 防火牆

Windows 防火牆配置用來設置 Windows 防火牆描述檔設定，以及要在裝置上強制執行的自訂規則集。 此配置可用來管理非網域裝置，並針對連接企業網路的所有系統降低網路安全威脅的風險。

設定 Windows 防火牆配置

程序

1. 前往**組態 > +新增**。
2. 選取**防火牆**組態。
3. 按一下 **Windows** 圖示。
4. 輸入配置的名稱。
5. 輸入該防火牆組態的說明。
6. 在「組態設定」區段中，按照下表所述指定其餘設定。

設定	方法
描述檔	
啟用	將切換滑到「開啟」以啟用描述檔。
類型	顯示描述檔的類型。 例如：網域。
預設入埠動作	選擇應針對入埠流量執行的預設動作選項。 **允許**：允許流量 **封鎖**：封鎖流量。
預設出埠動作	選擇應針對出埠流量執行的預設動作。 **允許**：允許流量 **封鎖**：封鎖流量。

7. 若要新增規則，請按一下 **+新增**，然後進行下列設定:

設定	方法
規則	
開	滑動切換以啟用描述檔。
規則名稱	輸入可識別此規則的名稱。
描述	輸入可說明此規則用途的描述。
方向	選擇規則應套用的流量方向： • **入埠**：入埠流量 • **出埠**：出埠流量 • **雙向**：兩個方向。
動作遊戲	選擇要執行的動作 • **允許**：允許流量 • **封鎖**：封鎖流量。
描述檔	選擇規則應套用的描述檔： • **全部** • **網域** • **私人** • **公用**
應用程式	輸入套件系列名稱 (PFN) 或 app 的執行路徑。
通訊協定	選擇規則應套用的通訊協定： • **TCP** • **UDP** • **ICMP**
本機位址範圍	輸入本機 IPv4/IPv6 位址範圍或子網路遮罩。
本機連接埠範圍	輸入以逗號分隔的本機連接埠或連接埠範圍清單。 例如：20,50,100-120。
遠端位址範圍	輸入遠端 IPv4/IPv6 位址範圍或子網路遮罩。
遠端連接埠範圍	輸入以逗號分隔的本機連接埠或連接埠範圍清單。 例如：20,50,100-120。
介面類型	選擇下列其中一個介面類型選項： • **全部** • **遠端存取** • **無線** • **LAN**

設定	方法
	• **行動寬頻** 若未選擇「介面類型」選項，則套用預設選項**全部**。

8. 按**下一步**。
9. 請選擇下列發佈選項之一：
   - 所有裝置
   - 沒有裝置 (預設)
   - 自訂
10. 按一下**完成**。

10.10.4.64. Windows 資訊保護

授權：Gold

適用於：Windows 10+

Windows 資訊保護 (WIP) 配置定義 WIP 設定以保護企業資料。 此配置適用於登記接受管理的裝置。 您也可以在已設好裝置的概覽頁面上，檢視該裝置的 WIP 詳細資料。

設定 Windows 的 Windows 資訊保護

程序

1. 前往**組態 > +新增**。
2. 選擇 **Windows 資訊保護**組態。
3. 輸入組態的名稱。
4. 輸入描述。
5. 在「組態設定」區段中，按照下表所述指定其餘設定。
6. 按一下**下一步**。
7. 選擇此組態的發佈方式。

類別	設定	方法
	名稱	輸入可識別此配置的名稱。
	描述	輸入可說明此配置用途的描述。
企業資訊	**所有版本 (Windows 10+)**	
	受保護的網域名稱	指定要設定資料保護原則的身份清單。 與這些身分關聯的電子郵件和其他資料，將視為企業資料並受到保護。 • 這是以 | 分隔的網域清單，清單中的第一個網域視為 Windows UI 用途的主要身份。 • 例如：「domain1.com|domain2.co.uk」
	網路網域名稱	指定包含企業界限的網域。 來自這些網域之一並傳送到裝置的資料，將視為企業資料並受到保護。 • 這些位置將視為可與其共享企業資料的安全目的地。 • 這是以逗號分隔的網域清單。 • 例如："mail.domain3.com, domain4.com"
	雲端資源	包含需要受到保護的雲端代管企業資源網域清單。 這些資源的連線視為企業資料。 指定一個或多個網域名稱，並在括弧中註明選用的 Proxy 位址。 • 例如：「domainname1.com, domainname2 (10.0.0.1)」。 • 如果 Proxy 與雲端資源配對，則雲端資源的資料流量將透過指定的 Proxy 伺服器 (在連接埠 80)，經由企業網路遞送。 • 此欄位中指定的所有 Proxy 位址也應輸入下列「內部 Proxy 伺服器」欄位中。
	IP 範圍	設定定義企業網路電腦的企業 IP 範圍。 來自那些電腦的資料將視為企業的一部分並受到保護。 這些位置將視為可與其共享企業資料的安全目的地。 這是以逗號分隔的 IPv4 和 IPv6 範圍清單。 • 這是以逗號分隔的 IPv4 和 IPv6 範圍清單。 • 當用戶端必須接受設好的清單而不使用 Heuristic 以嘗試搜尋其他子網路時，請選擇 **IP 範圍是權威**選項。
	中性資源	指定可用於工作或個人資源的網域名稱清單。
	Proxy 伺服器	指定以逗號分隔的 Proxy 伺服器清單。 此清單上的任何伺服器皆視為非企業。 • 例如：「157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59」。 • 當用戶端必須接受設好的 Proxy 清單而不嘗試偵測其他的 Work Proxy 時，請選擇 **Proxy 伺服器是權威**選項。
	內部 Proxy 伺服器	指定以逗號分隔的內部 Proxy 伺服器清單。 • 例如：「157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59」。

類別	設定	方法
		• 這些 Proxy 是管理員設定好，用於連接網際網路上的特定資源。 它們視為企業網路位置。 這些 Proxy 僅用於設定 EnterpriseCloudResources 原則，以強制資料流量透過這些 Proxy 遞送到雲端資。
資料保護	**所有版本 (Windows 10+)**	
	施行等級	選擇下列其中一個施行等級。 • 關閉 - 不保護 (之前加密的資料將不使用加密)。 • 無訊息自動執行 - 加密資料並在資料受到保護之後稽核裝置上的活動。 系統不會針對任何負面資料/app 資訊提示帳號使用者。 • 覆寫 - 類似於無訊息自動執行模式。 但是，如果 app 或資料使用不正確，系統會提示使用者選擇繼續或取消使用者正在執行的作業。 • 封鎖 - 類似於無訊息自動執行模式。 但是，如果 app 或資料使用不正確，系統會封鎖使用者正在執行的作業，同時警告使用者並提供封鎖作業的原因。 除了「關閉」模式，裝置將會記錄不應該使用企業資料或資源的所有資料或 app。 您可使用其他配置服務提供者 (CSP) 來移除該資料。
	資料復原憑證	指定可用於加密檔案資料還原的還原憑證。 • 這與用於加密檔案系統 (EFS) 的資料復原代理程式 (DRA) 憑證相同。 不過，此憑證是透過 MDM 提供，而不是透過「群組原則」。 您也可以選擇下列一或多個選項： • 允許使用者解密 • 於取消註冊時撤銷 • 顯示 EDP 圖示 • 鎖定時需要保護 (僅限 Windows 10 行動裝置版)
RMS	**所有版本 (Windows 10+)**	
	允許 Azure RMS	指定是否允許 WIP 使用 Azure Rights Management (Azure RMS) 加密。
	RMS 範本 ID	指定 TemplateID GUID 以使用 RMS 加密。 RMS 範本允許管理員設定誰有權存取受 RMS 保護的檔案與權限期間等詳細資料。
應用程式控制	**所有版本 (Windows 10+)** 針對在 **App > 應用程式目錄**頁面中建置的 app 集合，指定一個 WIP 值。 針對使用下列參數集的 app，指定規則定義。	
	App 類型	選取以下應用程式類型之一: • 發行者/PFN 等於 - 適用於支援 PFN 的 Windows 10+。 • EXE/Win32 等於 - 僅適用於 Windows 桌面。

類別	設定	方法
	App 識別碼	從顯示的選項中選擇 app，並將其新增至「App 識別碼」。 您也可以按一下**查閱 App**。
	App 描述	輸入 app 的描述。

10.10.4.65. Windows 限制

Windows 限制决定了 Windows 10+ 装置上啟用哪些功能。

Windows 限制設定

類別	設定	方法
	名稱	輸入可識別此配置的名稱。
	描述	輸入可說明此配置用途的描述。
裝置功能	**所有版本 (Windows 10+)**	
	停用 Wi-Fi 卸載	選擇防止裝置存取相容的網路並將預期用於獲授權之無線網路的資料攜出。
	停用網際網路共享	選擇防止裝置透過其他無線裝置來存取網際網路。
	停用位置	選擇停用位置服務。
	停用行動數據漫遊	選擇在裝置處於行動網路模式時停用數據漫遊。
	停用 Bluetooth	選擇防止裝置建立 Bluetooth 連線。
	漫遊或使用行動網路時停用 VPN	選擇當裝置不在 WiFi 模式時防止裝置建立 VPN 連線。
	停用 Wi-Fi 手動組態	選取此項可防止使用者在裝置上手動設定 Wi-Fi 設定。
	停用 Wi-Fi	選取此項可允許或拒絕 WiFi 連線。
遙測 - 允許裝置傳送診斷和使用狀況遙測資料。	**僅限 Windows 10**	
	遙測層級	選擇下列四種資料報告的遙測層級之一： • **安全性** - 傳送「已連線使用者體驗」、「遙測元件設定」、「惡意軟體移除工具」和 Windows Defender 的相關資訊。 • **基本** - 傳送基本的裝置資訊，包括與品質相關的資料、app 相容性、app 使用量資料，以及來自「安全性」層級的資料。 • **增強型** - 傳送詳細資訊，包括 Windows、Windows Server、System Center 和 app 的使用量和效能。 亦包括進階的穩定性資料，以及來自「基本」和「安全性」層級的資料。 • **完整 (預設)** - 所有用來識別並協助修正問題的資料，以及來自「安全性」、「基本」和「增強型」層級的資料。
預防資料遺失 (DLP)	**所有版本 (Windows 10+)**	
	停用相機	選擇防止使用者使用相機 app。
	停用儲存卡 (SD) 的存取	選擇防止裝置存取儲存卡。
	停用畫面擷取 (僅限桌面)	選取此項可防止使用裝置內的螢幕擷取應用程式來擷取畫面。
	停用 USB 大容量儲存裝置 (僅限 HoloLens)	選取此項可防止 HoloLens 存取大容量儲存裝置。

類別	設定	方法
數據用量	**Windows 10+**	
	3G 連線的成本	請選擇下列選項之一： • **無限制** - 連線無限制，也不受限於用量費用和容量限制。 • **固定** - 連線在超出特定數據限制後，將受限於用量費用和容量限制。 • **變動** - 連線按位元組數量收費。
	4G 連線的成本	
Defender	**Windows 10+**	
	停用 Defender 即時監控功能	選擇停用 Defender 即時監控功能
DeviceGuard	**Windows 10+**	
	停用虛擬式安全性 (VBS)	選擇防止虛擬式安全性提供安全性服務支援。
	Credential Guard 與虛擬式安全性	請選擇下列選項之一： • **停用** - 停用 Credential Guard 與虛擬式安全性。 • **啟用並搭配 UEFI 鎖定** - 啟用 Credential Guard 與虛擬式安全性，並搭配 Unified Extensible Firmware Interface (UEFI) 鎖定。 • **啟用但無鎖定** - 啟用 Credential Guard 與虛擬式安全性，但沒有 (UEFI) 鎖定。
	平台安全性層級 (需要平台安全性功能)	請選擇下列選項之一： • **VBS 與安全開機** - 選擇此選項以啟用虛擬式安全性與安全開機。 • **VBS、安全開機與直接記憶體存取** - 選擇此選項以啟用虛擬式安全性、安全開機與直接記憶體存取。
隱私權	**Windows 10+**	
	停用廣告 ID	選擇停用廣告 ID。
	進行停用以發佈 App/作業系統所饋送的活動	選擇防止 App/作業系統發佈至活動摘要。
Windows 及應用程式	**所有版本 (Windows 10+)**	
	停用 Microsoft 電子郵件以外的服務帳戶	選擇防止使用者使用 Microsoft 帳戶來進行非電子郵件的服務驗證。
	停用非 Microsoft 帳戶	選擇防止使用者使用非 Microsoft 帳戶來設定電子郵件。
	停用 Cortana 個人助理	選擇防止使用者存取 Microsoft 的個人助理。
	停用以位置為基礎的搜尋	選擇防止使用裝置位置進行搜尋。

類別	設定	方法
	停用開發人員解鎖	選擇防止使用者啟用 app 互傳。 當裝置註冊 MDM 時，其預設模式為啟用側載。
	僅限 11+ 支援的版本	
	在工作列上設定 Teams Chat 圖示	請選擇下列選項之一： • **顯示：**預設圖表圖示會出現在工作列上。 使用者可在「設定」中顯示或隱藏它。 • **隱藏：**預設會隱藏圖表圖示。 使用者可在「設定」中顯示或隱藏它。 • **停用：**不顯示圖表圖示，且使用者無法在「設定」中顯示或隱藏它。 • **未設定：**圖表圖示的行為會根據您 Windows 版本的預設設定。 必須等到 Windows 裝置重新啟動後，變更才會生效。
	僅限 Windows 10+ 支援的版本	
	停用自動更新來自 Microsoft Store 的 app 停用啟動先前安裝或下載之所有來自 Microsoft Store 的 app	選擇以防止從 Microsoft Store 自動更新 app。 選擇以防止一般使用者啟動先前安裝或下載之所有來自 Microsoft Store 的 app。僅支援 Enterprise 和 Education Windows 版本。
	讓 app 在背景中執行	請選擇下列選項之一： • **使用者控制**：允許使用者控制在背景執行的 app。 • **強制允許**：允許在背景執行 app。 • **強制拒絕**：防止在背景執行 app。
其他限制	**所有版本 (Windows 10+)**	
	停用從 UEM 取消註冊與刪除 Workplace 帳戶的功能。 禁止使用者設定裝置鎖定寬限期 (僅限 HoloLens)。	選擇防止使用者從 UEM 取消註冊與刪除公司帳戶影像。 選取此項可防止使用者設定裝置鎖定寬限期。
	僅限 Windows 10+ 支援的版本	
	停用使用者透過控制台及硬體按鍵組合，將裝置還原為出廠設定 要求使用者在裝置設定期間連接到網路 (需要 Autopilot 設定檔)	選擇時，可防止使用者設定裝置鎖定的寬限期。 選擇此選項可啟用 TenantLockdown 以鎖定使用 Autopilot 功能註冊的所有 Windows 裝置。

類別	設定	方法
	僅限 Windows 11+ 支援的版本 停用使用者透過使用者介面對 eSIM 進行變更。	選取此選項以限制使用者對 eSIM 描述檔進行任何變更。

10.10.4.66. Windows Desktop 的限制

適用於：Windows 10+ Desktop

本節包含以下各主題：

- 設定 Windows Desktop 限制
- 建立抽取式儲存裝置允許清單

管理員可限制使用者存取裝置上的以下區域，藉此控制受管理 Windows 10 Desktop 裝置的相關作業系統資訊：

- 控制台
- 工作管理員
- 檔案總管
- 登錄編輯程式

上述功能可讓使用者大幅度變更他們的裝置。 管理員可利用此功能來限制存取系統層級的控制項，藉此保護存取安全。

此功能需要 Bridge。 請參閱 Ivanti Bridge 以取得詳細資料。

設定 Windows Desktop 限制

程序

1. 前往**配置 > +新增**。
2. 選擇 **Windows Desktop 限制**配置。
3. 輸入配置的名稱。
4. 輸入描述。
5. 在「配置設定」區段中，按照下表所述指定其餘設定。

設定	方法
工作管理員 **控制台** **登錄編輯程式** **檔案總管**	針對應拒絕存取權的設定，選擇**拒絕存取**勾選框。 選擇**限制功能**勾選框以限制檔案總管的功能。 例如：移除對映網路磁碟機。 按一下所提供的連結以檢視遭限制的功能清單。
抽取式儲存裝置	
抽取式儲存裝置的存取模式	• **限制讀取權**：這可以阻止任何存取，是限制程度最高的配置。 • **限制寫入權**：這允許有限存取，但可以阻止未經授權移除資料或添加病毒 至裝置的能力等等。

6. 按**下一步**。
7. 請選擇下列發佈選項之一：

- 所有裝置

- 沒有裝置 (預設)
- 自訂

8. 按一下**完成**。

> 為了讓配置完全生效，裝置在套用配置後應重新開機。

建立抽取式儲存裝置允許清單

如果您想建立允許的儲存裝置允許清單，請先完成下列步驟：

- 將 USB 儲存裝置附加到您想允許連接的 PC。
- 開啟裝置管理員，然後按一下 USB 控制器。
- 查看每個控制器的設定，以取得裝置資訊。
- 儲存裝置資訊，以便在建立您的允許清單時使用。

若要建立抽取式儲存裝置允許清單：

程序

1. 在 **Windows Desktop 限制**配置頁面中，按一下**列入允許清單的抽取式儲存裝置**區段下的 **+新增**。
2. 在**新增硬體 ID** 視窗中，輸入您想要從允許清單中移除並作為儲存裝置封鎖的一或多部裝置的硬體 ID。
3. 按一下**新增硬體 ID**。 列入允許清單的硬體 ID 會顯示在**列入允許清單的抽取式儲存裝置**區段。

> 若要編輯或刪除清單中的硬體 ID，請選擇**動作**欄下方的「編輯」或「刪除」選項。
>
> 為了讓配置完全生效，裝置在套用配置後應重新開機。

10.10.4.67. Windows 10 的桌面設定

「Windows 10 的桌面設定」配置可讓您自訂桌面設定，並將它們推送到 Windows 10 裝置。 您可以利用此配置來設置下列桌面設定：

- 桌面背景影像
- 鎖定畫面影像
- 上傳自訂螢幕保護程式
- 桌面捷徑

> 此功能需要 Bridge。 請參閱 **Ivanti Bridge** 以取得詳細資料。

程序

1. 在**組態**下，按一下 **+ 新增**。
2. 選擇 **Windows 10 的桌面設定**組態。 **Windows 10 的桌面設定**頁面隨即顯示。
3. 在**名稱**欄位中，輸入適當的設定名稱。
4. (選用) 按一下 + **新增說明**連結，新增組態的描述。
5. 在**組態設定**區段中，設定下列設定項目:

設定	描述
檔案傳送	為「桌面設定」任選下列其中一個檔案傳送選項: • **上傳檔案** - 將設定上傳至 Ivanti Neurons for MDM。 • **覆寫 URL** - 提供覆寫 URL 與待下載的設定檔案。
桌布設定：	按一下**選擇檔案**，尋找並上傳一張桌布圖片: 支援的檔案格式為 BMP、JPG、JPEG、PNG。
鎖定畫面桌布設定 (Windows 10 專業版裝置**不**支援鎖定螢幕桌布設定)	按一下**選擇檔案**以尋找與上傳桌布影像。 支援的檔案格式為 BMP、JPG、JPEG、PNG。
螢幕保護程式設定	按一下**選擇檔案**，尋找並上傳螢幕保護程式檔案。 僅上傳 Windows 相容 .SCR 檔案。 若要設定密碼解鎖螢幕保護程式模式，請選擇**螢幕保護程式的密碼保護**。 選擇**螢幕保護程式逾時**期限 (以分鐘為單位)。
桌面捷徑	按一下**新增捷徑**，以設定要新增到裝置桌面的桌面捷徑。 **新增捷徑**視窗隨即顯示。 請使用下列選項填寫表格： • **位置** - 輸入捷徑在 Windows 裝置上的出現位置。 • **目標路徑** - 輸入捷徑所導向的本機路徑，或是 UNC 路徑或磁碟機代號。 目標路徑也可以是 URL。 • **引數** - 輸入要在開啟目標檔案時使用的引數。 • **工作目錄** - 包含目標所需檔案的資料夾路徑。 • **圖示檔案** - 上傳有效的 Windows .ico 檔案。 設定好選項之後，請按一下**新增捷徑**。

6. 按**下一步**。
7. 請選擇下列發佈選項之一：
   - 所有裝置
   - 沒有裝置 (預設)
   - 自訂
8. 按一下**完成**。

10.10.4.68. Windows Hello 企業版配置

此配置可讓管理員在裝置中設定 Windows Hello。 設定 Windows Hello 需要設定 PIN 碼以登入裝置。

適用於：Windows 10

Procedure程序

1. 前往配置 > +新增。
2. 在搜尋欄位中輸入 windows，然後按一下 Windows Hello 企業版配置。
3. 輸入配置的名稱和描述。
4. 將啟用/停用 Windows 10 裝置的 Windows Hello 企業版切換為開。

> 此切換預設為「開」。 停用 Windows Hello 企業版並不會移除裝置的 PIN 碼。

5. 設定 PIN 碼複雜度。
6. 選擇所需的配置：
    - 需要 Trusted Platform Module (TPM) 才能使用 Windows Hello 企業版
    - 將 Windows Hello 企業版憑證做為智慧卡憑證
    - 使用生物特徵，例如臉部和指紋做為 Windows Hello 企業版 PIN 登入的替代方式。
    - Windows Hello 臉部身份認證需要用於臉部特徵識別的增強反電子欺騙功能。
    - 動態鎖
    - 讓使用者使用 FIDO2 安全金鑰登入。
7. 按下一步。
8. 選擇啟用此配置選項。
9. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂。
10. 按一下完成。

10.10.4.69. Windows AI 管理組態

Ivanti Neurons for MDM 可讓管理員管理 Windows AI 設定和組態。 Windows AI 管理可透過強大的 AI 助理，增強創造力和生產力。 使用 **Windows AI 管理**組態管理已註冊 Windows 裝置上的 Windows AI 功能。 此組態可讓管理員透過 Windows AI 組態服務提供者 (CSP) 原則控制 Microsoft Copilot、Windows Recall 和 Microsoft Paint AI 功能。

管理員可以停用選取的 AI 功能、移除對 Copilot 功能的存取權、控制 Windows Recall 行為，以及管理 Microsoft Paint 中 AI 驅動的映像產生功能。

適用於: Windows 10+

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取 **Windows AI 管理**組態。
3. 輸入配置的**名稱**和**描述**。
4. 在**組態設定**區段中，從下列選項中選取:### Copilot 設定

設定	描述
停用 Windows Copilot	防止使用者存取 Windows Copilot。
停用 Copilot 硬體按鍵	停用受支援裝置上的專用 Copilot 硬體按鍵。
移除 Microsoft Copilot 應用程式	從裝置移除 Microsoft Copilot 應用程式。

Recall 設定

設定	描述
停用 AI 資料分析	停用 Windows Recall 使用的 AI 資料分析。
設定 Recall 快照的最大儲存空間 (GB)	指定 Windows Recall 可用於儲存快照的最大儲存量。

Paint AI 設定

設定	描述
停用 Image Creator	停用 Microsoft Paint 中的 Image Creator 功能。
停用 Cocreator	停用 Microsoft Paint 中的 Cocreator 功能。
停用 Generative Fill	停用 Microsoft Paint 中的 Generative Fill 功能。

Microsoft 已取代此組態所使用的 **TurnOffWindowsCopilot** 原則。 因此，此組態不再影響裝置上的 Copilot 應用程式。

如果未選取**停用 Windows Copilot** 核取方塊，此組態將覆寫裝置上先前的組態選取項目，以啟用 Windows AI 管理。

5. 按**下一步**，確認發佈設定。
6. 選取其中一個發佈選項以設定 **Windows AI 管理**組態。 如需有關設定發佈選項的詳細資訊，請參閱**使用配置**。
7. 按一下**完成**。

10.10.4.70. Play Integrity (前身為 SafetyNet Attestation)

Play Integrity (前身為 SafetyNet) 有助於使用 Google 的 Play Integrity API 評估 Android 裝置的安全性和相容性。 設定後，它可讓您在定期的時間間隔後分析裝置，以判斷裝置是否已遭到篡改。

> 現在所有 Android 版本均支援 Play Integrity。

程序

1. 在**組態**索引標籤中，按一下 **+新增**。
2. 選取 **Play Integrity** 組態。 **Play Integrity 組態**頁面隨即顯示。
3. 在**名稱**欄位中，鍵入 Play Integrity 組態的適當名稱。
4. 按一下 **+新增描述**連結新增組態的描述。 此為選用欄位。
5. 在**組態設定**區段中，鍵入應套用於評估裝置安全性和相容性檢查的最小間隔時間 (以小時為單位)。 值應該介於 1 到 24 之間。
6. 按**下一步**，然後選擇下列其中一個發佈選項：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂

按一下**完成**。

> 當 Play Integrity 和 SafetyNet 亂數傳送到裝置時，Play Integrity 亂數將優先於 SafetyNet 亂數。

10.10.4.71. 進階 Android 密碼與鎖定畫面

Couldn't convert your doc.

10.10.4.72. Microsoft Defender for Endpoint

Microsoft Defender for Endpoint (MDE) 組態 (前身為 Windows 進階威脅防護)，允許客戶執行 MDE 服務的裝置上線和離線操作。

程序

1. 前往**配置 > +新增**。
2. 選取 **Microsoft Defender for Endpoint** 組態。
3. 輸入配置的名稱。
4. 輸入描述。
5. 在「配置設定」區段中，按照下表所述指定其餘設定。

設定	描述
上線或離線 Blob	貼上從 Microsoft Defender for Endpoint Security Center 網站取得的上線或離線 Blob

6. 按**下一步**。
7. 請選擇下列發佈選項之一：

- 所有裝置
- 沒有裝置 (預設)
- 自訂

8. 按一下**完成**。

10.10.4.73. 憑證型驗證

Ivanti Neurons for MDM支援憑證型驗證，這允許管理員使用數位憑證和租用戶特定 (虛名) 主機名稱登入。 當已啟用和配置時，管理員可使用數位憑證而非基本驗證 (使用者名稱和密碼) 登入。

> 此功能預設為停用。 管理員應聯絡支援中心為其租戶啟用此功能。 只有支援中心啟用時，才能在 NA3 叢集環境中使用此功能。 請確定您的超級管理員使用者名稱和密碼已測試並就緒，因為一旦啟用憑證型驗證，您只能使用這些憑證登入，直到您已成功設定您的虛擬網域。

程序

1. 在**管理員**索引標籤中，選取**虛擬主機組態**。
2. 在虛擬主機配置頁面中，設定以下選項：
3. 按一下**儲存**。
   需要幾分鐘的時間才能存取您的虛擬主機。

設定	方法
建立虛擬網域	輸入虛擬網域名稱。 此網域名稱可能和您的公司身份更一致，您可使用數位憑證登入。
上傳受信任發行 CA 憑證	按一下**選擇檔案**以選擇並上傳發行憑證的 CA 憑證給您的管理員。 如要啟用憑證撤銷檢查，選擇**為此憑證啟用憑證狀態驗證設定** (選用)。 此選項預設為已啟用。 取消選取此選項以停用憑證撤銷。 按一下**新增更多**，以新增更多憑證。 確定憑證格式為 .p7b、.pem、.der、.crt 或 .cer。
憑證屬性對應	憑證屬性對應配置憑證身份元素對應至管理的帳戶屬性。 在**從憑證**欄位中，選擇以下憑證元素： • **NTPrincipalName** • **RFC 822 名稱** 在**至變數**欄位中，選擇以下管理的帳戶屬性： • **UserUPN** • **$UserEmailAddress** • **$EDIPI**

10.10.5. 使用者資源配置

本節包含以下各主題：

- CalDAV 配置
- CardDAV 配置
- Google 配置
- 電子郵件配置
- Exchange 組態
- 字型配置
- 訂閱的行事曆配置
- 建立 Web 剪輯組態
- Office 365 安裝
- Windows GPO 設定
- BitLocker Encryption 配置

10.10.5.1. CalDAV 配置

CalDAV 配置可定義使用 CalDAV 網際網路標準之 Web 行事曆的存取權。

CalDAV 設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
主機名稱和連接埠	輸入行事曆伺服器的主機名稱和連接埠。
主體 URL	輸入可存取行事曆服務的 URL。
使用者	輸入可進行存取的使用者名稱。
密碼	輸入可進行存取的密碼。
使用 SSL	選擇僅使用 Secure Socket Layer 進行裝置和伺服器之間的通訊。
個別 App VPN	**必要條件**：在 CalDAV 配置中設定個別 app VPN 之前，先設定 Tunnel 或任一個別 app VPN 配置。 從下拉式功能表中，選擇預設的個別 app VPN 配置。 **適用於**：iOS 14+

如需更多資訊，請參閱如何建立配置

10.10.5.2. CardDAV 配置

CardDAV 可定義使用 CardDAV 網際網路標準的 Web Address Book 存取權。

CardDAV 設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
主機名稱和連接埠	輸入 Address Book 伺服器的主機名稱和連接埠。
主體 URL	輸入可存取 Address Book 服務的 URL。
使用者名稱	輸入可進行存取的使用者名稱。
密碼	輸入可進行存取的密碼。
使用 SSL	選擇僅使用 Secure Socket Layer 進行裝置和伺服器之間的通訊。
個別 App VPN **iOS 10+**	**必要條件**：在 CardDAV 配置中設定個別 app VPN 之前，先設定 Tunnel 或任一個別 app VPN 配置。 從下拉式功能表中，選擇預設的個別 app VPN 配置。 **適用於**：iOS 14+
通訊服務規則	選擇要用來與 CardDAV 系統中的聯絡人進行音訊通話的預設 app。

如需更多資訊，請參閱如何建立配置

10.10.5.3. Google 配置

Google 帳戶組態會將 iOS 9.3.2 和 visionOS 1.1 或 Android 6.0+ 裝置或支援的較新版本連線到 Google 帳戶。 Android enterprise 需要 Google 帳戶。 配置可設定多個 Google 電子郵件地址，以及使用者在進行身份認證之後所啟用的任何其他 Google 服務。

程序

1. 前往**配置 > +新增**。
2. 選擇 **Google 帳戶**配置。
3. 輸入配置的名稱。
4. 輸入描述。
5. 在「配置設定」區段中，按照下表所述指定其餘設定：

設定	方法
iOS 9.3.2+ ，Android 6.0+	
名稱	輸入可識別此配置的名稱。
帳戶描述	輸入帳戶的顯示名稱。
帳戶名稱	輸入帳戶使用者的完整名稱。
電子郵件地址	輸入帳戶的 Google 電子郵件地址
個別 App VPN	**必要條件**：在 Google 帳戶配置中設定個別 app VPN 之前，先設定 Tunnel 或任一個別 app VPN 配置。從下拉式功能表中，選擇預設的個別 app VPN 配置。 **適用於**：iOS 14+
iOS 10+	
通訊服務規則	選擇下列選項之一，藉此選擇要用來與 Google 系統中的聯絡人進行音訊通話的預設 app： • **從 App Catalog 與系統 App**：輸入 app 名稱的前幾個字母以便搜尋 app。 • **輸入套件 ID (僅限 Apple 系統 App)**：輸入系統 App 套件 ID。 套件 ID 的開頭必須為「com.Apple」。

6. 按**下一步**。
7. 請選擇下列發佈選項之一：

- 所有裝置
- 沒有裝置 (預設)
- 自訂

8. 按一下**完成**。

當 Google 帳戶配置套用到裝置，Go 用戶端會提示使用者登入 Google。

如需更多資訊，請參閱如何建立配置

10.10.5.4. 電子郵件配置

電子郵件配置可設定裝置上的 POP 或 IMAP 電子郵件。

電子郵件設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
帳戶描述	輸入您想用來識別此電子郵件的文字。
帳戶類型	選擇 IMAP 或 POP。 如果您選擇 IMAP，也可以輸入路徑字首。 網際網路服務供應商 (ISP) 會提供您哪類帳戶可供使用的相關資訊。 一般來說，當所有 IMAP 資料夾都列在「收件匣」底下時，就需要字首。 如果 ISP 需要字首，通常他們也會提供可配置的特定字首相關資訊。
使用者顯示名稱	輸入您想用來識別電子郵件帳戶使用者的文字。 請注意，使用者也可以在裝置上設定這個值。
電子郵件地址	輸入可指定帳戶的電子郵件地址的變數。
允許移動	選擇您是否允許此帳戶的電子郵件受到移動。
啟用 S/MIME	選擇開啟 S/MIME 加密支援。 接著，您可以選擇簽署並加密憑證。 需要憑證快取。 請確認「身分憑證」配置所使用的「憑證授權中心」裡已啟用快取。 **iOS 10.3+：** 針對 **S/MIME 簽署**和 **S/MIME 加密**欄位，選擇下列其中一個選項： • 關閉 • 開啟 • 使用者選擇 **iOS 12.0+：** • 使用者可以覆寫 S/MIME 簽署設定 • 使用者可以選擇 S/MIME 簽署身份 • 使用者可以覆寫 S/MIME 加密設定 • 使用者可以選擇 S/MIME 加密身份 視需要**針對每個訊息簽署和加密啟用 S/MIME**。
允許 Mail Drop	選擇允許此帳戶的 Mail Drop。 Mail Drop 可讓使用者將大型附件存放在 iCloud 中，並在電子郵件中提供連結，以傳送含大型附件的電子郵件。 如需 Mail Drop 的詳細資訊，請參閱：https://support.apple.com/
個別 App VPN	可在 Apple 支援的郵件網域上對多個不同的個別 app VPN 描述檔建立關聯。 現在透過個別 app VPN 支援 IMAP 和 POP3 電子郵件配置。 **必要條件**：在電子郵件配置中設定個別 app VPN 之前，先設定 Tunnel 或個別 app VPN 配置。 從下拉式功能表，**選擇個別 App VPN 配置**。

內送郵件

設定	方法
郵件伺服器和連接埠	網際網路服務供應商 (ISP) 可提供您這個位址。
使用者名稱	輸入可存取內送電子郵件伺服器的使用者名稱。 這通常和電子郵件地址相同。 您的 ISP 會提供格式。
憑證類型	選擇 ISP 定義的憑證類型。
密碼	輸入可存取內送電子郵件伺服器的密碼。
使用 SSL	選擇僅使用 Secure Socket Layer 進行裝置和伺服器之間的通訊。

外送郵件

設定	方法
郵件伺服器和連接埠	網際網路服務供應商 (ISP) 可提供您這個位址。
使用者名稱	輸入可存取外送電子郵件伺服器的使用者名稱。 這通常和電子郵件地址相同。 您的 ISP 會提供格式。
憑證類型	選擇 ISP 定義的憑證類型。
密碼	輸入可存取外送電子郵件伺服器的密碼。
外送密碼和內送密碼相同	選擇 SMTP 驗證是否要使用與 POP/IMAP 相同的密碼。
僅用於郵件	選擇您是否要將此配置僅用於電子郵件用戶端。 其他傳送電子郵件的 app (包括使用本地電子郵件用戶端傳送內容的 app) 都不能使用此配置。
使用 SSL	選擇僅使用 Secure Socket Layer 進行裝置和伺服器之間的通訊。

10.10.5.5. Exchange 組態

Exchange 組態會在 Android、iOS 和 visionOS 裝置上設定 ActiveSync 型電子郵件，並設定適用於 macOS 裝置的 Exchange Web Services (EWS) 型電子郵件。

> 使用 Android 9 的 Samsung 裝置已經棄用 Exchange 組態。 針對使用 Android 9 及更新版本的 Samsung 裝置，在裝置管理員模式下不支援 Exchange 組態。

Exchange 設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
Exchange 主機	如果您是使用 Sentry 來存取電子郵件，請輸入 Sentry 伺服器主機名稱。 否則，請輸入 ActiveSync 伺服器的位址。*
允許移動	**若是 iOS 和 Android：**選擇您是否允許此帳戶的電子郵件遭到移動。 **Windows 10:** 不適用。
啟用 S/MIME	選擇開啟 S/MIME 加密支援。 接著，您可以選擇簽署並加密憑證。 需要憑證快取。 請確認「身分憑證」配置所使用的「憑證授權中心」裡已啟用快取。 **iOS 10.3+：** 針對 **S/MIME 簽署**和 **S/MIME 加密**欄位，選擇下列其中一個選項： • 關閉 • 開啟 • 使用者選擇 **iOS 12.0+：** • 使用者可以覆寫 S/MIME 簽署設定 • 使用者可以選擇 S/MIME 簽署身份 • 使用者可以覆寫 S/MIME 加密設定 • 使用者可以選擇 S/MIME 加密身份 視需要**針對每個訊息簽署和加密啟用 S/MIME**。
同步處理最近使用過的電子郵件地址	選擇同步處理裝置和伺服器間最近聯絡過的電子郵件地址。
僅用於郵件	選擇您是否只要將此配置用於電子郵件用戶端。 其他傳送電子郵件的 app (包括使用本地電子郵件用戶端傳送內容的 app) 都不能使用此配置。
使用 SSL	選擇僅使用 Secure Socket Layer 進行裝置和伺服器之間的通訊。
啟用 OAuth 以交換裝載	iOS 12.0+ 與 macOS 10.14+： 選擇啟用使用 OAuth 進行驗證的選項。 如果啟用此選項，支援使用 OAuth 進行驗證的電子郵件 app 將提供下列額外設定： • OAuth 登入 URL • OAuth 權杖要求 URL
網域	請輸入此電子郵件帳戶的網域 (如果您不想提示使用者輸入的話)。
使用者	輸入代表此帳戶的電子郵件地址的變數。
帳戶密碼	請輸入此帳戶的密碼 (如果您不想提示使用者輸入的話)。
電子郵件地址	輸入代表此帳戶的電子郵件地址的變數。
郵件同步天數上限	選擇要同步處理裝置和伺服器之電子郵件的天數。

設定	方法
個別 App VPN **Android 與 Windows**	**必要條件**：在 Google 帳戶配置中設定個別 app VPN 之前，先設定 Tunnel 或任一個別 app VPN 配置。 從下拉式功能表中，選擇預設的個別 app VPN 配置。 **適用於**：iOS 14+
同步行事曆	**Android 和 Windows 10:** 選取此選項可在裝置和伺服器之間同步行事曆項目。 **若是 Samsung 裝置：**不使用此設定 (其預設為「開啟」)。 **若是 Android Email+ app：**使用此設定。
同步聯絡人 同步電子郵件	**Android 和 Windows 10:** 選取此選項可在裝置和伺服器之間同步聯絡人。 **若是 Samsung 裝置：**不使用此設定 (其預設為「開啟」)。 **若是 Android Email+ app：**使用此設定。 **Android 和 Windows 10:** 選取此選項可在裝置和伺服器之間同步電子郵件。 **若是 Samsung 裝置：**不使用此設定 (其預設為「開啟」)。 **若是 Android Email+ app：**不使用此設定 (其預設為「開啟」)。
同步作業 **iOS 13.0+** • 同步行事曆 • 同步聯絡人 • 同步電子郵件 • 同步備忘錄 • 同步提醒 身份憑證 **Android**	**Android 和 Windows 10:** 選取此選項可在裝置和伺服器之間同步任務。 **若是 Samsung 裝置：**不使用此設定 (其預設為「開啟」)。 **對於 Android Email+ 應用程式:** 不適用。 指定個別同步 Outlook Exchange 項目，例如「行事曆」、「聯絡人」、「備忘錄」和「提醒事項」。 針對每個項目，選擇或取消選擇**啟用**和**允許使用者覆寫**的選項。 在這些項目中，至少有一項必須啟用同步功能。 如果您停用其中一個選項的同步功能，但允許使用者覆寫，使用者仍可啟用它。 如果您想要伺服器使用憑證來驗證裝置，請從清單中選擇身份憑證。 清單中僅會顯示已使用身分憑證配置設定過的憑證。
僅使用憑證式驗證	使用所選的身分憑證作為 Exchange 伺服器驗證的唯一方式。
接受所有 SSL 憑證 Exchange App 優先順序 **iOS 10+** 通訊服務規則	選擇允許裝置使用者將 Android 裝置設為接受所有 SSL 憑證。 這項設定會套用至 Android Email+ 及 Samsung Knox 電子郵件。 • 啟用此設定時請務必小心使用，因為裝置使用者可能會在不知情的情況下讓裝置曝露在風險中。 • 如果 Sentry 憑證為自我簽署或未知憑證，就必須啟用此選項。 選擇預設要在 Android 裝置上設定的電子郵件用戶端 - Android Email+ 和 Samsung 電子郵件。 Email+ app 會新增至已啟用 Exchange app 優先順序的所有租戶。 選擇要用來與 CardDAV 系統中的聯絡人進行音訊通話的預設 app。

設定	方法
僅限 Windows 10+	
設定 Outlook	選擇此選項以便在裝置設定 Microsoft Outlook。 僅在啟用 Bridge 時才支援此選項。

*輸入 $ 可查看支援的變數清單 (如果此欄位適用的話)。

10.10.5.6. 字型配置

字型配置可讓您提供 iOS 7 裝置的其他 TrueType 或 OpenType 字型檔案。 下表列出描述字型設定：

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
上傳字型	將字型檔案拖曳到虛線方塊中，或按一下**選擇檔案**，從檔案系統中進行選擇。 字型檔案必須為 .otf 或 .ttf 檔案。

如需更多資訊，請參閱如何建立配置

10.10.5.7. 訂閱的行事曆配置

訂閱的行事曆配置可定義公用 Web 行事曆的存取權。

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
網址 (URL)	輸入用於存取行事曆的 URL。*
使用者	輸入用於存取的使用者名稱。*
密碼	輸入可進行存取的密碼。
使用 SSL	選擇僅使用 Secure Socket Layer 進行裝置和伺服器之間的通訊。

若適用，鍵入 $ 可查看此欄位的支援**變數**清單。

如需更多資訊，請參閱**如何建立配置**

10.10.5.8. 建立 Web 剪輯組態

Web Clip 是從 iOS 裝置到網站或網頁的捷徑。 使用 Web Clip 配置可在裝置上建立標準的 Web Clip。 您可以將 Web 剪輯圖示新增至將啟動特定網站的 iOS 裝置。 Web 剪輯可以協助您在裝置的主畫面上快速查找和使用書籤。 您也可以控制 Mobile Safari 的部分參數，進而檢視網站的體驗。

> 此組態可使用具有自訂分發選項的委派。 如需更多資訊，請參閱使用配置中的*分發組態*主題。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 按一下**配置**。
3. 按一下 **+新增**。
4. 搜尋並選取 Web 剪輯組態。
5. 在此頁面上進行設定。 請參閱**Web 剪輯組態設定**主題中的表格，以取得相關值的說明。
6. 按**下一步**，確認發佈設定。
7. 選取**自訂**，然後選取**裝置/裝置群組**。
8. 按一下**完成**。

Web 剪輯組態設定

下表列出了 Web 剪輯組態設定:

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
標籤	在裝置螢幕上的捷徑下方輸入要顯示的文字。*
網址 (URL)	請輸入 Web Clip 將存取的網址 (URL)。*
可移除	選取核取方塊，讓裝置使用者可以刪除 Web 剪輯。
圖示	將圖示檔案拖曳到虛線方塊中，或按一下**選擇檔案**，從檔案系統中進行選擇。
預製圖示	選擇避免更新版 Safari 新增的特效。
全螢幕	選擇在全螢幕模式中顯示 Web Clip，而非顯示為瀏覽器中的內容。
忽略資訊清單範圍	選取即可允許在不顯示 Safari 瀏覽器的情況下瀏覽至外部網站。 未選取全螢幕時，此選項沒有作用。
目標應用程式套組識別碼	應用程式套組識別碼，用於指定打開 URL 的應用程式。 **範例**: com.google.chrome.ios

> 若適用，鍵入 $ 可查看此欄位的支援變數清單。

相關主題：

- iOS 多位使用者安全登入
- 如何建立配置

10.10.5.9. Office 365 安裝

授權：Silver

適用於：Windows 10+

設定 Office 365 安裝

Office 365 安裝是一種配置設定，可套用至所選裝置以安裝或解除安裝 Office 365。 您可以使用 Microsoft Office 部署工具，定義 xml 格式的配置設定，然後將檔案上傳。 上傳檔案後，您即可將配置選項推送給所選裝置。

程序

1. 在**配置**索引標籤中按一下 **+新增**。
2. 選擇 **Office 365 安裝**。 隨即顯示 **Office 365 安裝**頁面。
3. 在**名稱**欄位中，輸入適當的配置名稱。
4. 按一下 **+新增描述**連結，以新增配置描述。此欄位為選用。
5. 在**配置設定**區段中，更新下列欄位：

欄位名稱	描述
用於安裝 Office 365 的配置檔	按一下**選擇檔案**按鈕，瀏覽並選擇 XML 格式的配置檔，其中包括安裝 Office 365 安裝的定義設定。 範例: <Configuration> <Add OfficeClientEdition="64" Channel="Current"> <Product ID="O365ProPlusRetail"> <Language ID="en-us"/> </Product> </Add> </Configuration> 請確認配置檔格式為 xml，且在新增配置設定檔後有顯示綠色打勾記號。
用於解除安裝 Office 365 的配置檔	按一下**選擇檔案**按鈕，瀏覽並選擇 XML 格式的配置檔，其中包括解除安裝 Office 365 的定義設定。 範例: <Configuration> <Remove All="TRUE"/><Display Level="None" AcceptEULA="TRUE" /> </Configuration> 請確認配置檔格式為 xml，且在新增配置設定檔後有顯示綠色打勾記號。

6. 按**下一步**。
7. 選擇下列任一選項，以將設定發佈給裝置。

選項	描述
啟用此配置	選擇此勾選方塊時，可允許所選裝置使用這項配置。 取消選擇此勾選方塊時，即會移除這項配置 (若已套用至裝置的話)。
所有裝置	將設定發佈至所有裝置。
沒有裝置	保留設定，而不發佈給裝置。
自訂	將設定發佈給定義的裝置群組。 選擇要發佈設定之目標裝置類型旁的勾選方塊。 若要搜尋裝置群組，您也可以在**搜尋裝置群組**搜尋欄位中，輸入裝置群組名稱。 如果您想建立新的裝置群組，請按一下頁面底部的**建立新的裝置群組**連結。 如需詳細資訊，請參閱**裝置群組**。 選擇裝置類別時，可以查看裝置使用者清單的詳細資料 (**姓名**、**電話號碼**及**裝置類型**)，在**發佈摘要**區段之下找到所選裝置的類別。

8. 按一下**完成**，將設定發佈至所選裝置。

10.10.5.10. Windows GPO 設定

授權：Bridge

適用於：Windows Desktop

進行 Windows GPO 設定

群組原則物件 (GPO) 是一種設定集合，用來定義裝置允許執行或不允許執行的權限。 若要管理 GPO 設定，您必須進行 Bridge 設置。 如需更多詳細資訊，請參閱 Ivanti Bridge。

如果 GPO 中繼資料未上傳至資料庫，請聯絡您的網站管理員。 您可以藉由 PowerShell 指令碼並透過 Bridge 將 GPO 配置部署至裝置。 您可以使用 GPO 設定，來進行特定設定並將其推送給裝置。

程序

1. 在**組態**索引標籤中，按一下 **+新增**。
2. 選擇 **Windows GPO 設定**配置。 隨即顯示 **Windows GPO 設定**頁面。
3. 在**名稱**欄位中，輸入適當的 Windows GPO 設定名稱。
4. 按一下 **+新增描述**連結，以新增配置的描述。 此為選填欄位。
5. 在**配置設置**區段中，按一下 **+新增**。 隨即顯示**新增 Windows 群組原則物件 (GPO)** 視窗。
6. 從左窗格的 GPO 階層樹狀結構中，按一下相關元件，搜尋並選擇 GPO。 GPO 階層樹狀結構代表原則設定的路徑。 您也可以在搜尋欄位中，輸入 GPO 設定的名稱，以搜尋特定的 GPO 設定。
   選擇 GPO 設定之後，您即可在右窗格中檢視所選 GPO 設定的詳細資料。
7. 在**設定狀態**欄位中，可使用下列設定選項：

選項	描述
未設定	移除現有 GPO 設定。
啟用	啟用 GPO 設定。
停用	停用 GPO 設定。

8. 在**設定值**欄位中，輸入要提供給 GPO 的適當名稱。
   若要新增其他設定值，請按一下 **+** 圖示。 部分 GPO 設定可能不需要任何其他設定值。 有些則可能需在「設定值」下以文字值的形式指定其他資料。 在此類設定中，請從下拉式清單中選取任意值。

> 只有在**設定狀態**下選取**已啟用**選項才可編輯此欄位。

9. 按一下**儲存並關閉**，儲存 GPO 並關閉視窗。 如果您想新增其他 GPO，可以按一下**儲存並新增其他項目**進行儲存，以保持 GPO 視窗開啟。
   新增的 GPO 設定會顯示在**組態設定**區段中。

> 按一下**動作**欄中的相關圖示即可編輯或刪除 GPO 設定。

選項描述啟用此配置選擇此勾選方塊時，可允許所選裝置使用這項配置。 取消選擇此勾選方塊時，即會移除這項配置 (若已套用至裝置的話)。**所有裝置**將設定發佈至所有裝置。**沒有裝置**保留設定，而不發佈給裝置。**自訂**將設定發佈給定義的裝置群組。 選擇要發佈設定之目標裝置類型

旁的勾選方塊。 若要搜尋裝置群組，您也可以在**搜尋裝置群組**搜尋欄位中，輸入裝置群組名稱。 如果您想建立新的裝置群組，請按一下頁面底部的**建立新的裝置群組**連結。 如需詳細資訊，請參閱**裝置群組**。

選擇裝置類別時，可以查看裝置使用者清單的詳細資料 (**姓名**、**電話號碼**及**裝置類型**)，在**發佈摘要**區段之下找到所選裝置的類別。

10. 按一下**完成**，將 GPO 設定發佈至所選裝置。

10.10.5.11. BitLocker Encryption 配置

授權：Bridge

適用於：Windows Desktop

本節包含以下各主題：

- 設定 BitLocker Encryption
- 檢視 BitLocker 設定

設定 BitLocker Encryption

BitLocker Encryption 功能可在硬碟和卸除式磁碟機上強制加密，以提供資料保護。 若要管理 BitLocker Encryption 設定，您必須進行 Bridge 設置。 請參閱 **Bridge** 以取得詳細資料。 BitLocker Encryption 配置可協助您設置裝置的加密設定。

程序

1. 在**組態**索引標籤中，按一下 **+新增**。
2. 選擇 **BitLocker Encryption** 配置。 **BitLocker Encryption** 頁面隨即顯示。
3. 在**名稱**欄位中，輸入適當的 BitLocker Encryption 名稱。
4. 按一下 **+新增描述**連結，以新增配置的描述。 此為選填欄位。
5. 在「配置設置區段」中，設置下列設定：

設定	描述
加密方法和類型	根據加密的金鑰大小選擇加密演算法的類型。 可用選項如下： • **AES-CBL 128 位元** • **AES-CBL 256 位元**
加密所有硬碟	按一下切換按鈕，以**開啟**或**關閉**加密所有硬碟的設定。 如果裝置上有任何硬碟已經加密，則不會套用對此配置所做的編輯，因為加密程序無法透過編輯加以復原。
選擇磁碟機	選擇需要加密的磁碟機。 範例：**C:** 按一下 **+新增**，以新增更多磁碟機。 如果您已「開啟」**加密所有硬碟**設定，將不會顯示此欄位。
磁碟機硬體型加密類型	Trusted Platform Module (TPM) 是電腦主機板上的晶片，可協助進行防篡改加密。 如果您在搭載 TPM 的電腦上使用 BitLocker Encryption 或裝置加密，有部分的金鑰會儲存在 TPM 中。 您可從下拉式清單中選擇下列硬體型加密設定選項： • **啟動時需要 TPM** • **需要啟動 PIN 與 TPM** • **不使用 TPM** TPM 選項僅適用於作業系統磁碟機，以及 TPM 1.2 版及以上版本。 如果您對裝置套用硬體型加密設定，您再也無法編輯裝置的此設定。 如果裝置已設定某個 BitLocker 配置，則您無法推送內含不同 TPM 選項的第二個 BitLocker 配置。
選取下列組態核取方塊選項 (選用)： • **拒絕未受 BitLocker 保護之固定式磁碟機的寫入權限** • **拒絕未受 BitLocker 保護之卸除式磁碟機的寫入權限**	
預先加密的裝置動作	選擇以下任一選項，以定義處理未完全加密或已有金鑰保護裝置之磁碟機的方式。 • 停止加密 - 若任何所選磁碟機已經加密，則停止加密。 • 解密未在 Ivanti Neurons for MDM 中儲存復原密碼的所選取磁碟機 – 選擇此選項，以便只套用至在 Ivanti Neurons for MDM 中沒有復原密碼的磁碟機。
復原選項	如果使用者忘記密碼，便可使用復原選項。 您可以從裝置詳細資料頁面進行擷取。 您可設定下列復原選項： • **停用復原** • **使用密碼並儲存在 AD 中** • **使用密碼並儲存在 AD 和 MobileIron 中**
重新啟動間隔	將此配置推送到裝置之後，將會出現重新啟動提示。 重新啟動之後便會開始加密。 若要設定重新啟動間隔，請從下拉式清單選擇裝置在重新啟動前應等待的時間。 最短的重新啟動間隔為 1 分鐘，最長的重新啟動間隔為 120 分鐘 (2 小時)。

設定	描述
重新啟動訊息	輸入裝置中應顯示的重新啟動訊息。 如果適用，也會向使用者顯示啟動密碼或啟動 PIN 碼。 使用者可以記下來，以在重新啟動後出現提示時輸入。

6. 按**下一步**。
7. 選擇下列任一選項，以將設定發佈給裝置。

設定	描述
啟用此配置	選擇此勾選方塊時，可允許所選裝置使用這項配置。 取消選擇此勾選方塊時，即會移除這項配置 (若已套用至裝置的話)。
所有裝置	將設定發佈至所有裝置。
沒有裝置	保留設定，而不發佈給裝置。
自訂	將設定發佈給定義的裝置群組。 選擇要發佈設定之目標裝置類型旁的勾選方塊。 若要搜尋裝置群組，您也可以在**搜尋裝置群組**搜尋欄位中，輸入裝置群組名稱。 如果您想建立新的裝置群組，請按一下頁面底部的**建立新的裝置群組**連結。 如需詳細資訊，請參閱裝置群組。 選擇裝置類別時，可以查看裝置使用者清單的詳細資料 (**姓名**、**電話號碼**及**裝置類型**)，在**發佈摘要**區段之下找到所選裝置的類別。

8. 按一下**完成**，將設定發佈至所選裝置。

檢視 BitLocker 設定

您可透過 **BitLocker 設定**下的裝置詳細資料頁面 (**裝置>裝置>[裝置名稱]**) 檢視 BitLocker 設定。 依預設，詳細資料會隱藏。

您可以按一下每個欄位旁邊的檢視 (眼睛形狀) 圖示，以檢視下列詳細資料:

設定	描述
復原密碼	若選擇此選項，復原密碼將由 Windows 產生，並在推送 BitLocker 組態之後傳回 Ivanti Neurons for MDM。 如果裝置經歷復原模式，系統會提示使用者輸入此密碼。 如果有多個加密磁碟機，應使用相同復原密碼。 只有在選擇**使用密碼並儲存在 AD 和 MobileIron 中**的復原選項時，才會發佈復原密碼。
PIN 碼	顯示 6 位數的啟動 PIN 碼。 只有當您在 BitLocker 配置設定中選擇**需要啟動 PIN 碼與 TPM** 選項時，才會顯示 PIN 碼。
啟動密碼	針對裝置設定的啟動密碼。 只有當您在 BitLocker 配置設定中選擇**不使用 TPM** 選項時，才會顯示啟動碼。
TPM 版本	顯示所設定的 TPM 版本。

依據 BitLocker 配置設定中所配置的設定，某些欄位可能會顯示 **不適用**。

- 加密狀態顯示在「裝置詳細資料」頁面中的「裝置加密狀態」下。
- 相同的啟動密碼或 PIN 碼將用於套用 BitLocker 之裝置的所有磁碟機。
- 如果裝置已有一個磁碟機接受加密，而您要建立一個配置以加密該裝置的第二個磁碟機，則先前的密碼將會遭到覆寫。 因此，建議裝置中只有一個磁碟機使用「復原密碼」選項。

10.10.6. 企業網路存取配置

本節包含以下各主題：

- AirPlay 配置
- AirPrint 配置
- Always-on VPN 組態
- 預設的 App 執行時期權限
- 教育
- 全域 Proxy 配置
- LDAP 配置
- macOS Server 配置
- 網路轉送組態
- Tunnel
- 設定 AppTunnel
- 個別 App VPN 組態
- 單一登入配置
- iOS 多位使用者安全登入
- Android APN 設定配置
- VPN 組態
- 隨選即用 VPN
- Wi-Fi 組態

10.10.6.1. AirPlay 配置

授權：Silver

Airplay 配置可設定其他裝置的存取權，以便顯示媒體。 下表列出 AirPlay 設定：

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
允許清單	輸入每個獲許可之 AirPlay 目的地的裝置 ID。 如果您不提列 ID，AirPlay 目的地就不會受到限制。 **適用於：**iOS 7.0+ 和 macOS 10.10+ (受監管)。
裝置設定	輸入每個已知 AirPlay 目的地的裝置 ID (macOS) 或裝置名稱 (iOS) 及密碼。

如需更多資訊，請參閱如何建立配置

10.10.6.2. AirPrint 配置

授權：Silver

AirPrint 配置可設定無線列印。 下表列出 AirPrint 設定：

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
AirPrint 設定	**IP 位址：**輸入 AirPrint 印表機的 IP 位址。 **資源路徑：**輸入與 AirPrint 印表機相關聯的資源路徑。 此項目會對應於 _ipps.tcp Bonjour 記錄的 rp 參數。 範例： • printers/Canon_MG5300_series • printers/Xerox_Phaser_7600 • ipp/print • Epson_IPP_Printer. 資源路徑有區分大小寫。 **連接埠：**輸人 AirPrint 目的地的接聽連接埠。 如果未指定，AirPrint 將使用預設連接埠。 如需 Apple 標準連接埠的詳細資料，請參閱 https://support.apple.com/en-us/HT202944 **強制 TLS**：可讓您啟用使用 Transport Layer Security (TLS) 保護的連線。 預設為停用。

在 macOS 上安裝 **AirPrint** 配置後，會透過 **AirPrint** 配置將印表機詳細資訊推送至裝置。 使用者按一下系統偏好設定 > 印表機和掃描器 > +，即可檢視自動填入的印表機詳細資訊。 在**新增**畫面中，使用者必須選擇**預設**，然後選擇所需的印表機描述檔。 這可將所需的印表機新增至**印表機和掃描器**。

如需更多資訊，請參閱如何建立配置

10.10.6.3. Always-on VPN 組態

授權：

- **Gold for Android Enterprise**
- **Silver 適用於 iOS**

Always-on VPN 組態可確保使用者不需採取任何動作即可自動連線到 VPN (可使用時)。 此功能需要 Android 7.0 + 或 iOS 8 以及 VPN 供應商支援 IKEv2 通訊協定。

適用於 Android 的 Always-on VPN 設定

Always-on VPN 組態會傳送至搭載 Android 7.0+ 的 Android Enterprise 裝置。 在搭配工作描述檔的受管理裝置 (Android 8.0+) 上，工作描述檔中會套用 VPN 配置。

> 當裝置在 **AMA** 作為裝置註冊類型的情況下以 **COSU** 模式進行部署時，如果使用 **Always-on** 組態的應用程式推送至裝置，則 **Always-on** 組態也會推送至該裝置。

若要啟用此配置，請從 App Catalog 中選擇 app 或輸入套件名稱。

適用於 iOS 的 Always-on VPN 組態

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
行動電話和 Wi-Fi 使用相同通道配置 伺服器 本機識別碼	選擇不論透過行動電話或 Wi-Fi 網路建立連線時，都只為 VPN 連線定義一個伺服器識別碼配對。 輸入 VPN 伺服器的主機名稱或 IP 位址。 IKEv2 用戶端識別碼應為下列格式之一： • FQDN • UserFQDN • 位址 • ASN1DN
遠端識別碼	遠端識別碼應為下列格式之一： • FQDN • UserFQDN • 位址 • ASN1DN
啟用 EAP	選擇啟用擴充驗證。
機器驗證 EAP 驗證	僅有當未選擇「啟用 EAP」時才可使用此選項。 請選擇下列選項之一： • 認證 • 共用密碼 僅有當選擇「啟用 EAP」時才可使用此選項。 請選擇下列選項之一： • 認證 • 使用者名稱/密碼
共用密碼	僅有針對「機器憑證」選擇「共用密碼」時，才可使用。 輸入連線的共用密碼。
認證 帳戶 密碼 Dead Peer Detection 間隔	僅有針對「機器憑證」選擇「認證」時，才可使用。 選擇要使用的認證。 系統會傳送此認證，以供 IKE 用戶端驗證使用。 如果使用擴充驗證，此認證就可用於 EAP-TLS。 僅有當選擇「EAP 認證」的「使用者名稱/密碼」時，才可使用此選項。 輸入 VPN 伺服器的帳戶 ID。 僅有當選擇「EAP 認證」的「使用者名稱/密碼」時，才可使用此選項。 輸入 VPN 伺服器的密碼。 請選擇下列選項之一： • 無 (停用) • 低 (存留項目每隔 1 小時傳送) • 中 (存留項目每隔 30 分鐘傳送)

設定	方法
	• 高 (存留項目每隔 10 分鐘傳送)
加密演算法	請選擇下列選項之一： • DES • 3DES • AES-128 • AES-256 • AES-128-GCM • AES-256-GCM • ChaCha20-Poly1305
完整性演算法	請選擇下列選項之一： • SHA1-96 • SHA1-160 • SHA2-256 • SHA2-384 • SHA2-512
Diffie Hellman 群組	選擇 D-H 金鑰交換群組。
有效期 (分鐘)	以分鐘為單位，輸入 SA 有效期 (金鑰更新間隔)。 有效值為 10 到 1440。
語音郵件	選擇「允許透過通道傳輸流量」，以針對 Always-on VPN 豁免語音郵件。 選擇「捨棄流量」，以不豁免流量。
Airprint	選擇「允許透過通道傳輸流量」，以針對 Always-on VPN 豁免 Airprint 流量。 選擇「捨棄流量」，以不豁免流量。
行動電話服務	選擇「允許透過通道傳輸流量」，以針對 Always-on VPN 豁免行動數據服務流量。 選擇「捨棄流量」，以不豁免流量。
允許來自 VPN 通道外部 Captive Web Sheet 的流量	選擇允許來自 VPN 通道外部 Captive Web Sheet 的流量。
允許來自 VPN 通道外部所有 Captive Networking App 的流量	允許來自 VPN 通道外部所有 Captive Networking App 的流量，以便處理 Captive Networking。
Captive Networking App 套件識別碼	列出來自 VPN 通道外部之受允許 Captive Networking App 流量的套件 ID，以便處理 Captive Networking。 Captive Networking App 可能需要其他權限才能在 Captive 環境中運作。

如需更多資訊，請參閱[如何建立配置]

10.10.6.4. 預設的 App 執行時期權限

適用於：針對 Android API 23+ 所建立的 app，以及在 Android Enterprise 裝置上執行 Android 6.0+ 的 app。

管理員可針對部署至 Android Enterprise 裝置的 app 設定執行時期權限配置。 針對 API 23 (或以上版本) 和執行 Android 6.0 或以上版本所建立的 app，可在執行時期提示使用者提供權限。 「預設的 App 執行時期權限」配置會設定這些 app 執行時期的預設權限。 Ivanti Neurons for MDM 會依預設建立此組態。 您可以編輯這個預設的系統配置，或依據自己的需求建立新的配置。

特定 app 的權限會優先於一般 app 的權限配置。 內部開發的 app 則受制於全域權限。 內部開發的 app 不支援設定個別 app 權限。

設定全域執行時期權限

管理員可以編輯預設的 app 執行時期權限和這些配置的發佈，如下所示：

Procedure程序

1. 前往**配置**。
2. 執行下列其中一個動作：
   - 若要編輯預設系統配置，請按一下**預設 App 執行時期權限**，然後按一下**編輯**。
   - 若要新增配置，請按一下**新增 > 預設的 App 執行時期權限**。

輸入配置的名稱。

4. 輸入描述。
5. 在「配置設定」區段中，設定下列其中一個預設執行時期權限：
   - 使用者提示 (預設選項)
   - 自動授與
   - 自動拒絕 (請謹慎使用)

按**下一步**。

7. 選擇**啟用此配置選項**。

> 若取消選擇此選項，這項配置就不會套用至任何裝置。 如果之前有套用，則會將所有裝置的該項配置移除。

8. 請選擇下列發佈選項之一：
   - 所有裝置
   - 沒有裝置 (預設)
   - 自訂

按一下**完成**。

設定特定 app 的執行時期權限

管理員可以按照下列方式，為個別應用程式設定預設的執行時期權限：

程序

1. 前往 **App**。

2. 按一下 app 的名稱。
3. 按一下 **App 配置 > Android Enterprise**。
4. 按一下**新增**，或按一下配置名稱，以編輯現有的配置。
5. 針對名稱、描述和限制等配置選項，進行設定。
6. 在「執行時期權限」區段中，按一下**管理權限**。
7. 在顯示的視窗中選擇權限，然後按一下**選擇**。
   其中僅列出會對特定應用程式造成危險的權限，供您選擇。
   https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups 上列出了危險權限的完整清單 (例如讀取聯絡人、尋找裝置上的帳戶、寫入通話記錄等等)。
   - 僅有當應用程式要求權限時，才會套用這些權限。
   - 如果使用者之前已接受或拒絕權限，就不會套用這些權限。

在「執行時期權限」區段中，選擇下列其中一個預設執行時期權限：

- 預設/全域 (預設選項)
- 自動授與
- 自動拒絕 (請謹慎使用)

在「發佈此 App 配置」區段中，選擇下列其中一個發佈選項：

- 有此 App 的每個人
- 沒有人
- 自訂

按一下**儲存**。

10.10.6.5. 教育

授權： Gold

適用於：受監管的 iOS 9.3+

設定領導者和成員的「Apple 教育方案」內容及「課堂」app。 下表列出教育設定：

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
配置類型	選擇下列其中一個類型： • 領導者 • 成員
啟用此配置	• 選擇此選項時，可將這項配置套用到所選的裝置。 • 取消選擇此選項時，可將這項配置從之前套用的所有裝置中移除。
發佈	請選擇下列發佈選項之一： • 所有裝置 • 沒有裝置 • 自訂

如需更多資訊，請參閱如何建立配置

10.10.6.6. 全域 Proxy 配置

授權： Silver

全域 Proxy 配置可設定裝置將 HTTP 流量轉送至 Proxy 伺服器。 下表列出 全域 Proxy 設定：

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
類型	選擇**手動**或**自動**。 如果您選擇**手動**，Proxy 伺服器主機名稱和連接埠為必填項目，Proxy 伺服器的使用者名稱和密碼則為選填項目。 如果您選擇**自動**，即可輸入 Proxy 自動設定 (PAC) URL。
主機名稱和連接埠	如果您選擇**手動**，請輸入 Proxy 伺服器的主機名稱和連接埠號。
使用者	(選填) 用於存取代理伺服器的使用者名稱。*
密碼	(選填) 存取 Proxy 伺服器的密碼。
PAC URL	(選填) 如果您選擇**自動**，即可輸入用來定義 Proxy 配置之 PAC 檔的 URL。 如果您將此設定保持空白，裝置就會使用 Web Proxy 自動探索通訊協定 (WPAD) 來探索 Proxy。
如果無法取得 PAC 時，允許直接連線	(iOS 7 及更新版本) 基於任何原因，裝置無法存取 PAC 檔時，選擇允許直接連線。
允許旁路 Proxy 存取 Captive Network	(iOS 7 及更新版本) 選擇允許旁路 Proxy 以顯示 Captive Network 的登入頁面。

若適用，鍵入 $ 可查看此欄位的支援**變數**清單。

如需更多資訊，請參閱**如何建立配置**

10.10.6.7. 全域 Proxy 組態 - Android

> 僅適用於裝置所有者和 AOSP 模式下的 Android 裝置。

全域 Proxy 配置可設定裝置將 HTTP 流量轉送至 Proxy 伺服器。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 按一下**配置**。
3. 按一下 **+新增**。
4. 在搜尋欄位中輸入**全域**，然後按一下**全域 Proxy**:
   全域 Proxy 組態詳細資料頁面隨即出現。
5. 在**名稱**方塊中輸入組態的名稱。
6. 或者，您可以新增有關組態的一些說明。
7. 從**平台**清單中，選取 **Android**。 這時會顯示**配置設定**區段。
8. 在類型下，選取**手動**或**自動**。
   - **手動**
     - 輸入**主機名稱** (網域名稱/IP 位址) 和**連接埠**詳細資料。
     - 在**新增排除項目**下，您可以新增必須在排除清單下的多個主機名稱 (網域名稱/萬用字元)。
   - **自動**
     - 輸入 PAC URL。
9. 按**下一步**以進行發佈設定，然後按一下**完成**。

10.10.6.8. LDAP 配置

LDAP 配置可設定公司目錄的存取權。 下表列出 LDAP 設定：

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
主機名稱	輸入 LDAP 伺服器的主機名稱。*
使用者	輸入可存取 LDAP 帳戶的使用者名稱。*
密碼	輸入可存取 LDAP 帳戶的密碼。
使用 SSL	選擇是否要使用 SSL 進行 LDAP 伺服器的連線。
搜尋設定	輸入至少一個帳戶項目。 在要開始搜尋的 LDAP 樹狀目錄中，每個項目都代表一個節點。 按一下 + 按鈕即可新增項目並加以編輯。 一個項目中包含下列值： 描述：說明搜尋設定的用途。 範圍：選擇**起始點**、**子樹狀目錄**或**一層**，指出搜尋的範圍。 **起始點**指僅有節點層級；**子樹狀目錄**指節點和所有子項目；**一層**指節點和一層子項目。 搜尋起始點：指定節點的概念路徑 (例如 ou=people，o=mycorp)。
個別 App VPN	**必要條件**：在 LDAP 配置中設定個別 app VPN 之前，先設定 Tunnel 或任一個別 app VPN 配置。 從下拉式功能表中，選擇預設的個別 app VPN 配置。 **適用於**：iOS 14+
iOS 10+	
通訊服務規則	選擇要用來與 LDAP 系統中的聯絡人進行音訊通話的預設 app。

> 若適用，鍵入 $ 可查看此欄位的支援**變數**清單。

如需更多資訊，請參閱**如何建立配置**

10.10.6.9. macOS Server 配置

macOS Server 配置使用已設好的帳號類型和設定來定義 macOS Server 帳號。 此配置允許使用者啟用伺服器上的檔案共用。

適用於：iOS 10+

設定 macOS Server

程序

1. 前往**配置 > +新增**。
2. 選擇 **macOS Server** 配置，以顯示**建立 macOS Server 配置**頁面。
3. 輸入配置的名稱。
4. 輸入描述。
5. 輸入**主機名稱**以指定伺服器位址。
6. 輸入**使用者名稱**以指定使用者的登入名稱。
7. (選用) 輸入使用者的**密碼**。
8. (選用) 輸入帳號的**描述**
9. (選用) 在設好的帳號中，輸入要用來與文件字典帳號伺服器進行通訊的**連接埠**號。 如果未指定連接埠號，系統將會使用預設的連接埠號。
10. 按**下一步**。
11. 選擇此配置的發佈。

10.10.6.10. Tunnel

Ivanti Tunnel 在 iOS、Android 和 Windows 裝置上啟用 VPN 功能。 Ivanti Tunnel 會與統一端點管理 (UEM) 平台、Standalone Sentry 和 Access 互動，以安全地從企業網路外部存取企業資源。 企業資源可以位於內部或雲端。 UEM 平台包括: Ivanti EPMM 和 Ivanti Neurons for MDM。

> Android Enterprise 裝置已棄用個別應用程式組態。 您需要使用應用程式目錄中的 Ivanti Tunnel 受控組態。

關於 Ivanti Tunnel 組態

Ivanti Tunnel 的組態是在統一端點管理 (UEM) 平台中建立的。 Ivanti Tunnel 會從 UEM 用戶端接收組態。 Ivanti EPMM 的用戶端是 Mobile@Work，而 Ivanti Neurons for MDM 的用戶端是 Go。

最新文件

如需最新的 Tunnel 指示，請參閱產品文件:

- Tunnel for Android，請參閱 **Ivanti Tunnel for Android指南**
- Tunnel for iOS，請參閱 **Ivanti Tunnel for iOS指南**
- Tunnel for macOS，請參閱 **Ivanti Tunnel for macOS 指南**
- Windows Tunnel，請參閱 **Ivanti Tunnel for Windows 指南**

> Ivanti Tunnel for Windows 已棄用，現在不再受到 Ivanti Neurons for MDM 支援。

10.10.6.11. 設定 AppTunnel

針對每個 app 容器及工作網路之間的 app 工作階段，AppTunnel 可逐一保障其安全性，藉此保護 app 資料。

本節包含以下各主題：

- 設定 Sentry 搭配使用 AppTunnel 及憑證
- 上傳 Sentry 憑證
- 設定 App 搭配使用 AppTunnel
- 關於 AppTunnel 服務名稱

設定 Sentry 搭配使用 AppTunnel 及認證

> 首次安裝 Standalone Sentry 時，也會安裝自我簽署憑證。 Ivanti 強烈建議您將預設憑證替換為公開受信任的第三方憑證。

必要條件

- AppTunnel 需使用 Sentry 的最新支援版本。 在開始 AppTunnel 設定作業之前，先完成 Sentry 安裝。
- 如果您想使用 SCEP 身分：
  - 新增本機或外部認證授權中心。 需安裝 Connector。
  - 新增 App 身分認證配置。 這是您在設定 AppTunnel 時要使用的動態發佈。

您可以使用 X.509 憑證設定 ActiveSync 和/或 AppTunnel 進行身分驗證，以使用指派給設定檔的 Sentry 伺服器。

程序

1. 前往**管理 > Sentry**。
2. 按一下 **+ 新增 Sentry 描述檔**。
3. 按一下 **ActiveSync 及/或 AppTunnel 使用認證**。
4. 按**下一步**。
5. 使用以下表格中的準則來完成**全域設定**頁面。

表格：「管理」>「Sentry」的全域設定	
設定	**方法**
名稱	輸入可識別此描述檔的名稱。
描述	輸入可說明此描述檔用途的描述。
外部主機名稱和連接埠	輸入 Sentry 的主機名稱與連接埠。
裝置驗證模式	
使用 2 階段驗證的單一憑證	選擇使用單一認證進行驗證。 如果您尚未**更新認證**，可在所選選項下方顯示的區域進行更新。
選擇憑證	如要上傳裝置驗證所需的群組憑證： 1. 按一下**新增**。 **新增憑證**視窗顯示。 2. 在**憑證名稱**欄位中，輸入憑證名稱。 3. 輸入保護 PKCS12 檔案的密碼。 4. 按一下**選擇檔案**，上傳群組憑證。 確定檔案格式為 .p7b、.p12、.pfx、.pem、.der、.crt 或 .cer 檔案。
啟用憑證撤銷清單 (CRL)	選擇以依據 CA 發佈的憑證撤銷清單 (CRL) 來驗證裝置的憑證。
未受管理的裝置預設行為	
允許未受管理的裝置接收電子郵件和資料	如果無意封鎖不受 Ivanti Neurons for MDM 管理的裝置存取資料，請選取此選項。

6. 按**下一步**。
7. 在 **Sentry 伺服器組態**頁面中，設定以下欄位:
8. 按**下一步**。

表格：「管理 > Sentry」的Sentry 伺服器配置	
設定	方法
接聽者通訊協定	請選擇下列任何通訊協定選項： • **僅限 HTTPS** • **僅限 HTTP** • **HTTPS 及 HTTP**
Https 連接埠	輸入 Https 連接埠號。 如果「接聽者通訊協定」選取為「僅限 HTTP」，將不會顯示此欄位。
Http 連接埠	輸入 Http 連接埠號。 如果「接聽者通訊協定」選取為「僅限 HTTPS」，將不會顯示此欄位。
Sentry TLS 伺服器憑證/金鑰	
使用 Sentry 的自行簽署憑證	選擇以使用由 Ivanti Neurons for MDM 服務建立的自行簽署憑證，並將其做為此設定檔的一部分傳送給 Sentry。 此憑證用來進行 Sentry 和行動電話裝置之間的通訊。
新增	如要上傳驗證所需的憑證： 1. 按一下**新增**。 **新增憑證**視窗隨即顯示。 只有取消選取**使用 Sentry 的自我簽署憑證**選項後才能看見此選項。 2. 在**憑證名稱**欄位中，輸入憑證名稱。 3. 輸入保護 PKCS12 檔案的密碼。 4. 按一下**選擇檔案**，上傳憑證。 請確認檔案的格式為 .p12 檔案。 5. 按一下**新增**。 所有上傳的 TLS 伺服器憑證 (包括從 Sentry 主頁面和其他描述檔上傳的憑證) 都會顯示在「Sentry TLS 伺服器憑證/金鑰」區段中。 如要選擇驗證所需的 TLS 憑證，按一下該憑證旁的選項按鈕。
新增第二個憑證	選取以啟用第二個證書。 一旦主證書逾期，Sentry 會自動切換到保留證書，而無需管理員干預。 Tunnel 已經儲存了這兩個證書，並且可以比對其中任何一個，從而確保不間斷的連接。
通訊協定	選擇所需的傳入和傳出通訊協定。
Cipher 套件	Cipher 可用來和 Sentry 進行 SSL 加密通訊。 一般來說，建議使用強式 Cipher 較佳。 舊版裝置可能需要使用弱式 Cipher。 預設會選擇強式 Cipher。 選擇任何其他您要使用的 Cipher。 您必須至少選擇一個 Cipher。

9. 新增至少一項顯示的服務。
10. 按一下**儲存**。

註冊好 Sentry 之後，「未配置的 Sentry 伺服器」中的 Sentry 頁面就會顯示此 Sentry。 若要指派描述檔給 Sentry，請按一下**動作**欄位中的**指派**。

上傳 Sentry 憑證

在建立 Sentry 設定檔時，Ivanti Neurons for MDM 會上傳 TLS 伺服器憑證和群組憑證。 您也可以從 **Sentry 憑證**區段之下的 **Sentry** 頁面上傳這些憑證。

Ivanti Neurons 在上傳時確認 Sentry 憑證，根據憑證中的條件返回以下類型的信息：

條件	資訊類型
分葉憑證並未包含任何憑證授權單位的鏈結，或是上傳的檔案中並無憑證授權單位	錯誤
沒有可用的根憑證授權單位。	警告
根憑證授權單位並未簽核分葉憑證的中繼憑證授權單位。	警告

Ivanti Neurons for MDM 也會驗證此文章中的規則。

程序

1. 在 **TLS 伺服器憑證**區段中，按一下**新增**。 **新增憑證**視窗顯示。
2. 在**憑證名稱**欄位中，輸入憑證名稱。
3. 輸入保護 PKCS12 檔案的密碼。
4. 按一下**選擇檔案**以上傳群組憑證。 確定檔案格式為 .p7b、.p12、.pfx、.pem、.der、.crt 或 .cer。
5. 按一下**新增**。 上傳的憑證會顯示在表格中。
6. 如要刪除 TLS 伺服器憑證，請按一下**動作**欄中的刪除圖示。

> 如果 TLS 伺服器憑證用於任何 Sentry 設定檔，您將無法刪除該憑證。 如果執行了刪除動作，系統將顯示錯誤訊息。

新增群組憑證

程序

1. 在**群組憑證**區段中，按一下**新增**。 **新增憑證**視窗隨即顯示。
2. 在**憑證名稱**欄位中，輸入憑證名稱。
3. 輸入保護 PKCS12 檔案的密碼。
4. 按一下**選擇檔案**以上傳群組憑證。 確定檔案格式為 .p7b、.p12、.pfx、.pem、.der、.crt 或 .cer。
5. 按一下**新增**。

如要刪除上傳的群組憑證，請按一下**動作**欄中的刪除圖示。

編輯 Sentry 根憑證

身為管理員，您可以選擇編輯 Sentry 根憑證組態的發佈。 您還可以透過將組態委派給其他空間，來為自訂空間管理員提供編輯權限。

1. 前往**配置**。
2. 搜尋 **Sentry 根憑證**。
3. 按一下編輯圖示。
4. 選取與要發佈憑證的裝置或裝置群組相應的核取方塊。 或者，清除與裝置或裝置群組相應的核取方塊。
5. 從「發佈摘要」區段中選取以下選項之一 (如果適用):
   - **不套用至其他空間**
   - **套用至其他空間中的裝置**
6. (選用) 按一下**允許空間管理員編輯發佈**核取方塊。

7. 按一下**儲存**。
8. 將顯示警告訊息。 按一下**是**以進行確認。

設定 App 搭配使用 AppTunnel

如需最新的 Sentry 指示說明，請造訪**產品文件**並按一下 Sentry。 選擇適合您 Sentry 版本的文件。

關於 AppTunnel 服務名稱

AppTunnel 服務用來定義 AppConnect app 要透過通道傳送資料到哪個後端服務。

如需最新版說明書，請瀏覽**產品說明文件**然後選擇適合 **Sentry** 和 **AppConnect** 版本的文件。

10.10.6.12. 個別 App VPN 組態

授權：Silver

適用於: iOS、watchOS、visionOS 和 tvOS 裝置

個別 App VPN 配置可定義下列特定 app 的虛擬私用網路存取設定：

- 個別 App VPN 設定
- Psec (Cisco)
- Cisco AnyConnect
- Juniper SSL
- NetMotion VPN
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- 自訂 SSL
- Palo Alto Networks GlobalProtect

> 個別 App VPN 配置取決於 App 配置。 在 App 配置設定期間建立個別 App VPN 配置。 當個別 App VPN 配置已刪除或未發佈，中斷 App 與網路的連線會使 App 配置功能發生問題。

發佈配置

從 Ivanti Neurons for MDM 版本 91 開始，全域管理員可委派空間管理員編輯「所有裝置」和「自訂」發佈選項的「個別應用程式 VPN 組態」。 對於「個別應用程式 VPN 組態」，您可以選擇性地選取「允許在所有空間中提供此組態」選項。

> 發佈變更僅適用於特定空間。 所有其他空間會繼承預設空間發佈設定。

根據適用情況使用下表中的資訊，在欄位中指定組態設定，然後分發組態:

如需更多資訊，請參閱使用配置中的*分發組態*主題。

個別 App VPN 設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
連線類型 啟用隨選即用 VPN	選擇要設定的 VPN 類型。 其餘設定取決於這個選項而定。 選擇針對建立隨選即用 VPN 的網域及主機名稱使用此配置。
啟用 iOS 規則 (僅選擇「啟用隨選即用 VPN」時適用) 啟用隨選即用 match app 啟用 5G 網路切片	若是 iOS 和 macOS，您可設定： • 網路規則：允許或不允許連線，以及允許或忽略評估為 True 的網路。 • 連線規則：必要時允許或絕對不允許連線至評估為 True 的網路。 對於網路規則，您可指定下列參數類型： • DNS 網域相符 • DNS 伺服器位址相符 • SSID 相符 • URL 字串探查 • 介面類型相符 對於連線規則，您可指定下列參數類型： • DNS 網域相符 • DNS 伺服器位址相符 • SSID 相符 • URL 字串探查 • 介面類型相符 • 網域 • DNS 伺服器 • URL 探測器 選擇以啟用 Per App 隨選即用 VPN。 選取要作為通道連線的 **DNN** (網路提供者提供的資料網路名稱)，以將特定行動數據切片 VPN 做為目標。 選取**應用程式類別** (由網路提供者提供)，以識別要作為通道連線的行動網路切片類型。
網域	
Safari 網域 (iOS)	此陣列中的項目必須分別指定在 Safari 中會觸發 VPN 連線的一個網域。 每個輸入項目的格式都是 www.apple.com。
iOS 14.0+ 與 macOS 11.0+	
關聯的網域	指定一或多個關聯的網域。 與其中一個網域中的伺服器的連線會與個別 app VPN 關聯。
排除的網域	指定一或多個排除的網域。 與其中一個網域中的伺服器的連線會從個別 app VPN 排除。

設定	方法
iOS 13+ 與 macOS 10.15+	
郵件網域	按一下 **+ 新增**以輸入一或多個網域，將會在郵件中觸發此 VPN 連線。 每個輸入項目的格式都是 www.apple.com。
聯絡人網域	按一下 **+ 新增**以輸入一或多個網域，將會在聯絡人中觸發此 VPN 連線。 每個輸入項目的格式都是 www.apple.com。
行事曆網域	按一下 **+新增**以輸入一或多個網域，將會在行事曆中觸發此 VPN 連線。 每個輸入項目的格式都是 www.apple.com。
iOS 9 及更新版本	
提供者類型 (iOS 9+)	選擇下列其中一個通道提供者： • App-Proxy - App 層的通道流量。 如需 App Proxy 提供者的概觀，請參閱 **Apple 說明文件**。 • 封包通道 - IP 層的通道流量。 如需封包通道提供者的概觀，請參閱 **Apple 說明文件**。

IPsec (Cisco)

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
機器驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
包括使用者 PIN 碼	選擇提示使用者輸入 PIN 碼。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

Cisco AnyConnect

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
群組	輸入要用來驗證連線的群組。
使用者驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 若您選取**手動**，便會出現下列附加欄位: • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 若您選取**自動**，便會出現下列附加欄位: • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

Juniper SSL

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
領域	輸入要用來驗證連線的憑證領域。
角色	輸入要用來驗證連線的憑證角色。
使用者驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 若您選取**手動**，便會出現下列附加欄位: • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 若您選取**自動**，便會出現下列附加欄位: • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

NetMotion VPN

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
使用者驗證	**憑證**是要使用的身份認證方法。 有以下欄位可用： **憑證**：選擇要使用的身份認證。 僅 iOS 裝置支援使用者提供的憑證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。 選擇下列選項： • 啟用隨選即用 VPN - 新增要建立隨選即用 VPN 的網域或主機名稱。 • 啟用 iOS 規則。 • 已啟用隨選即用 match app。
Safari 網域	按一下 **+ 新增**以新增 Safari 網域。
提供者類型 (iOS 9.0+)	**封包通道**預設選取為通道提供者類型。 如需封包通道提供者的概觀，請參閱 Apple 說明文件。

F5 SSL

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
使用者驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 若您選取**手動**，便會出現下列附加欄位: • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 若您選取**自動**，便會出現下列附加欄位: • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

SonicWALL Mobile Connect

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
登入群組或網域	輸入要用來驗證連線的登入群組或網域。
使用者驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 若您選取**手動**，便會出現下列附加欄位: • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 若您選取**自動**，便會出現下列附加欄位: • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

Aruba VIA

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
使用者驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 若您選取**手動**，便會出現下列附加欄位: • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 若您選取**自動**，便會出現下列附加欄位: • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

自訂 SSL

設定	方法
識別碼	輸入此自訂 SSL VPN 的識別碼 (和 DNS 格式相反，例如 com.mycompany.myserver)。
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
自訂資料	輸入可定義此 VPN 自訂資料的索引鍵/值組。
使用者驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 若您選取**手動**，便會出現下列附加欄位: • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 若您選取**自動**，便會出現下列附加欄位: • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。
(iOS 9.0+) 在主 VPN 和子 VPN 字典中包含 ProviderType	選擇在產生 plist (預先定義的組態檔案) 時包含提供者類型。
提供套件識別碼	輸入 VPN 提供者的套件識別碼。 您可以使用不同的提供者套件識別碼，為相同的應用程式維護多個應用程式組態。

Palo Alto Networks GlobalProtect

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。
自訂資料	輸入可定義此 VPN 自訂資料的索引鍵/值組。
使用者驗證	憑證是使用者的驗證方法。 選擇要在**憑證**欄位中使用的身分憑證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 若您選取**手動**，便會出現下列附加欄位: • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 若您選取**自動**，便會出現下列附加欄位: • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

若適用，鍵入 $ 可查看此欄位的支援**變數**清單。

相關主題:

如何建立配置

10.10.6.13. 單一登入配置

Ivanti Neurons for MDM 透過可延伸 SSO 和可延伸 SSO Kerberos 配置啟用可延伸單一登入 (SSO)。 實作需要從身份識別提供者取得 app 擴充功能，例如 Microsoft Authenticator。 實作可延伸 SSO 後，使用者在存取企業資源時只需要驗證身份一次。 後續登入時不會提示使用者進行驗證。 如需有關設定預期身分識別提供者的資訊，請參閱**設定身份識別提供者**。

本節包含以下各主題：

- **單一登入帳戶設定**
- **可延伸單一登入帳戶設定**
- **可延伸單一登入 Kerberos 帳戶設定**

單一登入帳戶設定

適用於：

- iOS 7.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- visionOS 1.1 到 Ivanti Neurons for MDM 所支援的最新發行版本。

使用以下設定對 iOS 裝置上任何受管理的 app 和 Apple Safari 瀏覽器設定基於 Kerberos 的企業單一登入。

> 此配置需要 Tunnel 和 Sentry。 如需更多資訊，請參閱 *Tunnel for iOS 指南*中的「使用 Kerberos 設定單一登入」。

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
使用者名稱	輸入 Kerberos 主要名稱。
Kerberos 領域名稱	輸入 Kerberos 領域名稱。
認證	**若是擁有 Gold 授權的 iOS 8：**請選擇要用來更新 Kerberos 憑證的認證。
URL 字首相符	若要使用這個帳戶透過 HTTP 進行 Kerberos 驗證，則必須符合 URL 字首清單。
SSO 的允許清單應用程式	新增 App Catalog 的 app 以將其加入 SSO 允許清單。 例如，輸入「Safari」以新增 Apple Safari。 使用此類型的配置時，如果沒有 SSO 允許清單，則支援 iOS SSO 所有 app 都可以使用 SSO，包括內建 iOS app。

可延伸單一登入帳戶設定

適用於：

- iOS 13.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- macOS 10.15 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- visionOS 1.1 到 Ivanti Neurons for MDM 所支援的最新發行版本。

使用以下設定使用一般延伸類型設定 SSO 延伸描述檔，為原生 app 和網站使用多種驗證方法啟用 SSO。

> 在使用者通道中向 macOS 10.15.x 裝置推送配置時，不適用可延伸 SSO。

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。

選擇 SSO 類型	選擇下列其中一個 SSO 類型：
	• **認證**
	  ◦ 輸入一或多個可透過 app 擴充功能驗證的**主機**名稱或網域名稱。 主機或網域名稱不區分大小寫，且所有已安裝的可延伸 SSO 裝載的主機/網域名稱都必須是獨一無二的。 以「.」開頭的主機是萬用字元尾碼，並且將符合所有子網域，否則主機必須完全相符。
	  ◦ 輸入**領域**名稱。 此值應正確大寫。
	• **重新導向**
	  ◦ 輸入身份識別提供者的一或多個 **URL** 首碼，app 擴充功能會在這裡執行 SSO。 URL 將會以 http:// 或 https:// 為開頭，架構和主機名稱不區分大小寫，不允許查詢參數和 URL 片段，且所有已安裝的可延伸 SSO 裝載的 URL 都必須是獨一無二的。

延伸識別碼	針對指定的 URL 輸入執行 SSO 的 app 擴充功能套件識別碼。
團隊識別碼	app 擴充功能的團隊識別碼。 在 macOS 上需要此金鑰，其他的可忽略。
自訂資料	輸入一或多個自訂資料為鍵/值組。
驗證方式 (僅適用於 macOS 13+)	• 密碼 • 使用者 Secure Enclave 金鑰
註冊權杖	輸入權杖。 一旦您選取了其中一種驗證方式，此欄位便會啟用。
畫面鎖定行為 (適用於 iOS 15.0+ 和 macOS 12.0+)	請選擇下列選項之一： • **取消**: 畫面鎖定時，系統會取消驗證請求。 • **請勿處理**:畫面鎖定時，驗證請求會繼續，但不使用 SSO。
拒絕的捆綁包標識符 (適用於 iOS 15.0+ 和 macOS 12.0+)	針對不使用此擴充功能提供的 SSO 的應用程式，為其新增多個套件識別碼。 例如，*com.company.appname.www*。

適用於: macOS 14.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。

設定	描述
帳戶顯示名稱	輸入在通知和身分要求中顯示的帳戶名稱。
其他群組	輸入沒有管理員存取權限的群組名稱。
管理員群組	輸入具有管理員存取權限的群組名稱。
驗證方式	從下拉式清單中選取一個驗證方法: • 密碼 • 使用者 Secure Enclave 金鑰 • 智慧卡
授權群組	輸入群組名稱的授權權限。
啟用授權	選取核取方塊可為管理員群組、授權群組或其他群組啟用授權提示。
啟用登入時建立使用者	選取核取方塊可在登入期間使用密碼或智慧卡作為驗證方法來建立新的使用者。
登入頻率	系統完全登入而非完成重新整理所需的持續時間，以秒為單位。 預設值為 64,800 秒 (18 小時)。 最低值為 3600 秒 (1 小時)。
新使用者授權模式	從下拉式清單中為新使用者選取一種授權模式: • 標準: 標準使用者帳戶。 • 管理員: 系統會將帳戶新增至本機管理員群組。 • 群組: 系統會自動將新使用者分組到管理員群組、授權群組或其他群組下。
權杖對使用者對應	輸入新使用者的帳戶名稱和全名，以對應他們進行授權。
使用者授權模式	從下拉式清單中為使用者選取一種授權模式: • 標準: 標準使用者帳戶。 • 管理員: 系統會將帳戶新增至本機管理員群組。 • 群組: 系統會自動將新使用者分組到管理員群組、授權群組或其他群組下。
使用者共用裝置金鑰	選取核取方塊可為所有使用者啟用相同的登入和加密金鑰。

適用於: macOS 15.4 到 Ivanti Neurons for MDM 所支援的最新發行版本。

設定	描述
允許裝置識別碼證明	選取核取方塊以在平台 SSO 證明中包含裝置的 UDID 和序列號，從而允許對已註冊裝置進行後端追蹤。

適用於: macOS 14.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。

若要檢視可延伸單一登入帳戶設定，請選取**驗證方式**欄位的下拉式選項中的**密碼**。

設定	描述
FileVault 原則	啟用檢視以下設定的原則: • 嘗試驗證 • 需要身份認證 選取**需要驗證**核取方塊以啟用其他組態設定。 • 允許離線寬限期 • 允許驗證寬限期
登入原則	啟用檢視以下設定的原則: • 嘗試驗證 • 需要身份認證 選取**需要驗證**核取方塊以啟用其他組態設定。 • 允許離線寬限期 • 允許驗證寬限期
解除鎖定原則	啟用檢視以下設定的原則: • 嘗試驗證 • 需要身份認證 選取**需要驗證**核取方塊以啟用其他組態設定。 • 允許離線寬限期 • 允許驗證寬限期 • 允許 TouchID 或監視解除鎖定
驗證寬限期	選取其中一個原則後，輸入使用未註冊本機帳戶的時間長度。 如果您選取其中一個原則中的**允許驗證寬限期**核取方塊，則此欄位會變成必填欄位。
離線寬限期	成功登入平台 SSO 並選取其中一個原則後，輸入使用離線本機帳戶密碼的時間長度。 如果您選取其中一個原則中的**允許離線寬限期**核取方塊，則此欄位會變成必填欄位。
非平台 SSO 帳戶	選取 **+ 新增**以輸入不受 FileVault、登入或解除鎖定原則約束的使用者名稱清單。

可延伸單一登入 Kerberos 帳戶設定

適用於：

- iOS 13.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- macOS 10.15 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- visionOS 1.1 到 Ivanti Neurons for MDM 所支援的最新發行版本。

使用以下設定來設定使用 Kerberos 擴充功能執行 SSO 的 app 擴充功能。

> 在使用者通道中向 macOS 10.15.x 裝置推送配置時，不適用可延伸 SSO Kerberos。

設定	描述
基本設定	
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
使用者名稱	輸入 Kerberos 主要名稱。
領域	輸入 Kerberos 領域名稱。
認證	選擇要用於更新 Kerberos 認證的憑證。
URL 字首	若要使用這個帳戶透過 HTTP 進行 Kerberos 驗證，則必須符合 URL 字首清單。
進階設定	
允許自動登入	若為 False，則不允許將密碼儲存至 Keychain。 預設啟用此選項。
延遲使用者設定	若為 True 則不會提示使用者設定 Kerberos 擴充功能，直到管理員使用 app-sso 工具啟用它或收到 Kerberos 挑戰。 此選項適用於 macOS 11 到 Ivanti Neurons for MDM 所支援的最新版本。
需使用者在場	若為 True，使用者需要提供 Touch ID、Face ID，或密碼，以存取 Keychain 項目。
監視認證快取	若為 False，則在下次比對 Kerberos 挑戰或網路狀態變更時需要認證。 如果認證過期或遺失，將會建立新的認證。 此選項適用於 macOS 11 到 Ivanti Neurons for MDM 所支援的最新版本。 預設啟用此選項。
快取名稱	輸入要使用的 Kerberos 快取同屬安全服務 (GSS) 名稱。 此選項現已棄用。
網域領域對應	輸入和金鑰相同的領域名稱。 此值為對應領域的一組 DNS 尾碼。 按一下 **+新增**以新增一或多個鍵值組。
預設領域	如果有多個 Kerberos 擴充組態此屬性指出它是預設領域。
使用網站自動探索	若為 False，Kerberos 擴充功能就不會自動使用 LDAP 和 DNS 以判斷其 AD 站台名稱。 預設啟用此選項。
站台碼	輸入 Kerberos 擴充功能應使用的 Active Directory 站台名稱。
複寫時間	輸入複寫 Active Directory 網域中的變更所需的秒數時間。 在變更後檢查密碼有效期限時，Kerberos 擴充功能將會使用它。 此選項適用於 macOS 11 到 Ivanti Neurons for MDM 所支援的最新版本。 此選項現已棄用。
認證套件 ID ACL	按一下 **+新增**以新增允許存取 Ticket Granting Ticket (TGT) 進行驗證的套件 ID 清單。
將受管理的 App 包含在套件 ID ACL	若為 True，Kerberos 擴充功能將允許僅受管理的 app 存取和使用認證。 若指定，則除了認證套件 ID ACL 之外，還會使用它。 此選項適用於 iOS 14 或 Ivanti Neurons for MDM 所支援的更新版本。
將 Kerberos App 包含在套件 ID ACL	若為 true，Kerberos 擴充功能將允許標準 Kerberos 公用程式 (包括「票券檢視程式」和 klist) 存取和使用認證。 適用於 macOS 12 和更新版本。

設定	描述
自訂使用者名稱標籤	請輸入 Kerberos 延伸模組中所使用的自訂使用者名稱標籤，而非「使用者名稱」。例如，「公司 ID」。此選項適用於 macOS 11 到 Ivanti Neurons for MDM 所支援的最新版本。
說明文字	輸入使用者會在 Kerberos 在登入視窗底部看到的文字。 它可用於顯示說明資訊或免責聲明文字。 此選項適用於 iOS 14 和 macOS 11 到 Ivanti Neurons for MDM 所支援的最新版本。
認證使用模式	此設定會影響其他程序如何使用 Kerberos 擴充功能認證。 請使用下列任一： • 永遠 (預設) - 如果服務主體名稱 (SPN) 與 Kerberos 擴充功能主機陣列相符，將會一律使用擴充功能認證。 如果未在 credentialBundleIDACL 中叫用 app，將不會使用認證。 • 未指定時 - 只有當呼叫程式未指定其他認證且 SPN 與 Kerberos 擴充功能主機陣列相符時，才會使用此認證。 如果未在 credentialBundleIDACL 中叫用 app，將不會使用認證。 • Kerberos 預設 - 使用預設 Kerberos 程序來選擇認證時，通常會使用預設 Kerberos 認證。 這等同於關閉此功能。 (選用) 選擇**LDAP 需要 TLS**。
偏好的金鑰發佈中心	新增偏好的金鑰發佈中心。 按一下 **+新增**以新增偏好的 KDC。
	允許平台 SSO 驗證後援 - 若為 True 並且「使用平台 SSO TGT」為 True，則允許使用者手動登入。 適用於 macOS 13 及以上版本 **僅執行 Kerberos** - 若為 True，則 Kerberos 延伸模組僅處理 Kerberos 請求。 適用於 macOS 13 及以上版本。 **使用平台 SSO TGT** - 若為 True，則此組態會使用平台 SSO 中的 TGT，而不是申請新的 TGT。 適用於 macOS 13 及以上版本。
設定切換到密碼模式	如果為 True，則允許使用者將使用者介面切換到「密碼」模式。 適用於 macOS 15 及以上版本。
設定切換到智慧卡模式	如果為 True，則允許使用者將使用者介面切換到「智慧卡」模式。 適用於 macOS 15 及以上版本。
設定以智慧卡模式啟動	如果為 True，則使用者介面會以「智慧卡」模式啟動。 適用於 macOS 15 及以上版本。
身份頒發者自動選擇篩選器	篩選可用智慧卡的清單。 適用於 macOS 15 及以上版本。
密碼設定	
允許密碼變更	若為 False，停用密碼變更。 此選項適用於 macOS 10.15 到 Ivanti Neurons for MDM 所支援的最新版本。 預設啟用此選項。
密碼變更 URL	輸入當初始密碼變更時，將會在使用者預設的網頁瀏覽器中開啟此 URL。 此選項適用於 macOS 10.15 到 Ivanti Neurons for MDM 所支援的最新版本。
允許密碼複雜度	若為 true，則密碼必須符合 Active Directory 的「複雜」定義。此選項適用於 macOS 10.15 到 Ivanti Neurons for MDM 所支援的最新版本。

設定	描述
密碼長度下限	輸入網域的密碼最小長度 (字元數)。 此選項適用於 macOS 10.15 到 Ivanti Neurons for MDM 所支援的最新版本。
密碼到期通知	輸入在密碼到期之前，提前寄送密碼到期通知給使用者的天數。 此選項適用於 macOS 10.15 到 Ivanti Neurons for MDM 所支援的最新版本。 預設值為 15 天。
密碼到期覆寫	輸入密碼在此網域上可使用的天數。 針對大部分的網域，會自動計算此天數。 此選項適用於 macOS 10.15 到 Ivanti Neurons for MDM 所支援的最新版本。 (此選項現已被取代)
需要密碼文字	輸入網域的密碼要求文字版本。 僅用於如果未指定 pwReqComplexity 或 pwReqLength。 此選項適用於 macOS 10.15 到 Ivanti Neurons for MDM 所支援的最新版本。
密碼記錄計數	輸入在此網域上無法重複使用之前密碼的個數。 此選項適用於 macOS 10.15 到 Ivanti Neurons for MDM 所支援的最新版本。
密碼最短有效期限	輸入在此網域上的密碼最短有效期限 (天數)，之後就可變更密碼。 此選項適用於 macOS 10.15 到 Ivanti Neurons for MDM 所支援的最新版本。
一律同步本機密碼	若為 False，停用密碼同步。 如果使用者使用行動帳戶登入則不適用。 此選項適用於 macOS 10.15 到 Ivanti Neurons for MDM 所支援的最新版本。
密碼要求 RTF 資料	網域密碼要求的 RTF 檔案格式版本。 適用於 macOS 15 及以上版本。 僅在未指定 pwReqComplexity 或 pwReqLength 時使用。

如需更多資訊，請參閱**如何建立配置**

10.10.6.14. 網路轉送組態

Ivanti Neurons for MDM 可為承載啟用網路轉送組態，以用於配置裝置或應用程式的轉送設定，且無需 VPN 或通道來存取私人資源。

適用於

- iOS 17.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- macOS 14 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- visionOS 1.1 到 Ivanti Neurons for MDM 所支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取**網路轉送**組態。
3. 依下表配置**網路轉送**設定:

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
HTTP/3 轉送 URL	指定用作此組態 HTTP 欄位值的 URL 值。 包含 HTTP/2 轉送 URL 和/或 HTTP/3 轉送 URL。
HTTP/2 轉送 URL	指定用作此組態 HTTP 欄位值的 URL 值。 包含 HTTP/2 轉送 URL 和/或 HTTP/3 轉送 URL。
其他 HTTP 標頭欄位	為對應的標頭欄位名稱指定 HTTP 標頭欄位值。
認證	從下拉清單中選取您所建立的身分識別憑證之一。
原始公開金鑰	指定原始公開金鑰以在網路連線期間驗證伺服器。
+ 新增	選取 **+ 新增**以新增多個網路轉送組態。
比對網域	指定網域清單以判斷透過「轉送」中的伺服器路由哪個連線。
排除網域	指定網域清單以判斷透過「轉送」中的伺服器避免哪個連線。
比對 FQDN (在 iOS 18.4+ 和 macOS 15.4+ 裝置上受支援)	指定應透過轉送中包含的伺服器路由的完整網域名稱 (FQDN) (也稱為主機名稱) 清單。 任何與 此確切 FQDN 或主機名稱相符的連線都將使用轉送。 如果沒有列出 FQDN 和「MatchDomains」，則所有網域的流量 (與排除的域或排除的 FQDN 相符的除外) 都將路由到轉送伺服器。
排除 FQDN (在 iOS 18.4+ 和 macOS 15.4+ 裝置上受支援)	指定**不應**透過轉送中包含的伺服器路由的完整網域名稱 (FQDN) (也稱為主機名稱) 清單。 任何與 FQDN 完全相符的連線都不會使用轉送伺服器。 當還指定了「MatchDomains」時，「ExcludedFQDNs」中列出的任何 FQDN 都應該是至少一個 MatchDomain 的子域。 否則，它不會有任何效果。

4. 按**下一步**，確認發佈設定。
5. 選取其中一個發佈選項以設定**網路轉送**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
6. 按一下**完成**。

10.10.6.15. iOS 多位使用者安全登入

多使用者網頁剪輯可讓使用者登入和登出在 Ivanti Neurons for MDM 上註冊的 iOS 裝置。 當使用者初次登入時，會將與該使用者關聯的描述檔、app 和配置推送至裝置。 當他們完成工作時，可開啟 Web Clip 並選擇「登出」功能，只要配置和 app 尚未發佈至 Nobody 使用者，就可以將裝置指派給 Nobody 使用者，並移除與原始登入的使用者關聯之描述檔、app 和配置。 在登出後，Web Clip 會重設，以便讓下位使用者登入並取得其自訂配置、app 和原則。 使用多位使用者安全登入無需裝置監管。 請參閱支援知識庫文章 **Ivanti Neurons for MDM：適用於 iOS 的多使用者安全登入**以深入瞭解多使用者登入功能。

適用於: iOS 裝置 (不適用於使用者註冊的裝置)

本節包含以下各主題：

- **支援的認證**
- **瞭解 Nobody 使用者**
- **登入裝置**
- **登出裝置**

支援的認證

登入多使用者安全登入 Web Clip 必須使用使用者名稱和密碼。 多使用者安全 Web 剪輯不支援 PIN 碼型註冊。

程序

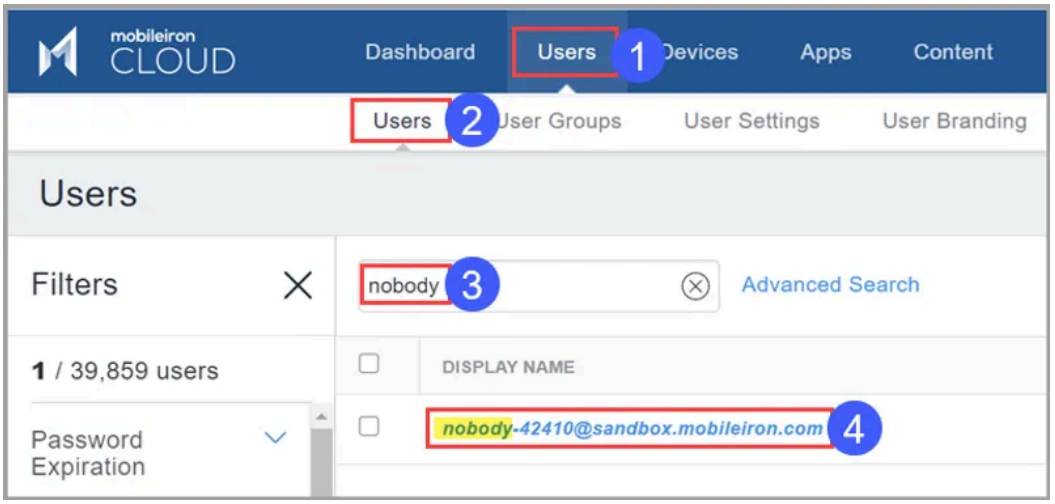
1. 前往**配置**。
2. 按一下 **iOS 多位使用者安全登入**。 如果配置有多頁，您可能需要使用搜尋功能以尋找它。 選擇 **+新增**無法存取此配置。
3. 按一下**編輯發佈**或關聯的圖示，將 Web Clip 發佈至適合的裝置群組。

如果您想要將它發佈至某個使用者群組，您可以建立綁定至使用者群組的動態裝置群組。
4. 選擇以下發佈選項之一，請記住您必須一律將 Web Clip 發佈至 Nobody 使用者，或是 Nobody 使用者關聯的裝置群組。 此動作預設為停用，請確定您將它發佈至 Nobody 使用者。
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂

按一下**儲存**。

瞭解 *Nobody* 使用者

當裝置已透過網頁剪輯登出時，它仍會註冊到 Ivanti Neurons for MDM 中稱為「Nobody 使用者」的特殊使用者。 當使用者登出時，如果您要從 app 和配置從裝置移除，您必須確定不會將那些 app 和配置發佈至 Nobody 使用者。 當使用者登出安全登入 Web Clip 時，如果您要讓某些配置 (例如 Wi-Fi) 保留在裝置上，則必須確定也會將這些配置發佈至 Nobody 使用者。



這表示您必須注意您將 app 和配置發佈至的使用者群組和裝置群組。 如果您將 app 發佈給每個人，而您希望當使用者登出裝置時將它移除，最佳做法是建立一個不包含 Nobody 使用者的使用者群組。 自訂屬性可讓您更容易建立一個包含「多使用者」的使用者群組，和另一個只包含 Nobody 使用者的使用者群組。 您可以從「管理 > 系統 > 屬性」建立使用者屬性，然後將「是」或「True」值指派給 Nobody 使用者。 然後您可以基於屬性建立使用者群組和裝置群組。

登入裝置

使用者可登入 iOS 裝置並將裝置指派給自己。 登入後，所有相關的應用程式、原則、配置和憑證隨即推送至裝置。

> 出於安全原因，iDP 使用者每次登入時都必須重新進行身分驗證，即使他們已經登入裝置。

登出裝置

使用後，使用者可以登出自己的 iOS 裝置。 登出後，應用程式、原則、配置和憑證隨即從裝置上移除；裝置會恢復到使用者登入前的狀態。 如此一來，裝置即可供其他使用者登入。

> 從多使用者 Web 剪輯登出之前，請先從所有 Microsoft 應用程式登出。

如需更多資訊，請參閱多使用者登入品牌化

10.10.6.16. Android APN 設定配置

Android APN 設定配置可讓您設定裝置在公用網路上所需的存取點名稱 (APN) 設定。 此配置適用於 Android Enterprise 受工作管理裝置和搭配公司擁有裝置上的工作描述檔的受管理裝置 (在 Android 9.0 版或支援的更新版本)。

程序

1. 前往**配置** > **+新增**。
2. 選擇 **Android APN 設定**配置。
3. 輸入配置的名稱。
4. 輸入描述。
5. 在「配置設置」區段中，設定下列選項：
6. 按**下一步**。

設定	描述
項目名稱	輸入存取點設定名稱。
存取點名稱	輸入存取點名稱。
存取點類型	從下列選項選擇存取點類型： • **預設** • **DUN** • **IMS** • **緊急** • MMS • **HIPRI** • **CBS** • **MCX** • **SUPL** • **FOTA** • **IA**
MVNO 碼類型	從以下選項中選擇行動虛擬網路業者類型： • **無** • **SPN** • **IMSI** • **GID** • **ICCID**
Bearer	從以下選項中選擇資料傳輸使用的載送服務類型： • **1xRTT** • **CDMA** • **EDGE** • **EHRPO** • **EVDO** • **EVDO A** • **EVDO B** • **GPRS** • **GSM** • **HSDPA** • **HASP** • **HSPAP** • **HSUPA** • **IDEN**

設定	描述
	• **IWLAN** • **LTE** • **NR** • **TD_SCDMA** • **UMTS**
APN 通訊協定	選擇 APN 所需的 APN 通訊協定。 下列為可用的選項： • **無** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP** (點對點通訊協定) • **非結構化**
APN 漫遊協定	選擇 APN 所需的 APN 漫遊協定。 下列為可用的選項： • **無** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP** (點對點通訊協定) • **非結構化**
啟用/停用 APN	啟動 APN 配置。
電信業者 ID	輸入電信業者 ID 的數值。
驗證類型	從下列選項選擇驗證通訊協定類型： • **無** • **PAP** (密碼驗證通訊協定) • **CHAP** (Challenge-Handshake 驗證通訊協定) • **PAP 或 CHAP**
使用者名稱	輸入登入使用者名稱。
密碼	輸入登入密碼。
確認密碼	再次輸入密碼以確認。
連接埠號	輸入連接埠號 (介於 1 到 65535 之間的數值)。
Proxy 位址	輸入 Proxy 位址。

設定	描述
行動電話國家/地區碼	輸入行動電話國家/地區碼。
行動電話網路碼	輸入行動電話網路碼。
MMS Proxy 位址	輸入多媒體訊息 Proxy 位址。
MMS 連接埠號	輸入多媒體訊息連接埠號 (介於 1 到 65535 之間的數值)。
MMS 伺服器位址 (mmsc)	輸入多媒體訊息伺服器位址。

7. 請選擇下列發佈選項之一：
8. 按一下**完成**。

- **所有裝置**
- 沒有裝置 (預設)
- **自訂**

如果裝置已有現有 APN 配置，且該配置在下列欄位中具有相同的值，您將無法新增具有這些值的其他 APN 配置：

- 行動電話國家/地區碼
- 行動電話網路碼
- 存取點名稱
- Proxy 位址
- 連接埠號
- MMS Proxy 位址
- MMS 連接埠號
- MMS 伺服器位址
- 啟用/停用 APN
- MVNO 碼類型
- APN 通訊協定
- APN 漫遊協定

Android APN 設定配置會覆寫已在裝置中手動或由網路業者配置的 APN 設定。

10.10.6.17. VPN 組態

適用於：

- Android (Android Enterprise 裝置已棄用。 您需要使用應用程式目錄中特定 VPN 的受控組態。)
- Windows
- iOS
- macOS
- tvOS
- visionOS

VPN 配置可定義虛擬私人網路的存取設定。

> 此組態可使用具有自訂分發選項的委派。 如需更多資訊，請參閱使用配置中的*分發組態*主題。

程序

1. 前往**配置** > **+新增**。
2. 選擇 **VPN** 配置。
3. 輸入配置的**名稱**。
4. 輸入描述。
5. 依下列描述進行 VPN 設定。
6. (僅限 iOS 9.0+) 在「相符網域」區段中，按一下 **+ 新增**，以輸入一或多個相符網域 (範例：company.com)。 當網域為下列指定網域之一時，請使用 Proxy 連線。
7. 按**下一步**。
8. (僅限 macOS) 在「發佈」頁面中，選擇下列其中一個發佈選項：
   - 裝置通道 - 此配置適用於裝置上的所有使用者，也是一般選項。
   - 使用者通道 - 此組態僅適用於裝置上目前註冊的使用者。
9. 選擇此配置的其餘發佈選項。
10. 按一下**完成**。

VPN 設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
連線類型	選擇要設定的 VPN 類型。 其餘設定取決於這個選項而定。

通訊協及其設定如下：

- L2TP (Ivanti Go 不支援)

- **PPTP** (Ivanti Go 不支援)
- **IPsec (Cisco)** (Ivanti Go 不支援)
- **Cisco AnyConnect** (Ivanti Go 支援)
- **Juniper SSL** (Ivanti Go 不支援)
- **NetMotion VPN** (Ivanti Go 不支援)
- Pulse Secure (Ivanti Go 支援)
- **F5 SSL** (Ivanti Go 不支援)
- **SonicWALL Mobile Connect** (Ivanti Go 不支援)
- **Aruba VIA** (Ivanti Go 不支援)
- **自訂 SSL** (Ivanti Go 不支援)
- **Palo Alto Networks GlobalProtect** (Ivanti Go 支援)
- **KEv2 (僅限 Windows)** (Ivanti Go 不支援)
- **IKEv2** (Ivanti Go 不支援)

L2TP

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
使用者驗證	選擇要使用的驗證方法：**密碼**或 **RSA SecurID**。
共用密碼	如果要啟動連線需具備共用密碼，請輸入。
傳送所有流量	選擇此選項，讓所有網路流量都使用此連線。 此選項有助於保護資料不受威脅，尤其是針對公用網路。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

PPTP

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
使用者驗證	選擇要使用的驗證方法：**密碼**或 **RSA SecurID**。
加密層級	選擇連線的資料加密層級：**無，自動**或**最大 (128 位元)**。
傳送所有流量	選擇此選項，讓所有網路流量都使用此連線。 此選項有助於保護資料不受威脅，尤其是針對公用網路。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

IPsec (Cisco)

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
機器驗證	選擇要使用的驗證方法：**共用密碼/群組名稱**或**認證**。
群組名稱 共用密碼 使用混合驗證	共用密碼/群組名稱驗證。 指定要使用的群組名稱。 如果使用混合驗證，字串結尾必須為「[hybrid]」。 共用密碼/群組名稱驗證。 輸入共用密碼。 共用密碼/群組名稱驗證。 選擇指定混合憑證，例如：伺服器提供驗證，而用戶端提供預先共用金鑰。
提示輸入密碼	共用密碼/群組名稱驗證。 指定連接時是否要提示使用者輸入密碼。
認證 包括使用者 PIN 碼	*認證驗證* 選擇要使用的身份認證。 *認證驗證* 選擇提示使用者輸入 PIN 碼。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

Cisco AnyConnect

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
群組	輸入要用來驗證連線的群組。
使用者驗證	選擇要使用的使用者驗證方法：**密碼**或**認證**。 如果選擇**認證**，即會顯示下列欄位： **憑證**：選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

Juniper SSL

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
領域	輸入要用來驗證連線的憑證領域。
角色	輸入要用來驗證連線的憑證角色。
使用者驗證	選擇要使用的使用者驗證方法：**密碼**或**認證**。 如果選擇**認證**，即會顯示下列欄位： **憑證**：選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

NetMotion VPN

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
使用者驗證	選擇要使用的使用者驗證方法：**密碼**或**認證**。 如果選擇**認證**，即會顯示下列欄位： **憑證**：選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

F5 SSL

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。
使用者驗證	輸入要使用的使用者驗證方法：**密碼**或**認證**。 如果選擇**認證**，即會顯示下列欄位： **憑證**：選擇要使用的身份認證。
Proxy 設定	選擇「手動」或「自動」，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

SonicWALL Mobile Connect

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
登入群組或網域	輸入要用來驗證連線的登入群組或網域。
使用者驗證	選擇要使用的使用者驗證方法：**密碼**或**認證**。 如果選擇「認證」，即會顯示下列欄位： **憑證**：選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

Aruba VIA

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
使用者驗證	選擇要使用的使用者驗證方法：**密碼**或**認證**。 如果選擇**認證**，即會顯示下列欄位： **憑證**：選擇要使用的身份認證。
Proxy 設定	選擇「手動」或「自動」，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

自訂 SSL

設定	方法
識別碼	輸入此自訂 SSL VPN 的識別碼 (和 DNS 格式相反，例如 com.mycompany.myserver)。
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
自訂資料	輸入可定義此 VPN 自訂資料的索引鍵/值組。
使用者驗證	選擇要使用的使用者驗證方法：**密碼**或**認證**。 如果選擇「認證」，即會顯示下列欄位： **憑證**：選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

Palo Alto Networks GlobalProtect

不適用於 Android 裝置。

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。
自訂資料	輸入可定義此 VPN 自訂資料的索引鍵/值組。
使用者驗證	選擇要使用的使用者驗證方法：**密碼**或**認證**。 如果選擇「認證」，即會顯示下列欄位： **憑證**：選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

IKEv2 (僅限 Windows)

設定	方法
伺服器	輸入 VPN 伺服器的主機名稱或 IP 位址。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

IKEv2

設定	方法
伺服器	輸入 VPN 伺服器的主機名稱或 IP 位址。
本機識別碼	IKEv2 用戶端識別碼應為下列格式之一： • FQDN • UserFQDN • 位址 • ASN1DN
遠端識別碼	遠端識別碼應為下列格式之一： • FQDN • UserFQDN • 位址 • ASN1DN
機器驗證	僅有當未選擇**啟用 EAP** 時才可使用此選項。 請選擇下列選項之一： • 認證 • 共用密碼
EAP 驗證	僅有當選擇**啟用 EAP** 時才可使用此選項。 請選擇下列選項之一： • 認證 • 使用者名稱/密碼
共用密碼	僅有針對「機器憑證」選擇「共用密碼」時，才可使用。 輸入連線的共用密碼。
認證	僅有針對「機器憑證」選擇「認證」時，才可使用。 選擇要使用的認證。 系統會傳送此認證，以供 IKE 用戶端驗證使用。 如果使用擴充驗證，此認證就可用於 EAP-TLS。
啟用 EAP	選擇啟用擴充驗證。
帳戶	僅有當選擇「EAP 認證」的「使用者名稱/密碼」時，才可使用此選項。 輸入 VPN 伺服器的帳戶 ID。
密碼	僅有當選擇「EAP 認證」的「使用者名稱/密碼」時，才可使用此選項。 輸入 VPN 伺服器的密碼。
Dead Peer Detection 間隔	請選擇下列選項之一： • 無 (停用) • 低 (存留項目每隔 1 小時傳送) • 中 (存留項目每隔 30 分鐘傳送) • 高 (存留項目每隔 10 分鐘傳送)
伺服器憑證發行者一般名稱	(選用) - 伺服器憑證發行者的一般名稱，使 IKE 伺服器根據憑證發行者傳送憑證要求給伺服器。
伺服器憑證一般名稱	(選用) - 伺服器憑證的一般名稱，用於驗證 IKEv2 伺服器傳送的憑證。
使用 IP4 和 IP6 子網路屬性	(選用) 選取以使用 IP4 和 IP6 子網屬性。

設定	方法
啟用 IKEv2 行動性與多宿主通訊協定 (MOBIKE)	(選用) 預設的設定為 0。 啟用 MOBIKE (其為一種功能，可支援使用多個 IP 位址連接至 Wi-Fi 和行動數據連結之多重網路介面的行動裝置)。 預設為啟用。 設為 1 可停用 MOBIKE。
啟用完整轉寄密碼 (PFS)	(選用) 設定為 1 時，啟用 IKEv2 連線的 PFS。 (選用) 預設值為 0。
啟用 IKEv2 重新導向	(選用) 預設的設定為 0。 如果伺服器收到重新導向要求時，系統會重新導向 IKEv2 連線。 預設為啟用。 設為 1 時，會停用 IKEv2 重新導向。
啟用 NAT Keepalive	啟用網路位址轉譯 KeepAlive，可在 IKE 對等項目之間有 NAT 時，防止任何缺失流量中的 NAT 項目受到刪除。
NAT keepalive 間隔	若啟用 NAT Keepalive，則這就是為裝置傳送 Keepalive 封包的時間 (以秒為單位)。
PPK	輸入支援 RFC 8784 之 VPN 伺服器的後量子預先共用金鑰 (PPK)。 如果此密鑰存在，則 PPK 識別碼也必須存在。
PPK 識別碼	輸入 PPK 識別碼。
強制要求 PPK	選取下列其中一個下拉式選項: • **授權**: 如果伺服器支援 RFC 8784 或接受在 PPK 識別碼中指定的 PPK 識別碼，則將成功建立 VPN 連線。 • **非授權**: 如果伺服器不支援 RFC 8784 或不接受在 PPK 識別碼中指定的 PPK 識別碼，則將無法建立 VPN 連線。
加密演算法	請選擇下列選項之一： • **DES** • **3DES** • **AES-128** • **AES-256** (預設) • **AES-128 GCM** • **AES-256 GCM**
完整性演算法	請選擇下列選項之一： • **SHA2-256** (預設) • **SHA2-384** • **SHA2-512**
Diffie Hellman 群組	請選擇下列選項之一： • **1** • **2** (預設值) • **5** • **14** • **15** • **16**

設定	方法
	• **17** • **18**
有效期 (分鐘)	以分鐘為單位，輸入 SA 有效期 (金鑰更新間隔)。 有效值為 10 到 1440。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

*輸入 $ 可查看支援的**變數**清單 (如果此欄位適用的話)。

如需更多資訊，請參閱**如何建立配置**

10.10.6.18. 隨選即用 VPN

適用於：iOS 裝置

隨選即用 VPN 配置可依據網域、主機名稱等項目來設定 VPN 伺服器的存取權。

隨選即用 VPN 設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
連線類型 啟用隨選即用 VPN	選擇要設定的 VPN 類型。 其餘設定取決於這個選項而定。 選擇針對建立隨選即用 VPN 的網域及主機名稱使用此配置。
啟用 iOS 規則 (僅選擇「啟用隨選即用 VPN」時適用) 提供者類型 (iOS 9+)	若是 iOS 和 macOS，您可設定： • 網路規則：允許或不允許連線，以及允許或忽略評估為 True 的網路。 • 連線規則：必要時允許或絕對不允許連線至評估為 True 的網路。 對於網路規則，您可指定下列參數類型： • DNS 網域相符 • DNS 伺服器位址相符 • SSID 相符 • URL 字串探查 • 介面類型相符 對於連線規則，您可指定下列參數類型： • DNS 網域相符 • DNS 伺服器位址相符 • SSID 相符 • URL 字串探查 • 介面類型相符 • 網域名稱 • DNS 伺服器 • URL 探測器 選擇下列其中一個通道提供者： • App-Proxy - App 層的通道流量。 如需 App Proxy 提供者的概觀，請參閱 Apple 說明文件。 • 封包通道 - IP 層的通道流量。 如需封包通道提供者的概觀，請參閱 Apple 說明文件。
EnforceRoutes	啟用後，VPN 的非預設路由會覆寫任何本機定義的路由。 • 如果啟用了 IncludeAllNetworks，系統將忽略 EnforceRoutes 設定 • 適用於 iOS 14.2 和更新版本。
ExcludeLocalNetworks	與 IncludeAllNetworks 一起啟用時，所有本機網路流量都會路由到 VPN 之外。
IncludeAllNetworks	啟用後，系統會透過 VPN 路由所有流量。

通訊協及其設定如下：

- IPsec (Cisco)

- Cisco AnyConnect
- Juniper SSL
- NetMotion VPN
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- 自訂 SSL
- Palo Alto Networks GlobalProtect

IPsec (Cisco)

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
機器驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
包括使用者 PIN 碼	選擇提示使用者輸入 PIN 碼。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

Cisco AnyConnect

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
群組	輸入要用來驗證連線的群組。
使用者驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

Juniper SSL

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
領域	輸入要用來驗證連線的憑證領域。
角色	輸入要用來驗證連線的憑證角色。
使用者驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

NetMotion VPN

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
使用者驗證	憑證是使用者的驗證方法。 **憑證**：選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

F5 SSL

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
使用者驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

SonicWALL Mobile Connect

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
登入群組或網域	輸入要用來驗證連線的登入群組或網域。
使用者驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

Aruba VIA

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
使用者驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

自訂 SSL

設定	方法
識別碼	輸入此自訂 SSL VPN 的識別碼 (和 DNS 格式相反，例如 com.mycompany.myserver)。
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。*
自訂資料	輸入可定義此 VPN 自訂資料的索引鍵/值組。
使用者驗證	僅支援認證驗證。
認證	選擇要使用的身份認證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

Palo Alto Networks GlobalProtect

設定	方法
伺服器	輸入 VPN 伺服器的 IP 位址或主機名稱。
帳戶	輸入要用來驗證連線的使用者帳戶。
自訂資料	輸入可定義此 VPN 自訂資料的索引鍵/值組。
使用者驗證	憑證是使用者的驗證方法。 選擇要在**憑證**欄位中使用的身分憑證。
Proxy 設定	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如果您選擇**自動**，就會出現下列其他欄位： • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。

> 若適用，鍵入 $ 可查看此欄位的支援**變數**清單。

如需更多資訊，請參閱**如何建立配置**

10.10.6.19. Wi-Fi 組態

適用於：

- Android
- Windows
- iOS
- macOS
- watchOS
- visionOS
- tvOS

本節包含以下各主題：

Wi-Fi 設定

- **WEP、WPA/WPA2/WPA3、任何 (人員) 設定**
- **WEP Enterprise、WPA/WPA2/WPA3 Enterprise、任何 (Enterprise) 設定**
- **iOS、macOS 和 visionOS**

Wi-Fi設定

Wi-Fi 配置可設定無線網路的存取權。

> 使用者可修改裝置的部分 Wi-Fi 設定。 不過，MDM 可能會也可能不會收到變更相關資訊，一切取決於裝置的作業系統。 因此，系統不會為了使用伺服器上的配置來取代裝置上的配置而自動將配置重新推送到裝置。

> 此組態可使用具有自訂分發選項的委派。 如需更多資訊，請參閱使用配置中的*分發組態*主題。

> 某些特定版本的 Android 裝置可能需要管理員輸入網域和其他資訊，才能連線到 TLS、TTLS、PEAP 等 (WPA2) 網路。 建議先確認在選取的裝置上對 Wi-Fi 組態進行變更，然後再對更多裝置進行變更。

> 在低於 94 的任何 Ivanti Neurons for MDM 版本上註冊的 Android 14.x 裝置的組態將處於「待安裝」狀態。 當您將 Ivanti Neurons for MDM 升級至 94 而未編輯 Wi-Fi 組態時，組態保持為「待安裝」狀態。 必須啟用 EAP_PEAP 的「網域」欄位並更新組態中的網域和憑證，以將狀態更新為「已安裝」。

程序

1. 前往**配置** > **+新增**。
2. 選擇 **Wi-Fi** 配置。
3. 輸入配置的**名稱**。
4. 輸入描述。
5. 依下列描述進行 Wi-Fi 設定。
6. 按**下一步**。

7. (僅限 macOS) 在「發佈」頁面中，選擇下列其中一個發佈選項：
    - 裝置通道 - 此配置適用於裝置上的所有使用者，也是一般選項。
    - 使用者通道 - 此組態僅適用於裝置上目前註冊的使用者。
8. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂。
9. 按一下**完成**。

下表列出 Wi-Fi 設定：

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
服務組識別元 (SSID) 自動加入 隱藏的網路	輸入要套用這些設定的無線網路名稱。 此欄位有區分大小寫。 選擇裝置是否應自動加入對應的 Wi-Fi 網路。 如果未選擇此選項，裝置使用者就必須點選裝置上的網路名稱才能加入網路。 如果網路存取不是廣播，請選擇此選項。
停用 Captive Network 偵測 (iOS 10+)	管理員可以啟用或停用 Wi-Fi Captive 旁路模式。 當 Apple 偵測到 Captive 入口網站時，它會開啟登入畫面以要求存取權。 您可以停用 Captive 入口網站偵測，並要求使用者手動啟動網頁瀏覽器以觸發 Captive Network 的入口網站登入。此新設定在以下時刻很好用：ISE Captive 入口網站阻擋登入畫面彈出，導致使用者認為他們的未連線裝置其實已連上網際網路。
Proxy 設定 安全性類型	選擇**手動**或**自動**，以設定 Proxy。 如果您選擇**手動**，就會出現下列其他欄位： • **伺服器和連接埠**：輸入 Proxy 伺服器的網址和連接埠號。* • **憑證**：如果必須提供有效使用者名稱才能連接 Proxy 的話，請輸入。* • **密碼**：如果必須提供有效密碼才能連接 Proxy 的話，請輸入。* 如要移除已新增的主機名稱，請按一下「減號」圖示。 如果您選擇**自動**，就會出現下列其他欄位： • **Proxy 伺服器 URL**：輸入 Proxy 的完整 URL。 選擇存取網路所需的安全性方法： • 任何 (人員) • 任何 (企業) • WEP • WEP 企業 • WPA • WPA Enterprise • WPA2 • WPA2 Enterprise • WPA3 • WPA3 Enterprise WPA3/WPA3 Enterprise 適用於 iOS 13+。 Windows 支援 WPA、WPA Enterprise、WPA2 以及 WPA2 Enterprise。

WEP、WPA/WPA2/WPA3、任何 (人員) 設定

設定	方法
密碼	(選用) 輸入存取此網路的密碼。 否則，系統會提示裝置使用者輸入存取網路所需的密碼。

WEP Enterprise、WPA/WPA2/WPA3 Enterprise、任何 (Enterprise) 設定

設定	方法
通訊協定	
接受的 EAP 類型	選擇可用來存取此網路的 EAP 類型： • TLS • TTLS - 在「內部身份」欄位中，選擇一項身份驗證通訊協定，例如 OS Default、PAP、CHAP、MSCHAP、MSCHAPv2 和 EAP。 • PEAP • LEAP (不支援 AMAPI 註冊裝置) • EAP-SIM • EAP-AKA • EAP-FAST (不支援 AMAPI 註冊裝置)
EAP-FAST	選擇用來定義驗證方法的 EAP-FAST 選項： • **使用 PAC**：選擇使用 Proxy 自動配置 (PAC)。 • **設置 PAC**：選擇允許設置 PAC。 否則的話，僅可使用裝置上已設置的 PAC。 只有當您選擇「使用 PAC」時，才可使用此選項。 • **匿名設置 PAC**：選擇允許設置 PAC 而不需驗證伺服器。 只有當您選擇「設置 PAC」時，才可使用此選項。
憑證	
使用者名稱	指定網路存取所需的使用者名稱。 若讓此項留白，系統就會提示裝置使用者輸入。*
使用個別連線的密碼	選擇以提示裝置使用者在每次連線時都要輸入密碼。 當裝置重新加入相同的網路時，系統會提示裝置使用者重新驗證以加入網路。 此選項不支援 AMAPI 註冊裝置。
密碼	(選用) 輸入存取此網路的密碼。 否則，系統會提示裝置使用者輸入存取網路所需的密碼。
身份憑證	(選用) 選擇要作為身分憑證的認證。 身分認證配置定義了所有可用的身分認證。
驗證憑證 (僅適用於 Windows 裝置)	在以下三種憑證存放區中擇一以挑選憑證，然後連線至 Wi-Fi 網路: • 電腦或使用者: 若選取此選項且使用者並未登入，則會從電腦存放區挑選驗證憑證。 若使用者已登入，則會從使用者存放區挑選特定憑證。 • 電腦: 若選取此選項，則會從電腦存放區挑選驗證憑證。 • 使用者: 若選取此選項，則會從使用者存放區挑選驗證憑證。 依預設，會選取「使用者」選項。
外部身份	(選用) 針對 TLS、TTLS、PEAP 及 EAP-FAST，選取以允許裝置使用者隱藏其身分識別。 只有在內部加密的 tunnel 中會顯示使用者的實際名稱。 由於攻擊者無法清楚查看正在驗證的使用者名稱，因此可提高安全性。
網域	當 EAP 類型為 TLS 和 TTLS 時支援。
信任	
受信任的憑證 (不支援 AMAPI 註冊裝置)	從清單中選取核取方塊，以選取多個憑證。

設定	方法
信任的伺服器認證名稱	按一下 **+ 新增**以輸入一或多個受信任的伺服器憑證。 (選填) 選取**允許信任例外狀況**以允許使用者在對話視窗中決定是否信任。

iOS、macOS 和 visionOS

設定	方法
所有版本	
網路類型	選擇此網路是否應視為： • 標準 • 舊版熱點 • Passpoint
允許 Proxy PAC 後援	(選用) 允許裝置在無法取得 PAC 檔時直接連接目的地。
設定模式 (選用)	包含要附加的連線模式類型的一組字串。 • 系統：在使用者登入裝置之前連接 Wi-Fi。 • 登入視窗：在使用者登入裝置之後可使用 Wi-Fi。 目前只有當「系統」和「登入視窗」模式已啟用時才能使用設定模式。
Passpoint 設定	如果您在「網路類型」選擇 Passpoint，便會出現此區段中的設定。
網域名稱	選擇用於 Passpoint 協商的網域名稱。
連接至漫遊合作伙伴 Passpoint 網路	(選用) 選擇允許連線至漫遊服務供應商。
漫遊聯盟組織識別碼	(選用) 輸入由 IEEE 指派給支援此 Wi-Fi 描述檔之實體的識別碼。
網路存取識別碼領域名稱	(選用) 輸入要用於 Passpoint 協商的網路存取識別碼領域名稱。
MCC 和 MNC 配對	(選用) 輸入要用於 Passpoint 協商的行動電話國家/地區碼 (MCC)/行動電話網路碼 (MNC) 配對。 每個字串都必須包含六位數。
顯示業者名稱	(選用) 輸入要顯示的網路業者名稱。
Cisco QoS 快速通道	此區段的設定會套用至 Cisco QoS 快速通道配置。 設定包括適用於 L2 和 L3 的允許清單 app，以及是否要提供內建音訊/視訊服務 (例如：FaceTime 和 Wi-Fi 通話) 的音訊和視訊流量允許清單。
限制 QoS 標記	如果取消選擇，則當網路支援 Cisco QoS 快速通道時，所有 app 將使用 L2 和 L3 標記。 如果選擇，請使用所顯示的**選擇 App** 設定，以新增您想要納入使用 L2 和 L3 標記的 app。 所有未選擇的 app 將不會使用 L2 和 L3 標記。
啟用 QoS 標記	針對已傳送至 Wi-Fi 網路的流量停用 L3 標記，僅使用 L2 標記。 當取消選擇時，系統會視 Wi-Fi 與 Cisco QoS 快速通道網路毫無關聯。
允許清單 Apple 音訊/視訊呼叫	指定是否要提供內建音訊/視訊服務 (例如：FaceTime 和 Wi-Fi 通話) 的音訊和視訊流量允許清單。
選擇 App **iOS 10+**	用來新增您想要納入使用 L2 和 L3 標記的 app。 所有未選擇的 app 將不會使用 L2 和 L3 標記。

設定	方法
Cisco QoS 快速通道	此區段的設定會套用至 Cisco QoS 快速通道配置。 設定包括適用於 L2 和 L3 的允許清單 app，以及是否要提供內建音訊/視訊服務 (例如：FaceTime 和 Wi-Fi 通話) 的音訊和視訊流量允許清單。
限制 QoS 標記	如果取消選擇，則當網路支援 Cisco QoS 快速通道時，所有 app 將使用 L2 和 L3 標記。 如果選擇，請使用所顯示的**選擇 App** 設定，以新增您想要納入使用 L2 和 L3 標記的 app。 所有未選擇的 app 將不會使用 L2 和 L3 標記。
啟用 QoS 標記	針對已傳送至 Wi-Fi 網路的流量停用 L3 標記，僅使用 L2 標記。 當取消選擇時，系統會視 Wi-Fi 與 Cisco QoS 快速通道網路毫無關聯。
允許清單 Apple 音訊/視訊呼叫	指定是否要提供內建音訊/視訊服務 (例如：FaceTime 和 Wi-Fi 通話) 的音訊和視訊流量允許清單。
選擇 App	用來新增您想要納入使用 L2 和 L3 標記的 app。 所有未選擇的 app 將不會使用 L2 和 L3 標記。
iOS 10.3+ 受監管 啟用 Wi-Fi 允許清單 **iOS 14.0+ 及 macOS 15.0+**	判斷裝置允許連接哪些 Wi-Fi 網路。 如果存在多個 Wi-Fi 配置，則套用最嚴格的配置。
停用 MAC 位址隨機化	在 iOS 14.0+ 及 macOS 15.0+ 中，Apple 已變更裝置報告其 Wi-Fi MAC 位址的預設行為，進而會報告新連線的隨機位址，而不是裝置的實際 Wi-Fi MAC 位址。 因此，對於使用 Captive 入口網站和篩選 MAC 位址的企業，這項功能可能會導致非預期的行為。 管理員可以編輯相關聯的 Wi-Fi 配置並開啟此選項 (預設為 false)，針對 Wi-Fi 網路**停用 MAC 位址隨機化**。 這將導致 Wi-Fi 配置重新推送到所有裝置。 此選項會在裝置設定中顯示隱私權警告，指出該網路的隱私保護已降低。 裝置使用者仍然可以透過其裝置設定，手動開啟或關閉此功能。
Android 11+	
MAC 位址隨機化	• 已停用: 在使用者登入裝置之前便已連線 Wi-Fi。 • 已啟用 - 自動: 在使用者登入裝置之後便可使用 Wi-Fi。 • 已啟用 - 非持續 • 已啟用 - 持續

> 若適用，鍵入 $ 可查看此欄位的支援**變數**清單。

如需更多資訊，請參閱**如何建立配置**。

10.10.7. 行動網路配置

本節包含以下各主題：

- APN 配置
- 行動數據
- Cellular Private Network Configuration.htm行動數據私人網路組態
- iOS 電信商預設配置
- eSIM 配置

10.10.7.1. APN 配置

APN 組態為裝置設定行動數據存取點名稱。 若是 iOS 7，請改用行動電話配置。

APN 設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
存取點名稱	輸入相應存取點的名稱。 此名稱通常是由服務業者定義。
存取點使用者名稱	輸入為此存取點授權的使用者名稱。*
存取點密碼	輸入與已輸入之使用者名稱的相應密碼。
Proxy 伺服器和連接埠	輸入 APN Proxy 的 IP 位址或 URL 與連接埠號。
EnableXLAT464	選取核取方塊以啟用存取點名稱 (APN)。 此選項可透過僅限 IPv6 網路提供 IPv4 服務。

若適用，鍵入 $ 可查看此欄位的支援變數清單。

如需更多資訊，請參閱如何建立配置。

10.10.7.2. 行動數據

適用於: iOS 7.0+ 和 watchOS 10.0+

本節包含以下各主題：

- 預設 APN 的行動數據設定
- 數據 APN 的行動數據設定
- 控制漫遊時的行動網路存取
- 控制行動網路存取

行動電話通訊組態為裝置設定行動電話通訊設定檔。 在執行 iOS 7.0+ 或 watchOS 10.0+ 的裝置上設定蜂窩網路設定。 有些企業會與行動電話業者簽約並取得唯一存取點名稱 (APN) 的存取權，以進行遠端網路存取或享受特殊計費方案。 請洽詢行動電話業者以取得配置參數。

- 一次只能安裝一個行動電話描述檔。
- 如果已安裝 **APN 描述檔**，就無法安裝行動電話描述檔。

您可針對**已設定的 APN 類型**下拉式方塊的下列 APN 類型，設定行動數據設定：

- 預設與數據 APN
- 預設 APN
- 數據 APN

針對所有配置，輸入可識別配置的名稱，並選擇性輸入描述。

預設 APN 的行動數據設定

預設 APN 設定	方法
APN 名稱	輸入相應存取點的名稱。 此名稱通常是由服務業者定義。
APN 身份憑證類型	(選擇性) 請選擇下列選項之一： • CHAP (Challenge Handshake 驗證通訊協定) • PAP (密碼驗證通訊協定)
使用者名稱	(選用) 輸入要用於驗證的使用者名稱。
密碼	(選用) 輸入要用於驗證的密碼。

數據 APN 的行動數據設定

數據 APN 設定	方法
APN 名稱	輸入相應存取點的名稱。 此名稱通常是由服務業者定義。
APN 身份憑證類型	(選擇性) 請選擇下列選項之一： • CHAP (Challenge Handshake 驗證通訊協定) • PAP (密碼驗證通訊協定)
使用者名稱	(選用) 輸入要用於驗證的使用者名稱。
密碼	(選用) 輸入要用於驗證的密碼。
Proxy 伺服器	指定 Proxy 伺服器。
Proxy 伺服器連接埠	指定 Proxy 伺服器連接埠。
10.3+	
允許的通訊協定遮罩	選擇 IPv4、IPv6 或兩者。
國內漫遊時允許的通訊協定遮罩	選擇 IPv4、IPv6 或兩者。
漫遊時允許的通訊協定遮罩	選擇 IPv4、IPv6 或兩者。

控制漫遊時的行動網路存取

當裝置在漫遊狀態時，您可以限制部分或所有受管理 app 的行動數據存取權。

程序

1. 前往 Ivanti Neurons for MDM 導覽主功能表的**組態**索引標籤。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入**網路**，然後按一下**網路使用情況**組態。
4. 選擇**針對所有受管理的 app 禁用**勾選框，以防止受管理的 app 在漫遊時或任何時刻存取行動數據。
5. 未選擇勾選框時，您可以依名稱或套件 ID 來指定受管理的 App 以防止它們接收行動數據。
6. 您可以使用「App」欄位中的下拉式功能表，依名稱或套件 ID 來搜尋 App。

控制行動網路存取

您可以限制部分或所有受管理 app 在漫遊時或任何時刻的行動數據存取權。 這些 app 仍可在受限的情況下使用，只是不能存取行動數據而已。

程序

1. 前往 Ivanti Neurons for MDM 導覽主功能表的**組態**索引標籤。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入**網路**，然後按一下**網路使用情況**組態。
4. 選擇**針對所有受管理的 app 禁用**勾選框，以防止受管理的 app 在任何時刻存取行動數據。
5. 您也可以不選擇勾選框，而指定受管理的 app 以防止它們接收行動數據。
6. 您可以使用「App」欄位中的下拉式功能表，依名稱或套件 ID 來搜尋 App。

如需更多資訊，請參閱**如何建立配置**。

10.10.7.3. 行動數據私人網路組態

Ivanti Neurons for MDM 讓行動數據私人網路組態承載能夠提供私人網路部署上的裝置資訊，包括地理位置、Wi-Fi 偏好設定和網路部署類型。

適用於

iOS 17.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取**行動數據私人網路**組態。
3. 依下表配置**行動數據私人網路**設定:

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
慣用行動數據	選取核取方塊以啟用和使用行動數據 (優先於 Wi-Fi)。
NR 獨立	如果行動數據網路具有獨立 NR 5G，請選取核取方塊。
資料集名稱	指定識別此組態的資料集名稱。
版本編號	指定資料集的版本編號以追蹤系統更新。
地理圍欄	指定每個地理 ID 的緯度、經度和半徑，以在某個地理位置部署私人網路。 您可以為私人網路建立包含最多一千個地理圍欄的清單。

4. 按**下一步**，確認發佈設定。
5. 選取其中一個發佈選項以設定**行動數據私人網路**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
6. 按一下**完成**。

10.10.7.4. iOS 電信商預設配置

iOS 電信商預設配置可設定漫遊限制和熱點限制的預設值。

iOS 電信商預設設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
可讓裝置在漫遊時使用語音服務	選擇啟用語音漫遊。 語音漫遊的可用性取決於業者而定。
可讓裝置在漫遊時使用數據服務	選擇啟用數據漫遊。 啟用裝置的數據漫遊時也會啟用語音漫遊。
可讓使用者啟用個人熱點	選擇啟用個人熱點功能。 此功能的可用性取決於業者而定。

如需更多資訊，請參閱**如何建立配置**。

10.10.7.5. 增強型 5G 網路切片組態

Ivanti Neurons for MDM 提供了增強型 5G 網路切片組態，用於為 Android 設定 5G 網路切片，這使得行動網路營運商可以配置專用的 5G 網路區段或「切片」，以便將具有類似需求 (例如低延遲或高頻寬) 的不同應用程式劃分到特定切片中，從而更好地最佳化網路資源。 這使得 MDM 管理員與網路提供者能夠直接管理切片，以獲得更好的應用程式效能。

關鍵功能

1. **專用網路**: 網路切片不是讓所有應用程式共用單一網路切片，而是讓不同的應用程式能夠根據其具體需求使用自己的網路切片

2. **自訂**: 管理員可以根據個人需求設定如何將應用程式指派給特定的網路切片 - 例如，在指派時確保即時通訊應用程式的低延遲，或在指派時確保 YouTube 等串流服務的高頻寬。 用於高效能遊戲的切片可能會優先考慮低延遲，而用於媒體串流的切片將針對高頻寬進行最佳化。

3. **合作夥伴參與**: 此功能通常需要與定義這些切片的網路提供者合作，並向 MDM 管理員告知切片清單及其重要性。

建立增強型 5G 網路切片組態

程序

1. **新增配置**

- 導覽至**組態 >> +新增**。 隨即顯示**新增組態**頁面。
- 在搜尋列中輸入**增強型網路切片**以設定增強型網路切片。 **建立增強型網路切片組態**頁面會顯示出來。
- 按一下 **+新增說明**以輸入組態的說明。

2. **設定應用程式**

- 在**組態設定 >> 應用程式目錄**下，輸入所需的應用程式名稱。
- 如果應用程式在 Play 商店或 App Store 中不可用，請按一下**手動新增**。
- 輸入**套件 ID**，然後從下拉式功能表中選取適當的**網路切片**。
- 從**選取切片**下拉式清單中選取所需的切片。
- 按一下**新增**。 應用程式現在將顯示在選定的網路切片下的**設定網路切片**中。
- 若要移除應用程式，請按一下**設定網路切片**區段下的**移除**。

3. **分發組態**

- 按一下**下一個**，選取或取消選取「**啟用此組態**」核取方塊，選擇分發選項 (所有裝置、無裝置，或自訂)，
- 按一下**完成**以完成組態。

增強型網路切片組態，適用於鎖定和 Kiosk

建立增強型 5G 網路切片組態可讓您將裝置設定為以受限方式執行，確保使用者只能存取指定的應用程式與設定。

在以下鎖定下方，有「**啟用 5G 網路切片**」核取方塊:

- **工作設定檔** - 在使用 Android Enterprise 12.0 版設定工作設定檔的員工自有裝置上，「啟用 5G 網路切片」核取方塊位於**組態設定 > 工作設定檔鎖定設定**下。
- **具有工作設定檔的受管理裝置/公司擁有的裝置上的工作設定檔** - 在「具有工作設定檔的受管理裝置/公司自有的 Android 12.0 版本裝置上的工作設定檔」下，有一個「啟用 5G 網路切片」核取方塊。

這是允許裝置使用 5G 網路切片的舊版設定。 它與新的增強型 5G 網路切片組態的關聯如下:

如果對裝置套用了上述任何鎖定，並且**未**選取*啟用 5G 網路切片*選項，則*增強型 5G 網路切片*組態將會失敗並出現錯誤。

範例

- **案例 1**: 如果未分發裝置鎖定，但分發了增強型網路切片組態，則增強型組態將啟動。
- **案例 2**: 如果分發了裝置鎖定，但未選取 5G 核取方塊 (false)，則增強型 5G 網路組態將會出錯。
- **案例 3**: 如果先分發增強型網路切片，然後在啟用核取方塊的情況下分發裝置鎖定，則增強型網路切片組態將繼續工作。 否則，它會出錯。

組態詳細資訊:

- 如果分發了裝置鎖定並推送/分發了增強型網路切片組態，則使用者必須確保啟用了「啟用 5G 網路切片」核取方塊以防止錯誤。
- 如果未啟用該核取方塊並傳送了組態，則它將在裝置上出錯。

10.10.7.6. eSIM 配置

eSIM 配置可透過 RefreshCellularPlans 命令在裝置上設定行動網路。 在將行動網路對應至裝置之前，管理員必須先取得 eSIM 電信業者 URL。

適用於: Android 15+、iOS、iPadOS 和 Windows 11

Android 15+ 裝置的程序

1. 前往**組態** > **+新增**。
2. 在搜尋欄位中輸入 eSIM，然後按一下 **eSIM** 配置。
3. 輸入配置的名稱和描述。
4. 從**平台**清單中，選取 **Android**。
5. 在**組態設定**區段下，輸入**航空公司 URL**。
6. **自動啟用** - 選取此選項下載 eSIM 設定檔並在裝置自動啟用。 如果未選取此選項，將下載 eSIM 設定檔，但不會自動在裝置上啟用。

> 此選項不適用於工作設定檔模式中的裝置。

7. 使用下列其中一個分發選項選取並分發組態:
   - 所有裝置
   - 沒有裝置 (預設)
   - 自訂
8. 按一下**完成**。

Android 13+ 裝置的 EID

要求 EID 選項現已在裝置詳細資訊和裝置清單頁面中可用。 此選項僅支援工作設定檔上與 eSIM 相容裝置、工作受管理裝置和公司擁有裝置模式下的工作設定檔。 如果裝置已註冊，將自動選取已註冊裝置 EID，並顯示在裝置詳細資料頁面下方。 如果不是，此欄位將啟用，您可以按一下**要求 EID** 來要求 EID。 您也可以使用裝置清單頁面中的**匯出為 CSV** 選項來匯出 EID。

> 在**裝置詳細資料**頁面中，**要求 EID** 選項適用於搭載 Ivanti Go R122 或更新版本的 Android 13+ 裝置。

保留 eSIM 資料計畫 (適用於 iOS 11+ Android 15.0+): 當您嘗試抹除使用 eSIM 組態註冊的裝置時，**抹除裝置**動作會提供其他選項以保留資料計畫。 如果您選取**保留 eSIM 資料計畫 (適用於 iOS 11+ 和 Android 15.0+)**，然後按一下**抹除**，現有 eSIM 資料計畫會保留，同時清除裝置所有其他資料。 您可以從**裝置詳細資料**頁面存取此選項，也可以選取裝置，開啟**動作**功能表，然後按一下**抹除**。

針對 iOS 與 iPadOS 裝置的程序

1. 前往**組態** > **+新增**。
2. 在搜尋欄位中輸入 eSIM，然後按一下 eSIM 配置。
3. 輸入配置的名稱和描述。
4. 選取 **iOS/iPadOS**。
5. 輸入電信業者 URL。
6. 按**下一步**。
7. 選擇啟用此配置選項。

8. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂
9. 按一下完成。

針對 Windows 11 裝置的程序

1. 前往**組態** > **+新增**。
2. 在搜尋欄位中輸入 eSIM，然後按一下 eSIM 配置。
3. 輸入配置的名稱和描述。
4. 在「選擇作業系統」區段中，按一下 **Windows**。
5. 在「組態設定」區段中，在「伺服器名稱」文字框中鍵入電信業者 URL (FQDN 格式)。
    - 是 Discovery 伺服器 - 選取此選項以將伺服器標記為可發現。
    - 自動啟用 - 選取此選項以在下載後於裝置上啟用設定檔。
6. 按**下一步**。
7. 選擇啟用此配置選項。
8. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂
9. 按一下**完成**。

將 eSIM 重設為出廠狀態 (僅適用於 Windows 11 裝置)

此選項在所有裝置的「裝置詳細資料」區段下可用。 按一下此選項將刪除裝置上下載的所有 eSIM 設定檔。

重要說明 - 僅適用於 Windows eSIM 組態

- 註冊裝置後，**裝置詳細資訊**區段現在會在**支援 ESIM** 下顯示裝置是否支援 eSIM。 對於支援 eSIM 的裝置，相應的 eSIM 識別碼詳細資訊也會顯示在 **ESIM 識別碼**下方。
- 當 Ivanti Neurons for MDM 已註冊裝置被抹除並重新註冊時，應從裝置頁面刪除此裝置的舊記錄 (狀態為「已抹除」)，以避免在此重新註冊的裝置上出現 eSIM 組態問題。
- 將相同的組態重新推送到已經下載設定檔的裝置，將無法再次下載設定檔。 如果管理員希望裝置重新下載設定檔，建議先將 eSIM 模組重設為出廠狀態，然後推送/重新推送 eSIM 組態。
- 當裝置上成功佈建 eSIM 組態時；在淘汰裝置之前，管理員應執行 eSIM 抹除動作，以確保從裝置中抹除下載的 eSIM 設定檔。
- 若移除 eSIM 組態，則只會從裝置中刪除該組態。 如果在裝置上發現、下載並啟動了任何 eSIM 設定檔，則這些 eSIM 組態將保持活動狀態，直到執行 eSIM 擦除。
- 若執行 eSIM 抹除動作，則將從裝置中移除所有已下載的 eSIM 設定檔。 但是，處於已安裝狀態的 eSIM 組態在裝置上保持不變。 管理員需要取消發佈 eSIM 組態，以便從裝置中刪除此組態。

10.10.8. 其他配置

本節包含以下各主題：

- 相關聯網域組態
- Android 檔案傳輸組態
- Apple TV 配置
- AirPlay 配置
- AirPlay 鏡像
- 瀏覽器設定
- 設定 iOS 的單一 App 模式
- 設定 iOS MDM 描述檔
- 設定 macOS MDM 設定檔
- 內容快取
- 建立 Android 捷徑
- 裝置名稱設定
- 乙太網路組態 (macOS)
- EMA 伺服器整合配置
- 裝置桌布配置
- 鎖定畫面訊息配置
- 建立螢幕保護程式組態
- 設定使用者的螢幕保護程式
- macOS 系統延伸配置
- 僅限 MAM
- 受管理的 Google Play 配置
- 移轉助手設定
- 通知組態
- 列印設定
- 移除膨脹配置
- Samsung 手機限制配置
- 單一 App 模式配置
- 開始功能表和工作列
- 系統更新組態
- Windows Update 管理
- Windows app 排程
- Windows BIOS 配置
- Windows BitLocker
- Windows 單一應用配置

- Windows 授權配置
- 軟體更新建議頻率配置

10.10.8.1. 相關聯網域組態

授權： Gold

相關聯網域組態是將應用程式對應到其相關聯網域的字典。 相關聯網域可與可延伸 AppSSO、通用連結及密碼自動填寫等功能搭配使用。

相關聯網域設定如下:

設定	方法
名稱	輸入可識別此配置的名稱。
應用程式識別碼	(必要) 與網域相關聯的應用程式識別碼。
關聯的網域	(必要) 與應用程式相關聯的網域。 每個字串的形式必須為 "service:domain"。 網域應為完整的合格主機名稱，如 www.example.com。
啟用直接下載	若為 true，應該會直接下載此網域的資料，而非透過 CDN 下載。 此網域的權益值必須設為 service:domain?mode=managed，或則會忽略此值。 適用於 macOS 11 及以上版本。 **預設**: False

10.10.8.2. Android 檔案傳輸組態

在 Android 11 中，Google 對裝置上應用程式的儲存存取進行了重大變更，同時影響了企業將檔案傳送到這些裝置上特定應用程式的方式。 考慮到這些變化，隨著裝置升級到 Android 11 及更高版本，許多大型企業在將檔案發佈到裝置和應用程式時面臨著挑戰。 任何依賴硬體供應商專屬 API 的方法，都會迫使企業在不同製造商和作業系統版本的不同裝置上，採用相同的方法。

Ivanti 開發了一套與 Android 版本和硬體供應商無關的檔案傳輸解決方案。 此解決方案依賴於 Android 的標準 *Content-Provider* 功能。 *Content-Provider* 允許 Ivanti Go 應用程式為透過 UEM 推送的每個檔案，產生唯一的裝置上位置。

檔案傳輸組態適用於完全受控裝置模式中的 Android 裝置。 使用此組態，管理員可以提供一個選項來傳輸裝置上的檔案，以便在同一裝置上存在的各個獲允許應用程式之間共用。 其他應用程式可以出於任何需要的原因使用這些檔案。 使用案例的範例包括使用 JavaScript 初始化應用程式組態，或使用 PDF 或影片顯示公司資訊。 上傳到 Ivanti 檔案傳輸組態中的每個檔案都會在 Ivanti Go 收到相應的組態和相關檔案時進行下載。 該檔案安全地儲存在 Ivanti Go 中。

其他應用程式無法任意存取此檔案。

應用程式沙箱中的每個下載檔都有唯一的參照位置，又稱為 *ContentURI* 或 *URI*。 自訂屬性用於在伺服器上儲存裝置上每個檔案的 ContentURI 值，可以協助管理員確定檔案在裝置上的可用性、形成動態裝置群組，以及按照要求使用受控應用程式組態將 ContentURI 傳達至目標應用程式等。

> 對於非 Ivanti 應用程式，管理員應諮詢第三方應用程式開發人員，瞭解他們為此方法提供的支援，這種方法通常稱為「使用以 FileProvider 為基礎的 ContentURI」。

先決條件:

- 新增以裝置為基礎的新自訂屬性，用於檔案傳輸操作。 對於每個檔案傳輸組態，應分別建立唯一的自訂屬性。 每個自訂裝置屬性只能為每個組態的一個檔案儲存來自裝置的 contentURI (檔案位置)。

程序

1. 前往**組態** > **新增組態** > **檔案傳輸**。 此時將開啟**建立檔案傳輸組態**頁面。
2. 在**名稱**方格中輸入組態的名稱。
3. 輸入組態的**說明**。
4. **配置設置**
   在**要傳輸的檔案**區段中，使用拖放選項或瀏覽**選擇檔案**選項，選取要傳輸的檔案。 預設情況下，檔案大小的上限為 50 MB。
5. 選取以下一個或多個**下載到裝置**選項 (選用):
   - **允許透過按流量計費的網路下載** - 選取後即使使用按流量計費的網路，仍繼續下載檔案
   - **需要充電** - 選取此項可確保裝置在檔案傳輸過程中充電
   - **需要裝置閒置** - 選取此項可確保裝置在檔案傳輸過程中閒置
6. 使用以下兩個選項之一與其他應用程式共用檔案
   - **使用 Android 受控應用程式組態進行傳輸** - 僅於目標應用程式能使用其受控應用程式組態使用內容 URI 時，才使用此選項。
   - **使用裝置上意圖的傳輸** - 意圖是應用程式專屬功能。 若要使用此選項共用檔案，請參閱目標應用程式說明文件並於下方的意圖區段中提供相關資訊。 意圖可讓 Ivanti Go 應用程式在檔案可供應用程式共用後，在裝置上廣播訊息。

使用 Android 受控應用程式組態來傳輸

程序

1. 在**選擇以裝置為基礎的現有自訂屬性，與其他應用程式共用此檔案**欄位中，輸入現有屬性名稱，例如 **Custom-Filename**。 如需詳細資訊，請參閱[指派自訂屬性給裝置]。
2. 自訂屬性名稱應該是僅用於此檔案傳輸操作的唯一新屬性。 每個自訂裝置屬性只能為每個組態的一個檔案儲存來自裝置的 contentURI (檔案位置)。
   提供下列應用程式和/或套件名稱的存取權: 您可以從應用程式名稱選取器選取應用程式名稱，並新增套件名稱。

> 這些將是唯一允許存取該檔案的獲授權套件。

   - **應用程式名稱** - 您可從應用程式名稱選取器選取應用程式名稱。
   - **套件名稱** - 您可以在此區域輸入套組 ID，例如用分號 (;) 分隔多個套件名稱。

```
Bash
com.mobileiron.filetransfer.android3。
```

按一下**儲存**。 新的檔案傳輸組態將顯示在「組態」頁面上。

配置目標應用程式

程序

1. 前往**應用程式 > 應用程式目錄**。
2. 選取要接收檔案的目標應用程式。
3. 瀏覽到**應用程式組態 > 適用於 Android 的受控組態**。
4. 建立新組態或使用現有組態。
5. 應用程式可能具有「清單資訊」等設定或其他屬性，管理員可以在其中定義替換變數，並將檔案的位置傳達給目標應用程式。 以 Ivanti Velocity 應用程式為例，在應用程式組態對話方塊中 > **提取組態 > 清單資訊**欄位中，輸入替換變數。 例如 $Custom-File-Name$。
   選取您的發佈。
6. 按一下**儲存**。

使用裝置上意圖進行傳輸

程序

1. 在**選擇現有的裝置屬性，以在意圖額外項中傳遞檔案路徑**欄位中，輸入新的自訂屬性名稱，例如 deviceIntentURI。
2. 自訂屬性用於保存伺服器上每個裝置的位置 (URI / ContentURI) 值，可協助管理員確定檔案在裝置上的可用性。 如需詳細資訊，請參閱[指派自訂屬性給裝置]。
   在**提供特定應用程式或套件名稱的存取權**欄位中，輸入應用程式名稱或**套件名稱**，例如 Velocity。

> 這些將是唯一允許存取該檔案的獲授權套件。

3. 在 Intents-Standard 區段中，提供以下詳細資訊:
   - **操作類型** - 從下拉清單中，根據應用程式選取**啟動活動** / **啟動服務** 或其他類似選項。 根據目標應用程式開發人員指南或參考目標應用程式說明文件，為此欄位選擇正確的值。
   - **類別名稱** (選用) - 根據目標應用開發人員指南或參考目標應用程式說明文件，為此欄位選擇正確的值。

- **操作** - 根據應用程式將操作設定為:或類似的值。

```
Bash

com.wavelink.nameofapp.action.INSTALL_CONFIG
```

- **類別** - 輸入用分號 (;) 分隔的值。
- **MIME 類型** (選用) - 在管理員的主機伺服器中，應使用 MIME 類型的應用程式/組態設定 custom.mobileconfig 檔案，以便下載裝置的 MDM 設定檔並將其安裝在裝置上。 根據目標應用程式開發人員指南或參考目標應用程式說明文件，為此欄位選擇正確的值。
- **旗標** (選用) - 選取要使用的旗標數。 根據目標應用程式開發人員指南，為此欄位選擇正確的值。

在機碼、類型和值下方提供 **Intents-Extras** (選用)。 如需更具體的參數，請參閱 OEM 應用程式說明文件。 根據目標應用程式開發人員指南或參考目標應用程式說明文件，為此欄位選擇正確的值。

5. 按一下**儲存**。
6. 在「組態」頁面中，選取新的「檔案傳輸組態」，然後選取**動作** > **套用至標籤**。 將開啟**套用至標籤**對話方塊。
7. 選取合適的標籤，然後按一下**套用**。
   與其他應用程式傳輸/共用檔案，只能透過從目標應用程式或裝置收集記錄進行驗證。

驗證檔案下載狀態

自訂屬性用於保存伺服器上每部裝置之每個檔案的位置 (ContentURI) 值，可協助管理員確定檔案在裝置上的可用性。

程序

1. 前往**裝置** > **裝置**。
2. 選取要部署檔案傳輸組態的特定裝置。
3. 在「裝置詳細資訊」頁面中，選取裝置，然後選取**動作** > **裝置強制簽入**。
4. 在「組態」索引標籤下，確認「檔案傳輸」組態是否顯示為**已套用**狀態。
5. 在「自訂屬性」索引標籤下，確認新自訂屬性的名稱是否與其相關值一起顯示 (例如 Custom-File-Name$)。 這裡提供有關檔案在裝置上儲存位置的資訊，並顯示該檔案已於本機下載到 Ivanti Go 應用程式沙箱內可用的裝置。
   與其他應用程式傳輸/共用檔案，只能透過從目標應用程式或裝置收集記錄進行驗證。

10.10.8.3. Apple TV 配置

授權： Silver

Apple TV 配置可用來定義 Apple TV 的語言和地區設定。

Apple TV 設定如下：

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
語言	輸入兩個字元的語言代碼，以指定 UI 語言。
地區設定	輸入地區設定 ID 以指定 UI 的國家/地區/語言組合。

如需更多資訊，請參閱**如何建立配置**。

10.10.8.4. AirPlay 鏡像

授權：Gold

AirPlay Mirroring 功能可讓您利用 Apple TV，在顯示器上顯示 iOS 裝置的畫面。 Apple TV 和 iOS 裝置必須連接相同 Wi-Fi 網路。 此功能需要以下裝置：

- iOS 7 和以上版本的裝置 - 受監管
- macOS 10.10 和以上版本的裝置 - 受監管
- Apple TV 版本 - 受監管
- AirPlay

> 切換為納入管理非 iOS 裝置是無法取消的。

本節包含以下各主題：

- 配置 Apple AirPlay
- 在行動裝置上設定 AirPlay
- 設定顯示器以搭配使用 Apple TV
- 連接 iOS 裝置與 Apple TV

配置 Apple AirPlay

如需 AirPlay 配置設定的詳細資訊，請參閱 AirPlay 配置。

程序

1. 前往**配置**。
2. 按一下 **+新增**。
3. 按一下 **AirPlay**。
4. 在適當欄位中，輸入配置的名稱和描述。
5. 對於所有受支援的 iOS 版本，請輸入裝置名稱和密碼。
6. 按一下 **+新增**，即可視需要新增其他配置。
7. 或者，對於受監督的 iOS 7+ 裝置或 macOS 10.10+，請將裝置 ID 新增至允許清單。
8. 按**下一步**。
9. 選擇發佈層級。
10. 按一下**完成**。

在行動裝置上設定 AirPlay

程序

1. 設定 Apple Configurator。
2. 前往**裝置 > 裝置**。
3. 按一下 iOS 裝置的名稱，以顯示該裝置的「詳細資料」頁面。

4. 按一下 ⋮ 圖示。
5. 選取 **AirPlay Mirroring** 以顯示 AirPlay Mirroring 對話方塊。
6. 從下拉式功能表中選擇 Apple TV。
7. 輸入掃描時間 (秒) 以指定搜尋所選擇裝置的時間限制。
8. 輸入 Apple TV 裝置的密碼。
9. 按一下**傳送要求**。

設定顯示器以搭配使用 Apple TV

程序

1. 在連接 Apple TV 的顯示器上，前往**設定 > 描述檔**。
2. 選取 **Ivanti Neurons for MDM Apple Configurator**。
3. 按一下 **新增描述檔**。
4. 按一下 ⋮ 圖示。
5. 選取 **AirPlay Mirroring** 以顯示 AirPlay Mirroring 對話方塊。
6. 從下拉式功能表中選擇 Apple TV。
7. 輸入掃描時間 (秒) 以指定搜尋所選擇裝置的時間限制。
8. 輸入 Apple TV 裝置的密碼。
9. 按一下**傳送要求**。

連接 iOS 裝置與 Apple TV

程序

1. 連接 Apple TV 裝置與顯示器。
2. 使用 Apple TV 遙控器，前往**設定 > 帳號 > 家庭共享**，以開啟「家庭共享」。
3. **將 iOS 裝置連線**至 **Apple TV 裝置**所使用的 Wi-Fi 網路。
4. 開啟 **iOS** 裝置上的「遙控器」app。
5. 啟用**家庭共享** (透過**遙控器設定**畫面)。

10.10.8.5. 瀏覽器設定

如果使用「瀏覽器設定」，您可在 Windows 10 裝置上設定 Google Chrome、Mozilla Firefox、Microsoft Edge 及 Internet Explorer 的設定與限制。

此功能需要 Bridge。 請參閱 **Ivanti Bridge** 以取得詳細資料。

> 套用瀏覽器設定之前，請確認裝置上已安裝該瀏覽器。

若要設置瀏覽器設定：

1. 前往**配置 > +新增**。
2. 選擇**瀏覽器設定**配置。
3. 輸入配置的名稱。
4. 輸入描述。
5. 在「配置設定」區段中，按照下表所述指定其餘設定。

設定	方法
瀏覽器	選擇設定所需的瀏覽器類型： • **Chrome** • **Firefox** • **Microsoft Edge** • **Internet Explorer**
瀏覽器設定	設定下列選項： **允許瀏覽器**： • 允許儲存密碼 • 允許安全瀏覽模式 • 允許過期的外掛程式停留在瀏覽器上 **Chrome 和 Firefox**： • **允許刪除瀏覽器歷程記錄** **Chrome 和 Internet Explorer**： • **允許瀏覽器列印** • **新建索引標籤頁面 URL** **僅限 Chrome**： • **在書籤列中顯示 app 捷徑** • **顯示主畫面按鈕** • **允許與 Google 進行資料同步** • **在 Chrome 關閉後繼續執行背景 app** **僅限 Firefox**： • **允許安裝擴充功能** **僅限 Internet Explorer**： • **允許從網站下載資料**
瀏覽器最愛項目	按一下 **+新增**。 **新增瀏覽器最愛項目**視窗隨即顯示。 設定下列欄位： • **顯示名稱**：嘗試顯示最愛項目的名稱 • **URL**：輸入瀏覽器最愛項目的 URL。 按一下**新增**。 所新增的瀏覽器最愛項目其詳細資料隨即顯示在頁面中。 在**動作**欄位中，按一下「編輯」圖示以編輯設定。 若要刪除瀏覽器最愛項目，請按一下「刪除」圖示。 **瀏覽器最愛項目資料夾名稱**：輸入瀏覽器最愛項目資料夾的名稱，最愛項目應列在此資料夾中。 您還可以用 CSV 格式新增瀏覽器最愛項目。 若要以 CSV 格式上傳： 1. 按一下「上傳 CSV 檔案」。 瀏覽與選擇要上傳的 CSV 檔案。 2. 按一下**上傳**。 CSV 檔案中的詳細資料應使用下列格式新增： • 第一欄 (顯示名稱) 應指定最愛項目的名稱。 範例：「購物」。 • 第二欄 (URL) 應指定最愛項目的 URL。 範例：「https://amazon.com」。

設定	方法
網站安全性	設置下列網站安全性設定： **所有網站 (Chrome 和 Firefox)** • **封鎖 Cookie** • **封鎖 Javascript** • **封鎖外掛程式** • **封鎖快顯視窗** 特定網站 (僅限 Chrome) **列入封鎖清單的網站 (Chrome 和 Edge)**: 新增您想要列入封鎖清單的網站。 按一下 **+新增**。 **新增列入封鎖清單的網站**視窗隨即顯示。 在**網站 URL** 中，輸入應列入封鎖清單之網站的 URL。 在**存取**欄位中，選擇**封鎖**以將網站列入封鎖清單。 預設選項為**允許**。 按一下**新增**。
瀏覽器擴充功能	**允許的擴充功能類型 (僅限 Chrome)**: 選取下列其中一個選項: • **擴充功能** • **使用者指令碼** • **佈景主題** • **封裝式 App** • **託管式 App** • **平台 App** **瀏覽器擴充功能原始碼 (僅限 Chrome)**: 按一下 **+新增**以新增瀏覽器擴充功能原始碼。 新增瀏覽器擴充功能原始碼之後，您可以按一下**動作**欄位中的相關選項，以編輯或刪除原始碼。 **強制安裝擴充功能 (僅限 Chrome)**: 按一下 **+新增**以新增強制安裝擴充功能。 新增強制安裝擴充功能之後，您可以按一下**動作**欄位中的相關選項，以編輯或刪除原始碼。

6. 按**下一步**。
7. 請選擇下列發佈選項之一：
   - 所有裝置
   - 沒有裝置 (預設)
   - 自訂
8. 按一下**完成**。

10.10.8.6. 設定 iOS 的單一 App 模式

授權：Silver

單一 app 模式可限制 iOS 和 tvOS 裝置使用指定的 app。 例如，您可以限制裝置只能貴組織開發的自訂 app。

程序

1. 前往**配置 > 新增 > 單一 App 模式**。
2. 使用下列準則來定義 app 及相關設定。
3. 按**下一步**。

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
選擇 App	選擇用來選擇 app 的方法： • **從應用程式目錄與系統應用程式：**選擇以搜尋 Ivanti Neurons for MDM 應用程式目錄與系統應用程式 (依預設預先安裝在 Apple 裝置上)。 • 輸入 app 的名稱，並在其顯示於 app 清單時選擇它。 • **輸入組合 ID:** 選擇此項以針對要選擇的系統應用程式輸入唯一識別碼。 如果您使用**從 App Catalog 與系統 App** 選項時找不到系統 app，請使用此選項。
停用觸控	選擇停用觸控畫面。
停用裝置的螢幕旋轉	選擇停用裝置的旋轉感應。
停用音量按鈕	選擇停用裝置的音量按鈕。
停用鈴聲轉換	選擇停用裝置的鈴聲轉換。
停用睡眠/喚醒按鈕	選擇停用裝置的睡眠/喚醒按鈕 (裝置邊緣右上角)。
停用自動鎖定螢幕	選擇不讓裝置在閒置期間後進入睡眠狀態。
啟用語音輔助	選擇啟用 VoiceOver 螢幕閱讀器 (輔助功能)。
啟用縮放	選擇啟用縮放 (輔助功能)。
啟用反轉顏色	選擇啟用反轉顏色調整 (輔助功能)。
啟用觸控助理	選擇啟用 AssistiveTouch (輔助功能)。
啟用朗讀選項	選擇啟用朗讀選項 (輔助功能)。
啟用單耳機功能	選擇從立體聲切換至單耳機功能 (輔助功能)。
語音輔助調整	選擇允許裝置使用者調整 VoiceOver。
縮放調整	選擇允許裝置使用者調整縮放。
反轉顏色調整	選擇允許裝置使用者反轉顏色。
觸控助理調整	選擇允許裝置使用者調整 AssistiveTouch。

4. 在**發佈**畫面中，選擇要接收此項配置的裝置群組。
5. 按一下**完成**。

如果您已將電話撥號程式設為要使用的應用程式，Home 鍵會在裝置進入單一應用程式模式後啟用。

10.10.8.7. 設定 iOS MDM 描述檔

iOS MDM 組態定義對 Ivanti Neurons for MDM 的存取限制。 iOS MDM 配置有兩種：

- **iOS MDM - 大量設置：**適用於由企業採購並做為大量發佈之部分設置的裝置。
- **iOS MDM - 個別設置：**適用於一對一設置的裝置。 將不會套用至受監管裝置和使用者註冊的裝置。

在所有的空間中只提供並允許其中一種配置。

編輯 iOS MDM 配置

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 前往**配置**。
3. 選擇要編輯的 iOS MDM 配置。
4. 按一下鉛筆 (編輯) 圖示，編輯組態。
5. 使用下列準則來進行變更：
6. 按一下**完成**。

設定	方法
MDM 存取權限	
允許裝置鎖定與密碼移除	取消勾選以免強制執行密碼相符性配置。
允許裝置清除	取消勾選以免強制執行裝置清除動作。
允許查詢網路資訊 (電話/SIM 編號、MAC 位址)	取消勾選以從網路資訊報告排除裝置。 若取消勾選此選項，裝置清單檢視及裝置詳細資料檢視將會針對不再報告的網路資訊顯示不適用。 此外，將不會對受影響裝置強制執行漫遊原則。
設定檔移除密碼	
移除設定檔的密碼	指定一個密碼。 從裝置中刪除設定檔時，系統將提示使用者輸入密碼。
新增必要的 APP (iOS 15+)	
藉由查閱來新增	在 App Store 輸入 App 名稱並搜尋 app，然後所需的 app。 一次只能新增一個。 選擇一個 app 會停用其他 app。
手動新增	輸入 app 的 iTunes ID。

所做的變更僅套用至更改後才佈建的裝置。

10.10.8.8. 設定 macOS MDM 設定檔

macOS MDM 組態定義對 Ivanti Neurons for MDM 的存取限制。 對於逐一佈建的裝置，系統將個別佈建 macOS MDM 配置。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 前往**配置**。
3. 選擇要編輯的 macOS MDM 配置。
4. 按一下鉛筆 (編輯) 圖示，編輯組態。
5. 使用下列準則來進行變更：
6. 按一下**完成**。

設定	方法
允許裝置鎖定與密碼移除	取消勾選以免強制執行密碼相符性配置。
允許裝置清除	取消勾選以免強制執行裝置清除動作。
允許查詢網路資訊 (電話/SIM 編號、MAC 位址)	取消勾選以從網路資訊報告排除裝置。 若取消勾選此選項，裝置清單檢視及裝置詳細資料檢視將會針對不再報告的網路資訊顯示不適用。 此外，將不會對受影響裝置強制執行漫遊原則。
設定檔移除密碼	
移除設定檔的密碼	指定一個密碼。 從裝置中刪除設定檔時，系統將提示使用者輸入密碼。

所做的變更僅套用至更改後才佈建的裝置。

10.10.8.9. 內容快取

授權：Gold

適用於：macOS 10.13.4 或支援的更新版本。

設定內容快取服務，以啟用 App Store 軟體的本機複本，並讓連線的用戶端更快速地下載軟體和 app。

內容快取配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入**快取**，然後按一下**內容快取**配置。
4. 輸入配置的名稱和描述。
5. 輸入內容快取配置設定。
6. 按**下一步**。
7. 選擇**啟用此配置**選項。
8. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂
9. 按一下**完成**。

內容快取配置設定

使用以下表格中的設定，以設定內容快取。 有關這些設定中的更多資訊，請參閱 **Apple 說明文件**。

設定	描述
允許系統自動清除快取內容 (適用於 macOS 10.15 或支援的更新版本。)	允許系統在需要磁碟空間供其他應用程式使用時自動清除快取中的內容 (即 當電腦上的可用磁碟空間不足時)。 預設啟用此選項。
允許個人快取	快取使用者的 iCloud 資料。 用戶端可能需要一些時間 (數小時或數日) 來反應對此設定所做的變更；它不會立即生效。 預設啟用此選項。
允許共享快取 允許自動啟用內容快取 允許自動啟用共用快取 (適用於 macOS 10.15.4 或支援的更新版本)	快取非 iCloud 內容，例如 app 和軟體更新。 用戶端可能需要一些時間 (數小時，數日) 來反應對此設定所做的變更；它不會立即生效。 預設啟用此選項。 在情況許可時自動啟用內容快取，並防止停用它。 在情況許可時自動啟用網際網路連線共用，並防止停用網際網路連線共用。
停用共用快取	停用共用快取。 「停用共用快取」選項會取代「允許自動啟用共用快取」選項。
快取限制 資料路徑	將用於內容快取的最大磁碟空間位元組數。 值設為 0 表示無限制磁碟空間。 預設值：0 用於儲存快取內容的目錄路徑。 手動變更此設定並不會自動將快取內容從原本位置移至新位置。 如要自動移動內容，請使用「共用」偏好設定的「內容快取」窗格。 此值必須為 (或結尾為) /Library/Application Support/Apple/AssetCache/Data。
允許顯示提示 (適用於 macOS 10.15 或支援的更新版本。)	「內容快取」會在畫面上方角落將例外條件 (警示)，顯示為系統通知。
保持裝置喚醒 (適用於 macOS 10.15 或支援的更新版本。) **聆聽範圍** 第一個 IP 位址 最後一個 IP 位址 IP 位址類型	當「內容快取」開啟時，防止電腦進入睡眠狀態 (系統偏好設定 > 共用 > 內容快取已設為開啟)。 描述要伺服的用戶端 IP 位址範圍的一組字典。 聆聽範圍內的第一個用戶端 IP 位址。 聆聽範圍內的最後一個用戶端 IP 位址。 請選擇下列選項之一： • IPv4 (預設) • IPv6
僅允許聆聽範圍	內容快取僅會向聆聽範圍內的用戶端提供內容。
允許聆聽對等項目和父系	內容快取會向聆聽範圍、對等聆聽範圍和父系內的用戶端提供內容。 預設啟用此選項。

設定	描述
僅允許本機子網路	內容快取僅會向目前在相同本機網路上的用戶端提供內容。 不會向內容快取可連接的其他網路上的用戶端提供內容。 如果此選項已啟用，將會忽略聆聽範圍。 預設啟用此選項。
記錄用戶端身份識別	內容快取會記錄要求內容的用戶端 IP 位址和連接埠號。
父系選擇原則	請選擇下列其中一個原則選項： • 第一個可用的 • URL 路徑雜湊 • 循環配置資源 (預設) • 隨機 • 可用相黏
父系	此快取應下載自或上傳至的其他內容快取的多個本機 IP 位址，而非直接下載自或上傳至 Apple。 按一下 **+新增**以新增一或多個 IP 位址。
僅允許對等本機子網路	內容快取僅會與相同本機網路上的其他內容快取建立對等，而與非使用和裝置相同的公用 IP 位址之內容快取。 預設啟用此選項。
連接埠	內容快取接受上傳或下載要求所用的 TCP 連接埠號。 將連接埠設為 0 則會隨機挑選可用的連接埠。 預設值：0
公用範圍	字典陣列，用於描述公用 IP 位址的範圍，Ivanti Neurons for MDM 應使用範圍中的公用 IP 位址將用戶端與內容快取進行匹配。
第一個 IP 位址	公用範圍內的第一個伺服器 IP 位址。
最後一個 IP 位址	聆聽範圍內的最後一個伺服器 IP 位址。
IP 位址類型	請選擇下列選項之一： • IPv4 (預設) • IPv6

如需更多資訊，請參閱[如何建立配置](#)。

10.10.8.10. 建立 Android 捷徑

捷徑僅適用於使用允許清單瀏覽器時的單一應用模式。 瀏覽器必須名列在「鎖定」和「單一應用」配置的允許清單中

配置的白名單中。 捷徑將顯示在 Ivanti Neurons for MDM Kiosk 啟動程式中。

程序

1. 前往**組態**。 **> +新增**
2. 按一下 **Android 捷徑**以顯示**建立 Android 捷徑組態**頁面。
3. 在**名稱**欄位中輸入組態的名稱。
4. 在**說明**欄位中輸入組態的說明。
5. 在**標籤**欄位中輸入捷徑的唯一標籤。
6. 在 **URL** 欄位中輸入捷徑的目標的 URL。
7. 或者，將檔案拖放至圖示欄位中，或按一下**選擇檔案**來瀏覽檔案以選擇捷徑的圖示。
8. 按**下一步**。

10.10.8.11. 建立輔助工具設定組態

此組態允許企業在 Apple 裝置上限制、變更或設定協助工具設定。

程序

1. 前往**配置**。
2. 按一下 **+新增**。
3. 按一下**協助工具設定組態**。
4. 設定下表中指定的設定:

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
選取協助工具設定之一 **協助工具設定** 近距檢視遠點 近距檢視近點 對比度值 游標大小 滑鼠驅動程式初始延遲 滑鼠驅動程式最大速度 啟用鍵盤選項中的「慢速鍵」 啟用慢速鍵的「點擊按鍵音效」 慢速鍵延遲 指定以毫秒為單位的值 選取核取方塊 - 以單音播放立體聲音效 啟用鍵盤選項中的相黏鍵 啟用為相黏鍵設定了輔助按鍵時發出嗶聲 針對相黏鍵啟用「在螢幕顯示按下的按鍵」 啟用語音輔助 啟用顯示調節中的反轉色彩 **協助工具限制**	• **協助工具設定**: 使用此項可以設定 macOS 裝置上的協助工具設定。 • **協助工具設定限制**: 使用此項可以限制對 iOS 裝置協助工具設定的變更。 **配置設置** 縮放設定中的最小縮放級別 縮放設定中的最大縮放級別 啟用縮放選項中的「使用捲動手勢」 啟用縮放選項中的「平滑影像」 指定值 選取核取方塊 - 啟用音訊選項中的「閃爍螢幕」 選取核取方塊 - 啟用滑鼠與觸控板選項中的滑鼠按鍵 指定值 選取核取方塊 - 忽略內建觸控板 指定值 指定值 選擇核取方塊 選擇核取方塊 選擇核取方塊 選擇核取方塊 選擇核取方塊 選擇核取方塊 選擇核取方塊 選擇核取方塊 選擇核取方塊 選擇核取方塊 選擇核取方塊 **配置設置**

設定	方法
啟用粗體文字	選擇核取方塊
啟用增加對比度	選擇核取方塊
啟用減少動作	選擇核取方塊
啟用降低透明度	選擇核取方塊
支援使用動態文字的協助工具文字大小應用程式	從下拉式清單中選取選項
啟用觸控調節	選擇核取方塊
啟用語音輔助	選擇核取方塊
啟用縮放	選擇核取方塊

5. 選擇分發選項，並在適用時指定必要的詳細資訊。
6. 按一下**完成**。

10.10.8.12. 建立螢幕保護程式組態

螢幕保護程式組態可讓您新增如密碼、閒置時間、模組路徑和名稱等選項。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 按一下**配置**。
3. 按一下 **+新增**。
4. 在搜尋欄位中輸入「螢幕」，然後按一下**螢幕保護程式**:
   隨即顯示「建立螢幕保護程式組態」詳細資料頁面。
5. 在此頁面上進行設定。 請參閱**螢幕保護程式組態設定**主題中的表格，以取得相關值的說明。
6. 按**下一步**以進行發佈設定，然後按一下**完成**。

螢幕保護程式組態設定

設定	方法
名稱 (必要)	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
提示輸入密碼核取方塊	選取該核取方塊，以於螢幕保護程式解除鎖定或停止時提示裝置使用者輸入密碼。 (適用於 macOS 10.13 和更新版本)。
提示密碼延遲	指定延遲期間 (秒數)。
登入視窗閒置時間	指定啟動螢幕保護程式前的閒置時間 (秒數)。
螢幕保護程式模組的路徑	指定螢幕保護程式模組的路徑。
螢幕保護程式模組的名稱 (必要)	輸入螢幕保護程式的名稱。

如需更多資訊，請參閱如何建立配置。

10.10.8.13. 設定使用者的螢幕保護程式

「使用者的螢幕保護程式」組態可讓您新增密碼、閒置時間、模組路徑和名稱等選項。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 按一下**配置**。
3. 按一下 **+新增**。
4. 在搜尋欄位中輸入「螢幕」，然後按一下**使用者的螢幕保護程式**:
   隨即顯示「建立使用者的螢幕保護程式組態」詳細資料頁面。
5. 在此頁面上進行設定。 請參閱**使用者的螢幕保護程式組態設定**主題中的表格，以取得相關值的說明。
6. 按**下一步**以進行發佈設定，然後按一下**完成**。

使用者的螢幕保護程式組態設定

設定	方法
名稱 (必要)	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
閒置時間	指定啟動螢幕保護程式前的閒置時間 (秒數)。
螢幕保護程式模組的路徑	指定螢幕保護程式模組的路徑。
螢幕保護程式模組的名稱 (必要)	輸入螢幕保護程式的名稱。

如需更多資訊，請參閱如何建立配置。

10.10.8.14. 裝置名稱設定

授權：Silver

預設裝置名稱組態讓您能建立新的組態，在註冊時或註冊後將之下推至裝置，並允許命名裝置。 管理員只能為**受監督的 iOS 8 裝置**定義預設裝置名稱。 您可使用下列變數來建構裝置名稱：

- 裝置序號
- 裝置 IMEI
- 裝置機型
- Ivanti Neurons for MDM 使用者名稱 (僅限本機使用者)
- LDAP 組織單位 (OU)
- LDAP 常用名稱 (CN)

例如，若是開頭為裝置序號且結尾為使用者組織 (如 LDAP 所定義) 的裝置名稱，可輸入 $-$。

預設裝置名稱設定 (適用於 iOS)

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
裝置名稱 描述	輸入預設裝置名稱的格式，包括可用的裝置與 LDAP 屬性。* 如果產生的裝置名稱超過 63 個字元，就會將名稱縮短以便正確顯示在裝置上。 輸入可說明此配置用途的描述。

> 若適用，鍵入 $ 可查看此欄位的支援**變數**清單。

裝置名稱設定 (Android)

Android 裝置名稱可透過 Go app 擷取。 當管理員產生「裝置詳細資訊」報告時，所顯示的是實際裝置名稱，而非裝置型號或製造商的名稱。 若使用者更改了裝置名稱，則下次產生報告時將顯示新名稱。 各個裝置名稱可在**裝置** > **設定** > **裝置名稱**下查看。

10.10.8.15. 裝置桌布配置

授權： Silver

裝置桌布組態定義 Android 7.0 裝置 (處於裝置擁有者模式) 或公司擁有的個人已啟用 (COPE) 裝置 (不含 Android 11 EPO 模式裝置) 的主畫面和鎖定螢幕的預設桌布影像。

Android 桌布設定

定義 Android 裝置的預設桌布圖片：

1. 前往**配置**。
2. 按一下 **+新增**。
3. 按一下**裝置桌布**。
4. 按一下 Android 圖示以檢視 Android 的配置設置區段，並進行以下設定
5. 按**下一步**。

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
上傳 Android 桌布	
在「首頁畫面」和「鎖定畫面」使用相同的影像	選擇以上傳用於這兩種畫面的單一圖片。
首頁畫面	拖曳影像檔案，或按一下**選擇檔案**來選擇。
鎖定畫面	拖曳影像檔案，或按一下**選擇檔案**來選擇。

6. 請選擇下列發佈選項之一：

- **所有裝置**
- **沒有裝置** (預設)
- **自訂**

7. 按一下**完成**。

> 上傳的圖片必須為 .jpg 或 .png 格式。

iOS 桌布設定

您可以定義 iOS 裝置的預設桌布影像。

> 此設定僅適用於受監督的裝置。

1. 前往**配置**。
2. 按一下 **+新增**。

3. 按一下**裝置桌布**。
4. 按一下 iOS 圖示以檢視 iOS 的配置設置區段，並進行以下設定
5. 按**下一步**。

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
上傳 iPhone 桌布	
在「首頁畫面」和「鎖定畫面」使用相同的影像	選擇上傳 iPhone 的單一影像。
首頁畫面	拖曳影像檔案，或按一下**選擇檔案**來選擇。
鎖定畫面	拖曳影像檔案，或按一下**選擇檔案**來選擇。
上傳 iPad 桌布	
在「首頁畫面」和「鎖定畫面」使用相同的影像	選擇上傳 iPad 的單一影像。
首頁畫面	拖曳影像檔案，或按一下**選擇檔案**來選擇。
鎖定畫面	拖曳影像檔案，或按一下**選擇檔案**來選擇。

6. 請選擇下列選項之一：

- **所有裝置**
- **沒有裝置** (預設)
- **自訂**

7. 按一下**完成**。

> 上傳的圖片必須為 640 (寬) x 1136 (高)，格式為 .jpg 或 .png。

macOS 桌布設定

定義 macOS 裝置的預設桌布圖片：

1. 前往**配置**。
2. 按一下 **+新增**。
3. 按一下**裝置桌布**。
4. 按一下 macOS 圖示以檢視 macOS 的配置設置區段。
5. 輸入至桌面圖片的路徑。
6. 按**下一步**。
7. 請選擇下列選項之一：
    - **所有裝置**
    - **沒有裝置** (預設)

- **自訂**

8. 按一下**完成**。

> 您可根據限制變更桌布。 如果 macOS 限制組態**允許修改桌布**已啟用，您就能修改桌布。

如需更多資訊，請參閱**如何建立配置**。

10.10.8.16. EMA 伺服器整合配置

EMA 伺服器整合配置能讓 Windows 10 裝置連結到已配置的 Intel EMA 伺服器。 若要將裝置連結到已配置的 Intel EMA 伺服器，您應提供原始 EMA 代理程式的安裝目錄，並從新的 EMA 伺服器上傳 EMA 代理程式 .msh 檔案。

此功能需要 Bridge。 請參閱 **Bridge** 以取得詳細資料。

程序

1. 前往**配置 > +新增**。
2. 選擇**EMA 伺服器整合**配置。
3. 輸入配置的名稱。
4. 在「配置設定」區段中，按一下**選擇檔案**以選擇 EMA 代理程式 .msh 檔案。

> msh 檔案是代理程式原則檔案，可從 EMA 伺服器下載取得。

5. 在原始 **EMA 代理程式安裝目錄**欄位中，輸入原始 EmaAgent.exe 檔案安裝的位置。
6. 按**下一步**。
7. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂
8. 按一下**完成**。

10.10.8.17. 省電組態

Ivanti Neurons for MDM 可為您在 Windows 和 macOS 裝置上用來設定能源節約程式設定的承載啟用能源節約程式組態。

適用於：

- Windows 10 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- macOS 10.7 到 Ivanti Neurons for MDM 所支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取**省電**組態。
3. 在「選擇作業系統」區段中，選取 **Windows** 或 **macOS**，然後按一下**下一步**。
4. 按一下 **+新增描述**以輸入配置的簡短描述。
5. 在 Windows 上，設定下列**能源節約程式**設定:
   - **裝置使用電池供電**
   - **裝置使用電源供應器供電**
6. 配置下列**省電**設定:
   - **桌上型電腦 AC 電源省電設定**
   - **電腦啟動或關機的排程設定**
   - **筆記型電腦 AC 電源省電設定**
   - **筆記型電腦電池電源省電設定**
7. 按**下一步**，確認發佈設定。
8. 選取其中一個發佈選項以設定**省電**組態。 如需有關設定發佈選項的詳細資訊，請參閱**使用配置**。
9. 按一下**完成**。

Windows 能源節約程式組態

對裝置套用新的能源節約程式組態時，或現有的能源節約程式組態設定經過修改時，使用者必須重新啟動裝置，變更才會生效。

裝置使用電池供電

裝置使用電池供電時，使用下表中的能源節約程式設定:

設定	描述
開啟能源節約程式的電力閾值	當裝置使用電池供電時，輸入開啟能源節約程式的電池電量，您可輸入 0 到 100 的值。 輸入表示電池電量的百分比值。 例如，設定為 80 時，能源節約程式會在電池電量為 80% 或更少電量時開啟。 如果您未輸入值，Ivanti Neurons for MDM 就不會變更或更新此設定。 Windows 會將此值預設為 70%。
蓋子闔上時	• **不採取行動**: 裝置保持開啟並繼續使用電池電量。 • **睡眠**: 裝置進入睡眠模式並使用少量電池電量。 電腦仍是開啟狀態，且開啟的應用程式和檔案會儲存在隨機存取記憶體 (RAM) 中。 • **休眠睡眠狀態**: 裝置進入休眠模式。 開啟的應用程式和檔案會儲存在硬碟上，且裝置會關閉。 • **關機**: 裝置關機。 開啟的應用程式和檔案會關閉且不會儲存。
選取電源按鈕時	• **不採取行動**: 裝置保持開啟並繼續使用電池電量。 • **睡眠**: 裝置進入睡眠模式並使用少量電池電量。 電腦仍是開啟狀態，且開啟的應用程式和檔案會儲存在 RAM 中。 • **休眠睡眠狀態**: 裝置進入休眠模式。 開啟的應用程式和檔案會儲存在硬碟上，且裝置會關閉。 • **關機**: 裝置關機。 開啟的應用程式和檔案會關閉且不會儲存。
選取睡眠按鈕時	• **不採取行動**: 裝置保持開啟並繼續使用電池電量。 • **睡眠**: 裝置進入睡眠模式並使用少量電池電量。 電腦仍是開啟狀態，且開啟的應用程式和檔案會儲存在 RAM 中。 • **休眠睡眠狀態**: 裝置進入休眠模式。 開啟的應用程式和檔案會儲存在硬碟上，且裝置會關閉。 • **關機**: 裝置關機。 開啟的應用程式和檔案會關閉且不會儲存。
開啟混合睡眠	• **True**: 裝置可進入混合睡眠模式。 開啟的應用程式和檔案會儲存在 RAM 和硬碟中。 在此情況下裝置使用少量電池電量。 • **False**: 防止裝置進入混合睡眠模式。

裝置使用電源供應器供電

裝置使用外接電源供電時，使用下表中的設定:

設定	描述
開啟能源節約程式的電力閾值	當裝置使用電源供應器供電時，輸入開啟能源節約程式的電池電量，您可輸入 0 到 100 的值。 輸入表示電池電量的百分比值。 例如，設定為 80 時，能源節約程式會在電池電量為 80% 或更少電量時開啟。 如果您未輸入值，Ivanti Neurons for MDM 就不會變更或更新此設定。 Windows 會將此值預設為 70%。
蓋子闔上時	• **不採取行動**: 裝置保持開啟並繼續使用外接電源。 • **睡眠**: 裝置進入睡眠模式並使用少量外接電源電量。 電腦仍是開啟狀態，且開啟的應用程式和檔案會儲存在 RAM 中。 • **休眠睡眠狀態**: 裝置進入休眠模式。 開啟的應用程式和檔案會儲存在硬碟上，且裝置會關閉。 • **關機**: 裝置關機。 開啟的應用程式和檔案會關閉且不會儲存。
選取電源按鈕時	• **不採取行動**: 裝置保持開啟並繼續使用外接電源。 • **睡眠**: 裝置進入睡眠模式並使用少量外接電源電量。 電腦仍是開啟狀態，且開啟的應用程式和檔案會儲存在 RAM 中。 • **休眠睡眠狀態**: 裝置進入休眠模式。 開啟的應用程式和檔案會儲存在硬碟上，且裝置會關閉。 • **關機**: 裝置關機。 開啟的應用程式和檔案會關閉且不會儲存。
選取睡眠按鈕時	• **不採取行動**: 裝置保持開啟並繼續使用外接電源。 • **睡眠**: 裝置進入睡眠模式並使用少量外接電源電量。 電腦仍是開啟狀態，且開啟的應用程式和檔案會儲存在 RAM 中。 • **休眠睡眠狀態**: 裝置進入休眠模式。 開啟的應用程式和檔案會儲存在硬碟上，且裝置會關閉。 • **關機**: 裝置關機。 開啟的應用程式和檔案會關閉且不會儲存。
開啟混合睡眠	• **True**: 裝置可進入混合睡眠模式。 開啟的應用程式和檔案會儲存在 RAM 和硬碟中。 在此情況下裝置使用少量外接電源電量。 • **False**: 防止裝置進入混合睡眠模式。

macOS 能源節約程式組態

桌上型電腦 AC 電源省電設定

使用以下設定以配置 macOS 桌面裝置的 AC 電源省電設定:

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
電腦當機時將自動重新開機	讓裝置在電源中斷後自動重新開機。
閒置持續下列時間後讓硬體進入睡眠	啟用核取方塊可讓硬碟在閒置 1 到 180 分鐘之間的固定時間間隔後進入睡眠狀態。 值為 0 分鐘時即表示永遠不會讓硬碟進入睡眠狀態。
閒置持續下列時間後關閉顯示器	啟用核取方塊可讓顯示器在閒置 1 到 180 分鐘之間的固定時間間隔後關閉。 值為 0 分鐘時即表示永遠不會關閉顯示器。
動態電源 STEP	選取核取方塊可啟用動態電源 STEP。
降低處理器速度	選取核取方塊可降低處理器速度。
閒置持續下列時間後讓電腦進入睡眠	啟用核取方塊可讓電腦在閒置 1 到 180 分鐘之間的固定時間間隔後進入睡眠狀態。 值為 0 分鐘時即表示永遠不會讓電腦進入睡眠狀態。
網路連線時喚醒	選取核取方塊可在存取網路時喚醒電腦。
數據機鈴響時喚醒	選取核取方塊可在數據機鈴響時喚醒電腦。

電腦啟動或關機的排程設定

使用以下設定以配置 macOS 裝置，從而進行裝置的排程啟動或關閉。

關閉裝置設定

選取**關閉裝置**核取方塊可在固定時間間隔後關閉裝置。

設定	描述
事件類型	從下拉式清單中選取一個事件類型: • 睡眠 • 重新啟動 • 關機
時間	選取一週中的一天或多天來排程事件類型。
時刻	選取排程事件類型的時間。

啟動或喚醒裝置設定

選取**啟動或喚醒裝置**核取方塊可在固定時間間隔後喚醒裝置。

設定	描述
事件類型	從下拉式清單中選取一個事件類型: • 喚醒 • 啟動/喚醒
時間	選取一週中的一天或多天來排程事件類型。
時刻	選取排程事件類型的時間。

筆記型電腦 AC 電源省電設定

使用以下設定以配置 macOS 筆記型電腦裝置的 AC 電源省電設定:

設定	描述
電腦當機時將自動重新開機	讓裝置在電源中斷後自動重新開機。
閒置持續下列時間後讓硬體進入睡眠	啟用核取方塊可讓硬碟在閒置 1 到 180 分鐘之間的固定時間間隔後進入睡眠狀態。 值為 0 分鐘時即表示永遠不會讓硬碟進入睡眠狀態。
閒置持續下列時間後關閉顯示器	啟用核取方塊可讓顯示器在閒置 1 到 180 分鐘之間的固定時間間隔後關閉。 值為 0 分鐘時即表示永遠不會關閉顯示器。
動態電源 STEP	選取核取方塊可啟用動態電源 STEP。
降低處理器速度	選取核取方塊可降低處理器速度。
閒置持續下列時間後讓筆記型電腦進入睡眠	啟用核取方塊可讓筆記型電腦在閒置 1 到 180 分鐘之間的固定時間間隔後進入睡眠狀態。 值為 0 分鐘時即表示永遠不會讓筆記型電腦進入睡眠狀態。
網路連線時喚醒	選取核取方塊可在存取網路時喚醒筆記型電腦。
數據機鈴響時喚醒	選取核取方塊可在數據機鈴響時喚醒筆記型電腦。

筆記型電腦電池電源省電設定

使用以下設定以配置 macOS 筆記型電腦電池電源省電設定:

設定	描述
電腦當機時將自動重新開機	讓裝置在電源中斷後自動重新開機。
閒置持續下列時間後讓硬體進入睡眠	啟用核取方塊可讓硬碟在閒置 1 到 180 分鐘之間的固定時間間隔後進入睡眠狀態。 值為 0 分鐘時即表示永遠不會讓硬碟進入睡眠狀態。
閒置持續下列時間後關閉顯示器	啟用核取方塊可讓顯示器在閒置 1 到 180 分鐘之間的固定時間間隔後關閉。 值為 0 分鐘時即表示永遠不會關閉顯示器。
動態電源 STEP	選取核取方塊可啟用動態電源 STEP。
降低處理器速度	選取核取方塊可降低處理器速度。
閒置持續下列時間後讓電腦進入睡眠	啟用核取方塊可讓筆記型電腦電池在閒置 1 到 180 分鐘之間的固定時間間隔後進入睡眠狀態。 值為 0 分鐘時即表示永遠不會讓筆記型電腦電池進入睡眠狀態。
網路連線時喚醒	選取核取方塊可在存取網路時喚醒筆記型電腦電池。
數據機鈴響時喚醒	選取核取方塊可在數據機鈴響時喚醒筆記型電腦電池。

10.10.8.18. 乙太網路組態 (macOS)

授權：Gold

適用於：macOS 10.13 +或支援的更新版本。

管理員可配置乙太網路介面變化。 以下裝載適用於配置乙太網路：

- 全域乙太網路
- 第一個主動式乙太網路
- 第一個乙太網路
- 第二個主動式乙太網路
- 第二個乙太網路
- 第三個主動式乙太網路
- 第三個乙太網路

> 配置乙太網路的不同裝載為預設後援全域、第一個、第一個主動式、第二個、第二個主動式、第三個和第三個主動式乙太網路介面。 現在已知 Apple 裝置在安裝第一個、第一個主動式、第二個、第二個主動式、第三個和第三個主動式乙太網路介面時會出現一個問題。

乙太網路配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。
3. 在搜尋欄位中輸入**乙太網路**，然後選取**乙太網路**組態。
4. 輸入配置的名稱和描述。
5. 從下拉清單中選取組態設定。
6. 輸入乙太網路配置設定。
7. 按**下一步**。
8. 選擇**啟用此配置**選項。
9. 選擇以下一個要套用配置的通道選項：
    - 裝置通道 (最常用)
    - 使用者通道 (目前註冊的使用者)
10. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂
11. 按一下**完成**。

乙太網路配置設定

使用以下表格中的設定，以設定乙太網路。 有關這些設定中的更多資訊，請參閱 **Apple 說明文件**。

設定	描述
通訊協定	
接受的 EAP 類型	選擇可用來存取此網路的 EAP 類型： • Transport Layer Security (TLS)：TLS 是在網際網路上兩部電腦之間建立加密工作階段的通訊協定。 它可驗證伺服器的身份，防止駭客攔截任何資料。 • TTLS：在**內部身份**欄位中，選擇一項身份驗證通訊協定，例如 OS Default、PAP、CHAP、MSCHAP、MSCHAPv2 和 EAP。 • PEAP • LEAP • EAP-SIM：在 **RAND 的 EAP SIM 編號**欄位中，從下拉式清單中選擇 RAND 數。 • EAP-AKA • EAP-FAST：選擇用來定義驗證方法的 EAP-FAST 選項： ◦ **使用 PAC**：選擇使用 Proxy 自動配置 (PAC)。 ◦ **裝置 PAC**：選擇允許裝置 PAC。 否則的話，僅可使用裝置上已設置的 PAC。 只有當您選擇「使用 PAC」時，才可使用此選項。 ◦ **匿名佈建 PAC**：選擇允許佈建 PAC 而不需驗證伺服器。 只有當您選擇「設置 PAC」時，才可使用此選項。
憑證	**使用者名稱**：指定網路存取所需的使用者名稱。 如果您保留空白，系統就會提示裝置使用者輸入。 • 使用者每次連線密碼：選擇以提示裝置使用者在每次連線時都要輸入密碼。 當裝置重新加入相同的網路時，系統會提示裝置使用者重新驗證以加入網路。 每當初始連線時，就需要輸入密碼。 • 當連線至網路時提示一次性密碼：當推送此配置至裝置後，只需輸入密碼一次。 每次連線和中斷連線網路時，將不需要輸入任何密碼。 **密碼**：(選用) 輸入存取此網路的密碼。 否則，系統會提示裝置使用者輸入存取網路所需的密碼。 **外部身份**：(選用) 針對 TTLS、PEAP 及 EAP-FAST，選擇允許裝置使用者隱藏身份。 只有在內部加密的 tunnel 中會顯示使用者的實際名稱。 由於攻擊者無法清楚查看正在驗證的使用者名稱，因此可提高安全性。 **系統模式認證來源身份**：系統模式用於電腦身份驗證。 使用系統模式的身份驗證發生在使用者登入電腦之前。 系統模式常用於使用當地憑證授權中心發出的電腦 X.509 憑證 (EAP-TLS) 提供身份驗證。
信任	**信任的憑證:** 從清單中選取核取方塊，以選取多個憑證。 **信任的伺服器憑證名稱**: 新增憑證名稱。 • **允許信任例外狀況**: 允許使用者做出信任決策 (透過對話方塊)。 • **需要 TLS 憑證** **使用 EAP 身份認證允許的最高 TLS 版本** **使用 EAP 身份認證允許的最低 TLS 版本** **TLS 信任的憑證：MobileIron 代理程式 CA 憑證**

如需更多資訊，請參閱如何建立配置。

10.10.8.19. Google BeyondCorp 組態

Ivanti Neurons for MDM 可與 Google BeyondCorp 整合以提供條件式存取。 Ivanti Neurons for MDM 會向 Google BeyondCorp 傳送裝置合規性狀態訊號。 這可確保只有 N-MDM 下的合規裝置才能存取 Google Workspace 應用程式。

適用於

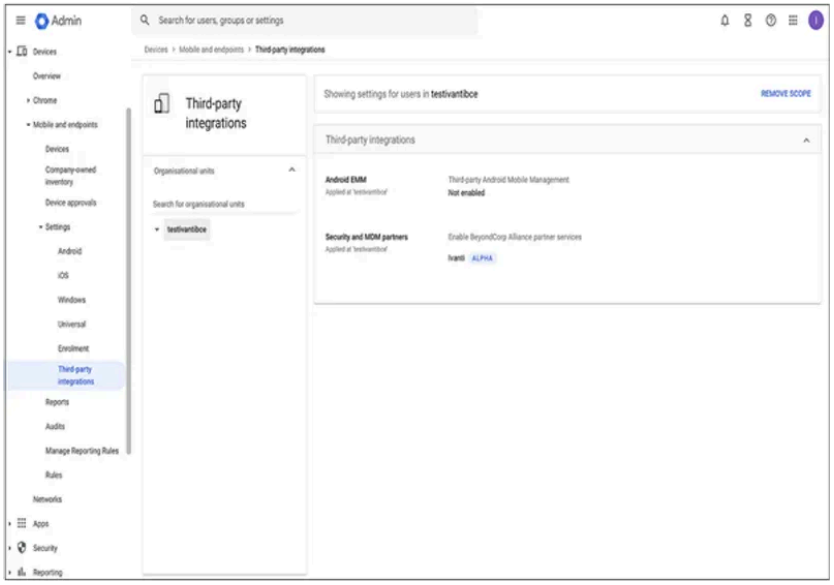
- iOS
- Android
- Windows

必要條件

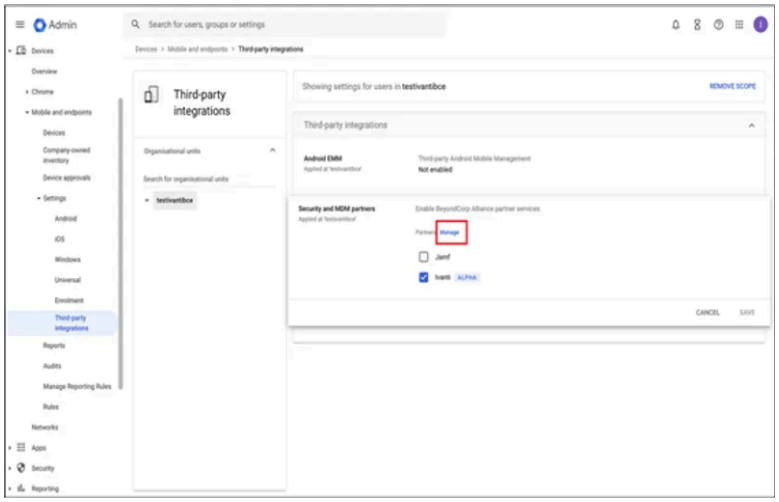
- 若使用 Ivanti Neurons for MDM，您必須有 Ivanti Professional Plus / Premium 授權。
- 若使用 Google，您必須有 BeyondCorp Enterprise、Google Workspace Enterprise 或 Cloud Identity Premium 授權。
- 對於 Windows，必須在裝置上安裝以下內容:
  - Ivanti Bridge
  - Google Chrome

程序 (Google)

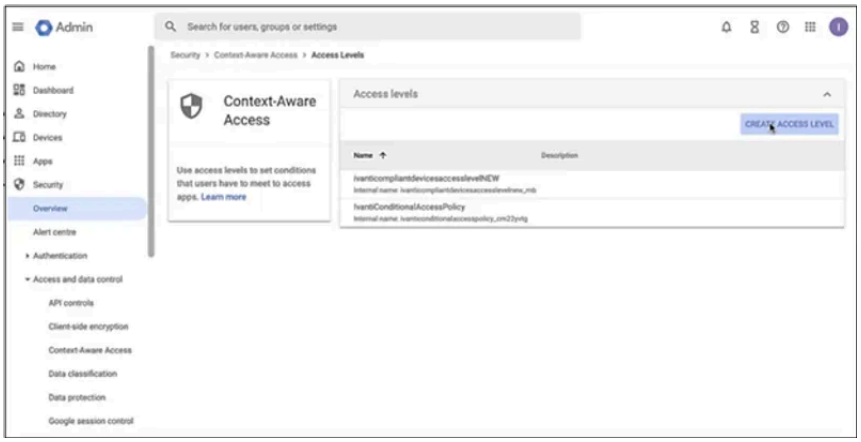
1. 使用管理員認證登入 **Google 管理控制台**。
2. 前往**裝置** > **行動與端點** > **設定** > **第三方整合**。



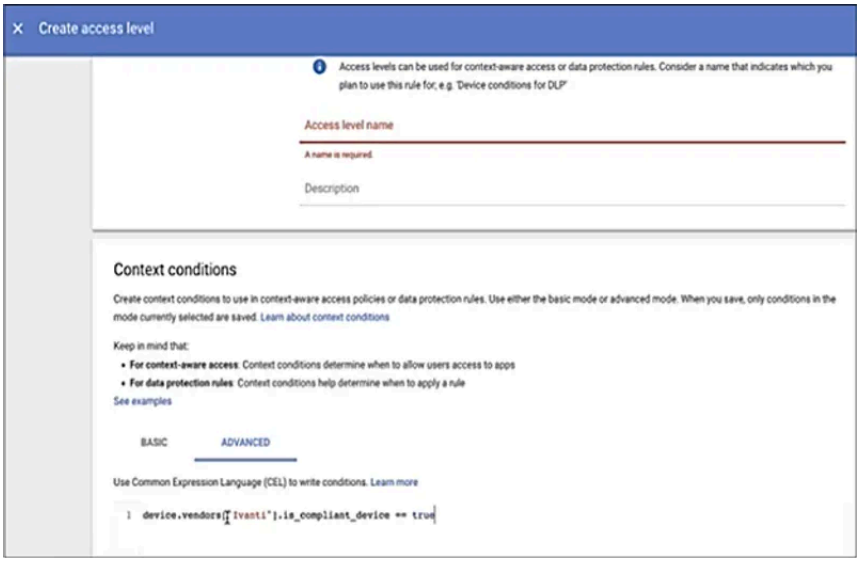
3. 按一下**安全性和 MDM 合作夥伴** > **管理**。



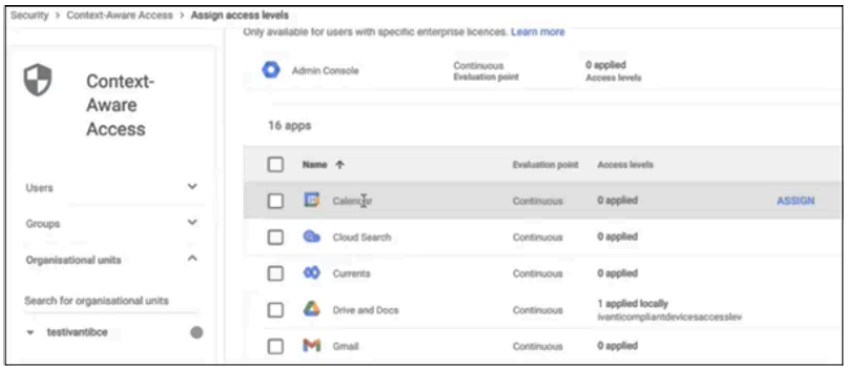
4. 在**管理合作夥伴連線**視窗中，選取 **Ivanti**。
5. 按一下**開啟連線**。
   您將重新導向至 Ivanti Neurons for MDM 登入頁面，需要輸入租用戶管理員認證。 登入租用戶後，您將看到 **Google BeyondCorp** 已啟用並自動連結到您的 Google 帳戶。
6. 在 Google 管理控制台中，前往**安全性** > **情境感知存取權** > **存取層級**。



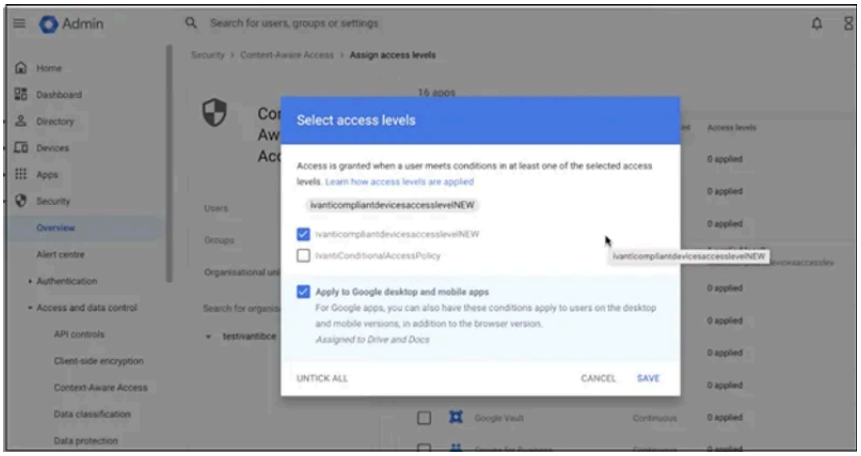
7. 按一下**建立存取層級**。
   在「建立存取層級」視窗的「情境條件」區段下，按一下**進階**並提供所需資訊。



8. 前往**安全性** > **情境感知存取權** > **存取層級**，選取要為其指派原則的應用程式。



9. 按一下**指派**。
10. 從**選取存取層級**視窗中，選取要指派的原則，然後按一下**儲存**。



完成上述設定後，您就可以使用 **Google BeyondCorp** 建立合作夥伴裝置合規性組態。

程序 (Ivanti Neurons for MDM**)**:

1. 前往**組態** > **新增組態**。

2. 選取**合作夥伴裝置合規性**組態。
3. 畫面上將出現「建立合作夥伴裝置合規性」組態頁面。
   輸入配置的名稱。
4. 在「選擇合作夥伴」清單下，選取 **Google BeyondCorp**。
5. 畫面上會出現「組態設定」區段。 確定「回報 iOS 和 Android 裝置的合規性狀態」選項設定為「開啟」。
   按**下一步**。
6. 選取**啟用此組態**。
7. 選取**自訂**作為發佈選項。
8. 在**自訂發佈**選項下，選取**使用者/使用者群組**。
9. 於**在下方選取以發佈此組態**區段下，從清單中選取使用者/使用者群組。
10. 按一下**完成**。

> Google BeyondCorp 伺服器可透過應用程式管理的組態 P 清單，以唯一方式標識每個裝置。
> 

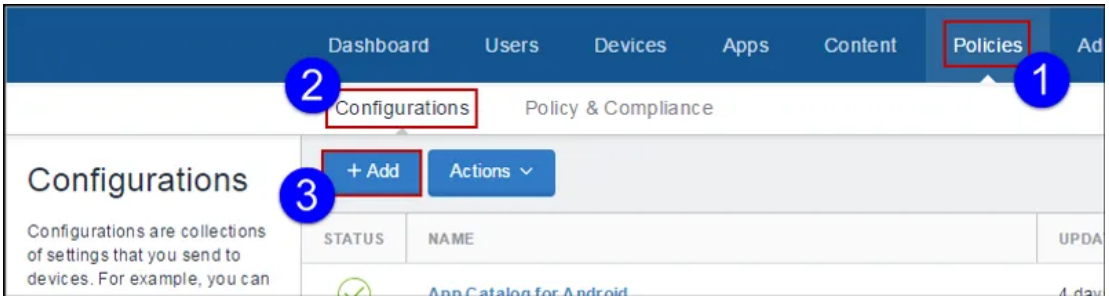
10.10.8.20. 鎖定畫面訊息配置

在登入與鎖定畫面中，顯示訊息與資產標記資訊。 這適用於使用 iOS 9.3 或支援的更新版本之受監管裝置。

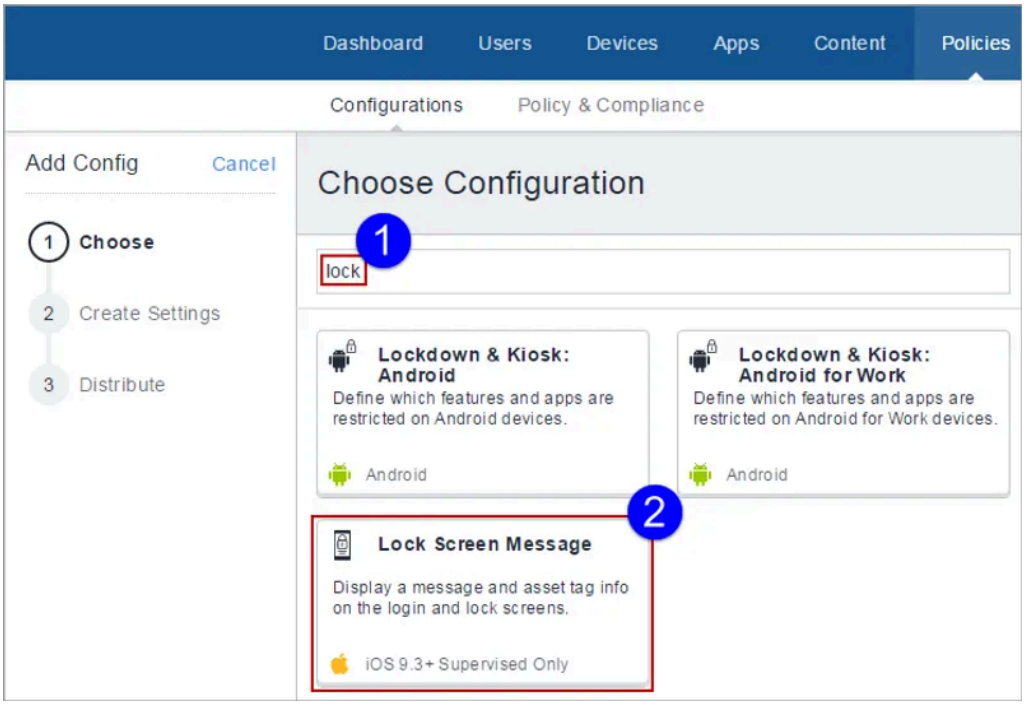
建立鎖定畫面訊息配置

程序

1. 選擇**配置**。
2. 按一下 **+新增**。



在搜尋欄位中，輸入**鎖定**，然後按一下**鎖定畫面訊息**配置：



隨即顯示「鎖定畫面訊息配置」詳細資料頁面。
在此頁面上進行設定。 請參閱鎖定畫面訊息組態設定一節中的表格，以取得相關值的說明。

5. 按**下一步**以進行發佈設定，然後按一下**完成**。

鎖定畫面訊息配置設定

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
鎖定螢幕註腳	這段文字會顯示在登入視窗與鎖定畫面中。
資產標記資訊	這段文字會顯示在登入視窗與鎖定畫面底端。

如需更多資訊，請參閱**如何建立配置**。

10.10.8.21. 登入視窗組態 - macOS

程序

1. 登入到 Ivanti Neurons for MDM。
2. 前往**組態** > **新增組態**。
3. 按一下 (或選取) **登入 Window**。
4. 在**名稱**欄位中，輸入登入視窗組態的名稱。
5. 按一下 **+ 新增描述**以加入詳細資訊。
6. 在**組態設定**區段下，提供下列欄位:
    - **管理員主機資訊**: 輸入主機名稱或 IP 位址或 SystemVersion。
    - **允許清單**: 系統允許使用者登入的使用者 GUID 或使用者群組 GUID 清單。 星號 ('*') 字串指定所有使用者或群組。
    - **自動登入密碼**: 輸入自動登入密碼。
    - **拒絕清單**: 系統不允許登入的使用者 GUID 或使用者群組 GUID 清單。 此清單的優先順序高於「AllowList」鍵中的清單。
    - **登入視窗文字**: 輸入登入視窗文字。
    - 選取核取方塊以取得其他選項，例如:
        - **停用主控台存取**
        - **停用 FDE 自動登入 (FileVault 磁碟加密)**
        - **停用立即螢幕鎖定功能**
        - **顯示使用者清單時隱藏管理員使用者**
        - **僅顯示網路和系統使用者**
        - **隱藏行動帳戶**
        - **顯示網路使用者**
        - **停用登出功能表項目**
        - **使用者登入時停用關機**
        - **使用者登入時停用重新啟動功能表項目**
        - **停用重新啟動項目**
        - **顯示名稱和密碼對話方塊**
        - **顯示其他使用者 - 受管理**
        - **顯示輸入功能表**
        - **停用關機按鈕**
        - **停用休眠按鈕**
        - **停用關機功能表項目**
7. 按一下**完成**。

10.10.8.22. macOS 系統延伸配置

「系統延伸」配置允許安裝延伸類型 (例如驅動程式延伸、網路延伸和端點安全性延伸)，無需核心層級存取。

程序

適用於：macOS 10.15+

1. 前往**配置** > **+新增**。
2. 在搜尋欄位中輸入 **extension**，然後按一下**系統延伸**配置。
3. 輸入配置的**名稱**和**描述**。
4. 在**允許的系統延伸**之下，**+新增允許的團隊識別碼**和**允許的系統延伸**。
5. 在**允許的系統延伸類型**之下，**+新增允許的團隊識別碼**和**允許的系統類型**。
6. 勾選**允許使用者覆寫**選項。
7. 按**下一步**。
8. 選擇**啟用此配置**選項。
9. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂。
10. 按一下**完成**。

> 在 macOS 12 中，RemovableSystemExtensions 允許應用程式在應用程式解除安裝期間停用其系統延伸模組，無需管理員核准。

10.10.8.23. 僅限 MAM

Ivanti Neurons for MDM 允許您將 iOS 和 Android 裝置指定為 MAM-only，並針對這類裝置提供行動裝置應用程式管理 (MAM)。 MAM-only 部署可讓您發佈與管理 app，完全不用管理裝置本身。

僅限 MAM 解決方案 - Ivanti AppStation 替代方案

作為 Ivanti AppStation 的替代解決方案，Ivanti 提供了一種使用 Ivanti Go 用戶端的現代靈活的行動應用程式管理 (MAM) 解決方案，可用於 iOS 和 Android 平台。

新的僅 MAM 解決方案引入了集成的應用程式目錄和 Ivanti Neurons for MDM Web 剪輯功能，共同滿足了 App Station 之前解決的核心用例要求，為使用者和管理員提供了簡化、安全和統一的應用程式管理體驗。

主要特色

- **應用程式內應用程式目錄**: 直接在 Go 用戶端中受管理和發佈經核准的受管理應用程式。
- **應用程式組態和更新**: 支援應用程式級組態和版本更新，透過 MAM 原則強制執行。
- Ivanti Neurons for MDM **要求**: 非常適合無法進行 Ivanti Neurons for MDM 註冊的 BYOD 和承包商場景。

使用 Web 剪輯以便於存取

- **直接存取應用程式目錄**: 透過 Ivanti Neurons for MDM 部署 Web 剪輯，提供應用程式目錄或特定基於 Web 的企業應用程式的捷徑。
- **自訂應用程式捷徑**: 允許使用者從主螢幕快速啟動常用資源。

增強的管理員和使用者體驗

- **統一介面**: 將應用程式目錄、Web 存取及合規性訊息組合到一個體驗中。
- **簡化管理**: 無需維護單獨的解決方案 (即App Station)，降低了組態漂移的複雜性和風險。

靈活性及自訂

- **自訂目錄檢視**: 依據使用者角色、地理位置或組織單位自訂應用程式目錄內容。
- **使用現有基礎結構**: 利用您現有的 Ivanti Neurons for MDM /MAM 投資 (不需要單獨的基礎結構)。

支援雙重角色使用者

Ivanti 僅限 MAM 解決方案旨在支援現代工作場景，包括具有雙重角色的使用者:

- **全職員工 - 組織 A**: 透過由 Ivanti Neurons for MDM 部署的 Web 剪輯 (例如 Apps@Work) 存取企業應用程式。
- **承攬人 - 組織 B**: 在僅限 MAM 模式下使用 Ivanti Go 用戶端安全存取受管理應用程式，而無需在 Ivanti Neurons for MDM 中進行裝置註冊。

這使得對必要應用程式的無縫、基於角色的存取成為可能，而不會出現設定檔衝突或裝置管理重疊。

移轉指導

Ivanti 強烈建議 App Station 客戶計畫並執行向基於 Go 用戶端的僅限 MAM 解決方案的過渡。 有關分步移轉協助，請參閱以下資源:

- Ivanti 僅限 MAM 解決方案

- **Go 用戶端中的應用程式目錄組態**
- **建立 Web 剪輯組態**

如果您有任何問題或需要移轉幫助，請連絡 **Ivanti 支援**或您的客戶成功經理。

10.10.8.24. 受管理的 Google Play 配置

管理員可配置自動更新設定，以供 Google Play 商店用於更新 Android Enterprise 裝置上的應用程式。

若要設置自動更新設定：

1. 前往**配置** > **+新增**。
2. 選擇**受管理的 Google Play** 配置。
3. 輸入配置的名稱。
4. 輸入描述。
5. 在「配置設置」區段中，選擇從 Google Play 更新 app 的選項。

設定	方法
使用者定義	裝置使用者可設定自動更新 app 維護視窗設定，以定義何時應更新 app。 1. 在**開始時間**欄位中，選擇要執行 app 更新的時間。 2. 在**期間**欄位中，選擇應執行更新的期間 (以小時為單位)。 最小和最大範圍在 1 小時到 24 小時之間。 可在開始時間到選取期間之間更新 app。 例如，如果「開始時間」設為 6 PM 且「期間」設為 12 小時，則可在 6 PM 到 6 AM 期間更新 app。
無	Google Play Store 永遠不會自動更新裝置上的 app。
僅限 WiFi	Google Play Store 會自動更新裝置上的 app，但僅使用 Wi-Fi 不使用行動連線。
一律	Google Play Store 會自動更新裝置上的 app，且使用 Wi-Fi 或行動連線。

6. 按**下一步**。
7. 請選擇下列發佈選項之一：
   - 所有裝置
   - 沒有裝置 (預設)
   - 自訂
8. 按一下**完成**。

10.10.8.25. 移轉助手設定

使用**移轉助手設定**在受監管的裝置上設定移轉助手設定。 此組態可協助管理員套用一致的原則型控制項，管理使用者在裝置設定或移轉期間傳輸資料、應用程式和設定的方式。

適用於：

- 受監管的 macOS 26.4+ 到 Ivanti Neurons for MDM 所支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取**移轉助手設定**組態。
3. 按照下表設定**移轉助手設定**:

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
應執行受管理移轉	選取核取方塊以啟用和管理裝置的移轉。 切換**推播至裝置**按鈕以啟用裝置移轉。
排除的帳戶	輸入您要從移轉排除的帳戶名稱。 切換**推播至裝置**按鈕以啟用帳戶排除。
排除的路徑	輸入要從移轉排除的路徑名稱。 切換**推播至裝置**按鈕以啟用路徑排除。
必要路徑	輸入您要包含在移轉中的路徑名稱。 切換**推播至裝置**按鈕以啟用路徑包含。
應移轉安全隱私權設定	選取核取方塊以啟用從裝置移轉安全性隱私權設定。 切換**推播至裝置**按鈕以啟用安全性隱私權設定移轉。

4. 按**下一步**，確認發佈設定。
5. 選取其中一個發佈選項，以設定**移轉助手設定**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
6. 按一下**完成**。

10.10.8.26. 通知組態

管理員可以使用通知組態，排程 iOS 裝置的無訊息和可見通知。 也可以複製、匯出或刪除通知組態。

程序

1. 前往**配置** > **+新增**。
2. 選取**通知**組態。
3. 輸入配置的名稱。
4. 輸入描述。
5. 在組態設定區段中，選取一個或兩個**通知排程**選項：
   - 無訊息通知排程 - 無訊息通知用於支援 Ivanti Neurons for MDM 啟動的背景裝置管理作業。 不需要使用者互動，即可啟用自動動作，例如合規性檢查、原則更新和應用程式更新。 Ivanti Neurons for MDM 會在設定的層級傳送無訊息通知至裝置。
   - 可見通知排程 - 當需要使用者意識或動作來維持裝置合規性、安全性或功能時，會使用可見通知。 可見通知只會在指定的間隔後觸發，即使在此期間發生多個動作或事件也是如此。 只有在可見的通知間隔期間未傳送無訊息通知時，裝置上才會顯示可見的通知。
6. 按**下一步**。
7. 請選擇下列發佈選項之一：
   - 所有裝置
   - 沒有裝置 (預設)
   - 自訂
8. 按一下**完成**。

MTD 裝置的可見通知內容 - 裝置可能容易受到威脅。 請啟動 Ivanti Go 應用程式並檢查威脅防禦狀態。

非 MTD 裝置的可見通知內容 - 若要接收增強的安全性功能並確保最新的保護措施，請在裝置上啟動應用程式，以獲得更安全的使用者體驗。

10.10.8.27. 列印設定

Ivanti Neurons for MDM 可讓您建立印表機設定檔，並將它們新增至裝置。 此功能需要 Bridge。 請參閱 **Bridge** 以取得詳細資料。

> 當印表機描述檔傳送至裝置時，印表機必須處於作用中，否則裝置無法探索描述檔。

如要為 Windows 裝置進行印表機設定：

1. 前往**組態 > +新增**。
2. 選取**印表機設定**組態。
3. 輸入配置的名稱。
4. 選擇 **Windows** 選項。
5. 在**配置設置**區段中，設置下列設定：

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
Windows 印表機設定	
共享印表機	如果選擇**共享印表機**選項，印表機將會與其他裝置共享。請設定下列欄位： **名稱**：輸入印表機配置的名稱。 **描述**：輸入印表機的描述。 **列印伺服器**：輸入列印伺服器的 IP 位址。 **共享印表機名稱**：輸入印表機名稱。
網路連接印表機	選擇**網路連接** 選項時，僅所連接網路內的裝置可以存取印表機。 設定下列欄位： **名稱**：輸入印表機配置的名稱 **描述**：輸入印表機的描述。 **列印名稱**：輸入網路內部的印表機名稱。 **印表機主機位址**：輸入印表機的主機 IP 位址。 **印表機埠號**：選擇網路印表機的埠號。 **印表機驅動程式名稱**：輸入印表機驅動程式的名稱。 **印表機驅動程式 URL**：輸入印表機驅動程式的 URL。 對於印表機驅動程式，上傳包含所需檔案的 ZIP 存檔。 ZIP 必須包含以下檔案: • .inf 檔案 (驅動程式資訊) • .cat 檔案 (目錄/簽名) • INF 引用的其他任何驅動程式二進制檔案 (例如 .dll、.sys 等)

6. 按一下**下一步**。
7. 請選擇下列發佈選項之一：

- 所有裝置
- 沒有裝置 (預設)
- 自訂

8. 按一下**完成**。

如要為 macOS 裝置進行印表機設定：

1. 前往**配置 > +新增**。
2. 選擇**印表機設定**配置。
3. 輸入配置的名稱。
4. 選擇 **macOS** 選項。
5. 在**建立印表機描述**區段中，設置下列設定：

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
配置設置	為 macOS 裝置更新以下欄位以設定印表機： • 允許本機印表機 • 預設印表機顯示名稱 • 頁尾字型名稱 • 頁尾字型大小 • 使用者印表機清單 • 新增印表機

6. 按一下**下一步**
7. 請選擇下列發佈選項之一：

- 所有裝置
- 沒有裝置 (預設)
- 自訂

8. 按一下**完成**。

10.10.8.28. 移除膨脹配置

移除膨脹配置可讓您選擇裝置上所安裝，但需要強制移除之應用程式的清單。 已針對此配置設置 Bridge 是必要條件。 請參閱 **Bridge** 以取得詳細資料。

若要執行或解除安裝 app：

1. 在**配置**索引標籤中按一下 **+新增**。
2. 選取**移除 Bloatware** 配置。 隨即顯示**移除 Bloatware** 配置頁面。
3. 在**名稱**欄位中，輸入適當的配置名稱。
4. 按一下 **+新增描述**連結，以新增配置描述。此欄位為選用。
5. 在**配置設置**區段中，選擇應該要移除會解除安裝的 app。 您也可以在「搜尋」欄位中，使用在桌上型電腦 App 清單中顯示的 App 名稱來搜尋 app。

> 建立**移除膨脹軟體**組態之前，應該先前往**應用程式 > 桌上型電腦應用程式 > 擷取應用程式**擷取應用程式。 否則，在建立**移除膨脹軟體**組態後，就無法搜尋或選擇任何應用程式。

可以移除 .appx、.appxbundles、.xap 和 .msi 檔案類型，但無法移除 .exe 檔案類型。

6. 在進階選項中，設定下列選項：

選項	描述
執行此配置的間隔，每	設定執行配置的間隔持續時間 (分鐘)。
在登入時執行	選擇該勾選框以便在登入時執行配置。
禁止解除安裝後強制重新啟動	選擇該勾選框以避免在解除安裝 app 後強制重新啟動。

10.10.8.29. Safari 擴充功能和設定組態

Safari擴充功能

Ivanti Neurons for MDM 可讓您在受監督的 iOS 和 macOS 裝置上管理 Safari 擴充功能。 管理員可以有效地管理標準瀏覽和私密瀏覽的 Safari 擴充功能。

適用於：

- 受監督的 iOS 18.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。
- 受監督的 macOS 15.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取 **Safari 擴充功能設定**組態。
3. 依下表設定 **Safari 擴充功能設定**的各項設定:

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
擴充功能 ID	輸入組成的擴充功能識別碼。 例如，「*識別碼 (TeamIdentifier)*」。 所有擴充功能都要輸入「*」。 若要產生此字串，請使用代碼符號 *-dv <path_to_appex>*。 瀏覽器擴充功能位於應用程式套組內的外掛程式資料夾。 預期的格式是「*識別碼 (TeamIdentifier)*」。若是 macOS 上未提供的擴充功能，應用程式開發人員應提供此資訊。
擴充功能狀態	請選擇下列選項之一： • **允許**: 使用者可以開啟或關閉擴充功能。 • **一律開啟**: 使用者的擴充功能一律為「開啟」。 • **一律關閉**: 使用者的擴充功能一律為「關閉」。
私密瀏覽狀態	請選擇下列選項之一： • **允許**: 使用者可以在私密瀏覽中開啟或關閉擴充功能。 • **一律開啟**: 使用者的擴充功能一律為「開啟」，即使在私密瀏覽時也一樣。 • **一律關閉**: 擴充功能將無法使用。
允許的網域	輸入網域或子網域值以授予 Safari 擴充功能存取權限。 您可以輸入多個網域或子網域值。 如果您在「擴充功能 ID」欄位中輸入「*」，則裝置上不適用「允許的網域」設定。
拒絕的網域	輸入網域或子網域值以限制 Safari 擴充功能存取權限。 您可以輸入多個網域或子網域值。 如果您在「擴充功能 ID」欄位中輸入「*」，則裝置上不適用「拒絕的網域」設定。

4. 按一下 **+新增**以新增多個**擴充功能**。
5. 按**下一步**，確認發佈設定。

6. 選取其中一個發佈選項以設定 **Safari 擴充功能設定**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
7. 按一下**完成**。

Safari 設定

Ivanti Neurons for MDM 可讓您在受監督的 iOS 和 macOS 裝置上管理 Safari 設定。 管理員可以有效地管理標準瀏覽和私密瀏覽的 Safari 擴充功能。

適用於：

- iOS 26.0+、iPad 26.0+、macOS 26.0+、visionOS 26.0+ 測試版，直至 Ivanti Neurons for MDM 支援的最新發行版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取 **Safari 擴充功能和設定**組態。
3. 按一下 **Safari 設定**。
4. 依下表設定 **Safari 設定**的各項設定:

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
組態設定	選取下列其中一個選項以設定開始頁面類型: • **開始**: 使用預設開始頁面。 Safari 停用現有首頁。 • **首頁**: 使用指定的首頁 URL。 Safari 將此設定為首頁。 • **擴充功能**: 使用 Safari 擴充功能指定的頁面，其識別碼為 ExtensionIdentifier。 Safari 停用現有首頁。

5. 按**下一步**，確認發佈設定。
6. 選取其中一個發佈選項以設定 **Safari 設定**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
7. 按一下**完成**。

Safari 隱私權設定

Safari 隱私權設定允許管理員使用宣告裝置管理 (DDM) 為 Safari 中的特定網站定義預設相機和麥克風權限。 功能可協助組織集中管理網站隱私權限，並在受管理的 Apple 裝置上提供更一致的瀏覽體驗。

適用於：

- iOS 27.0+ 和 macOS 27.0+，直至 Ivanti Neurons for MDM 支援的最新發佈版本。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取 **Safari 擴充功能和設定**組態。
3. 按一下 **Safari 隱私權設定**。
4. 依下表設定 **Safari 隱私權設定**的各項設定:

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。

組態設定	• **新增 URL**: 輸入 URL 以套用設定。
	• **+新增預設值**: 指定要套用在此設定的預設值。
	  ◦ 相機 - 允許/拒絕
	  ◦ 麥克風 - 允許/拒絕
	  ◦ 組織理由 (必填)

5. 按**下一步**，確認發佈設定。
6. 選取其中一個發佈選項以設定 **Safari 設定**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
7. 按一下**完成**。

10.10.8.30. Samsung 手機限制配置

配置

「Samsung 手機限制配置」可讓您設定 Samsung 裝置上的通話限制和例外狀況。 這些限制用來約束使用者可以撥打或接聽的電話號碼。

適用於：所有執行 Knox SDK 2.0+ 的 Samsung 裝置。

若要設定 Samsung 手機限制：

1. 在**配置**索引標籤中按一下 **+新增**。
2. 選擇 **Samsung 手機限制**配置。 隨即顯示 **Samsung 手機限制配置**頁面。
3. 在**名稱**欄位中，輸入適當的配置名稱。
4. 按一下 **+新增描述**連結，以新增配置描述。此欄位為選用。
5. 在**配置設置**區段中，設定下列選項：

   選項

   描述

   來電

   封鎖的號碼

   按一下「新增」圖示以新增號碼，按一下 Java 規則運算式以定義來電限制。

   列入允許清單的個數

   按一下「新增」圖示以新增號碼，按一下 Java 規則運算式以定義大型來電封鎖號碼集以外的允許號碼。

   如果沒有任何封鎖號碼，則此選項沒有任何效果。

   外撥電話

   封鎖的號碼

   按一下「新增」圖示以新增號碼，按一下 Java 規則運算式以定義外撥電話限制。

   列入允許清單的個數

   按一下「新增」圖示以新增號碼，按一下 Java 規則運算式以定義大型外撥電話封鎖號碼集以外的允許號碼。

   如果沒有任何封鎖號碼，則此選項沒有任何效果。
6. 按一下**完成**，將設定發佈至所選裝置。

> 裝置遭淘汰時，將移除裝置上的所有通話限制。

如需更多資訊，請參閱如何建立配置。

10.10.8.31. 預設瀏覽器組態 - iOS 和 visionOS

變更 iOS 和 visionOS 裝置上預設應用程式設定的組態。

必要條件

- 僅適用於 iOS (18.2+) 和 visionOS 2.2 版本。
- 這些應用程式在 iOS 裝置上的**設定** - **應用程式** - **預設應用程式**中設定。

程序

1. 在**裝置**頁面中，註冊 iOS (18.2+) 裝置或 visionOS 2.2 裝置。
2. 導覽至**組態** > **新增組態** > **預設應用程式設定**以設定 iOS 裝置上的預設瀏覽器。
3. 按一下**組態** > **建立設定** > **建立預設應用程式設定組態**
4. 在組態詳細資訊區段下方，提供**名稱**和**描述**資訊。
5. 在「組置設定 > 新增應用程式 > 透過尋找新增」下方，搜尋所想要的瀏覽器。 瀏覽器清單隨即顯示。
6. 從清單中選取想要的瀏覽器。
7. 在**建立預設應用程式設定組態**頁面，按一下**自訂**以將組態分發給特定裝置或裝置群組，或使用者或使用者群組。
8. 在**選擇這些自訂分發選項之一**下方，選取想要的選項來指定將此組態分發給使用者/使用者群組，還是裝置/裝置群組。
9. 在**全部可用**下方選取想要的選項以分發此組態。
10. 按一下**完成**。

10.10.8.32. 螢幕共用主機設定組態

螢幕共用主機設定組態使管理員能夠使用 Ivanti Neurons for MDM 安全地控制跨受管理裝置的 macOS 熒幕共用功能。 此功能允許指定授權使用者、驗證方式和服務限制，以確保相容和安全的遠端存取。

適用於: macOS 14.0 到 Ivanti Neurons for MDM 所支援的最新發行版本。

在您開始之前: 為了無縫整合**螢幕共用主機設定組態**組態，必須在其裝置上啟用「**遠端管理**」。 在您的裝置中，轉到**設定** > **遠端管理** > **啟用遠端管理**。

程序

1. 前往**配置** > **+新增**。
2. 搜尋並選取**螢幕共用主機設定組態**組態。
3. 依下表設定**螢幕共用主機設定**的各項設定:

設定	描述
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
連接埠基準	輸入連接到主機的初始 UDP 連接埠號。 熒幕共用需要多個連線，因此系統會為每個額外的連線將此值遞增 1。 這不會改變系統最初用於與主機建立連線的連接埠號，該連接埠號始終是 TCP 連接埠 5900。 **最小連接埠基準值**: 1024 **最大連接埠基準值**: 65535
最大虛擬顯示數	您最多可以使用兩個虛擬顯示器。
防止從主機複製檔案	選中核取方塊以防止使用者將檔案複製到熒幕共用主機。
防止將檔案複製到主機	選中核取方塊以防止使用者將檔案複製到熒幕共用主機。
防止高性能連線	選中該核取方塊可防止使用者與主機建立高性能連線。

4. 按**下一步**，確認發佈設定。
5. 選取其中一個發佈選項以設定**螢幕共用主機設定**組態。 如需有關設定發佈選項的詳細資訊，請參閱使用配置。
6. 按一下**完成**。

10.10.8.33. 單一 App 模式配置

配置

授權： Silver

單一 app 模式可限制 iOS 裝置使用指定的 app。 例如，您可以限制裝置只能使用貴組織開發的自訂 app。

單一 App 模式配置

設定	方法
名稱	輸入可識別此配置的名稱。
描述	輸入可說明此配置用途的描述。
選擇 App	選擇用來選擇 app 的方法： • **從應用程式目錄與系統應用程式：**選擇以搜尋 Ivanti Neurons for MDM 應用程式目錄與系統應用程式 (依預設預先安裝在 Apple 裝置上)。 • 輸入 app 的名稱，並在其顯示於 app 清單時選擇它。 • **輸入組合 ID:** 選擇此項以針對要選擇的系統應用程式輸入唯一識別碼。 如果您使用**從 App Catalog 與系統 App** 選項時找不到系統 app，請使用此選項。
停用觸控	選擇停用觸控畫面。
停用裝置的螢幕旋轉	選擇停用裝置的旋轉感應。
停用音量按鈕	選擇停用裝置的音量按鈕。
停用鈴聲轉換	選擇停用裝置的鈴聲轉換。
停用睡眠/喚醒按鈕	選擇停用裝置的睡眠/喚醒按鈕 (裝置邊緣右上角)。
停用自動鎖定螢幕	選擇不讓裝置在閒置期間後進入睡眠狀態。
啟用語音輔助	選擇啟用 VoiceOver 螢幕閱讀器 (輔助功能)。
啟用縮放	選擇啟用縮放 (輔助功能)。
啟用反轉顏色	選擇啟用反轉顏色調整 (輔助功能)。
啟用觸控助理	選擇啟用 AssistiveTouch (輔助功能)。
啟用朗讀選項	選擇啟用朗讀選項 (輔助功能)。
啟用單耳機功能	選擇從立體聲切換至單耳機功能 (輔助功能)。
語音輔助調整	選擇允許裝置使用者調整 VoiceOver。
縮放調整	選擇允許裝置使用者調整縮放。
反轉顏色調整	選擇允許裝置使用者反轉顏色。
觸控助理調整	選擇允許裝置使用者調整 AssistiveTouch。

如需更多資訊，請參閱如何建立配置。

10.10.8.34. 軟體更新建議頻率配置

管理員可以選擇允許使用者檢視裝置並將裝置更新至最高編號 (最新) 版本及/或較低編號 (最舊) 版本。

適用於：iOS 和 iPadOS 14.5 至 26.0 (受監管)

程序

1. 前往配置 > +新增。
2. 在搜尋欄位中輸入軟體更新建議，然後按一下軟體更新建議頻率配置。
3. 輸入配置的名稱和描述。
4. 從下拉清單中選擇所需的配置設定：
    - 顯示兩個軟體更新版本
    - 顯示較低版本 (最舊) 軟體更新版本
    - 僅顯示最高版本 (最新) 軟體更新版本
5. 按下一步。
6. 選擇啟用此配置選項。
7. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂。
8. 按一下完成。

10.10.8.35. 開始功能表和工作列

您可以定義開始功能表版面配置，讓您的使用者定義可安全使用的應用程式，並移除不需要的應用程式。 Windows 10 與 11 版本支援不同的功能，因為開始功能表版面配置有所不同。

若要設定開始功能表和工作列組態:

1. 前往**配置 > +新增**。
2. 選擇 **Windows 開始功能表和工作列**配置。
3. 輸入配置的名稱。
4. 選取 Windows 特定版本。
5. **Windows 10 裝置**:
   在**配置設置**區段中，設置下列設定：
   設定
   方法
   名稱
   輸入可識別此配置的名稱。
   描述
   輸入可說明此配置用途的描述。**選擇標準裝置**
   選擇已在其開始功能表和工作列中佈建應用程式的 Windows 10 裝置。
6. 按一下**從裝置擷取開始功能表版面配置**，然後設定下列選項。
7. **設定**
   方法開始功能表和工作列版面配置
   選擇下列其中一個 app 清單隱藏選項。
   - 無
   - 隱藏所有 app 清單
   - 隱藏所有 app 清單，並停用「設定」app 中的「在開始功能表中顯示 app 清單」
   - 隱藏所有 app 清單、移除所有 app 按鈕，並停用「設定」app 中的「在開始功能表中顯示 app 清單」

開始功能表版面配置自訂開始功能表
按一下**是**，自訂開始功能表和版面配置參數。**工作列自訂工作列**按一下**是**，以自訂工作列**先移除現有已釘選的工作列捷徑，然後再新增自訂工作列捷徑**按一下**是**，先移除現有已釘選的工作列捷徑，然後再新增自訂工作列。**App 類型**指定 app 的類型。**應用程式**輸入 app 的 ID。**還原**
按一下**還原**連結，可從原始 Golden 裝置工作列還原工作列。
按一下並拖曳列中的箭頭圖示，可以移動 (上移或下移) 指定列的位置。
按一下刪除圖示即可刪除列。
按一下**新增**按鈕以新增列。

8. **Windows 11 裝置**
   在**配置設置**區段中，設置下列設定：
   設定
   方法
   名稱
   輸入可識別此配置的名稱。
   描述
   輸入可說明此配置用途的描述。**選擇標準裝置**

選擇已將應用程式設定在其開始功能表的「已釘選」區段的 Windows 11 裝置。**開始功能表和工作列版面配置開始功能表和工作列版面配置**

選取下列其中一個選項以檢視工作列中的搜尋選項:

- **隱藏**
- **搜尋圖示**
- **搜尋圖示和標籤**
- **搜尋方塊 (預設)**

選取核取方塊**隱藏工作檢視**以隱藏工作檢視。**最常用的應用程式**

選取以下選項之一來設定「開始」功能表中最常用的應用程式:

- **不強制在「開始」中顯示最常用的應用程式清單。**
- **強制在「開始」中顯示最常用的應用程式清單。**
- **強制在「開始」中隱藏最常用的應用程式清單。**

核取方塊**允許釘選到工作列**預設為選取。

選取核取方塊**隱藏建議的區段**以隱藏所有建議的區段。

由於廠商問題，即使使用者登出或登入後，**隱藏建議的區段**核取方塊也不會在裝置上產生可見的作用。 目前，您無法隱藏建議的區段。**工作列 App 類型**

選取下列其中一個選項以指定應用程式類型:

- **應用程式使用者型號 ID**
- **桌面應用程式連結路徑**

應用程式指定應用程式的 ID 或路徑。**還原**

按一下**還原**連結，可從原始 Golden 裝置工作列還原工作列。

按一下並拖曳列中的箭頭圖示，可以移動 (上移或下移) 指定列的位置。

按一下刪除圖示即可刪除列。

按一下**新增**按鈕以新增列。

9. 按一下**從裝置擷取開始功能表版面配置**。
10. 從 Golden 裝置擷取設定後，所有設定在開始功能表「已釘選」區段內的應用程式將顯示，以供管理員檢閱。

    按一下**下一步**並發佈組態到所有適用的裝置與使用者群組。

> 由於供應商問題，未發佈組態時，已釘選的應用程式將保持原本設定。 然而，當發佈新組態時，便會覆蓋先前的版面配置，然後套用新的版面配置。

10.10.8.36. 系統更新組態

管理員可以限制裝置使用者，使其無法管理 Android 6.0 裝置或支援的較新版本上的系統更新。 此功能僅適用於 Android Enterprise 裝置。

如要配置：

1. 前往**配置 > +新增**。
2. 選擇**系統更新**配置。
3. 輸入配置的名稱。
4. 輸入描述。
5. 在「配置設置」區段中，設定下列選項：

設定	描述
自動	在有新的韌體可用時，無訊息自動套用系統更新。
延後	將系統更新安裝延後 30 天。 30 天後，系統會提示裝置使用者安裝更新。
具範圍限制 (當地時間)	排程一段時間以無訊息自動套用系統更新。 選擇時數的**開始時間**與**結束時間**。
手動作業系統更新 (Android 10+) Samsung 和 Zebra 裝置不適用或不支援	選取此項可在所有裝置上推出更新之前，對有限數量的裝置手動執行作業系統更新。 **韌體檔案** - 選取**自訂屬性**或 **HTTPS URL** 選項。 輸入下列詳細資訊: • 韌體位置 - 如果您已選取**自訂屬性**作為韌體檔案選項，則需提供用於檔案傳輸的自訂屬性。 韌體檔案可以自我裝載，或使用檔案傳輸組態上傳到 Ivanti Neurons for MDM。 請參閱**檔案傳輸組態**了解詳細資訊。 若上傳至 Ivanti Neurons for MDM 的檔案大於 50 MB，則需有外掛程式授權。 • 說明 (選用) • 指紋 (強制) - 驗證裝置上是否安裝了所需的作業系統版本。 解壓縮 OTA 資料夾並開啟 /META-INF/com/android/metadata 檔案，即可在 OTA 檔案中找到指紋。 搜尋與以下所示類似的項目: "post-build=google/xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxxxx:user/release-keys" 在上方項目中，**google/ xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxx:user/release-keys** 是指紋，而 TQ3A.230805.001.S1 是組建 ID (組建 ID 是指紋中以 '/' 分隔的值中左邊起算的第 4 個值)。 • 總和檢查碼 (選用) **更新設定 → 作業系統更新請求** - 此區段內的設定與 Zebra 韌體組態相同。 請參閱此表中的 *Zebra 韌體組態*區段。 如果您選取 **HTTPS URL** 作為韌體檔案選項，則需提供以下資訊: • 韌體位置 - 輸入不需任何驗證即可下載韌體的路徑。 說明 (選用) • 指紋 (強制) - 驗證裝置上是否安裝了所需的作業系統版本。 • 總和檢查碼 (選用) 除了「**作業系統更新請求**」區段之外，還有**起始下載要求**和**下載期間的條件**區段。 **起始下載要求**和**下載期間的條件**區段下可用的選項相同，因為兩者都在 **Zebra 韌體組態**區段下。 下載後在裝置中開始進行系統更新時，在兩次更新之間重新啟動裝置會中止更新程序。
凍結期間	在一段指定期間內凍結系統更新。 此選項僅適用於 Android 9.0+ 裝置。 按一下**新增凍結期間**。 選擇凍結期間的**開始日期**與**結束日期**。 凍結期間不能超過 90 天，您可以新增多個凍結期間。 下個凍結期間可以選在前一個日曆結束日期起算的 60 天後。 若要刪除凍結期間，請按一下「刪除」圖示。
Zebra 韌體配置	選擇**設定 Zebra OTA** 以升級或更新 Zebra 裝置的作業韌體 (在 Android 第 8.0 版到支援的更新版本)。 這僅適用於「裝置擁有者」模式。 如要設定 Zebra OTA 更新，您必須在**管理員 > 韌體管理 > Zebra OTA** 之下啟用 Ivanti Neurons for MDM OTA 服務，且 Zebra 裝置必須已存在於 Ivanti Neurons for MDM 上。 您必須在快顯視窗中輸入您的 Zebra 憑證。 如要建立您自己的憑證，請直接聯絡 Zebra。

設定	描述
	選取此選項時，即會顯示已註冊的 Zebra 裝置清單。 若要選取韌體並將其套用至裝置機型： 1. 在 Zebra 裝置的**動作**欄中，執行以下任一項動作： ◦ **無**：將不會對該裝置機型執行任何動作。 ◦ **完整升級**。 在**選擇目標 Zebra 韌體**視窗中，選擇要套用至該裝置機型的完整升級韌體版本。 在**完整升級**程序期間，僅需要連接埠 443。 在**搜尋**欄位中，您可以輸入組建 ID 的名稱字元，根據組建 ID 來搜尋升級。 組建 ID 會依遞減順序 (最新的在最上方) 排序和顯示。 **修補程式升級**選項將**不**適用於 Android 11 以上版本的裝置。 2. 設定下列任一選項: **起始下載要求** - Go app 將評估這些條件。 ◦ **所需最低電池電量**: 移動滑桿，在可用範圍內設定所需的最低電池電量。 ◦ **要求裝置進行充電**: 選取此選項，讓裝置在此程序中維持充電模式。 ◦ **下載排程**: 選取此選項，建立排程以起始下載要求和檔案下載。 ◦ **需要裝置閒置**、**需要充電**和**允許透過按流量計費的網路下載** 將傳遞至 Android Download Manager。 Go app 將在所提到的視窗中，使用上述參數將下載要求新增至 Android Download Manager。 **套用下載的排程** - 選取**星期**、**開始時間**和**結束時間**，以排程下載。 您可以選取多個天數，以排程下載。 例如，如果您選取星期六和星期日，開始時間和結束時間介於上午 12:00 到下午 11:00，則 Zebra 裝置只會在選取天數的這段期間執行下載。 在 Go app 中，當組態套用於裝置時，下載將按照排程開始。 下載無結束時間限制，可能會在排定的結束時間之後才完成。 ◦ 套用更新的排程 - 選取**星期**、**開始時間**和**結束時間**，排定安裝韌體更新的時程。 如果裝置的電池電力低於 32，將會暫停安裝。 如果未設定更新排程，將會在韌體下載完成後立即開始安裝。 3. 設定下列任一選項: **下載期間的條件** - Download Manager 將評估這些條件。 您可以根據準則進行選擇。 ◦ **要求裝置閒置時** (預設為已選取)：允許當裝置閒置時更新韌體。 ◦ **要求充電時** (預設為已選取)：允許當裝置在充電模式下更新韌體。 ◦ **允許透過按流量計費的網路下載**: 選擇此選項以允許在 Wi-Fi 模式中下載。 此選項預設為取消選取。 ◦ **需要裝置閒置**、**需要充電**和**允許透過按流量計費的網路下載** 將傳遞至 Android Download Manager。 Go app 將在所提到的視窗中，使用上述參數將下載要求新增至 Android Download Manager。 **允許在指定的「下載排程」之外繼續下載**: 選取此選項，允許在指定的下載排程之外下載。 **作業系統更新請求** ◦ **所需的最低電池電量** - 選取此選項可設定請求作業系統更新時必須達到的最低電池電量。 ◦ **要求裝置進行充電** - 選取此選項可讓裝置在此程序中維持充電模式。 ◦ **建立排程以在裝置上啟動作業系統更新** - 選取此選項可設定在裝置上啟動作業系統更新的排程。 在 Go app 中，當組態套用於裝置時，下載將按照排程開始。 下載無結束時間限制，可能會在排定的結束時間之後才完成。 按一下**套用**。

設定	描述
Samsung e-FOTA 配置	選擇**設定 Samsung E-FOTA** 以升級或更新 Samsung 裝置的作業韌體（在 Knox 2.7.1 版和更新版本）。 這僅適用於搭配公司擁有裝置上的工作描述檔之受管理裝置模式。 如果未註冊具 Samsung E-FOTA 功能的裝置，在此頁面上會顯示通知此資訊的訊息。 若要設定 Samsung e-FOTA 更新，必須在**管理 > 韌體管理 > Samsung E-FOTA** 下啟用 Samsung e-FOTA 授權。 選取此選項後，已註冊的 Samsung 裝置清單隨即顯示。 若要選取韌體並將其套用至裝置機型： 1. 在 Samsung 裝置的**動作**欄中，執行以下任一項動作： ◦ **最新：**已套用的最新韌體版本。 此選項預設為已選取。 ◦ **強制：**在「選擇目標 Samsung 韌體」視窗中，選擇要強制套用至裝置機型的特定韌體版本（無需使用者操作）。 當執行此動作時，會在 15 分鐘內開始下載韌體。 ◦ **目標：**在「選擇目標 Samsung 韌體」視窗中，選擇要套用至裝置機型的特定韌體版本（無需使用者操作）。 執行「強制」或「目標」動作時，如果未列出適用該裝置的韌體，在此頁面上會顯示通知此資訊的訊息。 2. **啟用韌體偵錯** (選用)：當**啟用韌體偵錯**選項啟用時，會套用此配置，並將裝置升級至虛設韌體。 Samsung 裝置韌體的虛設韌體可允許管理員在裝置上測試系統更新配置行為，而不會實際修改裝置上的任何東西。 若要升級至實際的韌體更新而非虛擬韌體，管理員應先確定**啟用韌體偵錯**選項已停用，然後再套用組態 3. 按一下**套用**。

6. 按**下一步**。
7. 請選擇下列發佈選項之一：

- 所有裝置
- 沒有裝置 (預設)
- 自訂

8. 按一下**完成**。

Samsung E-FOTA 組態 (已停用)

Samsung E-FOTA 組態已於 2022 年 7 月停用。 因此，此組態將無法供新裝置使用。 現在具有該組態的裝置僅可停用此組態。

10.10.8.37. Windows 10 更新管理

以管理員身分，可以使用「Windows 10 更新管理」檢視及批准要更新的 Windows 10 裝置所回報的更新。 您可使用此功能來防止在裝置上安裝不必要或未經測試的更新。

「更新管理」功能要求透過啟用了**需要更新核准**選項的**軟體更新**組態設定裝置。 唯有將此配置套月到裝置上，裝置才會報告待安裝的更新並等待核准。

管理更新

1. 前往**管理員 > Windows > Windows Update**。 頁面上會顯示更新的下列詳細資料。
   建立日期：建立更新的日期。**標題**：描述更新類型與知識庫文章編號。

> 按一下更新時，隨即顯示此描述。

分類: 將更新類型分為以下類別之一:

- 重要更新
- 定義更新
- 驅動程式更新
- 安全性更新
- 更新
- 升級
- 更新彙總

發佈：針對更新所執行的發佈。 例如，當更新要發佈給所有裝置時，它便會顯示**所有**。

> 如果更新要發佈給特定數目的群組，它便會顯示發佈計數。 例如，只針對 3 個群組執行發佈，則它會顯示 3。

2. 此外，您可以檢視更新是否已發佈至必要的裝置。 下列欄位的數字表示存在於不同更新類別中的裝置數目:
   - 合格的裝置
   - 已安裝的裝置
   - 安裝失敗的裝置
   - 重新啟動擱置中裝置

當您按一下任何數字時，您將被導向至「裝置」頁面中的篩選檢視以瞭解更新狀態，並執行必要動作。
檢閱更新，然後按一下更新的勾選方塊，藉此選擇您想發佈到裝置上的更新。

3. 在**動作**下，按一下**設定發佈**。
4. 在**發佈 Windows 更新**視窗中，選擇下列發佈選項之一：
   所有裝置：發佈更新到所有裝置。
   無裝置：暫停發佈更新到裝置。**自訂**：發佈更新到指定裝置群組。
5. 按一下**儲存**。

搜尋與篩選更新

您可以根據以下條件搜尋與篩選更新：

- 知識庫文章 ID
- 設定的發佈

根據知識庫文章 ID 進行篩選：

1. 在 **Windows 10 更新管理**頁面中，請在快速搜尋欄位中鍵入知識庫 ID (搜尋欄中只有數字)。
   範例：若是 KB4056892，請輸入 4056892。 頁面上隨即顯示符合搜尋條件的更新。

> 您可以按一下**支援**和**更多資訊**連結，藉此進一步搜尋其他資訊。 Microsoft 網頁的**支援**連結針對更新提供產品支援資訊，Microsoft 網頁的**更多資訊**連結則針對更新顯示更多資訊，例如知識庫文章。

根據所設定的發佈進行篩選：

在 **Windows 10 更新管理**頁面中，根據設定的發佈，選取下列任何一個篩選選項:

- **所有**：顯示所有更新。
- **已設定**：顯示要發佈到裝置上的更新清單。
- **未設定**：顯示在發佈中未指定的更新清單。

> 「已設定」和「未設定」的篩選器根據所執行的發佈，發佈也可以是**無**。

檢視裝置的更新

若要檢視裝置特有的詳細更新資訊：

1. 前往**裝置 > 裝置**。
2. 按一下裝置名稱，以檢視詳細資料頁面。
3. 前往**更新**索引標籤。 隨即顯示擱置中 (管理員已核准但尚未回報已在裝置上安裝)、失敗與已安裝的裝置更新。

> 您也可以透「儀表板」下的「通知」頁面，查看是否有新的 Windows 更新可用。 通知內容包含通知的建立日期、可用通知數目，以及通知目的。 在管理入口網站的右上角也可以看到 Windows 更新通知。

10.10.8.38. Windows app 排程

Windows Desktop app 可能會很大，結果在企業的主要使用時間造成額外與擴展的網路和伺服器負荷。 Windows app 排程功能可讓您安排在裝置上安裝 app 的選定時間，特別是大型 app。

若要設定 app 排程：

1. 前往 **App > 應用程式目錄**。
2. 按一下**新增**，然後選取一個 Windows 應用程式，繼續執行**新增應用程式**精靈中的後續步驟。
3. 在步驟 5 (設定) 中，按一下**安裝應用程式組態設定**以檢視**組態設定**頁面。
4. 選取**排程安裝**核取方塊。

> **排程安裝**勾選框只會在啟用無訊息自動安裝時顯示。

5. 選擇**開始時間**和**結束時間**以排程 app 的安裝時間。
6. 選取**開始日期**和**結束日期**以安排安裝應用程式的日期。

> 您也可以選取以下兩個動作之一，以便在錯過已排程日期時執行相關動作: **在下次簽入期間安裝**或**不安裝**。

7. 選取一個應用程式組態發佈選項: **使用應用程式的每個人**、**一律不**或**自訂**。
8. 按一下**完成**。

> 需要排程的 App 不應加入 Apps@Work。
> App 排程不適用於 Store app，因為不支援無訊息自動安裝 Store app。

10.10.8.39. Windows BIOS 配置

管理員可以在 Lenovo 裝置上設置 Windows BIOS 設定。 必須先註冊至少一個支援 BIOS 設定的 Lenovo 裝置，才能設定此配置。

如要配置：

1. 前往**配置 > +新增**。
2. 選擇 **Windows BIOS** 配置。
3. 輸入配置的名稱。
4. 輸入描述。
5. 在「選擇裝置模式」區段中，從下拉式清單中選擇裝置模式。
6. 在「配置設置」區段中，設定下列選項：

> 設定清單因註冊的特定裝置機型的可用內容而異。 有關更多資訊，請參閱相應裝置的網站。

設定	方法
AMT 控制	請選擇下列任何選項： • **停用** • **啟用**
自適應溫度管理 AC	請選擇下列任何選項： • **平衡** • **最大效能**
自適應溫度管理電池	請選擇下列任何選項： • **平衡** • **最大效能**
永遠於 USB 上	請選擇下列任何選項： • **停用** • **啟用**
BIOSPasswordAtBootDeviceList	請選擇下列任何選項： • **停用** • **啟用**
重新啟動需要 Bios 密碼	請選擇下列任何選項： • **停用** • **啟用**
無人重新啟動需要 Bios 密碼	請選擇下列任何選項： • **停用** • **啟用**
遠端用戶 Bios 更新	請選擇下列任何選項： • **停用** • **啟用**
Bluetooth 存取權	請選擇下列任何選項： • **停用** • **啟用**
啟動裝置列出 F12 選項	請選擇下列任何選項： • **停用** • **啟用**

設定	方法
啟動顯示裝置	請選擇下列任何選項： • **DisplayPort** • **顯示底座** • **HDMI** • **LCD**
啟動模式	請選擇下列任何選項： • **診斷** • **快速**
啟動模式鎖定	請選擇下列任何選項： • **停用** • **啟用**
BootTimeExtension	請選擇下列任何選項： • **1** • **10** • **2** • **3** • **5** • **停用**
BottomCover 篡改偵測	請選擇下列任何選項： • **停用** • **啟用**
CPU 電源管理	請選擇下列任何選項： • **自動** • **停用**
Computrace 模組啟動	請選擇下列任何選項： • **停用** • **啟用**
資料執行防護	請選擇下列任何選項： • **停用** • **啟用**
乙太網 LAN 存取	請選擇下列任何選項： • **停用** • **啟用**
乙太網 LAN 選項 ROM	請選擇下列任何選項： • **停用**

設定	方法
	• **啟用**
指紋密碼驗證	請選擇下列任何選項： • **停用** • **啟用**
指紋桌面前驗證	請選擇下列任何選項： • **停用** • **啟用**
指紋識別器存取	請選擇下列任何選項： • **停用** • **啟用**
指紋識別器優先順序	請選擇下列任何選項： • **外部** • **限內部**
指紋安全模式	請選擇下列任何選項： • **高** • **一般**
Fn Ctrl 鍵切換	請選擇下列任何選項： • **停用** • **啟用**
FnKeyAsPrimary	請選擇下列任何選項： • **停用** • **啟用**
FnSticky	請選擇下列任何選項： • **停用** • **啟用**
Ipv4 網路堆疊	請選擇下列任何選項： • **停用** • **啟用**
Ipv4 網路堆疊	請選擇下列任何選項： • **停用** • **啟用**
內建相機存取	請選擇下列任何選項： • **停用** • **啟用**

設定	方法
InternalStorageTamper	請選擇下列任何選項： • **停用** • **啟用**
鍵盤嗶聲	請選擇下列任何選項： • **停用** • **啟用**
鎖定 BIOS 設定	請選擇下列任何選項： • **停用** • **啟用**
記憶卡槽存取	請選擇下列任何選項： • **停用** • **啟用**
麥克風存取	請選擇下列任何選項： • **停用** • **啟用**
密碼長度下限	請選擇下列任何選項： • 4 • 5 • 6 • 7 • 8 • 9 • 10 • 11 • 12 • **停用**
NFFControl	請選擇下列任何選項： • **停用** • **啟用**
Nfc 存取權	請選擇下列任何選項： • **停用** • **啟用**
Ac Attach 開機	請選擇下列任何選項： • **停用** • **啟用**

設定	方法
PasswordBeep	請選擇下列任何選項： • **停用** • **啟用**
PasswordCountExceededError	請選擇下列任何選項： • **停用** • **啟用**
清除 Tpm 的 Physical Presence	請選擇下列任何選項： • **停用** • **啟用**
設置 Tpm 的 Physical Presence	請選擇下列任何選項： • **停用** • **啟用**
Rapid Start 技術	請選擇下列任何選項： • **停用** • **啟用**
安全啟動	選擇**啟用**
安全恢復防護	請選擇下列任何選項： • **停用** • **啟用**
安全晶片	請選擇下列任何選項： • **作用中** • **停用** • **啟用** • **非使用中**
智慧卡槽存取權	請選擇下列任何選項： • **停用** • **啟用**
SpeedStep	請選擇下列任何選項： • **停用** • **啟用**
啟動選項鍵	請選擇下列任何選項： • **停用** • **啟用**
TXT 功能	請選擇下列任何選項：

設定	方法
	• **停用** • **啟用**
總圖像記憶體	請選擇下列任何選項： • **256MB** • **512MB**
觸控板	請選擇下列任何選項： • **自動** • **停用**
TrackPoint	請選擇下列任何選項： • **自動** • **停用**
USB30 模式	請選擇下列任何選項： • **自動** • **停用** • **啟用**
USB BIOS 支援	請選擇下列任何選項： • **停用** • **啟用**
USB 埠存取權	請選擇下列任何選項： • **停用** • **啟用**
Uefi Pxe 啟動優先順序	請選擇下列任何選項： • **Ipv4 優先** • **IPv6 優先**
VTd 功能	請選擇下列任何選項： • **停用** • **啟用**
虛擬化技術	請選擇下列任何選項： • **停用** • **啟用**

設定	方法
LAN 喚醒	請選擇下列任何選項： • **限 AC** • **AC 與電池** • **停用** • **啟用**
無線 LAN 存取權	請選擇下列任何選項： • **停用** • **啟用**
無線 WAN 存取權	請選擇下列任何選項： • **停用** • **啟用**

7. 按**下一步**。
8. 請選擇下列發佈選項之一：
   - 所有裝置
   - 沒有裝置 (預設)
   - 自訂
9. 按一下**完成**。

10.10.8.40. Windows BitLocker

身為管理員，您可以透過上傳包含裝置 GUID 和復原密碼的 Excel 檔案，大量更新一組加密 Windows 10 裝置的復原金鑰。

如要上傳 Excel 檔案以大量更新復原金鑰：

1. 前往**管理員 > Windows BitLocker**。
2. 按一下**下載範例 csv 檔案**，以下載範例 csv 檔案並檢視 .csv 檔案範例。
3. 建立和新增 BitLocker 復原金鑰 .csv 檔案的記錄。
4. 按一下**上傳復原密碼**
5. 按一下**選擇檔案**以上傳您建立的 .csv 檔案。
6. 按一下**上傳**。 使用之前上傳的金鑰上傳新檔案將會覆寫舊項目。

> 每次上傳最多可提交 1,000 筆記錄。 上傳成功後，您可以檢視特定裝置的裝置詳細資料中之個別金鑰。

10.10.8.41. Windows 單一應用配置

您可以在 Windows 10 裝置上，使用 Windows 單一應用配置來設定單一或多個 app 單一應用。 套用此配置之後，即可限制單一應用使用者存取單一應用 app 以外的任何功能。 此配置需要啟用 Windows Bridge。

在下列 3 種模式中可套用此配置。

- 單一應用模式
- 多個應用模式 (擷取 Windows 裝置的應用程式清單)
- 多個應用模式 (從開始功能表配置選擇現有的版面配置)

> 在進入所配置的 Windows 單一應用模式之前，裝置上還應該安裝供 Windows 單一應用模式使用的應用程式。

若要設定 Windows 單一應用配置：

1. 前往**配置 > +新增**。
2. 選擇 **Windows 單一應用**配置。
3. 輸入配置的名稱。
4. 輸入描述。
5. 在「配置設定」區段中，按照下表所述指定其餘設定。

設定	方法
選擇單一應用模式：選擇下列 3 種選項之一。	
單一應用模式	選擇此選項可為裝置設定單一應用模式。 1. 在**選擇 Windows 裝置 (選用)** 區段中，選擇 Windows 10 裝置。 按一下**擷取裝置的 App**，以擷取裝置的 app 清單。您選擇的裝置應該在您的監管之下，而且需要登記才能成功擷取 app 資料。 若要略過這些步驟，請選擇**略過此步驟。 您可以稍後視需要變更**勾選框。 2. 按一下**從擷取的 App 清單新增**，可從所擷取的清單新增 app。 3. 按一下 app 的**名稱**欄位中的選項按鈕，藉此選擇單一 app。 按一下**新增**可為清單新增 app。 若要從清單刪除 app，按一下「刪除」圖示。
多個應用模式 (擷取 Windows 裝置的應用程式清單)	選擇此選項可為裝置設定多個應用模式。 1. 在**選擇 Windows 裝置 (選用)** 區段中，選擇 Windows 10 裝置。 按一下**擷取裝置的 App**，可擷取裝置的 app 清單。 您選擇的裝置應該在您的監管之下，而且需要登記才能成功擷取 app 資料。 若要略過這些步驟，請選擇**略過此步驟。 您可以稍後視需要變更**勾選框。 2. 在**單一應用 App 與開始功能表版面配置**中，按一下**從擷取的 App 清單新增**。 **選擇單一應用 App** 視窗隨即顯示。 從擷取的清單選擇 app，然後按一下**使用所選的 App**。 3. 在「其他允許的應用程式」區段中，按一下**從擷取的應用程式清單新增**。 **選擇單一應用 App** 視窗隨即顯示。 從擷取的清單選擇 app，然後按一下**使用所選的 App**。 其他允許的應用程式均被視同**「kiosk 應用程式」和「開始功能表版面配置」**中所選應用程式的相依項目。若沒有「允許的應用程式」，作業系統將不允許執行此應用程式，即使該應用程式圖示顯示在「開始」功能表中也是如此。 4. 按一下**新增**可為清單新增 app。若要從清單刪除 app，按一下「刪除」圖示。 您可以將清單中的 app 拖曳與移動到清單中的任何位置。 5. 在**多個 App 其他設定**中，選擇所需選項： ◦ **隱藏電源按鈕** ◦ **隱藏使用者磚** ◦ **隱藏工作列** 在 Microsoft Windows 11 中，不支援多應用程式 Kiosk 模式選項「**隱藏工作列**」。
多個應用模式 (從開始功能表配置選擇現有的版面配置)	如果您已建立「開始功能表版面配置」配置，您可以匯入該配置，然後藉由選擇此選項來設定多個應用模式。 1. 在**選擇版面配置**區段中，選擇之前已設為「開始功能表配置」的版面配置。 在下面的下拉式清單中隨即顯示包含適用版面配置參數的之前建立配置。 2. 在「多個 App 其他設定」中，選擇所需選項： ◦ **隱藏電源按鈕** ◦ **隱藏使用者磚** ◦ **隱藏工作列** 在 Microsoft Windows 11 中，不支援多應用程式 Kiosk 模式選項「**隱藏工作列**」。

6. 按**下一步**。
7. 請選擇下列發佈選項之一：

- 所有裝置

- 沒有裝置 (預設)
- 自訂

8. 按一下**完成**。

> 為了讓配置完整生效，裝置應在套用或更新 Windows 單一應用配置之後重新開機。視多個 app 單一應用配置的應用程式而定，可能需要再次執行裝置重新開機。 部分圖示可能會在第一次登入時遺失，但遺失的圖示將會在第二次重新開機後登入時顯示。

裝置必須在套用、刪除或更新單一應用配置後重新開機。 這可以透過裝置動作功能表的重新啟動/關機裝置命令。 如果未重新開機：

- 裝置在套用單一應用配置之後不會自動進入單一應用模式。
- 裝置在刪除所套用的單一應用配置之後不會自動退出單一應用模式。
- 裝置不會變更正在執行的單一應用配置。

如果已套用單一應用配置的裝置收到更新的配置，裝置上的 Windows 作業系統會移除現有的單一應用使用者，並使用新的單一應用配置來重新建立新的單一應用使用者。 目前使用者的工作階段應透過裝置重新開機明確結束。

多個 app 單一應用配置最好設定 .lnk 檔案，而單一 app 單一應用配置最好設定 .exe 檔案。 從裝置匯入的開始功能表配置使用 .lnk 格式。 手動為 .exe 應用程式建立的開始功能表項目有時可能不會顯示在依賴 .exe 應用程式之多個 app 單一應用配置的開始功能表。

例如，Windows Media Player 可使用下列其中一個 .lnk 檔案新增至開始功能表：

- %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Media Player.lnk
- %ALLUSERSPROFILE%\Microsoft\\Windows\Start Menu\Programs\Windows Media Player.lnk

如果此 app 直接使用下列其中任何一個 .exe 檔案來新增，將不會顯示對應的圖示，即使在上述的 .lnk 檔案內部使用第一個 .exe 路徑也一樣。

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
- C:\Program Files\Windows Media Player\wmplayer.exe

對於單一 app 單一應用配置，您可以在 exe 檔案中新增引數。 E.g. '%ProgramFiles%\Internet Explorer\iexplore.exe -k www.bing.com'。不過，內含引數之 exe app 的圖示無法顯示在多個 app 配置的開始功能表中。如果您的多個 app 單一應用配置中需要內含引數的 exe app，請使用可內含引數的 .lnk 檔案。 .lnk 在單一 app 單一應用配置中無法運作。

多個 app 單一應用配置中的相依項目

在多個 app 單一應用模式中，Win32/64 應用程式可能需要您在「其他允許的 App」區段中新增相依項目。 單一 app 單一應用模式不需要「其他允許的 App」。

範例 1：若是 Windows Media Player app，多個 app 單一應用模式需要下列相依項目：

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\setup_wm.exe

第一個相依項目是從對應 .lnk 檔案呼叫的 app 二進位檔。 第二個相依項目是從第一個相依項目呼叫的一次性精靈。

如果沒有「允許的 App」，作業系統不會允許執行此應用程式，即使應用程式圖示顯示在開始功能表中也一樣。

範例 2：若是 Internet Explorer，只要使用以下清單中的任何項目來設定它，其圖示便會顯示在開始功表中：

- %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 需要下列相依項目：

- 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

第一個相依項目是 .lnk 項目需要的 app 二進位檔，其他相依項目則用於一次性精靈。 如果沒有第一個相依項目，作業系統會封鎖內含蹦現視窗的 app。 如果沒有其他相依項目，應用程式會在啟動後關閉而且作業系統不會發出其他通知。

10.10.8.42. Windows 授權配置

Windows 授權配置會升級裝置的作業系統，例如從 Windows 10 專業版升級至 Windows 10 企業版。 此外，此配置可讓您啟用或變更 Windows 10 10 Desktop 裝置的產品金鑰。

若要升級 Windows 授權：

1. 前往**配置 > +新增**。
2. 選擇 **Windows 授權**配置。
3. 輸入配置的名稱。
4. 在**配置設置**區段中，輸入 Windows **產品金鑰**。
5. 按**下一步**。
6. 請選擇下列發佈選項之一：
    - 所有裝置
    - 沒有裝置 (預設)
    - 自訂
7. 按一下**完成**。

11. 政策

政策用來定義裝置的規範，包括當裝置不符合規範時的處置原則。 每種原則都包含一項規則和相符性動作 (違反規則時的作法)。 使用**原則**頁面來選擇、設定與發佈原則。

> 使用自動裝置登記流程，請注意以下變更:

- 僅對過去 90 天內登記的裝置進行評估。
- 在 90 天後和一年前登記的裝置上，只會觸發強制登記指令。
- 對過去一年內未登記的裝置不採取任何動作。

本節包含以下各主題：

- 使用原則
- 自訂原則
- 監控與控制允許的 App
- 優先排序原則
- Windows 硬體原則

11.1. 使用原則

本節包含以下各主題：

- 實施原則
- 合規性動作
- 尋找現有的原則
- 新增原則
- 編輯原則
- 刪除原則

實施原則

政策用來定義裝置的規範，包括當裝置不符合規範時的處置原則。 每種原則都包含一項規則和相符性動作 (違反規則時的作法)。 使用**原則**頁面來選擇、設定與發佈原則。

以下為可用的原則類型：

類型	用途
受威脅的裝置	優先順序 (1 = 最高) 違規 1 外掛程式遭破解 2 用戶端遭竄改 3 未知的裝置製造商：未知 4 偵測到可疑的資料夾：[路徑] 5 找到可疑的二進位檔：[路徑] 6 /data 資料夾可供瀏覽，或者，/data/data 資料夾可供瀏覽 7 找到 /system/app/Superuser.apk 8 套件管理員遭破解 9 找到可疑的 app：[套件] 將已遭越獄 (iOS) 或 root (Android) 的裝置標示旗幟 若要檢視系統將 Android 裝置標幟為遭 Root 破解的違規原因： 1. 按一下**原則**索引標籤。 2. 按一下**受威脅的裝置**連結。 3. 按一下**目前的違規**索引標籤。 4. 查看「違規」欄位中的違規原因。 若要檢視系統將 Android 裝置標幟為遭 Root 破解的違規原因： 5. 按一下**原則**索引標籤。 6. 按一下**受威脅的裝置**連結。 7. 按一下**目前的違規**索引標籤。 8. 查看**違規**欄位中的違規原因。 原因應為下列其中之一：
資料保護/加密已停用 (僅限 macOS)	為沒有密碼或未啟用加密的 macOS 裝置標示旗幟。
國際漫遊	將可能產生國際漫遊費用的裝置標示旗幟。 當裝置登記時，就會重新整理狀態。 若是 iOS，裝置會使用 iOS 設定與報告的漫遊旗幟。 僅有第一次違規會觸發相符性動作。
停用 MDM / 裝置管理	如果裝置已停用 MDM，在進行登記期間將不會進一步執行任何其他原則評估，或者配置或 app 的差異處理。
失去聯絡	標記在指定時間間隔內與 Ivanti Neurons for MDM 失聯的裝置。 選擇當裝置在一段指定的時數或天數內 (2-3 到 23-24) 皆未登記時要採取的行動。
MI 用戶端失聯 (僅限 iOS)	標記在指定時間間隔內與 Ivanti Neurons for MDM 失聯的 Ivanti Neurons for MDM 用戶端。 選擇當用戶端在一段指定的時數或天數內 (2-3 到 23-24) 皆未登記時要採取的行動。 上述動作也適用於透過 iReg 註冊的裝置。 如果裝置不含用戶端或其用戶端未在指定期間內登記，則此原則會將該裝置標示為違規。
允許的 App	將違反允許或必要 app 之規則的裝置標示旗幟。
自訂原則	根據指定的條件和相關動作建立自訂原則。

合規性動作

以下是可用的合規性動作:

相符性動作	用途
監控	在 Ivanti Neurons for MDM 裝置頁面中標記裝置。 此動作預設為開啟。
封鎖	若上次簽入詳細資訊顯示某裝置違反策略，則之後嘗試透過 Sentry 或 Access 存取資源時，此合規性操作將指示 Access 和/或 Sentry 封鎖該裝置。

傳送訊息給使用者	• 在 Ivanti Neurons for MDM 裝置頁面中標記裝置。
	• 傳送電子郵件給裝置擁有者。
	• 除了現有原則之外，下列原則現在也可使用「**使用合規性原則電子郵件範本**」切換開關:
	  ◦ 資料保護/加密已停用
	  ◦ 國際漫遊
	  ◦ 停用 MDM / 裝置管理
	  ◦ 失去聯絡
	  ◦ MI 用戶端失聯
	傳送推送通知給裝置。

隔離	• 移除裝置大多數的配置。 ◦ 例外情況：密碼配置、Wi-Fi 配置 (僅可使用 Wi-Fi 的裝置)、限制配置 (iOS)。 • 移除 Ivanti Neurons for MDM 安裝的所有應用程式。 • 移除由 Ivanti Neurons for MDM 發佈的所有內容，包括 iBook 和 ePub 檔案。 • 封鎖對於 Ivanti Neurons for MDM 目錄的存取。 • 暫停安裝其他 app 的提示。 • 封鎖 AppConnect app 的存取。 • 包括支援 AppConnect app。 • 若開啟，暫停隔離裝置個人端上的個人 app，指出裝置使用者需要處理裝置違規問題，才能讓裝置正常運作。 支援在 Android 11+ 裝置上佈建為公司擁有裝置上的工作描述檔。
其他的隔離動作 (選用):	**封鎖新的應用程式下載** - 防止下載新應用程式至裝置。 **隔離受控應用程式** - 移除裝置上 Ivanti Neurons for MDM 管理的應用程式，並啟用「阻擋新應用程式下載」選項，以阻擋裝置重新安裝應用程式。 請選擇下列選項之一： • **所有應用程式** • **除下列項目外移除所有應用程式** - 移除已新增至應用程式清單中的應用程式之外的所有應用程式。 • **指定應用程式**- 藉由查閱或手動 (使用套件 ID 或套件名稱)。 按一下**檢視 App** 索引標籤以檢閱新增 app 清單。 「封鎖 App Store 存取」預設隔離動作已無法使用。 在特定裝置上，因為特定裝置限制的關係，「隔離動作」將不會移除裝置上的應用程式。 預設會選取此選項 (針對全部三個選項:「所有應用程式」、「除下列項目外移除所有應用程式」和「指定的應用程式」)，且無法取消選取。 這會阻止 app 在裝置上進行重新安裝。 **移除組態** - 從裝置中移除 Ivanti Neurons for MDM 組態。 請選擇下列選項之一： • **所有配置**

相符性動作	用途
	• **指定配置**- 從清單選擇一或多個配置，或者搜尋配置。 按一下**所選配置** 索引標籤以檢閱所選 app 清單。 **推播指定組態** - 將指定組態作為自訂合規的一部分發佈。 此清單包含符合下列準則的配置： • 已啟用的配置 • 非系統配置 • 可隔離的配置 • 在目前空間中建立的配置，或從預設空間委派的配置 如需非應隔離的配置清單，請參閱非應隔離的配置。 **移除內容** - 從裝置移除 Ivanti Neurons for MDM 所發佈的一切與應用程式相關聯的內容和媒體。 **暫停個人應用程式** - 暫停被隔離裝置個人端的應用程式，指出裝置使用者需要解決裝置上的合規問題，才能讓裝置正常運作。 支援在 Android 11+ 裝置上佈建為公司擁有裝置上的工作描述檔。

尋找現有的原則

您可在原則頁面中使用篩選和搜尋功能，以尋找一或多個現有原則。

程序

1. 前往**原則**。
2. 如要篩選符合特定條件的原則清單，請按一下**篩選**。
3. 選擇一或多個篩選條件。
4. 如要依原則名稱搜尋現有的原則，在**搜尋**欄位中輸入原則名稱。

新增原則

程序

1. 前往**原則**。
2. 按一下 +**新增** (右上角)。
3. 選擇原則類型。
4. 完成設定。
5. 選擇要接收此原則的裝置群組。

> 您一次可發佈最多 100 個配置檔案。

6. 按一下**完成**。

編輯原則

程序

1. 前往**原則**。
2. 對於所需的原則，按一下「動作」欄之下的**編輯** (鉛筆) 圖示。
3. 進行變更。

4. 儲存變更。

刪除原則

程序

1. 前往**原則**。
2. 對於所需的原則，按一下「動作」欄之下的**移除**圖示。
3. 按一下**是**以進行確認。

如果您無法看到「原則」頁面，可能是您沒有所需的權限。 您需具備下列其中一個**角色**：

- 裝置管理
- 裝置唯讀

如需更多資訊，請參閱**優先排序原則**。

11.2. 自訂原則

原則

授權：Platinum

合格裝置： Android、iOS、macOS、Windows。

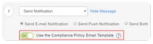
可讓您依據裝置和指定的使用者屬性、區段準則、值和合規動作，來建立自訂原則。

> Android Security 修補程式層級設定甚至可用於定義自訂原則。

新增自訂原則

1. 前往**原則**。
2. 按一下 **+新增**。
3. 選擇**自訂原則**。
4. 提供自訂原則的名稱。
5. 按一下 **+ 新增描述**，視需要輸入其他詳細資料。
6. 使用「規則建置器」來定義條件，以在條件評估為 True 時觸發動作。 請參閱**瞭解條件設定**，以取得建立條件的指引。 在規則建立器中選取「使用者群組名稱」屬性後，Ivanti Neurons for MDM 管理員主控台會顯示重複的使用者群組數量及對應的 GUID 數量，以識別重複的群組。 此外，此規則之下的表格會顯示重複使用者群組的清單以及其詳細資訊，例如使用者群組名稱、GUID、來源和可分辨的名稱 (DN)。
7. 選擇在符合指定條件時要採取的合規動作之一 (請參閱下面的「預設動作」)。 您可以在其他動作之間新增「**等待**」動作，讓裝置使用者先修正裝置並使其回到合規狀態，系統再採取其他動作。 例如，您可以傳送警告訊息，然後等待 24 小時之後才套用隔離動作。
8. 選擇**在裝置回到合規時傳送通知**選項，此選項預設關閉。

- **傳送電子郵件通知** - 將電子郵件傳送到裝置使用者的電子郵件地址，以便在裝置恢復合規性時通知他們。
  - 開啟**使用合規原則電子郵件範本**選項，將您在這裡設定的訊息插入您設定的原則通知電子郵件範本，如在**將電子郵件範本品牌化**中的**自訂電子郵件範本**所述。 如需概觀，請參閱**設定和使用原則遵循通知電子郵件**。

    
  - 您可以自訂訊息，在其中加入選用的替代變項，以提供收件人更多的原則違規細節與其他相關資訊。 按一下下列屬性類型以顯示完整的變項清單：
    - 原則屬性包括政策 $、$ 及 $。
    - 使用者屬性包括 $、$ 及 $。
    - 裝置屬性包括 $、$ 及 $。
    - 自訂在**管理 > 屬性**頁面中建立的 裝置/使用者/LDAP 屬性。
- **傳送推送通知** - 在裝置回到合規時傳送推送通知給裝置。
- **傳送兩者** - 在裝置回到合規時，傳送推送通知到裝置並傳送電子郵件到裝置使用者的電子郵件地址。 您可以自訂訊息，在其中加入選用的替代變項，以針對之前所描述的「傳送電子郵件」動作提供收件人更多的詳細資料。

9. 從表格中指定以下選項，以便在裝置擁有者違反原則規則時通知管理員和註冊的裝置擁有者:

選項	描述
主旨	輸入主旨文字。 例如，「您已經違反原則！」
本文	視需要輸入訊息。 例如，「需要採取動作！」
僅傳送電子郵件通知給管理員	選取此選項以僅將電子郵件通知傳送給管理員。
副本抄送給管理員	如果您已選取「僅傳送電子郵件通知給管理員」選項，此文字方塊將無法使用。
輸入管理員電子郵件地址	輸入管理員的電子郵件 ID。 若要新增多個電子郵件地址，請使用分號 (;) 作為分隔符號。
預覽電子郵件	按一下**預覽電子郵件**按鈕可檢視電子郵件地址。

10. 按一下**下一步**可儲存原則詳細資料。

預設動作：

1. 按一下**是**勾選方塊，確認您瞭解裝置之前已觸發此原則；若您新增分層原則，將會重設之前已套用的原則和任何合規動作。 新的自訂原則會在下一次裝置登記時生效。 如果您選擇「淘汰」動作，請按一下**是**，確認您瞭解此動作無法取消。

- **監控** - 目前一律選擇。 需要 Sentry 9.0.0 版或更新版本才能使用分層合規動作。
- **不採取動作**
- **傳送通知**
- **傳送電子郵件** - 將電子郵件傳送到裝置使用者的電子郵件地址，通知他們裝置不合規。
  - 您可依上述說明使用原則通知電子郵件。
  - 您可以自訂訊息，在其中加入選用的替代變項，以提供收件人更多的原則違規細節與其他相關資訊。 這提供使用者不合規的裝置與原則違規相關資訊，以便他們採取補救動作。 按一下下列屬性類型以顯示完整的變項清單：
    - 原則屬性包括政策 $、$ 及 $。
    - 使用者屬性包括 $、$ 及 $。
    - 裝置屬性包括 $、$ 及 $。
    - 自訂在**管理 > 屬性**頁面中建立的 裝置/使用者/LDAP 屬性。
- **傳送推送通知** - 傳送推送通知到違規裝置。
- **傳送兩者** - 選擇此選項可傳送推送通知到裝置，並傳送電子郵件到裝置使用者的電子郵件地址，以通知他們裝置違規。 您可以自訂訊息，在其中加入選用的替代變項，以針對之前所描述的「傳送電子郵件」動作提供收件人更多的詳細資料。
- **封鎖** - 使用Sentry 來封鎖受管理裝置存取電子郵件和支援 AppConnect 功能的應用程式。 需要 Sentry 9.0.0 版或更新版本才能使用封鎖動作。
- **淘汰** - 淘汰裝置。 **此動作無法取消**。 例如，可利用「已啟用使用者」條件來建立針對所有已停用使用者進行裝置淘汰的規則。
- **等待** - 延遲達到指定時間期 (小時數或天數) 的動作以容許使用者採取補救動作，之後如果裝置仍處於違規狀態，系統將採取其他動作。
- **隔離** - 依下列動作移除 app、內容及伺服器的存取權：

(選用) 其他的隔離動作	描述
隔離受管理應用程式	移除裝置上受 Ivanti Neurons for MDM 管理的應用程式，並啟用「阻擋新應用程式下載」選項，以阻擋裝置重新安裝應用程式。 請選擇下列選項之一： • **所有應用程式** • **指定應用程式**- 藉由查閱或手動 (使用套件 ID 或套件名稱)。 按一下**檢視 App** 索引標籤以檢閱新增 app 清單。 「封鎖 App Store 存取」預設隔離動作已無法使用。 在特定裝置上，因為特定裝置限制的關係，「隔離動作」將不會移除裝置上的應用程式。
封鎖新 App 下載	預防下載新 app 至裝置。 請選擇下列選項之一： • **所有應用程式** • **指定應用程式**- 藉由查閱或手動 (使用套件 ID 或套件名稱)。 按一下**檢視 App** 索引標籤以檢閱新增 app 清單。 「封鎖 App Store 存取」預設隔離動作已無法使用。 (對於「所有應用程式」和「指定應用程式」) 預設選擇此選項，而且無法取消選擇。 這會阻止 app 在裝置上進行重新安裝。
移除配置	從裝置移除 Ivanti Neurons for MDM 組態。 請選擇下列選項之一： • **所有配置** • **指定配置**- 從清單選擇一或多個配置，或者搜尋配置。 按一下**所選配置** 索引標籤以檢閱所選 app 清單。
推送指定配置	透過自訂合規發佈指定配置。 此清單包含符合下列準則的配置： • 已啟用的配置 • 非系統配置 • 可隔離的配置 • 在目前空間中建立的配置，或從預設空間委派的配置 如需非應隔離的配置清單，請參閱非應隔離的配置。 如需詳細資訊，請在完成此程序後參閱推送指定組態 章節。
移除內容	從裝置移除 Ivanti Neurons for MDM 所發佈的一切與應用程式相關聯的內容和媒體。
暫停個人 App	暫停隔離裝置個人端上的 app，指出裝置使用者需要處理裝置違規問題，才能讓裝置正常運作。 支援在 Android 11+ 裝置上佈建為公司擁有裝置上的工作描述檔。
預設的隔離動作 - 一律執行這些動作。	
封鎖 App Store 存取	防止裝置透過 Ivanti Neurons for MDM 存取應用程式商店。
封鎖 Content Store 存取	防止裝置透過 Ivanti Neurons for MDM 存取內容存放區。
封鎖 AppConnect	預防裝置使用 AppConnect 的功能。
封鎖 AppTunnel	預防裝置上的應用程式透過 AppTunnel 存取內容和伺服器。
封鎖 ActiveSync	預防裝置透過 ActiveSync 伺服器存取電子郵件。

2. 按**下一步**，以設定要將原則和動作套用至哪些裝置。
3. 按一下**完成**。

下表說明當 Ivanti Neurons for MDM 是隔離動作的啟動者時，在各種 Android 裝置上的隔離行為：

裝置中的下列目錄來判斷隱私權配置是否適用於屬意裝置	隔離行為
透過 Go 用戶端 app 之處於「裝置管理」模式的 Samsung 裝置	• 解除安裝受管理公用 app 和內部開發的 app • 移除特定設定檔 (不包括行動威脅防禦和其他設定檔)
透過 Go 用戶端 app 之處於「裝置管理」模式的非 Samsung 裝置 透過 AppStation app 的 MAM	• 不支援解除安裝或隱藏受管理公用 app 和內部開發的 app • 移除特定設定檔 (不包括行動威脅防禦和其他設定檔)
透過 Go 用戶端應用程式管理 Android Enterprise	• 隱藏受管理公用 app 和內部開發的 app • 移除特定設定檔 (不包括行動威脅防禦和其他設定檔)

推送指定組態

透過自訂合規發佈指定配置。 設定「自訂原則」，以在裝置違規時發佈一組配置。 在裝置狀態從違規變更成合規狀態時，透過補救動作將裝置重設為先前狀態。

> 管理員在「推送指定配置」索引標籤中嘗試委派其中具有非委派配置的自訂原則時發生錯誤。

以下是在特定情況下透過自訂原則推送配置時的行為：

條件	行為
選擇了兩個類型相同且設定了優先順序的配置	會將優先順序較高的配置推送到裝置上。
會選擇兩個類型相同但未設定優先順序的配置	兩種配置都將推送到裝置上。 可能會導致非預期的行為。
當裝置已具有類型相同且支援自訂原則中定義之優先順序的配置	會優先將自訂原則當中定義的配置推送到裝置上。 不論優先順序如何 (即使優先順序高於自訂原則當中定義的配置)，將會移除裝置上的現有配置。
當裝置已具有類型相同且不支援自訂原則當中定義之優先順序的配置	會將自訂原則當中定義的配置推送到裝置上。 兩種配置都將出現在裝置上。 可能會導致非預期的行為。
如果配置的優先順序在建立自訂原則後變更	在裝置登記時，將會依照自訂原則推送優先順序最高的配置。
當兩個條件都符合時： • 條件 A: 違規裝置已有作為自訂原則部分推送的組態 (且優先於裝置上已有的相同類型組態)。 • 條件 B: 已補救違規，裝置不再處於隔離狀態	將會移除自訂原則中定義的配置，且隔離前裝置上的相同類型配置會透過現有裝置群組的應用程式推送，將裝置還原回其原始狀態。

在隔離動作中，如果您選擇了「移除配置」與「推送指定配置」，請注意下列規則：

- 移除所有配置 + 推送指定配置：在這種情況下，將會移除裝置上的所有配置，而在「推送指定配置」中選定的配置將會推送到裝置上。
- 選擇指定組態 (在一個自訂原則中) + 「推送」指定組態 (在另一個自訂原則中) 後將二者連同通用組態移除」：由於在兩個不同的合規原則中選擇組態，因此將採用最嚴格的方法，也就是說 將從裝置中刪除組態。

您可以從預設**空間**委派自訂原則給自訂空間。 對於待委派的自訂原則，需要將在「推送指定配置」索引標籤下自訂原則中提到的配置委派給空間。

在**裝置**頁面中，您可以按一下裝置名稱，以造訪裝置詳細資料頁面。 在「配置」索引標籤下，「發佈方法」欄針對要推送至裝置的配置指出其發佈方法。 方法可是「裝置群組」或「合規動作」。

在「配置」頁面上的每個配置中，Ivanti Neurons for MDM 都會顯示透過裝置群組與合規動作收到配置的裝置計數。

瞭解條件設定

下表說明可用來建置規則的一些欄位：

UI 欄位	描述	可能的值	支援的平台
支援 APNS	此欄位指出裝置是否支援 APNS。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。	iOS/macOS/Android
防網路釣魚原生狀態	此欄位顯示防網路釣魚原生狀態	可能的運算子為: • 等於 • 不等於 可能的值為: • 未啟用 • 不適用 • 啟用 • 不明	iOS/Android
防網路釣魚狀態	此欄位顯示防網路釣魚狀態	可能的運算子為: • 等於 • 不等於 可能的值為: • 未啟用 • 不適用 • 啟用 • 不明	iOS/Android
防網路釣魚 VPN 狀態	此欄位顯示防網路釣魚 VPN 狀態	可能的運算子為: • 等於 • 不等於 可能的值為: • 未啟用 • 不適用 • 啟用 • 不明	iOS/Android
電池資訊	此欄位具有下列屬性: • 電池電力 - 顯示 Android 作業系統報告的目前電池電力 • 電池健全狀況 - Android 作業系統報告的狀態 • 電池充電狀態 - Android 作業系統報告的狀態	如需關於可能值的資訊，請參閱使用進階搜尋。	Android

UI 欄位	描述	可能的值	支援的平台
	• 電池健全狀況百分比 (OEM 特定) - 支援之裝置製造商裝置 (例如 Zebra 裝置) 的電池健全狀況百分比 • 電池生產日期 (OEM 特定) - 支援之裝置製造商裝置 (例如 Zebra 裝置) 的電池生產日期 • 電池充電週期 (OEM 特定) - 支援之裝置製造商裝置 (例如 Zebra 裝置) 完成的週期總數		
基頻健康狀態	此欄位表示裝置的基帶健康狀態。	可能的運算子為： • 等於 • 不等於 可能的值為正常或錯誤。	iOS 27.0+ 受監管裝置
可用的啟動程序權杖	此欄位指出啟動程序權杖是否可用於裝置。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。	macOS
已註冊 Autopilot	此欄位會指出裝置是否已註冊 Autopilot。	• 等於 • 不等於 可能的值為「是」和「否」。	Windows
Bridge 上次簽入	此欄位會指出用戶端的 Bridge 上次簽入時間。	可能的運算子為： • 小於 • 小於或等於 • 大於 • 大於或等於 • 在範圍內 • 不在範圍內 輸入 Bridge 上次簽入時間的數值。 選取以下任何選項作為持續時間: • 小時 • 天 範例: Bridge 上次簽入時間是不到 12 小時前。	Windows
相機健康狀態	此欄位表示裝置的相機健康狀態。	可能的運算子為： • 等於 • 不等於 可能的值如下： • 正常	iOS 27.0+ 受監管裝置

UI 欄位	描述	可能的值	支援的平台
		• 錯誤 • 非正品 (如果不是正品 Apple 元件)	
用戶端上一次登記	此欄位指出用戶端的上一次登記時間。	可能的運算子為： • 小於 • 大於 輸入上一次登記時間的數值。 選擇下列其中一個持續時間選項： • 小時 • 天 範例：用戶端上一次登記是在不到 12 小時前。	iOS/macOS/Android
已註冊的用戶端	此欄位指出已註冊的用戶端狀態。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。	iOS/macOS/Android
受威脅	此欄位指出裝置是否遭 Root/受威脅。	可能的運算子為： • 等於 • 不等於 可能的值如下： • 遭越獄或遭 Root 破解 • 未受威脅	iOS/Android
目前的國家/地區名稱	此欄位指出回報為目前連接裝置的目前國家/地區名稱 (與行動電話國家/地區碼 (MCC) 或行動電話網路碼 (MNC) 對應)。	可能的運算子為： • 等於 • 不等於 可能的值為下拉式清單值，其指出主要國家/地區名稱。	iOS/macOS/Android
目前的 MCC	此欄位指出目前行動國家代碼 (Mobile Country Code)	輸入要驗證的屬性值。 可能的運算子為： • 等於 • 不等於	iOS/macOS/Android
目前的 MNC	此欄位指出目前行動網路代碼 (Mobile Network Code)	輸入要驗證的屬性值。 可能的運算子為： • 等於 • 不等於	iOS/macOS/Android
自訂裝置屬性	此欄位可將現有的自訂裝置屬性新增為規則條件，以驗證其中的值。	輸入要驗證的屬性值。 可能的運算子為： • 等於 • 不等於 • 包含 • 不包含 值可以是 ASCII 字元的字串，包括空格和 Unicode 字	iOS/macOS/Android/Windows

UI 欄位	描述	可能的值	支援的平台
		元。	
自訂 LDAP 屬性	此欄位可將現有的自訂 LDAP 屬性新增為規則條件，以驗證其中的值。	輸入要驗證的屬性值。 可能的運算子為： • 等於 • 不等於 • 包含 • 不包含 值可以是 ASCII 字元的字串，包括空格和 Unicode 字元。	iOS/macOS/Android/Windows
自訂使用者屬性	此欄位可將現有的自訂使用者屬性新增為規則條件，以驗證其中的值。	輸入要驗證的屬性值。 可能的運算子為： • 等於 • 不等於 • 包含 • 不包含 值可以是 ASCII 字元的字串，包括空格和 Unicode 字元。	iOS/macOS/Android/Windows
數據漫遊	此欄位可將要使用的數據漫遊新增為規則條件，以驗證其中的值。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。 如果支援的裝置未報告此欄位的相關資訊，則預設值為「否」。	iOS/Android
裝置類型	此欄位代表裝置機型。	可能的運算子為： • 等於 • 不等於 • 開頭是 • 結尾是 可能的值為文字值。	iOS/macOS/Android/Windows
裝置類型 (Apple)	此欄位會指出裝置的 Pretty Model 名稱。	可能的運算子為： • 等於 • 不等於 • 開頭是 • 結尾是 可能的值為文字值。	iOS/macOS
顯示健康狀態	此欄位表示裝置的顯示健康狀態。	可能的運算子為： • 等於 • 不等於 可能的值如下：	iOS 27.0+ 受監管裝置

UI 欄位	描述	可能的值	支援的平台
		• 正常 • 錯誤 • 非正品 (如果不是正品 Apple 元件)	
加密已啟用	此欄位判定裝置是否已啟用加密/資料保護。	是 - 裝置已啟用加密/資料保護。 否 - 裝置未啟用加密/資料保護。	iOS/Android/Windows
GUID	此欄位列出裝置 GUID。	可能的運算子為： • 等於 • 不等於 • 開頭是 • 結尾是	iOS/macOS/Android/Windows
Face ID 健康狀態	此欄位表示裝置 Face ID 健康狀態。	可能的運算子為： • 等於 • 不等於 可能的值為正常或錯誤。	iOS 27.0+ 受監管裝置
主要國家/地區名稱	此欄位指出編入裝置 SIM 或 eSIM 的主要國家/地區名稱 (與行動電話國家/地區碼 (MCC) 或行動電話網路碼 (MNC) 對應)。	可能的運算子為： • 等於 • 不等於 可能的值為下拉式清單值，其指出主要國家/地區名稱。	iOS/Android/Windows
Windows 更新失敗	此欄位將決定裝置是否不符合最新的更新規則。	是 - 裝置不符合最新的更新。 否 - 裝置符合最新的更新。	Windows
歸屬 MCC	此欄位指出歸屬行動國家代碼 (Mobile Country Code)	輸入要驗證的屬性值。 可能的運算子為： • 等於 • 不等於	iOS/macOS/Android
歸屬 MNC	此欄位指出歸屬行動網路代碼 (Mobile Network Code)	輸入要驗證的屬性值。 可能的運算子為： • 等於 • 不等於	iOS/macOS/Android
IMEI	此欄位列出第一個 SIM 插槽的 IMEI 編號。	可能的運算子為： • 等於 • 不等於 • 開頭是 • 結尾是	iOS/Android/Windows
IMEI2	此欄位列出第二個 SIM 插槽的 IMEI 編號。	可能的運算子為： • 等於 • 不等於	Android

UI 欄位	描述	可能的值	支援的平台
IMSI	此欄位列出 SIM 卡的 IMSI 編號。	• 開頭是 • 結尾是 可能的運算子為： • 等於 • 不等於 • 開頭是 • 結尾是	Android/Windows
機構復原金鑰已啟用	此欄位指明裝置上是否啟用了機構復原金鑰。	可能的運算子為： • 等於 • 不等於	macOS
上一次登入	此欄位可讓您設定與透過 MDM 通道的受管理裝置其上一次登記時間相關的條件。	可能的運算子為： • 小於 • 大於 • 為空 輸入上一次登記時間的數值。 選擇下列其中一個持續時間選項： • 小時 • 天 範例：上一次登記是在 12 小時之前。	iOS/macOS/Android/Windows
上一個 Hotfix ID	此欄位可讓您設定與上一個 Hotfix ID 相關的條件	可能的運算子為： • 等於 • 不等於 • 小於 • 小於或等於 • 大於 • 大於或等於 • 包含 • 不包含 • 開頭是 • 開頭不是 • 結尾是 • 結尾不是	Windows
上一個 Hotfix 安裝在	此欄位可讓您設定與上次安裝之 Hotfix 相關的條件。	可能的運算子為： • 小於 • 大於	Windows

UI 欄位	描述	可能的值	支援的平台
定位服務已啟用	此欄位指出裝置是否已啟用定位服務 (例如：尋找我的 iPhone)。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。	iOS
製造商	此欄位可讓您設定與裝置製造商相關的條件。	可能的運算子為： • 等於 • 不等於 可能的值如下： • Samsung • NOKIA • HTC • LGE • Apple Inc	iOS/macOS/Android/Windows
MTD 啟用狀態	此欄位顯示 MTD 啟用狀態	可能的運算子為: • 等於 • 不等於 可能的值為: • 不適用 • 錯誤 • 擱置中 • 受保護	iOS/Android
MDM 已受管理	此欄位判定裝置是否已啟用 MDM/裝置管理員。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。	iOS/macOS/Android
MDM 註冊類型	此欄位表示裝置的註冊類型。	可能的運算子為： • 等於 • 不等於 可能的值如下： • 使用者 • 裝置 • 受監管 • 無	iOS 27.0+、macOS 27.0+、tvOS 27.0+、 visionOS 27.0+ 和 watchOS 27.0+
MDM 返回服務	此欄位表示使用應用程式保留的 MDM 返回服務的裝置狀態。	可能的運算子為： • 等於	iOS 27.0+ 和 visionOS 27.0+

UI 欄位	描述	可能的值	支援的平台
		• 不等於 可能的值為 True 或 False。	
多位使用者模式	此欄位指出裝置 (iPad) 是否使用多使用者模式。	可能的運算子為： • 等於 • 不等於 可能的值為是或否。	iOS 27.0+
近場健康狀態	此欄位表示裝置 NFC 健康狀態。	可能的運算子為： • 等於 • 不等於 可能的值為正常或錯誤。	iOS 27.0+ 受監管裝置
作業系統	此欄位代表裝置的作業系統類型。	可能的運算子為： • 等於 • 不等於 可能的值如下： • macOS • Android • iOS • Windows • visionOS	iOS/macOS/visionOS/Android/Windows
作業系統組建版本	此欄位代表裝置的作業系統組建版本。	可能的運算子為： • 等於 • 不等於 • 小於 • 小於或等於 • 大於 • 大於或等於 • 包含 • 不包含 • 開頭是 • 開頭不是 • 不為空 • 為空 • 結尾是 • 結尾不是	iOS/macOS/visionOS/Android/Windows
作業系統版本	此欄位代表裝置的作業系統版本。	可能的運算子為： • 等於	iOS/macOS/visionOS/Android/Windows

UI 欄位	描述	可能的值	支援的平台
		• 不等於 • 小於 • 小於或等於 • 大於 • 大於或等於 • 在範圍內 • 不在範圍內 可能的值為文字。	
作業系統及版本	此欄位表示裝置的作業系統和作業系統版本	可能的運算子為： • 等於 • 不等於 • 小於 • 小於或等於 • 大於 • 大於或等於 • 在範圍內 • 不在範圍內 可能的值為文字。	iOS/macOS/visionOS/Android/Windows
擁有權	此欄位代表裝置的擁有權類型。	可能的運算子為： • 等於 • 不等於 可能的值如下： • 使用者擁有 • 未設定 • 公司擁有	iOS/macOS/Android/Windows
個人復原金鑰已啟用	此欄位指明是否啟用了個人復原金鑰。	可能的運算子為： • 等於 • 不等於	macOS
密碼符合描述檔	此欄位指出裝置密碼是否符合描述檔。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。	iOS/macOS/Android
個人熱點已啟用	此欄位指出在裝置上是否已啟用個人熱點功能。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。	iOS

UI 欄位	描述	可能的值	支援的平台
		個人熱點設定僅適用於特定電信業者。	
電話號碼	此欄位列出裝置電話號碼。	可能的運算子為： • 等於 • 不等於 • 包含 • 開頭是 • 結尾是	iOS/Android/Windows
公用 IP 位址	此欄位顯示公用 IP 位址。 如果裝置使用 VPN 連線或 Proxy 伺服器連線至 Ivanti Neurons for MDM，則會顯示 Proxy WAN IP 位址。	可能的運算子為： • 在範圍內 • 不在範圍內 • 不為空 • 為空	Android/ChromeOS
漫遊	此欄位指出裝置的漫遊狀態。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。	iOS/Android/Windows
安全鎖定模式	此欄位指出裝置的鎖定模式是啟用或停用。	可能的運算子為： • 等於 • 不等於 可能的值為 True 或 False。	iOS 27.0+ 和 macOS 27.0+
Sentry 已封鎖	指示裝置是否被 Sentry 封鎖。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。	iOS/macOS/Android/Windows
狀態	此欄位指出註冊狀態。	可能的運算子為： • 等於 • 不等於 預設的可能值為「作用中」。 在自訂原則中，它透過移除所有其他潛在值將裝置狀態限制為「作用中」，因為當裝置針對「作用中」、「淘汰擱置中」和「抹除擱置中」狀態簽入時會進行原則評估，並且這些裝置的原則將在裝置簽入時接受評估。	iOS/macOS/Android
序號	此欄位列出裝置序號。	可能的運算子為： • 等於 • 不等於 • 開頭是 • 結尾是	iOS/macOS/Android/Windows

UI 欄位	描述	可能的值	支援的平台
受監管	此欄位指出裝置是否受監管。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。	iOS/macOS
補充建置版本	此欄位表示裝置的補充建置版本。	可能的運算子為： • 等於 • 不等於 • 小於 • 小於或等於 • 大於 • 大於或等於 • 包含 • 不包含 • 開頭是 • 開頭不是 • 結尾是 • 結尾不是 • 不為空 • 為空	iOS/macOS
補充作業系統/版本額外資訊	此欄位表示裝置的補充作業系統建置版本。	可能的運算子為： • 等於 • 不等於 • 小於 • 小於或等於 • 大於 • 大於或等於 • 包含 • 不包含 • 開頭是 • 開頭不是 • 結尾是 • 結尾不是 • 不為空 • 為空	iOS/macOS

UI 欄位	描述	可能的值	支援的平台
Touch ID 健康狀態	此欄位表示裝置 Touch ID 健康狀態。	可能的運算子為： • 等於 • 不等於 可能的值如下： • 正常 • 錯誤 • 不適用 (如果是 iPhone)	iOS 27.0+ 受監管裝置
已啟用使用者	此欄位指出裝置是否已啟用使用者。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。	iOS/macOS/Android/Windows
使用者群組	此欄位代表使用者群組。	可能的運算子為： • 等於 • 不等於	iOS/macOS/Android/Windows
超寬帶健康狀態	此欄位表示裝置的超寬帶健康狀態。	可能的運算子為： • 等於 • 不等於 可能的值為正常或錯誤。	iOS 27.0+ 受監管裝置
語音漫遊	此欄位指出在裝置上是否已啟用語音漫遊。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。 語音漫遊設定僅適用於特定電信業者。 停用語音漫遊也會停用數據漫遊。 如果支援的裝置未報告此欄位的相關資訊，則預設值為「不等於」。	iOS
Access 已封鎖	指示裝置是否遭 Access 封鎖。	可能的運算子為： • 等於 • 不等於 可能的值為「是」和「否」。	iOS/macOS/Android/Windows
相符性	指示裝置是否合規。	可能的運算子為： • 等於 • 不等於 可能的值為「合規」和「不合規」。	iOS/macOS/Android/Windows
合規性動作已封鎖	指示裝置是否遭到封鎖。	可能的運算子為： • 等於	iOS/macOS/Android/Windows

UI 欄位　　描述	可能的值　　支援的平台
	• 不等於 可能的值為「是」和「否」。

非應隔離的配置

下表顯示非應隔離的配置清單：

作業系統	非應隔離的配置
Android	• Android 應用程式目錄 • Android 加密 • Android Enterprise • Android Enterprise App • Android Zebra • 防網路釣魚保護 • Android 工作挑戰 • 裝置密碼 • 檔案下載 • 鎖定與單一應用：Android 裝置管理模式 • 鎖定與單一應用：Samsung Knox Standard • 僅限 MAM • 搭配工作描述檔的受管理裝置/公司擁有裝置上的工作描述檔 • 工作受管理裝置 (裝置擁有者) • Samsung 手機限制 • SafetyNet 證明 • 公司擁有裝置上的工作設定檔
iOS 與 macOS	• 防網路釣魚保護(iOS) • App 通知 (iOS) • AppStation 網站 (iOS) • FileVault 復原金鑰 (macOS) • FileVault 2 (macOS) • 全域代理 (iOS 和 tvOS) • 首頁畫面版面配置 (iOS 和 tvOS) • iOS App 控制 • iOS 限制 • iOS 軟體更新 (iOS) • macOS 防火牆 • macOS 軟體更新 • 僅限 MAM (iOS) • MI 用戶端隱私權 (iOS/macOS) • 網路用量 (iOS) • Office 365 帳戶建立 (macOS) • 單一應用程式模式 (iOS 和 tvOS) • 系統原則控制 (macOS)

作業系統	非應隔離的配置
	• 受管理的系統原則 (macOS) • 系統原則規則選項 (macOS) • 時間伺服器 (macOS) • Web 內容篩選 (iOS)
Windows	• Windows App 控制 • Windows 限制DDF (資料定義檔) • Windows 防火牆 • Windows 網路 Proxy • Windows 限制 • Windows 更新
全部	• Active Directory • 用戶端服務 • 行動裝置管理 • 行動威脅防護啟用 • 行動威脅防護本機動作 • 密碼 • 隱私權 • 隱私權聲明 • ServiceConnect • 同步

如果您無法看到「原則」頁面，可能是您沒有所需的權限。 您需具備下列其中一個角色：

- 裝置管理
- 裝置唯讀

11.3. 監控與控制允許的 App

授權：Silver

若要控制裝置上可安裝哪些 App，您可建立「允許的 App」原則。 此原則也支援 MobileIron 封裝工具 (MIP) 內部開發 macOS app。 此原則包含下列資訊：

- {{允許清單 app}}
- {{封鎖清單 app}}
- {{必要的 app}}
- {{相符性動作}}

如果 app 同時為必要的 app 和封鎖清單 app，則系統會優先將該 app 評估為必要的 app。 例如，如果 app A1 同時出現在必要清單和封鎖清單中，則此裝置的 app 原則評估行為如下：

- 如果裝置上安裝了 A1，裝置為合規。
- 如果裝置上未安裝 A1，裝置為違規。

支援裝置

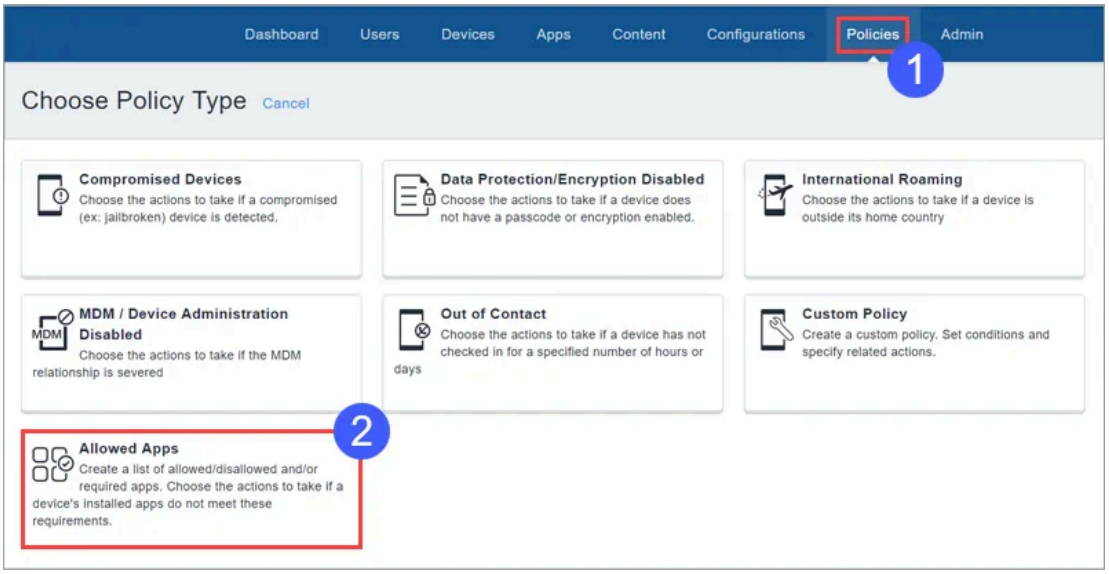
- Android 4.2 或支援的更新版本
- iOS 8.0 或支援的更新版本
- macOS 10.12 或支援的更新版本
- Windows 10 或支援的更新版本

必要條件

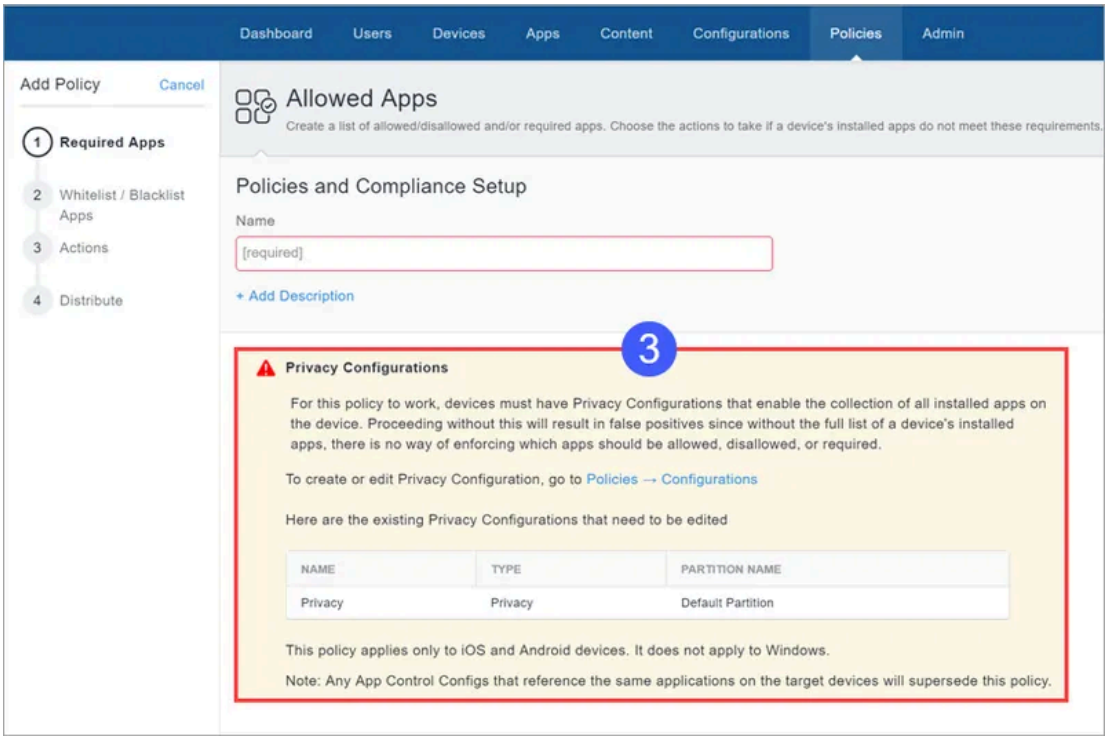
- 指派給裝置的隱私權配置必須允許收集 app 的資訊，「允許的 App」原則才能有效運作。 針對您要套用「允許的 App」原則的裝置，檢查指派給該裝置的隱私權配置。

如果您不確定哪些配置會受影響：

1. 前往**原則**。



按一下**允許的 App**。



3. 在**隱私權配置**下方，記下需要編輯的配置。
4. 前往**配置**。
5. 針對您記下的每一項隱私權配置：
    1. 選擇配置。
    2. 按一下**編輯**。
    3. 在**收集 App 庫存**下方，選擇**裝置上的所有 App**。
    4. 按一下**完成**。

建立允許的應用程式原則

必要條件

- 啟用 Android Enterprise 以存取 Google Play Store 並新增應用程式至允許的 App 原則。

程序

1. 前往**原則**然後按一下 **+新增**。

2. 按一下**允許的 App**。

3. 在**名稱**欄位中，輸入此原則的名稱。
4. 在**描述**欄位中，輸入說明原則用途的選填文字。
5. 按一下下列其中一個或兩個索引標籤，藉此選擇允許清單或封鎖清單的 app：

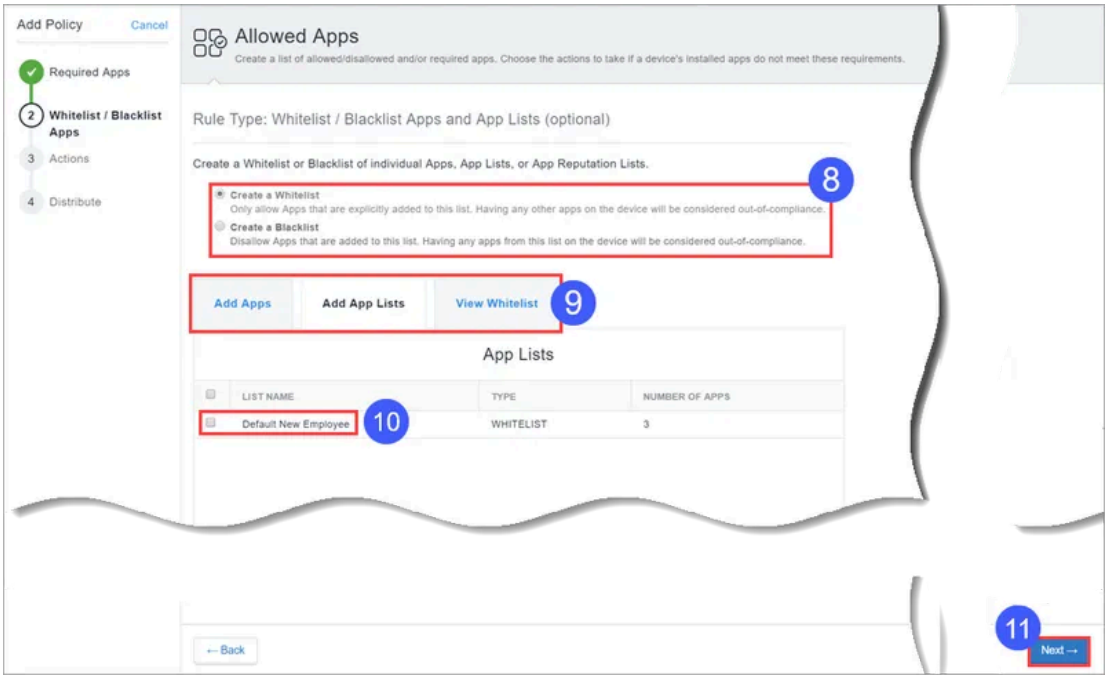
- 按一下藉由查閱來新增，從 App Store 或 App Catalog 搜尋並選擇 app。
  確保啟用 Android Enterprise 以存取 Google Play Store。
  
- 按一下**手動新增**，透過輸入 Android、Windows、iOS 或 macOS 系統應用程式的套組 ID 選擇應用程式。

選擇**新增 App 清單**索引標籤，然後選擇所需的必要 app 清單。

6. 使用產生的欄位來選擇必要的 app 或 app 清單。
7. 按**下一步**。

> 按一下**檢視必要清單**索引標籤，取得目前已選擇的應用程式清單。

8. 選擇要建立允許清單或封鎖清單。



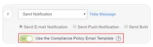
9. 使用**允許清單/封鎖清單 App 和 App 清單**區段，來選擇 app 和 app 清單。

> 裝置不能同時有允許清單和封鎖清單。 建立允許清單時，表示所有其他的 app 都會被列入封鎖清單。

10. 使用產生的欄位來選擇必要的 app 或 app 清單。
    - 選擇**新增 App 清單**索引標籤，然後選擇所需的 app 清單。
11. 按**下一步**。

> 您可以按一下**檢視允許清單或封鎖清單單**索引標籤，以取得目前已選擇的 app 清單。

12. 選擇當裝置違規時要採取的動作：

動作遊戲	方法
監控	目前一律選擇。 需要 Sentry 9.0.0 版或更新版本才能使用分層合規動作。
不採取動作	選擇當裝置違規時不採取任何動作。
傳送通知	
傳送電子郵件	選擇此選項可傳送電子郵件到裝置使用者的電子郵件地址，以通知他們裝置違規。 • 開啟**使用合規原則電子郵件範本**選項，將您在這裡設定的訊息插入您設定的原則通知電子郵件範本，如在**將電子郵件範本品牌化**中的**自訂電子郵件範本**所述。 如需概觀，請參閱**設定和使用原則遵循通知電子郵件**。  • 您可以自訂訊息，在其中加入選用的替代變項，以提供收件人更多的原則違規細節與其他相關資訊。 這提供使用者不合規的裝置與原則違規相關資訊，以便他們採取補救動作。 按一下下列屬性類型以顯示完整的變項清單： ◦ 原則屬性包括 $、$ 及 $。 ◦ 使用者屬性包括 $、$ 及 $。 ◦ 裝置屬性包括 $、$ 及 $。
傳送推送通知	選擇此選項可傳送推送通知到違規裝置。
傳送兩者	選擇此選項可傳送推送通知到裝置，並傳送電子郵件到裝置使用者的電子郵件地址，以通知他們裝置違規。 您可以自訂訊息，在其中加入選用的替代變項，以針對之前所描述的「傳送電子郵件」動作提供收件人更多的詳細資料。
等待	選擇此選項可顯示容許使用者採取補救動作的指定等待期間，之後如果裝置仍處於違規狀態，系統將採取其他動作。
封鎖	使用Sentry 來封鎖受管理裝置存取電子郵件和支援 AppConnect 功能的應用程式。
隔離	選擇此選項可依下表中的動作移除 app、內容及伺服器的存取權。 不允許移除所有的 app 動作。
在裝置回到合規時傳送通知	
傳送電子郵件	傳送電子郵件到裝置使用者的電子郵件地址，以通知他們裝置回到合規。 • 您可依上述說明使用原則通知電子郵件。 • 您可以自訂訊息，在其中加入選用的替代變項，以提供收件人更多的原則違規細節與其他相關資訊。 按一下下列屬性類型以顯示完整的變項清單： ◦ 原則屬性包括政策 $、$ 及 $。 ◦ 使用者屬性包括 $、$ 及 $。 ◦ 裝置屬性包括 $、$ 及 $。 ◦ 自訂在**管理 > 屬性**頁面中建立的 裝置/使用者/LDAP 屬性。
傳送推送通知	在裝置回到合規時傳送推送通知給裝置。
傳送兩者	在裝置回到合規時，傳送推送通知到裝置並傳送電子郵件到裝置使用者的電子郵件地址。 您可以自訂訊息，在其中加入選用的替代變項，以針對之前所描述的「傳送電子郵件」動作提供收件人更多的詳細資料。

如果您具備 Platinum 授權，允許的 App 原則即可支援**分級合規動作**。

(選用) 其他的隔離動作	描述
隔離受管理應用程式	移除裝置上受 Ivanti Neurons for MDM 管理的應用程式，並啟用「阻擋新應用程式下載」選項，以阻擋裝置重新安裝應用程式。 請選擇下列選項之一： • **所有應用程式** • **指定應用程式** - 藉由查閱或手動 (使用套件 ID 或套件名稱)。 按一下**檢視 App** 索引標籤以檢閱新增 app 清單。「封鎖 App Store 存取」預設隔離動作已無法使用。 在特定裝置上，因為特定裝置限制的關係，「隔離動作」將不會移除裝置上的應用程式。
封鎖新 App 下載	預防下載新 app 至裝置。 請選擇下列選項之一： • **所有應用程式** • **指定應用程式** - 藉由查閱或手動 (使用套件 ID 或套件名稱)。 按一下**檢視 App** 索引標籤以檢閱新增 app 清單。「封鎖 App Store 存取」預設隔離動作已無法使用。
移除配置	從裝置移除 Ivanti Neurons for MDM 組態。 請選擇下列選項之一： • **所有配置** • **指定配置**- 從清單選擇一或多個配置，或者搜尋配置。 按一下**所選配置** 索引標籤以檢閱所選 app 清單。
移除內容	從裝置移除 Ivanti Neurons for MDM 所發佈的一切與應用程式相關聯的內容和媒體。
暫停個人 App **預設的隔離動作** - 一律執行這些動作。	暫停隔離裝置個人端上的 app，指出裝置使用者需要處理裝置違規問題，才能讓裝置正常運作。 支援在 Android 11+ 裝置上佈建為公司擁有裝置上的工作描述檔。
封鎖 App Store 存取	防止裝置透過 Ivanti Neurons for MDM 存取應用程式商店。
封鎖 Content Store 存取	防止裝置透過 Ivanti Neurons for MDM 存取內容存放區。
封鎖 AppConnect	預防裝置使用 AppConnect 的功能。
封鎖 AppTunnel	預防裝置上的應用程式透過 AppTunnel 存取內容和伺服器。
封鎖 ActiveSync	預防裝置透過 ActiveSync 伺服器存取電子郵件。

按**下一步**。

14. 設定發佈。
15. 按一下**完成**。

有關對允許的 App 原則設定更高或更低優先排序的更多資訊，請參閱優先排序原則。

11.4. 優先排序原則

「允許的 App 原則」支援的優先順序與「配置」類似。 優先順序係用於判斷同類原則中何者應發佈至多個裝置群組，以及同一裝置出現在該等多重裝置群組中的情況。 例如，在下述情況中，原則優先順序對於判斷原則發佈非常有用：

- 「必要 App A」需發佈至裝置群組 1，
- 「必要 App B」需發佈至裝置群組 2，而
- 使用者的裝置是這兩個裝置群組的成員。

優先排序原則的方法如下：

1. 前往**原則 > 原則與相符性**。
2. 選擇**動作 > 優先排序原則**。 如果沒有顯示**動作**，就表示沒有需要優先排序的多個原則。
3. 使用方向箭頭將優先順序由最高 (頂端) 排列至最低 (底端)。 鎖定圖示代表您必須編輯原則內的「所有裝置」發佈設定，才能變更原則的優先順序。
4. 按一下**儲存**。

11.5. Windows 硬體原則

Couldn't convert your doc.

12. 管理

管理章節可協助您從 Ivanti Neurons for MDM 入口網站管理使用者、裝置和配置。 以下章節包含您以管理員身分可執行的所有工作清單：

- 系統
- 基礎架構
- 設定 (Apple)
- 使用 Windows 裝置
- 使用 Microsoft Azure 進行設置
- 連接 Google App
- 使用 ChromeOS 裝置
- 韌體管理
- 租戶停權
- 管理指令碼和檔案
- 品牌化
- 新增非 iOS 裝置管理

12.1. 系統

本節包含以下各主題：

- 屬性
- 裝置清理設定
- GDPR 設定檔
- 通知電子郵件
- 角色管理
- 空間
- 支援管理員
- 管理 > 系統使用通知

12.1.1. 屬性

使用「屬性」頁面執行下列工作:

- 管理可以為使用者、裝置及應用程式記錄的資訊類型。
- 檢視 Ivanti Neurons for MDM 追蹤的標準型資訊。

自訂使用者屬性包括部門或內部 ID 等資訊。 每個屬性都有一個對應變數，可用於建立群組或發佈組態。

> 在建立使用者規則群組條件時，若自訂屬性有數字值，Ivanti Neurons for MDM 不支援整數運算。

建立自訂屬性

可以從 Ivanti Neurons for MDM 管理入口網站建立自訂屬性。

程序

1. 登入管理入口網站。
2. 瀏覽至**管理** > **系統** > **屬性**。
3. 在**自訂屬性**之下，按一下 **+新增**。
4. 在**屬性名稱**欄位中，輸入要代表屬性的文字。

> 您輸入的文字，將會用來建立**用法**欄位中的對應變數。

從以下**屬性類型**選項中選擇任意屬性類型。

   - **使用者**
   - **裝置**
   - **應用程式**
   - **IDP** (如需詳細資訊，請參閱**使用 SCIM 進行使用者佈建** 或**將 Ivanti Neurons for MDM 連線至 Entra ID 使用者來源**)

如果屬性類型為「裝置」，則選取下列其中一種**資料類型**選項:

   - **數字**
   - **文字**

7. **保留屬性** (選用): 此選項只能在屬性類型為**裝置**時使用。 選取此選項可以保留自訂屬性，即使已在裝置上執行清除/淘汰作業。
8. 按一下**新增**。
   建立的自訂使用者屬性會顯示在屬性頁面中的**使用者屬性**區段。

> 支援任意順序的自訂屬性組合 $ + $ + $ + ${Static String}。

重新命名自訂屬性

重新命名自訂屬性，會將該自訂屬性用於下列實體的所有參照都重新命名：

- 自訂原則
- 使用者群組

- 裝置群組
- App 發佈篩選
- 空間

> 自訂屬性在任何其他實體 (例如配置、邀請電子郵件範本、原則合規動作中的電子郵件與推播訊息等等) 中的參照將不會予以更新。

程序

1. 在**管理員已新增**之下，按一下您要重新命名之屬性旁的 **+編輯**。
2. 在**屬性名稱**欄位中，輸入要代表屬性的新名稱。

> 您輸入的文字，將會用來建立**用法**欄位中的對應變數。

按一下**儲存**。

刪除自訂屬性

刪除自訂屬性時，會將其值從所有相關聯的使用者或裝置移除。 該動作無法取消。

若自訂屬性用於下列任一實體，則無法刪除該屬性：

- 自訂原則
- 使用者群組
- 裝置群組
- App 發佈篩選
- 空間

請先從實體移除自訂屬性，然後再嘗試刪除該自訂屬性。

如果您要刪除的屬性並未受上述任何實體參照，按一下該屬性旁的**刪除**將會顯示快顯視窗以確認動作。 確認動作，然後按一下**刪除**。

> 以下自訂屬性的欄位名稱會在適用的規則建立器中進行排序:

- 自訂 LDAP 屬性
- 自訂使用者屬性
- 自訂裝置屬性
- 自訂 IDP 屬性
- 自訂應用程式屬性

檢視系統屬性

系統屬性是預先定義的屬性，供您作為配置中的變數之用。 完整清單在**管理員** > **系統** > **屬性**頁面中的**系統屬性**區段提供。 系統屬性包括下列類型的屬性：

- 使用者屬性
- 裝置屬性
- 電子郵件範本屬性

- 系統屬性
- 時間戳記屬性
- Entra ID 自訂使用者屬性
- 原則屬性

使用者屬性

利用使用者屬性指定使用者相關資訊。

金鑰	描述
$	部門屬性 (需要 Entra ID)
$	電子資料交換 - 個人識別碼
$	使用者的受管理 Apple ID
$	sAMAccountName 屬性 (需要 Active Directory)
$	從辨別名稱中擷取的一般名稱 (CN) 屬性 (需要 LDAP)
$	顯示名稱
$	辨別名稱 (需要 LDAP)
$	電子郵件地址的網域部分 (「@」之後的部分)
$>	電子郵件地址的本機部分 (「@」之前的部分)
$	電子郵件地址
$	名字
$	姓氏
$	地區設定
$	從辨別名稱中擷取的組織單位 (OU) 屬性 (需要 LDAP)
$	Kerberos 領域資訊 (需要 Active Directory)
$	登入 ID 的網域部分 (「@」之後的部分)
$	登入 ID 的本機部分 (「@」之前的部分)
$	登入 ID (電子郵件地址格式)
$	userPrincipalName 屬性 (需要 Active Directory)

裝置屬性

利用裝置屬性指定行動裝置相關資訊。

金鑰	描述
$	用戶端上次簽入日期 (最近簽入 - MDM 或用戶端)
$	替代序號
$	用戶端應用程式使用的識別碼
$	全域唯一裝置識別碼
$	ICCID
$	IMEI2
$	IMEI
$	IMSI
$	裝置上次簽入日期 (最近簽入 - MDM 或用戶端)
$	內部裝置識別碼
$	用於 MDM 的識別碼
$	MEID
$	模型
$	裝置名稱
$	裝置電話號碼
$	叢集唯一裝置識別碼
$	序號
$	iOS UDID
$	Wi-Fi MAC 位址
	電話號碼 2
	ICCID 2

當您建立自訂屬性並在受管理應用程式組態中參照此屬性時，如果該屬性值已更新，則受管理應用程式組態內所參照的屬性也會隨之更新，而且受管理應用程式組態將被重新推送至裝置。

「自訂」或「裝置」屬性完成更新，且組態推送至裝置後，也應一併更新 Android Kiosk 品牌組態。

應用程式屬性

使用應用程式屬性指定與應用程式有關的資訊並建立自訂應用程式群組。

金鑰	描述
$	已將日期應用程式新增至 AppCatalog
$	應用程式名稱
$	應用程式作業系統
$	應用程式套組或套件 ID
$	說明應用程式的匯入來源
$	說明 iOS 或 macOS 應用程式是否為 VPP

電子郵件範本屬性

金鑰	描述
$	電子郵件正文
$	電子郵件主旨

時間戳記屬性

變數金鑰	描述
$	目前時間戳記 (自該時期起以毫秒計)

原則範本屬性

金鑰	描述
$	原則名稱已違規
$	傳送訊息後要採取的下一個階層式合規行動 (不同於等待和淘汰)
$	裝置處於不符合規範狀態的天數
$	首次觸發違反原則的時間戳記 (UTC DD-MM-YYYY 格式)
$	規則定義 (查詢字串現在顯示的方式)

相關主題：

- 指派自訂屬性給使用者
- 指派自訂屬性給裝置
- 移除使用者的自訂屬性
- 移除裝置的自訂屬性
- 變數

12.1.2. 裝置清理設定

裝置清理能實現未使用裝置的裝置生命週期自動化管理。 您可將已達到指定失聯天數的裝置淘汰。 您可將已達到指定淘汰天數的裝置刪除。 「稽核追蹤」頁面擷取「淘汰裝置」、「刪除裝置」和「刪除已抹除裝置」設定。

下表提供了有關支援裝置清理設定的 Android 裝置資訊:

模式	不合規即淘汰	刪除已淘汰	強制淘汰或淘汰擱置中	刪除已抹除	刪除抹除擱置中
Android 工作設定檔 (設定檔擁有者)	是	是	是	否	否
裝置管理/ 公司擁有裝置上的工作設定檔	是	是	是	是	是
工作受管理裝置 / 具有工作設定檔的 Android 受管理裝置	否	否	否	是	是

必要條件

您必須具備系統管理角色權限才能存取此設定。

淘汰裝置

程序

1.	前往**管理員 > 系統 > 裝置清理**。 「裝置清理」頁面隨即開啟。
2.	選取**淘汰裝置**。
3.	使用**淘汰裝置**表格來指定詳細資訊。
4.	按一下**顯示未簽入的裝置清單**。 顯示在指定天數內未簽入的裝置清單。
5.	按一下**立即淘汰裝置**，或者可以安排裝置的淘汰時間。
6.	Ivanti Neurons for MDM 管理入口網站將淘汰指定的裝置。
7.	按一下**儲存**以儲存您的設定。
8.	(選用) 如果您已更新值，可以按一下**重設**，將設定重設為初始設定。

淘汰裝置

欄位	描述
選取平台	選取應套用裝置清理設定的所需平台。 此選項目前僅適用於**淘汰裝置**和**淘汰待淘汰裝置**設定。
淘汰指定時間後尚未簽入的裝置 (依天數計)	天數: 預設值為 30 天，天數上限為 365 天。
每個工作階段可淘汰的裝置數量上限	選取 100、500 或 1000 (預設值 - 100)。
按排程自動淘汰裝置	選取核取方塊，根據預設排程淘汰裝置。
淘汰排程組態	選取下列其中一個選項設定淘汰頻率: • **每日 -** 設定為每天淘汰裝置。 • **每週 -** 指定一周中具體在星期幾安排淘汰。 • **每月 -** 設定為每個月的第一天淘汰裝置。

刪除已淘汰裝置

程序

1. 前往**管理員** > **系統** > **裝置清理**。 「裝置清理」頁面隨即開啟。
2. 選取**刪除已淘汰裝置**。
3. 使用**刪除已淘汰裝置**表格來指定詳細資料。
4. 按一下**顯示已淘汰裝置清單**。 顯示在指定天數內淘汰的裝置清單。
5. 按一下**立即刪除已淘汰裝置**，或者可以安排裝置的刪除時間。
6. Ivanti Neurons for MDM 管理入口網站將刪除指定的裝置。
7. 按一下**儲存**，儲存您的設定。
8. (選用) 如果您已更新值，可以按一下**重設**，將設定重設為初始設定。

刪除已淘汰裝置

欄位	描述
刪除遭淘汰時長已超過以下時間 (天數) 的裝置	天數: 預設值為 30 天，天數上限為 365 天。
每個工作階段可刪除的已淘汰裝置數量上限	選取 100、500 或 1000 (預設值 - 100)
按排程自動刪除已淘汰的裝置	選取核取方塊，根據預設排程淘汰裝置。
刪除排程組態	選取下列其中一個選項設定刪除頻率: • **每日 -** 設定為每天刪除裝置。 • **每週 -** 指定一周中具體在星期幾安排刪除。 • **每月 -** 設定為每個月的第一天刪除已淘汰裝置。

刪除已抹除裝置

程序

1. 前往**管理員** > **系統** > **裝置清理**。 「裝置清理」頁面隨即開啟。
2. 選取**刪除已抹除裝置**。
3. 使用**刪除已抹除裝置**表格來指定詳細資料。
4. 按一下**顯示已抹除裝置清單**。 顯示在指定天數內淘汰的裝置清單。
5. 按一下**立即刪除已抹除裝置**，或者可以安排已抹除裝置的刪除時間。
6. Ivanti Neurons for MDM 管理入口網站將刪除指定的裝置。
7. 按一下**儲存**以儲存您的設定。
8. (選用) 如果您已更新值，可以按一下**重設**，將設定重設為初始設定。

刪除已抹除裝置

欄位	描述
刪除抹除時長超過以下時間的裝置 (依天數計)	天數: 預設值為 30 天，天數上限為 365 天。
每個工作階段可刪除的已抹除裝置數量上限	選取 100、500 或 1000 (預設值 - 100)
按排程自動刪除已抹除裝置	選取核取方塊，根據預設排程刪除已抹除的裝置。
刪除已抹除排程組態	選取下列其中一個選項設定刪除頻率: • **每日 -** 設定為每天刪除已抹除的裝置。 • **每週 -** 指定一周中具體在星期幾安排刪除。 • **每月 -** 設定為每個月的第一天刪除已抹除的裝置。

刪除抹除擱置中的裝置

程序

1. 前往**管理員** > **系統** > **裝置清理**。 「裝置清理」頁面隨即開啟。
2. 選取**刪除抹除擱置中的裝置**。
3. 使用**刪除抹除擱置中的裝置**表格來指定詳細資料。
4. 按一下**顯示抹除擱置中的裝置清單**。 顯示要在指定天數內抹除的裝置清單。
5. 按一下**立即刪除抹除擱置中的裝置**，或者可以安排擱置中裝置的刪除時間。
6. Ivanti Neurons for MDM 管理入口網站將刪除指定的裝置。
7. 按一下**儲存**以儲存您的設定。
8. (選用) 如果您已更新值，可以按一下**重設**，將設定重設為初始設定。

刪除抹除擱置中的裝置

欄位	描述
刪除抹除擱置超過以下時間的裝置 (依天數計)	天數: 預設值為 30 天，天數上限為 365 天。
每個工作階段可刪除的抹除擱置中的裝置數量上限	選取 100、500 或 1000 (預設值 - 100)
按排程自動刪除抹除擱置中的裝置	選取核取方塊，根據預設排程刪除已抹除的裝置。
刪除抹除擱置排程組態	選取下列其中一個選項設定刪除頻率: • **每日 -** 設定為每天刪除抹除擱置中的裝置。 • **每週 -** 指定一周中具體在星期幾安排刪除。 • **每月 -** 設定為每個月的第一天刪除抹除擱置中的裝置。

淘汰停用擱置中的裝置

程序

1. 前往**管理員** > **系統** > **裝置清理**。 「裝置清理」頁面隨即開啟。
2. 選取**淘汰停用擱置中的裝置**。
3. 使用**淘汰停用擱置中的裝置**表格來指定詳細資料。
4. 按一下**顯示停用擱置中的裝置清單**。 顯示要在指定天數內淘汰的裝置清單。
5. 按一下**立即淘汰停用擱置中的裝置**，或者可以安排擱置中裝置的淘汰時間。
6. Ivanti Neurons for MDM 管理入口網站將淘汰指定的裝置。
7. 按一下**儲存**以儲存您的設定。
8. (選用) 如果您已更新值，可以按一下**重設**，將設定重設為初始設定。

淘汰停用擱置中的裝置

欄位	描述
淘汰指定時間後尚未簽入的停用擱置中裝置 (依天數計)	天數: 預設值為 30 天，天數上限為 365 天。
每個工作階段可淘汰的停用擱置中的裝置數量上限	選取 100、500 或 1000 (預設值 - 100)
按排程自動淘汰停用擱置中的裝置	選取核取方塊，根據預設排排淘汰停用擱置中的裝置。
淘汰停用擱置中排程組態	選取下列其中一個選項設定刪除頻率: • **每日 -** 設定為每天淘汰擱置中的裝置。 • **每週 -** 指定一週中具體在星期幾安排淘汰擱置中的裝置。 • **每月 -** 設定為每個月的第一天淘汰擱置中的裝置。

當裝置已淘汰，而且如果簽入發生在很久之前，則將僅考慮上次簽入時間來確定裝置刪除。 例如，如果裝置上次在 30 天內簽入，且裝置目前已淘汰 (可能是由於「停用超過 (天數) 未簽入的裝置」選項)，而且如果「刪除已淘汰超過 (天數) 的裝置」設為 30 天，則一旦「刪除淘汰裝置」工作執行，裝置就會立即被刪除。

12.1.3. GDPR 設定檔

Ivanti Neurons for MDM 管理入口網站目前包含 GDPR 設定檔頁面，可讓您將 GDPR 設定檔指派至使用者群組。 您可以將 GDPR 設定檔僅指派至使用者群組而非個別使用者。

注意以下幾點:

- 您必須先啟用 GDPR 設定檔才能將其指派至特定使用者群組。
- 若您停用 GDPR 設定檔，它將會關閉所有已指派至使用者群組的設定檔限制。
- 在啟用 GDPR 設定檔後，某些欄位的編輯功能將會受到限制或停用。

在 GDPR 設定檔指派後隱藏的欄位

若使用者具有 GDPR 設定檔，則 Ivanti Neurons for MDM 在顯示使用者相關資訊時會依預設隱藏下列欄位:

- **使用者 ID**
- **使用者名稱**
- **電子郵件地址**
- **序號**
- **ICCID**
- **IMSI**
- **MEID**
- **IP 位址**
- **電話號碼**
- **IMEI**
- **eSIM 識別碼**
- **定位**

如果將位置新增至 GDPR 設定檔中，則獲指派 GDPR 設定檔的使用者的裝置詳細資料中將遮罩上次定位的裝置位置欄位、緯度和經度。

啟用 GDPR 設定檔

您可以啟用 GDPR 設定檔並選取必須在 Ivanti Neurons for MDM 管理入口網站和裝置中隱藏的特定欄位。

Procedure程序

	1.	登入 Ivanti Neurons for MDM 管理入口網站。
2.		前往管理 > 系統 > GDPR 設定檔。
	3.	按一下啟用。
	4.	按一下編輯 (鉛筆) 圖示。

	5.	選取必須隱藏的欄位。

	6.	按一下**儲存**。 選取的欄位將被遮罩且不會顯示特定使用者的值。

指派 GDPR 設定檔給使用者群組

啟用 GDPR 設定檔後，您便能將其指派至特定使用者群組。

Procedure程序

	1.	登入 Ivanti Neurons for MDM 管理入口網站。

	2.	前往**使用者** > **使用者群組**。

3.	在清單中選取一個使用者群組。

	4.	按一下**動作**下拉式清單，並選取**指派 GDPR 設定檔**。 GDPR 設定檔會被指派至該特定群組的所有使用者，且所有選取的值都將被遮罩而無法在管理入口網站和使用者裝置中檢視。 由於管理員也位於「所有使用者」群組中，因此切勿將 GDPR 設定檔指派至「所有使用者」群組。

12.1.4. 通知電子郵件

授權： Silver

您可以根據通知的嚴重性層級來設定應接收電子郵件通知之使用者的電子郵件地址清單。

通知電子郵件功能為選用性，您可以視需要開啟或關閉該功能。 不過，指派系統管理角色給您，是使用此功能的必要條件。

1. 選取**管理 > 系統 > 通知電子郵件**。 **通知電子郵件**頁面隨即顯示。
2. 在通知電子郵件設定區段中，按一下**開**以啟用通知電子郵件功能。
3. 按一下**新增收件者**。 **新增收件者**快顯視窗隨即顯示。
4. 在**新增收件者**快顯視窗中，更新下列欄位：
    - 收件者電子郵件 ID - 輸入要傳送通知的收件者電子郵件。
    - 要傳送的通知類型 - 藉由選擇勾選框來選擇通知類型。 以下是通知類型選項：**重要通知**、**警告通知**、**資訊通知**。
5. 按一下**確定**。 設定的詳細資料隨即顯示在表格中。
6. 按一下**儲存**以套用變更。

12.1.5. 角色管理

角色是套裝的權限群組，目的是授予一組權限給管理使用者，同時將他們的存取權限制在控制特定領域的功能。 Ivanti Neurons for MDM 提供一組可供指派 (或編輯) 的系統角色，以及一個用來建立自訂角色的功能。 您可以基於類別搜尋特定權限，而且將會顯示使用者介面中與特定角色或權限相關的所有選項。 針對新增為相依權限的權限會顯示工具提示。

> 針對同時有權存取 Ivanti Neurons for UEM 和 Ivanti Neurons for MDM 的融合租用戶，會對其隱藏「角色管理」頁面及相關選項。

由於有兩種權限可用，所以有兩種角色：

- **空間專用角色** - 這類權限為空間專用，因此僅適用於特定空間。 範例包括空間中的裝置管理、App 管理。
- **跨空間角色**- 這類權限本質上就適用於所有角色。 範例包括租戶層級設定，例如 MDM 憑證、App Catalog 設定。

建立自訂角色

您可以建立自訂跨空間或空間專用角色。 當您選擇某個權限，系統會自動選擇相依權限。 因此，獲得自訂角色指派的使用者，當他們造訪「裝置」頁面或「裝置詳細資料」頁面時，只能執行特定動作 (例如淘汰、清除)。

套用「檢視使用者註冊 PIN」自訂角色時，使用者可以檢視具有相同存取層級或較低權限的其他使用者的 PIN，並且使用者不可為其他使用者建立 PIN。

> 無法自動指派剛建立的自訂角色給任何人。 超級租戶管理員需要將它指派給所需的管理員使用者，之後該使用者可視需要指派相同的角色給其他使用者。

程序

1. 前往**管理** > **角色管理**。
2. 按一下 **+新增自訂角色**。
3. 在**建立角色**頁面中，輸入新角色的**名稱**。
4. (選用) 新增新角色的說明。
5. 在**角色類型**下，選擇下列其中一個角色類型:
    - **跨空間角色**
    - **空間專用角色**
6. 在**權限**下，選擇所需的細微權限。
7. 有關管理員和使用者權限，請參見下表。
   按一下**儲存**。

以下表格列出可供您用來建立自訂角色的權限、角色和屬性:

角色類型	權限類別	精細權限
跨空間角色 **管理**		
	管理自訂屬性	• 新增自訂屬性 • 刪除自訂屬性 • 編輯自訂屬性 • 檢視自訂屬性
	支援管理員	• 新增管理員指南 • 刪除管理員指南 • 停用管理員指南 • 檢視 Support Admin 與顯示登入歷程記錄
	憑證授權中心	• 新增憑證授權中心 • 刪除憑證授權中心
	連接器	• 新增 Connector 日誌 • 刪除連接器記錄 • 檢視 Connector • 更新 Connector
	LDAP 管理	• 新增使用者/群組/OU • 新增伺服器 • 瀏覽伺服器 • 刪除伺服器 • 搜尋伺服器 • 同步伺服器 • 移除使用者/群組/OU • 檢視伺服器 本區段中的所有 LDAP 權限都需要有檢視 Connector 權限。 當您選取這些 LDAP 權限中的任一個時，將會在 Connector 區段中自動選取。
	授權管理	檢視授權
	管理應用程式發佈	**更新應用程式發佈** 在**管理應用程式發佈**下，**更新應用程式發佈**權限現在可用於自訂角色。 具有系統管理角色的使用者預設會自動收到此權限。 現在，應用程式發佈頁面包含**允許空間管理員編輯發佈**核取方塊，它預設針對新應用程式版本啟用。 已指派自訂角色 (具有此新權限) 的使用者，以及具有應用程式管理角色 (無系統管理存取權限) 的使

角色類型	權限類別	精細權限
		用者，可以修改此設定。 對於每個應用程式版本，鎖定應用程式發佈設定可用性會顯示在發佈頁面上，而且所有縮減範圍嘗試現在都會擷取在稽核跟蹤內。
使用者		
	使用者管理動作	• 檢視使用者 • 更新使用者 • 傳送訊息給使用者 • 附加/指派角色給使用者 • 建立使用者 • 刪除使用者 • 邀請使用者 • 檢視使用者註冊 PIN 碼
	指派自訂使用者屬性	• 刪除屬性 • 檢視屬性 • 新增/編輯屬性
	使用者群組	• 檢視使用者群組 • 編輯使用者群組 • 附加/指派角色給使用者群組 • 建立使用者群組 • 刪除使用者群組
	報告管理	• 建立報告 • 編輯報告 • 執行報告 • 刪除報告記錄 • 檢視報告 • 刪除報告 • 下載報告記錄
裝置中的下列目錄來判斷隱私權配置是否適用於屬意裝置		
	大量註冊	• 建立大量註冊 • 更新大量註冊

角色類型	權限類別	精細權限
空間專用角色		• 將使用者指派至大量註冊 • 檢視大量註冊 • 刪除大量註冊
裝置中的下列目錄來判斷隱私權配置是否適用於屬意裝置		
	裝置動作	• 指派裝置給使用者 • 清除裝置啟用鎖定 • 刪除裝置 • 停用裝置遺失模式 • 啟用裝置遺失模式 • 裝置強制登記 • 鎖定裝置 • 解鎖裝置 • 裝置強制登出 • 重新安裝裝置系統 App • 重新啟動裝置 • 排程 iOS 裝置更新 • 放棄裝置擁有權 • 淘汰裝置 • 取消淘汰裝置 • 關閉裝置 • 檢視裝置 • 抹除裝置 • 取消抹除裝置 • 更新裝置作業系統版本 • 透過上傳進行大量指派 • 啟動 TeamViewer 工作階段 • 進入單一應用模式 • 退出單一應用模式
	指派自訂	• 新增/編輯裝置自訂屬性

角色類型	權限類別	精細權限
	裝置屬性	• 刪除裝置自訂屬性 • 檢視使用者自訂屬性 本區段中的所有指派自訂裝置屬性權限都需要裝置讀取權限。 當您選取這些指派自訂裝置屬性權限中的任一個時，將會在裝置動作區段中自動選取。
	裝置配置	• 排除描述檔 • 推送描述檔 • 推送排除的描述檔 • 發生錯誤時重試安裝
	裝置群組	• 新增裝置群組 • 刪除裝置群組 • 編輯裝置群組 • 檢視裝置群組
	大量註冊	• 建立大量註冊 • 更新大量註冊 • 將使用者指派至大量註冊 • 檢視大量註冊 • 刪除大量註冊
	App 庫存	• 檢視 App 庫存
配置		
	配置	• 檢視/匯出配置 • 編輯/優先排序配置 • 新增/複製配置 • 刪除配置
原則		
	原則	• 檢視原則 • 編輯/優先排序原則 • 新增/複製原則 • 刪除原則

若要編輯此角色，請前往「管理，角色管理」頁面，對此角色的名稱按一下**動作**下的編輯圖示。 使用者無法將跨空間角色編輯為空間專用角色，反過來也一樣。

相關主題:

- 若要指派自訂角色給使用者，請參閱**指派角色**。
- 請參閱**使用者角色**以檢視預設角色清單。
- **使用自訂報告**
- **使用排程報告**

12.1.6. 空間

本節包含以下各主題：

- 空間
- 管理空間
- 空間範例
- 委派裝置
- 委派 App

12.1.6.1. 空間

授權： Silver

空間可用來將統合端點管理 (UEM) 系統分隔成多重獨立受管理實體，以便進行委派管理。 空間可以建立用來反映組織階層。 Ivanti Neurons for MDM 支援使用中央管理實體 (稱為預設空間) 及多個次級管理實體 (稱為委派空間) 進行單級委派。 每個 UEM 系統在建立時都具有一個預設空間。

> 針對同時有權存取 Ivanti Neurons for UEM 和 Ivanti Neurons for MDM 的融合租用戶，會對其隱藏「空間」頁面及相關選項。

空間可用於下列系統元件的委派管理。 目前無法委派使用者和使用者群組。

- 裝置
- 組態
- 政策
- 裝置群組
- 應用程式
- App Catalog
- Apple Apps and Books 權杖

當管理員登入至少擁有一個委派空間的租戶的 Ivanti Neurons for MDM 管理入口網站時，管理入口網站的登入提示蹦現視窗中將會顯示該管理員。 如果已建立過任何委派空間，則在委派空間建立後與使用者登入時將不會顯示提示蹦現視窗。

全域與委派空間管理員角色

擁有適當角色可存取預設空間的管理使用者稱為全域管理員。 預設空間的存取權可以是唯讀或讀寫。 擁有適當管理角色的全域管理員可建立委派空間，並指派委派管理員來管理它們。 可指派委派管理員來管理一或多個委派空間。

指定管理員可存取的空間會列在「裝置」和「App」索引標籤中左上角的空間選擇器下拉清單中。 若要檢視與管理空間，請使用空間下拉清單來切換到所需空間。

除了預設空間之外，全域管理員還可檢視與控制所有的委派空間。 委派管理員只能檢視與控制全域管理員指派給他們的空間。 全域管理員維持中央控制委派空間，而委派管理員擁有自主權可管理已委派給他們的空間。 此自主權層級由委派是否沿用或複製自預設空間。

下列為不同使用者角色以及他們可執行的任務：

委派空間中的沿用 app

- 委派時的現有評等或評論會被沿用，使用者可在委派空間中查看這些資訊，包括作者使用者名稱。
- 委派管理員無法刪除沿用 app 的評等/評論。
- 委派管理員可將沿用 app 的評等/評論匯出。
- 委派空間中的使用者可以新增評等/評論至沿用的 app。
- 委派空間中的使用者可以檢視由委派空間中的使用者所新增的評等/評論，包括作者使用者名稱。

委派空間中的 app (新增，非沿用的)，

- 只有全域管理員可以從 **App > 目錄設定 > 評等與評論**啟用或停用評論。

- 委派空間中的使用者可以新增評等/評論。
- 委派管理員可以刪除由相同委派空間中的使用者所新增的評論。
- 其他委派空間 (包括預設空間) 中的使用者，無法檢視由每個委派空間中的使用者所新增的評等或評論。
- 委派管理員可以匯出由所有使用者所新增的評論，包括使用者名稱。

預設空間中的委派 app

- 全域管理員可以刪除由委派空間中的使用者所新增的評等或評論。
- 全域管理員可以匯出所有評等或評論，包括那些由委派空間中的使用者所新增的。
- 委派空間中的使用者可以檢視由委派空間中的使用者所新增的評等/評論，包括使用者名稱。

委派空間的優先順序

UEM 系統中的預設空間一律擁有最低的優先順序。 委派空間與其他委派空間之間的相對優先順序是由全域管理員所設定，而且可隨時變更。委派空間的等級順序列在管理入口網站中「管理」索引標籤下的空間頁面，從最高到最低的優先順序。

透過沿用或複製委派

委派管理中的關鍵概念之一是系統元件是否沿用或複製自預設空間。

12.1.6.2. 管理空間

空間可讓您將裝置群組指派給不同管理員來管理 (委派管理)。 空間管理員可定義{{配置}}和{{原則}}，以便套用到空間當中的裝置上。 建立空間後，您可將每個空間指派給相關或適當的管理員。

此空間頁面包括:

- 搜尋功能，用於快速尋找空間。
- 分頁控制項，用於瀏覽大量空間。
- 空間優先順序控制項，用於管理委派的空間順序。
- 選取和刪除多個空格的選項。

> 預設空間無法刪除。

- 按字母順序排序空間。
- 空間選取器中最近檢視的空間清單。
- 在裝置、組態、原則和內容頁面上持續選取空間，減少在頁面之間瀏覽時重新選取空間的需求。

> 使用者只能檢視受指派的空間，無法檢視所有可用空間。 目前為止，此設定僅適用於**裝置**、**裝置群組**、**應用程式**、**應用程式詳細目錄**、**內容**、**組態**、**原則**及**憑證管理**模組。 在檢視上述任何模組時從「空間清單」選取的空間，會另存為管理員對該模組偏好的預設選擇項目。 不僅會對目前的登入工作階段儲存這些偏好設定，未來工作階段也適用。

您所建立的空間會沿用預設空間的所有配置。 因此，您之後於預設空間中建立的所有配置都可套用至其他空間。 不過，如果是對現有配置的變更就不會受到沿用。

您所建立的空間僅會接收當下預設空間中已存在的原則複本。 您之後於預設空間中建立的任何原則都只會套用至預設空間。

建立規則以定義空間中要有哪些裝置。 這些規則可使用適用的運算子進行篩選，包括「開頭是」、「結尾是」、「包含」、「不包含」、「開頭不是」、「結尾不是」、「小於」、「大於」、「範圍」、「等於」及「不等於」運算子。 這些規則可以用「任何 (或)」或「所有 (及)」選項來建立巢狀結構。 規則的正確性可透過出現在規則結尾的文字進行檢查。

在規則建立器中選取「使用者群組名稱」屬性後，Ivanti Neurons for MDM 管理入口網站會顯示重複的使用者群組數量及對應的 GUID 數量，以識別重複的群組。 此外，此規則之下的表格會顯示重複使用者群組的清單以及其詳細資訊，例如使用者群組名稱、GUID、來源和可分辨的名稱 (DN)。

規則可根據下列項目識別裝置：

- 已註冊 Entra ID
- 支援 APNS
- 替代序號 (僅限 Android - 適用於處於「裝置管理」或「裝置擁有者」模式的 Samsung 裝置)
- Android 5G 網路分段已啟用
- Android 工作受控裝置非 GMS 模式 (AOSP) 已啟用
- Android 專用裝置
- 支援 Android Enterprise
- 搭配工作描述檔的 Android 受管理裝置
- Android SafetyNet Attestation 類型

- Android Work 啟用
- Android 安全性修補程式層級 (Android 裝置)
- 已啟用 Android 受工作管理的裝置 (裝置擁有者)
- Android 工作設定檔已啟用
- 公司擁有的裝置上的 Android 工作設定檔已啟用
- 防網路釣魚原生狀態
- 防網路釣魚狀態
- 防網路釣魚 VPN 狀態
- 已註冊自動化 Device Enrollment
- 已啟用自動化 Device Enrollment
- 已註冊 Autopilot
- Azure 用戶端狀態代碼
- Azure 裝置相符性報告時間
- Azure 裝置合規性狀態
- Azure 裝置識別碼
- Sentry 已封鎖
- Access 已封鎖
- 可用的啟動程序權杖
- 大量佈建的類型 (Apple Configurator 或無)
- 電信業者
- 用戶端上一次登記
- 已註冊的用戶端
- 相符性
- 合規性動作已封鎖
- 目前的國家/地區名稱 (從下拉式清單中，選取目前的國家/地區名稱)
- 目前的 MCC
- 目前的 MNC
- 自訂裝置屬性
- 自訂 LDAP 屬性
- 自訂使用者屬性
- 數據漫遊
- 裝置來源
- 裝置類型
- 裝置類型 (Apple)
- 顯示名稱
- 加密已啟用
- 住家所在國家/地區名稱 (從下拉式清單中，選取住家所在國家/地區名稱)

- 歸屬 MCC
- 歸屬 MNC
- IMEI
- IMEI2 (僅適用於具有雙 SIM 卡插槽的 Android 裝置，並且裝置必須為 Android 8.0 或更高版本)
- 機構復原金鑰已啟用
- IP 位址
- 單一應用模式
- 上一次登入
- 啟用遺失模式
- 僅限 MAM
- 製造商
- MTD 啟用狀態
- 多位使用者模式
- 作業系統
- 作業系統版本
- 作業系統及版本
- 擁有權
- 個人復原金鑰已啟用
- 電話號碼
- 已隔離
- 已啟用復原鎖定
- 漫遊
- 安全 App 狀態
- 序號
- 狀態
- 受監管
- 補充建置版本
- 補充作業系統/版本額外資訊
- 可用的解除鎖定權杖 (iOS)
- 已使用者註冊
- 使用者群組
- 使用者名稱
- 語音漫遊
- macOS 個人復原金鑰已委付
- macOS 復原金鑰類型

> 這些規則僅適用於**銀級**授權與更高級授權。

建立空間

程序

1. 前往**管理員** > **系統** > **空間**。
2. 按一下**建立空間**。
3. 輸入空間名稱。
4. 為空間設定適當的規則和設定。
5. 按一下**儲存**。

優先排序空間

Ivanti Neurons for MDM 以出現順序評估空間。

程序

1. 按一下**為空間劃分優先順序**。
2. 選取空間旁的向上或向下圖示，以調整其優先順序。
3. 按一下**儲存**。

刪除空間

1. 前往**管理員** > **系統** > **空間**。
2. 使用核取方塊選取一個或多個空間。
3. 按一下**刪除**。 出現提示時確認刪除

指派管理員給空間

程序

1. 前往**使用者**。
2. 搜尋將成為管理員的使用者。
3. 按一下使用者的連結，即可顯示詳細資料。
4. 選取**動作** > **指派角色**。
5. 選擇**裝置管理**。
6. 在**裝置管理**下方，選擇此管理員的空間。
7. 按一下**完成**。

當此管理員登入時，就只能看到指派空間中的裝置、配置與原則。

複製配置或原則

您可以複製配置或原則 (如果您需要複製並做些微修改)。 您也可以將複製的配置或原則關聯至不同的裝置群組。 在空間中可複製所有原則。 除了使用者提供的身份認證和威脅防護，空間中的所有配置都可複製。 下列配置還可以從預設空間複製到其他空間：

- iOS 限制
- Web Clip

- 認證
- 密碼
- SCEP (iOS 及 Windows)
- 身分認證 (動態產生)

- 空間中的配置或原則類型名稱不應重複。 配置或原則的所有其他屬性都可以複製。
- 配置將複製到您 (即管理員) 有權存取的所有空間中。 即使您不是全域管理員也可以複製配置。

程序

1. 前往您想複製的**配置**或**原則**。
2. 按一下配置或原則的連結以顯示詳細資料。
3. 按一下**複製**圖示。
4. 在蹦現視窗中輸入**名稱**，並選擇性輸入**描述**。
5. 按**下一步**。
6. 按您的需求修改配置或原則。
7. 按**下一步**。
8. 設定發佈。
9. 按一下**完成**。

如需更多資訊，請參閱空間範例。

12.1.6.3. 空間範例

本主題提供有關管理員可以如何使用空間的範例。

依據位置設定專屬的管理員

ACME, Inc. 在北美和歐洲設有辦公室。 由於語言和時區問題，ACME 希望由美國的管理員來管理北美洲的裝置，而由德國的管理員負責管理歐洲的裝置。

為了設定這些空間，ACME 進行了下列變更：

1. 已針對歐洲地區的使用者建立 Ivanti Neurons for MDM 的使用者群組。
2. 在 Ivanti Neurons for MDM 中為北美使用者建立使用者群組。
3. 使用下列規則建立歐洲空間：
4. 使用者群組 = 歐洲
   使用下列規則建立北美洲空間：
5. 使用者群組 = 北美
   針對每個空間，皆指派裝置管理角色給適當的管理員。

現在，ACME 就具備了下列空間：

- 歐洲
- 北美
- 預設

依據位置與作業系統設定專屬的管理員

ACME 決定 Android 裝置應該讓 Android 專業人員來管理。 因此，公司在北美洲的組織和歐洲組織都各新增一名 Android 專業人員。 這樣一來，也需要兩個新的空間。

為了新增空間，ACME 進行了下列變更：

1. 使用下列規則建立歐洲的 Android 空間：
2. 使用者群組 = 歐洲
   作業系統 = Android
   使用下列規則建立北美洲的 Android 空間：
3. 使用者群組 = 北美
   作業系統 = Android
   針對每個空間，皆指派裝置管理角色給適當的管理員。

現在，ACME 就具備了下列空間：

- 歐洲–Android
- 北美–Android
- 歐洲
- 北美
- 預設

主管管理員

ACME 的主管們決定要一位特殊的管理員來提供特別的服務。 只有最重要的主管榜上有名。

為了新增這個空間，ACME 進行了下列變更：

1. 使用下列規則建立主管空間：
2. Username = jdoe@acme.com
   Username = gkunz@acme.com
   Username = prizzo@acme.com
   Username = fvanhoff@acme.com
   將空間移到**空間**頁面的清單頂端。
3. 不然的話，具備 Android 裝置的主管就會被歸給錯誤的管理員。
   針對該空間，指派裝置管理角色給特殊的管理員。

現在，ACME 就具備了下列空間：

- 高階主管
- 歐洲–Android
- 北美–Android
- 歐洲
- 北美
- 預設

所有其他裝置的管理員

當 ACME 在日本新開一家辦事處時，只要沒有新建日本空間，新增的裝置都會指派給預設空間的管理員。

12.1.6.4. 委派裝置

空間用來將您的裝置區隔為獨立受管理的實體。 空間的成員關係是由您建立的規則來決定。 裝置委派可讓全域管理員分割與獨立管理 UEM 系統中的裝置。 當裝置受到委派時，那些裝置的存取權可指派給一組委派管理員子集，從而發佈管理責任。

委派裝置可組成裝置群組，套用不同的自訂配置，但不影響預設空間或其他空間中的裝置。

建立委派裝置的規則

您為空間所定義的規則會決定哪些裝置屬於該空間。 裝置有可能僅屬於一個空間。 如果裝置不符合您所建立的空間規則，則會自動歸屬到預設空間。

1. 如果符合任一規則的裝置都可列入此項定義中，請選擇**任一**。
2. 如果符合所有規則的裝置才可列入此項定義中，請選擇**全部**。
3. 從下拉清單中選擇其中一項規則類型：
    - **自訂 LDAP 屬性：**適用於建基於 LDAP 屬性的規則。
    - **作業系統**：依據裝置作業系統而定的規則。
    - **使用者群組**：依據裝置使用者群組而定的規則 (如裝置管理服務中所定義)。
    - **使用者名稱**：依據裝置相關聯之使用者名稱而定的規則。
4. 定義所選規則類型的準則：
    - **自訂 LDAP 屬性：**針對在 LDSP 設定中設好的自訂 LDAP 屬性輸入名稱。
    - **作業系統**：選擇 Android、 iOS、macOS 或 Windows。
    - **使用者群組**：選擇下拉清單中顯示的其中一個使用者群組。 這些使用者群組都是在**使用者 > 使用者群組**。
    - **使用者名稱**：輸入使用者名稱。
5. 若要針對此空間新增其他原則，請按一下上一個規則旁的 +。
6. 按一下**預覽**，即可查看哪些裝置會指派至該空間。
7. 當空間中的裝置滿足需求時，按一下**儲存**。

如果裝置不再符合某空間的原則，就會將其自動移至下一個符合的空間中。 如果裝置不符合現有空間的原則，就會將裝置移至預設空間。 例如，若將使用者從使用者群組中移除，可能導致該使用者的裝置被移至不同的空間。 如果移動到不同的空間，可能會導致原則和配置有所變更。

12.1.6.5. 委派 App

應用程式委派可讓全域管理員分割與獨立管理 Ivanti Neurons for MDM 系統中的應用程式。 全域管理員可以集中取得來源與發佈公開和內部 app，同時維護委派空間所提供的區隔和控制。

全域管理員可藉由集中發佈 app，透過 app 配置和 app 的發佈規則來預先定義 app 的管理行為。 接著可在委派空間的 App Catalog 中進行委派與提供使用。

然後委派 app 可發佈給指定委派空間當中的使用者。 當應用程式受到委派時，那些應用程式的存取權可指派給一組委派管理員子集，從而發佈管理責任。

App 委派需要先定義一或多個委派空間。 當應用程式受到委派時，會將其指派給所有空間。 App 委派空間會分成：

- 預設空間
- 委派空間

新增 app 至委派空間

應用程式可由委派或全域管理員新增至委派空間。 此 app 僅出現在獲得新增之委派空間的 App Catalog 中。 如果您將之前委派的 app 從預設空間新增至委派空間，將會導致錯誤發生。 在這種狀況下，您必須先在預設空間中停用 app 沿用，然後才能將 app 新增至委派空間。 如需更多資訊，請參閱使用配置中的**新增配置**。

委派空間中的 app 發佈

從預設空間委派 app 時，其發佈規則為沿用。 此 app 裝置將發佈至指派給委派空間且符合 app 發佈規則的所有裝置。

全域管理員可委派空間管理員，針對所有裝置和自訂發佈選項編輯動態產生的身分憑證。

> 發佈變更僅適用於特定空間。 所有其他空間會繼承預設空間發佈設定。

> Android 應用程式的應用程式審核設定: 不支援針對 Android 應用程式的每個空間進行應用程式審核設定。 自訂空間中核准的應用程式在所有空間中生效。

> 現有 Android 目錄應用程式: 在已在預設空間中新增公用 Android 應用程式的租用戶上，需要取消委派應用程式，然後才能將該公用應用程式新增至另一個非預設空間中。

> Android Enterprise 應用程式只能由租用戶層級管理員新增，**不能**由空間層級管理員新增。 受管理的 Google Play 是在組織層級設定，而不是依照委派空間。 因此，新的 Android Enterprise 應用程式只能在預設空間中核准。 委派管理員可以在自己的空間內指派和管理已核准的應用程式，但無法在委派空間內核准或新增新的 Android Enterprise 應用程式。 所有新的應用程式必須先在預設空間中得到核准，然後才能指派至適當的群組。

如需更多資訊，請參閱使用配置中的**新增配置**。

12.1.7. 支援管理員

建立暫時的 Support Administrator 可讓服務支援團隊使用您的角色和權限來登入。 這個使用者會自動在 7 天後過期，您也可以隨時終止存取權。 建立 Support Administrator 可讓支援團隊更輕鬆進行問題的疑難排解。

建立支援管理者

程序

1. 在 **Support Administrators** 頁面中，按一下**新增 Support User**。
2. 按一下**建立使用者**以確認。

此步驟會傳送一封電子郵件給裝置管理服務支援團隊。

> 支援團隊成員啟用新帳戶前，**顯示名稱**欄位顯示「(停用)」。 產生的顯示名稱格式如下：

support-[random_ID]-[your_username]@[your_company].com

建立好支援管理者之後，選擇**管理 > 支援管理者**即可讓您直接前往現有支援管理者的清單。 因此，如果您要建立其他 Support User，請直接前往上述的步驟 2。

> 預設情況下，新建立的支援管理員帳戶為唯讀。 自訂角色並非自動指派，降低意外組態變更的風險。 管理員稍後可視需要新增角色和權限。

檢視使用者歷程記錄

在**支援管理員**頁面中，按一下**使用者歷程記錄**以檢視支援管理員的登入記錄。 支援管理員頁面中僅提供最近 90 天的登入記錄資料。

終止支援管理者的存取權

程序

1. 在 **Support Administrators** 頁面中，按一下要移除之帳戶右側的**刪除**連結。
2. 收到提示時，按一下**移除使用者**以確認。

暫停支援管理者的存取權

在 **Support Administrators** 頁面中，按一下要暫停之帳戶右側的**停用**連結。

12.1.8. 管理 > 系統使用通知

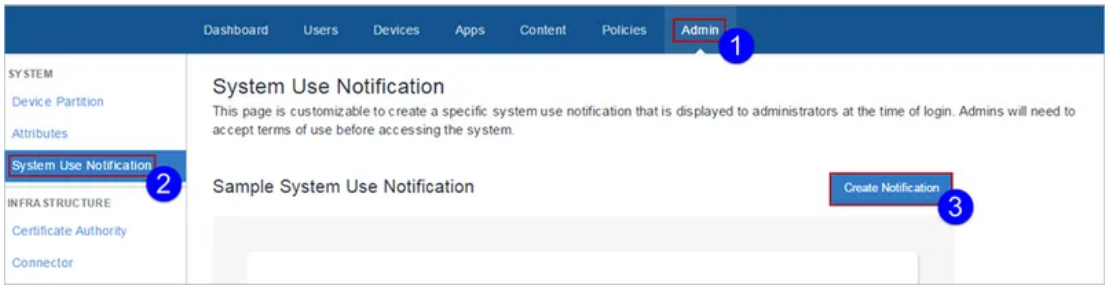
授權： Silver

您可使用「系統使用通知」功能，來建立自訂的系統使用通知，以在管理員登入時顯示該通知，並要求管理員接受使用條款後才能存取系統。

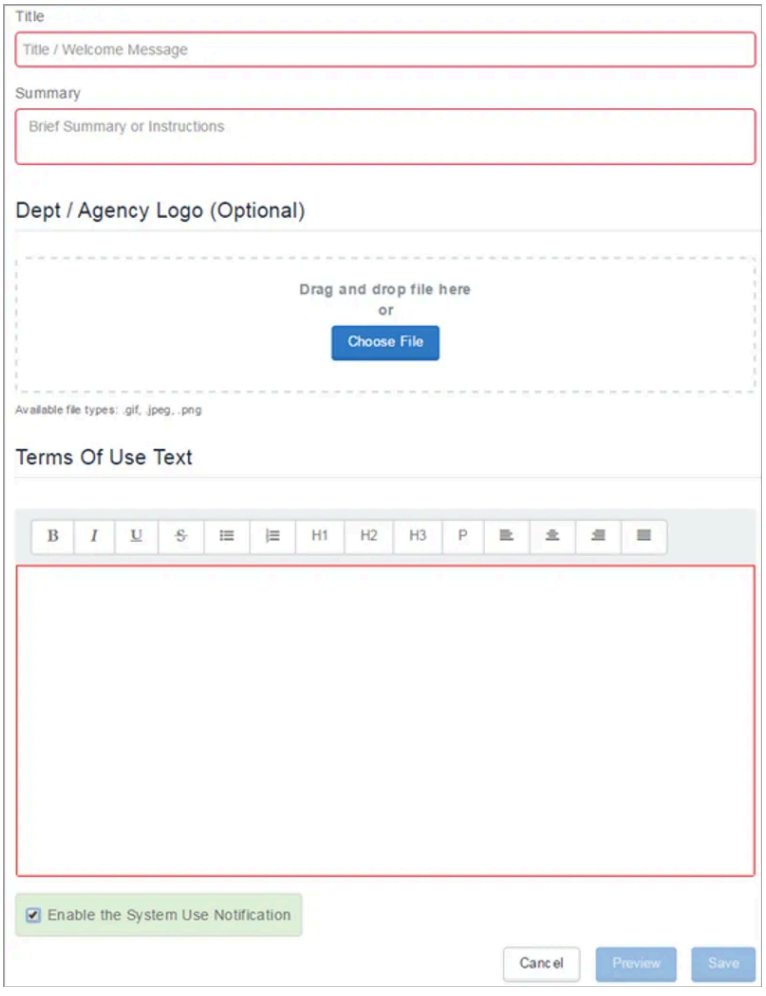
建立系統使用通知

程序

1. 選擇**管理 > 系統使用通知**。
2. 按一下**建立通知**。



隨即顯示「系統使用通知詳細資料」頁面。



在**標題**欄位中，輸入標題。

4. 在**摘要**欄位中，輸入摘要或指示。
5. 視需要選擇標誌。
6. 在**使用條款文字**欄位中，輸入使用條款文字。 此為管理員登入時必須接受的文字。
7. 勾選**啟用系統使用通知**勾選方塊，以開啟通知。
8. 按一下**預覽**，以叫用系統使用通知的預覽。
9. 當系統使用通知符合需求時，可按一下**儲存**。

12.2. 基礎架構

本節包含以下各主題：

- 存取
- App 清單
- 匯出稽核追蹤
- 憑證管理
- 適用於外部認證授權中心的 SCEP 配置
- 衍生的憑證提供者
- 連接器
- 對 Connector 使用 httpproxy 命令
- Help@Work
- 基礎架構身份識別
- 設定 LDAP 伺服器
- Sentry
- 在 Ivanti Neurons for MDM 和 SCEP 伺服器之間啟用 Kerberos 驗證

12.2.1. 存取

適用於： iOS 和 Android 裝置。

Access 可保護商業資料安全，並在任何裝置或 app 上啟用無縫與具生產力的使用者體驗。 而且 Access 會建立資料界限，以防使用者透過不安全的裝置、app 或雲端服務存取企業雲端服務。

最新文件

造訪**產品說明文件**，然後按一下 Access 以獲取有關 Access 以及如何設定 Access 的詳細資訊。 選擇適合您 Access 版本的文件。

12.2.2. App 清單

授權：Silver

您可以建立必要的 app 清單、app 允許清單和 app 封鎖清單，以搭配使用**允許的 App 原則**；在此原則中，這些清單有助您指定當裝置安裝的 app 不符合 app 清單需求時，要採取何種動作。 一旦建立 app 清單之後就無法編輯，因為**允許的 App 原則**可能已參照到這些 app 清單。 同樣地，您無法刪除任何允許的 App 原則所參考的 app 清單。

建立 app 清單

程序

1. 按一下**管理員 > 基礎架構 > 應用程式清單**。
2. 按一下**新建清單**。
3. 在**應用程式清單名稱**方塊中，輸入清單的名稱。
4. 選取清單類型: **白名單**、**黑名單**或**必要**。
5. 在**新增應用程式**部分下，選取應用程式類型: **App Store**、**OS X store**、**Google Play** 或**應用程式目錄**。
6. 輸入搜尋準則，以縮減選擇範圍。
7. 使用勾選方塊來選擇 app。 您可以使用多種搜尋，並啟用多個勾選方塊。
8. 按一下**檢視應用程式**索引標籤，取得目前已選取的應用程式清單。
   按一下**儲存**。

現在，當您設定**允許的 App 原則**時，即可使用這份清單。

如果您無法看到 **App 清單**頁面，可能是您沒有所需的權限。 您需具備下列其中一個**角色**：

- 系統管理
- 系統唯讀

12.2.3. 匯出稽核追蹤

稽核追蹤匯出是用來將所有稽核追蹤資訊匯出並上傳到特定伺服器位置的功能。 該伺服器應該可以從預設連接埠存取。 使用者可設置「稽核追蹤匯出」設定，以取得每天自動上傳到特定位置的稽核追蹤封存檔。

> 在基於 Linux 和 Windows 的 SFTP 伺服器支援稽核記錄匯出功能。

若要設置稽核追蹤匯出設定：

1. 選擇**管理員 > 基礎架構 > 稽核追蹤**。 隨即顯示**稽核追蹤**頁面。
2. 在**稽核追蹤**頁面，按一下**開啟**以啟用稽核追蹤匯出。
3. 在**匯出**區段中，更新下列欄位：

功能	描述
匯出格式	選取稽核追蹤資料匯出時應使用的格式： • **JSON** • **CEF** (常見事件格式) CEF 日誌訊息包含下列預設值： ◦ 版本：CEF 格式版號。 v25 是目前支援的版本。 ◦ 裝置製造商: Ivanti Inc ◦ 裝置產品: Ivanti Neurons for MDM ◦ 裝置版本：事件產生時的最新 Ivanti Neurons for MDM 版本。 ◦ 裝置事件類別 ID：對每個稽核來說不重複的實體 ID ◦ 名稱：對每個稽核來說的實體名稱與動作。 範例：推廣發佈配置設定 - 建立。 ◦ 嚴重性：指定事件的重要性。 範例：低。 CEF 日誌訊息還包含擴充欄位，即由下列鍵值配對組成的集合： ◦ CS1 與 CS1Label：稽核追蹤中繼資料，例如：createdAt、 entityType、entityName 及 actionType。 ◦ CS2 和 CS2Label: 執行者資訊。 ◦ CS3 & CS3Label：之前動作狀態。 ◦ CS4 & CS4Label：之後動作狀態。 在 CEF 匯出中，如果有任何欄位 (範例：CS3 或 CS4 鍵) 超出指定限制，則實際值會被“Value for this key exceeds mapped dictionary key allowed length”文字取代。
伺服器	輸入用來匯出稽核追蹤的伺服器名稱。
使用者	輸入用來登入伺服器的使用者名稱。
密碼	輸入伺服器登入密碼。
伺服器路徑	輸入伺服器的路徑，並確認伺服器上存在指定路徑。 範例：/Users/Test/Export。
金鑰交換演算法	針對外送 SFTP 配置，選擇用來匯出稽核追蹤的金鑰交換演算法清單。 預設下會選取以下金鑰交換演算法： • **diffie-hellman-group-exchange-sha1** • **diffie-hellman-group14-sha1** • **curve25519-sha256** • **diffie-hellman-group-exchange-sha256** (預設已選取)
Cipher	針對外送 SFTP 配置，選擇用來匯出稽核追蹤的加密 cipher 清單。 預設會選取以下加密 cipher： • **aes128-ctr** • **aes192-ctr** • **aes256-ctr** (預設已選取)
HMAC	針對外送 SFTP 配置，選擇用來匯出稽核追蹤的 HMAC 演算法清單。 • **hmac-sha1 (預設已選取)** • **hmac-sha2-256**

功能	描述
	• **hmac-sha2-512**

如果已設置上述欄位，這些欄位處於唯讀模式。 若要編輯已設置的欄位，您應按一下**編輯**按鈕。 如果管理已設為 SFTP 匯出，在升級後，會選取所有金鑰演算法。

按一下**測試連線並儲存**，以測試伺服器連線並儲存稽核追蹤匯出配置。

已封存的稽核追蹤透過 .zip 檔案以 JSON 格式提供使用。

在儲存稽核追蹤匯出設定之前，請先確認所有欄位中的配置設定。 如果有任何輸入的欄位值無效，將會顯示錯誤訊息。

在空間中啟用裝置註冊和取消註冊的稽核追蹤

啟用後，系統會將空間之間的裝置移動記錄於稽核日誌，包括裝置註冊、裝置刪除以及空間更新或刪除所觸發的事件。 空間管理員可以識別受影響的裝置、依空間和活動類型篩選記錄，並將稽核記錄匯出為 CSV。

12.2.4. 憑證管理

授權： Silver

認證驗證是一種保護行動電話裝置的有效方式。 認證比密碼更加安全，還可讓您使用單一憑證以保護 VPN、無線網路、電子郵件等項目。 如果您的組織具備外部認證授權中心的存取權，您就可以使用 Connector 來存取。 如果您的組織無權存取認證授權中心，您可使用 Ivanti Neurons for MDM 作為認證授權中心。 您也可以將 MobileIron Cloud 作為其他認證授權中心的中繼認證授權中心。 Ivanti Neurons for MDM 產生的認證稱為自行簽署認證。

- 建立身分憑證時，SHA-1 憑證已被取代。 您可以選擇其他演算法。 更新憑證時，如果舊版憑證使用 SHA-1，即可使用相同的 SHA-1 演算法。 如果舊版憑證使用 SHA-1 以上的演算法，就不允許還原為 SHA-1。
- 在設定本機或外部認證授權中心時，請選擇**快取 MobileIron Cloud 上的身分**Ivanti Neurons for MDM選項，以透過 Ivanti Neurons for MDM 服務儲存認證。 在每次有需要時清除快取以產生憑證。
- 憑證將以隱含方式重新核發。
- 為了改善系統的效能，會使用先進先出 (FIFO) 佇列來離線產生管理員建立的配置憑證。 在離線產生配置的期間中，配置狀態為**憑證產生擱置中** (位於**裝置詳細資料**頁面中**配置**索引標籤的**狀態**欄位下)。 產生憑證後，配置狀態就會進入**安裝擱置中**，並透過自動強制登記，將這些配置與憑證推送給裝置。
- 在發生裝置淘汰、抹除、重新產生憑證時，所有的憑證授權中心憑證都會遭到撤銷，包括 DigiCert PKI 平台或 GlobalSign 外部憑證授權中心所簽署的憑證。

身為管理員，您可以為智慧卡登入和自訂物件 ID (OID) 產生 Ivanti Neurons for MDM 憑證。 您可以從以下驗證選項產生憑證：

  - 用戶端驗證 - 預設為啟用
  - IPSEC - 選用，管理員可啟用
  - 智慧卡登入 - 選用，管理員可啟用
  - 自訂 OID - 選用，管理員可啟用

> 此功能僅適用於以下認證授權中心：
>
> - 本機憑證授權中心
> - 中繼憑證授權中心
> - 外部憑證授權中心 - 在 NDES 伺服器中設定 CA 範本的套用規則，以支援 IPSEC、智慧卡登入和自訂 OID

> 在裝置管理員、App Station 或其他非 Android Enterprise 模式下，使用 Samsung API 的 Samsung 裝置不支援憑證管理。 建議根據 Samsung 的建議針對移轉至 Android Keystore 進行驗證。

如需詳細資訊，請參閱憑證配置。

連線至內部部署 SCEP 憑證授權單位

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 安裝並設定 Connector (**管理 > Connector**)。 如需詳細資訊，請參閱 連接器。
3. 前往**管理** > **基礎架構** > **憑證管理**。
4. 按一下**憑證授權單位**區段下的**新增**。

5. 選取**新增內部部署 SCEP 憑證授權單位**並按一下**繼續:**
6. 輸入可識別該組態的名稱。
7. 選擇下列其中一個憑證授權中心類型：
    - Microsoft
    - EJBCA
    - 泛型 SCEP 伺服器
      「一般 SCEP 伺服器」選項適用於大多數具有靜態 Challenge 密碼的 SCEP 伺服器。

填妥顯示的表單。

9. 按一下**完成**。

建立外部認證授權中心

如果您想使用第三方憑證授權中心，請選擇此選項。

程序

1. 在**憑證管理**頁面中，按一下**憑證授權中心**區段之下的**新增**。
2. 在「新增憑證授權中心」頁面的「建立外部憑證授權中心」下方，按一下**繼續**。
3. 選擇 GlobalSign 或 DigiCert PKI 平台為外部憑證授權中心。
4. 填妥顯示表單上的其餘欄位。
5. 按一下**完成**。

檢視外部憑證授權中心的憑證。

您可以檢視憑證的詳細資料，並上傳此憑證授權中心的中繼/替代根憑證以取代現有的儲存副本。

程序

1. 在**憑證管理**頁面中的**憑證授權中心**之下，按一下外部憑證授權中心旁的**動作**，然後按一下**檢視憑證**。 **檢視認證**視窗隨即顯示。
2. 在**查看憑證**視窗中，按一下**上傳憑證**。 **上傳憑證：外部 CA** 視窗隨即開啟。
3. 按一下**選擇檔案**以選擇要上傳的憑證。
4. 按一下**完成**。

建立中繼認證授權中心

- 如果您需要認證，可以產生 CSR 並將其提交至簽署授權中心。 收到簽署授權中心的認證後，即可上傳認證。
- 如果您已具備必要的憑證，請您上傳。

產生 CSR (認證簽署要求)

程序

1. 在**憑證管理**頁面中的**憑證授權中心**區段之下，按一下**新增**
2. 在「新增憑證授權中心」區段中，於「建立中繼憑證授權中心」下方，按一下**產生 CSR**。
3. 填妥顯示的表單。
4. 按一下**產生**。

5. 將 BEGIN CERTIFICATE REQUEST 和 END CERTIFICATE REQUEST 之間的內容複製到文字檔中。
6. 將文字檔案上傳到憑證授權中心。
7. 按一下**完成**。

上傳已簽署的認證

收到憑證授權單位的簽署憑證後，您便可上傳簽署憑證。

程序

1. 在**憑證管理**頁面中的**憑證授權中心**區段之下，尋找您產生的 CSR。
2. 在此區段之下，選擇**動作 > 上傳新簽署的憑證**。
3. 按一下**選擇檔案**。
4. 選擇新簽署的認證。
5. 按一下**完成**。

上傳現有的認證

此主題說明如何上傳簽署憑證。

程序

1. 在**憑證管理**頁面中的**憑證授權中心**區段之下，按一下**新增**。
2. 在「新增憑證授權中心」區段中，於「建立中繼憑證授權中心」下方，按一下**上傳現有身份識別**。
3. 在**名稱**欄位中，輸入此認證的名稱以便與其他認證區隔。
4. 按一下**上傳**。
5. 選擇認證。
6. 輸入認證的密碼。
7. 按一下**上傳**。

檢視中繼認證授權中心的認證。

您可檢視認證的詳細資料，並取得認證授權中心的 CRL (認證撤銷清單) URL。

程序

1. 在**憑證授權中心**區段中，按一下憑證授權中心旁的**動作**，然後按一下**檢視憑證**。 **檢視認證**視窗隨即顯示。
2. 您可以在**檢視認證**視窗的 **CRL URL** 欄位中檢視 URL。
3. 按一下 **複製**，將 URL 複製到剪貼簿，然後貼入其他應用程式。 此 URL 可用來設定 Office 365，以接受憑證授權中心所發出的憑證。

建立獨立的認證授權中心

如果您想要新建完全獨立的認證授權中心 (本機與自簽署)，請選擇此選項。

程序

1. 在**憑證管理**頁面中的**憑證授權中心**區段之下，按一下**新增**。
2. 在「新增認證授權中心」頁面的「建立獨立認證授權中心」下方，按一下**繼續**。

3. 填妥顯示的表單。
4. 按一下**產生**。

獨立憑證授權中心到期通知

如果憑證到期日期小於 30 天，獨立 (本機) 憑證授權中心到期資訊當前在**到期日期**欄下顯示為工具提示。

如果到期日少於 365 天，除了傳送的通知外，還可以在 **儀表板** > **通知**下檢視此資訊。 選取**到期**做為篩選器。

設定獨立認證授權中心核發的憑證的到期時間。

您可設定獨立認證授權中心的到期時間。

程序

1. 在**憑證管理**頁面中，於**憑證授權中心**之下，按一下獨立憑證授權中心旁的**動作**。
2. 按一下**編輯**。
   隨即顯示**編輯認證授權中心**。
3. 在「用戶端認證範本」區段的**認證有效期**欄位中，輸入新的到期時間 (天)。
4. 按一下**儲存**。

當本機憑證授權中心發出的憑證即將過期或已過期時，您可以接收通知和電子郵件 (若已選擇啟用)。

- 憑證到期的天數通知 - 系統會在憑證有效期間的預定間隔產生通知。 第一則通知會在到期前 365 天發出，其他通知則會在到期前 180 天、60 天、45 天和 7 天發出。 您會持續收到此通知，直到您導覽至**管理 > 憑證管理 > 動作 > 上傳新簽署的憑證**，並取代憑證為止。
- 過期憑證通知 - 您會在憑證過期時收到通知。 您必須取代憑證，以便恢復正常服務。
- 已上傳新有效憑證的通知 - 當上傳新的已簽署憑證時，系統會傳送通知。

檢視獨立認證授權中心的認證。

您可檢視憑證的詳細資料並取得本機憑證授權單位的 CRL (憑證撤銷清單) URL。

程序

1. 在**憑證管理**頁面的**憑證授權單位**區段下，按一下當地憑證授權單位旁的**動作**，然後按一下**檢視憑證**。 **檢視認證**視窗隨即顯示。
2. 您可以在**檢視認證**視窗的 **CRL URL** 欄位中檢視 URL。
3. 按一下 **複製**，將 URL 複製到剪貼簿，然後貼入其他應用程式。 此 URL 可用來設定 Office 365，以接受本機憑證授權中心所發出的憑證。

檢視憑證授權中心的 CRL 有效期

您可以檢視並編輯本機或中繼憑證授權中心的 CRL 有效期。

程序

1. 在**憑證管理**頁面的**憑證授權單位**區段下，按一下當地憑證授權單位旁的**動作**，然後按一下**編輯**。 隨即顯示**編輯認證授權中心**。
2. 在**編輯憑證授權中心**視窗中，您可以檢視「CRL 有效期」的值。 最短預設值為 24 小時。 可輸入的最長值為 10950 小時。
3. 編輯 CRL 有效期的值，並按一下**儲存**。

建立雲端憑證授權中心

如果您想使用憑證授權中心，請選擇此選項。

程序

1. 前往**管理** > **基礎架構** > **憑證管理**。
2. 在**憑證管理**頁面的**憑證授權單位**區段下，按一下**新增**。
3. 在**新增憑證授權單位**頁面的**連線到受到公開信任的雲端憑證授權單位**下，按一下**繼續**。
4. 在**名稱**方塊中輸入名稱。
5. 從下列選項中選取「雲端憑證授權單位」：
   - **Atos IDnomic CMS**
   - **DigiCert One PKI 平台**
   - **DigiCert PKI 平台**
   - **Entrust**
   - **GlobalSign**
6. 輸入基礎 URL 並上傳憑證資料。
7. 按一下**完成**。

對憑證使用進階搜尋

您可使用「進階搜尋」選項根據規則來搜尋已發行的憑證，以識別和檢視符合特定準則的憑證。 這些規則可使用適用的運算子進行建構，包括「開頭是」、「結尾是」、「包含」、「不包含」、「開頭不是」、「結尾不是」、「小於」、「大於」、「範圍」、「等於」及「不等於」運算子。 這些規則選項可以用「任何 (或)」或「所有 (及)」選項來建立巢狀結構。 符合規則的已發行憑證會顯示在此區段下方。 從 Ivanti Neurons for MDM 76 版本起，所有憑證管理範本的運算子均包含標準運算子。 在本版本中已標準化以下範本的運算子：

- 管理 > 憑證管理 > 已發行的憑證 > 進階搜尋

對已發行憑證執行進階搜尋

程序

1. 在**憑證管理**頁面的**已發行的憑證**區段中，按一下**進階搜尋**連結。
2. 如果使用者需要符合至少一項規則，請按一下**任一**；如果使用者必須符合所有規則，則請按一下**全部**。
3. 針對下列屬性，建立一項定義搜尋準則的規則：
   - **CA**
   - **配置名稱**
   - **到期**
   - **是私密金鑰**
   - **作業系統**
   - **序號**
   - **狀態**
   - **使用類型**
   - **使用者**
4. (選用) 按一下 + 以視需要建立其他規則。

5. (選用) 按一下**儲存**以儲存查詢。
6. 按一下**搜尋**。 符合搜尋準則的使用者清單會顯示在此頁面。

對使用者提供的憑證執行進階搜尋

程序

1. 在**憑證管理**頁面的**使用者提供的憑證**區段中，按一下**進階搜尋**連結。
2. 如果使用者需要符合至少一項規則，請按一下**任一**；如果使用者必須符合所有規則，則請按一下**全部**。
3. 針對下列屬性，建立一項定義搜尋準則的規則：
   - **憑證名稱**
   - **有效日期**
   - **核發機構**
   - **上傳時間**
4. (選用) 按一下 + 以視需要建立其他規則。
5. (選用) 按一下**儲存**以儲存查詢。
6. 按一下**搜尋**。 符合搜尋準則的使用者清單會顯示在此頁面。

載入已發行的憑證搜尋查詢

檢視已儲存的搜尋查詢的清單。

程序

1. 在**憑證管理**頁面的**已發行的憑證**區段中，按一下**進階搜尋**連結。
2. 按一下「資料夾」圖示。 **進階搜尋**視窗顯示。 建立的搜尋查詢清單會顯示在**載入查詢**區段。 此區段會顯示下列詳細資訊：
   - **查詢名稱** - 載入查詢的名稱。
   - **查詢內容** - 顯示定義搜尋查詢的規則內容。
   - **動作** - 選擇要對查詢執行的動作。
3. 按一下**動作**欄中的**載入查詢**，以檢視符合載入查詢中定義準則的已發行的憑證清單。
   如要刪除載入查詢，按一下刪除圖示。

> 按一下**匯出至 CSV**，以 CSV 檔案形式下載搜尋結果報告內容，供日後參考或分析。

檢視已發行的憑證的有效期

在**已發行的憑證**區段之下，在**有效日期 (天)** 欄中，如果到期日在 30 天內，您可以查看憑證還剩幾天到期。 如果憑證在過去 30 天內已到期，憑證的**有效日期 (天)** 欄會顯示有效日期已過期幾天。

如需更多資訊，請參閱[適用於外部憑證授權中心的 SCEP 配置]。

匯出至 CSV

您可將憑證匯成 CSV 檔案，以供日後參考或分析。

程序

1. 在**憑證管理**頁面中，前往下列其中一個索引標籤。
    - **憑證授權單位**
    - **已發行的憑證**
    - **使用者提供的憑證**
2. 按一下**匯出至 CSV**。
3. 按一下**下載**。
4. (選用) 按一下**刪除**以刪除報告。

12.2.5. 適用於外部認證授權中心的 SCEP 配置

此功能支援在 Windows 10 裝置上使用外部憑證授權單位的簡單憑證註冊協議 (SCEP) 組態。

> 此組態可使用具有自訂分發選項的委派。 如需更多資訊，請參閱使用配置中的*分發組態*主題。

設置外部認證授權中心

您必須先設置外部 CA。 如果您已具備外部 CA，則可略過下一節。

1. 前往**管理員 > 基礎架構 > 憑證管理**。
2. 按一下 **+新增**。
3. 輸入認證授權中心的名稱。
4. 使用下拉式功能表將 Microsoft 選為**憑證授權中心類型**。
5. 輸入 **SCEP URL**。
6. 輸入**使用者名稱**和**密碼**。
7. 輸入**查問 URL**。
8. 按一下**儲存**。

SCEP 組態

現在您可以繼續進行 SCEP 組態。

1. 前往**配置 > +新增**。
2. 選擇 Windows 圖示。
3. 選擇**身分憑證**，以前往**建立身分憑證配置**頁面。
4. 輸入配置的名稱。
5. 從**憑證發佈**下拉式功能表中，選擇 SCEP 配置清單的 **Windows 配置**。
6. 選擇外部 CA。
7. 輸入認證發佈詳細資料。
   - 輸入主體。 例如：CN=$
   - 從**重試**下拉式功能表中，選擇重試次數。
   - 從**重試延遲**下拉式功能表中，選擇每次重試之間等候的秒數。
   - 從**金鑰長度**下拉式功能表中，選擇金鑰大小。
   - 至少選擇一個憑證使用方法選項。
   - 在**有效性**欄位和下拉式功能表中，輸入時間長度。
   - 輸入 CA 指紋。
   - 前往 SCEP 查問 URL，複製 CA 指紋並將其在此貼上或按一下**從憑證建立**... 上傳可從中建立 CA 指紋的憑證。
     從**雜湊演算法系列**選項中，選擇至少一個雜湊演算法。
8. 按**下一步**。

12.2.6. 衍生的憑證提供者

在「衍生的憑證提供者」頁面中，您可以檢視用於憑證發佈的衍生憑證提供者清單。 您可指定哪些憑證提供者應設為預設值，也可新增您使用的其他自訂衍生憑證提供者。

如要將衍生的憑證提供者設為預設值：

1. 前往**管理 > 衍生的憑證提供者**。頁面中隨即列出下列衍生的憑證提供者。
    - **Entrust**
    - **Intercede**
    - **Purebred**
2. 對於要設定為預設的提供者，請按一下**動作**欄下方的**設定為預設**。 設定時在提供者欄，**預設提供者**下方會顯示核取標記圖示，表示這是預設的認證提供者。

如要新增自訂衍生憑證提供者：

1. 前往**管理 > 衍生的憑證提供者**。
2. 按一下 **+新增**。
3. 在**名稱**欄下的文字欄位中，輸入衍生的憑證提供者名稱。
4. 按一下**儲存**。
   新增後，此自訂衍生憑證提供者就會成為**品牌**欄位中的一個選項，供您在**身分憑證**配置下設定衍生的憑證發佈時選擇。

按一下**動作**欄位下的**刪除**，即可刪除衍生的憑證提供者。

> 如果衍生的憑證提供者已設為預設值，您將無法刪除該提供者。

12.2.7. 連接器

授權： Silver

Ivanti Neurons for MDM Connector 可讓您從 Ivanti Neurons for MDM 服務存取企業資源，例如 LDAP 伺服器或憑證授權單位 (CA)。 針對您想存取的每個資源設定一個 Connector。

如果您使用 Microsoft Active Directory 或在 Amazon Web Services (AWS) 中託管的 LDAP 伺服器，您可以在 AWS 中託管 Ivanti Neurons for MDM Connector。 不需要任何內部部署 Connector。

Connector 會自動更新至最新軟體版本。

如需最新的「Ivanti Neurons for MDM Connector 安裝指南」，請造訪 **https://help.ivanti.com/#106** 並搜尋「Connector」。

Connector 託管選項

您可以將 Ivanti Neurons for MDM Connector 本地託管在資料中心或 Amazon Web Services (AWS) 中：

- 在 AWS 中託管 Connector (如果您使用 AWS 託管的 Microsoft AD 或在 AWS 中自行管理 Microsoft Active Directory)。 在這個情況下，您不需要 Connector 內部部署。
- 若要存取內部部署資源，例如 LDAP 伺服器或 CA，請設置 Connector 內部部署。

在 AWS 中託管 Connector

客戶可在 AWS 中託管 Connector，並搭配使用下列 AWS 託管的 Microsoft Active Directory 選項：

- 適用於 Microsoft Active Directory 的 AWS 目錄服務
- 在 Amazon VPC 中由客戶管理的 Microsoft Active Directory

如需適用於 Microsoft Active Directory 的 AWS Directory Service 詳細資訊，請參閱 **https://aws.amazon.com/directoryservice**。 請參閱 AWS 文件，以瞭解如何在 Amazon VPC 中託管 Microsoft Windows Server 及 Microsoft Active Directory。 Ivanti Neurons for MDM Connector 支援 Windows Server 2012、2012 R2、2015。

在 AWS 中設定 Ivanti Neurons for MDM Connector AMI

若要設定 Ivanti Neurons for MDM Connector AMI:

1. 使用管理員憑證登入 AWS。
2. 在 AWS 服務頁面，於 **Compute** 之下選擇 **EC2**。
3. 在左邊窗格中，展開**圖片**並選擇 **AMI**。
4. 在右邊窗格中，從下拉式清單選擇**公用圖片**。
5. 使用關鍵字 (例如「mobileiron-kocab」) 搜尋 Ivanti Neurons for MDM Connector。
6. 從清單中選擇最新版本的 Connector，然後按一下 **Launch** (啟動)。
7. 按照 Connector 安裝說明進行操作，即 *Ivanti Neurons for MDM Connector 安裝指南*中的「在 AWS 中部署 Ivanti Neurons for MDM Connector」，該章節可見於 https://help.ivanti.com/mi/help/en_us/cld/*<version>*/inst/default.htm，其中*版本*是正在安裝的 Ivanti Neurons for MDM Connector 版本。 例如，如為 74 版 Ivanti Neurons for MDM Connector，可在 https://help.ivanti.com/mi/help/en_us/cld/**74**/inst/default.htm 中找到該指南。

在內部部署中託管 Connector

若要在資料中心本地託管 Ivanti Neurons for MDM Connector，請按一下**下載 Connector**，以下載並設定 Ivanti Neurons for MDM Connector。 從下載的套件將內容解壓縮，然後遵循套件隨附的 Ivanti Neurons for MDM Connector 安裝指南中的設定說明。

存取 Connector 日誌

可以透過 Connector 服務來存取 Connector 日誌，以協助針對 Connector 相關問題進行疑難排解。 您必須具備「系統管理員」或「系統唯讀」角色。

1. 前往**管理 > Connector** 以檢視 Connector 頁面。
   Connectors 介面會顯示 Connector 狀態 (「啟用」或「停用」)、Connector 名稱、連線 (「連線」或「尚未連線」)、版本號、記錄層級、動作 (「停用」或「移除 Connector」)。
2. 使用**記錄層級**下拉式功能表來選擇層級。
   下拉式功能表會顯示可用的記錄層級，並以最低記錄層級到最高記錄層級的順序排列：
   - 錯誤
   - 警告
   - 資訊
   - 偵錯
   - 追蹤

「資訊層級」是預設的記錄層級設定。 如果您選擇其他記錄層級，即會出現「同步」圖示 指出系統將會收集您選取的記錄層級資訊。 一個小時後，系統會將記錄層級重設為「資訊」層級。 「追蹤」層級是最高的記錄層級設定。 您可使用此層級來收集其他層級的所有訊息。 在請求期間會顯示「同步」圖示。

3. 如有需要，可將游標移到「同步」圖示 ，即會顯示「取消」圖示。 按一下「取消」圖示，記錄層級隨即改變。
4. 將游標移到「請求」圖示上方，即會顯示「請求」資訊。 按一下「請求」圖示 ，即可請求目前日誌資料夾中的檔案 (以 .zip 檔案格式提供)。
   要求建立時，即會將日誌檔新增至 .zip 檔案。 建立新的要求時，系統就會將上一個要求的 .zip 檔案刪除。
5. 如有需要，可將游標移到「請求」圖示 ，即會變成「取消」圖示 。 按一下「取消」圖示，即可停止要求。
   如果在完成要求之前取消，系統就不會顯示「下載」圖示 ，因為已從伺服器中刪除先前的日誌 .zip 檔。 但您仍可要求 Connector 上的原始日誌檔案。
6. 當要求已完成並可下載日誌的 .zip 檔案 (其中包含最新要求期間所收集的日誌檔) 時，請按一下「下載」圖示。
   記錄檔名稱格式為: kocab.log。 下載的 zip 檔名稱包含伺服器名稱、連線版本以及時間戳記 (包括日、月、年與當天時間)，格式如下: <Connector_Hostname>_<Connector_Version>_<TimeStamp>.zip。 封存的 .zip 檔案名稱格式為：kocab.yyyy-mm-dd.0.log.gz。
7. 您也可以使用**動作**下拉式功能表，以「停用」或「移除 Connector」。

如果您無法看到 **Connector** 頁面，可能是您沒有所需的權限。 您需具備下列其中一個角色：

- 系統管理
- 系統唯讀

如需更多資訊，請參閱對 Connector 使用 httpproxy 命令。

12.2.8. 對 Connector 使用 httpproxy 命令

已建立新的 klish shell 指令，以協助編輯 Ivanti Neurons for MDM 安裝的 Connector 組態。 請使用此指令來變更登入資訊和其他參數以設定 Connector。

此版本現在提供 httpproxy 指令以因應這些需求。

- klish 殼層

若要設定 Connector

1. 請登入 klish shell。
2. 輸入問號? 取得可用的 klish 殼層指令清單。
3. 輸入 **httpproxy** 以顯示下列參數的目前值：
    1. 已啟用
    2. 配置
    3. 伺服器
    4. 驗證類型
    5. 使用者名稱
    6. 密碼
4. 輸入 **httpproxy ?** 以查看可搭配 httpproxy 使用的指令清單。
    1. authtype - 將 Proxy 的身份認證設成 NONE、BASIC 或 NTLM
    2. disable - 停用 http proxy
    3. enable - 啟用 http proxy
    4. host - 設定 http proxy 的主機 - 必須是 FQDN 或 IP (http 或 https)
    5. password - 設定 http proxy 的身份認證密碼
    6. port - 設定 http proxy 的連接埠
    7. scheme - 設定 http proxy 的架構 - 必須是 http 或 https
    8. show - 顯示目前的 http proxy 設定
    9. username - 設定 http proxy 的身份認證使用者名稱
5. 使用上面所列的指令來設定您的 Connector 執行個體。

12.2.9. Help@Work

授權：Platinum

支援：Ivanti Neurons for MDM 支援的 Android 和 iOS 裝置

使用適用於 Android/iOS 的 Help@Work，遠端協助 Android 和 iOS 裝置的使用者。 適用於 Android/iOS 的 Help@Work 是以 TeamViewer QuickSupport app 為基礎。 您需具備 TeamViewer 帳戶才能使用適用於 Android/iOS 的 Help@Work。 如果您還沒有帳戶，請前往 teamviewer.com 以取得詳細資料。

Help@Work 讓使用者按一個按鈕即可尋求協助，並向服務台人員共享螢幕擷取畫面，藉此轉變 iOS 11.0+ 和 Android 裝置的服務台體驗。 使用者不用再浪費寶貴的時間說明問題，而 IT 人員也可更有效率地疑難排解裝置相關問題。 本產品不支援 MAM Only 的 iOS 裝置。

> 在處於單一應用模式的「Android 裝置擁有者」裝置上支援 TeamViewer。

> 如果 app 退出或裝置重新開機，TeamViewer 啟動命令將不復存在。

> 如果 Android 裝置未安裝 Teamviewer QuickSupport app，系統就會提示使用者下載 app。 如果 iOS 裝置已透過 App Catalog 推送 app，或裝置上已安裝 app，此 app 即會轉換為受管理的 app。

> Teamviewer QuickSupport app 應在前景執行，才能將工作階段套用到應用程式。 「自動」模式需要 TeamViewer 主機應用程式。

> 管理員安裝的桌上型電腦應用程式版本應與用戶端裝置上安裝的 Quicksupport 版本相容，才能支援遠端工作階段。

設定適用於 Android 或 iOS 的 Help@Work

以下是適用於 Android 或 iOS 的 Help@Work 品牌化與發佈的一次設定步驟:

1. 前往**管理**索引標籤。
2. 按一下「基礎架構」底下的 **Help@Work**。
3. **Help@gWork** 需要 TeamViewer。 在「啟動 TeamViewer」區段中，透過按一下**立即啟動**按鈕啟動 **TeamViewer 手動**或 **TeamViewer 自動 (僅限 Android)** 選項。
4. 檢視 TeamViewer 授權合約，然後按一下**同意**繼續。 您的企業授權已啟用。 現在已可在授與存取權時，識別出 Ivanti 客戶與 TeamViewer 客戶。

> 在啟動 TeamViewer 後，**移除啟用**選項會變成可用。 當您按下**啟用 TeamViewer** 區段下的**移除啟用**時，畫面上會出現**確認移除啟用**視窗。 按一下**移除啟用**以移除 TeamViewer 啟用，此舉將移除所有受支援裝置上的 Help@Work 功能。 不過，您可在之後使用現有帳戶或其他帳戶再次啟用 TeamViewer。

> 若您要在「自動」模式下刪除 **TeamViewer** 帳戶，您必須取消佈建已啟用自動模式的相關裝置。 若要取消佈建相關裝置，您必須在相關裝置中取消發佈 **TeamViewer** 應用程式並執行強制簽入。 確認已從所有裝置中刪除 TeamViewer 應用程式，然後在管理主控台中刪除帳戶的繫結。

使用標準 app 發佈工作流程，將 TeamViewer app 發佈給您想啟動遠端工作階段的使用者。 這專屬於**手動**和**自動**模式。 若管理員想要控制裝置，則 TeamViewer 的通用附加元件或 OEM/特定型號的附加元件也需要散發到裝置。 請參閱 App 配置以取得指示。

使用適用於 Android 或 iOS 的 Help@Work 啟動遠端工作階段

當一般使用者需要協助時，就會啟動適用於 Android 或 iOS 的 Help@Work 典型工作階段。

透過使用者的裝置來啟動 Help@Work 工作階段：

1. 在 Ivanti Neurons for MDM 中，前往**裝置**。
2. 在裝置清單頁面中，按一下需要支援的裝置。
3. 從「動作」功能表中，按一下 Android 裝置的**啟動 TeamViewer 遠端控制**，或 iOS 裝置的**遠端顯示**。 會看見兩個選項:
    - 「手動」模式 (預設) – 此選項需在目標裝置中安裝 **TeamViewer 快速支援**應用程式並將其列入白名單。
    - 「自動」模式 (僅可用於 Android 上) - 此選項需在目標裝置中安裝 **TeamViewer Host** 應用程式並將其列入白名單。

> 如果要將主機名稱列入白名單或覆寫內容安全原則，請聯絡支援團隊。

> 「自動」模式選項也適用於 kiosk 模式。 其應從 TeamViewer 整合頁面啟用。 「自動」遠端控制需要裝置上的 TeamViewer 主機應用程式、某個裝置上的一次啟動，以及 MI 附加元件授權。 針對一次性啟用，授權提示將在初次安裝及啟動 TeamViewer 主機應用程式時顯示。 如有需要，管理員可在安裝後使用「自動啟動 (受管理應用程式組態內的設定)」TeamViewer 應用程式。 授權數量是根據 TeamViewer 主機應用程式發佈計算而得。 若將 TeamViewer 主機應用程式散發到裝置，則會用掉一個「自動」遠端主機工作階段授權。 除了 TeamViewer 主機應用程式之外，可能還需要其他附加元件應用程式，並應可在 Kiosk 或共用 Kiosk 模式下使用。 根據裝置型號和製造商的不同，可能還需要其他附加元件。

> Google Pixel 裝置不會保留此類授權，而且每個工作階段都需要取得權限同意。

如果管理員具備有效的 TeamViewer 權杖，桌上型電腦用戶端就會啟動裝置的支援工作階段。 否則，會要求管理員登入 TeamViewer 並授與權限。

若要快速啟動遠端工作階段，管理員可以事先登入桌上型電腦應用程式。

安裝 TeamViewer

在桌上型電腦中安裝 TeamViewer app，才可存取使用者的遠端裝置並提供支援。 若要安裝 TeamViewer：

1. 前往下列網址，下載適用於 Mac、Windows 或 Android 的 TeamViewer 完整版安裝套件：https://www.teamviewer.com/en/download/。
2. 啟動 TeamViewer 安裝程式。
3. 選擇**基本安裝**。
4. 選擇**公司 / 商業用途**。
5. 按一下**接受 – 完成**。

申請 TeamViewer 帳戶

您必須具備 TeamViewer 帳戶，才能使用 TeamViewer 提供支援。 若要取得 TeamViewer 帳戶：

1. 前往 https://login.teamviewer.com/。

2. 輸入您的電子郵件、名稱和密碼。
3. 按一下**註冊**。
4. 請使用您在步驟 2 中輸入的電子郵件帳戶，以便接收 TeamViewer 帳戶啟用電子郵件。
5. 完成電子郵件中的指示，以啟用您的 TeamViewer 帳戶。

確認 TeamViewer 工作階段 ID

TeamViewer 會在建立管理員電腦與使用者行動裝置間的連線時，產生一個工作階段 ID。

1. 工作階段 ID 產生後，Ivanti Neurons for MDM 會使用受管理 app 配置將它傳遞給 TeamViewer QuickSupport app，以便使用此工作階段 ID 來呼叫裝置上的 TeamViewer 用戶端。 針對 iOS，工作階段 ID 會在 30 分鐘後過期。
2. 系統會提示使用者接受 TeamViewer EULA。

12.2.10. 基礎架構身份識別

本節包含以下各主題：

12.2.10.1. 設定身份識別提供者

授權：Silver

設定身分識別提供者 (IdP) 以驗證想要向 Ivanti Neurons for MDM 註冊裝置、存取此管理入口網站，或存取自助式入口網站的使用者。 需要內部部署 LDAP 相容使用者目錄。 Ivanti Neurons for MDM 適用於任何與 SAML 2.0 相容的 IdP。 Microsoft Entra ID 驗證 (Entra ID)、Microsoft ADFS (Active Directory 同盟服務)、Okta、OneLogin、PingOne 和 Ping Identity 的 PingFederate 均已經過驗證，可與 Ivanti Neurons for MDM 一起使用。

之前，如果您設定 SAML auth/IdP，SAML 驗證用於裝置註冊和入口網站驗證。 現已佈建切換按鈕，可供選擇不同的管理入口網站存取和裝置註冊驗證方法。 略過切換僅適用於裝置註冊。

裝置註冊期間，管理員可繞過身分識別提供者選項，並為使用者提供使用 PIN 碼進行身分驗證的選項，取代使用身分識別提供者頁面進行身分驗證。

概覽

- 如果您是使用 Microsoft AD 或其他內部部署 LDAP 目錄，則需要設定 Connector 以連接 Ivanti Neurons for MDM，並將使用者匯入。 設定 **Connector** 或 LDAP (如果尚未設定)。
- 新增 IdP 之後，使用者身份認證會自動從 LDAP 切換至 IdP。
- 僅允許一個 IdP 提供者。
- 如果您的 IdP 變成無法存取，請使用 Ivanti Neurons for MDM 租用戶管理員 (TA) 帳戶來存取此管理入口網站與進行疑難排解。 TA 是本機帳戶，不需要外部身分認證。 在佈建好 Ivanti Neurons for MDM 並將資訊提供給組織的技術聯絡人或類似人員後，即會建立 TA 帳戶。 如果您沒有 TA 帳戶資訊，請聯絡您的支援代表。
- Ivanti Neurons for MDM 支援 Microsoft Entra ID (Entra ID)，以便在註冊 Windows 10 裝置期間驗證使用者。

> 設定 LDAP 使用者的身分認證類型時，請使用 IdP 供應商所提供的工具。 IdP 驗證架構優先順序會高於 Ivanti Neurons for MDM 設定。 Ivanti Neurons for MDM 驗證設定可在以下位置找到：**使用者 > 使用者設定 > 裝置註冊設定 > 裝置註冊驗證類型**。

- Apple Device Enrollment 和 Configurator 裝置授權並非使用 IdP 進行使用者身分認證。
- 若要將身分識別提供者設定為用於註冊 Apple Business Manager iOS 和 macOS 裝置，必須前往**管理員 > Apple > 裝置註冊 >*編輯裝置註冊設定檔*，啟用啟用自訂註冊**和相關的 **Ivanti 受控網頁**設定。如需詳細資訊，請參閱**裝置註冊**:



IdP 設定類型

Ivanti Neurons for MDM 身分識別頁面可引導您設定下列類型的 IdP 提供者：

- **Ivanti Neurons for MDM IdP 設定** - 支援的 Ivanti Neurons for MDM IdP 提供者包括 Entra ID、OneLogin、Okta 和 PingOne。
- **內部部署 IdP 設置** - 支援的內部部署 IdP 提供者為 ADFS 3.0、PingFederate 8.2.1 和 PingFederate 8.1.3。
- **一般 IdP 設置** - 如果您不是使用 Microsoft ADFS、Okta、OneLogin 或 PingFederate，即可使用這個一般設定路徑。

設定身分提供者 (IdP)

程序

1. 前往**管理** > **身分識別** > **SAML 驗證**。

2. 按一下身分識別提供者設定類型:
    - **Ivanti Neurons for MDM IDP 設定**
    - **內部部署 IDP 設定**
    - **一般 IDP 設定**
3. 選擇對應的 IdP。 如果您在步驟 3 中已選擇**一般 IDP 設定**，則可略過此步驟，並從步驟 5 繼續。
4. 遵循畫面上針對所選 IdP 顯示的指示。
5. 按一下**完成**。

> 允許管理員使用 IdP 提供的初始身份認證每次登入最多 2 小時。

設定您可能需要完成的任務

依據您選擇的 IdP 而定，系統將會引導您瀏覽下列相關頁面並執行相應步驟:

IdP	程序
• Entra ID • Okta • OneLogin • PingOne	• 產生金鑰，並將其上傳至 IdP。 • 登入您的 IdP 並上傳產生的金鑰。 • 從 IdP 匯出中繼資料檔案，然後將其匯入 Ivanti Neurons for MDM。
• ADSF 3.0 • PingFederate 8.2.1 • PingFederate 8.1.3	• 從 Ivanti Neurons for MDM 下載中繼資料檔案。 • 在 ADFS 上設定「信賴憑證者信任」或在 PingFederate 上設定「SP 連線」，並匯入 Ivanti Neurons for MDM 中繼資料檔案。 • 從 IdP 匯出中繼資料檔案，然後將其匯入 Ivanti Neurons for MDM。
• 一般 IdP	1. 從 Ivanti Neurons for MDM 下載中繼資料檔案。 2. 按照 IdP 供應商所提供的說明書，將 IdP 伺服器或服務設定為以「服務提供者」身分與 Ivanti Neurons for MDM 服務通訊。這可能包括: 1. 將上述步驟 1 的中繼資料檔案上傳至您的 IdP。 此組態檔包含的基本資訊，可讓 Ivanti Neurons for MDM 以 SAML 2.0 服務提供者的形式與 SAML 2.0 身分識別提供者進行通訊。 標準 SAML 2.0 URL、憑證和設定都包含在中繼資料檔案中。 Ivanti Neurons for MDM 預期 SAML 2.0 相容 IdP 能夠匯入與處理從服務提供者匯出的 XML 中繼資料。 2. 將您的 IdP 設為使用 RSA-SHA-1 來簽署 SAML 驗證要求。 「簽署憑證」相關資訊可用來確認步驟 1 所下載的中繼資料檔案含有驗證要求。 3. 設定您的 IdP，以便在傳送給 Ivanti Neurons for MDM 的 SAML 回應中包含使用者名稱。 指定使用來自 IdP 的 SAML 回應中 [名稱 Id] 項目內含的使用者名稱。 從 IdP 匯出中繼資料檔案，然後將其匯入 Ivanti Neurons for MDM。 3. (選用) - 在 SAML 驗證要求中包含使用者名稱: 在驗證要求中包含正在驗證之使用者的使用者名稱，並在使用 IdP 進行驗證時移除額外的使用者輸入。 若您啟用此選項，可能會發生驗證失敗的情況。 如果您對 IdP 驗證已有充分的瞭解，則可選取**我理解此變更的影響**選項，並將**在 SAML 驗證要求中包含使用者名稱**設定切換成**開啟**。 Ivanti Access 是經驗證的 IdP，適用於此設定。

啟用要略過 IdP 驗證的本機使用者

當 IdP 或 Ivanti Neurons for MDM 連線功能關閉但需要從 Ivanti Neurons for MDM 端進行疑難排解時，特定管理員需要能夠登入 Ivanti Neurons for MDM 且不用依賴外部系統 (例如 LDAP 或 IdP) 進行驗證。 僅擁有系統管理角色的本機使用者可略過 IdP身份認證。

建立要略過 IdP 驗證的本機使用者清單。

程序

1. 按一下**管理 > 身份**。

2. 在「本機使用者可略過 IdP 驗證」區段中，按一下 **+新增使用者。**
3. 從僅顯示具有系統管理角色的本機使用者清單中，選擇一些使用者。
4. 按一下**儲存**。

> 若要將使用者從略過 IdP 驗證的本機使用者清單中移除，請按一下要刪除之項目旁的移除圖示。

如果您無法看到「身份」頁面，可能是您沒有所需的權限。 您需具備下列其中一個**角色**：

- 系統管理
- 系統唯讀

12.2.10.2. 使用 SCIM 進行使用者佈建

本節包含以下各主題：

- 使用者佈建
- 從 Ivanti Neurons for MDM 產生權杖
- 變更權杖狀態
- 從「稽核追蹤」檢視權杖狀態
- 在 SCIM 佈建中設定屬性

使用者佈建

使用者佈建使用 SCIM 通訊協定將 IdP 與 Ivanti Neurons for MDM 同步，並允許部分使用者和群組同步。 使用者佈建使用 SCIM 通訊協定自動建立使用者和群組物件，並將來源從 IdP 更新為 Ivanti Neurons for MDM。 就像目前與 Entra ID 和 Okta 的整合一樣，使用者和群組佈建程序已自動化；若變更 IdP 中的使用者或群組，則相同的變更會反映在 Ivanti Neurons for MDM 中。

> 如果透過 SCIM 佈建的使用者的使用者名稱在 Ivanti Neurons for MDM 中是唯一的，則可以在身分識別提供者 (IdP) 中重新命名它。

> 現在可以使用 SCIM 使用者和群組的外部 ID 來搜尋它們。

從 Ivanti Neurons for MDM 產生權杖

若要啟動使用者佈建 IdP，請從 Ivanti Neurons for MDM 產生權杖和目標 URL。

> 請確定要儲存權杖和目標 URL。

> 任何時候，最多可產生 2 個權杖。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 前往**管理員** > **身分識別** > **使用者佈建**。
3. 從下拉清單中選取身分提供者 (IdP)。
4. 若要產生新權杖，按一下**產生**。 通知訊息隨即顯示，按一下**產生**。 新頁面隨即開啟，其中包含權杖和目標 SCIM URL 的詳細資訊。
5. 按一下**複製**以複製權杖或 SCIM URL。
6. 重新整理頁面。 **使用者佈建**頁面隨即顯示權杖狀態表。

變更權杖狀態

您可以變更現有權杖的狀態。

程序

1. 按一下**使用者佈建 Entra ID** 頁面上的**選取**下拉式功能表。
2. 按一下**選擇**，然後對權杖進行如下變更:

- **設為作用中**
- **設為無作用**
- **更新**
- **移除**

從「稽核追蹤」檢視權杖狀態

您可以從「稽核追蹤」區段檢視 SCIM 權杖上發生的操作/事件記錄。 SCIM 權杖可具備下列其中一種狀態:

- SCIM 權杖已建立 - 已經建立 SCIM 權杖。
- SCIM 權杖已啟用 - 已經啟用 SCIM 權杖。
- SCIM 權杖已停用 - 已經停用 SCIM 權杖。
- SCIM 權杖已更新 - 已經更新 SCIM 權杖。
- SCIM 權杖已刪除 - 已經刪除 SCIM 權杖。

「詳細資訊」欄位還列出了 SCIM 廠商名稱 (IDP)，例如 Azure、Okta 等。 這樣可以更方便地與 Ivanti Neurons for MDM 通訊。

在 SCIM 佈建中設定屬性

本節內容描述如何在使用者佈建期間為 IdP 建立自訂及企業屬性。

對應屬性

建立連線後，即可對應 IdP 和 Ivanti Neurons for MDM 之間的屬性。 Ivanti Neurons for MDM 支援下列使用者屬性:

核心屬性

- id
- userName
- displayname
- active
- givenName
- familyName
- emails

> 對於 Entra ID IdP，支援外部 IdP。

允許更新作業的屬性清單

- userName
- displayName
- emails
- givenName
- familyName
- active

- urn:ietf:params:scim:schemas:extension:ivanti:2.0:User
- urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

自訂屬性

結構描述 - urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<CustomAttribute123Name>

企業屬性

目前僅支援「部門」屬性。

結構描述 - urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department

12.2.10.2.1. Entra ID IdP 的使用者佈建

本節包含以下各主題：

- 建立與 Ivanti Neurons for MDM 的連線
- 佈建已指派的使用者和群組
- 佈建所有的使用者和群組
- 驗證已指派使用者佈建
- Entra ID IdP 的使用者佈建
- 編輯設定
- 配置自訂和企業屬性
- 移轉考量 - 從 Entra ID 使用者來源移轉至使用者佈建 SCIM
- 移轉考量 - 從 LDAP 移轉至使用者佈建 SCIM
- 重要說明 - SCIM

建立與 Ivanti Neurons for MDM 的連線

在 Entra ID Enterprise 應用程式上建立使用者和群組後，您可以在 Entra ID 和 Ivanti Neurons for MDM 之間建立連線。

程序

1. 登入 Entra ID 入口網站。
2. 前往**企業應用程式** > 按一下 **+ 建立自己的應用程式**。 「建立自己的應用程式」視窗隨即開啟。
3. 指定應用程式的名稱 (**預設: 不在資源庫內**)，然後按一下**建立**。 例如，Ivanti Neurons for MDM 使用者佈建。
4. 前往**佈建** > **編輯佈建** > **管理員認證**。
5. 從 Ivanti Neurons for MDM 管理員入口網站複製目標 SCIM URL，然後在 Entra ID 入口網站的**租用戶 URL** 欄位中貼上。
6. 從 Ivanti Neurons for MDM 中複製權杖，然後將其在 Entra ID 入口網站的**密碼權杖**欄位中貼上。
7. 執行下列其中一個步驟：
    - 選擇**僅同步已指派的使用者和群組**。 如需更多資訊，請參閱「佈建已指派的使用者和群組」
    - 選擇**同步所有的使用者和群組**。 如需更多資訊，請參閱「佈建所有的使用者和群組」。

    > 選擇同步所有的使用者和群組以移轉使用者。

按一下**測試連線**。 綠色打勾標記出現，確認連線。

9. 按一下**儲存**。
10. 在 Entra ID 入口網站的**佈建**頁面上展開**對應**。
11. 按一下**佈建 Entra ID 使用者**。 「屬性對應」頁面隨即開啟。
12. 按一下**刪除**，刪除不受支援的屬性。

佈建已指派的使用者和群組

在 Entra ID 和 Ivanti Neurons for MDM 之間建立連線後，即可佈建使用者或群組。

佈建群組時，Entra ID 不會將巢狀群組的成員新增至所選群組。 同步過程中，Entra ID 只將直接成員和群組名稱新增至該群組，而不新增子群組成員。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 在應用程式中，前往**使用者和群組** > 按一下 **+ 新增使用者/群組**。 新增指派頁面開啟。
3. 從**搜尋**欄位搜尋使用者或群組，按一下**選擇**，然後再按一下**指派**。 使用者和群組頁面開啟。
4. 選取相應的使用者或群組核取方塊。
5. 按一下**佈建**，然後按一下**開始佈建**。 成功組態的詳細資訊隨即顯示。

佈建所有的使用者和群組

在 Entra ID 和 Ivanti Neurons for MDM 之間建立連線後，您可以佈建使用者或群組。

程序

- 按一下**佈建**，然後按一下**開始佈建**。 頁面開啟，其中列出成功佈建的詳細資訊，以及將佈建至 Ivanti Neurons for MDM 的使用者。

驗證已指派使用者佈建

在 Entra ID 入口網站上佈建已指派的使用者後，請在 Ivanti Neurons for MDM 管理員入口網站上驗證佈建。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 在主功能表之下，前往**使用者**索引標籤。 已佈建的使用者將會列在此頁面的使用者清單中。

佈建過程可能需要長達一個小時。

驗證群組的佈建

在 Entra ID 入口網站上佈建群組後，請在 Ivanti Neurons for MDM 上驗證佈建。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 前往**使用者**索引標籤 > **使用者群組**。 已佈建的群組將會列在此頁面的群組清單中。

佈建過程可能需要長達一個小時。

編輯設定

本主題有助您進行 Entra ID 設定。

程序

1. 前往**管理員 > Microsoft Azure > 使用者佈建 Entra ID**。
2. 按一下**產生權杖**，然後複製權杖。

3. 重新整理頁面。「Entra ID 設定」頁面隨即開啟。
4. 按一下**編輯設定**。
5. 設定**自動邀請從 Entra ID 匯入的使用者** - 管理是否自動邀請從 Entra ID 匯入 Ivanti Neurons for MDM 的使用者以透過電子郵件註冊。
6. 設定**受控 Apple ID** - 此選項預設為停用。 按一下切換按鈕啟用它。 在佈建過程中，可以透過以下方式設定受管理 Apple ID:
   - **使用者電子郵件地址**
     - (選擇性) 選取納入 "appleid" 子網域選項，避免與現有 Apple ID 衝突。
   - 對應至**自訂屬性**

     > 自訂屬性應計算為唯一的電子郵件地址。
7. (選擇性) 按一下**新增自訂屬性** - 從您想要套用至裝置管理的目錄服務，指定自訂使用者屬性。 然後，每個屬性即可供支援變數之配置欄位中的 $ 參照。 使用此選項時，所有 Entra ID 伺服器的自訂屬性實作都必須保持一致。 如果實作中包含的 Entra ID 伺服器並未使用此屬性，則相依於此屬性的功能可能無法如預期運作。 **屬性類型**欄顯示了**編輯設定**區段內**自訂屬性**表格中的 **IDP** 屬性。
8. 修改 Entra ID 設定後，按一下**儲存變更**。

配置自訂和企業屬性

程序

1. 前往**管理員** > **身分識別** > **使用者佈建**。
2. 在**編輯設定**下，按一下 **+新增自訂屬性**。
3. 在**屬性名稱**欄位中輸入一個名稱 (例如 custAttr1) 並按一下**儲存變更**。 該屬性會在**管理員** > **系統** > **屬性**頁面中列出並可供使用。 該屬性會記為 IdP 屬性，而且您僅能執行刪除動作。
4. 登入 **Entra ID** 入口網站。
5. 前往**首頁** > **企業應用程式** > 按一下 SCIM 應用程式。
6. 在**對應**區段中按一下**佈建 Entra ID 使用者**。
7. 選取**顯示進階選項**核取方塊。
8. 按一下**編輯 customappsso 的屬性清單**。
9. 為您在 Ivanti Neurons for MDM 使用者介面中建立的自訂屬性輸入一個新項目。
10. 新增自訂/企業 (部門) 屬性的結構描述，如下所示:
    自訂屬性 - **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<custAttr1>** - 請參閱步驟 3。
    企業屬性 - **urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department**
11. 按一下**儲存變更**。
12. 按一下**新增對應**，並從下拉式功能表中選取來源與目標屬性。
13. 按一下**確定**，然後按一下**儲存對應**。
14. 前往**首頁** > **企業應用程式** > 按一下 SCIM 應用程式 > **使用者與群組**。
15. 按一下使用者名稱。 設定檔頁面隨即開啟。
16. 驗證與該屬性相關的值是否會出現在設定檔頁面中。
17. (選用) 按一下 SCIM 應用程式 > 佈建 > 隨選佈建，搜尋特定使用者，然後按一下佈建。 若要驗證在先前步驟中執行的新屬性對應。
18. 登入 Ivanti Neurons for MDM 管理入口網站。
19. 前往**使用者** > **使用者** > 選取使用者。

20. 按一下**屬性**索引標籤，然後驗證屬性值。 該屬性是針對特定使用者對應的。

移轉考量 - 從 Entra ID 使用者來源移轉至使用者佈建 SCIM

- 從 Entra ID 使用者來源移轉至使用者佈建 Entra ID (SCIM) 時，請選取「同步所有使用者和群組」。
- 使用 SCIM Entra ID 來源更新使用者和群組後，返回 Azure 中的「Azure 佈建」頁面，使用「僅同步已指派的使用者和群組」選項，將特定的使用者和群組設定為由使用者佈建 Entra ID 管理。
- 同步完成後，即可從 Ivanti Neurons for MDM 使用者和群組清單中移除未在 Azure 中定義的使用者和群組。
- 移轉開始時，只能在唯讀狀態下存取「Entra ID 使用者來源」頁面。

移轉考量 - 從 LDAP 移轉至使用者佈建 SCIM

先決條件:

1. **啟用此 LDAP 伺服器**預設為已選取。 移轉前必須先取消選取此選項。
2. 在 Entra ID 中建立一個企業應用程式，將同步的 LDAP 使用者/群組 (Ivanti 中存在的相同 LDAP 使用者/群組) 新增到 SCIM 應用程式中。 開始佈建。

LDAP 移轉至 SCIM 的重要注意事項

- LDAP 不會擷取已同步使用者/群組的所有資訊，而 SCIM 會在稽核記錄中記錄使用者/群組事件。
- 具有自訂屬性的 LDAP 使用者其類型會定義為 ldap，而 SCIM 則是 IdP。 因此，當具有自訂屬性的使用者從 LDAP 移轉至 SCIM 時，應在 SCIM 應用程式中建立對應的 IdP 自訂屬性，使用者才會移轉。 若使用者後續想要更新 ldap 自訂屬性，在移轉後，ldap.custom 屬性值將不會在 MDM 中更新。 IdP 屬性值將會更新。
- 移轉與一或多個自訂屬性 (特別是「ldap.custAttr1」) 相關聯的 LDAP 使用者，指出 LDAP 裝置的註冊，以及推送至 SAN 類型對應 LDAP 自訂屬性值的裝置之組態 (身分識別憑證組態)。
- 移轉受託管 Apple ID 與電子郵件地址關聯的 LDAP 使用者 - 因此，在從 LDAP 移轉到 SCIM 之前，如果使用者希望保留 LDAP 使用者的受管理 Apple ID 的值，則必須啟用 SCIM 設定中的受管理 Apple ID 並儲存設定。
- 若已在 LDAP 伺服器中移除 LDAP 使用者，該使用者仍會保持作用中，但該特定已同步 LDAP 使用者的同步旗標不會設定為 true。 在 SCIM 中，刪除已佈建使用者時，其使用者狀態會是已停用。
- 一旦為 SCIM 使用者設定身分識別提供者 (IdP) 的 SAML 後，來自本機和 LDAP 等不同來源的所有使用者都將透過 SAML 進行驗證。 只能將本機使用者新增至例外清單，以繞過 IdP 驗證流程。 此組態可以在 SAML 頁面中的**管理員** > **身分識別** > **SAML** 下進行管理。
- 為已移轉的 IDP (SCIM) 使用者設定 SAML 後，來自本機和 LDAP 等不同來源的其他使用者就可以繞過裝置註冊 (不透過 IDP)。 此設定可在**使用者** > **使用者設定**下進行管理。
- 在 LDAP 中，可支援使用者、群組和 OU，而在 SCIM 中，可支援使用者和群組，但不支援 OU。
- SCIM 不支援巢狀群組佈建流程。

重要說明 - SCIM

- 電子郵件地址是佈建和移轉使用者或成員的必填欄位。
- SCIM 提供從 Microsoft Entra ID 到 Ivanti Neurons for MDM 的單向佈建。 Ivanti Neurons for MDM 不提供任何同步選項。 如果從 Ivanti Neurons for MDM 中刪除 SCIM 佈建的群組或使用者，請確保同時從 Microsoft Entra ID 中移除該使用者或群組。
- 一個屬性 (來源或目標) 只能在 Microsoft Entra ID 的 SCIM 應用程式對應視窗中使用一次。 同一來源不能對應到特定目標屬性兩次。
- 非使用中使用者無法使用 SCIM 佈建或移轉至 Ivanti Neurons for MDM。
- Ivanti Neurons for MDM 目前不支援 SCIM 事件通知。

- 移轉或佈建持續時間取決於所涉及的使用者或群組數。
- Microsoft Azure 可控制佈建間隔，大約為 40 分鐘或更長時間。
- 在重新佈建期間，Microsoft Entra ID 將僅重試失敗的項目。 您可以下載佈建記錄，驗證已從 Microsoft Entra ID 成功佈建或佈建失敗的使用者。
- SCIM 中不允許來自不同來源的重複群組。
- 從 Microsoft Entra ID 中實刪除已佈建的使用者時，即會在 Ivanti Neurons for MDM 中停用該使用者。
- 從 Microsoft Entra ID 中刪除已佈建的使用者群組時，即會在 Ivanti Neurons for MDM 中刪除該群組，並停用屬於已刪除群組的獨立成員，並將其關聯到所有使用者群組。
- 從 Microsoft Entra ID 中實刪除已佈建群組的已佈建成員時，即會在 Ivanti Neurons for MDM 中停用該成員，但是，該成員仍與 Ivanti Neurons for MDM 中的群組保持關聯。
- 從應用程式中移除屬性 (企業屬性或自訂屬性) 對應時，被移除的屬性值仍會反映在 Ivanti Neurons for MDM 中。
- 當已佈建使用者的使用者屬性更新為空白值或空值時，更新的屬性值不會反映在 Ivanti Neurons for MDM 中。
- 如果從 Microsoft Entra ID 移轉或更新到 SCIM 時，使用者屬性 FName 和 LName (name.formatted) 為空白值，則移轉或更新將失敗。
- 如果從 Entra ID 中刪除使用者，則對應的 SCIM API 不會永久刪除該使用者，而會執行虛刪除並將使用者狀態從作用中變更為非作用中。如果要永久刪除使用者，請登入 Ivanti Neurons for MDM 管理入口網站並手動刪除非作用中/已停用使用者。
- 當 Ivanti Neurons for MDM 中存在具有特定使用者 ID 的本機使用者時，具有相同使用者 ID 的類似使用者將從 Entra ID 佈建到 MDM，使用者來源將從本機更新為 SCIM Entra ID。
- 具有 Entra ID Premium P1 訂閱的 Entra ID 有權佈建要指派和佈建的所需群組。

12.2.10.2.2. Okta IdP 使用者佈建

本節包含以下各主題：

- 建立與 Ivanti Neurons for MDM 的連線
- 佈建使用者和群組
- 驗證已指派使用者佈建
- 驗證群組的佈建
- 編輯設定
- 在 SCIM 使用者佈建期間設定自訂/企業屬性

建立與 Ivanti Neurons for MDM 的連線

在 **Okta** 應用程式上建立使用者和群組後，您可以在 **Okta** 和 Ivanti Neurons for MDM 之間建立連線。

程序

1. 登入 **Okta**。
2. 前往**應用程式** > **應用程式** > **瀏覽應用程式目錄**。
3. 搜尋**新增 SCIM 2.0 Test App** (OAuth Bearer 權杖) 並安裝應用程式。
4. 按一下此應用程式並前往**佈建** > **整合**。
5. 按一下**編輯**，提供基本 url 並貼上產生的權杖。
6. 按一下**儲存**。
7. 前往**佈建**，然後按一下**編輯**。
8. 啟用必要的使用者動作並按一下**儲存**。

佈建使用者和群組

在 **Okta** 和 Ivanti Neurons for MDM 之間建立連線後，即可佈建使用者或群組。

程序

1. 前往**指派** >**指派** >**指派給人員**或者**指派給群組**。
2. 2. 選取或搜尋現有使用者或群組，然後按一下**指派**。
3. 重複該過程以新增更多**使用者**或者**群組**。
4. 按一下**完成**。
5. 選取群組並按一下**按名稱推送群組**以儲存並同步群組。

驗證已指派使用者佈建

在 Okta 入口網站上佈建已指派使用者後，請在 Ivanti Neurons for MDM 管理入口網站上驗證使用者佈建。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 在主功能表之下，前往**使用者**索引標籤。 已佈建的使用者將會列在此頁面的使用者清單中。

驗證群組的佈建

在 Okta 入口網站上佈建群組後，請在 Ivanti Neurons for MDM 上驗證佈建。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 前往**使用者**索引標籤，然後按一下**使用者群組**。 已佈建的群組將會列在此頁面的群組清單中。

編輯設定

此主題有助您進行 Okta 設定。

程序

1. 前往**管理員** > **身分識別** > **使用者佈建 Okta**。
2. 按一下**編輯設定**。
3. 設定**自動邀請從 Okta 匯入的使用者** - 管理是否自動邀請從 Okta 匯入 Ivanti Neurons for MDM 的使用者以透過電子郵件註冊。
4. (選擇性) 按一下**新增自訂屬性** - 從您想要套用至裝置管理的目錄服務，指定自訂使用者屬性。 然後可在支援變數的「組態」欄位中透過 $ 引用每個屬性。 使用此選項時，所有 Okta 伺服器的自訂屬性實作都必須保持一致。 如果實作中的 Okta 伺服器並未使用自訂屬性，則相依於該自訂屬性的功能可能無法如預期般運作。 **屬性類型**欄顯示了**編輯設定**區段內**自訂屬性**表格中的 **IDP** 屬性。
5. 修改 Okta 設定後，按一下**儲存變更**。

在 SCIM 使用者佈建期間設定自訂/企業屬性

程序

1. 前往**管理員** > **身分識別** > **使用者佈建**。
2. 按一下**編輯設定**。
3. 輸入自訂屬性(例如 custAttr1) 並按一下**儲存變更**。
4. 在 Okta 入口網站中，按一下**目錄** > **設定檔編輯器**。
5. 按一下 **SCIM 2.0 Test App (OAuth Bearer 權杖) 使用者**應用程式
6. 按一下**新增屬性**。
7. 新增以下自訂屬性值，例如:
   - 顯示名稱 (與我們在 N-MDM 中提供的自訂屬性值相同，請參閱步驟 3)。
   - 變量名稱: custAttr1
   - 外部名稱: custAttr1
   - 外部命名空間: **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User**
   - 使用者權限: (讀/寫)
8. 按一下**儲存屬性**。
9. 按一下**設定檔編輯器** > **對應**。 您將看到兩個對應的部分 (SCIM 和 Okta)。
10. 將 N-MDM 中建立的自訂屬性對應到 Okta 中定義的屬性，並儲存對應。
11. 前往**使用者**，然後按一下所需使用者。
12. 按一下**設定檔** > **編輯**以編輯屬性。
13. 前往**應用程式** > **SCIM 2.0 Test App (OAuth Bearer 權杖)** 應用程式。

14. 在**指派**索引標籤下，按一下**指派**並選取**指派給人員**。
    將 SCIM 2.0 Test App (OAuth Bearer 權杖) 指派給人員視窗在螢幕上出現。
15. 選取所需的使用者，並按一下**指派**。
16. 按一下**完成**。

要在 Ivanti Neurons for MDM 中驗證自訂屬性及其對應:

- 前往**使用者** > **使用者** (任何特定使用者) > **屬性**。 確保 Okta 的對應自訂屬性在使用者屬性部分下可見。

12.2.11. 設定 LDAP 伺服器

授權： Silver

設定 LDAP 伺服器和 Connector 可讓您從公司目錄匯入使用者和群組。 安裝至少一個 Connector 之後，即可新增一或多部 LDAP 伺服器。

新增 LDAP 伺服器意謂著必須設定下列項目：

- LDAP 伺服器的*連線*
- 用來檢視目標目錄資料所需的*搜尋詞彙*
- 要*匯入*的目錄部分
- 針對所選的目錄部分，是否要自動*邀請使用者*

新增 LDAP 伺服器之後，您即可返回此頁面以**編輯 LDAP 伺服器資訊**或**變更選擇的 LDAP 使用者**。

> 設定好 LDAP 使用者之後，也必須匯入 LDAP 使用者。 請參閱**匯入 LDAP 使用者**。
> LDAP 使用者名稱與其他本機使用者名稱一樣，都必須是全域唯一。 請確認使用者尚不具備相同使用者名稱的本機帳戶，或者，使用者名稱並未與其他租戶建立關聯 (若組織具有多重租戶的話)。

新增 LDAP 伺服器

程序

1. 按一下 **+新增伺服器**。
2. 提供下列資訊：
3. 按一下**測試連線並繼續**。

設定	方法
名稱	輸入可識別此伺服器的名稱。
描述	輸入可說明此伺服器用途的描述。
目錄 URL	輸入目錄的 URL。 請使用下列任一格式： ldap://IP address 或 ldap://IP address 或 例如：ldap://myserver1.mycompany.com:389
使用者 ID	針對具有下列特性的帳戶，輸入使用者 ID： • 受 LDAP 伺服器所管理 • 可以與 LDAP 伺服器綁定，並搜尋使用者、群組和組織單位的子樹狀目錄 這通常是指具有目錄管理員憑證 (DN 或可辨別名稱和密碼) 的帳戶。
密碼	輸入帳戶密碼。
確認密碼	重新輸入帳戶密碼。
目錄類型	從支援的目錄清單中，選擇目錄類型。 • Microsoft Active Directory • 開啟 LDAP • 其他 (Open LDAP 相容)

4. 此步驟可驗證您目前提供的資訊。

- 如果資訊證實有效，服務就可以擷取 LDAP 命名內容，並使用這些內容填入下一頁的部分欄位。
- 如果 LDAP URL 無法連線，您仍可繼續接下來的步驟。 不過，在連線問題解決之前，可能會導致功能受限。

完成其餘的設定：

5. 按**下一步**。

設定	方法
目錄容錯移轉 URL	輸入次要目錄的 URL。 請使用下列格式： ldap://IP address 或 例如：ldap://myserver2.mycompany.com:389
同步間隔	輸入每次從 LDAP 伺服器嘗試進行 LDAP 資料同步的時間間隔。 預設值為 15 分鐘。 當您已成功同步所有目標 LDAP 的資料並確認 LDAP 設定符合需求後，即可考慮拉長間隔。
啟用捨棄同步	如果重新載入的資料集有嚴重衰退，則選擇自動捨棄 LDAP 同步資料。 此選項可確保部分 LDAP 系統的異常行為不會導致服務產生不必要的破壞性更新，並導致已註冊裝置的配置受到移除。 如果您打算在 LDAP 設定或 LDAP 伺服器進行主要更新，請不要選擇這個選項。
啟用此 LDAP 伺服器	選擇搭配使用這部 LDAP 伺服器與服務。 如果您想要淘汰這部 LDAP 伺服器或停用它的服務，請清除此設定。 雖然已設定容錯移轉的第二部 LDAP 伺服器會自動取代此伺服器，但使用這個選項可讓您未雨綢繆，避免容錯移轉期間的短暫斷線問題。
每當匯入使用者時即自動邀請。	選擇此選項時，每當從 LDAP 伺服器匯入使用者時，即會自動傳送邀請。
上傳 CA 憑證	按一下**選擇檔案**以上傳已安裝在此 LDAP 伺服器上的 CA 發行之 TLS 憑證。 您可上傳多個 CA 憑證。
追蹤轉介	僅有當您使用多樹系網域時，才適用。 此選項指出當目標網域控制器不具備要求物件的複本時，是否要使用其他網域控制器。 • 如果您想要使用轉介，請選擇**遵循**。 • 如果您不想使用其他網域控制器，請選擇**忽略**。 • 目前，**擲回**選項與**忽略**有相同的效果。 選擇**追蹤**延遲 LDAP 身分驗證。
搜尋結果逾時	如果您在瀏覽從 LDAP 伺服器同步的資料時發現效能問題或未完成的結果時，可增加此逾時。
搜尋結果計數	設定從 LDAP 伺服器一次可傳回的記錄上限數。 可能需要變更此設定以提升效能的案例包括： • LDAP 伺服器的位置太遠，或位在高度延遲的連結後方。 這種情況下，如果搜尋結果數量很大，會需要比少量結果更長的時間來擷取，因此定義較少的數量可讓您更快看到更新好的部分資料。 • LDAP 很大，每項搜尋都會傳回大量的結果集。 這種情況下，如果效能不是問題，則可定義較大量的結果集應以讓少量搜尋傳回所有的資料。

對於沙盒環境，LDAP 同步間隔不能小於 8 小時。

6. 使用下列方針，設定整合 LDAP 伺服器：
7. 按一下**瀏覽**或**搜尋**。

設定	方法
群組成員格式	選擇 **DN** 或 **UID** 指出搜尋中要使用可辨別名稱或使用者 ID。
OU 搜尋屬性	指定要在組織單位層級進行搜尋的準則。
起始點 DN	輸入要 root 或開始搜尋之起始層級的可辨別名稱。 您選擇的項目決定了其他若干欄位的預設值，您可視需要進行變更。
物件 GUID	若有必要，您可將預設值變更為符合 LDAP 環境的值。 在時間與 OU 名稱變更後，這是可唯一辨別組織單位的屬性。
屬性名稱	若有必要，您可將預設值變更為符合 LDAP 環境的值。
描述	若有必要，您可將預設值變更為符合 LDAP 環境的值。
屬性 DN	若有必要，您可將預設值變更為符合 LDAP 環境的值。
搜尋篩選	若有必要，您可將預設值變更為符合 LDAP 環境的值。
搜尋範圍	選擇要設為目標的 LDAP 階層： • **起始點** (僅搜尋起始點項目的層級) • **一層** (搜尋起始點下一層) • **子樹狀目錄** (搜尋 base DN 下之目錄資訊樹狀目錄中的子樹狀目錄)
使用者搜尋屬性	指定在給定目錄層級中搜尋使用者的準則。
起始點 DN	輸入您想搜尋之起始層級的可辨別名稱。
屬性 UID	若有必要，您可將預設值變更為符合 LDAP 環境的值。
物件 GUID	若有必要，您可將預設值變更為符合 LDAP 環境的值。 在時間與使用者名稱變更後，這是可唯一辨別使用者的屬性。
屬性 DN	若有必要，您可將預設值變更為符合 LDAP 環境的值。
名字	若有必要，您可將預設值變更為符合 LDAP 環境的值。
姓氏	若有必要，您可將預設值變更為符合 LDAP 環境的值。
顯示名稱	若有必要，您可將預設值變更為符合 LDAP 環境的值。
電子郵件地址	若有必要，您可將預設值變更為符合 LDAP 環境的值。
主體名稱	若有必要，您可將預設值變更為符合 LDAP 環境的值。
地區設定	若有必要，您可將預設值變更為符合 LDAP 環境的值。
成員	若有必要，您可將預設值變更為符合 LDAP 環境的值。
搜尋篩選	若有必要，您可將預設值變更為符合 LDAP 環境的值。
搜尋範圍	選擇要設為目標的 LDAP 階層： • **起始點** (僅搜尋起始點項目的層級)

設定	方法
	• **一層** (搜尋起始點下一層) • **子樹狀目錄** (搜尋 base DN 下之目錄資訊樹狀目錄中的子樹狀目錄)
受管理的 Apple ID	選擇為 LDAP 使用者同步受管理的 Apple ID。 • **無** • **模式** - ◦ **使用者電子郵件地址** ◦ **userUPN** 或者，選擇**包含「appleid」子網域**選項以避免與現有的 Apple ID 發生衝突。
+新增自訂屬性	(選用) 您可從欲套用裝置管理的目錄服務，指定最多 7 個自訂使用者屬性。 然後，每個屬性即可供支援變數之配置欄位中的 $ 參照。 **重要事項：**使用此選項時，所有 LDAP 伺服器的自訂屬性實作都必須保持一致。 如果實作中的 LDAP 伺服器未使用相同屬性，相依於此屬性的功能可能無法如預期般運作。
群組搜尋屬性	
起始點 DN	輸入您想搜尋之起始層級的可辨別名稱。
物件 GUID	若有必要，您可將預設值變更為符合 LDAP 環境的值。 在時間與群組名稱變更後，這是可唯一辨別群組的屬性。
屬性 DN	若有必要，您可將預設值變更為符合 LDAP 環境的值。
屬性名稱	若有必要，您可將預設值變更為符合 LDAP 環境的值。
描述	若有必要，您可將預設值變更為符合 LDAP 環境的值。
成員	若有必要，您可將預設值變更為符合 LDAP 環境的值。
搜尋篩選	若有必要，您可將預設值變更為符合 LDAP 環境的值。
搜尋範圍	選擇要設為目標的 LDAP 階層： • **起始點** (僅搜尋起始點項目的層級) • **一層** (搜尋起始點下一層) • **子樹狀目錄** (搜尋 base DN 下之目錄資訊樹狀目錄中的子樹狀目錄)

8. 確認您的配置可傳回預期的資料。
9. 您可在目錄中瀏覽或搜尋已知項目，以進行這項確認。

按**下一步**。

刪除自訂 LDAP 屬性

您可以刪除自訂 LDAP 屬性，並將這些值從相關聯使用者或裝置上移除。

程序

1. 前往**管理 > 屬性**。

2. 在**自訂屬性**區段中，按一下要刪除的 LDAP 屬性旁的**刪除**連結。 隨即顯示確認視窗。
3. 按一下**刪除**以確認刪除。

> **刪除**按鈕依預設為停用。您應選擇**本人瞭解刪除自訂屬性是無法取消的**選項中的勾選框，才能啟用**刪除**按鈕。

編輯 LDAP 伺服器資訊

程序

1. 前往**管理 > LDAP**。
2. 在 LDAP 伺服器項目中，選擇**動作**欄位的**編輯**圖示，即可檢視「連接 LDAP 伺服器」頁面。
3. 進行所需變更。
4. 按一下**測試連線並繼續**。
   如果 LDAP URL 無法連線，您仍可繼續接下來的步驟。 不過，在連線問題解決之前，可能會導致功能受限。
5. 按一下**瀏覽**或**搜尋**。
6. 確認您的配置可傳回預期的資料。
   您可在目錄中瀏覽或搜尋已知項目，以進行這項確認。
7. 按一下**完成**。

匯入 LDAP 使用者

程序

1. 前往**使用者**。
2. 按一下 **+新增 > 邀請來自 LDAP 的使用者**。
3. 按一下 LDAP 伺服器項目中的**選擇使用者**。
4. 在「新增 LDAP 使用者」頁面的搜尋欄位中，輸入使用者、群組或 OU 的名稱。
5. 若要加入新的使用者或群組，請按一下要加入之項目旁的 **+新增**。
6. 按**下一步**。
7. 選擇是否要傳送邀請：
   - 不邀請任何使用者
     若要稍後再傳送邀請，請前往**使用者 > 使用者**，然後選擇**動作 > 傳送邀請**，即可傳送邀請。
   - 邀請全部

按一下**完成**。

更新所選的使用者、群組或組織單位

程序

1. 前往**管理 > LDAP**。
2. 在 LDAP 伺服器項目中，選擇**動作**欄位的**管理使用者**圖示，即可檢視新增 LDAP 使用者頁面。
3. 若要新增使用者或群組，請在搜尋欄位中，輸入使用者或群組名稱。
4. 按一下您要新增之項目旁的 **+新增**。

5. 若要移除使用者、群組或 OU，請按一下要刪除之項目旁的移除圖示。
6. 按一下**完成**。

啟用捨棄 LDAP 同步通知

「啟用捨棄 LDAP 同步」通知用來預防因意外的大規模 LDAP 環境變更而造成服務中斷。

程序

1. 前往**管理 > LDAP**。
2. 在 LDAP 伺服器項目中，選擇**動作**欄位的**編輯**圖示，即可檢視「連接 LDAP 伺服器」頁面。
3. 選擇**啟用捨棄同步**勾選方塊。
4. 輸入重新載入 LDAP 資料的百分比值以觸發捨棄同步。
5. 按一下**測試連線並繼續**。
   如果 LDAP URL 無法連線，您仍可繼續接下來的步驟。 不過，在連線問題解決之前，可能會導致功能受限。
6. 按一下**完成**。
7. 按一下 LDAP 伺服器項目中的**立即同步**圖示。
   當從 LDAP 同步至 Ivanti Neurons for MDM 的變更差異超過所設的捨棄百分比時，就會產生「警告」通知。 當變更回落到所設的百分比以下時，就會將通知清除。

觸發	嚴重性	通知類型	元件類型	元件
捨棄 LDAP 同步	警告	資料同步	LDAP	LDAP 伺服器名稱
LDAP 同步已恢復	資訊	資料同步	LDAP	LDAP 伺服器名稱

「捨棄部分同步通知」產生於一或多位使用者記錄無法與 LDAP 同步時。 在這種情況下，無法同步的使用者清單會隨附附件。 如果使用者因為缺少屬性而遭捨棄時，缺少的屬性清單也會隨附在匯出的 CSV 檔案中。

同步處理來自 LDAP 伺服器的變更

在 LDAP 頁面中，按一下 LDAP 伺服器項目的**立即同步**圖示。

> 如果顯示名稱超過 128 個字元，LDAP 同步將忽略此類使用者，並繼續與其他使用者或使用者群組同步。

疑難排解 LDAPS 伺服器連線問題

如果無法順利連線 LDAPS (LDAP over SSL) 伺服器，可能是遇到認證問題。

若要解決問題：

- 請確認您在 LDAPS 伺服器上使用的不是自行簽署認證。
- 請確認 LDAPS 認證未過期或遭撤銷。 另請檢查主機名稱是否不相符。

驗證之後，請等待 LDAP 自動同步處理，或使用 LDAP 伺服器項目中的**管理 > LDAP > 立即同步**圖示，手動同步處理。

如果您無法看到「LDAP」頁面，可能是您沒有所需的權限。 您需具備下列其中一個**角色**：

- 系統管理

- 系統唯讀

12.2.12. Sentry

Sentry 是一種元件，可作為行動電話裝置和 ActiveSync 電子郵件系統之間的 gateway。 使用 Sentry 可控制哪些裝置可存取電子郵件。 它可以 ISO 檔案的形式下載，以便您安裝在虛擬機器上。 組織應考慮使用負載平衡器來維持多個 (備援) Sentry。

授權： Silver

最新文件

如需最新的 Sentry 指示說明，請造訪產品文件並按一下 Sentry。

如需最新的 Sentry 安裝指示，請選擇適當版本的 *Standalone Sentry On-Premise Installation Guide*。

如需 Sentry 升級指示，請選擇適當版本的 *Sentry Guide*。 請參閱 Sentry Guide 的下列章節：

- 如需使用獨立 Sentry System Manager UI 進行升級的指示，請參閱 "Standalone Sentry software updates”。
- 若是獨立 Sentry 命令列介面 (CLI)，請參閱 "Upgrading using CLI"。

升級之前，請參閱更新目標版本的獨立 Sentry 版本注意事項。

12.3. Apple 設定

本節包含以下各主題：

- Apple Configurator
- 裝置註冊
- 設定安裝小幫手
- 安裝 MDM 憑證
- 商務共享 iPad 裝置
- School Manager
- 設定 (Apple)

12.3.1. Apple Configurator

可使用此頁面來準備 Apple Configurator，以便在 iOS 裝置上設定 Ivanti Neurons for MDM 裝置管理。 Apple Configurator 可讓您大量並輕鬆部署 iOS 裝置。 此外，Configurator 可讓管理員將 iOS 裝置設為受監管裝置，以擁有更廣泛的配置和管理功能。 如需 Apple Configurator 的詳細資訊，請參閱 Mac App Store。

基本步驟為：

1. 從您的 Ivanti Neurons for MDM 租戶匯出 MDM 設定檔。
2. 將 MDM 描述檔匯入 Configurator。
3. 使用 Configurator 將 MDM 描述檔套用至綁定的裝置。

定義裝置的預設使用者

透過 Apple Configurator 設定的裝置將會指派給 Ivanti Neurons for MDM 中的 Nobody 使用者，除非您選擇不同的使用者：

1. 按一下**將配置的裝置指派到**欄位。
2. 開始輸入所選 Ivanti Neurons for MDM 使用者的使用者名稱。
3. 當下拉清單顯示使用者名稱時，即可選擇。
4. 按一下**儲存**。

使用 Apple Configurator 安裝 app

在使用 Apple Configurator 安裝 app 之前：

- 裝置配置應已設定 Apple App Store 的取用限制。
- 裝置配置應允許安裝 app。
- 用來設定裝置的電腦必須安裝 Apple Configurator。

若要使用 Apple Configurator 安裝 app：

1. 在 Ivanti Neurons for MDM 中，前往**管理 > Apple Configurator**。
2. 將註冊裝置切換開關轉換為「開啟」。
3. 按一下下列選項之一：
    - **預設使用者的 plist**。
    - **特定使用者的 plist** - 輸入特定使用者的使用者名稱或電子郵件 ID。

在 Apple Configurator 中，前往**準備 > App**。

5. 前往**準備 > 設定和停用監管**。
6. 在「更新 iOS」中，選擇**永不更新裝置**選項。
7. 按一下**準備** (位於 Apple Configurator 底部)。
   裝置登記後，裝置上「已安裝的 App」清單即會顯示 app。

使用 UEM 伺服器安裝 app

若要使用 UEM 伺服器安裝 app：

1. 從「應用程式」索引標籤中的內部商店下載 app。
2. 選擇 app。
3. 按一下 **App 配置**索引標籤。
4. 選擇**安裝到裝置上**。
   完成配置設定。
5. 選擇**動作 > 強制登記**。

一般使用者該怎麼做

Apple 要求一般使用者必須啟動 Go 至少一次，否則 Ivanti Neurons for MDM 定位功能將無法正常運作。 這是為了確保一般使用者瞭解他們的位置正受到追蹤。

注意：如果裝置是使用 Configurator 部署為單一應用模式，就無法使用此方法。

如果您無法看到**安裝 Apple Configurator** 頁面，可能是您沒有所需的權限。 您需具備下列其中一個角色：

- 系統管理
- 系統唯讀

12.3.2. 帳戶導向註冊

本節適用於帳戶導向使用者和帳戶導向裝置註冊。

支援的裝置

- 搭載 iOS 15+ (用於帳戶導向使用者註冊) 和 iOS17+ (用於帳戶導向裝置註冊) 的裝置
- macOS 14+ 裝置
- visionOS 1.1+ 裝置

必要條件：

針對帳戶導向使用者註冊

- Ivanti Neurons for MDM 中具有受管理 Apple ID 的使用者帳戶 (Apple 商務管理或 Apple 校務管理中的使用者)。
- 在 **Apple 註冊**區段下，選取**選取 Apple 註冊類型**下拉式清單中的**使用者註冊**。
- 在**使用者 → 使用者設定**底下 → 將**裝置擁有者設定**設為**開啟** > 選取**使用者擁有**選項。

針對帳戶導向裝置註冊

- 在 Ivanti Neurons for MDM 中具有受管理 Apple ID 的使用者帳戶 (Apple 商務管理或 Apple 校務管理中的使用者)。
- 在 **Apple 註冊**區段下，選取**選取 Apple 註冊類型**下拉式清單中的**裝置註冊**。
- 在**使用者 → 使用者設定**底下 → 將**裝置擁有者設定**設為**開啟** > 選取**公司擁有**選項。

適用於 iOS 15+、macOS 14+ 及 visionOS 1.1+ 裝置的**帳戶導向使用者註冊**是專為實作自攜裝置 (BYOD) 的公司而設計的註冊選項。 「帳戶導向使用者註冊」為 MDM 通訊協定和透過 Apple Business Manager 進行使用者註冊的修改版本，更注重使用者隱私權，以企業所需的安全性層級建置。

適用於 iOS 17+、macOS 14+ 及 visionOS 1.1+ 裝置的**帳戶導向使用者註冊**是專為需要註冊公司擁有裝置/企業裝置的公司而設計的註冊選項。帳戶導向裝置註冊運用 MDM 通訊協定，而使用 Apple 商務管理進行裝置註冊則更注重使用者隱私權，以企業所需的安全性層級實作。 一般使用者可以使用「設定」中的「工作帳戶」功能註冊其裝置。

設定探索服務

如果貴企業具備企業網域名稱 (例如 acme.com)，則您裝置的電子郵件 ID 會是 devicename@acme.com。

1. 使用者輸入 username@acme.com 以登入其工作或學校帳戶，然後裝置會發出 HTTP GET 要求呼叫至 URL:
   https://acme.com/.well-known/com.apple.remotemanagement?user-identifier=user@acme.com
   如需詳細資訊，請參閱 - https://developer.apple.com/documentation/devicemanagement/discover_authentication_servers
2. 在 acme.com 網域上，為 URI - /.well-known/com.apple.remotemanagement 設定重新導向規則，將其重新導向至下列 URL:
   https://<n-MDM cluster>/.well-known/com.apple.remotemanagement

簡化帳戶導向裝置註冊的服務探索

> 適用於 iOS 18.2+、macOS 15.2+ 和 visionOS 2.2+ 裝置。

對於帳戶導向註冊，當使用者輸入其組織電子郵件登入其工作或學校帳戶時，裝置首先會在組織網域中搜尋知名的 HTTP 資源，其中包含指向 MDM 註冊 URL 的連結。

程序

1. 登入工作或學校帳戶。
2. 在 **Apple Business Manager** 和 **Apple School Manager** 中驗證網域 - 僅適用於已在 Apple Business Manager 或 Apple School Manager 中驗證的網域。 如果已經驗證網域，則裝置可以向 Apple Business Manager /Apple School Manager 查詢，取得替代的 MDM 註冊 URL。
3. 為 **Mac**、**Apple Vision Pro**、**iPhone**、和 **iPad** 等平台類型，設定預設 Ivanti Neurons for MDM 指派。
   若要設定預設裝置指派，請依照下列步驟進行：
   1. 在 **Apple Business Manager** / **Apple School Manager** 中，使用具有管理員或裝置註冊管理員角色的使用者身分登入。
   2. 在側邊列底部選取您的姓名，選取偏好設定，然後執行下列其中一項操作：
      - 選取裝置管理服務下方的裝置管理服務指派，然後選取預設裝置管理服務指派旁的編輯。
      - 選取裝置管理服務下的現有服務，然後選取預設裝置指派下的變更。
   3. 如果您沒有任何其他已設定的裝置管理服務，請將所有自動裝置指派變更為所選服務，然後選取**儲存**。
4. 在 Ivanti Neurons for MDM 控制台，瀏覽移到到**管理** > **Apple** > **裝置註冊**。 在**裝置註冊**畫面，新增了 **ADDE URL** 和 **ADDE URL SET TIME** 欄。

> **第一優先**: 裝置會檢查組織網域的知名 HTTP 資源。

後備選項: 如果第一種方法失敗，裝置會聯絡 Apple ABM/ASM 以取得由 Ivanti Neurons for MDM 指定的備用目的地。

5. 在**動作**下方，選取**設定 ADDE URL**。
6. 重新整理頁面。

裝置使用者說明

本主題說明裝置使用者在進行帳戶導向使用者註冊或帳戶導向裝置註冊時需要採取的動作。

程序

1. 在裝置上前往下列其中一個位置:
   - **iOS** 裝置 - **設定** > **一般** > **VPN** 和**裝置管理**。
   - **macOS** 裝置 - **系統設定** > **隱私權和安全性** > **設定檔**。
   - **visionOS** 裝置 - **設定** > **一般** > **VPN** 和**裝置管理**。
2. 前往**登入工作或學校帳戶**。
3. 輸入工作或學校帳戶電子郵件地址。 確定電子郵件地址的格式如下：
   username@<enterprise domain name>，例如，username@acme.com。
4. 登入頁面會自動使用受管理的 Apple ID，並引導使用者進入 iReg 流程。 確認您輸入了 Ivanti Neurons for MDM 憑證。
5. 輸入工作或學校帳戶認證，然後按一下**繼續**。
6. 在進行雙因子身分認證後，裝置註冊完成。

12.3.3. 裝置註冊

「裝置註冊」屬於 Apple Business Manager 的一部分，可讓客戶大量購買裝置，並於啟動期間在 MDM 中自動註冊這些裝置。 如果您選擇參與，可使用 Ivanti Neurons for MDM 做為管理這些裝置的 MDM·伺服器。 如需更多資訊，請參閱 https://business.apple.com/。

將 Ivanti Neurons for MDM 連接至「裝置註冊」

如要使用 Ivanti Neurons for MDM 做為「裝置註冊」的 MDM 伺服器，請在 Ivanti Neurons for MDM 中設定 Apple Business Manager 伺服器權杖。

每一部 Apple Business Manager 伺服器都可在 Ivanti Neurons for MDM 中執行下列動作：

- 測試連線
- 新增 Device Enrollment 描述檔
- 下載公用金鑰
- Device Enrollment 完整同步 - 起始完整同步。 可能需要一段時間才能完成。 同步完成之後，您將可以在上次同步欄中看到資訊。 如果完整同步已在進行中，您將無法起始它。

> 當 DEP 伺服器同步失敗時 Ivanti Neurons for MDM 會通知管理員，以便更容易識別問題。 如果您刪除 DEP 伺服器，系統也會刪除其相關通知。

- 上傳新權杖
- 刪除

> **編輯身份認證**和**指派 Device Enrollment 裝置屬性**動作現在適用於 Device Enrollment 描述檔而非 Device Enrollment (MDM 伺服器)。

程序

1. 前往**管理** > **Apple** > **Device Enrollment**。
2. 按一下**下載金鑰**。
3. 儲存您的 Ivanti Neurons for MDM金鑰。
4. 按一下 **business.apple.com**。
5. 使用符合 Device Enrollment 資格的 Apple 憑證登入。
6. 在 Apple Device Enrollment 網站上：
7. 在 Ivanti Neurons for MDM中，按一下**上傳**。
8. 按一下**開始使用**。
9. 選擇受信任的手機，以與 Apple 服務進行驗證。
10. 輸入傳送給所選手機的驗證碼。
11. 按一下**新增 MDM 伺服器**。
12. 輸入可識別要搭配服務使用之 MDM 伺服器的名稱。
13. 按**下一步**。
14. 上傳您之前下載的公用金鑰。
15. 按**下一步**。

16. 按一下**您的伺服器權杖**，以下載權杖。
17. 按一下**完成**。
18. 按**下一步**。
19. 選擇驗證選項：

- **提示使用者註冊/登入**

> 不支援使用 visionOS 平台操作的裝置。 請改用**略過使用者登入**來註冊裝置。

> 系統會提示使用者輸入使用者名稱和密碼。 使用者可在密碼欄位中輸入密碼或 PIN 碼。 對於 macOS 15+ 裝置，iDP 使用者還可以在支援金鑰的身分提供者上使用 **Face ID**、**Touch ID** 或**安全金鑰**等其他選項。 您可在與驗證相關聯的「**使用者**」> 使用者設定中，設定密碼和 PIN 碼。

- **略過使用者登入**

> 如果裝置未指派給任何人 (匿名) 或已指派給定義使用者，則可在稍後透過**裝置**頁面重新指派給特定使用者。

請選擇下列選項之一：

  - **定義要指派所有裝置的一位使用者**
  - **指派所有裝置給匿名使用者**

10. 所選的選項即會覆寫使用者設定下方的選項。

按一下**上傳**，即可安裝在步驟 3 中收到的金鑰。

11. 填妥顯示的表單，以定義 Device Enrollment 裝置的描述檔：
12. 定義使用者在幫裝置啟用下列設定選項時可略過哪些步驟：

設定	方法
名稱	輸入可識別此 Device Enrollment 描述檔的名稱。
描述	輸入描述檔的描述。
部門	輸入與此描述檔相關聯的組織部門。
受監管模式 iOS 17+	可啟用配置與限制方面的其他管理控制權。 對於 iOS 13+ 和 macOS 10.15+ 裝置，此選項預設為啟用。 **用於註冊的作業系統版本** • **註冊時需要具備最低作業系統版本**: 管理員可以設定裝置註冊所需的最低作業系統版本。 如果裝置不符合最低作業系統版本標準，系統會提示使用者升級到所需版本。 如果使用者拒絕升級，將無法註冊。 **最新版本**: 管理員可以設定用於裝置註冊的最新作業系統版本。 如果裝置不符合最新作業系統版本標準，系統會提示使用者升級到所需版本。 如果使用者拒絕升級，將無法註冊。 **特定版本**: 管理員可以設定裝置註冊所需的最低作業系統版本。 如果裝置不符合最低作業系統版本標準，系統會提示使用者升級到所需版本。 如果使用者拒絕升級，將無法註冊。 • **最低 iOS 版本**: 如果組建版本與在 '**OSVersion**' 機碼中指定的作業系統版本不一致，則作業系統版本優先。 • **最低組建版本**: 如果組建版本與在 '**OSVersion**' 機碼中指定的作業系統版本不一致，則作業系統版本優先。 如果您輸入的組建編號不正確，則此為選填欄位。 • **訊息**: 適合向使用者顯示的錯誤說明。 如果需要， ◦ 用戶端將盡量嘗試顯示訊息，但可能會 ◦ 因為本機條件而無法顯示。 慣例上，應該新增此訊息。 • **將裝置新增至 Beta 版程式** **iOS 的測試版程式**: 在自動裝置註冊期間在 iOS 上強制執行測試版軟體。
macOS 14+	**用於註冊的作業系統版本** • **註冊時需要具備最低作業系統版本**: 管理員可以設定裝置註冊所需的最低作業系統版本。 如果裝置不符合最低作業系統版本標準，系統會提示使用者升級到所需版本。 如果使用者拒絕升級，將無法註冊。 **最新版本**: 管理員可以設定用於裝置註冊的最新作業系統版本。 如果裝置不符合最新作業系統版本標準，系統會提示使用者升級到所需版本。 如果使用者拒絕升級，將無法註冊。 **特定版本**: 管理員可以設定裝置註冊所需的最低作業系統版本。 如果裝置不符合最低作業系統版本標準，系統會提示使用者升級到所需版本。 如果使用者拒絕升級，將無法註冊。 • **最低 macOS 版本**: 如果組建版本與在 '**OSVersion**' 機碼中指定的作業系統版本不一致，則作業系統版本優先。 • **最低組建版本**: 如果組建版本與在 '**OSVersion**' 機碼中指定的作業系統版本不一致，則作業系統版本優先。 如果您輸入的組建編號不正確，則此為選填欄位。 • **訊息**: 適合向使用者顯示的錯誤說明。 如果需要， ◦ 用戶端將盡量嘗試顯示訊息，但可能會 ◦ 因為本機條件而無法顯示。 慣例上，應該新增此訊息。 • **將裝置新增至 Beta 版程式** **macOS 的測試版程式**: 在自動裝置註冊期間在 macOS 上強制執行測試版軟體。

設定	方法
自動下載並安裝 iOS 更新	(僅限 iOS 9.0+) 若在裝置上的**設定 > iTunes 與 App Store** 下選取了「自動下載」選項，系統將自動下載作業系統更新但不安裝，即使在「裝置註冊設定檔」選項已關閉時也是如此。 出現適用於已註冊 Device Enrollment 的受監管裝置的「iOS 軟體更新」配置時，將會優先使用此設定。 對此設定所做的任何更新將會套用至已註冊 Device Enrollment 的受監管裝置，即使未重設裝置也一樣。
MDM 可移除	定義使用者在裝置註冊後是否無法從 MDM 取消註冊。 此設定不適用於**共享 iPad**。
MDM 為必要	定義使用者在啟用程序期間是否無法略過安裝 MDM。 對於 iOS 13+ 和 macOS 10.15+ 裝置，此選項預設為啟用。
不使用備份中的設定檔	啟用時，當您從備份復原裝置時，裝置不會使用此設定檔。 僅適用於 iOS 26+ 和 visionOS 26+ 裝置。
允許配對	(不適用於 iOS 13+ 和 macOS 10.15+) 允許主機配對功能，例如 iTunes 同步。 具備有效配對憑證的主機一律允許配對。
恢復服務	將**恢復服務**設定為 **True**，以確保應用程式在執行**恢復服務**動作時得到保留。 這使裝置能夠對應用程式拍攝快照，並在恢復服務過程中提供更快的體驗。 如果停用的裝置仍然可以執行恢復服務，則必須在重新註冊過程中再次下載應用程式。 為了利用 **Apple Migration ABM** 功能，需要停用此功能。 如果**恢復服務**設定為 **True**，則無法移轉裝置。 僅適用於 iOS 26+ 和 visionOS 26+ 裝置。
認證	按一下 **+新增**以上傳憑證。
支援電話號碼	提供裝置使用者在需要協助時可聯絡的電話號碼。
支援電子郵件地址	提供裝置使用者在需要協助時可聯絡的電子郵件地址。
自訂註冊	(iOS 13.0+ 和 macOS 10.15+) 建立自訂註冊網頁。 指定您在 Device Enrollment 期間用來認證使用者身份的自訂網頁 (web view)。 使用此頁面來顯示自訂資訊，例如身份認證類型、品牌化、同意文字和隱私權政策。 請參閱「*新增自訂裝置註冊網頁*」一節，依照此程序以取得詳細資訊。 • 選擇**啟用自訂註冊**以啟用此功能。 • 輸入 **URL**，例如 https://mycustomweburl.com。 此 URL 定義在 web view 中向使用者顯示的自訂 URL 值。
多使用者	(iOS 13.4+) 商務用共享 iPad 讓企業在多名員工之間共用裝置，同時仍能提供個人化體驗。 選擇**多使用者模式**，在裝置上啟用共享 iPad。 如需更多資訊，請參閱**商務共用 iPad**。 • 此設定不變更為 Apple 教育。 • 選擇**受監管模式**設定來修改多使用者設定。
額度大小	(iOS 13.4+) 商務用共享 iPad。 此值以 MB 為單位，表示裝置中為使用者配置的儲存空間。 如果此值太小，裝置將配置預設配額大小。

設定	方法
常駐使用者人數	(iOS 13.4+) 商務用共享 iPad 此值代表保留或常駐在裝置上的使用者人數。 如果此值大於裝置支援的使用者人數上限值，MDM 伺服器會使用該值（使用者人數上限值）為預設值。 管理員可提供額度大小或常駐使用者人數值。 如果這兩個值都提供，MDM 伺服器會使用額度大小為預設值。
使用者工作階段逾時	(iOS 14.5+) 商務用共享 iPad 顯示使用者工作階段的逾時秒數。 在閒置指定秒數後，使用者工作階段會自動登出。 最小值為 30 秒。 將此值設為 0 會移除逾時，並設為裝置預設逾時。 1 到 29 的值為無效。 設定後，裝置會預設為逾時。
暫存工作階段逾時	(iOS 14.5+) 商務用共享 iPad 顯示訪客或暫存工作階段的逾時秒數。 在閒置指定秒數後，暫存工作階段會自動登出。 最小值為 30 秒。將此值設為 0 會移除逾時，並設為裝置預設逾時。 1 到 29 的值為無效。 設定後，裝置會預設為逾時。
僅限暫存工作階段	(iOS 14.5+) 商務用共享 iPad 如為 true，使用者僅會看到訪客觀迎窗格，而且只能登入為訪客使用者。 如為 false，使用者可使用受管理的 Apple ID 登入（現有的行為）。 預設：false
受管理的 Apple ID 預設網域	(iOS 16.0+) 商務用共享 iPad 指定網域清單。 使用者可透過 QuickType 鍵盤在網域清單中選取其帳戶網域。
線上驗證寬限期	(iOS 16.0+) 商務用共享 iPad 指定使用者可在不連線至網路的情況下登入的天數。 如果將此值設定為零，則使用者每次登入時都必須進行線上驗證。 **預設值**: 0
自動鎖定時間	(iOS 17.0+) 指定裝置在經過多少時間後進入睡眠模式 (秒)。 最小值為 120 秒。
「密碼鎖定」寬限期	指定在經過多少時間後裝置使用者必須輸入設備密碼以解除鎖定 (秒)。 最小值為 0 秒，最大值為 14400 秒。
時區	指定裝置必須歸屬的時區。 **範例**: Pacific/Midway

設定選項

- 略過密碼輸入 - 選取此選項將自動啟用「略過 Apple Pay」設置和「略過 Touch ID」
- 略過位置服務
- 略過從備份還原
- 略過從 Android「移動至 iOS」
- 略過服務條款
- 略過 Apple ID 和 iCloud 登入 - 選擇此選項將會自動啟用「略過 Apple Pay 設定」.
- 略過 Touch ID 設定 (僅限 iPhone 5s、6、6+、iPad Air 2、iPad Mini 3) - 選擇此選項將會自動啟用「略過 Apple Pay 設定」。
- 略過 Apple Pay 設定 (僅限 iPhone 6、 6+、iPad Air 2、iPad Mini 3)
- 略過縮放設定
- 略過 Siri
- 略過 Intelligence (iOS 18+ 和 macOS 15+)
- 自動略過傳送診斷資訊
- 略過 Cloud Storage (iOS 10.3+ 與 macOS 10.13.4+)
- 略過顯示色調設定 (iOS 9+ 與 macOS 10.14+)
- 略過主畫面按鈕敏感度
- 略過鍵盤選擇畫面
- 略過開始使用資訊畫面 - 此資訊用於使用者教育訓練。 例如：封面頁、多工處理與控制中心。
- 略過 Apple Watch 移轉畫面
- 略過選擇您的外觀畫面 (iOS 13.0+ 與 macOS 10.14+)
- 略過螢幕時間 (iOS 12.0+ 與 macOS 10.15+)
- 略過隱私權 (macOS 10.13.4+ 與 tvOS 11.3+)
- 略過啟用鎖定模式 (iOS 17.1+ 和 macOS 14.0+)
- 略過軟體更新 (iOS 12.0+ 和 macOS 15.4+)
- 略過新增行動方案窗格 (iPhone Xs 與 iPhone Xs Max、iPhone XR)
- 在登入頁面中顯示自訂文字 - 選擇此選項以在文字方塊中輸入自訂文字訊息。 此訊息將會在設定 Device Enrollment 時顯示於裝置的登入頁面中，以提供更多指示給一般使用者，協助他們逐步完成程序。
- 自動前進設定 - 選擇此選項以設定助理在裝置設定畫面中自動前進。 預設設為 false。 支援 tvOS 和 macOS 11 及更新版本。 自動前進設定不適用於 Wi-Fi 連線，裝置應透過乙太網路連接。
- 稱謂詞 - 跳過「稱謂詞」窗格。 (iOS 16+)
- 略過 Liquid Glass 窗格 (iOS 27.0+ & macOS 27.0+)

iOS

- 略過開始使用窗格 (13.0+)
- 略過 iMessage & FaceTime (12.0+)
- 跳過 Spoken Language (13.0+)
- 略過還原完成 (14.0+)

設定選項
• 略過更新完成 (14.0+) • 略過 Safety (16.0+) • 略過動作按鈕設定窗格 (17.0+) • 略過 Web 內容篩選窗格 (18.2+) • 略過安全與處理窗格 (18.4+) • 略過多任務窗格(26.0+) • 略過作業系統展示窗格 (26.0+) • 略過協助工具外觀窗格 (27.0+)
macOS
• 略過 iCloud Analytics 畫面 • 略過原彩顯示器畫面 (10.13.6+) - (選用) 選取此選項可略過原彩顯示器視窗。 • 略過協助工具 (11.0+) • 略過使用手錶解鎖 (12.0+) • 略過啟用鎖定模式 (14.0+) • 略過桌布選擇 (14.1+) • 略過其他設定隱私窗格 (26.0+) • 略過更新完成 (26.0+)
tvOS • 略過 Apple TV 主畫面版面配置同步畫面 • 略過 Apple TV 提供者登入畫面 • 略過點一下設定選項 • 略過空照圖螢幕保護程式設定 **macOS 帳號設定輔助程式選項** • 略過管理帳戶的建立 • 略過主要設定帳號建立 • 以一般使用者的形式建立主要帳戶 (若未勾選則會以管理員的形式建立) 在裝置註冊設定期間等待裝置組態 • 等待組態和高優先順序的應用程式推送至裝置 - 選取此選項可將組態和高優先順序應用程式推送至裝置，然後再繼續執行其餘裝置註冊設定畫面上的操作。 此設定將防止一般使用者在所需的組態和高優先順序應用程式尚未推送到裝置之前即使用裝置。 • 時間限制 - 預設的時間限制為 3 分鐘。 時間最長 10 分鐘。 若要啟用此功能，請在編輯 Device Enrollment 描述檔時選擇**受監管模式**選項。

按一下**儲存**。

在**管理** > **Apple** > **裝置註冊**頁面中填入下表:

設定	方法
名稱 (按一下欄標題以英數字元排序。) 使用「搜尋」欄位來搜尋此欄中的項目	MDM 伺服器名稱
Apple 帳戶名稱 (按一下欄標題以英數字元排序。) 使用「搜尋」欄位來搜尋此欄中的項目	受管理的 Apple ID
裝置數目	已指派的裝置數
註冊設定檔	指派的裝置註冊設定檔計數
上次同步時間 (按一下欄標題以英數字元排序。)	上次聯絡時間
過期的權杖 (按一下欄標題以英數字元排序。)	權杖到期日

- 將新裝置新增到「Apple 裝置註冊」時，Ivanti Neurons for MDM 可能要會花 15 分鐘才可以發現這些新裝置。 這些新裝置接著會指派給註冊描述檔。 如果您無法將新裝置加入 Device Enrollment，請前往**儀表板 > 通知**，檢查是否有來自 Apple 的 Device Enrollment 通知。 如果 EULA 有任何更新，您將會收到通知電子郵件，其中說明接受新 EULA 的步驟。
- 您可以檢視租戶中存在的所有自訂裝置屬性，並在裝置透過 Apple Device Enrollment 進行註冊時，將這些屬性指派給裝置。
- 在共用的 macOS 裝置中，ListUsers 指令顯示裝置上的所有本機使用者清單，並且僅顯示已註冊裝置使用者的上次簽入詳細資訊。

編輯 Device Enrollment 描述檔

程序

1. 前往**管理** > **Apple** > **Device Enrollment**。
2. 在「Apple 帳戶名稱」欄位中，尋找 Apple Business Manager 伺服器的名稱 (您在 Apple 網站上建立)。
3. 按一下「Enrollment 描述檔」欄位中的數字連結。
4. 針對特定描述檔，選擇**動作** > **編輯 Device Enrollment 描述檔**。
5. 更新並儲存描述檔。

- 如果已編輯裝置註冊描述檔，不久便會更新已修改之描述檔的裝置計數。
- 如果您重新整理 Apple 網站的伺服器權杖，現有的權杖就會失效。 不過，在「Device Enrollment」頁面的顯示項目，包括權杖的到期日都仍會保持原狀，直到您上傳新的權杖為止。
- 如果建立或編輯了裝置註冊描述檔，則可以在「稽核試驗」區段檢視對描述檔所做的更改。 按一下「詳細資訊」下的連結時，可以檢視「屬性」，以及「下列時間之前」和「下列時間之後」欄下對屬性所做的更改。 您可以注意到每個裝置註冊描述檔的狀態為「已建立」(用於新描述檔)、「已更新」(用於編輯任何現有描述檔) 或「已刪除」(用於刪除任何現有描述檔)。 要篩選稽核追蹤下的裝置註冊描述檔，您需要選取管理系統作為類別，並選取自動化裝置註冊類型作為類型。

裝置註冊設定檔包含下列詳細資料:

設定	方法
設定檔名稱 (按一下欄標題以英數字元排序。)	輸入可識別此 Device Enrollment 描述檔的名稱。
描述 (按一下欄標題以英數字元排序。)	輸入描述檔的描述。
部門 (按一下欄標題以英數字元排序。)	輸入與此描述檔相關聯的組織部門。
支援電話號碼 (按一下欄標題以英數字元排序。)	提供裝置使用者在需要協助時可聯絡的電話號碼。
裝置數目	顯示設定檔的裝置數目
動作	管理設定檔

管理多個 Device Enrollment 描述檔

您可以針對每一部 Apple Business Manager 伺服器，建立多個 Device Enrollment 描述檔。 如此一來，不同組合的裝置即可收到不同的配置。 裝置也可以從某個 Device Enrollment 描述檔移到另一個。

程序

1. 前往**管理** > **Apple** > **Device Enrollment**。
2. 在「Apple 帳戶名稱」欄位中，尋找 Apple Business Manager 伺服器的名稱。
3. 按一下「Enrollment 描述檔」欄位中的數字連結。
4. 如要建立新的 Device Enrollment 描述檔，以便與所選伺服器建立關聯，請按一下**新建描述檔**。 建立並儲存描述檔。
5. 如要管理每個描述檔，請按一下**動作**，並選擇下列其中一個選項：
   - **設為預設值描述檔** - 將描述檔設為相同虛擬伺服器內的預設描述檔。 新裝置註冊將會接收此預設描述檔。
   - **編輯描述檔** - 更新現有的描述檔。
   - **編輯身份認證** - 編輯 Device Enrollment 身份認證設定。
   - **指派 Device Enrollment 裝置屬性** - 管理員可利用裝置的自訂屬性，來建立額外屬性與這些物件的關聯。 然後，這些屬性可用來建立群組或發佈配置。
   - **刪除** - 無法刪除預設描述檔。 刪除非預設描述檔時，所有相關聯的裝置都將重新指派給預設描述檔。

6. 如要在相同的虛擬伺服器內 (而非不同的 Apple Business Manager 伺服器之間) 將已註冊的裝置從某個描述檔移到另一個描述檔，請按一下「裝置數量」欄位下的數字連結。 描述檔重新指派設定適用於尚未註冊的裝置。
    1. 如要移動單一裝置，請針對特定裝置按一下**指派 Enrollment 描述檔**，從下拉式清單中選擇描述檔，然後按一下**指派**。
    2. 如要移動多個裝置，請選擇裝置並按一下**動作** > **指派 Enrollment 描述檔**，從下拉式清單中選擇描述檔，然後按一下**指派**。

- 如果已編輯 Device Enrollment 描述檔，不久便會更新已修改之描述檔的裝置計數。
- 如果您重新整理 Apple 網站的伺服器權杖，現有的權杖就會失效。 不過，在「Device Enrollment」頁面的顯示項目，包括權杖的到期日都仍會保持原狀，直到您上傳新的權杖為止。

新增自訂「Device Enrollment」網頁

適用於：iOS 13.0 和 macOS 10.15 及支援的更新版本。

在「自訂註冊」區段中，您可指定您在 Device Enrollment 期間用來認證使用者身份的自訂網頁 (web view)。 使用此頁面來顯示自訂資訊，例如身份認證類型、品牌化、同意文字和隱私權政策。

程序

1. 前往**管理** > **Apple** > **Device Enrollment**。
2. 找出您在 Apple 網站建立的伺服器名稱。
3. 選擇**動作** > **編輯 Device Enrollment 描述檔**。
4. 在「自訂註冊」區段中，選擇**啟用自訂註冊**。
5. 請選擇下列選項之一：
    - **MobileIron 託管網頁** - 如果使用身份提供者 (例如 Microsoft Active Directory Federation Services (ADFS) 或 Okta) 註冊，重新指向身份識別提供者 (IDP)。 這也可以針對非 IDP 型身份認證的 Ivanti Neurons for MDM 使用者重新指向自助式入口網站。
    - **自訂 URL** - 輸入 URL，例如 https://mycustomweburl.com。 此 URL 定義於初始設定新的 Device Enrollment 裝置或已清除的裝置期間，在 web view 中向使用者顯示的自訂 URL 值。 使用此欄位定義您自己的身份認證 UI 和驗證方法。 在使用者身份認證後，會下載 MDM 註冊描述檔。

自訂 Device Enrollment 網頁的工作流程

此區段描述自訂 Device Enrollment 網頁的行為以及建立自訂網頁 (web view) 的程序。

當初始載入 **URL** 欄位中指定自訂網頁時：

- 配置網頁 URL 包含 **https** 架構，為 **GET** 要求。 網頁應使用公開信任憑證。
- 自訂標頭 **x-apple-aspen-deviceinfo** 會附加至已啟動註冊的 Apple 裝置之 GET 要求。 它包含 base64 編碼的 CMS（密碼編譯訊息語法）信封，其中具有含裝置屬性的 plist。 這和使用權杖型裝置註冊的初始 POST 要求中包含的資訊及格式相同。

當之後載入自訂網頁時：

- 裝置使用者與網頁 (網頁檢視) 互動，直到管理員的主機伺服器為用戶端提供 **custom.mobileconfig** 檔。 Ivanti Neurons for MDM 伺服器會傳回位元組碼的 MDM 描述檔。 在管理員的主機伺服器中，應使用 MIME 類型的 **application/x-apple-aspen-config** 設定 custom.mobileconfig 檔，以下載裝置的 MDM 描述檔並將它安裝在裝置上。
- 如要使用 Ivanti Neurons for MDM 進行身份認證，網頁應包含身份認證使用者名稱和密碼認證。 建議在 Ivanti Neurons for MDM 中建立個別的使用者，並指派自訂註冊角色給使用者，讓使用者透過 Ivanti Neurons for MDM 伺服器 URL（例如，

https://micloudDomain.com/c/i/dep/custom.mobileconfig）擷取 MDM 描述檔。

- 針對裝置註冊和從 Ivanti Neurons for MDM 取得 MDM 描述檔，管理員的主機網頁伺服器應向 Ivanti Neurons for MDM 伺服器 URL 發出 POST 呼叫。 此外，當裝置叫用 GET URL 以載入自訂網頁時，也會傳送標頭 x-apple-aspen-deviceinfo 和裝置提供的值。 如果未提供註冊使用者 ID，則裝置未指派給任何人。 以下為額外的詳細資訊：
  - 當裝置叫用在 Device Enrollment 描述檔中設定的自訂網頁 URL 時，管理員的主機網頁伺服器應擷取裝置顯示的標頭「x-apple-aspen-deviceinfo」。
  - 如要為該裝置及其相關使用者取得 MDM 描述檔，管理員的主機網頁伺服器應使用標頭 x-apple-aspen-deviceinfo 向 Ivanti Neurons for MDM伺服器 URL 發出 POST 呼叫。 它應包含使用Ivanti Neurons for MDM使用者 ID 的基本身份認證做為要求參數（例如，https://miCloudDomain.com/c/i/dep/custom.mobileconfig?user=name@company.com）。 應指派自訂註冊角色給使用者。
  - 在管理員的主機網頁伺服器接收到位元組碼後，應藉由設定回應標頭 Content-Disposition = attachment;filename="profile.mobileconfig" 和 Content-Type = application/x-apple-aspen-config，下載位元組碼至裝置。
- Web view 關閉且 OS 會嘗試安裝描述檔（必須為 MDM 註冊描述檔）。

> Ivanti Neurons for MDM 不會對傳回的 MDM 描述檔的使用者 ID 進行身份認證。 因此，在要求 MDM 描述檔之前，管理員應對使用者 ID 執行必要的身份認證。

針對 iOS，在初始設定已清除的裝置期間支援此工作流程。 針對 macOS，如果在執行設定助理期間略過 Device Enrollment，設定助理和「描述檔喜好設定」窗格均支援此工作流程。

如需建立自訂網頁相關的開發人員資訊，請參閱以下 Apple 說明文件偏好設定：

- **Web View**
- **透過 Web View 進行身份認證**
- **實作簡易 iPad 網頁瀏覽器的範例代碼，可用來檢視桌面或行動版本網站**

編輯 Device Enrollment 身份認證設定

程序

1. 前往**管理** > **Apple** > **Device Enrollment**。
2. 找出您在 Apple 網站建立的伺服器名稱。
3. 選擇**動作** > **編輯身份認證**。

行動帳戶的啟動程序權杖管理

適用於：macOS 10.15 裝置以及支援的更新版本，且該等版本已使用 Apple School Manager 或 Apple Business Manager 在 MDM 中完成裝置註冊。

Ivanti Neurons for MDM 支援行動帳戶的啟動程序權杖管理。 啟動程序權杖可讓行動帳戶登入使用 FileVault 的 macOS 裝置。 使用此功能時，所有登入的行動帳戶都會自動取得 SecureToken。 當有多位使用者登入加密機器時，這項功能非常實用。

當受管理的管理員帳戶嘗試登入裝置時：

- 初次登入時，將會向 MDM 伺服器要求啟動程序權杖。
- 如果 MDM 伺服器提供啟動程序權杖，裝置便會自動為帳戶建立 SecureToken。
- 裝置會為使用者啟用 FileVault。

「可用的啟動程序權杖」是裝置詳細資料頁面中提供的欄位，做為建立新裝置群組或自訂原則的篩選屬性。

為了進行疑難排解與驗證，請前往裝置的裝置詳細資料頁面。 使用「日誌」頁面，利用篩選功能根據動作名稱「設定啟動程序權杖」和「取得啟動程序權杖」來縮減裝置日誌。

使用 Device Enrollment 設定受管理的 macOS 管理員帳戶

Ivanti Neurons for MDM 支援針對已重設為出廠預設值或初次啟動的裝置，進行 Device Enrollment 註冊。 您可以使用 Device Enrollment 在 macOS 裝置上建立管理員帳號。 Ivanti Neurons for MDM 僅支援 macOS 的選用註冊，因此 Ivanti Neurons for MDM 會忽略「裝置註冊」設定檔中的 **MDM 為必要**欄位，因為此欄位只適用於 iOS 裝置。

程序

1. 前往**管理 > Apple > Device Enrollment**。
2. 找出您在 Apple 網站建立的伺服器名稱。
3. 選擇**動作 > 編輯 Device Enrollment 描述檔**。
4. 從 macOS 帳戶設定輔助程式選項中，選擇下列其中一個選項：
   - **略過建立管理員帳戶** - 選擇此選項時，即表示不允許建立管理員帳戶 (不論可見或隱藏)。 取消選擇此選項時，即表示允許在**設定受管理的 macOS 管理員帳戶**區段中建立管理員帳戶 (如下所述)。
   - **略過主要設定帳戶建立** - 選擇此選項時，即表示略過設定 macOS 裝置上的主要帳戶。 除了管理員帳戶之外，不會建立任何其他帳戶。 系統會另外顯示**設定受管理的 macOS 管理員帳戶**區段 (如下所述)，以建立受管理的 macOS 管理員帳戶。 您也可以在「使用者與群組」中隱藏這個帳戶。
   - **將主要帳戶建立為一般使用者 (如果未勾選，則會建立為管理員)** - 選擇此選項時，即表示要在註冊期間同時建立一個非管理員的標準帳戶。 系統管理員仍可建立管理員帳戶，並將其推送至裝置。 系統會另外顯示**設定受管理的 macOS 管理員帳戶**區段 (如下所述)，以建立受管理的 macOS 管理員帳戶。 您也可以在「使用者與群組」中隱藏這個帳戶。

選擇上述其中一個選項之後，如果您想建立受管理的 macOS 管理員帳戶，請在**設定受管理的 macOS 管理員帳戶**區段中，輸入下列詳細資料：

- 全名
- 帳戶名稱
- 密碼
- 確認密碼
- (選擇性) 在「使用者與群組」中隱藏受管理的管理員帳戶

如果您未選擇**略過主要設定帳戶建立**，在**設定主要帳戶**區段中輸入以下詳細資料。 這會新增使用者通道支援受管理的管理員帳戶，將受管理的本機使用者簡短名稱設為管理員的簡短名稱。

- **全名**
- **簡短名稱**
- (選用) **防止使用者修改** - 如果完整名稱及/或簡短名稱有替換變數而且被評估為空白，將會覆寫此設定。 如果您選擇此選項，請確認您瞭解只有當以下其中一個選項已正確設定時才適用此主要帳戶設定：
  1. 驗證設定檢視中提示使用者註冊/登入。
  2. 針對註冊自訂選取的 MobileIron 託管網頁。

7. 選擇**略過主要設定帳戶建立**，為受管理的管理員帳戶啟用使用者通道支援。 您可以將受管理的本機使用者簡短名稱設為管理員的簡短名稱。
8. 按一下**儲存**。

變更本機 macOS 管理帳戶密碼

管理員可變更「設定助理」在 Device Enrollment 期間所建立之本機 macOS 管理帳戶的本機密碼。

適用於：macOS 10.11 或支援的更新版本。

程序

1. 前往**裝置**。
2. 按一下裝置的相關聯使用者名稱，以檢視裝置的詳細資料頁面。
3. 從「動作」功能表中，按一下**設定 macOS 管理員密碼**。此動作可在「裝置清單」頁面中執行，也可以選擇一或多個裝置來執行。
4. 輸入密碼。
5. 按一下**儲存**。

匯出至 CSV

Ivanti Neurons for MDM 可讓您將「裝置註冊」裝置匯出至 CSV 檔案。

程序

1. 前往**管理** > **Apple** > **裝置註冊**。
2. 按一下**裝置數量**欄底下的特定裝置計數連結。
3. 按一下**匯出至 CSV** 選項，將裝置清單及相關詳細資料匯出至 CSV 檔案。 報告就緒後，系統會以訊息提示您下載或刪除報告。 您也會收到一封包含報告下載連結的電子郵件。
4. 按一下**下載**。
5. (選用) 按一下**刪除**以刪除報告。

12.3.4. 測試版註冊

如果裝置受到監管並執行 iOS 18、iPadOS 18、macOS 15 或更高版本，則 Ivanti Neurons for MDM 可以稍後自動遠端註冊裝置。 如有必要，可以從 Beta 版程式中移除受監管的裝置，並限制使用者手動註冊。 這消除了使用者執行手動步驟的需要，並允許在整個 Beta 版測試生命週期中簡化流程。

必要條件

- 裝置註冊是 Beta 版註冊的必要條件。 如需有關裝置註冊的更多資訊，請參閱**裝置註冊**。
- 若要在無需 Apple 帳戶的情況下提供 AppleSeed for IT Beta 版，Apple Business Manager 或 Apple School Manager 中的管理員必須登入 AppleSeed for IT 入口網站，並代表其組織接受目前 Beta 版測試期的條款與條件。

將 Ivanti Neurons for MDM 連接至「Beta 版註冊」

如要使用 Ivanti Neurons for MDM 做為「Beta 版註冊」的 MDM 伺服器，請在 Ivanti Neurons for MDM 中設定 Apple Business Manager 或 Apple School Manager 伺服器權杖。

「Beta 版註冊」區段

名稱	描述
組織名稱	組織的名稱。
上次同步時間	執行同步的日期與時間。
狀態	同步的狀態。
「Beta 版註冊」權杖同步	按一下**同步**以同步新可用的測試版註冊權杖以進行測試版更新。

12.3.5. 設定安裝小幫手

「安裝小幫手組態」可讓您在 iOS 和 macOS 裝置的裝置安裝過程中選擇要跳過或包含的安裝畫面。

程序

1. 登入 Ivanti Neurons for MDM 管理主控台。
2. 前往**配置**。
3. 選擇**安裝小幫手**。
4. 按一下鉛筆 (編輯) 圖示。
5. 勾選核取方塊以跳過裝置中的特定安裝畫面。
6. 按一下**完成**。
7. 選擇**裝置通道**。
8. 選擇**所有裝置**。 「安裝小幫手」組態推送至裝置，「裝置詳細資料」頁面中的「組態」索引標籤顯示「已安裝」狀態。
9. 登入裝置。 跳過所有初始安裝畫面。

12.3.6. 安裝 MDM 憑證

您必須要求並安裝 Apple MDM 認證，以管理 iOS 裝置。 您也必須每年更新這個認證。 (接近到期日時，用於建立憑證的 Apple 帳戶會收到 Apple 網站發出的通知。) 使用「 MDM 憑證」頁面新增或續訂此憑證。

取得並安裝 MDM 認證

程序

1. 使用 **MDM 憑證**頁面，從 Ivanti Neurons for MDM 租用戶下載憑證簽署要求 (CSR)。
2. 將 CSR 上傳到 Apple 以建立新的認證。
3. 在 Apple 網站上，新增附註以說明認證的用途。 要更新認證時，此附註很有助益。
   儲存產生的認證。
4. 為您的 Ivanti Neurons for MDM 租戶安裝憑證。

更新 MDM 認證

程序

1. 按一下**更新認證**。
2. 從 Ivanti Neurons for MDM 租用戶下載憑證簽署要求 (CSR)。
3. 將 CSR 上傳到 Apple 以更新對應的認證。
4. 在 Apple 網站上，確認要更新的是正確的認證。 若上傳不同憑證到 Ivanti Neurons for MDM，系統將自動淘汰所有已註冊的 iOS 裝置。
   為您的 Ivanti Neurons for MDM 租戶安裝憑證。

如果您嘗試上傳錯誤的認證，就會收到警告。

如果您無法看到**安裝 MDM 憑證**頁面，可能是您沒有所需的權限。 您需具備下列其中一個角色：

- 系統管理
- 系統唯讀

12.3.7. 商務共享 iPad 裝置

商務共享 iPad 裝置適用於使用 iOS 13.4 或支援的更新版本在 Apple Business Manager 所建立的受管理 Apple ID。

- 共享 iPad 裝置使企業能在多名員工之間共用裝置，同時還能提供個人化體驗。
- 員工可以使用「受管理的 Apple ID 」登入，開始載入自己的資料，包括郵件帳戶、檔案、iCloud 照片圖庫、應用程式資料等。
- 資料儲存在 iCloud 中，因此員工可以登入屬於該組織的任何共用 iPad 裝置。

共享 iPad 裝置可用於醫療保健、零售業及工業應用。 例如，醫生和護士可以共用一台 iPad 裝置，因為他們可以各自安全存取專為他們而設計的使用者設定檔。 在零售商店，第一線的工作者獲得授權存取產品資訊、資源、專業知識，讓客戶滿意並提供更好的購物體驗。

運作方式

- iPad 裝置將新增到 Apple Business Manager 中，並使用開啟共用模式的自動註冊設定檔進行註冊。
- 員工使用公司提供的受管理 Apple ID 和密碼登入共用 iPad 裝置。 Apple 商務管理管理員可以為使用者手動建立帳戶或透過與身分識別提供者 (例如 Entra ID) 結盟來建立帳戶。
- 每個使用者在登入共用 iPad 裝置時都可以擁有自己的自訂設定檔。 管理員可以根據使用者職務、職責和部門散發應用程式。
- 使用者可以在共用 iPad 裝置上以來賓使用者身分登入。 訪客使用者登入預設為啟用狀態。 訪客使用者無需使用受管理的 Apple ID 和密碼登入。 在 **iOS 限制**組態中，將**允許共享 iPad 的訪客工作階段**選項設定為**否**，即可停用訪客使用者登入。
- 轉到 Ivanti Neurons for MDM **> 裝置**，按一下共用 iPad 裝置名稱，然後按一下**使用者**索引標籤檢視裝置上的使用者清單及其詳細資訊 (如受管理 Apple ID、按位元組計可以資料、按位元組計的已使用資料、有資料要同步到 Ivanti Neurons for MDM)。
- 前往**記錄**索引標籤，從篩選器中選擇**報表使用者清單**操作，檢視其他的使用者詳細資料。
- 共用 iPad 裝置上的來賓使用者登入名與 Ivanti Neurons for MDM 的來賓使用者管理不同。 預設下，訪客使用者帳戶在 Ivanti Neurons for MDM 中已停用。 要在共用 iPad 裝置中管理來賓使用者，請啟用來賓使用者帳戶。
- 共用 iPad 裝置上的控制中心提供螢幕錄製。
- Ivanti Neurons for MDM 支援 Managed Apple ID 的替換變數 `${managedAppleID}`。 此系統變數會顯示在系統屬性區段和裝置屬性區段中。
- Ivanti Neurons for MDM 限制管理員更改過去登入共用 iPad 裝置的常駐使用者以及目前登入使用者的受管理 Apple ID 。 如果您嘗試更改受管理 Apple ID，則會顯示一條錯誤消息，指出由於使用者正在使用共用 iPad 裝置，因此無法更改使用者的受管理 Apple ID。
- 如為 **Apple App 和書籍**，不論是否已選取裝置型授權，都會根據裝置型授權在共用 iPad 裝置上安裝 App 與書籍。

必要條件

確定以下必要條件已符合：

- 共用 iPad 裝置需要受管理 Apple ID。 管理員可以手動建立帳戶或與身分識別提供者 (例如 Entra ID) 結盟。
- 共用 iPad 裝置必須包含 iOS 13.4 或支援的更新版本。
- 裝置必須與 Apple Business Manager 帳戶相關聯。
- 裝置必須包含 32GB 或更大的儲存空間。

注意以下幾點:

- Ivanti Neurons for MDM 限制共用 iPad 裝置的某些組態 (例如密碼)，因為 Apple 不支援它們。 此類配置不會推送至裝置 (裝置 > 按一下裝置名稱連結 >「配置」標籤)。

- 密文組態不適用於共用 iPad 裝置，因為它們需要與密碼而非密文關聯的受管理 Apple ID。 Ivanti Neurons for MDM 管理入口網站的解鎖動作不會清除共用 iPad 裝置上的密文。
- 在將 iOS 限制組態發佈到共用 iPad 裝置期間，選取裝置通道或使用者通道。 您可以在發佈個別的配置並強制僅套用限制至裝置或使用者通道。
- Ivanti Neurons for MDM 驗證過期帳戶，並將有過期帳戶作為擁有者的裝置淘汰。 但是，對於共用 iPad 裝置，裝置所有者是最後登錄的使用者，可能不是合法所有者。 如果所有者帳戶預期，則 Ivanti Neurons for MDM 會從停用項中排除共用 iPad 裝置。
- 共用 iPad 裝置不支援 Go for iOS 用戶端。
- 使用者無法在共用 iPad 裝置上執行淘汰和擦除等操作。 只有管理員才能從 Ivanti Neurons for MDM 管理入口網站執行淘汰和抹除操作。
- 管理員無法從 Ivanti Neurons for MDM 管理入口網站更改共用 iPad 裝置的所有者。
- 共用 iPad 裝置不支援零登入。
- 啟用 ListUsers 命令後，所有受管理使用者 ID 及其簽入時間將顯示在**管理員**索引標籤下的「裝置註冊」(Apple Business Manager 的其中一部分) 中。

設定共用 iPad 裝置

您可以設定共用 iPad 裝置並配置設定。

程序

1. 前往**管理** > **Apple** > **裝置註冊**。
2. 使用自動化 Device Enrollment 描述檔註冊裝置，將裝置新增至 Apple Business Manager。 有關此程序的更多資訊，請參閱 Device Enrollment。
3. 在 Device Enrollment 設定中，啟用：
   - **受監管模式**。
   - **商務共享 iPad 裝置**下的**多使用者模式**。
4. (選用) 建立本機使用者帳戶。 裝置將會註冊給此使用者。 在註冊期間，使用者身份驗證僅會發生一次。
5. 重置共用 iPad。

> 只有在重設後，註冊程序才會開始。 將裝置註冊並設定為共用 iPad 裝置需要幾分鐘的時間。

6. 合法擁有者指派給註冊裝置的使用者帳戶。 管理員可以從**裝置**頁面變更合法擁有者。
7. 在裝置登入畫面上，輸入使用者的受管理 Apple ID 認證。
   - 與 macOS 裝置類似，您可以透過裝置和使用者通道在共用 iPad 裝置上推送組態。
   - 使用者替代變數不替換裝置通道中所推送的組態 (包括受管理應用程式組態)。
   - 如果共用 iPad 裝置中的登入使用者不是受管理使用者 - 受管理 Apple ID 不屬於 Ivanti Neurons for MDM 管理入口網站中的任何使用者，則該裝置不會分配給任何人。 使用者將不受管理 – 管理員無法從 Ivanti Neurons for MDM 推送使用者通道組態。
   - 預設下，Ivanti Neurons for MDM 會停用預設訪客使用者。 訪客使用者登入時，裝置未指派給任何使用者，而使用者也不受管理。若必須管理訪客使用者，則必須啟用 Ivanti Neurons for MDM 所建立的預設訪客使用者，並在訪客使用者登入後將裝置分派給預設訪客使用者。 然後就可以管理使用者了。
   - 裝置擁有者資料顯示在 Ivanti Neurons for MDM > **裝置**頁面中及裝置記錄 (裝置詳細資料頁面 > **記錄**) 中。

共享 iPad 的受管理合法擁有者

您可以從裝置清單頁面使用共用 iPad 裝置的電子郵件 ID 搜尋和檢視其合法所有者。 您可以透過將現有合法所有者重新指派給新的合法所有者來更改共用 iPad 裝置的合法所有者。 如果非共用 iPad 裝置的合法所有者被重新指派，則 Ivanti Neurons for MDM 忽略此指派。

程序

1. 前往**裝置**。
2. 按一下齒輪圖示，選擇**合法擁有者**欄位並將其新增至裝置清單頁面。
3. 選取共用 iPad 裝置。
4. 按一下**動作 > 指派給合法擁有者**。

向共用 iPad 裝置的合法所有者傳送電子郵件

您可以向共用 iPad 裝置的合法所有者傳送電子郵件。

程序

1. 前往**裝置**。
2. 按一下共用 iPad 裝置的名稱。
3. 按一下**電子郵件**圖示。
4. 編寫電子郵件。
5. 按一下**傳送**。

使用多使用者模式屬性

您可以在 Ivanti Neurons for MDM 中使用共用 iPad 裝置的「多位使用者模式」屬性。

程序

1. 在**裝置**頁面中，使用**多使用者模式**屬性。
2. 按一下**進階搜尋**，然後建立一個規則，使用**多使用者模式**屬性查找裝置。
3. 在**裝置 > 裝置群組**頁面中，使用**多位使用者模式**屬性為共用 iPad 裝置建立動態裝置群組。 例如，您可使用此群組做為發佈配置的發佈篩選條件。
4. 在**原則**頁面中，使用**多位使用者模式**屬性為共用 iPad 裝置建立自訂原則。
5. 在**應用程式 > 發佈篩選器**中，使用**多使用者模式**屬性限制可用於安裝的應用程式數量。

- Ivanti Neurons for MDM 針對 Apple School Manager 裝置不支援多使用者模式。 不建議啟用設定和推送 Device Enrollment 描述檔至 Apple School Manager 裝置。
- iOS 多位使用者安全登入組態不適用於共用 iPad 裝置。

從共用 iPad 裝置中刪除使用者

您可以從共用 iPad 裝置中刪除一個使用者或多個使用者帳戶。 在「使用者清單」索引標籤中，現在登入的使用者標籤顯示為**作用中**。 刪除選項不適用於共用 iPad 裝置上目前登入的使用者。 可以從**裝置**或**使用者**索引標籤中刪除使用者。

從「裝置」索引標籤中刪除使用者

程序

1. 前往**裝置**索引標籤 > **裝置詳細資料**。
2. 前往**使用者**索引標籤。 使用者清單隨即顯示。
3. 按一下**刪除所有使用者**。
4. 按一下「**-**」 減號可刪除指定的使用者。
    - (選用) 在**刪除使用者**視窗中，選取**即使資料同步到 Ivanti Neurons for MDM 擱置中仍強制刪除使用者**選項，然後按一下**是**。

    > 選取**即使資料同步到 Ivanti Neurons for MDM 擱置中仍強制刪除使用者**將強制刪除使用者，即使資料尚未同步到 Ivanti Neurons for MDM 管理入口網站也是如此。

從「使用者」索引標籤中刪除使用者

程序

1. 前往**使用者**索引標籤。
2. 選擇一個或多個使用者，前往**動作**下拉式功能表，按一下**刪除**。 確認訊息隨即顯示。 確認後，隨即將刪除使用者命令發送給裝置。
3. 轉到裝置詳細資訊中的**裝置記錄**，並驗證是否已將刪除使用者命令傳送給共用 iPad 裝置的已選取使用者。

讓使用者從共用 iPad 裝置中登出

管理員可以從共用 iPad 裝置讓使用者登出。

程序

1. 在**裝置**頁面中，選擇一個共用 iPad 裝置。
2. 從**動作**功能表選擇**強制登出**。 一個快顯視窗提示使用者確認從共用 iPad 裝置登出。
3. 按一下**確定**以核准強制登出。

12.3.8. School Manager

授權： Gold

適用於：受監管的 iOS 9.3+

Apple School Manager 是專供教育機構使用的 Apple 雲端服務，提供包括以 Apple Apps and Books 購買應用程式、透過 Apple Device Enrollment 註冊 iPad 以及建立受管理的 Apple ID 等在內的各項服務。 Ivanti Neurons for MDM UEM 解決方案與 Apple School Manager 完全整合，提供可充分管理教師和學生專用 iPad 的無懈可擊方法，以利善用 School Manager 生態系統與諸如「課堂」之類的應用程式。

> Apple Books 不支援。

設定 School Manager

1. 前往**管理 > School Manager**。
2. 如果**設置教育**選項為關閉，請按一下該選項。
3. 請選擇下列選項之一：
   - **與 Apple School Manager 帳戶同步以匯入學校資訊**:
     1. 前往**管理 > Apple > Device Enrollment** 下載貴組織的金鑰檔案。
     2. 將金鑰檔案上傳到您的 Apple School Manager 帳號，以產生加密金鑰。
     3. 從 Apple School Manager 下載加密金鑰，並將金鑰上傳到 Ivanti Neurons for MDM (**管理員 > Apple > 裝置註冊**)。

        > 現有的 Apple Device Enrollment 帳戶可用於 Apple 教育。 在您存取 Apple School Manager 時，Apple 可讓您升級 Device Enrollment 帳戶，以包括教育的功能。 如需升級指示，請參閱 https://support.apple.com/zh-tw/HT206960。

     當系統接受加密金鑰時，隨即顯示**立即同步**按鈕。

     4. 按一下**立即同步**，隨即開始與 Apple School Manager 同步資料。
   - **從 CSV 檔案匯入資料**:
     1. (選擇性) 按一下**下載 CSV 範本 ZIP 檔案**，下載內含所有資料類型範本的 zip 檔。
     2. 按一下**選擇檔案**...
     3. 新增下列六個 CSV 檔案：
        - 學生資料檔案 (students.csv)
        - 名冊資料檔案 (roster.csv)
        - 職員資料檔案 (staff.csv)
        - 類別資料檔案 (classes.csv)
        - 課程資料檔案 (courses.csv)
        - 位置資料檔案 (locations.csv)

        > 每次上傳之前，您都必須同時選擇這六個 CSV 檔案。

     按一下**上傳**。

4. (選擇性) 如果您需要修改 CSV 檔案，請在之前上傳的這六個檔案中保留所有必備資料。 進行必要的編輯，並再次將檔案全數上傳。

從**班級**與**個人**索引標籤中搜尋資料。

> 個人 (學生和教職員工) 也會顯示在 Ivanti Neurons for MDM 的**使用者**頁面中。

5. 為學生和教職員工將用於教學的裝置建立兩個裝置群組，如下所示:
    1. 前往**管理 > 自訂屬性**。
    2. 針對要用來建立動態管理之裝置群組的學生和職員，建立自訂屬性。
    3. 前往**裝置 > 裝置群組**。
    4. 按一下**新增+**。
    5. 將之前建立的自訂屬性作為篩選條件，針對學生和職員各建立一個動態管理的裝置群組。
6. 在**裝置**頁面中，使用**動作 > 指派給使用者**選項，將登記的裝置指派給學生和職員。
7. 新增**配置 > 教育**內容，以建立「領導者」(職員) 配置和「成員」(學生) 配置。
8. 將「領導者」(職員) 配置和「成員」(學生) 配置發佈到職員和學生裝置群組。
   上述發佈會將這些配置分發到各裝置，並在其中安裝憑證。

> 在**管理 > School Manager** 頁面上，若「班級名稱」未顯示任何值，即會從班級系統來源識別碼和課程識別碼欄位衍生此值。 在 Apple School Manager 或 CSV 檔案中，這些欄位都是選用的。 不過，建議您總是輸入相關的值，因為系統會在缺少「類別名稱」時，使用這些組合來作為預設的識別碼。

將課堂 app 分發給教師

使用課堂 app 時，教師 (領導者) 可以管理下列案例：

- 遠端控制 iPad 和 app 的課堂管理。
- 建立類別群組。
- 教師可以檢視該群組的學生成員。
- 教師可以傳送內容給該群組的學生。
- 限制學生可以檢視哪些 app 和內容。

可以從 Apple App Store 推送「課堂」應用程式。

程序

1. 前往 **Apps > App Catalog** 頁面。
2. 按一下 **+新增**按鈕。
3. 搜尋並選擇 Apple 的課堂 app。
4. 按**下一步**。
5. 輸入類別和描述。
6. 按**下一步**。
7. 將 app 發佈到之前建立的教師裝置群組。
8. 在「App 配置」頁面中，進行 app 設定。

9. 按一下**完成**。

停用 School Manager

停用 School Manager 時，將會抹除所有現有資料。 因此請務必謹慎進行這項作業。

1. 前往**管理 > School Manager**。
2. 如果**設置教育**選項為開啟，請按一下該選項。
3. 按一下**是**。

12.3.9. 設定 (Apple)

管理員可以設定、啟用、停用 Apple 裝置的各種設定。

無訊息自動註冊 (僅限 macOS)

macOS 裝置的無訊息自動註冊已鎖定為啟用。 此功能適用於租用戶中所有新裝置的註冊，並支援 Mobile@Work 1.4 及/或支援的更新版本。

一般設定

停用裝置協調 - 如果管理員想要再次註冊相同的裝置，現在可以保留裝置項目。 預設不會選取此選項。 選取此選項可以保留非使用中裝置詳細資料。

> 停用裝置協調未啟用時，如果裝置重新註冊相同的使用者，將建立新的項目。 否則，將使用新的註冊資訊來更新裝置項目。

描述檔設定

管理員可以針對未安裝 MDM 描述檔的情況，啟用或停用傳送電子郵件給一般使用者，並傳送通知給 macOS 和適用於 iOS 用戶端的 Go。 MDM 描述檔通知功能預設為啟用。

程序

1. 前往**管理員 > 設定**。
2. 選取或取消選取**若未安裝 MDM 描述檔，即傳送電子郵件給使用者，並傳送通知給用戶端**選項。
3. 選取電子郵件/通知的數量上限 (介於 1 到 4 之間)。
4. 按一下**儲存**。

適用於自動裝置註冊的作業系統更新 (僅限 iOS)

管理員可開啟適用於自動裝置註冊的 iOS 作業系統更新。 如果此選項已啟用，Device Enrollment 裝置將會使用軟體更新配置，而非 Device Enrollment 描述檔中的排程作業系統更新設定。

此選項預設為停用，在此情況下會使用 Device Enrollment 描述檔中的排程作業系統更新設定。 開啟此設定為永久性的，無法關閉。 此設定將會移除所有可用的 Device Enrollment 描述檔中的排程作業系統更新設定。

> 受監管的非 Device Enrollment 裝置會使用「軟體更新」配置。

程序

1. 前往**管理員 > 設定**。
2. 選取或取消選取**使用適用於自動 Device Enrollment 的軟體更新配置**選項。
3. 按一下**是**以進行確認。
4. 按一下**儲存**。

多位使用者安全登入

管理員可在使用者於 iOS 共享裝置上從多使用者安全登入 Web Clip 登出後清除裝置密碼。如要這麼做，請在**多使用者安全登入**區段，「於管理 > Apple > 設定」之下，選擇**使用者登出後清除密碼**選項。

限制優先順序設定配置

管理員可配置以啟用多個 iOS 和 macOS 限制的優先順序設定。如要這麼做，請在**管理 >Apple > 設定**之下的**限制優先順序設定配置**區段選擇 **iOS 限制配置**或 **macOS 限制配置**選項。 此選項預設為停用。 關於如何安排優先順序的詳細資訊，請參閱優先排序配置

程序

1. 前往**管理 > Apple > 設定**。
2. 在**限制優先順序設定配置**區段中，選擇 **iOS 限制配置**或 **macOS 限制配置**選項。
3. 按一下**儲存**以啟用優先順序。 「**限制優先順序設定配置 (iOS 或 macOS) 已啟用**」橫幅顯示。 在優先順序之前為**已核准**：
   - **編輯發佈摘要 (如適用)**：當優先順序設定已啟用時，所選限制配置的發佈摘要會預設從「**套用至其他空間中的裝置**」變更為「**以最高優先順序套用至其他裝置空間中的所有裝置**」。
   - **依建立順序指派預設優先順序**：針對所選的限制類型配置，會依建立的順序指派現有的預設優先順序。
   - **暫停配置管理**：暫停對所選限制配置 (例如，iOS 限制配置) 的管理，直到您核准該優先順序。

> 在啟用優先順序後，對限制所做的任何變更都必須取得核准後才會處理。 在核准之前，管理員可在**配置**區段中編輯限制配置的發佈，發佈摘要以及或優先順序。

4. 選擇**核准**選項使優先順序生效。
5. 按一下**儲存**。

> 當取消選取 iOS 或 macOS 限制配置選項時不適用**核准**選項，將會立即套用變更。

當優先順序設定停用時，配置不會有關聯的優先順序。 如適用，所有限制配置都會推送至裝置 (在下次裝置同步時)。

- **發佈摘要 (如適用)：當已停用限制配置的優先順序設定時，發佈摘要會從以最高優先順序套用至其他裝置空間中的所有裝置或以最低優先順序套用至其他裝置空間中的所有裝置變更為「套用至其他空間中的裝置」。**
- **未指派優先順序**：將指派的優先順序從所選的限制配置移除。

12.4. 使用 Windows 裝置

本節包含以下各主題：

- 設定 Windows Autopilot 描述檔
- Windows Autopilot 設定檔上的稽核追蹤
- TenantLockdown CSP
- ADMX (GPO) 瀏覽器
- 配置 app 庫存間隔
- 硬體庫存

12.4.1. 設定 Windows Autopilot 描述檔

Windows Autopilot 是一種 Microsoft 功能，可協助系統管理員設定和預先配置新裝置，以便在工作中使用它們。 Autopilot 功能可幫助快速、可靠且無縫佈建 Windows Desktop 或 HoloLens2 裝置。 此外，Autopilot 功能可幫助執行以下工作：

- 自動將裝置加入 Entra ID (Entra ID)
- 自動將裝置註冊至 MDM 服務
- 根據裝置描述檔建立和自動指派裝置至配置群組
- 自訂註冊體驗
- 套用配置和原則
- 安裝必要的應用程式

必要條件

若要在 Windows Autopilot 頁面中進行所需操作，請查看 Ivanti Neurons for MDM 合作夥伴步驟和 Azure 授權需求。 務必滿足以下先決條件，Autopilot 功能才能按預期運作:

- **Azure Autopilot 授權需求**: 查看「Windows Autopilot 授權需求」。
- **Azure Windows Autopilot 裝置註冊**: 查看「Windows Autopilot 註冊概述」。
- **經銷商將裝置新增到客戶帳戶**: 選取「在新裝置上使用 Windows Autopilot 設定檔來自訂客戶的開箱即用體驗」。

額外需求

1. 整合 Entra ID 租用戶和 Ivanti Neurons for MDM。 如需更多資訊，請參閱**使用 Microsoft Azure 進行設置**。
2. 確認您在 Ivanti Neurons for MDM 和 Entra ID 中都有管理員帳戶。
3. 若要利用自行部署設定檔，請建立一個虛構使用者，以在 Ivanti Neurons for MDM 中註冊無使用者自行部署裝置。
4. 從 Entra ID 主要網域建立並同步虛擬使用者 fooUser@Entra IDPrimaryDomain.com。

> 建立和同步虛擬使用者不需要 Microsoft 授權。

5. Entra ID 中的「自訂網域名稱」頁面會顯示 Entra ID 環境的主要網域。
6. 確認使用者可以註冊裝置並且未遭停用。 例如，如果主網域是 contoso.com，則產生的使用者會是 fooUser@contoso.com。 如果主網域是 contoso.onmicrosoft.com，則產生的使用者會是 fooUser@contoso.onmicrosoft.com。
7. 若要透過 SCIM 將使用者佈建到 Ivanti Neurons for MDM，請在 Entra ID 中編輯使用者詳細資訊，並新增電子郵件地址。 通常電子郵件地址會與 UPN 相同。
8. 確認所有使用者，包括 fooUser，都存在於 Azure 和 Ivanti Neurons for MDM 中。
9. 管理員可以使用 Microsoft Store for Business 或 Ivanti Neurons for MDM 建立 Autopilot 設定檔。 若要使用 Ivanti Neurons for MDM 建立設定檔，管理員需要具備 Entra ID 全域管理員和 Intune 管理員權限。

> 管理員需要 Azure P1 或 P2 授權，且需要 Ivanti Neurons for MDM Secure UEM 或 Secure UEM Premium 授權。 管理員不需要 Intune 授權。

> 在 Neurons for MDM 中，建立 Autopilot 設定檔功能需要利用適用於 Autopilot 的 Microsoft Graph API，這些 API 仍處於測試階段。

Autopilot註冊模式

在您將裝置與特定使用者描述檔群組建立關聯後，就可以根據裝置使用情況，將 Autopilot 註冊模式設為允許使用者快速開始使用其裝置。 Ivanti Neurons for MDM 提供以下 Autopilot 註冊模式：

- 自我部署模式
- 使用者驅動 (預先佈建模式)
- 使用者驅動

自行部署 Autopilot 模式 - 自行部署 Autopilot 裝置註冊模式會透過跳過初始裝置設定，並推送裝置安全啟動所需的所有必要組態檔案，確保為使用者順暢部署企業裝置。 此模式可確保硬體安全，同時使用虛擬使用者 ID 將裝置連線至企業網路，將裝置註冊至 Entra ID (Entra ID)、MDM 服務和 Ivanti Neurons for MDM 管理員入口網站，並在使用者登入之前將所有必要的組態檔推送至裝置。 在將必要的配置檔推送至裝置後，裝置會重新啟動並顯示登入畫面，供企業使用者開始使用。 針對可當成單一應用或數位簽署的裝置，您可使用自我部署模式。

使用者導向預先佈建設定檔模式 - 在管理員建立使用者導向預先佈建設定檔後，該設定檔即會指派給使用者群組，且裝置硬體 ID 會上傳並指派給 Entra ID 群組。 該裝置將會與使用者導向預先佈建描述檔建立關聯。 管理員會使用此模式設定裝置，然後將裝置移交給企業使用者。

程序

請按照預先佈建部署的步驟進行操作:

1. 將新的硬體裝置連線至 LAN，然後按下 Windows 按鈕五次。
2. 裝置會顯示問題提示。 選擇 Windows Autopilot 佈建選項，然後按一下「繼續」。 Entra ID 會偵測使用者導向預先佈建設定檔模式，且所有基本組態設定都會在裝置中部署。 Windows Autopilot 配置畫面出現。
3. 按一下「繼續」。 裝置會繼續執行並確保硬體安全，同時使用虛擬使用者 ID 將裝置連線至企業網路，將裝置註冊至 Entra ID (Entra ID)、MDM 服務和 Ivanti Neurons for MDM 管理員入口網站，並將所有必要的組態檔推送至裝置，接著會出現確認訊息。
4. 您現在可將裝置交給使用者。 當使用者登入裝置時，會使用裝置詳細資料將使用者 ID 註冊至 Ivanti Neurons for MDM 管理入口網站。

在使用者登入裝置之前，會自動推送以下配置：

身份憑證

Wi-Fi

Windows Hello 企業版

Windows 限制

> 其餘組態會處於擱置狀態，等到使用者透過電子郵件地址登入裝置後才會推送。

> 在自行部署和使用者驅動 (預先佈建) 模式下的 Autopilot 註冊程序中，將在裝置上安裝已指派的 .MSI 和 .EXE 應用程式，以完成註冊程序。 在 Autopilot 註冊程序期間安裝 .MSI 和 .EXE 應用程式時，若應用程式在安裝程序中回報或無法回報，則將完成 Autopilot 程序並啟用「重新封裝」按鈕。

建立 Windows Autopilot 使用者描述檔

在設定 Entra ID (Entra ID) 使用者來源，並將使用者和 Entra ID 使用者群組與 Ivanti Neurons for MDM 租用戶同步之後，您就可以建立 Autopilot 設定檔。

程序

1. 登入 Ivanti Neurons for MDM 管理員入口網站。

2. 前往**管理員 > Microsoft Azure > Windows 裝置管理**。

> 如果未設定 Entra ID 使用者來源，**新增**按鈕將會遭到停用。 您必須使用 **Microsoft Azure** 區段下方顯示的 **Windows 裝置管理**選項，來設定使用者來源。

3. 按一下**新增**。
   畫面上出現**新增 Windows Autopilot 描述檔**頁面。
4. 在**名稱**方塊中，輸入描述檔名稱。
5. 使用本程序下方的表格完成**描述檔設定**。
6. 按**下一步**。
   畫面上將會出現一個新頁面，其中列出所有 Entra ID 裝置群組。
7. 選取必須要為其指派 Autopilot 設定檔的一或多個 Entra ID 裝置群組。
8. 您也可以建立 Entra ID 裝置群組，並將 Autopilot 設定檔指派至此新建立的群組。 如需詳細資訊，請參閱**建立 Entra ID 裝置群組**。
   如果您想要將 Autopilot 設定檔指派給所有 Entra ID 群組，請選取**指派給所有 Entra ID 群組**選項。

> 由於 Microsoft 的限制，您無法將多個描述檔指派至「所有群組」。

9. 按一下**完成**。

設定	描述
裝置類型	視裝置而定，從以下兩個選擇中選擇其一： • **Windows PC** • **HoloLens** - 當選取此選項時，預設的部署模式應設為**自我部署**模式。 當使用 Autopilot 註冊 HoloLens 2 裝置時，註冊有可能會卡在「設定工作裝置」畫面，不過這是非常罕見的情況。 在此罕見的情況下，使用者必須按下電源按鈕，將裝置關機後再開機。 然後裝置會顯示「登入」畫面，讓使用者輸入 Entra ID 認證，以完成註冊。
部署模式	• **自我部署**：在此模式中，裝置部署幾乎不需要手動操作。 • **使用者導向**：系統管理員可使用此選項來選擇註冊模式，為使用者配置新裝置，然後將裝置交給使用者。
使用者帳戶類型	• **系統管理員**：如果使用者在裝置部署後需要取得完整控制，請選擇此選項。 • **標準**：如果使用者在裝置部署後需要授權以取得基本選項，請選擇此選項。
語言	預設下，語言為作業系統使用的語言。 您可從清單中變更不同的語言。
將所有目標裝置轉換為 Autopilot	選擇此選項，將指派群組中的所有裝置都轉換為 Autopilot。
允許預先佈建	選擇此選項以使用正常註冊程序向 Autopilot 註冊裝置。 當選取**自我部署**選項後，此選項將無法使用。
自動設定鍵盤	如果將**語言**選項設為和預設值不同的值，選擇**是**以略過鍵盤選擇。
裝置名稱範本	在裝置註冊程序期間，輸入要使用的範本名稱。
Microsoft 軟體授權條款	只有在使用者導向部署模式下，才能顯示或隱藏此選項。
隱私權設定	只有在使用者導向部署模式下，才能顯示或隱藏此選項。
變更帳戶選項	只有在使用者導向部署模式下且使用者帳戶類型為標準類型時，才能顯示或隱藏此選項。

Windows 裝置管理

管理員可使用新選項「Windows 裝置管理」設定租戶上的 Autopilot 功能。 如果使用者有 Entra ID 環境，利用此選項可更輕鬆與 Ivanti Neurons for MDM 整合。

存取此選項: **管理員** > **Microsoft Azure** > **Windows 裝置管理**。

此整合會授予 Ivanti Neurons for MDM 管理裝置、Autopilot 設定檔、檢查 Windows 裝置合規性及驗證 Azure 租用戶的權限。

相關主題

- TenantLockdown CSP

建立 Entra ID 裝置群組

管理員可以在需要時，從「Entra ID 裝置群組」區段建立 Entra ID 裝置群組。 必須在「裝置合規性」區段底下設定 Entra ID 租用戶驗證後，才能建立 Entra ID 裝置群組。

程序

1. 前往**管理員** > **Microsoft Azure** > **Entra ID 裝置群組**。
2. 畫面上將會出現 **Entra ID 裝置群組**頁面。
   按一下**新增**。
3. 畫面上將會出現**群組設定**頁面。
   提供下列詳細資料:
   - 群組名稱
   - 群組說明
   - 成員資格類型
     - 靜態裝置 - 管理員將在**將成員指派給群組**視窗中取得可用靜態裝置的清單。 選取所需的裝置，並按一下**儲存**。
     - 動態裝置 - 管理員必須在**動態查詢**視窗中提供特定條件。

新的 Entra ID 裝置群組將會建立，而且管理員能夠新增裝置至新建立的群組。

> 動態群組建立完成後，裝置將在一段時間後列在特定裝置群組的「裝置」索引標籤底下。

編輯 Autopilot 裝置

使用者可從 Ivanti Neurons for MDM 管理入口網站編輯 Autopilot 裝置。

必要條件

確認滿足以下先決條件:

- IT 管理員使用者應具有 Azure 全域管理員和 Intune 管理員權限。
- 只有設定使用者之後，才能設定使用者易記名稱。
- 裝置名稱設定後，就無法取消。

程序

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 前往**管理** > **Windows** > **Autopilot**。 Autopilot 裝置會列在 Autopilot 裝置標籤之下。
3. 按一下**編輯**（鉛筆圖示）。 編輯頁面出現。
4. 編輯下列詳細資料：
   - **使用者**
   - **使用者易記名稱**
   - **裝置名稱**
   - **群組標籤**

按一下**儲存**。 裝置詳細資料已更新。

刪除 Autopilot 裝置

使用者可從 Ivanti Neurons for MDM 管理入口網站刪除 Autopilot 裝置。

1. 登入 Ivanti Neurons for MDM 管理入口網站。
2. 前往**管理** > **Windows** > **Autopilot**。 Autopilot 裝置會列在 Autopilot 裝置標籤之下。

3. 按一下**刪除**。 裝置詳細資料已刪除。

12.4.2. Windows Autopilot 設定檔上的稽核追蹤

稽核追蹤會記錄在 Ivanti Neurons for MDM 內所有實體上執行的所有活動。 這些活動包括新增、刪除、更新新裝置等。

如需更多資訊，請參閱稽核追蹤。

管理員可以在 Autopilot 模式中註冊的所有 Windows 裝置上使用「稽核追蹤」執行下列活動:

Autopilot 設定檔

- 建立
- 編輯
- 刪除
- 指派設定檔給群組

Autopilot 裝置

- 上傳 CSV
- 編輯
- 刪除

12.4.3. TenantLockdown CSP

管理員可使用 TenantLockdown CSP 功能，將所有 Windows 裝置鎖定至租戶。 如要使用此功能，必須使用 Autopilot 選項來註冊裝置。 可在裝置層級完成此配置。

在 Autopilot 自我部署和使用者導向模式中，管理員可直接將裝置鎖定至租戶。 當裝置遺失或遭竊時，此功能十分有用。 在自我部署模式下，當發生此情況時，即使裝置已被重設，仍可強制使用者連線至該租戶，而且不支援建立本機帳戶。 但是，如果已在使用者導向模式下禁止建立帳戶，在 Autopilot 描述檔配置期間，管理員必須在**變更帳戶選項**設定中啟用**隱藏**選項。

管理員可建立 Windows 限制配置，並在**其他限制**之下選擇**在裝置設定期間，要求使用者連線至網路（需要 Autopilot 描述檔）**選項，以啟用 TenantLockdown CSP。

如要從 TenantLockdown CSP 移除裝置，管理員必須手動從群組移除該裝置，或是變更限制。

12.4.4. ADMX (GPO) 瀏覽器

您可使用 ADMX (GPO) 瀏覽器來檢視根據存在於租戶的 ADMX 物件進行彙整的 GPO 設定。 您可搜尋並檢視預設的 ADMX 物件，並新增 (上傳) 自訂 ADMX 檔案，以提供用於定義 GPO 設定顯示畫面的 XML 型結構。

若要上傳自訂 ADMX 物件：

1. 選擇**管理 > ADMX (GPO) 瀏覽器**。 **ADMX (GPO) 瀏覽器**頁面隨即顯示。
2. 按一下**附加**。 **附加自訂 ADMX (GPO) 物件**視窗隨即顯示。
3. 按一下**選擇檔案**以選擇要上傳的 ADMX 檔案。

> 確認 ADMX 檔案是 zip 檔案。

4. 按一下**附加**。 隨即顯示上傳成功的確認訊息。

> 解壓縮 zip 檔案後，確認根資料夾包含 *.admx* 副檔名檔案。

搜尋 GPO 設定

在 ADMX (GPO) 瀏覽器中，您可以按一下左側窗格中 GPO 階層樹狀結構中的相關元件來搜尋並選取 GPO。 GPO 階層樹狀結構代表原則設定的路徑。 或者，您可搜尋特定的 GPO 設定，方法是在搜尋欄位中輸入 GPO 名稱或 ADMX 檔案名稱。 所選 GPO 設定的詳細資料顯示在右窗格中。

12.4.5. 配置 app 庫存間隔

您可以為多個 app 來源類型庫存設定 Windows 10 應用程式庫存收集的間隔。 在設定用來從裝置收集所有 app 的隱私權配置時會用到此間隔。

1. 瀏覽至**管理員 > 應用程式庫存間隔**。
2. 從下拉式清單中選擇下列 app 來源類型收集 app 庫存的間隔 (單位為小時)。
    - **非 App Store 庫存間隔**
    - **App Store 庫存間隔**
    - **系統庫存間隔**
    - **Win32 庫存間隔**
      收集 Windows 應用程式詳細目錄的間隔選項介於 **24** 至 **48** 小時之間。 預設值為 **24** 小時。

12.4.6. 硬體庫存

您可以啟用收集 Windows 10 裝置的硬體資訊。 系統會使用 Bridge 來擷取硬體清查詳細資料。

1. 瀏覽至**管理員 > 硬體詳細目錄**。
2. 將**啟用收集硬體清查**選項啟用。
3. 在**清查間隔**中，選取收集硬體清查的頻率。 下列為可用的選項：
    - **一天一次** (預設)
    - **一週一次**
    - **每 30 天**

啟用硬體清查選項時，您可以在裝置詳細資料頁面的**硬體**索引標籤下方，檢視裝置的硬體詳細資料。

12.5. 使用 Microsoft Azure 進行設置

本節包含以下各主題：

- 使用 Microsoft Azure
- Entra ID Windows 10 統一端點管理設定
- 指派 Entra ID UEM 應用程式
- 將 Ivanti Neurons for MDM 連線至 Entra ID 使用者來源
- Azure 租戶
- 管理 > Microsoft Azure > Office 365 App 保護

12.5.1. 使用 Microsoft Azure

您可以透過 Microsoft Azure 來設定 Ivanti Neurons for MDM，實現在 Windows 桌面裝置和執行 Windows 10 的平板電腦中進行使用者的無縫註冊。 請遵循下列步驟，設定並連接您的執行個體。

本節包含以下各主題：

- 設定 Entra ID 帳戶
- 在 Entra ID 上建立使用者
- 針對 Windows 10 裝置將 Entra ID 連線至 UEM
- Windows 裝置的多使用者支援

設定 Entra ID 帳戶

若要設定 Entra ID:

1. 前往 https://azure.microsoft.com/en-in/pricing/purchase-options/ 以購買您的 Azure 帳戶。
2. 使用您現有的 Hotmail 或 Outlook.com 帳戶，或建立新帳戶並註冊為新使用者。
3. 購買 Azure 帳戶時，請使用其中一種付款選項並遵循驗證步驟。
4. 要求 Microsoft 將 Ivanti Neurons for MDM 租戶列入允許清單。
5. 使用您在步驟 2 中使用的相同 Hotmail 或 Outlook.com 帳戶，以管理員身分登入 Entra ID，網址為 https://manage.windowsazure.com/https://manage.windowsazure.com/。
6. 前往**網域**索引標籤。
   系統已針對您的帳號建立預設網域 TestMiBGLRoutlook.onmicrosoft.com，您建立的任何使用者將會屬於此網域。 如有需要，您可以重新建立自訂網域。

在 Entra ID 上建立使用者

若要在 Entra ID 上建立使用者:

1. 前往 **Active Directory →預設目錄 →使用者**。
2. 選取「新增使用者選項 → 選擇您組織中的新使用者」。
3. 輸入使用者名稱。 按下一步 **(→)**。
   隨即顯示**使用者描述檔**頁面。
4. 新增使用者資訊，例如名字和姓氏以及顯示名稱。
5. 使用下拉式功能表，指派適當角色給使用者。
6. 產生暫時密碼。
   使用者需要在首次登入時變更此密碼。

針對 Windows 10 裝置將 Entra ID 連線至 UEM

若要將 Entra ID 連線至 UEM:

1. **前往管理員 > Microsoft Azure > 使用 Entra ID 的 Windows 註冊與合規。**
2. 完成在Entra ID Windows 10 統一端點管理設定一節中所述的 UEM 設定步驟。
3. 在 Azure 入口網站中，完成指派 Entra ID UEM 應用程式設定。

4. 在 Ivanti Neurons for MDM 管理員入口網站中，輸入 Entra ID 帳戶的網域名稱，並按一下「連線 Azure 入口網站」，然後選取核取方塊。
5. 在成功登入後，同意 MobileIron AD 租用戶驗證應用程式驗證您的 Ivanti Neurons for MDM UEM 應用程式是否已正確設定。 隨即出現一則訊息，指出連線成功。

Windows 10 裝置的 Microsoft Passport for Work

Microsoft Passport for Work 由 Windows Hello 企業版取代。 如需更多資訊，請參閱 Windows Hello 企業版配置。

Windows 裝置 Entra ID 註冊

必要條件

使用者必須在 Ivanti Neurons for MDM 中註冊。

連線您的網域，在 Windows 10+ 裝置上註冊使用者。

1. 按一下**加入 Entra ID**。
2. 輸入使用者名稱和密碼。
3. 按一下**登入**。
4. 接受 EULA
5. 按一下**建立 PIN**。
   - 如果您啟用 Microsoft Passport for Work PIN 碼複雜性，系統會提示您設定符合既定原則的複雜 PIN 碼。
   - Entra ID 會驗證使用者並將 JWT (JSON Web 權杖) 下載到裝置中。
   - 裝置現已註冊。
   - 系統會透過裝置聯絡使用者以進行驗證。
6. 請輸入並確認 PIN 碼。
7. 按一下**確定**。

Windows 裝置的多使用者支援

Ivanti Neurons for MDM 支援 Windows 10 Entra ID 註冊裝置適用的多使用者功能。 此功能的優點包括可將一些描述檔 (例如 VPN、Wi-Fi、預設電子郵件用戶端等描述檔) 和憑證推送到個別使用者而非裝置。 它也對登入使用者支援內部開發和公用 app。 每當有新的 Entra ID 使用者登入裝置時，Ivanti Neurons for MDM 不只會評估裝置，還會評估使用者。 若是新使用者，Ivanti Neurons for MDM 將會更新該使用者的裝置。 若是裝置上的現有使用者，將會評估自其上一次登入後是否有任何裝置變更和使用者設定需要更新。

Ivanti Neurons for MDM 管理員入口網站會報告已登入裝置的 Entra ID 使用者的詳細資訊。 當使用者登出裝置且第二名使用者登入裝置時，在裝置詳細資料頁面中會更新第二名使用者的詳細資料。

設定搭配使用商務用 Microsoft Store 與 UEM

商務用 Microsoft Store 是 Microsoft 透過 Azure 提供的入口網站。 管理員可登入此入口網站，然後購買 app 並發佈至所有的受管理裝置。 可使用商務用 Microsoft Store 設定 Ivanti Neurons for MDM，以便您在 Ivanti Neurons for MDM 管理入口網站中藉由設定下列步驟來管理應用程式。

步驟 1: 在 Microsoft Azure 入口網站中註冊 Entra ID 應用程式

1. 開啟第一個瀏覽器並登入 Microsoft Azure 入口網站 (https://portal.azure.com/https://portal.azure.com/)。

2. 按一下左側窗格中的 **App 註冊**。
3. 按一下 **+新增應用程式註冊**
4. 輸入下列資訊，將 MobileIron 註冊為 Azure app：
   - **名稱**：輸入 MobileIron app 的名稱。 (此欄位的最小長度為 4 個字元。)
   - **應用程式類型**：選擇 Web app / API。
   - **登入 URL**：輸入裝置使用者用來登入 MobileIron 的 URL (必填)。
5. 按一下**建立**以新增 app，然後返回 Azure 首頁。
6. 前往「設定」，然後建立新的金鑰。

步驟 2：將應用程式新增為管理工具

1. 在「商務用 Microsoft Store 設定」中，按一下「管理
2. 發佈設定」
3. 在「新增管理工具」中啟動所建立的應用程式。

透過管理入口網站連線帳戶

1. 前往**管理 > Microsoft Azure > 商務用 Microsoft Store**。
2. 在步驟 1 **註冊 Entra ID 應用程式**底下，選取**是，我已完成此步驟**核取方塊。
3. 在步驟 2 中，**新增管理工具**，選擇**是，我已完成此步驟**勾選框。
4. 在步驟 3 中，連線帳戶、更新下列欄位：
   - Entra ID 網域
   - 應用程式識別碼
   - 應用程式金鑰
   - 同步間隔 (小時)
5. 按一下**連線**。您將會看到「已成功設定商務用 Microsoft Store」的確認訊息。
6. 按一下**同步 App**。成功同步時，狀態顯示為**應用程式已成功同步**。

當商務用 Microsoft Store app 已推送至裝置時，即可在裝置詳細資料中**已安裝的 App** 索引標籤下找到 app 詳細資料。 裝置回報的每個商務用 Microsoft Store app，都會在**來源**欄位中識別為**商務用 Microsoft Store**。

12.5.2. Entra ID Windows 10 統一端點管理設定

如要設定 Windows 10 Unified Endpoint Management (UEM)：

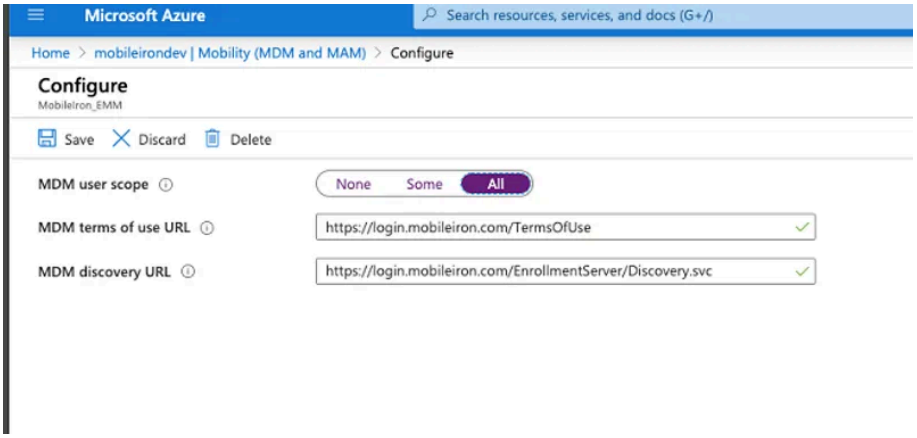
1. 以管理員身分登入 https://portal.azure.com/，然後選取 Entra ID。
2. 在左側窗格中選擇「Mobility (MDM and MAM)」，然後按一下 **+新增應用程式**。

3. 從 App 庫選擇 MobileIron_UEM 應用程式，然後按一下**新增**。


12.5.3. 指派 Entra ID UEM 應用程式

如要完成指派使用者設定：

1. 按一下在 **Entra ID Windows 10 統一端點管理設定**步驟 2 中建立的 MobileIron UEM 應用程式。
2. 在 MDM 使用者範圍之下，將它指派給您的自訂使用者群組或選擇**全部**。



12.5.4. 將 Ivanti Neurons for MDM 連線至 Entra ID 使用者來源

若要使用 Entra ID (Entra ID)，您必須使用 Microsoft Entra ID 帳戶的詳細資訊設定 Ivanti Neurons for MDM。 您需要現有與已設定的 Microsoft Entra ID 帳戶。 此解決方案不需要任何內部部署 Connector 或 LDAP。

本節包含以下各主題：

- 使用案例
- 使用 Entra ID
- Entra ID 設定

使用案例

針對以下其中一個使用案例，您可以將 Ivanti Neurons for MDM 連線至 Entra ID:

- 使用 Microsoft Office 365
- 設定 Microsoft Entra ID、Microsoft ADFS 或其他 SAML 2.0 身分識別提供者 (IdP) 以進行使用者驗證
- 將 Microsoft Entra ID 設為使用者來源
- 從 Microsoft Entra ID 同步使用者並開始進行。 您 Entra ID 網域中的所有使用者和群組，會同步至您的 Ivanti Neurons for MDM 執行個體

  如果下列原因導致 Entra ID 同步發生錯誤，**通知**頁面會顯示一則通知:
  - 無法連線 Entra ID 服務
  - 所有使用者屬性都未與 Entra ID 同步
  - 部分使用者屬性未與 Entra ID 同步
- 目前不支援具有多 IdP 的環境。
- 如果不想使用 Microsoft Entra ID 作為使用者來源，您可以使用本機帳戶或 LDAP 中的來源使用者。 這需要設定 Ivanti Neurons for MDM Connector 以存取內部部署 LDAP 資源。
- Microsoft Entra ID 僅用於使用者驗證，目前不支援將內部部署 LDAP 用於使用者目錄。

使用 Entra ID

若要使用 Entra ID，請設定身分識別提供者，以下列其中一種方法進行使用者驗證:

- 若要將 Microsoft Entra ID 同時用於使用者來源和使用者驗證，請將 Entra ID 設為您的 IdP。 前往**管理員 > 身分識別 > Ivanti Neurons for MDM IdP 設定**，然後從功能表選取 **Entra ID**。
- 若要將 Microsoft Entra ID 用於使用者來源，然後將 ADFS 用於使用者驗證，請將 ADFS 設為您的 IdP。 前往**管理 > 身分 > 內部部署 IdP 設定**並從選單選取 ADFS。
- 若要讓 SAML 2.0 IdP (而非 Entra ID) 及 ADFS 用於使用者身分驗證，請前往**管理 > 身分識別 > 一般 IdP 設定**，然後遵循頁面指示。

如需更多資訊，請參閱設定身份識別提供者。

Entra ID 設定

本主題有助您進行 Entra ID 設定。

程序

1. 前往**管理員 > Microsoft Azure > Entra ID 使用者來源**。
2. 指定下列詳細資訊:
    1. **Entra ID 名稱**。
    2. **同步間隔** - 修改 Ivanti Neurons for MDM 與您的 Entra ID 同步使用者資料的頻率。
    3. **啟用此 Entra ID** - 使用此選項啟用或停用 Entra ID 執行個體。
    4. 選取**自動邀請從 Entra ID 匯入的使用者** - 管理是否自動邀請從 Entra ID 匯入 Ivanti Neurons for MDM 的使用者以透過電子郵件註冊。
    5. 選取**受管理 Apple ID** - 選擇此選項可同步 Entra ID 使用者的受管理 Apple ID。
        - **無**
        - **模式** -
            - **使用者電子郵件地址**
            - **userUPN**
            - (選擇性) 選取納入 "appleid" 子網域選項，避免與現有 Apple ID 衝突。
    6. (選擇性) 按一下**新增自訂屬性** - 從您想要套用至裝置管理的目錄服務，指定自訂使用者屬性。 然後，每個屬性即可供支援變數之配置欄位中的 $ 參照。 使用此選項時，所有 Entra ID 伺服器的自訂屬性實作都必須保持一致。 如果實作中包含的 Entra ID 伺服器並未使用此屬性，則相依於此屬性的功能可能無法如預期運作。

修改 Entra ID 設定後，按一下**儲存**。

12.5.5. Azure 租戶

本節包含以下各主題：

- 需求
- 將 Intune 授權套用至裝置使用者
- 將 MobileIron 新增為合規性合作夥伴
- 在 Microsoft Endpoint Manager 中建立條件式存取原則
- 將 Microsoft Azure 連線至 Ivanti Neurons for MDM
- 建立合作夥伴裝置合規性原則
- 從 Ivanti Neurons for MDM 到 Azure 的裝置狀態報告
- 取消佈建 Azure 租戶

12.5.5.1. Azure Tenant Requirements

本節說明如何透過 Microsoft Azure 租用戶設定 Ivanti Neurons for MDM。

需求

Microsoft

Ivanti Neurons for MDM 客戶必須具有有效的 Microsoft Intune 訂閱，並指派 Microsoft Intune 授權給裝置使用者。

MobileIron

- Ivanti Neurons for MDM - Ivanti Neurons for MDM 版本 75 到 MobileIron 支援的最新版本。
- 額外授權 - Azure Device Compliance 是 Premium 方案，適用於 **Secure UEM Premium** 和 Platinum 客戶。 Platinum 授權對現有客戶已足夠。
- 適用於 iOS 的 Go (用戶端) 或適用於 Android 的 Go (用戶端) 版本 75.0 到 MobileIron 支援的最新版本。

多個 Ivanti Neurons for MDM 版本支援

如果您有多個 Ivanti Neurons for MDM 連線至同一個 Azure 租用戶，請中斷所有 Ivanti Neurons for MDM 的連線，或停用特定 (單一) Ivanti Neurons for MDM 的 Entra ID 合規性整合之合規性原則，以此禁止將裝置資料上傳至 Azure

> 在中斷與 Ivanti Neurons for MDM 的連線之前，請務必先停用合規性原則。

Ivanti Neurons for MDM 管理員程序

對於 Ivanti Neurons for MDM 管理員，該程序：

1. 管理員會將 Intune 授權套用至裝置使用者。 請參閱**將 Intune 授權套用至裝置使用者**。
2. 管理員登入 Azure 入口網站。
3. 管理員將 MobileIron 新增為 Azure 合規性合作夥伴。 請參閱**將 MobileIron 新增為合規性合作夥伴**。
4. 管理員為 app 建立條件式存取原則。 請參閱**在 Microsoft Endpoint Manager 中建立條件式存取原則**。
5. 管理員在 MobileIron 和 Azure 之間設定連線。 請參閱**將 Microsoft Azure 連線至 Ivanti Neurons for MDM**。
6. 管理員在 Ivanti Neurons for MDM 中建立裝置合規性原則。 請參閱**建立合作夥伴裝置合規性原則**。
7. 條件式存取原則生效。 視裝置是否合規而定，授予或拒絕存取 app。

> Ivanti 建議管理員在每個 Microsoft app 上執行測試。

12.5.5.2. 將 Intune 授權套用至裝置使用者

- 如有以下情況，請勿使用此功能：
  - 您正在變更使用者或管理使用者可能會改變的情況
  - 裝置被多名使用者所擁有
- Ivanti 建議您不要執行指派給使用者，也不要將裝置合規性配置發佈至多使用者裝置，例如：
  - 具安全登入 WebClip 的裝置
  - 共享 iPad 裝置
  - Android 單一應用模式裝置

Ivanti Neurons for MDM 授權需求

裝置合規性是 Premium 方案，適用於 Secure UEM Premium 和 Platinum 客戶。 針對現有的客戶，Platinum 授權已足夠。

指派大量授權給裝置使用者

如要大量指派授權給現有的裝置使用者：

基於群組的指派

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

基於 PowerShell 的指派

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. 將 MobileIron 新增為合規性合作夥伴

必要條件

- 安裝 Microsoft Intune 授權。 請參閱**將 Intune 授權套用至裝置使用者**。
- 在 Microsoft Azure 中建立的使用者
- 在 Microsoft Azure 中建立的群組

程序

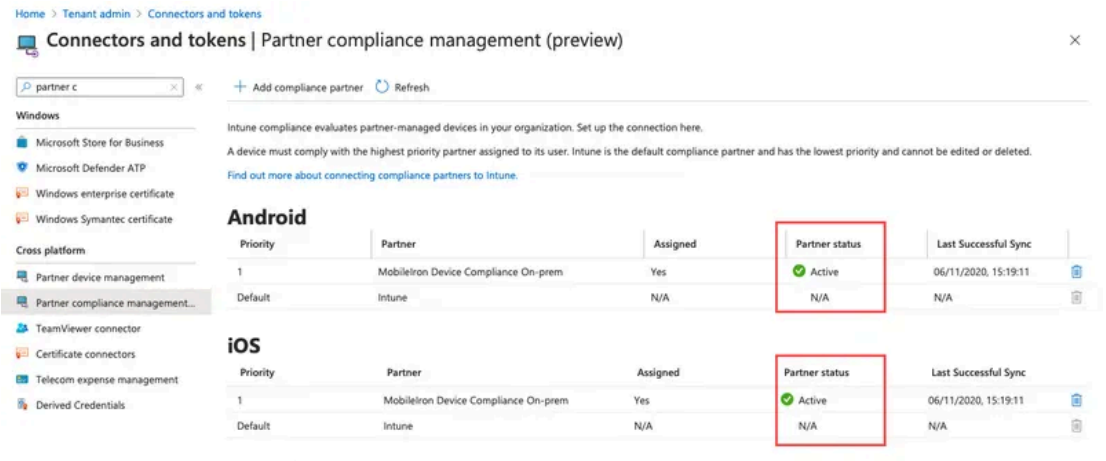
1. 登入：**https://endpoint.microsoft.com**。
2. 在 Microsoft Endpoint Manager 管理中心頁面的左側面板，按一下租用戶系統管理員。 按一下連接器與語彙基元 > Partner Compliance Management。

3. 至搜尋欄位的右側，按一下 +Add compliance partner。

4. 在「Basics」索引標籤中，從「Compliance Partner」欄位的下拉式清單中選擇 MobileIron Device Compliance Cloud。

5. 在「平台」欄位中，選擇 iOS 或 Android，然後按一下下一步。
6. 按一下 Assignments 索引標籤。 在「Assign to」下拉式清單中，選擇合規性狀態所指的使用者/裝置使用者群組。 選擇有授權的使用者/群組。

7. 選擇下一步。
8. 按一下建立。 新增的合規性合作夥伴會出現在「Partner Compliance Management」頁面上。



12.5.5.4. 在 Microsoft Endpoint Manager 中建立條件式存取原則

程序

1. 登入 Microsoft Endpoint Manager https://endpoint.microsoft.com。
2. 在 Microsoft Endpoint Manager 管理中心頁面中，移至首頁 > 端點安全性 > 條件式存取。
3. 按一下原則，然後按一下 +新增原則。

4. 輸入條件式存取原則的名稱。

5. 在指派中，按一下以指派原則至使用者和群組。

6. 按一下 Cloud app 或動作，然後按一下選擇。 搜尋並選擇需要保護的 app。

7. 按一下條件，然後按一下裝置平台。 選擇適合的裝置平台。

8. 在新增條件式存取原則頁面 > 存取控制，按一下授予，然後提供存取並封鎖選擇。

9. 如要啟用新原則，請按一下開啟。

10. 按一下建立。

12.5.5.5. 將 Microsoft Azure 連線至 Ivanti Neurons for MDM

程序

1. 登入Ivanti Neurons for MDM並前往**管理** > **Microsoft Azure**。
2. 在左側導覽窗格中，按一下 **Microsoft Azure** > **裝置合規性**。
3. 在「連線帳戶」區段下，提供下列詳細資料:
   - **Azure Tenant ID** - 找到您的 Microsoft Azure 執行個體。
   - **註冊 URL (選用)** - 如果裝置未向 MDM 註冊，會將裝置使用者指向 URL 進行註冊。 進行設定時，使用 HTTPS 格式。 如果您在貴組織中代管頁面，想要重新導向您的裝置使用者輸入註冊資訊，請在這裡新增該連結。
   - **補救 URL (選用)** - 如果裝置不合規，會將裝置使用者指向此 URL 進行補救。 進行設定時，使用 HTTPS 格式。 如果您在貴組織中代管頁面，想要重新導向您的裝置使用者輸入補救資訊，請在這裡新增該連結。
4. 按一下**連線帳戶**。 「Azure 租用戶驗證」對話方塊隨即開啟。

> 目前連線至 Azure 的租用戶若想要為 macOS 裝置新增裝置合規性，必須中斷帳戶連線，然後重新建立連線。

5. 在「Azure 租用戶驗證」對話方塊中，按一下步驟 1 中出現的**連結**。
6. **登入**。
7. 檢視權限，然後按一下**接受**。

> 如果您已登入但頁面提示您再次登入，請關閉瀏覽器索引標籤/視窗。

8. 返回 Ivanti Neurons for MDM。 在「連線 Azure 帳戶」對話方塊，選擇**我已同意**核取方塊。 按一下**確認**。

- 如要編輯帳戶，請按一下**編輯帳戶**。
- 如要中斷連線帳戶，請按一下**中斷連線帳戶**。 如需其他說明，請參閱取消佈建 Azure 租戶。
- 所有新增、編輯和停用帳戶的活動都記錄在日誌中。

12.5.5.6. 建立合作夥伴裝置合規性原則

在 Ivanti Neurons for MDM 中建立夥伴裝置合規原則，並套用所需標籤。 合作夥伴合規性原則將裝置合規狀態回報給 Azure 或 BeyondCorp，以進行條件存取。

適用於

- iOS
- Android
- Windows

必要條件

必須設定 Azure 租用戶 ID 或 Google BeyondCorp ID。 如需有關 Azure 合作夥伴裝置合規性的詳細資訊，請參閱**將 Microsoft Azure 連線至 Ivanti Neurons for MDM**。



程序

1. 登入 Ivanti Neurons for MDM，前往**組態**。
2. 按一下**新增**並搜尋**合作夥伴裝置合規性**組態。
3. 在**建立合作夥伴裝置合規性組態**頁面上輸入下列詳細資訊:

個項目	描述
名稱	輸入名稱。
+新增描述	輸入說明。
選擇合作夥伴	選取**Microsoft Azure 合規性**。 或 **Google BeyondCorp 合規性 - 試用版**。
配置設置 將 iOS、macOS 和 Android 裝置的合規性狀態回報給 Azure	預設已設為開啟。 若看不見此欄位，則需要設定 Azure 租用戶 ID。 若啟用「回報 iOS、macOS 和 Android 裝置的合規性狀態」選項，且合規性原則套用至用戶端，則用戶端將在裝置的「設定」下顯示「Microsoft 365 Access」。 在以下情況會報告裝置的合規性狀態： • 裝置不合規範 • 裝置符合規範 • 裝置重新符合規範 • 經過 24 小時。 若狀態沒有變化，則每週/每七天傳送一次報告。
將 iOS、macOS、Android 和 Windows 裝置的合規性狀態回報給 Google BeyondCorp	預設已設為開啟。 在以下情況會報告裝置的合規性狀態： • 裝置不合規範 • 裝置符合規範 • 裝置重新符合規範 • 經過 24 小時。 若狀態沒有變化，則每 24 小時後傳送一次報告。

4. 按**下一步**。

5. 預設為已選取**啟用此配置**。
6. 選擇此配置的發佈層級。 如需有關組態發佈的詳細資訊，請參閱**新增配置**。
7. 按一下**完成**。

12.5.5.7. 從 Ivanti Neurons for MDM 到 Azure 的裝置狀態報告

針對以下情況，Ivanti Neurons for MDM 會報告裝置詳細目錄和合規性狀態。

- 裝置上的合規性狀態變更
- 裝置上的庫存變更
- Ivanti Neurons for MDM 會每週報告一次合規性和詳細目錄狀態

視在合規性原則中所選的動作而定，將會傳送以下裝置狀態：

動作遊戲 **(套用最嚴格的)**	**Ivanti Neurons for MDM 傳送的內容**
封鎖電子郵件、AppConnect App、隔離	裝置不合規
傳送警示	符合 Azure 規範
淘汰裝置	裝置資料已從 Azure 平台移除

裝置詳細資料頁面

如要檢視有關裝置的 Azure 資訊，請至裝置詳細資料頁面。 欄位描述及其可能的值：

欄位	描述
Azure 裝置識別碼	Microsoft 向 iOS 或 Android 裝置報告的裝置 ID 例如：007c8232-9489-4074-9b35-345b16f0a72d。 Ivanti Neurons for MDM 會接收此裝置 ID，因為裝置使用者需要向 Microsoft Authenticator 應用程式註冊才能使用此功能。 如果無法擷取裝置 ID，此欄位會留空。
Azure 裝置合規性狀態	在 Azure 中列出裝置的合規性狀態。 可能的值： • 進行中 • 成功 • 失敗
Azure 用戶端狀態代碼	指出裝置是否連線至 Azure。 可能的值： • Success - 可擷取裝置 ID。 • Internal_Error - 在用戶端或伺服器端上發生無法復原的錯誤。 • Workplace_Join_Required - 需要裝置註冊。 裝置使用者可降低此狀態。 • Interaction_Required - 需要互動式登入。 裝置使用者可降低此狀態。 • Server_Declined_Scopes - 未授權存取某些範圍。 • Server_Protection_Policies_Required - 要求的資源受到 Intune Conditional Access 原則的保護。 • User_Canceled - 裝置使用者已在網頁瀏覽器中點選「完成」或「取消」按鈕，取消網頁 Auth 工作階段。 • Account_logged_out - 帳戶已登出。
Azure 裝置相符性報告時間	Ivanti Neurons for MDM 向 Microsoft Intune 報告裝置合規性狀態的時間。 空白欄位表示以下其中一種情況： • 功能已停用。 • Ivanti Neurons for MDM 已接收資料，但尚未呼叫 Microsoft API • 發生錯誤，例如 user_Cancelled 或內部錯誤

12.5.5.8. 取消佈建 Azure 租戶

若已啟用多個 Ivanti Neurons for MDM 以使用相同的 Azure 租戶，則從所有的 Ivanti Neurons for MDM 取消佈建。 如果有單一 Ivanti Neurons for MDM 需要停止使用 Azure，您可僅針對該 Ivanti Neurons for MDM 停用合作夥伴合規性原則。

如果管理員在 Ivanti Neurons for MDM 上執行中斷連線，Ivanti Neurons for MDM 會停止向 Azure 報告裝置詳細目錄和合規性狀態。

先決條件

- 確定所有裝置為未受管理
- 確定所有裝置為不合規

程序

Microsoft

1. 登入 Microsoft Azure。
2. 移至 Intune > 條件式存取。 確定條件式存取原則已停用。

Ivanti Neurons for MDM

1. 登入 Ivanti Neurons for MDM 並前往管理。
2. 在左側導覽窗格中，按一下 Microsoft Azure > iOS 和 Android 的裝置合規性。
3. 按一下中斷連線帳戶。

4. 按一下是。

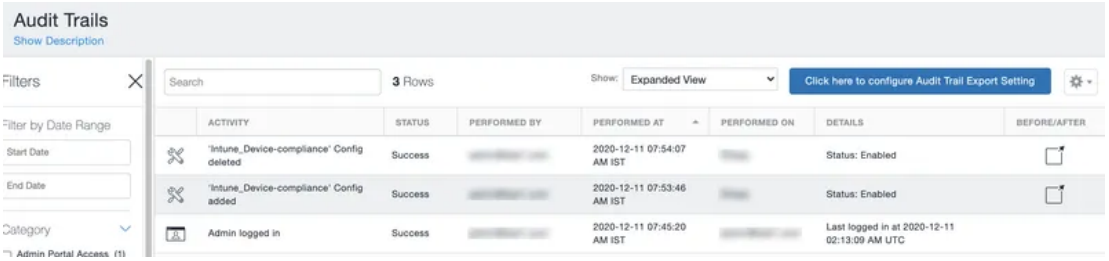
從 Azure 淘汰裝置

淘汰裝置時，Ivanti Neurons for MDM 會向 Azure 報告該裝置已不受管理且不合規。

Azure 在 90 天後會刪除淘汰的裝置。

Azure 帳戶活動會記錄在日誌中

所有活動會記錄在日誌中。



12.5.6. 管理 > Microsoft Azure > Office 365 App 保護

授權：Gold

您可使用 Office 365 App 保護原則，來協助保護您公司的資料。 強制執行預防資料遺失 (DLP) 的原則利用 Microsoft Graph API 來控制 Microsoft Office 365 app。 其中部分的 Graph API 允許管理員針對使用 Graph SDK 的原生 iOS 及 Android app 強制進行 app 保護。

使用此功能來強制執行原則，例如：

- 防止使用者從 Office 365 app 進行列印。
- 防止從 Office 365 app 對外共用資料。
- 強制 Office 365 app 使用 PIN 碼。
- 停用從 Office 365 app 進行聯絡人同步。

使用 Office 365 app 保護的必要條件

您必須擁有以下項目才能使用 Office 365 app 保護：

- 有效的 MobileIron 授權。
- Ivanti Neurons for MDM 中已啟用 Office 365 應用程式保護功能
- Intune 訂閱或包含 Intune 在內的 Microsoft EMS 訂閱。
  - 每次使用套用原則以要求授權，但是啟用和測試整合只需要單一授權。
- 內含企業 Office 365 app 行動裝置存取權的 Office Enterprise 或 Business 訂閱。
- 一或多個 Office 365 app。
- 將您的 Active Directory 使用者同步到您的 Entra ID。
- 在裝置上安裝 One Drive for Business，以保護 Word、Excel 及 PowerPoint 上的資料。 這並非必要。
- 存取 Microsoft Azure 入口網站 (https://portal.azure.com/) 以設定 Intune app 保護政策。
- 安裝在 Android 裝置上的 Intune 公司入口網站應用程式
  使用者無需登入，但裝置上必須安裝此 app 才能保護裝置上的資料。 當使用者登入 app 時便會套用保護。

將 MobileIron 註冊為 Azure app

本主題說明如何在 Ivanti Neurons for MDM 軟體上註冊與儲存 Azure 租用戶憑證，以及如何從遠端管理 Microsoft Azure 雲端中適用於 Android 及 iOS Office 365 應用程式的應用程式保護原則。 雖然並非必要，但您可以開啟兩個瀏覽器以執行下列程序步驟。 使用第一個瀏覽器來登入 Microsoft Azure 入口網站。 使用第二個瀏覽器來登入 Ivanti Neurons for MDM 管理入口網站。

Microsoft Azure 入口網站的程序

> Microsoft 可能會不定時變更 Azure 入口網站使用者介面。 這些說明假設您熟悉 Microsoft Azure 入口網站，當您將 MobileIron 註冊為 Azure app 時進入必要調整。

1. 開啟第一個瀏覽器並登入 Microsoft Azure 入口網站 (https://portal.azure.com/)。
2. 按一下左側窗格中的 **App 註冊**。
3. 按一下 **+新增應用程式註冊**。
4. 輸入下列資訊，將 MobileIron 註冊為 Azure app。

- **名稱：**輸入 MobileIron app 的名稱。 (此欄位的最小長度為 4 個字元。)
- **應用程式類型：**選擇 Web app / API。
- **登入 URL：**輸入裝置使用者用來登入 MobileIron 的 URL (必填)。

按一下窗格底端的**建立**，以新增 app 然後返回 Azure 首頁。

6. 按一下 Azure 首頁中新建立的 MobileIron app。
7. 返回 Azure 首頁，指派 MobileIron Azure app 的權限。
8. 如要為剛建立的 MobileIron app 設定所需的 API 權限，請在 App 註冊之下按一下 app 名稱。
9. 按一下 **API 權限** > **新增權限**。
10. 在 **Microsoft Graph > 委派權限 > 裝置管理**區段中，選擇 **DeviceManagementApps.Read.All** 權限，然後按一下**儲存**。 預設針對 app 啟用 user.Read 權限。
11. 如要取得存取權限，按一下**授予 MobileIron 管理同意**。
12. 執行 Ivanti Neurons for MDM 管理入口網站的以下程序。

Ivanti Neurons for MDM 管理員入口網站的程序

1. 開啟第二個瀏覽器並登入 Ivanti Neurons for MDM 管理入口網站。
2. 前往**管理 > Microsoft Azure > Office 365 App 保護**。
3. 將**應用程式 ID** 貼到 Ivanti Neurons for MDM 管理入口網站中。
4. **程序**
    1. 前往 Azure 入口網站。
    2. 選擇 MobileIron app > **屬性**。
    3. 複製**應用程式 ID**。
    4. 在管理入口網站上回到**管理 > Microsoft Azure > Office 365 App 保護**。
    5. 在 **應用程式 ID** 欄位中貼上應用程式 ID。

在 Ivanti Neurons for MDM 管理入口網站中貼上**應用程式密碼** (用戶端密碼)。

5. **程序**
    1. 前往 Azure 入口網站。
    2. 選擇 MobileIron app。
    3. 按一下**金鑰**，在**金鑰描述**中輸入名稱，然後在**持續時間**中選擇到期期限。
    4. 按一下**儲存**，然後複製**金鑰**值。
    5. 在管理入口網站上回到**管理 > Microsoft Azure > Office 365 App 保護**。
    6. 在**應用程式密碼** (用戶端密碼) 欄位中貼上應用程式密碼。

將**租用戶 ID** 貼到 Ivanti Neurons for MDM 管理入口網站中。

6. **程序**
    1. 前往 Azure 入口網站。
    2. 按一下左窗格中的 Entra ID，然後按一下「屬性」。
    3. 複製目錄 ID。

4. 在管理入口網站上回到**管理 > Microsoft Azure > Office 365 App 保護**。
5. 在 **租戶 ID** 欄位中貼上租戶 ID。

輸入您的 Intune 管理員**使用者名稱**和**密碼**。

- Azure 帳戶應該有全域管理權限或有限的管理 + Intune 服務管理權限。
- Ivanti 建議僅使用 Intune 服務管理權限建立本機 Azure 帳戶。 Microsoft 使用 Graph API 進行身份認證時不支援使用者帳戶為身份識別提供者的同盟。

按一下**驗證並儲存**。
如果提交的日期不正確，系統將會顯示錯誤訊息。

Office 365 app 保護的原則

設定 Microsoft Graph 憑證之後，前往 **Apps > Office 365 App 保護**，為不同的使用者群組新增 iOS 或 Android 裝置的 Office 365 App 保護原則。

這些原則列在 **App > Office 365 App 保護**頁面中 (**App 原則**索引標籤下)。 此原則清單提供表格式詳細資料，例如更新的時間戳記、平台、指派的 app 及部署的使用者群組。

新增 iOS 裝置的 Office 365 app 保護原則

程序

1. 前往 **App > Office 365 App 保護**。
2. 按一下 **App 原則 > +新增**。
3. 輸入原則的**名稱**並選擇性輸入原則的**描述**。
4. 在「選擇作業系統」下，按一下 **iOS**。
5. 在**資料重新配置**下，從下列設定和選項中挑選：
   - 禁止 iTunes 和 iCloud 備份
   - 允許 app 將資料傳送到其他 app - 所有 app (預設)、受原則管理的 app、無
   - 允許 app 接收來自其他 app 的資料 - 所有 app (預設)、受原則管理的 app、無
   - 禁止「另存新檔」
   - 限制從其他 app 剪下、複製與貼上資料 - 任何 app (預設)、鎖定的、受原則管理的 app、受貼上原則管理的
   - 限制可在「受管理瀏覽器」中顯示的 Web 內容
   - 加密 app 資料 - 裝置鎖定時 (預設)、裝置鎖定且沒有開啟中檔案時、裝置重新啟動後、使用裝置設定
   - 停用聯絡人同步
   - 停用列印
6. 在**存取**下，從下列設定和選項中挑選：
   - 需要 PIN 碼才可存取
   - 重設 PIN 碼之前的嘗試次數 (預設 5)
   - 允許簡單 PIN 碼
   - PIN 碼長度 (預設 4)
   - 允許指紋而不是 PIN 碼 (iOS 8+)

- 在裝置 PIN 碼受管理時，停用 app PIN 碼
- 需要公司憑證才可存取
- 封鎖已進行破解或 root 的裝置執行受管理的 app
- 重新檢查存取需求前的等候時間 (分鐘)
  - 逾時 - 必須是介於 1 到 65535 之間的值 (預設 30)
  - 離線 - 寬限期必須是介於 1 到 65535 之間的值 (預設 720)
  - 清除 app 資料前的離線間隔 (天) - 必須是介於 1 到 65535 之間的值 (預設 90)

需要最低 iOS 作業系統

- 需要最低 iOS 作業系統 (僅警告)
- 需要最低 app 版本
- 需要最低 app 版本 (僅警告)
- 需要最低的 Intune app 保護原則 SDK 版本

按**下一步**。

8. 選擇與指派要套用此原則的 app。
9. 按**下一步**。
10. 選擇要套用此原則的使用者群組。
11. 按一下**完成**。

新增 Android 裝置的 Office 365 app 保護原則

程序

1. 前往 **App > Office 365 App 保護**。
2. 按一下 **App 原則 > +新增**。
3. 輸入原則的**名稱**並選擇性輸入原則的**描述**。
4. 在「選擇作業系統」下，按一下 **Android**。
5. 在**資料重新配置**下，從下列設定和選項中挑選：
   - 禁止 Android 備份
   - 允許 app 將資料傳送到其他 app - 所有 app (預設)、受原則管理的 app、無
   - 允許 app 接收來自其他 app 的資料 - 所有 app (預設)、受原則管理的 app、無
   - 禁止「另存新檔」
   - 限制從其他 app 剪下、複製與貼上資料 - 任何 app (預設)、鎖定的、受原則管理的 app、受貼上原則管理的
   - 限制可在「受管理瀏覽器」中顯示的 Web 內容
   - 加密 app 資料
   - 在啟用裝置加密時，停用 app 加密
   - 停用聯絡人同步
   - 停用列印
6. 在**存取**下，從下列設定和選項中挑選：

- 需要 PIN 碼才可存取
- 重設 PIN 碼之前的嘗試次數 (預設 5)
- 允許簡單 PIN 碼
- PIN 碼長度 (預設 4)
- 允許指紋而不是 PIN 碼 (Android 6+)
- 在裝置 PIN 碼受管理時，停用 app PIN 碼
- 需要公司憑證才可存取
- 封鎖已進行破解或 root 的裝置執行受管理的 app
- 重新檢查存取需求前的等候時間 (分鐘)
  - 逾時 - 必須是介於 1 到 65535 之間的值 (預設 30)
  - 離線 - 寬限期必須是介於 1 到 65535 之間的值 (預設 720)
  - 清除 app 資料前的離線間隔 (天) - 必須是介於 1 到 65535 之間的值 (預設 90)
- 封鎖螢幕擷取和 Android 助手
- 需要最低 Android 作業系統
- 需要最低 Android 作業系統 (僅警告)
- 需要最低 app 版本
- 需要最低 app 版本 (僅警告)
- 需要最低的 Intune app 保護原則 SDK 版本

7. 按**下一步**。
8. 選擇與指派要套用此原則的 app。
9. 按**下一步**。
10. 選擇要套用此原則的使用者群組。
11. 按一下**完成**。

修改 Office 365 app 保護原則

程序

1. 前往 **App > Office 365 App 保護**。
2. 按一下 **App 原則**。
3. 按一下待修改原則的名稱。
4. 在原則詳細資料頁面上，按一下**編輯**。
5. 修改原則配置設定。
6. 按**下一步**。
7. 修改要套用此原則的 app 清單。
8. 按**下一步**。
9. 修改要套用此原則的使用者群組。
10. 按一下**完成**。

刪除 Office 365 app 保護原則

程序

1. 前往 **App > Office 365 App 保護**。
2. 按一下 **App 原則**。
3. 在**動作**欄下，按一下待刪除原則名稱的移除圖示。
4. 按一下**是**以進行確認。

Office 365 App 配置

前往 **App > Office 365 App 保護**頁面 (在 **App 配置**索引標籤下)，以新增、修改或刪除不同使用者群組的 Office 365 App 配置。 在這些 app 配置中，管理員可新增鍵值配對清單。 並指派配置給一或多個 Office 365 app。 「App 配置」索引標籤清單提供表格式詳細資料，例如更新的時間戳記、平台、指派的 app 及部署狀態。

新增 Office 365 App 配置

程序

1. 前往 **App > Office 365 App 保護**。
2. 按一下 **App 配置> +新增**。
3. 輸入配置的**名稱**並選擇性輸入配置的**描述**。
4. 輸入鍵值配對。
5. 按**下一步**。
6. 選擇與指派要套用此配置的 app。
7. 按**下一步**。
8. 選擇要套用此配置的使用者群組。
9. 按一下**完成**。

修改 Office 365 App 配置

程序

1. 前往 **App > Office 365 App 保護**。
2. 按一下 **App 配置**。
3. 按一下待修改配置的名稱。
4. 在組態詳細資料頁面上，按一下**編輯**。
5. 或者，按一下 **App 發佈**或**使用者群組發佈**索引標籤。 按一下**編輯**以僅修改那些設定，然後按一下**儲存**。
6. 修改配置設定。
7. 按**下一步**。
8. 修改要套用此配置的 app 清單。
9. 按**下一步**。
10. 修改要套用此配置的使用者群組。
11. 按一下**完成**。

刪除 Office 365 App 配置

程序

1. 前往 **App > Office 365 App 保護**。
2. 按一下 **App 配置**。
3. 在**動作**欄位中，按一下待刪除配置名稱的移除圖示。
4. 按一下**是**以進行確認。

違規的 Office 365 app 使用者。

管理員可檢閱違規的使用者及其裝置清單。 使用此頁面來清除被標示裝置上的任何 Office 365 app。

清除 Office 365 app

程序

1. 前往 **App > Office 365 App 保護**。
2. 按一下**違規使用者**。
3. 執行下列其中一個動作：
   - 從清單選擇使用者，然後按一下**清除 Office 365 App**。
   - 按一下使用者名稱，以顯示含有違規 app 的裝置清單。 在**動作**欄位中，按一下特定裝置的**清除 Office 365 App** 圖示。
   - 按一下使用者名稱，以顯示含有違規 app 的裝置清單。 按一下特定裝置的名稱，以檢視列有套件 ID/套件名稱和標示原因的 App。 按一下**清除 Office 365 App**。
4. 按一下**是**以確認動作。

或者，執行下列步驟：

1. 前往**使用者**。
2. 按一下使用者的名稱，以開啟使用者詳細資料頁面。
3. 按一下**動作 > 清除 Office 365 App**。
4. 選擇要清除 Office 365 app 的裝置。
5. 按一下**確定**以確認動作。

取消 Office 365 app 的清除請求

程序

1. 前往**使用者**。
2. 按一下使用者的名稱，以開啟使用者詳細資料頁面。
3. 按一下 **Office 365 保護**索引標籤。
4. 從**選擇報告類型**下拉式方塊，選擇**清除請求**報告，以顯示對應資訊。
5. 選擇要取消清除請求的裝置。 只能選擇狀態為「清除擱置中」的裝置。
6. 按一下**取消清除**。
7. 按一下**確定**以確認動作。

使用 Office 365 App 保護之使用者的 App 報告

管理員可選擇下列其中一種報告，以檢閱使用 Office 365 App 保護的使用者清單及相關資訊。

- App 原則報告
- App 配置報告
- 抹除請求

「App 報告」中的資訊包括套件 ID/套件名稱、裝置名稱、裝置類型、原則或配置 (部署到裝置)、狀態 (同步、同步但已過時或未同步)，以及上一次登記的時間。 App 報告的資訊可以匯出至 CSV 檔案，以供日後參考或分析。

「清除請求」報告中的資訊包括顯示名稱、使用者名稱、裝置名稱、裝置類型及清除狀態 (清除擱置中或完成清除)。

執行下列步驟以檢視其中一種報告：

1. 前往**使用者**。
2. 按一下使用者的名稱，以開啟使用者詳細資料頁面。
3. 按一下 **Office 365 保護**索引標籤。
4. 從**選擇報告類型**下拉式方塊，選擇其中一種報告以顯示對應資訊。
5. (選用) 從「清除請求」頁面選擇要取消清除請求的裝置，然後按一下**取消清除**。 只能選擇狀態為「清除擱置中」的裝置。
6. (選用) 按一下**匯出至 CSV**，透過 CSV 檔案形式下載報告內容，以供日後參考或分析。

12.6. 連接 Google App

本節包含以下各主題：

- 受管理的 Google Play 帳戶 (Android Enterprise 帳戶)
- Android 裝置註冊
- Android 管理 API
- Google Apps API
- 管理 - Android Enterprise

12.6.1. 受管理的 Google Play 帳戶 (Android Enterprise 帳戶)

授權：Silver

您需要受管理的 Google Play 帳戶才能啟用 Android Enterprise 裝置的使用與配置。 您不必再使用 Google Apps Directory Sync (GADS) 或使用 Google 帳戶來註冊裝置。

重要事項：如果您已設定 Android Enterprise，則必須先淘汰此類裝置才能使用此功能。

使用受管理的 Google Play 帳戶設定 Android Enterprise

程序

1. 登入 Ivanti Neurons for MDM 入口網站。
2. 前往**管理 > Google > Android Enterprise**。
3. 在**受管理的 Google Play 帳戶**下，按一下**授權 Google**，以顯示 **Google Play for Work** 頁面。
4. 輸入您的 **Google Play 帳戶電子郵件ID**。
5. 按一下**開始使用**。
6. 接受 Android Enterprise 協議。
7. 按一下**確認**。
8. 按一下**完成註冊**。
   已配置 Android Enterprise區段會顯示下列資訊:
   - **狀態**
   - **管理員電子郵件**
   - **企業類型**
   - **Google Enterprise ID**

當 Android Enterprise 設為使用受管理的 Google Play 帳戶，每位使用者的裝置註冊數目將會受限。 若要在建立新使用者時克服此限制，請選擇 **Android Enterprise 裝置帳戶**選項，以便讓附加至此帳戶的 Android Enterprise 受工作管理的裝置註冊自動接受 Google 裝置帳戶指派。

裝置帳戶專門用於 COSU (單一使用) 部署 (例如採用單一應用模式)。 擁有裝置帳戶的使用者其 Google Play 存取權可能會受到限制。

偶而，受管理 Google Play 帳戶或其權杖會因為各種理由而到期，例如身份認證權杖到期或者帳戶或企業遭刪除。 在這類情況下，Google Play 服務會透過廣播動作通知用戶端，以觸發用戶端藉由移除現有帳戶並為帳戶新增從 UEM 伺服器取得的新權杖的方式來重新佈建裝置。

如果帳戶重新佈建失敗，無論原因是舊帳戶無法移除或多次嘗試重新佈建，系統將會通知使用者藉由淘汰用戶端或執行裝置原廠重設來重新開始，至於採用哪一種方式則取決於裝置處於工作設定檔模式還是受管理裝置模式。

將現有的受管理的 Google Play 帳戶移轉至受管理的 Google 網域帳戶 (BTE)

此功能可讓 Android Enterprise 帳戶和裝置從**受管理的 Google Play 帳戶**移轉至**受管理的 Google 網域帳戶**。

移轉包含:

- 帳戶升級
- 裝置移轉

必要條件

- 裝置必須以工作受管理裝置或工作描述檔模式註冊；在公司擁有裝置上工作描述檔 (WPCOD) 模式中註冊的裝置必須執行 Android 12 或更高版本。
- 裝置已被指派有效的公司或商務電子郵件 ID。

> 如果裝置已指派至非公司電子郵件 ID，管理員必須重新指派有效的公司電子郵件 ID，裝置才能符合移轉資格。

升級 Android Enterprise 帳戶

將 Android Enterprise 帳戶從受管理的 Google Play 帳戶升級為受管理的 Google 網域帳戶。

程序

1. 前往**管理員** → **Google** → **Android Enterprise**。
2. 按一下**升級帳戶**。
3. 使用有效的公司或商務電子郵件 ID 登入。
4. 完成升級程序。
5. 重新整理頁面。

套用裝置移轉組態

程序

1. 導覽至組態 >> +新增。
2. 選取 **Android Enterprise: 從受管理 Google Play 到受管理 Google 帳戶的裝置移轉** 組態 > **編輯** > **下一步** > **所有裝置或自訂** > **慢速推出發佈** - 預設會選取**手動推出**選項 > 在下拉清單**在選擇摘要中自訂的裝置 % (慢速推出)** 或**選擇摘要中的所有裝置**中進行選擇。
3. 按一下**完成**。

完成裝置移轉

程序

1. 在裝置上，當出現「新增工作帳戶」提示時，點選**繼續**。
2. 驗證**公司電子郵件 ID**。
3. 輸入**密碼**。
4. 如果可用，請完成**雙因素驗證 (2FA)**。
5. 完成帳戶設定程序。

驗證移轉

在裝置上

1. 開啟 **Google Play 商店**。
2. 確認帳戶類型已從工作帳戶變更為公司網域帳戶。

在管理員控制台中

- 若要檢視**Android Enterprise: 從受管理 Google Play 到受管理 Google 帳戶的裝置移轉**組態狀態，請導覽至**裝置** > **裝置** > **裝置詳細資料** > **組態** > **Android Enterprise: 從受管理 Google Play 到受管理 Google 帳戶的裝置移轉**。 確保組態狀態處於已安裝狀態。

監視移轉狀態

管理員可以使用下列方式追蹤移轉 (**移轉至受管理的 Google 帳戶**) 進度:

- **裝置詳細資訊** – 檢視每個裝置移轉狀態
- **進階搜尋** – 篩選已移轉及未移轉的裝置
- **裝置群組** – 將已移轉與未移轉的裝置分組

這些選項有助於識別需要進一步動作的裝置。

使用受管理 Google 網域帳戶 (BTE) 的新註冊

Android Enterprise 可使用**受管理的 Google 網域帳戶**進行設定，無論是否使用 Google 驗證。

程序

1. 登入至入口網站。
2. 前往**管理** > **Google** > **Android Enterprise**。
3. 在**受管理的 Google Play 帳戶**下，按一下**授權**。
4. 輸入您的**公司**或**商務電子郵件 ID**，然後按一下**下一步**。
5. 選取**建立新繫結於..** 在**選取繫結選項**頁面。
6. 按一下**確認**。 此時會顯示**略過**和**啟用**選項。
- **略過** - 在沒有驗證的情況下繼續
- **啟用** – 進行驗證後繼續

已配置 Android Enterprise區段會顯示下列資訊:

- **狀態**: 顯示連線狀態。
- **管理員電子郵件**: 顯示公司或企業電子郵件 ID。
- **企業類型**: 顯示企業類型。
- **Google 驗證設定**: 根據驗證需求顯示否/是。
- **Google Enterprise ID**: 顯示唯一的 Google Enterprise ID。
- **企業名稱**: 顯示企業名稱。

12.6.2. Android 裝置註冊

在 Android 裝置註冊期間，如果您需要使用者提供電話權限 (需要有此權限才能報告 IMEI、電話號碼及其他電話識別碼以完成註冊)，您可配置此選項。 進行配置時，系統會提示裝置使用者授與權限，以允許 Go 用戶端存取裝置識別碼。

> 此配置僅適用於新註冊的所有 Android 裝置 (執行 Android 6.0 以上版本)。

1. 選擇**管理 > Google > 註冊**。
2. 選取**註冊期間需要 Android 裝置識別碼 (工作設定檔和裝置管理員)**。
3. 按一下**儲存**。

有關遺失模式的更多資訊，請參閱**管理遺失模式下的 Android 裝置**

12.6.3. Android 管理 API

Android 管理 API (AMAPI) 是 Google 的雲端平台 API，將 Google Android UEM 功能整合至 Ivanti Neurons for MDM。 在 Android Enterprise 設定中，您可以啟用 Android 管理 API 架構以管理 Android Enterprise 裝置，無需在裝置上安裝用戶端應用程式就能進行裝置管理。 目前，不支援針對其他功能 (例如 MTD 等) 將 Go app 推送至裝置。

當您在設定中已設定 Android Enterprise 帳戶時，您將可以啟用和使用 Android 管理 API 架構。 啟用後，您就可以：

- 新增註冊描述檔，為 Device Enrollment 使用 QR 碼。
- 針對註冊的裝置建立專屬的裝置配置 (公司擁有的單一使用，或 COSU) 以符合特定目的。

僅在已安裝 Google Play 並在專屬模式中佈建的 Android 第 9 版或更新版本裝置支援 Android 管理 API。 企業專屬模式也是指公司擁有的單一使用 (COSU) 是一種裝置擁有者模式。 此外，此功能也支援以下裝置動作：

- 鎖定
- 重新開機
- 同步至伺服器
- 抹除

定期排定裝置登記 (每小時)。 如要立即採取行動，在裝置詳細資料頁面中使用裝置動作「同步至伺服器」。 AMAPI 裝置不會傳送強制簽入至 Ivanti Neurons for MDM。 當裝置上有活動時，會執行庫存更新。

啟用 Android 管理 API

若要啟用 Android 管理 API，請前往**管理員 > Android Enterprise > 授權 Google (需要有效的 Google 位址) > 已啟用 Android Enterprise**。

已啟用 Android 管理 API 功能的狀態 (**是**表示已啟用，而**否**表示已停用) 也會顯示在「裝置詳細資訊」頁面中。

> COSU 目前不支援 GSuite 帳戶。

新增註冊描述檔

需要建立註冊描述檔才能使用 QR 碼掃描或權杖的英數字元字串註冊 Android 裝置。 只有在啟用 Android 管理 API 後，才能建立註冊描述檔。 您也可以建立與註冊描述檔關聯的自訂裝置屬性。

1. 選擇**管理 > Android Enterprise > 註冊描述檔**。
2. 在**註冊描述檔 - 公司擁有的專屬裝置**視窗中進行以下設定。
3. 按一下**儲存**。 **描述檔摘要**視窗顯示以下權杖詳細資料：

設定	描述
名稱	輸入可識別此註冊描述檔的名稱。
描述	輸入可說明此註冊描述檔用途的描述。
使用者名稱	輸入有效使用者名稱的前幾個字母，然後從顯示的相符結果中做選擇。 有效的使用者名稱可來自本機使用者或 LDAP 使用者。 針對個別使用者建立註冊描述檔，註冊描述檔會在描述檔中使用 QR 碼標記要顯示為屬於該使用者的已註冊裝置。
權杖有效性	輸入驗證權杖 QR 碼掃描的有效天數。 輸入的數字應在 1-30 之間。 如果您使用權杖或註冊後註冊描述檔有效期，裝置會重設。
自訂裝置屬性	在動作欄中，按一下 **+新增**以新增要與註冊描述檔建立關聯的自訂裝置屬性。 1. 從**屬性名稱**欄中的下拉清單中選擇自訂裝置屬性。 2. 在**值**欄中，輸入自訂屬性的值。 3. 按一下**儲存**。 表格中會顯示新增的自訂裝置屬性。 如要刪除，在「動作」欄中按一下**刪除**選項。 自訂屬性只能在設定檔建立期間新增至註冊設定檔。 在建立描述檔後，就無法編輯屬性欄位。

- 名稱
- 描述
- 使用者名稱
- 權杖建立日期
- 權杖到期日
- 權杖值
- QR 碼
- 自訂裝置屬性。

> 如果在註冊過後 10 分鐘內無法取得裝置的適當配置，裝置將會重設。 在此情況下，您應使用註冊權杖/QR 碼重新註冊。

在建立註冊描述檔後，它會列在**註冊描述檔**頁面。 您可以執行**動作**欄中下列其中任何一項動作。

- 在描述檔摘要視窗中，按一下檢視圖示以檢視註冊描述檔的詳細資料。 QR 碼也會顯示在此視窗中。
- 按一下編輯圖示以編輯註冊描述檔的詳細資料。

> 您只能編輯權杖有效性。 無法編輯其他的屬性。

按一下刪除圖示以刪除註冊描述檔。

建立 COSU 配置

管理員可使用 Android Enterprise 設定用於特定目的之專屬裝置 (公司擁有的單一使用，或 COSU) 配置。COSU 配置會發佈至受工作管理的裝置 (裝置擁有者模式)，僅在單一應用模式下為使用者提供一種可用的 app。 不支援啟用公司擁有裝置上的工作描述檔的裝置。

使用此配置，管理員可以將裝置設為將 app 釘選至畫面，如此單一應用模式使用者就無法取消釘選此 app，並離開此 app 前往裝置的其他畫面，或使用裝置上的任何其他 app。

> 在「進階選項與 App 配置」之下選擇「在裝置上安裝」選項，也可以將其他 app 強制安裝在 AMA 裝置上，但是當透過配置將單一應用 app 釘選至畫面上時，您將無法與它們互動。 針對多個 app 單一應用，建議使用受工作管理的裝置 (裝置擁有者) 的單一應用功能。 這可讓您更能控制 app 和裝置設定，並可延伸至多使用者模式。

管理員可以根據需求檢視不同的選項變更配置，例如允許系統導覽和可以使用透過 Google DPC 為使用者推送至裝置的其他 app。

會依所指派給配置的優先順序來判斷 COSU 配置。 在推送原則配置至 Google 時使用最高優先順序配置。 COSU 配置會套用至定義空間內的裝置。 如果在預設空間已定義，則可以委派給其他空間。

如要配置：

1. 前往**配置 > +新增**。
2. 在**鎖定與單一應用：Android Enterprise 配置**中，按一下**專屬裝置 (公司擁有的單一使用，或 COSU)**。
3. 輸入配置的名稱。
4. 輸入描述。
5. 按一下相關標籤，您可進行以下設定：

- **App 設定**
- **一般鎖定**
- **單一應用自訂**
- **系統設定**

下表提供可設定欄位的詳細資料：

設定	描述
App 設定	
App 名稱	輸入 app 的名稱時，輸入 app 的名稱開頭的幾個字母直到您在下拉式清單清單中看到所需的 app，然後選擇要釘選在 app 上的裝置。 如果您在下拉清單中未看到所需的 app，請確定您要部署的 app 在 Play Store 中為公用/私人 app，而且已新增至 App Catalog。 此欄位為必填。 如果您在此欄位中未選取要新增的 app，將無法建立配置。 您只能新增公用和私人 app。 無法新增內部開發的 app 和 Web app (私人)。
一般鎖定	
保持顯示	針對裝置所處的模式設定連接的電源。 請選擇下列任何選項： • **AC** - 電源為 AC 充電器 • **無線** • **USB** - 電源為 USB 連接埠 • **任意** - 電源是來自 AC 充電器或 USB 連接埠或無線充電器。
單一應用自訂	
自訂狀態列	請選擇下列任何選項，在目標裝置上自訂狀態列： • **通知與系統資訊已啟用** - 在狀態列中顯示系統資訊和通知。 • **僅系統資訊已啟用** - 在狀態列中僅顯示系統資訊。
自訂系統導覽	請選擇下列任何一個選項，在 kiosk 模式下指定導覽功能的存取 (「首頁」及「概覽」按鈕): • **已啟用** - 啟用主畫面和概覽按鈕導覽。 如果此選項已選取，使用者可離開指定的 app。 • **已停用** - 停用主畫面和概覽按鈕導覽。 • **僅限首頁按鈕** - 僅啟用首頁按鈕導覽。 所有這些選項都可使用返回按鈕。
啟用全域動作	選擇在單一應用模式中啟用的全域動作。 您可透過此選項來控制重新啟動並關閉與電源按鈕關聯的功能。
啟用系統錯誤對話方塊	選擇此選項，為單一應用模式中當機或無回應的 app 啟用錯誤對話方塊。
系統設定	
系統更新設定	設定以下管理系統更新設定： • **系統更新** - 選擇所需的系統更新類型。 ◦ **自動** – 有可用的更新時，就會自動安裝。 ◦ **延後** - 將自動安裝延後最長 30 天。 ◦ **範圍限制** - 在每日維護期間自動安裝。 為維護期間設定開始和結束時間。 在裝置上安裝更新視支援的功能集、Android 版本，以及安裝在裝置上的 Google DPC 版本而定。

設定	描述
	• **凍結期間** - 當裝置設在凍結期間內，將會封鎖而且不會安裝所有傳入的系統更新。 按一下**新增凍結期間**，以設定凍結期間的**開始日期**和**結束日期**。 當裝置不在凍結期間，會套用正常的更新行為。 如果結束日期早於開始日期，凍結期間會延長至當年到來年之間。 凍結期間可設為最長 90 天。 兩個連續凍結期間之間必須相隔至少 60 天。

6. 按**下一步**。
7. 請選擇下列發佈選項之一：

- **所有裝置**
- **沒有裝置** (預設)
- **自訂**

8. 按一下**完成**。

管理 AMAPI 裝置上的 app。

當 COSU 配置發佈至裝置時，會將 app 推送並釘選至 AMA 裝置的畫面上。 不論推送至裝置的 COSU 配置為何，仍可以管理已安裝在 AMA 裝置上的 app。 以下為這些裝置上的 app 管理詳細資訊：

- 僅支援公用、私人 app；不支援內部開發 app 和 Web Clip。
- 僅當「在裝置上安裝」或「無訊息自動安裝」選項已啟用時，才會推送 app。 未啟用這些選項之下，在裝置或在裝置的 Play Store 上的任何使用者動作將不會看到指派至使用者/裝置的 app。
- 支援的 app 配置為 Managed Google Play 和工作管理裝置 (Android for Work) 設定。 支援應用程式的受管理組態，包括用於 OEMConfig 應用程式的受管理組態。

> 組態安裝和解除安裝的完成時間視 Google (傳訊服務) 關於是否已執行所需動作的通知而定。

- 現在作為 AMA 裝置註冊的一部分，將會依預設安裝 Go app。 在註冊程序期間，應用程式將會釘選在畫面上，並且在設定完成時於背景中執行。

> 不支援基於製造商、OS 版本和安全性修補程式等級實施的裝置註冊要求以外之原則。 裝置允許清單功能，僅允許列入允許清單的裝置向 Ivanti Neurons for MDM 註冊。

管理 AMAPI 裝置上的應用程式回饋支援

可以在 AMAPI (COSU) 裝置上管理應用程式回饋支援。 當裝置在 AMAPI (COSU) 模式下註冊時，受管理的應用程式組態將直接從 Google 推送至 Ivanti Neurons for MDM 而不會受到 Go app 的任何干預。 您可以在**裝置詳細資訊 > 已安裝的應用程式 > 檢視回饋**中檢視裝置層級的受管理應用程式回饋資訊，或者可瀏覽到「應用程式組態回饋」索引標籤下方應用程式目錄中的特定 Android 應用程式，檢視個別應用程式層級的相關資訊，瞭解所有裝置的整體報告。 如需有關應用程式回饋機制的資訊，請參閱**同步並擷取 App 回饋**。

AMAPI 限制

目前，AMAPI 有以下限制:

- 僅支援專屬的裝置 (COSU 模式)。

支援的配置

以下配置支援 AMAPI：

- App 發佈 (單一或多個 app)
- 受管理的 App 配置用於推送至裝置的 app
- Wi-Fi 配置
- Android Enterprise 鎖定專屬 (COSU) 配置
- Always-on VPN 組態

12.6.4. Google Apps API

若 Google 客戶是使用單一登入 (SSO) 來驗證使用者的 Google Apps 服務存取權，則可能無法透過 Exchange 讓使用者連線電子郵件、聯絡人和行事曆，這是由於通訊協定的限制，導致裝置不支援由 SSO 觸發的外部驗證服務重新導向。 此服務可以透過安全地建立與管理用來進行 ActiveSync 連線的帳戶密碼，來解決這個問題。

必要條件

在嘗試設定 Google Apps API 功能之前，您需要：

- 在 https://console.developers.google.com/ 上管理帳戶的存取權。
- 在 https://admin.google.com 上管理帳戶的存取權。

啟用 Google Apps API 功能

程序

1. 選擇**管理 > Google > Google Apps API**。
2. 按一下左側標示 1 之矩形底部的**步驟 1：Google Dev**。
3. 隨即出現「步驟 1：Google Dev」頁面。
   請遵循顯示在「步驟 1：Google Dev」頁面中的指示，然後按一下**完成**。
4. 按一下中間標示 2 之矩形底部的**步驟 2：Google 管理**。
5. 隨即出現「步驟 2：Google 管理員」頁面。
   請遵循顯示在「步驟 2：Google 管理員」頁面中的指示，然後按一下**完成**。
6. 在右側標示 3 之矩形中的**輸入 Google 管理員使用者名稱**欄位裡輸入 Google 管理員的使用者名稱，
7. 在同一矩形中，按一下**選擇檔案**，上傳在步驟 1 中下載的 JSON 檔案。
8. 按一下**儲存**。
9. 如果您無法看到 Google Apps API 頁面，可能是您沒有所需的權限。 您需具備下列其中一個角色：
   - 系統管理
   - 系統唯讀

12.6.5. 管理 - Android Enterprise

授權：Silver

- 已啟用 Android Enterprise 的 Ivanti, Inc 生產力應用程式 (如 Email+、Docs@Work 及 Web@Work) 需要金級授權。
- Tunnel for Android Enterprise 需要白金級授權。

Android Enterprise 啟用 Android Enterprise 應用程式的使用與組態。 Android Enterprise 使用者可從 應用程式目錄及透過 Google Play 檢視及安裝應用程式

如果您是新客戶，app 發佈預設為按裝置。 您無法變更此設定。 若是升級客戶，您可以選擇按使用者或按裝置發佈 app。 此外，若是升級客戶，app 發佈預設為按使用者。 許多使用者擁有多個裝置。 如果使用者擁有多個裝置，當 app 發佈設為按裝置，則您可以在每個裝置上製作不同的 app 組合。

本節包含以下各主題：

- 設定 Android Enterprise
- 設定 Android Enterprise 工作描述檔

設定 Android Enterprise

1. 在 Ivanti Neurons for MDM 入口網站中，按一下**管理員 > Google > Android Enterprise**。
2. 請選擇下列選項之一：
    - **受管理 Google Play 帳戶:** 針對並未訂閱 G Suite 的企業，此方法可讓使用者直接註冊 Android Enterprise，無須傳送任何個人資訊 (將電子郵件地址傳送至 Google)。 Ivanti Neurons for MDM 將透過 Google 自動佈建與管理使用者。 系統會請您使用管理員 Google 帳戶授權 Android Enterprise。
    - **受管理 Google 帳戶:** 針對已訂閱 G Suite 的企業，此方法可讓使用者利用其 Google 帳戶註冊 Android Enterprise。 每位使用者都必須擁有 Google 帳戶，方可註冊 Android Enterprise。

遵循畫面上的指示，完成配置程序：

4. 若是自動方法，此程序包括：
    - 啟用 UEM API 並建立企業憑證。
    - 授權給整合擁有者，以向 Google 註冊。 您應使用 IT 帳戶，而非個人帳戶。
    - 拖曳服務帳戶 JSON 用戶端 ID，以設定憑證。

若是其他方法，此程序包括：

- 參閱下節中的用戶端 ID，並將其新增至 Google 管理入口網站。
- 在 Google 管理入口網站中尋找您的 MDM 權杖，並在 Google Cloud Console 中尋找服務帳戶。
- 在 Ivanti Neurons for MDM 中輸入您的 MDM 權杖、企業 Google 網域及企業管理員電子郵件地址，以連線到 Google 服務。
- 在 Ivanti Neurons for MDM 中拖放您的服務帳戶 JSON 用戶端 ID。
- 在 Ivanti Neurons for MDM 中，按一下**授權**以授權 Ivanti Neurons for MDM 檢視和/或管理您的 Google 使用者。

Ivanti Neurons for MDM 使用者介面會引導您完成這些步驟。

可將 Ivanti Neurons for MDM 繫結至受管理 Google 帳戶的用戶端 ID

在管理主控台中將用戶端 ID 新增為 **140561810807-tiiglke17laibbrt5darupmvo4ae7cbj.apps.googleusercontent.com**，將 Ivanti Neurons for MDM 租用戶與受管理 Google 帳戶繫結。

設定 Android Enterprise 工作描述檔

1. 在 Ivanti Neurons for MDM 入口網站中，前往**組態**。
2. 按一下 **+新增**。
3. 選擇**鎖定與單一應用：Android Enterprise** 配置。
4. 輸入配置名稱與說明。
5. 按一下**工作描述檔**鎖定類型。
   選擇您要套用至目標裝置的**鎖定設定**。
   重要事項：當使用者使用「設定」中的「新增帳戶」來新增 Google 帳戶時，Google 驗證伺服器會檢查帳戶的網域是否註冊為 UEM 管理的網域。 確認已勾選**在 Android 裝置上強制執行 UEM 原則**。 如果勾選，Go 用戶端會自動安裝或更新 (如果裝置尚未安裝) 並啟動。 在使用者完成註冊程序後，系統會提示使用者建立工作描述檔，且 Google 帳戶會自動移轉至工作描述檔。

12.7. 使用 ChromeOS 裝置

本節包含以下各主題：

- ChromeOS 和 Ivanti Neurons for MDM
- 將 Android 應用程式發佈至 ChromeOS 裝置
- ChromeOS 藍圖組態
- 裝置動作
- 常見問題
- 建議的評估步驟

12.7.1. ChromeOS 和 Ivanti Neurons for MDM

ChromeOS 由 Google 製作及發佈，是一款以 Linux 為基礎的作業系統。 Ivanti Neurons for MDM 支援執行 Android、Windows、iOS 和 macOS 的裝置。 而目前也已擴充支援範圍，涵蓋 ChromeOS 裝置。 Ivanti Neurons for MDM 提供了一款簡單且統一的行動管理解決方案，可用於設定及管理您的 ChromeOS 裝置。 Ivanti 提供了一款適用於 ChromeOS 裝置的解決方案，操作簡單、功能豐富，可實現統一管理，類似於在 Ivanti Neurons for MDM 上專為 iOS、Android、Windows 及 Mac 所設的管理工作流程。 管理員只需使用**管理員 > Google > ChromeOS 管理**中的簡易整合，很輕鬆就能將 Ivanti Neurons for MDM 與其 Google Cloud (也稱為 Google 管理控制台) 連接起來。

必要條件

1. 必須具備受管理的 Google 管理員帳戶。
2. 必須在 Google 管理控制台上匯入 LDAP 使用者和 OU。 Ivanti Neurons for MDM 僅支援從 LDAP 來源匯入的 OU。 不支援本機 OU。
3. 管理員必須將組織單位 (使用者群組) 同步至 Ivanti Neurons for MDM。 此操作可經由設定 LDAP 伺服器及新增組織單位來完成。

授權 Google

Google 管理控制台上的 ChromeOS 裝置無法直接在 Ivanti Neurons for MDM 上註冊。 相反地，這些裝置會註冊 Google，並且這些裝置的相關資訊會在 Google 和 Ivanti Neurons for MDM 之間進行同步。 而管理員必須授權 Google 匯入裝置，以及執行像是指派應用程式、組態等其他動作。

程序

1. 前往**管理員 > Google > ChromeOS 管理**。
2. 按一下**授權 Google**。
3. 選取您要授權的 Google 管理員帳戶。
4. 按一下**繼續**，接受提供所需服務需要的權限。
   ChromeOS 已成功設定確認訊息隨即出現。 您也可以在確認訊息底下找到網域資訊。

從 Google 同步 ChromeOS 裝置

管理員必須從 Google 管理控制台同步 ChromeOS 裝置。 首次使用 Google 管理控制台存取 ChromeOS 裝置時，管理員必須使用 ChromeOS 管理頁面的「立即同步」選項手動同步裝置。

> 在首次手動同步裝置後，後續的同步將每小時自動進行一次。

刪除 Google 管理員主控台與 Ivanti Neurons for MDM 的整合

刪除整合會撤銷我們從 Google 所收到用於存取 Google 資源的 OAuth 權杖。 此動作會刪除 ChromeOS 裝置、與藍圖組態和應用程式組態相關聯的清單，以及註冊中繼資料。 藍圖組態和上傳的應用程式不會被刪除。

若租用戶註冊未刪除，您可以提交票證來排查問題。

程序

1. 前往**管理員 > Google > ChromeOS 管理**。
2. 在 ChromeOS Ivanti Neurons for MDM 註冊區段下，按一下**刪除**。
   螢幕上會出現一個快顯視窗，詢問您是否要繼續「刪除」作業，以及與此整合相關聯的所有裝置都將被刪除。 選取**確定**。

12.7.2. 將 Android 應用程式發佈至 ChromeOS 裝置

管理員可從應用程式目錄發佈 Android 應用程式至 ChromeOS 裝置。

必要條件

1. 必須設定 Android Enterprise。 如需有關設定 Android Enterprise 的資訊，請參閱**設定 Android Enterprise**。
2. Android 應用程式必須存在於應用程式目錄中。
3. 在發佈 Android 應用程式和 ChromeOS 藍圖組態前，請確保 ChromeOS 裝置 (Chromebook) 使用者隸屬於使用者群組 (也稱為組織單位)。

Android 應用程式一經識別，您便需要依照類似於任何其他應用程式的發佈程序來發佈該應用程式。 在您發佈 Android 應用程式時，請務必選取您想發佈該應用程式的使用者群組，然後在裝置上執行無訊息自動安裝。

如果您的現有 Android 應用程式部署是設為發佈至裝置/裝置群組或使用者，則必須將發佈方式變更為基於使用者群組。 如果應用程式已在使用中，此操作可能會影響現有的部署。 建議先在全新的應用程式上進行此操作。

安裝設定可讓管理員控制最後的無訊息自動安裝，這是將應用程式推送至 ChromeOS 裝置的必要條件。 必須在此選取使用者群組。

12.7.3. 新增和分發 ChromeOS 擴充功能應用程式

管理員可以將 ChromeOS 擴充功能應用程式新增到應用程式目錄，然後將這些應用程式分發到 ChromeOS 裝置。

程序

1. 前往**應用程式** > **應用程式目錄**。
2. 按一下 **+新增**。
3. 從清單中選取 **ChromeOS**。 畫面上會出現**新增 ChromeOS 應用程式詳細資訊**頁面。
4. 此頁面提供以下詳細資訊: **應用程式名稱** - ChromeOS 擴充功能應用程式的名稱、**擴充功能 ID** - 可以從 Chrome 線上應用程式商店取得此資訊。
5. 按**下一步**。 畫面上會出現**應用程式組態**頁面。 您可以選擇在下一次裝置登記時執行立即更新，或選擇在新版本推出時自動更新 app。
6. 選擇應用程式分發選項之一，然後提供所需的詳細資訊。

> ChromeOS 應用程式分發僅適用於 LDAP 使用者群組。

ChromeOS 擴充功能應用程式一經識別，您便需要依照類似於任何其他應用程式的分發程序來分發該應用程式。 在您分發 ChromeOS 擴充功能應用程式時，請務必選取您想分發該應用程式的使用者群組，然後在裝置上執行無訊息自動安裝。

> 安裝設定可讓管理員控制最後的無訊息自動安裝，這是將應用程式推送至 ChromeOS 裝置的必要條件。 必須在此選取使用者群組。

可以編輯有關 ChromeOS 擴充功能應用程式的資訊，或從應用程式目錄中刪除 ChromeOS 擴充功能應用程式。 必須遵循與從應用程式目錄中編輯或刪除任何其他應用程式類似的程序。

編輯 ChromeOS 擴充功能應用程式

1. 前往**應用程式 > 應用程式目錄 > 詳細資訊**。
2. 按一下**編輯**。 做出必要的變更，然後按一下**儲存**。

如需關於刪除應用程式的詳細資訊，請參閱從應用程式目錄刪除應用程式。

12.7.4. ChromeOS 藍圖組態

ChromeOS 藍圖組態具有以下設定:

- 裝置設定
- 使用者與瀏覽器設定
- 受管理的訪客工作階段設定

您可對特定使用者群組 (也稱為組織單位) 套用 ChromeOS 組態。 當您嘗試發佈 ChromeOS 藍圖組態時，將僅有「使用者群組」區段可用，而且所有與授權的 Google 管理控制台相關的 LDAP 使用者群組均將列於該區段之下。 您可從列出的群組中選取一個或多個群組並套用組態。

程序

1. 前往**組態 > 新增**。
2. 在作業系統區段下選取 **Google ChromeOS**。 畫面上將出現 **ChromeOS 藍圖組態**索引標籤。
3. 按一下 **ChromeOS 藍圖**。 畫面上將出現**建立 ChromeOS 藍圖組態**頁面。
4. 在**名稱**方格中輸入組態的名稱。
5. 在組態設定下，您可以視需要修改裝置設定、使用者與瀏覽器設定，以及受管理訪客工作階段設定，並切換「推送至裝置」按鈕來套用修改後的設定。
6. 按**下一步**。
7. 針對發佈選項選取**自訂**。

> 只有 LDAP 使用者群組可用於發佈組態。

> 若要將組態發佈給所有人，只能對 Ivanti Neurons for MDM 及 Google 管理控制台中可用的 LDAP 使用者群組進行。

選取一個或多個群組並按一下**完成**。

> 取消發佈已發佈的設定時，已套用的設定將不會還原。

> 可以在 ChromeOS 藍圖組態中上傳檔案。

12.7.5. 裝置動作

ChromeOS 裝置支援下列動作:

- **抹除** - 抹除動作會刪除裝置上的所有資料，而且裝置會重設為原廠設定。 如需詳細資訊，請參閱**清除裝置**。
- **鎖定** - 鎖定動作會阻止您在裝置上執行任何進一步的動作。 如需詳細資訊，請參閱**鎖定裝置**。
- **解除鎖定** - 解除鎖定動作將解放裝置以供進一步使用。 如需詳細資訊，請參閱**解除鎖定裝置**。

12.7.6. 常見問題

本節列出了您在 Ivanti Neurons for MDM 上使用 ChromeOS 裝置時，可能會遇到的一些一般常見問題集清單。

- Chromebook 管理與其他作業系統的管理有何差異？
- Google 目前僅允許以 LDAP 使用者群組為基礎的組態發佈，管理員在執行組態或應用程式操作時，應確保發佈是以 LDAP 使用者為基礎。 ChromeOS 裝置管理不支援本機使用者群組和裝置群組。
  透過 Ivanti 管理 ChromeOS 裝置時需要何種授權？
- ChromeOS 裝置應具備像是 Chrome Enterprise 升級版或 Chrome Education 升級版的授權。 這些可作為硬體的一部分或作為獨立授權向經銷商購買。 如需詳細資訊，請參閱 Google 說明文件。 若要開始使用 Chrome 裝置管理，Ivanti 需要安全 UEM (統一端點管理) 授權。
  是否會有行動威脅防禦 (MTD) 或類似的解決方案可用？ 我是否需要 MTD 的個別授權？
- 該產品目前並未提供上述項目，詳請參閱目前限制。 我們將透過常見問題集與發佈公告來提供更多關於功能性能變更的資訊。
  為何在組態及應用程式索引標籤內，不會像其他裝置那樣顯示詳細資訊？
- 由於組態是發佈至使用者群組，而不是依據使用者登入來套用，因此目前在裝置詳細資訊中不會顯示組態。 應用程式會遵循相同的發佈邏輯且存在相同限制。 我們將透過常見問題集與發佈公告來提供更多關於這些限制變更的資訊。
  目前 ChromeOS 支援多少種組態？
- 透過 ChromeOS，我們已減少了組態動態磚的數量，同時也減少了與組態相關的管理工作。 我們將此種組態稱為「ChromeOS 藍圖」。 ChromeOS 藍圖在這些裝置上可支援將近 700 種的組態。 有關組態選項的資訊，請參閱 Google 說明文件。
  如何輕鬆地管理單一組態，卻可以用於所有裝置？
- 管理員只需複製現有組態，然後依據各個使用者群組進行修改即可 (如有需要的話)。 您無需從零開始。
  如何將 VPN 組態新增至 Chrome 裝置？
- 這可以使用 Android 應用程式來完成，而不是使用原生 VPN。
  比如「淘汰」和「抹除」之類的裝置動作在這些裝置上是否可用？
- 企業內的 Chromebook 一律是由組織管理，而且此類裝置上的資料被認為完全歸屬於組織所有。 考量到這點:
  - 已封鎖「淘汰」
  - 可允許「抹除」
  - 可允許「鎖定」
  - 可允許「解除鎖定」
  - 其他動作 – 不支援

就硬體方面，Ivanti 支援哪些 Chromebook？

- Ivanti 原本就規劃支援 Google Cloud 裝置管理解決方案所支援的裝置。 Ivanti 目前並未發佈 Ivanti 解決方案所支援的具體硬體清單。
  支援哪個版本的 Chrome 作業系統？
- Google Cloud 僅支援 ChromeOS 的最新穩定版本，而基於後端整合性質的考量，Ivanti 的支援也同樣遵循 Google 的支援形式。
  由於剛推出此項功能，是否能列出目前的限制？

憑藉全新的 Chrome 作業系統支援，我們正致力於提供客戶所殷切期盼的功能。 以下是管理員應注意的一些限制:

- 目前不支援將 Chrome 作業系統擴充功能 (瀏覽器應用程式) (作為「應用程式」) 發佈。
- 目前不支援 Android 應用程式的受管理應用程式組態。
- Wi-Fi 組態 API 已於近期發佈，但目前並不支援。
- 目前不支援憑證發佈。

- 目前不支援發佈 Ivanti Go (其前身為 MobileIron Go) Android 應用程式。
- 目前不支援 Ivanti Tunnel (VPN) 應用程式。
- 目前不支援空間和空間委派。
- 目前不支援行動威脅防禦解決方案。
- 在這些歸類為未受管理的裝置上支援 Ivanti 的 Zero Sign-on 解決方案。
- 未能完全支援原則動作。

12.7.7. 建議的評估步驟

建議採用下列步驟來驗證解決方案:

1. 建立一個在目錄來源 (例如，Active Directory) 中具有一位測試使用者的個別 OU (使用者群組)。 這能避免對使用中的組織單位產生任何影響。
2. 同步 Ivanti、Google 以及目錄來源 (LDAP) 之間的使用者。 確認「測試 OU」在使用者群組中是否可用。
3. 如上述步驟所示，將 Ivanti Neurons for MDM 與 Google 進行整合。
4. 建立 ChromeOS 藍圖組態，並僅將此發佈至「測試 OU」使用者群組。
5. 啟動 Chromebook (全新系統或先前已經註冊)。 確保其在「裝置」清單中可用。
6. 確認裝置上的 ChromeOS 藍圖設定是否可用。
7. 依照類似的步驟進行 Android 應用程式發佈。

12.8. 韌體管理

本節包含以下各主題：

- 註冊 Zebra OTA 服務
- Samsung E-FOTA 授權管理 (已停用)

12.8.1. 註冊 Zebra OTA 服務

註冊 Zebra OTA (無線更新) 服務後，您可以啟用 Zebra OTA 組態，以接收並更新已註冊 Ivanti Neurons for MDM 的 Zebra 裝置之韌體詳細資料。

程序

1. 前往**管理員 > 基礎架構 > Zebra OTA**。 隨即顯示 **Zebra OTA 服務**頁面。
2. 在 **Zebra OTA 服務的連結**下，按一下**開始**。
3. 輸入您的 Zebra OTA 憑證，登入並遵循步驟，以要求核准您使用 Zebra 服務。
4. 按一下**完成驗證**，以確認 Zebra 服務連線。 確認連線時，「Zebra OTA 服務」頁面隨即顯示註冊成功的狀態。

若要撤銷註冊，請按一下**動作**欄中的**撤銷**。 **撤銷**動作將從現有組態中移除所有 Zebra OTA 組態。 如要重新註冊 Zebra OTA，請按一下**重新整理**。 重新整理動作對現有的配置沒有影響。

在註冊後，您可在「裝置擁有者」模式中啟用 Zebra 韌體配置，Go 用戶端會接收此韌體配s置並將之套用至 Zebra 裝置 (使用 Android 8.0 版或支援的更新版本)。 套用配置時，即會下載韌體並按照設定的排程將韌體安裝到裝置上。 如需啟用 Zebra 韌體配置的詳細資訊，請參閱系統更新配置。

在完成韌體更新後，您可以在「裝置」頁面的**系統更新**欄底下，檢視 Zebra 裝置的韌體更新狀態。 下列為可能的狀態：

- **未知** - 用戶端或作業系統不支援
- **最新** - 裝置已有最新的更新可用
- **擱置中** - 已套用系統更新配置，但尚未下載或套用更新
- **下載中** - 正在下載系統更新至用戶端
- **可用** - 目前已提供適用於裝置的系統更新
- **錯誤** - 下載或安裝時發生錯誤。

「裝置」頁面的 **Zebra 修補程式版本**欄位會顯示裝置的 Zebra 修補程式資訊。

> 在 Android 11 及更新版本的裝置上不支援 **Zebra 修補程式版本**；僅支援 **Zebra 完整升級**。

12.8.2. Samsung E-FOTA 授權管理 (已停用)

Samsung E-FOTA 服務已於 2022 年 7 月停用。 如需詳細資訊，請參閱 Samsung 公告。

> 從現在起，您已無法設定 Samsung E-FOTA 服務。 不過，如果您現在具有 E-FOTA 組態，則可以瀏覽至**管理** > **韌體管理** > **Samsung E-FOTA** 並按一下**停用**選項來停用該組態。

12.9. 管理指令碼和檔案

管理員可以管理可在組態中使用並推送到裝置的指令碼和檔案。

本節包含以下各主題：

所有指令碼

檔案

12.9.1. 所有指令碼

適用於: macOS 和 Windows 裝置

在**管理 > 指令碼和檔案 > 所有指令碼**頁面中，Ivanti Neurons for MDM 允許具有系統管理角色的使用者建立或上傳及管理可用於配置並發佈到裝置的指令碼。 您可以在自訂屬性和指令碼之間建立關聯，然後將所產生的值指派給已設定的裝置。 使用稽核追蹤來檢視指令碼變更的記錄，並使用裝置詳細資料頁面來檢視執行結果。

您可以編寫指令碼來設置裝置上的任何設定。 例如，您可以執行指令碼以實現：

- 強制裝置使用者每月變更其密碼；
- 在閒置 5 分鐘後鎖定螢幕；或
- 設定安全的 Wi-Fi 網路。

本節包含以下各主題：

- 新增指令碼
- 修改指令碼
- 使用指令碼變數 (適用於 Windows 和 macOS)
- 測試指令碼
- 驗證指令碼執行結果

新增指令碼

您可以建立或上傳 bash 指令碼 (適用於 macOS) 和 ps1 指令碼 (適用於 Windows) 的存放庫。 此儲存庫可以用於組態，以選擇指令碼並根據組態中的指定排程發佈至裝置上執行。

例如，您可以建立 Shell 指令碼以在裝置上執行。 必要時，您可使用包裝函式。 不支援從殼層指令碼中執行二進位檔。

> Ivanti 強烈建議您先測試自己的殼層指令碼，然後才在裝置上執行它們，以確保它們的健全性和品質。 在本機執行您的指令碼，並更正所產生的任何錯誤。

程序

1. 前往**管理員 > 指令碼 > 所有指令碼**。
2. 按一下 **+新增**。
3. 輸入指令碼的名稱和說明。
4. 在平台類型下，選取 macOS 或 Windows。
5. 選取下列**指令碼類型**之一：
    - **bash**
    - **zsh**
    - **python**
    - **swift**
    - **ps1**
6. 選擇**以 root 身分執行**選項，以在裝置上以 root 身分執行指令碼。 預設清除此選項。

7. 在**指令碼編輯器**中，可以在文字方塊內輸入、拖放或複製並貼上指令碼。
8. 或者，按一下**從指令碼匯入代碼**以拖放現有指令碼檔案，或按一下「選擇檔案」以瀏覽並選擇要上傳至 Ivanti Neurons for MDM 的指令碼檔案。 這將會取代指令碼編輯程式中的任何現有指令碼。 此動作無法取消。 按一下**匯入**。 所上傳指令碼的代碼將會顯示在指令碼編輯程式中。
9. (選擇性) 在**自訂可用屬性**區段中，選擇一或多個顯示的裝置自訂屬性，以便在它們和指令碼之間建立關聯。 它們可以用於將所產生的指令碼執行值指派給所設定裝置的裝置自訂屬性。 按一下**自訂屬性的範例代碼**，以檢視在指令碼中使用自訂屬性的範例代碼。
10. 按一下**儲存**。

指令碼中的自訂屬性應使用小寫。 如果自訂屬性獲得任何指令碼的參照，則該屬性將無法移除。 當您修改自訂屬性 (例如名稱)，而它與某個指令碼相關聯，則您應該要在相關聯的指令碼中進行對應變更。

修改指令碼

若要編輯或移除指令碼：

1. 前往**管理員 > 指令碼 > 所有指令碼**。
2. 在指令碼的**動作**欄位中，按一下對應圖示以編輯或刪除動作。
3. 遵循畫面指示以完成動作。

當指令碼 (內容、名稱、描述) 變更時，指令碼的所有關聯配置都會重新發佈至裝置。

使用指令碼變數 (適用於 Windows 和 macOS)

在指令碼儲存庫中定義並儲存指令碼輸入，例如環境和替換變數。 在適用於 macOS 的 Mobile@Work 組態或適用於 Windows 指令碼和動作的 Ivanti Bridge 組態中，視連結的指令碼而定，相關的指令碼變數將可視需要供使用。 對於 macOS，此功能需要 **Mobile@Work for macOS** 1.71.0 及以上版本，最高支援至 Ivanti Neurons for MDM 所支援的最新發行版本。 對於 Windows，此功能需要 **Ivanti Bridge**。

請使用變數，在每次指令碼執行時以不同的值執行它。 例如，管理員可建立指令碼，以使用 $ 環境變數做為指令碼變數，並使其與適用於 macOS 的 Mobile@Work 指令碼組態或 Windows 組態產生關聯。 將該組態發佈並安裝至每一台使用者裝置後，Ivanti Neurons for MDM 便會針對每台裝置傳送一個不同的已註冊使用者電子郵件地址來執行特定動作。 Ivanti Neurons for MDM 管理入口網站支援自訂變數。

如要新增指令碼變數：

1. 前往**管理員 > 指令碼 > 所有指令碼**。
2. 在「指令碼輸入」區段中，按一下 **+新增**。
3. 在「新增指令碼輸入 - 環境變數」快顯頁面中，輸入下列詳細資料：
    - 要顯示的標籤 - 在適用於 macOS 的 Mobile@Work 指令碼配置頁面中，此文字將會顯示為標籤。 例如，輸入作業系統資料夾、輸入 Apache 編號等等。
    - 環境變數名稱 - 例如，JAVA_HOME、OS_VERSION 等等。 在將配置詳細資料傳送至目標裝置時，Ivanti Neurons for MDM 會替換掉指令碼變數的值，因為這些值將保留在資料庫中。
    - 環境變數預設值 - 例如，1024、bin/java、$ 等等。 輸入變數將會用在管理員所上傳或編輯的指令碼中。 另請參閱下面的附註。

在預覽區中，檢視環境變數的值將如何顯示成配置頁面上的指令碼輸入。

5. 按一下**儲存**。

如此一來，只有標籤和預設值可用於配置，而非提供抽象層的環境變數名稱。

- 可接受英數字元值 (例如，1024、bin/java、root@localhost) 或系統屬性 (例如，$) 做為環境變數的值。

- 在配置頁面中進行部署時，可修改或刪除環境變數的值。
- 如果沒有提供環境變數的值，請確定在指令碼部署期間已提供值。 否則，將會傳送空白值至指令碼。
- 在裝置上發佈並安裝指令碼組態後，在**管理 > 指令碼和檔案 > 所有指令碼**頁面中編輯環境變數不會影響與指令碼關聯的現有組態。 另請參閱**適用於 macOS 的 Mobile@Work 指令碼組態**。 對於 Windows，請參閱 **適用於 Windows 指令碼和動作的 Ivanti Bridge 組態**。

編輯指令碼變數

如要修改指令碼變數，請對該變數按一下編輯 (鉛筆) 圖示並儲存變更。

如果指令碼配置參照至具有指令碼變數的指令碼，則對現有指令碼變數之標籤所做的編輯，也會反映在指令碼配置中。 不過：

- 指令碼變數預設值中的變更並不會反映在現有的配置中。
- 指令碼變數預設值中的變更將會反映在使用先前指令碼建立的任何新配置中。

刪除指令碼變數

如要刪除指令碼變數，請對該變數按一下刪除 (減號) 圖示並確認。

新建立的指令碼變數或者刪除現有的指令碼變數，甚至會反映在已經存在的配置中。

測試指令碼

在裝置上測試指令碼之前，請先在偵錯工具中對其進行快速測試執行，且無需儲存。

必要條件

- 對於 macOS，此功能需要適用於**macOS** 1.67 到Ivanti Neurons for MDM 支援之最新發行版本的 Mobile@Work。
- 對於 Windows，此功能需要 **適用於 Windows 指令碼和動作的 Ivanti Bridge 組態**。

程序

1. 前往**管理員 > 指令碼 > 所有指令碼**。
2. 在指令碼編輯程式中，新增或匯出指令碼。
3. 如果租戶有多個空間，可選擇其中一個空間。
4. 在「測試指令碼」區段中，選擇 **macOS** 或 **Windows** 做為平台。
5. 在**選擇裝置**文字欄位中，尋找並選擇要測試指令碼的裝置。 可依序號、使用者名稱、裝置名稱和作業系統版本來搜尋裝置。
6. 按一下**立即測試**。 如此一來，即可新增、編輯及刪除環境變數，且可使用該狀態測試指令碼 (甚至無需儲存已做的變更)。 對於 **Windows** 指令碼，畫面上會出現快顯，表示指令碼執行將開始，而且您可以在一段時間後從裝置詳細資料記錄索引標籤檢視狀態。
7. 按一下**儲存**。
8. 對於 macOS，等待指令碼被推送至裝置並執行。
9. 在「指令碼輸入」、「指令碼輸出」和「自訂屬性」等區段中檢視發佈的測試結果。 環境變數的預設值也會顯示。

驗證指令碼執行結果

若要檢視指令碼執行結果日誌：

1. 前往**裝置**。
2. 按一下裝置的名稱。
3. 按一下**日誌**索引標籤。

4. 在「指令碼執行」動作顯示列中，您可以驗證下列資訊：
    - 「詳細資料」欄位中的指令碼名稱。
    - 「指令碼」欄位中的指令碼執行狀態。
    - 「日期」欄位中的指令碼執行日期和時間。
    - 指令碼執行日誌 (裝置日誌 plist) - 按一下「動作」欄位中的眼睛圖示。

使用篩選來顯示**指令碼執行**列。 這些資料列的日誌包含標準輸出的輸出 (plist) 和指令碼的標準錯誤。

6. 使用篩選來顯示**指令碼執行結果處理**列。 這些資料列的日誌包含有關結果處理方式的詳細資料 (plist)。
    - 如果指令碼沒有相關聯的自訂屬性，則系統不會處理任何結果。 這類指令碼將不會顯示在已篩選資料列的清單中。
    - 如果指令碼有相關聯的自訂屬性，而且它們使用預期格式，則在結果中將會出現對應的自訂屬性，而且狀態將顯示為「成功」。 您可以在**屬性**索引標籤中驗證對應的自訂屬性和屬性值。
    - 如果指令碼有相關聯的自訂屬性，但它們未使用預期格式，則在結果中將不會出現對應的自訂屬性，而且狀態將顯示為「錯誤」。
    - 如果結果格式正確但在結果中並未收到所有的相關聯自訂屬性，則狀態將顯示為「錯誤」。
    - 如果指令碼變數與指令碼一起傳送，「指令碼執行結果處理」日誌中將會包含指令碼變數的詳細資料 (plist)。

相關主題：

- 適用於 macOS 的 Mobile@Work 指令碼配置
- 如何建立配置
- 適用於 Windows 指令碼和動作的 Ivanti Bridge 組態

12.9.2. 檔案

適用於：macOS 裝置

Ivanti Neurons for MDM 允許具有系統管理角色的使用者建立或上傳以及管理用於配置和分發到裝置的檔案。

程序

1. 前往**管理** > **指令碼和檔案** > **檔案**。
2. 在**檔案**頁面中，按一下 **+ 新增**。
3. 在**建立檔案**視窗中，輸入以下詳細資訊:
    1. 在**名稱**欄位中，輸入一個名稱以標識檔案。
    2. 在**描述**欄位中，輸入描述以闡明此檔案的目的。
    3. 在**上傳文檔**窗格中，按一下**選擇檔案**以上傳 .zip 檔案。 或者，您可以從裝置中拖放檔案。
4. 按一下**儲存**。
   新增的檔案將顯示在**檔案**頁面上。

編輯檔案

1. 前往**管理** > **指令碼和檔案** > **檔案**。
2. 選取要編輯的檔案，然後按一下**編輯**。
   編輯檔案視窗出現。
3. (選用) 您可以編輯**名稱**和**描述**欄位。
4. 在**上傳文檔**窗格中，按一下**選擇其他檔案**以上傳 .zip 檔案。 或者，您可以從裝置中拖放檔案。
5. 按一下**更新**。

刪除檔案

要刪除現有的**檔案**，請導覽到**管理** > **指令碼和檔案** > **檔案**，選擇要刪除的所有檔案，然後按一下 **+刪除**。

如果**檔案**與組態相關，Ivanti Neurons for MDM 將顯示**警告**訊息，**「無法刪除檔案，因為它正被其他原則使用。」**

12.10. 品牌化

本節包含以下各主題：

- 管理 > Apple 應用程式目錄 (品牌)
- 將 Android App Catalog 品牌化
- 管理 > Android 單一應用品牌化
- 將電子郵件範本品牌化
- 自助式入口網站
- 自助式入口網站 (品牌化)
- 多位使用者登入 (Webclip) 品牌
- 組織

12.10.1. 管理 > Apple 應用程式目錄 (品牌)

授權：Gold

您可以將 Apple {{App Catalog}} 品牌化，讓您 iPhone、iPad 及 Mac 裝置的一般使用者感覺很熟悉。 您可自訂 Apple app catalog 的下列項目：

- App 圖示 (PNG，360px 正方形)
- App 名稱
- App 橫幅影像 (PNG，360x64)
- 文字色彩

> 存取 Apple App Catalog 的模式有兩種：獨立 App Catalog 和整合 App Catalog。 獨立 App Catalog 適用於 iPhone、iPad 和 Mac 裝置。 整合式應用程式目錄適用於 iOS 和 Mac 裝置。

Apple App Catalog 品牌

在本頁面中所做的變更將會影響首頁畫面、登入過程畫面和 App 首頁畫面。 獨立 App Catalog 和整合 App Catalog 的程序類似。

程序

1. 在**將 Apple App Catalog 品牌化**頁面中，按一下**自訂** (右上角)。
2. 在 **App 圖示**區段中，將標誌檔案拖曳到虛線方塊中，或按一下**選擇檔案**，從檔案系統中進行選擇。 此 App 圖示會顯示在 iOS 首頁畫面
3. 在 **App 名稱**區段中，編輯 **App Catalog 名稱**文字，以變更顯示在登入過程畫面中的標籤。
4. 在首頁畫面橫幅上套用名稱和圖示。 如要變更自訂橫幅影像，請取消選取**在首頁畫面橫幅上套用名稱和圖示**選項。 這將顯示**應用程式橫幅影像**區段。
5. 若要變更 App 橫幅影像，請將新的橫幅影像檔案拖曳到虛線方塊中，或按一下**選擇檔案**，從檔案系統中進行選擇。 App 橫幅影像會出現在 App 首頁畫面的最上方列。
6. 在**文字色彩**區段中，按一下十六進位色彩代碼方塊，以挑選色彩或輸入十六進位色彩代碼，以指定文字和圖示。 這將會將文字套用至登入過程畫面、App 名稱、橫幅和動作按鈕。
7. 按一下**儲存變更**。

您輸入的 App Catalog 名稱會套用至 Android、iOS 和 macOS。

12.10.2. 將 Android App Catalog 品牌化

授權：Gold

您可將 Android {{App Catalog}} 品牌化，讓一般使用者對其外觀更有熟悉感。 您可自訂 Android 應用程式目錄的下列項目：

- 目錄標誌 (PNG，360x64)
- 目錄名稱
- 動作列色彩
- 捷徑圖示
- 捷徑名稱

Android App Catalog 品牌

程序

1. 在 **Android App Catalog 品牌化**畫面中，按一下**自訂** (右上角)。
2. 若要變更 App Catalog 標誌，請將標誌檔案拖曳到虛線方塊中，或按一下**選擇檔案**，從檔案系統中進行選擇。
3. 按一下**動作列色彩**欄位，以顯示調色盤，您可選擇其中的色彩或輸入偏好色彩的十六進位編號。
4. 編輯**應用程式目錄名稱**文字，以變更目錄的標籤。
5. 您輸入的 App Catalog 名稱會套用至 Android、iOS 和 macOS。
   若要變更「捷徑」圖示，請將圖示檔案拖曳到虛線方塊中，或按一下**選擇檔案**，從檔案系統中進行選擇。
6. 編輯**捷徑名稱**文字以變更 app 捷徑的標籤。
7. 按一下**儲存變更**。

12.10.3. 管理 > Android 單一應用品牌化

授權：Silver

您可將 Android 單一應用頁面品牌化，讓一般使用者對其外觀更有熟悉感。 您可以自訂下列項目：

- 橫幅標誌 (PNG，840x114) 或文字
- 橫幅邊界色彩
- 橫幅背景色彩
- 畫面背景色彩
- 畫面背景影像 (1280x800)
- 畫面背景格式

在 Android 單一應用畫面上建立品牌

程序

1. 導覽至**管理 > Android 單一應用**。
2. 在**單一應用模式品牌化**頁面中，按一下**建立品牌化**。
3. 在**名稱**欄位中，輸入單一應用模式品牌的名稱。
4. 如果您想關閉橫幅，請取消勾選**啟用頂端橫幅**。
5. 按一下**橫幅背景色彩**欄位，以顯示調色盤，您可選擇其中的色彩或輸入偏好色彩的十六進位編號。
6. 按一下**橫幅邊界色彩**欄位，以顯示調色盤，您可選擇其中的色彩或輸入偏好色彩的十六進位編號。
7. 選擇**影像/標誌**或**文字**，即可查看橫幅內容。
8. 如果您選擇**影像/標誌**，可拖曳影像檔或按一下**選擇檔案**進行選擇。
9. 如果您選擇**文字**，可輸入要在橫幅中顯示的文字。
10. 按一下**背景**索引標籤。
11. 按一下**背景色彩**欄位，以顯示調色盤，您可選擇其中的色彩或輸入偏好色彩的十六進位編號。
12. 若要變更背景影像：
13. a. 刪除預設圖片。
    b. 拖放偏好的影像或按一下**選擇檔案**來選擇一個檔案。
    c. 選擇偏好的版面配置。
    按一下**儲存變更**。
    所建立的單一應用模式品牌化會顯示在**單一應用模式品牌化**頁面中。 若要進一步編輯自訂品牌，請按一下**動作**欄位中的「編輯」圖示。 若要刪除自訂品牌，請按一下「刪除」圖示。 刪除自訂單一應用品牌化時，使用該品牌化的配置會還原為預設品牌化。

12.10.4. 將電子郵件範本品牌化

您可將一般使用者電子郵件邀請品牌化，讓一般使用者對其外觀更有熟悉感。 按一下**還原為預設設定**以清除自訂。

您也可以使用所有支援的語言來自訂下列電子郵件範本：

- **使用者邀請** - 邀請使用者連接裝置以存取 app 和配置。
- **密碼重設通知** - 系統會在本機帳戶密碼到期前 7 天和前 24 小時傳送提醒電子郵件。 此選項不適用於 LDAP 帳戶。
- **註冊確認** - 於使用者完成註冊後傳送的電子郵件。 您可使用它來感謝使用者註冊並為他們提供更多學習資源。
- **原則遵循通知** - 當裝置不符規則遵循時會傳送電子郵件。

本節包含以下各主題：

- 預覽及測試電子郵件範本
- 自訂訊息標題
- 自訂電子郵件範本
- 支援的電子郵件變數

預覽及測試電子郵件範本

您可以預覽及測試電子郵件範本。 這項測試可讓您將以範本為依據的電子郵件傳送給指定的電子郵件地址。

若要預覽及測試電子郵件範本：

1. 按一下**管理**。
2. 在「電子郵件範本」之下，按一下**使用者邀請**、**密碼重設通知**、**註冊確認**或**原則遵循通知**。
3. 針對您想預覽及測試的電子郵件範本，按一下相關聯的**預覽及測試**連結。
4. 在呈現的範本窗格中，加以檢視。
5. 指定要傳送測試電子郵件的目標測試電子郵件地址。
   如果您指定的電子郵件地址屬於目前的使用者，測試電子郵件就會替換掉大多數的電子郵件範本變數值，以更精準掌握使用者對這封電子郵件的體驗。 不過，測試電子郵件不會替換掉 Ivanti Neurons for MDM 在產生實際電子郵件邀請時產生的變數值。
6. 按一下**傳送測試電子郵件**。

自訂訊息標題

1. 按一下**管理**。
2. 按一下**電子郵件範本**。
3. 針對您要編輯的電子郵件範本，按一下與它相關聯的**編輯**圖示連結 (「動作」欄位下方)。
4. 針對**電子郵件顯示名稱**、**寄件者電子郵件地址**、**回覆電子郵件地址**，以及**設定 SMTP 電子郵件組態**，提供所需的新設定。
5. 如果您要自訂「寄件者」和「收件者」電子郵件地址，建議您允許 Email Relay Service，以確保您的電子郵件不會遭到電子郵件 SPAM 篩選服務封鎖。 如需更多資訊，請參閱本文件。
   按一下**儲存**。
6. 檢閱電子郵件範本的預覽畫面，然後按一下**儲存**。

使用 SMTP 組態

新增**設定 SMTP 電子郵件組態**，方便管理員針對輸出通知設定自己的電子郵件伺服器整合。

1. 前往**管理員 > 品牌 > 電子郵件設定**，然後啟用**設定 SMTP 電子郵件組態**選項。
2. 更新下列欄位:
    - SMTP 伺服器
    - SMTP 伺服器連接埠
    - 通訊協定
    - 使用者名稱
    - 密碼
3. 按一下**測試**以傳送測試郵件，**測試郵件**快顯畫面隨即顯示。
4. 輸入訊息的**收件者**名稱和**正文**，然後按一下**儲存**。

> 如果認證不正確，系統會顯示錯誤訊息。

5. 按一下**儲存**

下表摘要列出了「SMTP 組態」視窗中的欄位和說明:

欄位	描述
SMTP 伺服器	指定 Ivanti Neurons for MDM 伺服器要使用的 SMTP 伺服器的 IP 位址或完整主機名稱。
SMTP 伺服器連接埠	指定為 SMTP 伺服器設定的連接埠。
通訊協定	如果您要設定的 SMTP 伺服器是受保護伺服器，即表示其會使用 SMTPS 通訊協定，則選取 SMTPS 按鈕。 否則，請選取 SMTP。
使用者名稱	輸入 SMTP 驗證所需的使用者名稱。
密碼	輸入 SMTP 驗證所需的密碼。

自訂電子郵件範本

1. 選擇**管理 > 品牌化 > 電子郵件範本**。
2. 選擇要編輯的範本，**使用者邀請**、**密碼重設通知**、**註冊確認**或**原則遵循通知**。
3. 按一下您要自訂的電子郵件範本旁的編輯鉛筆圖示。

4. 視需要編輯主旨行。
5. 在內文窗格中，編輯含有 HTML 元素的電子郵件範本，以自訂訊息內容。



您可以使用電子郵件內文右側顯示的變數。 請參閱[支援的電子郵件變數](#)。

6. 按一下**預覽**，即可預覽電子郵件範本；您可重複作業直到滿意為止。
7. 當您決定要儲存範本，請按一下**預覽**。 隨即呈現預覽，並提供儲存功能。



8. 如果您滿意預覽成果，請按一下**儲存**。

自訂使用者邀請中的允許清單和封鎖清單內容

當您在**使用者邀請**中自訂使用者邀請電子郵件範本時，系統會提供一份允許的 HTML 標記和屬性允許清單。 系統也會提供一份使用者邀請中不允許使用的字串封鎖清單，以防止跨網站指令碼 (XSS) 漏洞。

您只能在邀請電子郵件中，使用允許清單提列的標記和屬性。 下表列出允許使用的允許清單標記和對應屬性。

> 有些「允許清單」標籤 (例如: <big>) 不應具有任何「允許清單」屬性，因此顯示空白。

列入允許清單的標記	列入允許清單的屬性
<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"]
	[]

列入允許清單的標記	列入允許清單的屬性
	[]
<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"]

下列為自訂使用者邀請中不允許使用的字串封鎖清單。

- Script, @import, ¼script¾, script>, <script, <script>, </script>, javascript, alert(, moz-binding, expression(, +ADw-SCRIPT+AD4-,+ADw-/SCRIPT+AD4-, xml:base
- 特殊字元和搜尋 Javascript 或指令碼
- 包含 "url=" 的中繼內容屬性 (區分大小寫)
- 不含 .svg. 的 img src
- 包含 "\00" 的屬性值

如果使用者邀請的 HTML 內容中有使用上述任何列入封鎖清單的字串，當您按一下**預覽**時就會顯示錯誤訊息。 這則錯誤訊息會列出使用者邀請中不允許出現的 HTML 內容。 編輯並移除不允許出現的 HTML 內容，然後按一下**預覽**繼續。

> 如果編輯的範本包含列入封鎖清單的 HTML 內容，您就無法儲存該範本。

支援的電子郵件變數

Ivanti Neurons for MDM 提供各種變數，可讓您自訂電子郵件範本。

使用者邀請變數

變數	描述
$	使用者啟用 URL - 這是包圍$文字的超連結。
$	叢集註冊 URL - 在預設範本中找不到，但可 (透過 $變數) 間接參照。
$	商品品牌名稱 – 這在預設範本的頁首中被定義為 <title> 標籤。
$	公司標誌URL - 這是預設範本中的一個影像 - 它指向 MobileIron CDN 中的影像 更新**使用者品牌**設定會變更 **$** 引用的值。
${message:$	註冊使用者裝置標題。
${message:$ }	電子郵件邀請標題。
${message:$ }	驗證使用者在其裝置上。
${message:$ }	電子郵件邀請開始使用文字。
${message:$ }	登入與註冊指示。
${message:$ }	推送到裝置資訊的電子郵件和 app 。
${message:$ }	若使用者不在其裝置上的註冊資訊，其中包含叢集註冊 URL。
${message:$ }	含有公司網站標籤的電子郵件邀請頁尾。
$	公司網站標籤 - 在預設範本中找不到，但可 (透過 $ 變數)間接參照。

密碼到期通知變數

變數	描述
$	密碼重設 URL。
$	商品品牌名稱 – 這在預設範本的頁首中被定義為 <title> 標籤。
$	公司標誌URL - 這是預設範本中的一個影像 - 它指向 MobileIron CDN 中的影像 更新**使用者品牌**設定會變更 **$** 引用的值。
${message:$}	密碼到期通知標題。
${message:$}	密碼到期通知簡介段落。
${message:$}	密碼重設 URL 名稱。
${message:$}	含有公司網站標籤的電子郵件邀請頁尾。
$	公司網站標籤 - 在預設範本中找不到，但可 (透過 $ 變數)間接參照。

註冊確認變數

變數	描述
$	商品品牌名稱 – 這在預設範本的頁首中被定義為 <title> 標籤。
$	公司標誌URL - 這是預設範本中的一個影像 - 它指向 MobileIron CDN 中的影像 更新**使用者品牌**設定會變更 **$** 引用的值。
${message:$}	註冊確認標題。
${message:$}	註冊確認簡介段落。

原則與規則遵循

變數	描述
$	此變數將被取代成在原則內傳送電子郵件合規動作中主旨行裡輸入的內容。
$	此變數將被取代成在原則內傳送電子郵件合規動作中訊息部分裡輸入的內容。
$	商品品牌名稱 – 這在預設範本的頁首中被定義為 <title> 標籤。
$	公司標誌URL - 這是預設範本中的一個影像 - 它指向 MobileIron CDN 中的影像 更新**使用者品牌**設定會變更 **$** 引用的值。
${message:$}	含有公司網站標籤的電子郵件邀請頁尾。
$	公司網站標籤 - 在預設範本中找不到，但可 (透過 $ 變數)間接參照。

自訂使用者屬性變數

在下列情況下，管理員可以將自訂使用者屬性作為自訂電子郵件範本中的電子郵件變數：

- **管理 > 屬性**頁面中已存在自訂使用者屬性。
- 管理員已將自訂使用者屬性指派給使用者，其中含有要提供給每個使用者的自訂使用者屬性值。

12.10.5. 自助式入口網站

註冊邀請中包含自助式入口網站的連結。 一般使用者可以使用此入口網站進行下列作業：

- 鎖定
- 解除鎖定
- 檢視位置 (若已在**隱私組態**中啟用)
- 抹除
- 淘汰
- 變更帳戶資訊 (名稱、密碼、電子郵件地址)
- 強制簽入
- 新增加密和簽署憑證

若要註冊其他裝置，一般使用者可以按一下自助式入口網站中顯示的註冊入口網站連結。

如果使用者遺失自助式入口網站的 URL，請傳送以下 URL 給他們 **https://mydevices.mobileiron.com/user/login.html**。 若是 iOS 使用者，請考慮建立自助式入口網站的 **Web Clip 配置**。

上傳簽署和加密憑證

您可以允許一般使用者在使用者提供的憑證配置中，使用自助式入口網站上傳他們的電子郵件簽署和加密憑證。 此設定可以使用使用者提供的憑證配置來進行設定。 當設定好時，一般使用者可以上傳他們的電子郵件簽署和加密憑證。

1. 在**我的憑證**索引標籤中，按一下**新增憑證**。 **新增憑證**視窗隨即顯示。
2. 更新下列欄位：

欄位名稱	描述
憑證類型	選擇要上傳的憑證類型。 選項包括： • **加密憑證** • **簽署憑證** 這些選項是從 Ivanti Neurons for MDM 管理入口網站建立的。 如需詳細資訊，請參閱**身份識別憑證配置**。
待上傳憑證	按一下**選擇檔案**以選擇要上傳的憑證檔案。 請確認檔案的格式為 PKCS12。
密碼	輸入用於檔案的密碼。

3. 按一下**上傳**。

上傳之後，您可以在顯示下列詳細資料的表格中檢視憑證清單。

欄位名稱	描述
憑證名稱	指定憑證的類型為**加密**或**簽署**。
核發機構	核發之憑證的詳細資料。
上傳時間	上傳憑證的日期。
有效日期 動作	憑證的到期日期。 您可執行下列動作： • **編輯憑證** - 編輯憑證詳細資料。 • **清除私密金鑰** – 將私密金鑰從憑證套件 (PKCS#12) 中刪除。 • **刪除憑證** - 將憑證從 Ivanti Neurons for MDM 伺服器刪除。

當使用者上傳憑證配置時，伺服器會重新推送正在使用該憑證的配置。

> 由使用者刪除和清除私密金鑰時，並不會重新推送配置。

如需更多資訊，請參閱**自助式入口網站品牌化**。

12.10.6. 自助式入口網站 (品牌化)

授權： Silver

您可以使用組織標誌自訂自助式入口網站。 如果您不新增自己的標誌，自助式入口網站就會顯示預設的服務標誌。

將自助式入口品牌化

程序

1. 在「自助式入口網站品牌」畫面中，按一下**自訂** (右上角)。
2. 將標誌檔案 (PNG，182x34) 拖曳到虛線方塊中，或按一下**選擇檔案**，從檔案系統中進行選擇。
3. 按一下**儲存變更**。

12.10.7. 多位使用者登入 (Webclip) 品牌

您可以新增標題和 Webclip 圖示，以自訂 iOS 的多重使用者安全登入。

程序

1. 前往**管理 > 多重使用者登入 (Webclip)**。
2. 在「多重使用者登入 (Webclip)」畫面中，按一下**自訂**。
3. 將標誌檔案拖曳到虛線方塊中，或按一下**選擇檔案**，從檔案系統中進行選擇。
4. 若要變更標籤，請編輯**安全登入**文字。
5. 若要變更 Webclip，請將 Webclip 檔案拖曳到虛線方塊中，或按一下**選擇檔案**，從檔案系統中進行選擇。
6. 預覽更新內容，然後按一下**儲存變更**。

若是 iPhone 和 iPod touch 裝置，請建立 120 x 120 畫素或 60 x 60 畫素 (標準解析度) 的圖示。

若是 iPad 裝置，請建立 152 x 152 畫素或 76 x 76 畫素 (標準解析度) 的圖示。

如需更多資訊，請參閱 **iOS 多使用者安全登入**。

12.10.8. 組織

您可以為組織提供品牌名稱，或透過在每個主題中包含租用戶特定的識別碼 (例如客戶名稱) 來個性化系統警報電子郵件主題行。 如果不更新組織名稱，「組織」螢幕將顯示預設值。

組織品牌化

程序

1. 在「組織」螢幕的**名稱**欄位中輸入所需名稱。
2. 要新增字首，可按一下**編輯**並啟用選項**在所有系統生成的電子郵件中新增組織名稱首碼，例如許可證到期**。
3. 按一下**儲存**以套用變更。

12.11. 新增非 iOS 裝置管理

授權：Gold

您目前使用的 Ivanti Neurons for MDM 版本最適合搭配 iOS 裝置。 本節說明如何切換為允許管理非 iOS 裝置。 切換以後，您就可以管理下列裝置：

- Android 5.0 或支援的更新版本
- Windows 10+

切換為納入管理非 iOS 裝置是無法取消的。

若要切換為納入管理非 iOS 裝置：

1. 按一下**管理 > 允許的平台**。
2. 按一下**允許所有平台**按鈕。
3. 勾選**本人瞭解此動作是無法取消的**，以確認您知道與瞭解此作業無法取消。
4. 按一下**允許所有平台**按鈕。

13. 套件

本節包含以下各主題：

- 升級
- Secure UEM 和 Secure UEM Premium 套件
- 舊版銅級、銀級與金級套件
  - 銀級
  - 金級
  - 白金級
- 用於預覽或者測試的沙盒

Secure UEM 和 Secure UEM Premium 套件

Secure UEM 和 Secure UEM Premium 套件提供下列功能:

	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)		✓

這些套件隨時可能有所變更。 您應聯絡 **Ivanti 銷售代表**以確認目前的方案。

舊版銅級、銀級與金級套件

本節說明舊版銅級、銀級與金級套件的相關資訊。 該封裝已發展成 **Secure UEM 和 Secure UEM Premium** 方案。

銅級

Bronze 套件中提供 Ivanti Neurons for MDM 基本功能。 您可藉由以下方式擴充 Bronze 套件：

- 新增更多裝置
- 新增 Silver
- 新增 Gold
- 新增 Platinum

這些新增項目可以將您的行動解決方案，擴充至基本裝置配置以外。

如果管理員有意幫他們的租戶啟用一或多個依預設停用的隨選即用功能，他們可以聯絡支援中心。

銀級

升級到 Silver 將新增下列功能：

- **LDAP 和 Connector：**支援將公司目錄和憑證授權單位新增至 Ivanti Neurons for MDM。
- **Sentry：**支援控制電子郵件存取控制。
- **空間**：支援將裝置指派給不同管理員來管理 (委派管理)。
- **受監管模式**：裝置層級支援更精細的配置，包括單一 App 模式。
- **自助式入口網站品牌**：可在自助式入口網站中使用您的標誌。
- **憑證授權單位：**使用 Ivanti Neurons for MDM 做為憑證授權單位。
- **無訊息 app 安裝/解除安裝**：可自動從行動電話裝置部署與移除 app。
- **App 允許清單/封鎖清單/必要 app：**監控並控制要在裝置上安裝哪些 app。
- **Web 內容篩選：**套用網站允許清單/封鎖清單原則至所有 Web 瀏覽器。
- **Apple 專用功能**：啟用/限制 AirPlay、 AirDrop、iOS 桌布發佈與 Apple TV。
- **Open-in 管理**：控制行動電話 app 可以開啟哪些企業內容。
- **Apple Apps and Books**：將行動電話 app 授權發佈給裝置，並在裝置淘汰時，取回並重新指派這些授權。
- **Android enterprise (Android for Work) 支援**
- **Device Enrollment：**可讓客戶大量購買裝置，並於啟動期間自動在 MDM 中註冊 Apple 裝置。
- **個別 App 配置：**可大量部署已配置的行動電話 app，且一般使用者幾乎可以不進行任何動作。
- **第三方個別 App VPN：**VPN 安全性現在具即時和隱藏的特性，而且專門針對行動 app 量身打造。
- **原則階層式動作**
- App 發佈篩選
- **稽核追蹤**
- **Android 單一應用模式**：支援將 Android 裝置配置為可在單一應用模式中運作。
- **Android 單一應用品牌：**變更裝置在單一應用模式中運作時，單一應用畫面顯示的背景和橫幅。
- **使用 Graph API 的 Office 365 預防資料遺失 (DLP)**：透過 Graph API 強制執行 Office 365 app 的 DLP 控制。

金級

升級至 Gold 將新增 Silver 提供的功能與下列功能：

- **單一登入**：使用者只需驗證一次，即可自動登入其他的企業行動電話 app。
- **iOS 和 Android App Catalog 自訂品牌：**在 App Catalog 中顯示貴公司的標誌。
- **增加內容限制**：50 個檔案，每個可達 25 MB
- **iOS 版 AppConnect：**保護並設定啟用 AppConnect 的 app。
- **iOS 版 AppTunnel：**保護可存取企業資源的 app。
- **iOS 版 Docs@Work：**可讓使用者檢視、儲存並共享文件。
- **iOS 8 認證式單一登入**

- **iOS 8 iBook/ePub 管理**
- **macOS 支援**
- **使用者品牌**
- **Mobile Application Management (MAM) 搭配 AppConnect**
- **衍生認證**
- **Windows 10 (包括 Bridge) 支援**

白金級

升級至 Platinum 將新增 Gold 提供的功能與下列功能：

- **Tunnel：**配置特定 app 的企業資料存取權。
- **Help@Work**
- **監控**
- **ServiceConnect (ServiceNow、Splunk)**

用於預覽或者測試的沙盒

Ivanti Neurons for MDM 客戶若有購買 **Premium Plus** 支援，即可取得沙箱租用戶，以預覽並測試新版本後再開始生產。

13.1. 升級

本節包含以下各主題：

- 升級授權
- 要求升級
- 從舊版本升級

升級授權

基本功能透過 Bronze 套件提供。 您可藉由以下方式擴充 Bronze 套件：

- 新增更多裝置
- 新增 Silver
- 新增 Gold
- 新增 Platinum

這些新增可將您的行動電話解決方案擴充為擁有比基本裝置配置更多的功能。

要求升級

程序

1. 從管理下拉式功能表中，選擇**升級選項**。
2. 按一下**要求升級 / 新增裝置** (右上角)。
3. 選擇您要新增的項目，並輸入您的電話號碼。

相關代表即會在 24 小時內聯絡您，並告知詳細資訊。

從舊版本升級

從舊版本升級時，不會保存**編輯 Device Enrollment 描述檔**頁面的設定。 請先記下您的選項設定，再進行升級。

- 如果您在升級前已啟用**略過登入 Apple ID 和 iCloud**，在升級後就會啟用**略過 Apple Pay 設定**。
- 如果您在升級前已啟用**略過輸入密碼**，在升級後就會啟用**略過 Touch ID** 以及**略過 Apple Pay 設定**。

程序

1. 升級完成後，返回**編輯 Device Enrollment 描述檔**頁面，對 Device Enrollment 描述檔進行編輯，以還原所需的設定。
2. 按一下**儲存**。

升級之後，有幾個配置設定會受到影響。

- 將推廣選項設定為**關閉**。
  將安裝設定設為**否**。
  不再選取**不要顯示於 App Catalog** 選項。
  Android Samsung Knox 上的無訊息自動安裝已設為 False。

iOS 管理旗幟已設定為：

- 備份至 iCloud。

- 於取消註冊時移除。

您可以個別為每一個 app 選擇這些 iOS 管理旗幟設定。

App 設定：

- App 設定現在稱為配置。
- 所有其他 app 設定會保持與升級前相同。

如需更多資訊，請參閱套件。

14. 裝置授權

Ivanti Neurons for MDM 裝置授權定義了您可註冊的裝置數量、可配置並發佈到裝置的內容數量，以及可供使用的功能。 當您達到裝置限制時，「管理」頁面就會顯示一個紅色的三角形。 當您達到內容限制時，服務就不會再讓您新增更多項目，並會顯示一則訊息，指出您已達到限制。

14.1. 租戶停權

若租用戶是搭配評估授權或生產授權使用，Ivanti Neurons for MDM 可能會暫停對該租用戶的存取權。 評估期間已過或已超過允許的使用量時，就可能會停用評估授權。 訂閱期間已過或已超過允許的使用量時，就可能會停用實際授權。 更新授權或購買額外授權 (適用於超額情況) 之後，Ivanti Neurons for MDM 就會恢復暫停的租用戶。

當租戶授權被停用時，會發生下列情況：

- 現有的已註冊裝置仍可繼續正常使用。
- 管理員無法登入管理入口網站。
- 新的裝置無法註冊。
- 該租戶的 API 存取遭到封鎖。
- 使用者可以繼續存取自助式入口網站。

租戶停權動作與錯誤訊息

停權動作	錯誤	顯示的錯誤訊息	定位
一般客戶的整合 API 存取遭到封鎖。	API 呼叫失敗。	存取遭拒。 您的評估授權已過期。 請更新您的授權以重新啟用 API 存取。 請聯絡您的系統管理員，以取得詳細資料。	API 錯誤 401。
系統會封鎖新裝置的註冊。	註冊畫面會顯示錯誤訊息。	無法註冊您的裝置。 您的系統授權已過期。 請聯絡您的系統管理員，以取得詳細資料。 之前註冊的裝置可持續正常運作。	在密碼驗證之後出現。
管理員無法登入管理入口網站。	登入畫面會顯示錯誤訊息。	無法登入。 您的授權已過期。 請更新您的授權，以重新取得管理入口網站的存取權，並註冊新的裝置。 之前已登記的裝置將繼續正常運作。 請聯絡您的銷售代表，以更新授權。 請注意，管理密碼一年 (365 天) 後失效。	在密碼驗證之後出現。

15. 開啟支援票證

請瀏覽 **Ivanti 支援入口網站**開啟一個支援票證。

16. 第三方屬性

Ivanti Neurons for MDM 包含由第三方開發的元件。 您可以在此處檢視清單。

17. Apps@Work

從 Ivanti Neurons for MDM 版本 83 開始，可以從 Go 應用程式轉換為 Apps@Work 原生體驗。 對於新建租戶，依預設不將 Apps@work Webclip 組態散發給透過 iReg 或用戶端安裝的 iOS 裝置。 管理員必須手動將 webclip 組態散發給透過 iReg 或用戶端註冊的裝置。 注意以下幾點:

Ivanti Neurons for MDM**管理入口網站**:

- 依預設，只有新租戶才能獲得已散發到 iOS 裝置的「原生用戶端應用程式目錄」組態。
- 對於現有租戶，依預設，不散發 Apps@Work 原生應用程式。
- 管理員必須將「原生用戶端應用程式目錄」組態推送到裝置，使 Apps@Work 可用於「原生應用程式商店」體驗中。

用戶端:

- Go 應用程式現在顯示 Apps@Work 的索引標籤。
- 「原生用戶端應用程式目錄」組態具有「原生用戶端應用程式目錄身分識別」憑證和 App Station 身分識別憑證。 Ivanti Neurons for MDM 透過「原生用戶端應用程式目錄」組態推送憑證。

Apps@Work 功能

Apps@Work 索引標籤具有下列功能:

- 從 Go 應用程式存取 Apps@Work 索引標籤
- 搜尋
- 安裝應用程式 - 按鈕狀態
- 精選應用程式和橫幅
- 應用程式更新通知
- 應用程式更新通知

從 Go 應用程式存取 Apps@Work 索引標籤

- 在 Go app 中為 Apps@Work 新增了一個新索引標籤。
- 兩個預設索引標籤可用於 Apps@Work–所有應用程式和類別中。
- 所有應用程式索引標籤按字母順序列出所有應用程式。
- 類別索引標籤僅顯示其中含有任何應用程式的類別。
- 每個類別都顯示其中存在的應用程式數量。
- 類別下的 MyApps 是清單項目，其中包含所有已安裝的應用程式。 MyApps 將始終為第一個類別，其餘類別按字母順序列出。
- 未安裝應用程式時，MyApps 列表顯示「無」。
- 按一下某個類別後，就會列出專屬該類別的所有應用程式及「安裝」選項。 精靈可讓您個別安裝每個應用程式，也可以按一下「全部安裝」，以安裝該類別中的所有應用程式。 系統將詢問是否允許安裝每個應用程式。

搜尋

- 點擊搜尋 (透鏡) 圖示搜尋以下內容:
  - 新版本 – 搜尋列中未鍵入任何文字時顯示新發佈的應用程式清單

- 鍵入任何文字，搜尋欄位將動態預測並顯示相符的應用程式。
- 搜尋結果計數顯示為子標題
- 可以點擊「安裝」按鈕安裝應用程式，無需瀏覽至詳細資訊頁面。

安裝應用程式 - 按鈕狀態

- 由於應用程式安裝需要伺服器處理要求並將應用程式下推至裝置，因此安裝按鈕不會即時顯示進度
- 安裝按鈕將依序按「安裝」>「已要求」>「已安裝」變更狀態。
- 警示訊息第一次出現，表示已要求安裝。
- 點擊「已要求」按鈕後也會出現警示。
- 已安裝狀態並非按鈕。

精選應用程式和橫幅

- 「精選」索引標籤根據管理員組態顯示。
- 「精選」索引標籤是無可用更新時的預設登陸頁面。
- 「精選應用程式橫幅」在橫幅中顯示一個應用程式。
- 「精選應用程式」包含所有精選應用程式的清單。

應用程式更新通知

- 有任何應用程式更新可用時，Go 即傳送通知。 通知不顯示應用程式名稱。
- 若點擊應用程式更新通知，將被重新導向至 Apps@Work 中的「所有應用程式」頁面。
- 在 Go 應用程式中，Apps@Work 索引標籤圖示顯示有擱置中更新的應用程式數量的徽章計數。
- 在 Apps@Work 索引標籤中，「可用更新」子區段出現在「所有應用程式」索引標籤下，並顯示可更新應用程式的計數。
- 需要更新的每個應用程式都顯示一個紅點圖示。

設定 – 我的裝置

- 「我的裝置」索引標籤現在已移至「設定」下。
- 若點擊應用程式更新通知，將被重新導向至 Apps@Work 中的「所有應用程式」頁面。
- 在 Go 應用程式中，Apps@Work 索引標籤圖示顯示有擱置中更新的應用程式數量的徽章計數。
- 在 Apps@Work 索引標籤中，「可用更新」子區段出現在「所有應用程式」索引標籤下，並顯示可更新應用程式的計數。
- 需要更新的每個應用程式都顯示一個紅點圖示。

18. 在 Ivanti Neurons for MDM 和 SCEP 伺服器之間啟用 Kerberos 驗證

可以使用 Kerberos 驗證在 Ivanti Neurons for MDM 和 SCEP 之間進行通訊。 以下章節討論如何在 SCEP 伺服器和 Ivanti Neurons for MDM 上啟用 Kerberos 驗證。

> 此功能將在 Ivanti Neurons for MDM 連接器 93 版本可用時運作。

預先設定步驟

1. 檢查 SCEP 伺服器上 SCEP 服務正在使用哪個服務帳戶。
2. 在 SCEP 伺服器上，檢查服務帳戶是否為本機 IIS_USRS 群組的成員。
3. 在正在佈建的 CA 伺服器憑證範本上，檢查服務帳戶是否具有註冊權限。

設定 Windows 伺服器

1. 在網域控制器上執行以下指令:
   setspn -s http/<SCEP-SERVER-FQDN> <domain>\<service account>
2. 在 **Active Directory 使用者和電腦**中，按一下服務帳戶的**委派**索引標籤:
   1. 在**信任此使用者並僅將其委派給指定服務**下，選取**僅限使用 Kerberos**。
   2. 按一下**新增**，然後新增 SCEP 伺服器名稱。
   3. 選取 HTTP 服務。
   4. 按一下**確定**。
3. 在 IIS 伺服器上執行下列操作，確保使用應用程式集區憑證解密 Kerberos 票證:
   1. 檢查 SCEP 應用程式集區是否在先前驗證過的服務帳戶下執行。
   2. 若要啟用 useAppPoolCredentials，請前往 Microsoft SCEP 管理員 (mscep_admin) 或 Microsoft SCEP (mscep) 網頁上，選取**組態編輯器 > System.webServer > 安全性 > 驗證 > Windows 驗證**，然後將值設定為 useAppPoolCredentials=True。
4. 選取**驗證 > 匿名驗證**，然後按一下**停用**，即可在 Microsoft SCEP 管理員網頁 (mscep_admin) 上停用**匿名驗證**。
5. 在 Windows 驗證進階設定中停用核心模式驗證。

> 務必使用**協商**作為身分驗證服務中的第一個選項。

6. 在 Windows 驗證進階設定網頁中停用核心模式驗證。
7. 重新啟動 IIS 服務。

設定 Kerberos

本節討論如何在 Ivanti Neurons for MDM 伺服器上設定 Kerberos。

在 Ivanti Neurons for MDM 中進行 Kerberos 設定

瀏覽至**管理員 > 基礎架構 > Kerberos**，按表中所示輸入以下設定:

UI 部分	選擇
Active Directory 的 Kerberos 領域	IVANTI.COM
對應的金鑰分發中心 (KDC) 伺服器	kdc.ivanti.com
服務使用者認證	使用者@領域 例如: serviceuser@IVANTI.COM
用於與 Microsoft AD 憑證服務進行出站通訊的網域 (主機名稱不區分大小寫，且必須以 .ivanti.com 或 .IVANTI.COM 結尾) SCEP 或 NDES 伺服器: 也可以使用主機名稱，例如: ndes.ivanti.com 或 scep.ivanti.com	

針對現有憑證授權單位的 Microsoft SCEP 憑證註冊組態啟用 Kerberos 驗證

執行下列步驟，針對現有憑證授權單位啟用 Kerberos 驗證:

1. 在 Ivanti Neurons for MDM 中，選取**管理員 > 基礎架構 > 憑證管理**。
2. 使用**外部**選項，選取憑證授權單位類型。

> 這些外部憑證授權單位類型應表示為 Microsoft。

3. 從**動作**下拉式功能表中，選取**編輯**。
4. 在**編輯外部 CA** 視窗中，選取**偏好 Kerberos 驗證**核取方塊以啟用 Kerberos 驗證。

針對新憑證授權單位的 Microsoft SCEP 憑證註冊組態啟用 Kerberos 驗證

執行下列步驟，針對新憑證授權單位啟用 Kerberos 驗證:

1. 在 Ivanti Neurons for MDM 中，選取**管理員 > 基礎架構 > 憑證管理**。
2. 選取 **+新增**選項。
3. 在**新增憑證授權單位**視窗中，選取**連線至本地 SCEP 憑證授權單位**選項。
4. 按一下繼續。
5. 在**新增外部憑證授權單位**視窗中，執行下列步驟:
    1. 從**憑證授權單位類型**下拉式功能表中選取 **Microsoft** 選項。
    2. 選取**偏好 Kerberos 驗證**核取方塊以啟用 Kerberos 驗證。
    3. 填寫所有的必填欄位。
    4. 按一下**完成**。

19. Ivanti Neurons for MDM 127 管理員指南

2026 年 9 月

Ivanti Neurons for MDM 是確保行動安全的新型方式，在高度可擴充、安全且方便更新的基礎架構中提供統一端點管理 (UEM) 解決方案，該基礎架構支援全球數百萬部裝置。

{{如果您的語言不提供}}

新功能摘要

以 PDF 檢視

影片

20. Welcome

21. Welcome CSH

22. Windows Update 管理

以管理員身分，可以使用「Windows 更新管理」檢視及批准要更新的 Windows 裝置所回報的更新。 您可使用此功能來防止在裝置上安裝不必要或未經測試的更新。

「更新管理」功能要求透過啟用了**需要更新核准**選項的**軟體更新**組態設定裝置。 唯有將此配置套月到裝置上，裝置才會報告待安裝的更新並等待核准。

管理更新

1. 前往**管理員 > Windows 更新**。 頁面上會顯示更新的下列詳細資料。
   建立日期：建立更新的日期。**標題**：描述更新類型與知識庫文章編號。

> 按一下更新時，隨即顯示此描述。

分類: 將更新類型分為以下類別之一:

- 重要更新
- 定義更新
- 驅動程式更新
- 安全性更新
- 更新
- 升級
- 更新彙總

發佈：針對更新所執行的發佈。 例如，當更新要發佈給所有裝置時，它便會顯示**所有**。

> 如果更新要發佈給特定數目的群組，它便會顯示發佈計數。 例如，只針對 3 個群組執行發佈，則它會顯示 3。

2. 此外，您可以檢視更新是否已發佈至必要的裝置。 下列欄位的數字表示存在於不同更新類別中的裝置數目:
   - 合格的裝置
   - 已安裝的裝置
   - 安裝失敗的裝置
   - 重新啟動擱置中裝置

當您按一下任何數字時，您將被導向至「裝置」頁面中的篩選檢視以瞭解更新狀態，並執行必要動作。
檢閱更新，然後按一下更新的勾選方塊，藉此選擇您想發佈到裝置上的更新。

3. 在**動作**下，按一下**設定發佈**。
4. 在**發佈 Windows 更新**視窗中，選擇下列發佈選項之一：
   所有裝置：發佈更新到所有裝置。
   無裝置：暫停發佈更新到裝置。**自訂**：發佈更新到指定裝置群組。
5. 按一下**儲存**。

搜尋與篩選更新

您可以根據以下條件搜尋與篩選更新：

- 知識庫文章 ID
- 設定的發佈

根據知識庫文章 ID 進行篩選：

1. 在 **Windows 更新管理**頁面中，請在快速搜尋欄位中鍵入知識庫 ID (只能在搜尋欄中鍵入數字)。
   範例：若是 KB4056892，請輸入 4056892。 頁面上隨即顯示符合搜尋條件的更新。

> 您可以按一下**支援**和**更多資訊**連結，藉此進一步搜尋其他資訊。 Microsoft 網頁的**支援**連結針對更新提供產品支援資訊，Microsoft 網頁的**更多資訊**連結則針對更新顯示更多資訊，例如知識庫文章。

根據所設定的發佈進行篩選：

在 **Windows 更新管理**頁面中，根據設定的發佈選取下列其中一個選項:

- **所有**：顯示所有更新。
- **已設定**：顯示要發佈到裝置上的更新清單。
- **未設定**：顯示在發佈中未指定的更新清單。

> 「已設定」和「未設定」的篩選器根據所執行的發佈，發佈也可以是**無**。

檢視裝置的更新

若要檢視裝置特有的詳細更新資訊：

1. 前往**裝置 > 裝置**。
2. 按一下裝置名稱，以檢視詳細資料頁面。
3. 前往**更新**索引標籤。 隨即顯示擱置中 (管理員已核准但尚未回報已在裝置上安裝)、失敗與已安裝的裝置更新。

> 您也可以透「儀表板」下的「通知」頁面，查看是否有新的 Windows 更新可用。 通知內容包含通知的建立日期、可用通知數目，以及通知目的。 在管理入口網站的右上角也可以看到 Windows 更新通知。