ivanti

NMDM Admin Guide ENGB

ivanti

CONTENTS

1. **About Ivanti Neurons for MDM** **9**
2. **What's New - 127** **10**
3. **Videos** **14**
4. **Getting Started** **17**
   - 4.1. Configuring macOS devices 24
   - 4.2. Configuring and using registration confirmation emails 27
   - 4.3. Configuring and using policy compliance notification emails 28
   - 4.4. On-demand features 29
   - 4.5. Preparing for Android Enterprise device support 32
5. **Dashboard** **33**
   - 5.1. Working with Widgets 34
   - 5.2. App Insights 40
   - 5.3. Using Scheduled Reports 44
   - 5.4. Using Custom Reports 51
6. **Users** **59**
   - 6.1. Adding Users 60
   - 6.2. User Groups 64
   - 6.3. User Settings 68
   - 6.4. User Branding 79
   - 6.5. User Enrollment with Apple Business Manager 80
   - 6.6. User Licences 88
   - 6.7. Managing Users 89
     - 6.7.1. Adding an API user for Cisco ISE operations 90
     - 6.7.2. Assigning Roles to Users 91
     - 6.7.3. User Roles 93
     - 6.7.4. Finding and Filtering Users 96
     - 6.7.5. Assigning Users to User Groups 99
     - 6.7.6. Inviting Users 100
     - 6.7.7. Enabling and Disabling Users 101
     - 6.7.8. Managing Multiple Administrator Logins 103
     - 6.7.9. Changing a Password 104
     - 6.7.10. Sending a Message 106
     - 6.7.11. Removing Users from User Groups 108
     - 6.7.12. Deleting a User 109
     - 6.7.13. Exporting Users 110
     - 6.7.14. Assigning Custom Attributes to Users 111
     - 6.7.15. Removing Custom Attributes from Users 112
     - 6.7.16. Changing the User Locale 113
     - 6.7.17. Editing a Username 114
     - 6.7.18. Opting Out of Location Data Collection 115
     - 6.7.19. Timeout Information 116
     - 6.7.20. Opting Out of System Usage Analytics 117
     - 6.7.21. Device Registration by PIN Generation 118
7. **Devices** **119**
   - 7.1. Getting Started with Devices 120
   - 7.2. Device Groups 133
   - 7.3. Unmanaged Devices 139
   - 7.4. App Inventory 140
   - 7.5. Managing Devices 143
     - 7.5.1. Deploying Apple Devices 145
     - 7.5.2. Deploying Windows devices 153
     - 7.5.3. Setup Apple Remote Desktop on macOS devices 157
     - 7.5.4. Device Registration (iOS, macOS, and Android) 158
     - 7.5.5. Device Registration (Windows 10+ PC and Microsoft HoloLens 2) 162
     - 7.5.6. Local Admin Password Solution (LAPS) 165
     - 7.5.7. Provisioning Package Enrolment with PIN 167
     - 7.5.8. Using Bulk Enrollment for Windows devices 170
       - 7.5.8.1. Ivanti Bulk Enrollment 171
     - 7.5.9. Changing Passcode Settings 173

7.5.10. Changing the Device Name ... 174
7.5.11. Finding and Filtering Devices ... 175
7.5.12. Using Device Owner ... 177
7.5.13. Managed Device with Work Profile ... 184
7.5.14. Using Bulk Enrolment for Android ... 185
7.5.15. Bulk Enrollment using CSV File Upload ... 187
7.5.16. Device_to_User_BulkEnrollment ... 190
7.5.17. Using Samsung Knox Mobile Enrolment ... 191
7.5.18. Enrolling Oculus devices ... 192
7.5.19. Enabling Bluetooth on a Device ... 194
7.5.20. Schedule iOS Update ... 195
7.5.21. Re-install iOS System Apps ... 196
7.5.22. Assigning a Device to a new user ... 197
7.5.23. Reassigning an Android device ... 198
7.5.24. Forcing a device to Check-in ... 199
7.5.25. Locating a Device ... 200
7.5.26. Locking a Device ... 201
7.5.27. Managing Apple devices in lost mode ... 202
7.5.28. Managing Android devices in Lost Mode ... 204
7.5.29. Requesting debug logs ... 206
7.5.30. Apple_Enhanced_Logging ... 207
7.5.31. Retiring a Device ... 208
7.5.32. Relinquishing Ownership of a Device ... 209
7.5.33. Wiping a Device ... 210
7.5.34. Deleting devices ... 211
7.5.35. Unlocking a Device ... 212
7.5.36. Restarting or shutting down devices ... 214
7.5.37. Clearing the Restrictions Password (iOS only) ... 216
7.5.38. Deleting Sentry association for a device ... 217
7.5.39. Assigning Custom Attributes to Devices ... 218
7.5.40. Removing Custom Attributes from Devices ... 219
7.5.41. Synchronising and fetching app feedback ... 220
7.5.42. Setting firmware password ... 222
7.5.43. Reissuing a new Personal Recovery Key ... 223
7.5.44. Setting or changing recovery lock ... 225
7.5.45. Apple Access Management ... 226
7.5.46. Group Policy Enrollment ... 227
8. Apps ... 228
8.1. App Catalogue ... 229
8.2. Declarative Device Management (DDM) App Management ... 247
8.2.1. DDM App Management Settings ... 249
8.3. Apps@Work (iOS, Android, Windows, and macOS) ... 252
8.4. iOS Apps@Work AppStore Features ... 255
8.5. iOS Go Advanced Features ... 258
8.6. Viewing App Details ... 263
8.7. App Configuration ... 266
8.8. Assigning Custom Attributes to Apps ... 282
8.9. Managed Configurations for Android ... 283
8.10. Managing Google Play Apps ... 288
8.11. Deleting Apps from the App Catalogue ... 290
8.12. Upgrading In-House Apps ... 291
8.13. Finding the Package Name for an Android App ... 292
8.14. Categories ... 293
8.15. Distribution Filters ... 294
8.16. Exclude or Distribute apps ... 297
8.17. Reviews ... 298
8.18. Apple Apps and Books ... 300
8.19. Catalogue Settings ... 309
8.20. Deploying app dependencies ... 312
8.21. Deploying Divide Productivity with Android Enterprise ... 315
8.22. Setting up the Provisioner app ... 318
8.23. Managing Windows Applications ... 320

8.24. Ivanti Bridge ... 323
9. Content ... 328
9.1. Managing Content ... 329
9.2. Categories ... 331
10. Configurations ... 332
10.1. Working with Configurations ... 333
10.2. Creating a User Self-Service Portal Configuration ... 345
10.3. Custom Configuration ... 347
10.4. Pushing SyncML to Devices using Custom Configurations ... 349
10.5. Home Screen Layout Configuration ... 350
10.6. App Control Configuration: Control Which Apps Are Installed Per Device ... 352
10.7. App Notifications Configuration ... 354
10.8. Exporting Configurations ... 356
10.9. Prioritising Configurations ... 357
10.10. Managing Configurations ... 358
10.10.1. Configuration Types ... 359
10.10.2. Variables ... 373
10.10.3. AppConnect Configurations ... 378
10.10.3.1. AppConnect Overview ... 379
10.10.3.2. AppConnect Passcode ... 380
10.10.4. Security Configuration ... 381
10.10.4.1. Android Enterprise ... 383
10.10.4.2. Apple PassKeys Attestation ... 385
10.10.4.3. App Privacy Defaults ... 386
10.10.4.4. Editing the Android Enterprise default configuration ... 388
10.10.4.5. Setting up Android Enterprise ... 389
10.10.4.6. Android Enterprise: Work Managed Device Non-GMS mode (AOSP) ... 395
10.10.4.7. Android Work Challenge ... 396
10.10.4.8. Certificate configuration ... 401
10.10.4.9. Certificate Transparency ... 403
10.10.4.10. Certificate Revocation Checking Configuration ... 404
10.10.4.11. Create Autonomous Single App Mode Configuration ... 405
10.10.4.12. Creating DNS Proxy Configuration ... 406
10.10.4.13. Device Logging configuration ... 407
10.10.4.14. Disk Management Configuration ... 409
10.10.4.15. Android Encryption ... 410
10.10.4.16. Encrypted DNS ... 411
10.10.4.17. External Intelligence Settings ... 414
10.10.4.18. Threat Defence ... 415
10.10.4.19. FileVault 2 ... 416
10.10.4.20. FileVault Recovery Key ... 417
10.10.4.21. FileVault Options Configuration ... 418
10.10.4.22. Identity Certificate ... 419
10.10.4.23. Apple Activation Lock Configuration ... 425
10.10.4.24. iOS Custom Configuration ... 428
10.10.4.25. Intelligence Settings ... 429
10.10.4.26. iOS Restrictions ... 432
10.10.4.27. Conference Room Display ... 449
10.10.4.28. Keyboard Settings ... 450
10.10.4.29. Lockdown & Kiosk: Android Device Admin Mode ... 452
10.10.4.30. Setting up Kiosk Mode for Android ... 455
10.10.4.31. Setting up Android shared device kiosk ... 457
10.10.4.32. Lockdown & Kiosk: Android Enterprise ... 458
10.10.4.33. Lockdown & Kiosk: Samsung Knox Standard ... 482
10.10.4.34. Local Administrator Password Solution Configuration ... 486
10.10.4.35. macOS Firewall ... 487
10.10.4.36. macOS Restrictions ... 488
10.10.4.37. macOS AppStore Restrictions ... 495
10.10.4.38. macOS Disk Burning Restrictions ... 496
10.10.4.39. Allowed Media Control (Deprecated) ... 497
10.10.4.40. macOS Finder Settings ... 500
10.10.4.41. macOS Kernel Extension Policy ... 501

10.10.4.42. Mobile@Work for macOS ... 502
10.10.4.43. macOS Software Update Rules Configuration ... 507
10.10.4.44. Certificate Preference ... 508
10.10.4.45. Active Directory (macOS) ... 509
10.10.4.46. Identity Preference ... 512
10.10.4.47. Office 365 Auto Account Creation (macOS) ... 513
10.10.4.48. Authenticate ... 515
10.10.4.49. Apple App Catalogue ... 517
10.10.4.50. Managed Domains ... 518
10.10.4.51. Passcode Configuration ... 519
10.10.4.52. Privacy Preference (macOS) ... 522
10.10.4.53. Privacy Configuration ... 524
10.10.4.54. Client Privacy Statement Information ... 527
10.10.4.55. Ivanti Go Client Settings ... 528
10.10.4.56. Siri Settings ... 530
10.10.4.57. Services Configuration Files Configuration ... 532
10.10.4.58. Software Updates ... 533
10.10.4.59. Software Update Settings Configuration ... 540
10.10.4.60. Security Preferences Configuration ... 544
10.10.4.61. Time Server ... 545
10.10.4.62. Web Content Filter ... 546
10.10.4.63. Windows Firewall ... 549
10.10.4.64. Windows Information Protection ... 552
10.10.4.65. Windows Restrictions ... 556
10.10.4.66. Windows Desktop restrictions ... 561
10.10.4.67. Desktop Settings for Windows 10 ... 563
10.10.4.68. Windows Hello for Business Configuration ... 565
10.10.4.69. Windows AI Management Configuration ... 566
10.10.4.70. Play Integrity (Previously SafetyNet Attestation) ... 568
10.10.4.71. Advanced Android Passcode and Lock Screen ... 569
10.10.4.72. Microsoft Defender for Endpoint ... 570
10.10.4.73. Certificate-based authentication ... 571
10.10.5. User Resource Configurations ... 572
10.10.5.1. CalDAV Configuration ... 573
10.10.5.2. CardDAV Configuration ... 574
10.10.5.3. Google Configuration ... 575
10.10.5.4. Email Configuration ... 577
10.10.5.5. Exchange Configuration ... 580
10.10.5.6. Font Configuration ... 584
10.10.5.7. Subscribed Calendar Configuration ... 585
10.10.5.8. Create a Web Clip Configuration ... 586
10.10.5.9. Office 365 Installation ... 588
10.10.5.10. Windows GPO Settings ... 590
10.10.5.11. BitLocker Encryption Configuration ... 592
10.10.6. Enterprise Network Access Configuration ... 596
10.10.6.1. AirPlay Configuration ... 597
10.10.6.2. AirPrint Configuration ... 598
10.10.6.3. Always-on VPN Configuration ... 599
10.10.6.4. Default App Runtime Permissions ... 603
10.10.6.5. Education ... 605
10.10.6.6. Global Proxy Configuration ... 606
10.10.6.7. Global Proxy Configuration (Android) ... 607
10.10.6.8. LDAP Configuration ... 608
10.10.6.9. macOS Server Configuration ... 609
10.10.6.10. Tunnel ... 610
10.10.6.11. Setting Up AppTunnel ... 611
10.10.6.12. Per-app VPN Configuration ... 616
10.10.6.13. Single Sign-On Configuration ... 624
10.10.6.14. Network Relay Configuration ... 634
10.10.6.15. Multi-user Secure Sign-in for iOS ... 636
10.10.6.16. Android APN Settings Configuration ... 638
10.10.6.17. VPN Configuration ... 642

10.10.6.18. VPN On Demand 654
10.10.6.19. Wi-Fi Configuration 661
10.10.7. Mobile Network Configuration 670
10.10.7.1. APN Configuration 671
10.10.7.2. Mobile 672
10.10.7.3. Cellular Private Network Configuration 675
10.10.7.4. iOS Telecom Presets Configuration 676
10.10.7.5. Enhanced 5G Network Slicing Configuration 677
10.10.7.6. eSIM Configuration 679
10.10.8. Other Configuration 682
10.10.8.1. Associated Domains Configuration 684
10.10.8.2. Android File Transfer Configuration 685
10.10.8.3. Apple TV Configuration 689
10.10.8.4. AirPlay Mirroring 690
10.10.8.5. Browser Settings 692
10.10.8.6. Configuring Single App Mode for iOS 695
10.10.8.7. Configuring an iOS MDM Profile 698
10.10.8.8. Configuring a macOS MDM Profile 699
10.10.8.9. Content Caching 700
10.10.8.10. Creating an Android Shortcut 704
10.10.8.11. Creating Accessibility Settings Configurations 705
10.10.8.12. Create Screen Saver Configuration 708
10.10.8.13. Configure User's Screen Saver 709
10.10.8.14. Device Name Settings 710
10.10.8.15. Device Wallpaper Configuration 711
10.10.8.16. EMA Server Integration Configuration 714
10.10.8.17. Energy Saver Configuration 715
10.10.8.18. Ethernet Configuration (macOS) 721
10.10.8.19. Google BeyondCorp Configuration 725
10.10.8.20. Lock Screen Message Configuration 729
10.10.8.21. Login Window Configuration - macOS 731
10.10.8.22. macOS System Extension configuration 732
10.10.8.23. MAM-Only 733
10.10.8.24. Managed Google Play Configuration 735
10.10.8.25. Migration Assistant Settings 736
10.10.8.26. App Notifications Configuration 737
10.10.8.27. Printer Settings 738
10.10.8.28. Remove Bloatware Configuration 740
10.10.8.29. Safari Extension and Settings Configuration 741
10.10.8.30. Samsung Phone Restrictions Configuration 745
10.10.8.31. Default Browser Configuration - iOS and visionOS 746
10.10.8.32. Screen Sharing Host Settings Configuration 747
10.10.8.33. Single App Mode Configuration 748
10.10.8.34. Software update recommendation cadence configuration 751
10.10.8.35. Start menu and Taskbar 752
10.10.8.36. System Update Configuration 754
10.10.8.37. Windows 10 Update Management 759
10.10.8.38. Windows app scheduling 761
10.10.8.39. Windows BIOS Configuration 762
10.10.8.40. Windows BitLocker 770
10.10.8.41. Windows Kiosk Configuration 771
10.10.8.42. Windows Licence Configuration 775
11. Policies 776
11.1. Working with Policies 777
11.2. Custom Policy 783
11.3. Monitoring and Controlling Allowed Apps 805
11.4. Prioritising Policies 812
11.5. Windows Hardware policy 813
12. Admin 814
12.1. System 815
12.1.1. Attributes 816
12.1.2. Device Cleanup Settings 822

12.1.3. GDPR Profiles ... 827
12.1.4. Notification emails ... 829
12.1.5. Roles Management ... 830
12.1.6. Spaces ... 836
12.1.6.1. Spaces ... 837
12.1.6.2. Managing Spaces ... 839
12.1.6.3. Space Examples ... 844
12.1.6.4. Delegating Devices ... 846
12.1.6.5. Delegating Apps ... 847
12.1.7. Support Administrators ... 849
12.1.8. Admin > System Use Notification ... 850
12.2. Infrastructure ... 852
12.2.1. Access ... 853
12.2.2. App Lists ... 854
12.2.3. Exporting Audit Trails ... 855
12.2.4. Certificate Management ... 858
12.2.5. SCEP Configuration for External Certificate Authorities ... 865
12.2.6. Derived Credential Providers ... 867
12.2.7. Connector ... 868
12.2.8. Using the httpproxy command for Connector ... 871
12.2.9. Help@Work ... 872
12.2.10. Infrastructure Identity ... 875
12.2.10.1. Configure Identity Provider ... 876
12.2.10.2. User Provisioning with SCIM ... 880
12.2.10.2.1. User Provisioning for Entra ID IdP ... 883
12.2.10.2.2. User Provisioning for Okta IdP ... 888
12.2.11. Configuring LDAP server ... 891
12.2.12. Sentry ... 900
12.3. Apple Settings ... 901
12.3.1. Apple Configurator ... 902
12.3.2. Account-driven Enrollment ... 904
12.3.3. Device Enrollment ... 907
12.3.4. Beta Enrollment ... 922
12.3.5. Configuring the Setup Assistant ... 923
12.3.6. Install MDM Certificate ... 924
12.3.7. Shared iPad devices for business ... 925
12.3.8. School Manager ... 930
12.3.9. Settings (Apple) ... 933
12.4. Work with Windows Devices ... 935
12.4.1. Configuring Windows Autopilot Profiles ... 936
12.4.2. Audit Trails on Windows Autopilot Profiles ... 942
12.4.3. TenantLockdown CSP ... 943
12.4.4. ADMX (GPO) Browser ... 944
12.4.5. Configuring app inventory intervals ... 945
12.4.6. Hardware Inventory ... 946
12.5. Setup with Microsoft Azure ... 947
12.5.1. Using Microsoft Azure ... 948
12.5.2. Entra ID Windows 10 Unified Endpoint Management Setup ... 951
12.5.3. Assigning Entra ID UEM app ... 952
12.5.4. Connect Ivanti Neurons for MDM with Entra ID User Source ... 953
12.5.5. Azure Tenant ... 955
12.5.5.1. Azure Tenant Requirements ... 956
12.5.5.2. Apply the Intune licence to device users ... 957
12.5.5.3. Adding MobileIron as a compliance partner ... 958
12.5.5.4. Creating a conditional access policy in Microsoft Endpoint Manager ... 959
12.5.5.5. Connecting Microsoft Azure to Ivanti Neurons for MDM ... 960
12.5.5.6. Creating a partner device compliance policy ... 961
12.5.5.7. Device status reporting from Ivanti Neurons for MDM to Azure ... 963
12.5.5.8. De-provisioning of the Azure tenant ... 965
12.5.6. Admin > Microsoft Azure > Office 365 App Protection ... 966
12.6. Connect with Google Apps ... 974
12.6.1. Managed Google Play Accounts (Android Enterprise Accounts) ... 975

12.6.2. Android device registration 979
12.6.3. Android Management API 980
12.6.4. Google Apps API 986
12.6.5. Admin - Android Enterprise 987
12.7. Work with ChromeOS Devices 989
12.7.1. ChromeOS and Ivanti Neurons for MDM 990
12.7.2. Distribute Android apps to ChromeOS devices 992
12.7.3. Add and distribute ChromeOS extension apps 993
12.7.4. ChromeOS Blueprint Configuration 994
12.7.5. Device Actions 995
12.7.6. FAQs 996
12.7.7. Recommended Steps for evaluation 998
12.8. Firmware Management 999
12.8.1. Enrolling to Zebra OTA service 1000
12.8.2. Samsung E-FOTA License Management (Decommissioned) 1001
12.9. Manage Scripts and Files 1002
12.9.1. All Scripts 1003
12.9.2. Files 1007
12.10. Branding 1008
12.10.1. Admin > Apple App Catalogue (Branding) 1009
12.10.2. Branding the Android App Catalog 1010
12.10.3. Admin > Android Kiosk Branding 1011
12.10.4. Branding Email Templates 1012
12.10.5. Self-Service Portal 1020
12.10.6. Self-Service Portal (Branding) 1022
12.10.7. Multi User Sign-In (Webclip) Branding 1023
12.10.8. Organisation 1024
12.11. Adding management of non-iOS devices 1025
13. Packages 1026
13.1. Upgrading 1030
14. Device Licences 1032
14.1. Tenant Suspension 1033
15. Opening a Support Ticket 1034
16. Third-Party Attributes 1035
17. Apps@Work 1036
18. Enable Kerberos Authentication between Ivanti Neurons for MDM and SCEP server 1038
19. Ivanti Neurons for MDM Administrator Guide 1040
20. Welcome 1041
21. Welcome CSH 1042
22. Windows Update Management 1043

1. About Ivanti Neurons for MDM

A modern approach to mobile security, Ivanti Neurons for MDM provides unified endpoint management (UEM) solutions in a highly scalable, secure, and easy to update infrastructure that supports millions of devices around the world.

- Instant updates: Get automatic software and security updates and access to the new features the moment they become available.
- On-demand scalability: Scale your deployment as business needs change without having to worry about capacity planning.
- Minimise hardware costs: By eliminating the need to maintain on-premise hardware, cloud-based services require zero footprint to manage.
- High up-time and high availability.
- Maximise existing investments: Re-allocate IT resources from hardware maintenance to more strategic tasks that add value to the business.

You can view the summaries of **New features summary** available in this release.

2. What's New - 127

This section provides summaries of new features and enhancements that are available in this release. References to documentation describing these features and enhancements are also provided, when available.

General features and enhancements

Android features

iOS, macOS, watchOS, visionOS, and tvOS features

Windows features

General features and enhancements

- **Enhanced macOS Package ID Handling**: Improved macOS in-house PKG app deployment by automatically detecting and populating the correct package ID during app upload and ensuring the same package ID is sent to devices. This enhances app identification accuracy, resolves server-device install state mismatches, and improves installation status reporting. Bundle IDs can be reviewed and edited during upload before being locked after deployment.
- **Bundle ID Visibility for Installed Apps**: The Installed Apps section on the Device Details page now includes a Bundle ID column, which can be enabled or hidden from the page settings.
- **Automatic Retry for Failed Android App Installations**: Android app installations that enter an Error Install state are now automatically retried starting one hour after device registration. Installation commands are re-sent every 30 minutes for up to five attempts to improve app deployment success.
- **Device Movement Audit Trails for Spaces**: Added the Enable Audit Trails for Device Enrollment and Unenrollment in Spaces setting to track device movement between spaces. For more information, see Exporting Audit Trails.
- **OS Platform filter for Device Cleanup Settings**: Administrators can now filter device cleanup actions by OS platform when removing Retired and Retire Pending devices. By default, all supported platforms remain selected, preserving the existing behavior. Administrators can modify the selection and restrict cleanup operations to specific platforms as required. For more information, see Device Cleanup Settings.
- **Office 365 App Protection Policy Synchronization**: Previously, administrators could select apps directly within Ivanti Neurons for MDM while creating or modifying app protection policies. Microsoft has deprecated the API that was used to retrieve the available apps list, causing protected app lists to appear empty in Ivanti Neurons for MDM. Microsoft Office 365 App Protection policy management is updated to align with changes in Microsoft Intune. Applications configured in Intune are now automatically synchronized to Ivanti Neurons for MDM, ensuring continued visibility of protected apps. While app removal remains supported from Ivanti Neurons for MDM, new app assignments must be configured in Microsoft Intune and will be reflected automatically.
- **Device Movement Audit Logging for Spaces**: Administrators can now track device movement between spaces through Audit Logs. When enabled, the new audit setting records events whenever a device is removed from one space and added to another, providing greater visibility into automated and rule-based space assignments. For more information, see Exporting Audit Trails.
- **Automatic Custom Attribute assignment using Device Groups**: Administrators can now assign custom attributes at the device group level. Devices that are members of a device group automatically inherit the configured attribute values, reducing manual configuration and helping ensure consistent device categorization. Device GroupsSee Device Groups for more information.
- **OS-Level Device Registration Restrictions**: Restrict device registration by platform, allowing only approved **Apple**, **Android**, and **Windows** devices to enroll. For more information, see User Settings.

Android features

- **Prevent App Updates While App Is in Use**: Administrators can now prevent managed Android apps from being updated while they are actively in use. When **Do Not Update While App Is In Use** is enabled, app updates are deferred until the user closes the app or moves it to the background, helping minimise disruptions during active sessions. For more information, see **App Configuration**.
- **Maintain Kiosk Mode across Lockdown Policy changes**:Added support for maintaining kiosk mode across lockdown policy changes. Devices automatically return to kiosk mode after a lockdown policy update, reducing manual intervention and minimizing disruptions on dedicated-purpose devices. For more information, see **Lockdown & Kiosk: Android Enterprise**.
- **Enable Unredacted Notifications**: Added support for configuring lock screen notification visibility on Device Owner devices. Administrators can display, hide, or redact notification content on the lock screen to help protect sensitive information while maintaining notification functionality. For more information, see **Advanced Android Passcode and Lock Screen**.
- **Support for Device-to-User Mapping during Bulk Enrollment of Profiles**: Added support for device-to-user mapping in bulk enrollment profiles. Administrators can assign a specific user to each device through the bulk enrollment CSV file or during manual device addition, enabling automatic user assignment during enrollment and reducing post-enrollment administrative tasks. Administrators can also update user assignments before device enrollment. For more information, see **Device-to-User Mapping in Bulk Enrollment Profiles**.

iOS, macOS, watchOS, visionOS, and tvOS features

- **New Skip Keys for Device Enrollment profiles**: Administrators can now use the following Skip Keys when creating Device Enrollment profiles:
  - **Skip Liquid Glass Pane** (iOS 27.0+ and macOS 27.0+)
  - **Skip Accessibility Appearance Pane** (iOS 27.0+)
    These skip keys help streamline the enrollment experience by allowing administrators to hide specific setup panes during device enrollment. For more information, see **Device Enrollment**.
- **Support for DDM Device System Health Status**: Ivanti Neurons for MDM now supports the DDM Device System Health status on the **Device Details** page. Administrators can view this status under the **Device Component Health** section to monitor the system health reported by the Supervised devices. For more information, see **Getting Started with Devices**.
- **Added new Device Details fields for Apple devices**: Added new **Device Details** fields to provide more visibility into Apple Device Management states. Administrators can now view the following details:
  - **Multi-User Mode** for devices operating on iOS 27.0+. This field indicates whether an iPad is configured as a shared device.
  - **MDM Enrollment Type** for devices operating on iOS 27.0+, macOS 27.0+, tvOS 27.0+, visionOS 27.0+, and watchOS 27.0+.
  - **MDM Return to Service** with app preservation for devices operating on iOS 27.0+ and visionOS 27.0+.
    These fields help administrators review device configuration and enrollment information directly from the Device Details page. For more information, see **Getting Started with Devices**.
- **Support for App Privacy Defaults Configuration**: Administrators can now configure **App Privacy Defaults** for one or more apps using Apple Device Declarative Management (DDM). When an app first launches, users receive a single consent prompt to allow or defer recommended permissions for supported privacy components, such as camera, microphone, location, Bluetooth, and local network access. For more information, see **App Privacy Defaults**.

> The App Privacy Defaults configuration is now supported on macOS 27.0+ supervised devices.

- **Added new DDM app management attribute**: Added the DDM app management attribute **Apple DDM App Enabled** field to the 'Advanced Search' and device listing pages. It shows which devices have apps distributed via DDM. Admins can turn this on through User Settings. For more information, see **Getting Started with Devices**.
- **Enhanced macOS Extensible SSO Configuration**: Updated macOS Extensible SSO configuration to correctly map token attributes such as **preferred_username** and **name**. This resolves configuration errors caused by invalid token-to-user mappings and allows SSO profiles to be successfully deployed to devices.
- **Apple Enhanced Logging**: Administrators can initiate Apple Enhanced Log Collection on supported Apple devices using an AppleCare-provided token. Device details display session status, token, and timestamp information, and active sessions can be canceled if required. For more information, see **Apple Enhanced Logging**.
- **Lockdown Mode Status** (iOS 27+, macOS 27+): Added support for viewing and filtering devices by Lockdown Mode status using the new **Security Lockdown Mode** field on the **Device Details** page, **Advanced Search**, and device group rules. This field indicates whether Lockdown Mode is enabled (**true**) or disabled (**false**) on a device. For more information, see **Getting Started with Devices** , **Device Groups** and **Custom Policy**.
- **macOS Software Update Settings Support Update**: The **macOS Software Update Settings** configuration is no longer supported on macOS 27 and later devices. This configuration now applies only to supported versions up to macOS 26.x. For more information, see **macOS Software Update Rules Configuration**.
- **Restrictions Support Update** (iOS 27+, macOS 27+): Updated the **Allow Background Security Improvements Installation** and **Allow Background Security Improvements Removal** restrictions to indicate that they are no longer supported on iOS 27 and later and macOS 27 and later devices. For more information, see **iOS Restrictions** and **macOS Restrictions**.
- **Updates to Siri Settings Configuration** (iOS 27.0+, macOS 27.0+, tvOS 27.0+, and visionOS 27.0+): Added support for new restriction settings in the Siri Settings configuration . For more information, see **Siri Settings**.
- **Updates to Intelligence Settings Configuration** (iOS 27.0+, macOS 27.0+, and visionOS 27.0+): Added support for new restriction settings in the Intelligence Settings configuration. For more information, see **Intelligence Settings**.
- **Safari Privacy Settings** (iOS 27.0+, macOS 27.0+): Added support for Safari Privacy Settings in the Safari Extension and Settings configuration, allowing administrators to configure default Camera and Microphone permissions for specific websites using Apple Declarative Device Management (DDM). For more information, see **Safari Extension and Settings Configuration**

Windows features

- **Windows AI Management Configuration**: Windows AI Management now supports additional Windows AI CSP policies for managing Microsoft Copilot, Windows Recall, and Microsoft Paint AI features. Administrators can disable the Copilot hardware key, remove the Microsoft Copilot app, disable AI data analysis for Recall, configure Recall snapshot storage limits, and disable Image Creator, Cocreator, and Generative Fill in Paint. Support for both user-scoped and device-scoped policies has also been added, enabling more granular control of AI capabilities on Windows devices. For more information, see **Windows AI Management Configuration**.

Mobile Threat Defense features

Mobile Threat Defense (MTD) protects managed devices from mobile threats and vulnerabilities affecting device, network and applications. For information on MTD-related features, as applicable for the current release, see the Mobile Threat Defense Solution Guide for your platform, available under the MOBILE THREAT DEFENSE section on the Ivanti **Product Documentation** page.

> Each version of the MTD guide contains all Mobile Threat Defense features that are currently fully tested and available for use on both server and client environments. Because of the gap between server and client releases, new versions of the MTD guide are made available with the final release in the series when the features are fully functional.

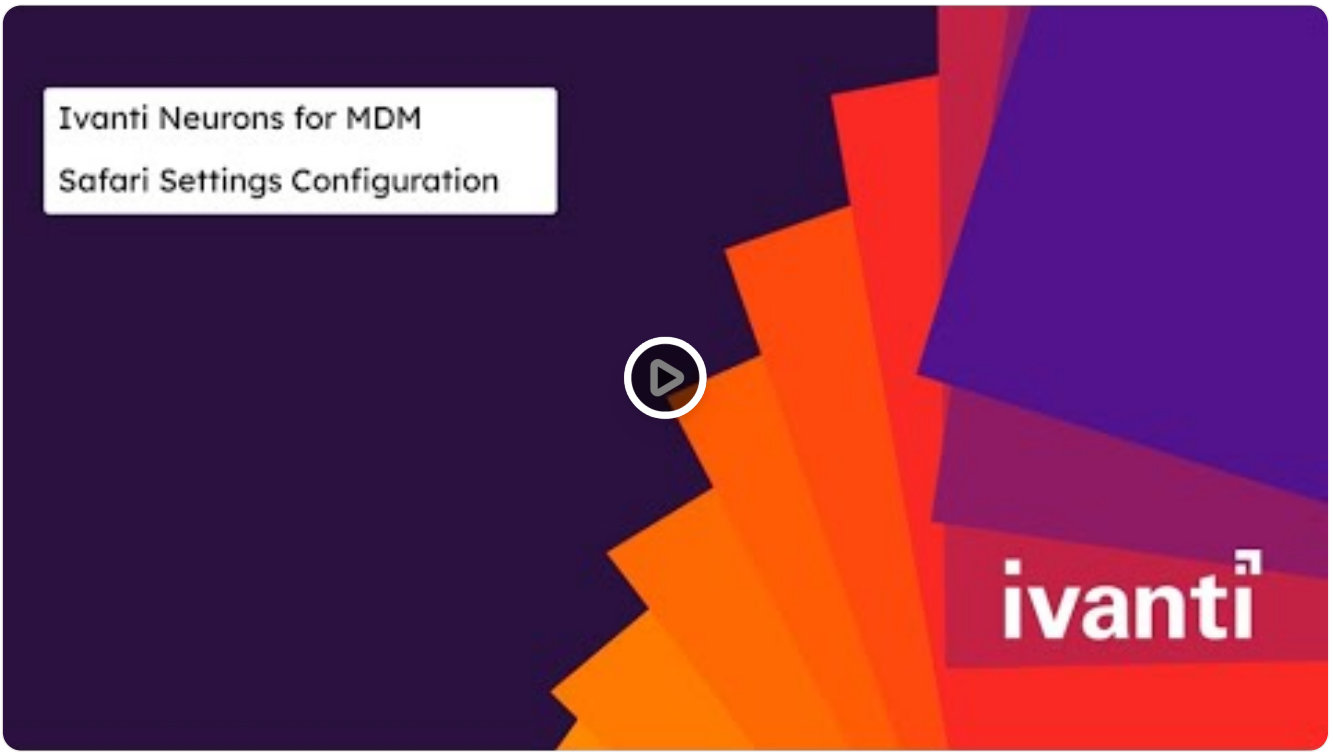
3. Videos

Featured videos




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.



Looking for a video on a specific feature or functionality in Ivanti Neurons for MDM? Let us know by sharing your feedback in the "**Was this article useful?**" section on any page of this document.

4. Getting Started

This section provides setup and usage overviews of features that require interaction across the Ivanti Neurons for MDM portal. This section contains the following topics:

- Solution Overview
  - Key features
  - Architecture diagram
  - Ivanti Neurons for MDM applications
  - Roles
  - Getting started
- Setting preferred language in a browser
- Unified navigation interface for Ivanti Neurons for MDM and Access
- Device Admin (DA) mode to manage Android devices - deprecated

Solution Overview

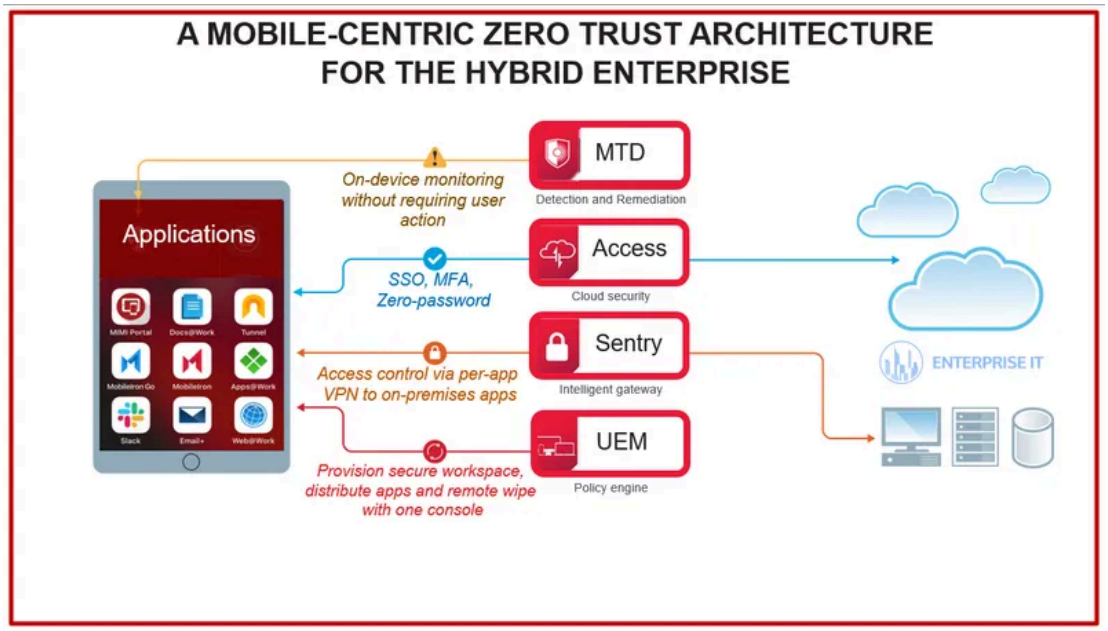
Continuous access to business data on mobile devices and other endpoints outside the corporate network requires a dedicated focus on security. To keep up with current security needs, enterprises need to consider how they can:

- Provision endpoints such as mobile phones and laptops
- Grant access based on a set of imperative data
- Protect data at rest and in motion
- Enforce measures as required

The Ivanti solution to this modern problem meets all the challenges. You can monitor endpoints and trigger adaptive policies to remediate threats, quarantine devices and maintain compliance. Together, the following components help your organisation realise the mobile-centric zero trust framework:

- Ivanti Neurons for MDM - Helps you create a secure workspace on any device with apps, configurations, and policies for the user based on their role. Users get easy and secure access to the resources they need for their productivity
- **Sentry** - An in-line intelligent gateway that helps your secure access to on-premise resources
- **Access** – Helps you verify the user, device, app, network type and presence of threats. The adaptive access control check is the basis of the zero-trust model. Access provides single sign-on and security on the cloud
- **Mobile Threat Defense** - The combination of Ivanti Neurons for MDM and Mobile Threat Defense (MTD) protects data on-device and on-the-network with state–of–the–art encryption and threat monitoring to detect device, network, and app-level attacks

The following illustration shows the solution overview:



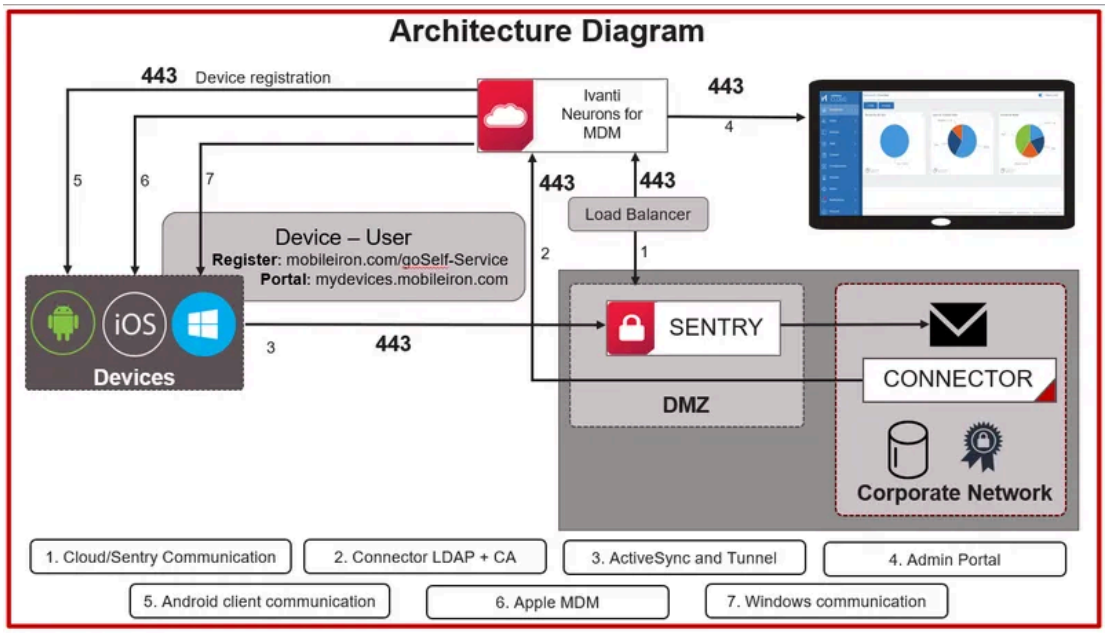
Key features

The Ivanti Neurons for MDM platform provides the fundamental visibility and IT controls needed to secure, manage, and monitor any corporate or employee-owned mobile device or desktop that accesses business-critical data. Ivanti Neurons for MDM platform allows organisations to secure a vast range of employee devices being used within the organisation while managing the entire life cycle of the device including:

- Policy configuration management and enforcement
- Application distribution and management
- Script management and distribution for desktop devices
- Device actions
- Access control and multifactor authentication
- Threat detection and remediation

Architecture diagram

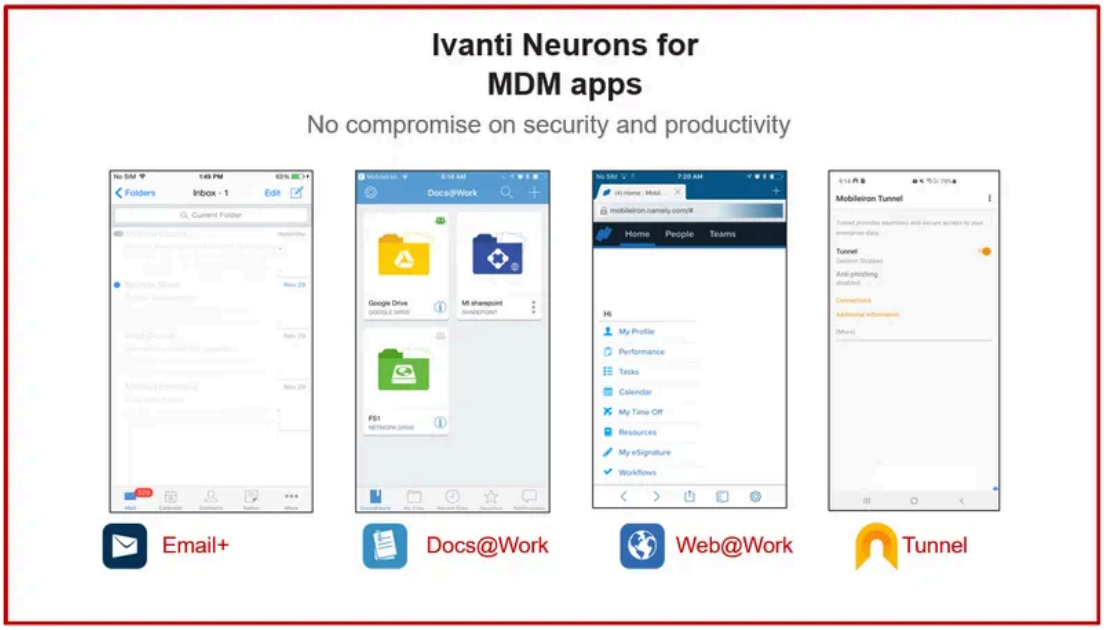
The following diagram shows the architectural overview of the Ivanti Neurons for MDM UEM platform:



Ivanti Neurons for MDM applications

- **App Catalog** – The App Catalog is a customisable enterprise app shopfront. IT administrators can directly publish private or in-house apps to their end-users devices. The App Catalog can also be combined with Apple Volume Purchase Program to facilitate a secure distribution of mobile apps on iOS devices. Further, Ivanti can harness the capabilities found in iOS managed apps and Android Enterprise. This allows for easy configuration within the Ivanti Neurons for MDM UEM platform of app-level settings and security policies for both advanced app security functions.
- **Email+** - A cross-platform to secure PIM application for iOS and Android. Email+ provides secure email, calendar, contacts, and tasks on corporate-owned and personal devices by communicating with an ActiveSync server in your enterprise.
- **Docs@Work** - Allows users to access, create, edit, markup, and share content securely from repositories such as Microsoft Share Point, and cloud services such as Box and Dropbox. This is important so users can maximise productivity on the go.
- **Web@Work** - Is a secure browser that allows enterprise users to securely access web content in their corporate intranet. Using Web@Work you can limit access to enterprise data to authorised users. When Web@Work is deployed in conjunction with App Tunnel, you secure the enterprise data in motion. With Web@Work users can access internal web resources quickly and easily.

The following image shows the Ivanti Neurons for MDM applications:



Roles

Administrator - As an Enterprise Administrator, you are responsible for the following tasks:

- Provide enterprise users with seamless and secure access to workspace emails, applications, configurations and connectivity such as Wi-Fi and VPN.
- Separate personal data from business data on employee devices so that business data does not leak into the personal apps and personal data is not inadvertently accessed by IT.

User – As an Enterprise User, you can seamlessly access business applications and personal data from secure modern mobile devices, desktops and cloud services. For more information about the various tasks that you can perform as a user, see **Users**. and **Roles Management**.

Getting started

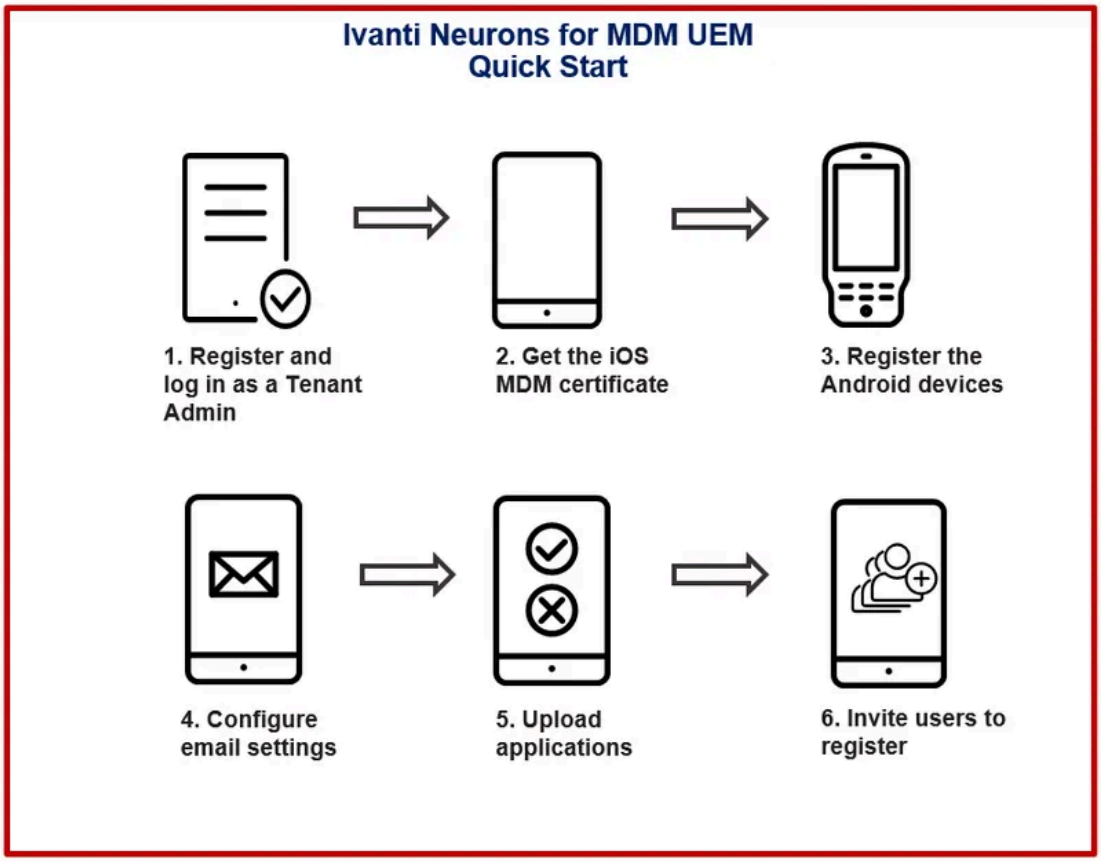
If you are a registered new user, follow the steps provided in this section to quickly get onboarded to the Ivanti Neurons for MDM services.

After you subscribe to the Ivanti Neurons for MDM platform, Ivanti creates a Ivanti Neurons for MDM tenant for you. You receive an email to the registered email address and the email contains a PDF with the following information about the tenant created for your enterprise:

- Information about the software bundle you purchased
- The URL and super admin login credentials of the tenant
- How to access Support Community and FAQs for Ivanti Neurons for MDM
- Where to access technical documentation and download the software

> Ivanti, Inc does not provide software keys. By logging into your Ivanti Neurons for MDM tenant with the Super Admin credentials and accepting the terms of service, you activate the Ivanti Neurons for MDM product.

The following diagram depicts the steps to get started with Ivanti Neurons for MDM:



Procedure

1. Click the URL provided in the tenant registration email. The password reset prompt appears.
2. Change your password.
3. Log in to the tenant account using the ID and password. The Welcome wizard appears.
4. Complete the details in the **Welcome** form, accept the terms and agreement, and click **Continue**.
5. To install iOS MDM certificate, see **Install MDM Certificate**.

> If you want to manage your iOS devices at a later point in time, you can skip the iOS MDM certificate installation. Then the wizard prompts you to register the Android devices of your enterprise. Note: Skipping the iOS MDM certificate installation means iOS devices will not be able to register. Users will see a message stating that iOS device enrolment has not been enabled.

6. To register the Android devices in Android Enterprise (AE) mode, see **Managed Google Play Accounts (Android Enterprise Accounts)**. The wizard then prompts you to setup email accounts.

> If you want to manage your Android devices at a later point in time, you can skip the Android managed Google Play account enrolment. Skipping the Managed Google Play Account enrolment will not allow you to register Android Enterprise devices. Android devices can still be registered with Device Admin, but key features such as Managed Google Play, and App Configuration will not be available for use.

7. To configure the email settings and ActiveSync, see **Exchange Configuration** and **Email Configuration**.
8. Click **Continue**. The pass code creation prompt appears.

9. Select a pass code type and click **Continue**.
10. Select the applications you want to upload and click **Continue**.
11. Specify the email addresses of the users and click **Continue**. The users will receive an email to register their mobile devices. A summary of the configuration is displayed.
12. Click **Finished**. The Dashboard page is displayed.
13. To explore further, do the following:
    - Go to **Users**. All the invited users are listed.
    - Go to **Apps**. All the applications that you uploaded are listed.
    - Go to **Configurations**. All the configurations that you pushed during registration are listed.

For more information about the various tasks that you can perform as an administrator, see the **Admin** section.

Setting preferred language in a browser

If a user has set their browser language as one which is not supported, the user can set en_US (English, United States) as the default language for the portal.

To set language preference for Safari browser running on macOS 10.15+ devices, users can set the preferred language as follows:

1. On the macOS device, go to **System Preference**.
2. Go to **Language and Region > General**.
3. Set **en_US** (or any other language option) as the **Preferred Language**.

Unified navigation interface for Ivanti Neurons for MDM and Access

For new customers in some clusters, Access is available as a unified navigation interface with Ivanti Neurons for MDM. Log in with your Ivanti Neurons for MDM administrator credentials. The Access options are available in the left navigation pane as a separate tab. Visit **Product Documentation** and click Access for more information about Access and how to set up Access.

The unified navigation interface includes the following features:

- Unified log in for both Ivanti Neurons for MDM and Access.
- Product picker in the left navigation pane to switch between Ivanti Neurons for MDMand Access products.
- Product selection memory: upon the first log in, Ivanti Neurons for MDM admin portal appears. Upon subsequent log ins, Ivanti Neurons for MDM or Access appears, mirroring the product selected upon first log in.
- Left navigation pane for both Ivanti Neurons for MDM and Access.
- Unified account settings pane with links to options such as Upgrade Options, Documentation, Support Portal, Change Password, and Sign Out.

Device Admin (DA) mode to manage Android devices - deprecated

Device Admin (DA) mode of managing Android devices is being deprecated in phased manner from Ivanti Neurons for MDM 78 onwards.

Any new users with a new tenant created on Ivanti Neurons for MDM 78, will not be able to register any devices (Android 6 and later) in DA mode. Any new tenants that need to enable DA registration for Android 6 to Android 9 must contact Ivanti Support.

- Android 10 and later devices will continue to be blocked from registering to DA mode.

- For existing users (with or without existing DA deployments), there are no changes in terms of managing the existing DA devices (Android 6 to Android 11). However, on upgrading to Ivanti Neurons for MDM 78, any newly registered devices running Android 10+ on existing tenants will also not be allowed to run in DA mode. Such existing tenants would only be able to enrol devices from Android 6 to Android 9 versions in DA mode.
- If any users are planning to migrate DA devices from a Core instance to the Ivanti Neurons for MDM R78, ensure that Android Enterprise is enabled and at least one system configuration is distributed to the target set: PO, DO, or COPE before triggering the migration. This step is essential to prevent the retirement of devices post migration.

DA registration type	Existing tenant (upgraded to 78)	New tenant
New DA registration of device with OS >=10	Not Allowed	Not allowed
New DA registration of device with OS < 10	Allowed	Not allowed
Existing DA devices with OS >= 10	Will remain active	NA
Existing DA devices with OS < 10	Will remain active	NA
Migrated DA devices with OS >= 10	Will Retire	Will Retire
Migrated DA devices with OS < 10	Will remain active	Will Retire

4.1. Configuring macOS devices

This is an overview topic that provides a list of common procedures and other content related to configuring macOS devices in Ivanti Neurons for MDM. You can access all the macOS topics in the Ivanti Neurons for MDM*Administrator Guide*.

Contents

- Registering devices
- Configuring user invitation template
- Setting up Zero Sign-on features
- Setting up Mobile@Work for macOS client
- Setting up macOS shell scripts
- Setting up macOS configurations
- Setting up macOS policies

Registering devices

Most users start by registering a device. You can use any of the following approaches to start the registration process:

- Send an invitation to one or more end users (iReg registration). For more information, see the *macOS Device Registration* topic in the **Device registration** section.
- **Device Enrollment** and **User Enrollment with Apple Business Manager**

For more information, see Device registration.

Configuring user invitation template

You can brand the end user email invitation to make its appearance more familiar to your end users. For more information, see **Branding Email Templates**.

You can customise the device registration process with names and logos that your users will recognise. For more information, see **User Branding**.

For more information, see **Configuring and Using Registration Confirmation Emails**.

Setting up Zero Sign-on features

For Zero Sign-on related documentation, see Zero Sign-on with Access in the *Access Guide*.

For zero-touch automated enrollment, see the User settings topic, Configuring the settings for new device registrations section, Step 13.

Setting up Mobile@Work for macOS client

Mobile@Work for macOS app provides:

- Scripting capabilities on macOS devices
- App Catalog for end users
- Push notifications

- User onboarding (welcome/status) screen for automated device enrollment registrations

Before pushing Mobile@Work to the end users, ensure that **Mobile@Work for macOS Configuration.htmMobile@Work for macOS** is created and is set to be distributed to the target macOS devices.

You can enable user onboarding for macOS devices during the automated **Device Enrollment** process. As soon as the Device Enrollment is completed, Mobile@Work for macOS is pushed to the device along with the profiles, configurations and apps.

Setting up macOS shell scripts

Ivanti Neurons for MDMallows you to create your own macOS shell scripts, which you can then upload to Ivanti Neurons for MDM and run on managed macOS devices. In , you can configure the scripts using the Mobile@Work for macOS Script configuration. Mobile@Work for macOS returns the script execution results to Ivanti Neurons for MDM, which are shown in the device logs. You can check the device logs from the device details page of the macOS device, in the **Logs** tab. For more information about creating, uploading, and managing the scripts repository, see **All Scripts**.

Before you can run shell scripts on macOS devices, ensure that the users have the Mobile@Work for macOS app running on their devices and have a Mobile@Work for macOS configuration pushed to their devices. Scripts can be run once or on a recurring basis. Scripting on Ivanti Neurons for MDM also allows administrators to collect information from a device and then be stored in Ivanti Neurons for MDM as a custom attribute. For example, if you need to know Java version on a macOS device, you can collect this information and store it on a per-device-basis in a custom device attribute. For more information, see *Creating a Mobile@Work for macOS Script Configuration* in **Mobile@Work for macOS**.

Setting up macOS configurations

Configurations are collections of settings that you send to devices. For example, you can use configurations to automatically set up VPN settings and passcode requirements on these devices. Use the **Configurations** page to select, set up, and distribute configurations. There are many **types of configurations** available. In the **page**, you can view a list of available macOS configurations, including the following configurations:

- **Wi-Fi**
- **Passcode**
- **VPN**
- **Encrypted DNS**
- **FileVault 2**
- **FileVault Recovery Key**
- **macOS Firewall**
- **macOS Restrictions**
- **macOS AppStore Restrictions**
- **macOS Finder Settings**
- **macOS Kernel Extension Policy**
- **Active Directory (macOS)**
- **Office 365 Auto Account Creation (macOS)**

You can use **custom configurations** to import and distribute a predefined configuration file.

Setting up macOS policies

Policies define requirements for devices, as well as what will happen if a device does not comply with requirements. Each policy consists of a rule and a compliance action (what happens if the rule is violated). Use the **Policies** page to select, set up, and distribute policies. Data Protection/Encryption Disabled and Allowed apps are macOS-related policies. You can use Custom Policies to create a custom policy based on device and user attributes, section criteria, values and compliance actions you specify.

Distributing macOS apps

Ivanti Neurons for MDM supports macOS apps distribution via Apple's MDM protocol and using the Mobile@Work app. Administrators can choose to use one or both of the following approaches:

- Apple's MDM protocol - Administrators can upload only specific PKG formats (distribution format) as in-house apps and can also distribute apps from Mac App Store (Apple's Apps and Books licensing support is included). However, this approach does not allow administrators to distribute DMG and other PKG formats.
- Mobile@Work for macOS app - As a way to distribute apps to users, administrators can use MobileIron Packager (MIP) app to convert any PKG, DMG or .app files to an MIP file. Upload the MIP file into Ivanti Neurons for MDM as an in-house app.

> You can download Ivanti Neurons for MDM Mac Packager utility from MobileIron software downloads.

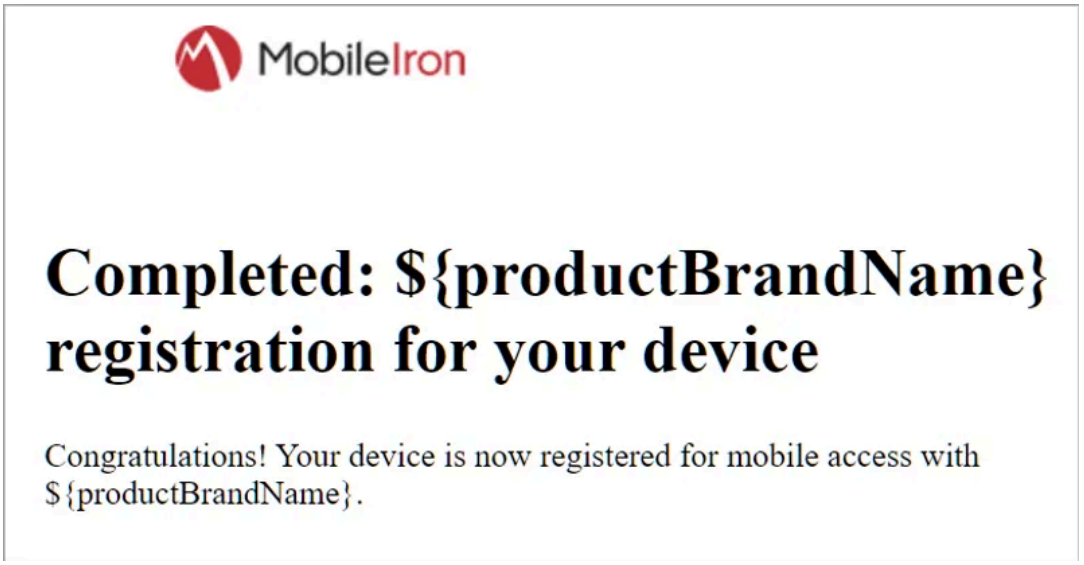
Administrators can use Mobile@Work to distribute in-house apps that are in the DMG, PKG or .app format. For apps that are only available in the Mac App Store, administrators can continue to use Apple's native MDM capabilities, which includes Apple Apps and Book licences capabilities.

4.2. Configuring and using registration confirmation emails

Administrators can configure and trigger emails to users after they have completed registration. This email can contain, for example, additional instructions for users after having successfully registered. Administrators can enable sending of this email during user invitation.

The process:

- **Configuring the feature:**
  - Configure the email template: The English email template looks like this by default, but you can revise it to better suit your purposes by following the instructions at **Customising an email template** in **Branding Email Templates**.



  - Turn on the registration confirmation email. See **Configuring User Registration Confirmation emails** in **User Settings**.
- **Using the feature:**
  - Send the user the invitation to register, as described in **Inviting Users**. When the user successfully registers, Ivanti Neurons for MDM will send that user the registration confirmation email.

4.3. Configuring and using policy compliance notification emails

Administrators can wrap in a policy compliance notification email template, the emails sent by the Custom and Allowed Apps policies' send email actions to users whose devices have fallen out of compliance. The following process describes the configuration:

- **Configuring the feature:**
  - **Configure the email template**.
    The English email template looks like this by default, but you can revise it to better suit your purposes by following the instructions at **Customising an email template** in **Branding Email Templates**



  - **Turn on the policy compliance notification template**. This template works in conjunction with the message you craft using the Custom and Allowed Apps policies' send email actions. Ivanti Neurons for MDM inserts the information you specify in those email actions into the policy compliance notification template. You can turn on the policy compliance email template when you create or edit a Custom or Allowed Apps policy. For more information about instructions on enabling the policy compliance notification template for a Custom policy or Allowed apps policy, see **Adding a custom policy** and **Creating an Allowed Apps policy** respectively.
- **Using the feature:**
  - When a device falls out of compliance with a Custom or Allowed apps policy with the policy notification template enabled, Ivanti Neurons for MDM sends the device owner an email, first wrapping the email in the policy notification template. Your interaction with the feature is to configure it as summarised above, whereas Ivanti Neurons for MDM itself uses the feature.

4.4. On-demand features

Ivanti Neurons for MDM includes certain on-demand features that are disabled by default. Such features may have some impact on performance and may not yet be fully ready for deployment in production.

Administrators can contact **Support** if they are interested in enabling one or more on-demand features on their tenant(s) devices that are disabled by default.

The following table includes the list of documented on-demand features:

Feature	Description	Platform(s)	Licence
Windows 10 features	Features applicable to Windows 10 devices.	Windows 10	• Legacy: Gold • Current: Secure EUM See **Packages** for more information about legacy and current offerings.
App catalogue URL copy to clipboard	Provides the ability for the administrators to copy the app catalogue URL to clipboard for apps. This URL can be distributed to the users via email. If the user clicks the link from a registered device, the app catalogue with the app will be opened in the browser, where the user can choose to install the app. The administrators are responsible for restricting the distribution of this URL to the intended users.	• iOS • macOS	NA (Tenant specific)
Set up a web clip as an app	Set up a **web clip** as an app in the app catalog to make the web application available in the app catalog for the users. The web clip can be defined as a configuration, but a configuration can only be pushed by the admin. Users can choose to install the web application on their devices or opt out, whereas users have no option to opt out of a web clip configuration.	iOS	NA (Tenant specific)
Turn on registration of Allowlisted devices	Allow device registration based on Allowlisted serial numbers in Users > **User Settings** > Default Device Registration Setting.	• iOS • macOS	NA (Tenant specific)
Certificate based authentication	**Certificate based authentication** feature allows administrators to log in using digital certificates and a tenant specified hostname or a vanity host name. This authentication setting can be configured using the Vanity Host configuration under the **Admin** tab.	This feature is not platform-specific.	NA (Tenant specific) This feature is only available on NA3 cluster environments, and only if enabled by Support.
Create a dedicated devices configuration (corporate-owned single-use, or COSU)	Administrators can configure dedicated devices that can be used for a specific purpose using Android enterprise using the Dedicated devices (corporate-owned single-use, or COSU configuration .The **COSU configuration** is distributed to Work Managed Devices (Device Owner mode) to provide only one app available to users in Kiosk mode.	Android Enterprise	Silver

Feature	Description	Platform(s)	Licence
Dashboard inactivity period	By default, the dashboard inactivity period is set to 15 days. This can be updated based on the tenant needs and to a maximum of 30 days. If you need a longer inactivity period, contact the **Support** team.	This feature is not platform-specific.	

4.5. Preparing for Android Enterprise device support

This section describes the minimum network requirements for Android Enterprise devices. Android devices generally do not require you to open inbound ports on the firewall in order to function correctly. However, there are a number of outbound connections that administrators need to be aware of when setting up their network environments for Android Enterprise devices.

The list of network changes provided in the following table is not exhaustive and may change. It covers known endpoints for current and past versions of enterprise management API and GMS apps.

> In addition to the ports listed in the following table, Android Enterprise devices require access to Ivanti Neurons for MDM.

For information about the requirements for Android Enterprise devices, see **Android Enterprise Network Requirements** from the Android Enterprise Help.

Google does not provide specific IPs, so you should allow your firewall to accept outgoing connections to all IP addresses contained in the IP block listed in Google's ASN of 15169 listed here **http://bgp.he.net/AS15169#_prefixes**.

> IPs of Google peers and edge nodes are not listed in the AS15169 blocks. See **https://peering.google.com/** for more information about Google's Edge Network.

5. Dashboard

The dashboard shows important statistics about registered devices and users. Each section on the dashboard is called a widget. For each widget, you define:

- the category of data displayed (such as devices or users)
- how the data is grouped (such as by OS build version or model)
- how the data is filtered (such as displaying only iOS devices or display by OS build version)
- how the data is displayed (such as pie chart or bar chart)

Verifying reports and other information

The **Dashboard** shows important statistics about registered devices and users. Each section on the dashboard is called a widget.

You can verify additional information as follows:

- Review notifications - Go to the Dashboard > Notifications page (or click the bell icon (top right) to review notifications and take actions where necessary.
- Reports - Go to the Dashboard > Reports page to access the data in your Unified endpoint management (UEM) system.
- Audit Trails - Go to the Dashboard > Audit Trails page to access the chronological set of records that capture activities performed on all entities within Ivanti Neurons for MDM. To enable this feature, go to the **Admin > Infrastructure >Audit Trails** page and click **Enable Audit Trails**.
- App Insights - Go to the **Dashboard > App Insights** page to view and analyse the app distribution and other app details.

This section contains the following topics:

- **Working with Widgets**
- **App Insights**
- **Using Scheduled Reports**
- **Using Custom Reports**

5.1. Working with Widgets

This section contains the following topics:

- Adding a widget
- Arranging the widgets
- Editing a widget
- Reviewing notifications
- Reports
- Audit Trails

The dashboard shows important statistics about registered devices and users. Each section on the dashboard is called a widget. For each widget, you define:

- the category of data displayed (such as devices or users)
- how the data is grouped (such as by OS version or model)
- how the data is filtered (such as displaying only iOS devices)
- how the data is displayed (such as pie chart or bar chart)

Adding a widget

1. Click **Add** (upper right).
2. Assign a name to the widget.
3. Select a data category.
4. Complete the filtering options as they display.
5. Select the default display type (pie chart, bar chart, line graph).
6. Click **Done**.

Arranging the widgets

Widgets always display three to a row. However, you can change the order in which the widgets are displayed:

1. Click **Arrange** (upper right).
2. Drag the boxes into the order in which the widgets should appear.
3. Click **OK**.

Editing a widget

1. Click the settings icon for the widget (upper right).
2. Select **Edit**.
3. Make your changes.
4. Click **Done**.

Reviewing notifications

Click the bell icon (top right) or go to **Dashboard > Notifications** page to review notifications and take actions where necessary based on the following criteria:

- Component Type
  - APP
  - LDAP
  - Entra ID
  - Device Allowlist
  - Apps and Books
  - iOS
  - Android
  - macOS
  - visionOS
  - watchOS
  - tvOS
  - Tenant
  - CA
  - Connector
  - Sentry
  - Device Enrollment Server Token

Notification Type

  - Expiration
  - Data Sync
  - Usage Limit
  - Admin Action
  - Server Authentication Error
  - Validation Error
  - Status Change

Severity

  - Cleared
  - Information
  - Critical
  - Warning

Admins can select the APP component to quickly review all app-specific notifications on the Notifications page and also in the bell notification section. If there are new permissions to be accepted for Google Play apps, then the admins can accept them upon clicking the notifications rather than visiting each app page to review and accept the permissions.

> Ivanti Neurons for MDM customers/tenants will get the Android Go app approval notifications even though the Android Go app is not imported into the App Catalog.

Reviewing user password expiration and ID change notifications

Admins can review the upcoming password expiration in the **Notifications** page. They are also notified of the password expirations from two weeks to one day in advance, including links to CSV report files containing the list of corresponding users. After the password expires, notifications will no longer be generated.

Admins can also review a notification that lists the users whose IDs (UIDs) were detected to have changed during the last LDAP sync.

Clearing a notification

You can manually clear these notifications of any severity whenever required from the **Notifications** page.

1. In the **Notifications** page, click on the icon in the **Actions** column for the notification you wish to clear. The **Confirm Clear Notification** window is displayed.
2. Click **Clear Notification**. When cleared, the status of notification changes to **Cleared** in the **Status** column.

> The total count of the notifications that are cleared are displayed in the **Notifications** page.

Reports

On the **Dashboard > Reports** page, you can access the data in your Unified endpoint management (UEM) system. For example, administrators can add information such as Device Space Name and Device Custom Attributes to reports using the corresponding filter option while creating Devices and Blocked Devices reports. Accordingly, these reports have columns for Device Space Name and Device Custom Attributes respectively. Custom Device Attributes are available under filtering options while creating a report. Administrators can pick from the list of custom device attribute keys used for devices and select the available operators.

Ivanti Neurons for MDMStarting with 76, the operators for all the report templates have standard operators. The operators of the following templates are standardized in this release:

- Dashboard> Reports> Create Report

The following is the workflow of a report:

1. Choose - select from a predefined report template.
2. Define Scope - set the period of time for report data.
3. Set Details - name and customise your report.
4. Run or schedule - run the report immediately or create a schedule.
5. Share - specify who will receive your report.

Related topics:

- **Dashboard > Reports (Scheduled)**
- **Dashboard > Reports (Custom)**

Quick Search: Navigate to the Reports tab. The quick search field lets you search from the following columns, it lets you search even if you include space or special characters:

- NAME
- DESCRIPTION
- TEMPLATE NAME

Audit Trails

Audit Trails provide a chronological record of activities performed in Ivanti Neurons for MDM. These records include actions performed by administrators, end users, and system components.

Administrators use **Audit Trails** to review changes, verify actions, troubleshoot issues, and support compliance checks. **Audit Trails** track actions such as adding, updating, and deleting managed entities, including devices. For more information, see **Device Registration (iOS, macOS, and Android)**.

Enabling Audit Trails

You need to enable the **Audit Trails** option to capture activities performed within Ivanti Neurons for MDM.

Procedure

1. Select Admin > Infrastructure > Audit Trails.
   The **Audit Trails** pane appears.
2. Select and set the **Audit Trails Export** toggle button to ON.

> Note: You will not be able to disable the Audit Trails feature after you enable it. To disable, contact Ivanti Support.

Viewing Audit Trails

Follow the steps to view more details about **Audit Trails**:

Procedure

1. Go to **Dashboard** > **Audit Trails**.

The **Audit Trails** pane appears.

2. The following tables lists the details that appear in the **Audit Trails** pane:

Setting	Description
Icon	Shows the activity icon for the audit event.
Activity	Shows the action that occurred, such as device check-in or admin login.
Status	Shows whether the activity was Successful or Failed. If a report fails, you can retry the report job from **Report History**. Use this option to rerun the failed job without creating a new report schedule.
Performed By	Shows the administrator or user who performed the activity.
Performed At	Shows the date and time when the activity occurred.
Performed On	Shows the device, account, or object affected by the activity.
Details	Shows additional information about the activity.
Type	Shows the activity type, such as Device Action or Account.
Category	Shows the functional area related to the activity, such as Device Management or Admin Portal Access.

3. Click the **Actions** button to perform the following options:

- **Configure Audit Trail Setting**: Select this option and it displays **Audit Trails** configuration in **Admin** > **Infrastructure** > **Audit Trails**.
- **Export to CSV**: Select this option to export and download the **Audit Trails**.

4. (Optional) You can use the **Filters** to view specific **Audit Trails**.

Activity Details View

The **Changes - Before & After** icon appears in the **Dashboard** > **Audit Trails** > **Details** column. It helps administrators compare attribute values before and after an audited action. This comparison makes it easier to identify what changed, verify user or system activity, and troubleshoot configuration updates.

Click the icon to view the audit trail comparison details in the **Audit Trails Changes - Before & After** pane and it displays the following details:

Setting	Description
Attribute	Displays the name of the modified attribute. For example, `createdAt`.
Before	Displays the attribute value before the action was performed. Highlights in Red colour.
After	Displays the attribute value after the action was performed. Highlights in Green colour.

Using Advanced Search for Audit Trails

Use the Advanced Search option to search audit trails based on rules. Define specific criteria to identify and view activities. You can use the following attributes to perform the search:

- **Activity**
- **Category**
- **Created At**
- **Performed By**
- **Performed On**
- **Space Name**
- **Status**
- **Type**

Creation of Reports for Audit Trails

You can schedule **Audit Trail** reports to run every 12 hours or 24 hours, or generate custom reports. Additionally, you can run **Audit Trail** reports on demand. On-demand reports are not scheduled and include **Audit Trail** data from the last 24 hours.

You can generate a Audit Trail report in one of the following formats:

- CSV
- JSON
- CEF

Additionally, while creating a report for **Audit Trail** > **Report Distribution**, you can select the **SFTP Export** option to export and upload all audit trail information to a specific server location. Audit Trail export uses Secure Shell File Transfer Protocol (SFTP). The server must be accessible through the default port. You can configure **Audit Trail Export** settings to automatically upload Audit Trail archives to a specific location daily. For more information, see **Exporting Audit Trails**.

For more information on creating a report, see **Using Scheduled Reports** and **Using Custom Reports**.

5.2. App Insights

This section contains the following topics:

- Viewing app distribution
- Viewing app details
- Adding single app distribution charts
- Adding an unmanaged iOS apps chart
- Adding top 10 installed managed apps
- Adding top 5 rated in-house apps

App Insights is a feature in the Dashboard that helps you to view and analyse the following app distribution:

- In-house app distribution requiring installation
- Public app distribution requiring installation
- Unmanaged iOS apps
- Top 10 installed managed apps
- Top 5 Rated In-House Apps

Analysis of top 5 apps requiring installation: These are In-House or Public apps that have been distributed to a large number of users but have proportionately low installation rates. The Unmanaged iOS apps chart provides information on the unmanaged apps on devices. You will have the ability to see the list of unmanaged apps, on what devices they are installed, and take action to convert the app to a managed app. These are the app distributions that require an administrator's attention or action to improve the distribution. These charts represent the devices that already have the app installed. The doughnut chart provides a high-level overview of the distribution of public and in-house apps which not only helps in analysing the number of devices requiring app installation, but also allows you to further drill down to get more app specific information by clicking on a specific region of the chart. Additionally, you can also add a single distribution chart that represent a version specific distribution for a single app.

> The dashboard only shows information about devices that are checked in the last 15 days.

Viewing app distribution

In the **Apps** page under **Dashboard**, you can view the following charts:

- In-house app distribution requiring install
- Public app distribution requiring install
- Unmanaged iOS apps

The charts for 5 in-house apps, 5 public and Unmanaged iOS apps are displayed by default. The graphs are ordered left to right starting with the app with the highest uninstalled rate.

The doughnut charts display 2 colours to represent the installation status. The blue colour represents the number of devices where the app is installed. The red colour represents the number of devices that requires installation. The count of devices are displayed if you hover over each colour region.

You can delete a chart by clicking the delete option on top right corner of the chart.

Viewing app details

The centre of the doughnut chart also displays the number of devices that requires installation. Example: 750/1000 which means 750 out of 1000 devices requires installation.

The doughnut charts display 3 colours to represent the distribution of the app.

- The blue colour represents represents the number of devices where the app is installed. Clicking the blue region in the chart navigates to the **Devices** page. In the **Devices** page, the **App Version** column displays the installed app version and the date when the app was installed.

> You can also view devices based on the installed app versions by selecting the options from the **Versions** section in the left panel.

- The red colour represents the number of devices requiring app installation. Clicking the red region in the chart navigates to the **Devices** page. In the **Devices** page, you can view devices that requires installation of the app.

An app icon is displayed in the centre of the chart. When the icon is clicked, it navigates to the app details page under **Apps> App Catalogue**.

In this page, click the **Devices with App installed** tab to view the list of devices for the selected app.

Click the **Devices without App installed** tab to view the list of devices not installed for the selected app.

Adding single app distribution charts

You can add a single distribution doughnut charts for a specific version of an app in the Apps page. The red colour represents the list of eligible devices that should have the app installed. These charts graphically represent the following details of the distribution of apps:

- Devices installed with a specified version of the app
- Devices installed with other versions of the app
- Devices that are not installed with the app

Procedure

1. Click **+Add** in the **Apps** page. The **Add App Chart** window is displayed.
2. In the **Chart type** drop-down list select **Single App Distribution**.
3. Select the checkbox for the list of apps for which you wish to view the single app distribution chart.

> Alternatively, you can search for a specific app by typing the app name in the Search for Apps field.

4. Click **Add Chart**. The single app distribution charts are displayed in the Apps page.

> You can select a maximum of 9 apps from the list.

The centre of the chart displays the number of devices that are installed with the specified app version.

Example: 5/10 which indicates that 5 out of 10 devices are installed with the specified app version.

The doughnut charts displays 3 colours to represent the distribution of the app.

- The green colour represents the number of devices where the specific version of the app is installed. Clicking the green region in the chart navigates to the **Devices** page that displays the list of devices installed with the specified version of the app. You can also view devices based on other installed app versions by selecting the options from the **AppVersion** section in the left panel.
- The light green colour represents the number of devices where other versions of the app is installed. Clicking the light green region in the chart navigates to the **Devices** page that displays the list of devices installed with other versions of the app. You can also view devices based on other installed app versions by selecting the version options from the **AppVersion** section in the left panel.
- The red colour represents the number of devices where the app is not installed. The count of devices are displayed if you hover over each colour region. Clicking the red region in the chart navigates to the **Devices** page where you can view the devices that are not installed with the app. The left panel also displays the date from when the app is available in the app catalogue.

An app icon is displayed in the centre of the chart. When the icon is clicked, it navigates to the app details page under **Apps> App Catalogue**. In this page, click the **Devices with App installed** tab to view the list of devices for the selected app. Click the **Devices without App installed** tab to view the list of devices not installed for the selected app.

You can delete a chart, by clicking the delete option on top right corner of the chart.

Adding an unmanaged iOS apps chart

You can identify and view the list of unmanaged apps by adding the unmanaged iOS apps chart to the Apps page. This chart appears automatically when an administrator adds an unmanaged iOS app to the catalogue. The administrator can delete or add this chart as needed.

Procedure

1. Click **+Add** in the **Apps** page. The **Add App Chart** window is displayed.
2. In the **Chart type** drop-down list select **Unmanaged iOS Apps**.
3. Click **Add Chart**. The unmanaged iOS apps chart is displayed in the **Apps** page.

The chart displays the number of apps in the app catalogue that are unmanaged. The bottom of the chart displays 3 columns with the following details:

- **Devices with unmanaged iOS apps** - Indicates the number of unmanaged iOS apps. Click the link to view the list of devices with unmanaged apps in the Devices with unmanaged iOS apps window.
- **Total apps in app catalogue** - Displays the total number of apps available in the app catalogue.
- **Unmanaged iOS apps (%)** - indicates the unmanaged iOS apps in percentage.

If an app is already installed from iTune App Store, you can convert the app and its data to a managed app. To convert such app to a mananged app:

1. Click the number link in the **Devices with unmanaged iOS apps column**. The **Unmanaged iOS apps** window is displayed.
2. Select one or more unmanaged apps from the list and click on the number link under unmanaged iOS apps. The selected apps will be converted to managed apps and the status will be updated in the next device check-in.

> You can export the data on the unmanaged apps in CSV format by clicking the **Export to CSV** link.

Adding top 10 installed managed apps

You can identify and view the list of top 10 installed managed apps using a Top 10 Installed Managed Apps chart in the Apps page. The administrator can delete or add this chart as and when required.

By default, Top 10 installed managed apps chart is available in **Apps** page. If the chart is deleted, the Admin can add it from the **Apps** page.

Procedure

1. Click **+Add** in the **Apps** page. The **Add App Chart** window is displayed.
2. In the **Chart type** drop-down list select **Top 10 Installed Managed Apps**.
3. Click **Add Chart**. The Top 10 Installed Managed Apps chart is displayed in the **Apps** page.

You can view the top 10 installed managed apps based on the category selected under the **Show** drop-down list. The available categories are:

- **All Apps** (selected by default)
- **In-House Apps**
- **Public Apps**

Each bar in the chart is displayed to represent each specific app and the name of the app is also displayed. Hover over each bar to view the platform (Android, iOS or Windows) and the number of devices installed with the app.

Clicking the bar of a specific app navigates to the **Devices** page that displays the details of the device(s) installed with the app. The left panel in the Devices page indicates the number of devices installed with the app. Clicking the X button in the left panel navigates back to the **Apps** page in the Dashboard.

You can delete the chart by clicking the delete option on the top right-hand corner of the chart.

Adding top 5 rated in-house apps

You can identify and view the list of top 5 rated In-house apps using the Top 5 Rated In-house Apps chart in the Apps page. The administrator can delete or add this chart as and when required.

By default, the Top 5 Rated In-house apps chart is available in **Apps** page. If the chart is deleted, the Admin can add it from the **Apps** page.

Procedure

1. Click **+Add** in the **Apps** page. The **Add App Chart** window is displayed.
2. In the **Chart type** drop-down list select **Top 5 Rated In-house Apps**.
3. Click **Add Chart**. The Top 5 Rated In-house Apps chart is displayed in the **Apps** page.

This chart represents the data via a logo for the App, with the star rating for that App. The star rating is represented by star images, along with the integer representation (maximum rating as 5). The number of users who have rated the App is also displayed.

> The number of ratings for an app is not just devices restricted to that administrator and space but its is based on ratings from all users of the app. The rating is the average of all the ratings for that app given by different users who viewed that app from Apps@Work on their registered devices.

Clicking the specific app navigates to the **App details** page that displays specific details of the app.

You can delete the chart by clicking the delete option on the top right-hand corner of the chart.

5.3. Using Scheduled Reports

Licence: Silver

The Scheduled Reports feature enables you to schedule and generate reports on various metrics with pre-packaged templates ready to use. You must have the System Administrator or the System Read Only role to access this feature. You can currently create a maximum of 40 reports.

> The Policy Violations report might have multiple records for the same device if the device has multiple Tunnel instances created for it. This is applicable for both Standard reports as well as Custom reports.

Generating a Report

You can schedule and generate a report.

Procedure

1. Go to **Dashboard** > **Reports**.
2. Click **Create a report** to display the Choose a Report Template page.
3. Choose a template for your report from the options you have configured.
   - **Blocked Device**s - Report on devices currently blocked access by Sentry.
   - **Devices** - Report on devices from all partitions in your system.
   - **Policy Violations** - Report on policy violations in your system.
   - **Users** - Report on users in your system
   - **User Password Expiry Status** - Report on password expiry status of the users in your system.
   - **Most Installed Apps** - Report on all applications in your system, sorted on the number of times each application has been installed.
   - **Unmanaged Apps** - Report on the unmanaged applications in your system.
   - **All Applications** - Report on all applications in devices managed by you.
   - Audit Trails keeps track of all the activities performed on all entities within Ivanti Neurons for MDM.
4. Click **Next**.
   The **Report Details** page is displayed.
   - Enter a **Report Name**.
   - (Optional) Enter a **Description** for the report.

Select the **Event Range** from the following options:
For existing reports:

- **All Events**
- **Previous Day**
- **Previous Week**
- **Previous Month**
- **Previous Range** - Displays the report that was created using the range slider from the previous release of Ivanti Neurons for MDM administrative portal. If the administrator selects and saves any one of the above options for a

report, the Previous Range option will not be displayed. The range value is visible on the Report Summary page.

For new reports:

- **All Events**
- **Previous Day**
- **Previous Week**
- **Previous Month**

Click **Next**. The Report Data page is displayed.

6. Click **Customise Columns** to add, remove, or reorder columns in the **Report Columns** section. Alternatively, click the column name to remove the added column.
7. (Optional) Use the **Select all columns** check box to select all the displayed columns in the list.
8. Click **Restore Defaults** to revert to the previously generated columns. To revert to the columns without any customisations, you can choose one of the templates from the **Choose a Report Template** page.
9. Create filters based on specific rules in the **Advance Filter** section.

> All filter options are not available for all reports. For more information about the list of available filters, see the **Filters** topic below this procedure.

> The following new hardware attributes are available for Windows devices when creating Reports - BitLocker Encryption, OS Edition, System Version, Motherboard Manufacturer, Motherboard Product, Motherboard Status, BIOS Manufacturer, BIOS Version, Hard Drive Partitions, Optical Drive Type, CPU Name, and CPU Status.

10. (Optional) you click the **+** icon to add another rule or click the **Add Group** icon to add another group of rules.
11. Click **Next**. The Report Schedule page is displayed.
12. Select *one* of the following formats for downloading the report:
    - CSV
    - PDF
    - **CSV and PDF**
      For PDF report files, up to 10 columns are allowed. In the Report Charts section, two types of charts that will be included in the PDF reports are displayed.
      All Applications report supports only the CSV format.

Click **Auto Schedule** to setup a report to run automatically by setting up the recurrence. Alternatively, click **Manual** to run the report once and it will be sent in an email.

- Select *one* of the **Recurring Report** options:
  - **Daily**
  - **Weekly**
  - **Monthly**
  - **Previous Schedule** - For existing reports
- Select the **Start Date** and the **End Date** (Optional).

14. Click **Next**. The Report Distribution page is displayed. Select the recipients of the report.

15. (Optional) add external email IDs by clicking the **Add External Email** link.
16. Click **Done**. The **Report DistributionSummary** appears.
17. (Optional) click **Edit** to modify your report.
18. Click **Save**.
19. Click the download icon to select the format of the report. An email containing a **Download Report** button to download the report is sent to the recipients of the report.

Filters

Rule Options	Description
Activation Lock Enabled	Rules based on activation lock enabled as **Yes** or **No**. Rule Example: 'Activation Lock Enabled is equal to Yes'.
App Tunnel Status	Rule for app tunnel status as **BLOCK** or **ALLOW**. Rule Example: 'App Tunnel Status is equal to Block'.
Battery level	Value of the battery level of the device. Rule Example: 'Battery Level is equal to 1,080' The value entered for the battery level should be in seconds.
Client Last Checkin	Rule based on client last checkin within the date range. Rule Example: 'Client Last Checkin is in range 02/04/2019 06:00:00,05/04/2019 17:00:00'.
Compliance State	Rule based on compliance state as **Yes** or **No**. Rule Example: 'Compliance State is equal to Yes'.
Current Country Name	Enter the current country name. Rule Example: 'Compliance State is equal to France'.
Current MCC	Rule based on current Mobile Country Code. Rule Example: 'Current MCC is equal to 410'.
Current MNC	Rule based on current Mobile Network Code. Rule Example: 'Current MNC is equal to 06'.
Device Enrollment Enabled	Rule based on Device Enrollment enabled as **Yes** or **No**. Rule Example: 'Device Enrollment Enabled is equal to Yes'
Anti-phishing Native Status	Select any of the following Anti-phishing Native Status options: • is equal to • is not equal to Possible values are: • Not Enabled • N/A • Enabled • Unknown
Anti-phishing VPN Status	Select any of the following Anti-phishing VPN Status options: • is equal to • is not equal to Possible values are: • Not Enabled • N/A • Enabled

Rule Options	Description
	• Unknown
Enrolled in Device Enrollment	Rule based on Enrolled in Device Enrollment as **Yes** or **No**. Rule Example: 'Enrolled in Device Enrollment is equal to Yes'
Data Protection	Indicates whether the data protection is enabled on the device. Possible values are **Yes** or **No**. Rule Example: 'Data Protection is equal to Yes'.
Data Roaming Enabled	Rule based on data roaming enabled as **Yes** or **No**. Rule Example: 'Data Roaming Enabled is equal to Yes'
Device Block Status	Rule based on device block status. Rule Example: 'Device Block Status is equal to Block'
Device ID	Rule for a specific Device ID or a within a range of Device IDs. Rule Example: 'Device ID is greater than 45'. x
Home MCC	Rule based on home Mobile Country Code. Rule Example: 'Home MCC is equal to 310'.
Home MNC	Rule based on home Mobile Network Code. Rule Example: 'Home MNC is equal to 510'.
IMEI	Rule for a specific IMEI value. Rule Example: 'IMEI begins with 9900'
Invite State	Select any of the following Invite State options: • None • Pending • Expired • **Completed** Rule Example: 'Invite State is equal to Pending'.
Locator Service Enabled	Rule based on Locator service enabled as **Yes** or **No**. Rule Example: 'Locator Service Enabled is equal to Yes'
MTD Activation Status	Select any of the following MTD Activation Status options: • is equal to • is not equal to Possible values are: • N/A • Error • Pending • Protected

Rule Options	Description
Quarantine Status	Rule based on Locator service enabled as **Yes** or **No**. Rule Example: 'Quarantine Status is equal to Yes'
Registered At	Rule to select the date and time range from when the device was registered. Rule Example: 'Registered At is in range 03/10/2017 09:00:00, 20/10/2017 17:00:00'.
Roaming	Rule based on roaming as **Yes** or **No**. Rule Example: 'Roaming is equal to Yes'
Status	Select any of the following Invite Status options: • Active • Retire Pending • Retire Sent • Retired • Retire Cancelled • Wipe Pending • Wipe Sent • Wiped • Wipe cancelled Rule Example: 'Status is equal to Retire Pending'.
Voice Roaming Enabled	Rule based on voice roaming enabled as **Yes** or **No**. Rule Example: 'Voice Roaming Enabled is equal to Yes'
Wifi Mac Address	Enter a specific Mac address value. Rule Example: 'Wifi Mac Address is not equal to 00-14-22-01-23-45'.
iCloud Backup Enabled	Rule based on iCloud Backup enabled as **Yes** or **No**. Rule Example: 'iCloud Backup Enabled is equal to Yes'
iTunes Store Account Activation Status	Rule based on iTunes Store Account Activation Status as **Yes** or **No**. Rule Example: 'iTunes Store Account Activation Status is not equal to No'.
Platform Type	Applicable for All Applications report.
Source	Applicable for All Applications report.
Custom Attributes	Applicable for All Applications report.
Managed	Applicable for All Applications and Most Used Applications report.
App Identifier	Is default for All Applications report.
Meid	Applicable for Unmanaged Apps report.

Performing Actions on a Report from the Scheduled Reports page

You can perform various actions from the Scheduled Reports page.

Procedure

1. Go to **Dashboard** > **Reports**.
2. In the **My Scheduled Reports** page, click the **Actions** drop-down menu, and select one of the following options:

Actions Options	Action Performed
View	Lets you view the report.
Edit	Lets you edit the report. The report also lets you view the range that was selected in the last release as Previous Range.
Run Now	Runs the report.
Download CSV	Downloads the report in CSV format.
Download PDF	Downloads the report in PDF format.
Delete	Deletes the report.

Viewing report details

You can view the report details and perform some actions on the created report.

Procedure

1. Go to **Dashboard** > **Reports**.
2. In the **My Scheduled Reports** page, click the report name to view the report details. The report page opens.
3. You can view the Report Summary and Report History on this page.

Related topics:

- To assign a custom role to a user, see **Assigning Roles**.
- See **User Roles** for a list of default roles.
- **Roles Management**
- **Using Custom Reports**

5.4. Using Custom Reports

Licence: Gold

The custom reports feature enables you to customise and generate reports on various metrics with templates ready to use. You must have the System Administrator or the System Read Only role to access this feature. You can currently create a maximum of 40 reports.

This section contains the following topics:

Generating a report

Performing Actions on a Report

Viewing report details

Generating a report

You can schedule and generate a report from the Ivanti Neurons for MDM administrative portal.

Procedure

1. Go to **Dashboard** > **Reports**.
2. Click **Create a report** to display the Choose a Report Template page.
3. Choose a template for your report from the options you have configured.
   - **Blocked Devices** - Report on devices currently blocked access by Sentry.
   - **Devices** - Report on devices from all partitions in your system.
   - **Policy Violations** - Report on policy violations in your system.
   - **Users** - Report on users in your system
   - **User Password Expiry Status** - Report on password expiry status of the users in your system.
   - **Most Installed Apps** - Report on all applications in your system, sorted on the number of times each application has been installed.
   - **Unmanaged Apps** - Report on the unmanaged applications in your system.
   - **All Applications** - Report on all applications in devices managed by you.
   - Audit Trails keeps track of all the activities performed on all entities within Ivanti Neurons for MDM.
4. Click **Next**. The Report Details page is displayed.
5. Enter a **Report Name**.
6. (Optional) Enter a **Description** for the report.
7. Select the **Event Range** from the following options:
   For existing reports:
   - **All Events**
   - **Previous Day**
   - **Previous Week**
   - **Previous Month**
   - **Previous Range** - Displays the report that was created using the range slider from the previous release of Ivanti Neurons for MDM administrative portal. If the administrator selects and saves any one of the above options for a

report, the Previous Range option will not be displayed. The range value is visible on the Report Summary page.

For new reports:

- **All Events**
- **Previous Day**
- **Previous Week**
- **Previous Month**

Click **Next**. The Report Data page is displayed.

9. Click **Customise** to generate a custom report:

> In the **Dashboard > Reports** page, the Template Name column will display "custom" in brackets to indicate that the report is customised.

10. Click **Customise Columns** to add, remove, or reorder columns in the **Report Columns** section. Alternatively, click the column name to remove the added column.
11. (Optional) Use the **Select all columns** check box to select all the displayed columns in the list.
12. Click **Restore Defaults** to revert to the previously generated columns. To revert to the columns without any customisations, you can choose one of the templates from the **Choose a Report Template** page. The default columns are indicated with a lock icon.
13. Create filters based on specific rules in the **Advance Filter** section.

> All filter options are not available for all reports. For more information about the list of available filters, see the **Filters** topic below this procedure.

> The following new hardware attributes are available for Windows devices when creating Reports - BitLocker Encryption, OS Edition, System Version, Motherboard Manufacturer, Motherboard Product, Motherboard Status, BIOS Manufacturer, BIOS Version, Hard Drive Partitions, Optical Drive Type, CPU Name, and CPU Status.

14. (Optional) you click the **+** icon to add another rule or click the **Add Group** icon to add another group of rules.
15. Click **Next**. The Report Schedule page is displayed.
16. Select *one* of the following formats for downloading the report:
    - **CSV**
    - **PDF**
    - **CSV and PDF**
      For PDF report files, up to 10 columns are allowed. In the Report Charts section, the two types of charts that will be included in the PDF reports are displayed.
      All Applications report supports only the CSV format.

Click **Auto Schedule** to setup a report to run automatically by setting up the recurrence. Alternatively, click **Manual** to run the report once and it will be sent in an email.

- Select *one* of the **Recurring Report** options:
  - **Daily**
  - **Weekly**

    - **Monthly**
    - **Previous Schedule** - For existing reports
  - Select the **Start Date** and the **End Date** (Optional).

> The Run Now option will generate a one-time report. You can use the same template to generate scheduled reports. In the **Dashboard > Reports** page, the Frequency and Next Scheduled columns will display Unscheduled status for these reports.

18. Click **Next**. The Report Distribution page is displayed. Select the recipients of the report.
19. (Optional) add external email IDs by clicking the **Add External Email** link.
20. Click **Done**. The **Report DistributionSummary** appears.
21. (Optional) click **Edit** to modify your report.
22. Click **Save**.
23. Click the download icon to select the format of the report. An email containing a **Download Report** button to download the report is sent to the recipients of the report.

Filters

Rule Options	Description
Activation Lock Enabled	Rules based on activation lock enabled as **Yes** or **No**. Rule Example: 'Activation Lock Enabled is equal to Yes'.
App Tunnel Status	Rule for app tunnel status as **BLOCK** or **ALLOW**. Rule Example: 'App Tunnel Status is equal to Block'.
Battery level	Value of the battery level of the device. Rule Example: 'Battery Level is equal to 1,080' The value entered for the battery level should be in seconds.
Client Last Checkin	Rule based on client last checkin within the date range. Rule Example: 'Client Last Checkin is in range 02/04/2019 06:00:00,05/04/2019 17:00:00'.
Compliance State	Rule based on compliance state as **Yes** or **No**. Rule Example: 'Compliance State is equal to Yes'.
Current Country Name	Enter the current country name. Rule Example: 'Compliance State is equal to France'.
Current MCC	Rule based on current Mobile Country Code. Rule Example: 'Current MCC is equal to 410'.
Current MNC	Rule based on current Mobile Network Code. Rule Example: 'Current MNC is equal to 06'.
Device Enrollment Enabled	Rule based on Device Enrollment enabled as **Yes** or **No**. Rule Example: 'Device Enrollment Enabled is equal to Yes'
Anti-phishing Native Status	Select any of the following Anti-phishing Native Status options: • is equal to • is not equal to Possible values are: • Not Enabled • N/A • Enabled • Unknown
Anti-phishing VPN Status	Select any of the following Anti-phishing VPN Status options: • is equal to • is not equal to Possible values are: • Not Enabled • N/A • Enabled

Rule Options	Description
	• Unknown
Enrolled in Device Enrollment	Rule based on Enrolled in Device Enrollment as **Yes** or **No**. Rule Example: 'Enrolled in Device Enrollment is equal to Yes'
Data Protection	Indicates whether the data protection is enabled on the device. Possible values are **Yes** or **No**. Rule Example: 'Data Protection is equal to Yes'.
Data Roaming Enabled	Rule based on data roaming enabled as **Yes** or **No**. Rule Example: 'Data Roaming Enabled is equal to Yes'
Device Block Status	Rule based on device block status. Rule Example: 'Device Block Status is equal to Block'
Device ID	Rule for a specific Device ID or a within a range of Device IDs. Rule Example: 'Device ID is greater than 45'. x
Home MCC	Rule based on home Mobile Country Code. Rule Example: 'Home MCC is equal to 310'.
Home MNC	Rule based on home Mobile Network Code. Rule Example: 'Home MNC is equal to 510'.
IMEI	Rule for a specific IMEI value. Rule Example: 'IMEI begins with 9900'
Invite State	Select any of the following Invite State options: • None • Pending • Expired • **Completed** Rule Example: 'Invite State is equal to Pending'.
Locator Service Enabled	Rule based on Locator service enabled as **Yes** or **No**. Rule Example: 'Locator Service Enabled is equal to Yes'
MTD Activation Status	Select any of the following MTD Activation Status options: • is equal to • is not equal to Possible values are: • N/A • Error • Pending • Protected

Rule Options	Description
Quarantine Status	Rule based on Locator service enabled as **Yes** or **No**. Rule Example: 'Quarantine Status is equal to Yes'
Registered At	Rule to select the date and time range from when the device was registered. Rule Example: 'Registered At is in range 03/10/2017 09:00:00, 20/10/2017 17:00:00'.
Roaming	Rule based on roaming as **Yes** or **No**. Rule Example: 'Roaming is equal to Yes'
Status	Select any of the following Invite Status options: • Active • Retire Pending • Retire Sent • Retired • Retire Cancelled • Wipe Pending • Wipe Sent • Wiped • Wipe cancelled Rule Example: 'Status is equal to Retire Pending'.
Voice Roaming Enabled	Rule based on voice roaming enabled as **Yes** or **No**. Rule Example: 'Voice Roaming Enabled is equal to Yes'
Wifi Mac Address	Enter a specific Mac address value. Rule Example: 'Wifi Mac Address is not equal to 00-14-22-01-23-45'.
iCloud Backup Enabled	Rule based on iCloud Backup enabled as **Yes** or **No**. Rule Example: 'iCloud Backup Enabled is equal to Yes'
iTunes Store Account Activation Status	Rule based on iTunes Store Account Activation Status as **Yes** or **No**. Rule Example: 'iTunes Store Account Activation Status is not equal to No'.
Platform Type	Applicable for All Applications report.
Source	Applicable for All Applications report.
Custom Attributes	Applicable for All Applications report.
Managed	Applicable for All Applications and Most Used Applications report.
App Identifier	Is default for All Applications report.
Meid	Applicable for Unmanaged Apps report.

Performing Actions on a Report

You can perform various actions from the Scheduled Reports page.

Procedure

1. Go to **Dashboard** > **Reports**.
2. In the **My Scheduled Reports** page, click the **Actions** drop-down menu, and select one of the following options:

Actions Options	Action Performed
View	Lets you view the report.
Edit	Lets you edit the report.
Run Now	Runs the report.
Download CSV	Downloads the report in CSV format.
Download PDF	Downloads the report in PDF format.
Delete	Deletes the report.

Viewing report details

You can view the report details and perform some actions on the created report.

Procedure

1. Go to **Dashboard** > **Reports**.
2. In the **My Scheduled Reports** page, click the report name to view the report details. The report page opens.
3. Select one of the following options

Actions Options	Action Performed
Toggle	Lets you enable or disable the report.
Run Now	Runs the report.
View	Lets you view the report details. Use the Actions drop-down menu to perform any of the following tasks: • **Disable** • **Download latest CSV/PDF** (based on the type of report selected be it CSV, PDF, or CSV & PDF, its shows the Download option) • **History** • **Delete**
Delete	Deletes the report.

Related topics:

- To assign a custom role to a user, see **Assigning Roles**.
- See **User Roles** for a list of default roles.

- Roles Management
- Using Scheduled Reports

6. Users

Before you invite someone to register mobile devices, you need to create a user entry for that person. You also need to create a user for anyone who will use Ivanti Neurons for MDM to help manage devices or publish content (administrators).

This section contains the following topics:

- User Groups
- User Settings
- User Branding
- User Enrollment with Apple Business Manager
- Account driven User Enrollment
- User Licences
- Managing Users

6.1. Adding Users

This section contains the following topics:

- Adding Users
- Adding multiple users
- Adding multiple users by uploading a file
- Adding an administrator
- Nobody user
- Viewing the device registration PIN information

You can add a single user or several users at a time. Once you have added many users, you might want to filter the display to show only the ones you are interested in.

Other things you can do with users in this page include:

- assign to/ remove from a user group
- send a message
- invite to register
- assign roles
- change a password
- delete
- generate a pin

All Device owner profiles are assigned a device account. Device accounts do not have any restrictions in the number of devices assigned to it. Work profiles (employee owned) are assigned user accounts.

Adding a user

Procedure

1. Go to **Users**.
2. Click **+ Add** (top right).
3. Select **Single User**.
4. Complete the form with the user's information:
    - email address (required)
    - Forename
    - Surname

> The Username field displays the email address you entered. In most cases, you should not edit this default. For more information, see When to Edit a Username

    - Display Name

> If you want to change the display name for this user, edit the default text in the **Display Name** field.

5. If you want to assign a password, enter it in the **Password** and **Confirm Password** fields.
    - If you assign a password, you need to communicate it to the user for device registration.
    - If you do not assign a password, the user will need to create a password during device registration.
6. Select **Locale** from the drop-down list.
7. Enter **Managed Apple ID**. You can include "appleid" as a subdomain for Managed Apple ID to avoid any conflicts with existing Apple IDs. For example, user@appleid.yourdomain.com. The subdomain has to be a valid verified subdomain on Apple Business Manager.

> The account cannot be updated with a different Managed Apple ID if there is an active User Enrolled device with the current account's Managed Apple ID.

(Optional) Assign one or more user groups. Managed Apple ID cannot be updated when there is a device with status "Active" and "Retire Pending."

10. If you want to set up other features before inviting this user, clear the **Send this invitation now** option. Otherwise, the invitation email will be sent when you click **Done**.
11. Click **Done** to add the user.

For Android devices, Device accounts are designed for single-use managed devices where a single local service account can be used to enrol a large number of devices. While creating a new user, the Android enterprise device Account available under **Admin > Google > Android Enterprise** must be enabled. Device Accounts are enabled by default (Instead of User Accounts) for Device Owner Managed Google Play Account enrollments.

Select the checkbox **Android enterprise device Account** to enable Android Enterprise work managed device enrollments attached to this account to be automatically assigned a Google Device Account.

While editing a local or LDAP user for Android devices, the Android Enterprise Device Owner Managed Google Play Account devices associated with the user will be assigned Device Accounts on the next device check-in, provided the following conditions are met:

- The feature is enabled by selecting the checkbox **Android Enterprise Device Account**.
- The Go App version on the Android device is 47 and above.

Adding multiple users

Procedure :

1. Go to **Users** .
2. Click **+ Add** (top right).
3. Select **Multiple Users**.
4. By default, you can enter email addresses **Manually** . Type or paste the email addresses of the users, separated by commas.
5. Example: jdoe@mycompany.com, jsmith@mycompany.com, tjones@mycompany.com
   If you want to set up other features before inviting this user, clear the **Send this invitation now** option.
6. Otherwise, the invitation email will be sent when you click **Done**.
   Click **Done** to add the users.

Adding multiple users by uploading a file

Procedure:

1. Go to **Users**.
2. Click **+ Add** (top right).
3. Select **Multiple Users**.
4. Select **Upload CSV**.
5. Click **Download CSV Template**.
6. Edit the template with the following information for each user:
    - user ID (required)
    - email address (required)
    - password
    - first name
    - surname
    - display name
    - user groups
    - custom attributes
7. This is the same information you enter when **adding a single user**. Do not exceed 10,000 entries in the file.
   Save the file.
8. Drag it to the upload area or select **Upload CSV** to select the file.
9. Once the uploaded user information is displayed, make any necessary edits.
10. Click **Next** (lower right).
11. If you do not want to send invitations right away, select **Do not send invitations** .
12. Click **Done**.

Adding an administrator

Procedure :

1. Click **Add** (top right).
2. Select **Single User** .
3. Complete the form with the user's information:
    - Email Address
    - Forename
    - Surname
4. The **Username** field displays the email address you entered.
   If you want to change the display name for this user, edit the default text in the **Display Name** field.
5. Assign a password in the **Password** field.
6. Enter the password again in the **Confirm Password** field.
7. Click **Done** to add the user.

8. Communicate the password to the person who will help manage devices.

Nobody user

The nobody user is a default user that cannot be deleted. The service applies this user to devices that do not have associated users, such as retired devices.

Viewing the device registration PIN information

While adding new users, the generated registration PIN information is displayed to admins if the Device Registration Authentication Type is set to PIN Only. This information can be useful to assist users with device enrolments.

- For single users, the PIN is displayed via the **Users > Invite User to Register** action and also in the PIN Info section of the User Details page.
- For multiple users, the PINs are displayed as a column in the User List page in addition to the PIN Status (Valid or Expired), PIN Issued, and PIN Expires columns.

If you cannot perform tasks on the **Users** page, it might be that you do not have the required permissions. You need one of the following **roles** :

- System Management
- User Management

6.2. User Groups

This section contains the following topics:

- Creating a dynamically managed user group
- Creating a manually managed user group
- Creating a user group from one of the duplicate user groups
- Creating a user group by CSV file upload

Create a user group so that you can assign apps and roles to multiple users. For example, you might create a Managers group if you want all department managers to be administrators for apps and content.

You can create a user group to be managed in one of the following methods:

- **Dynamically Managed (Most Common):** Local and LDAP users are added/removed to/from a group dynamically based on certain rules and/or attributes.
- **Manually Managed (Limited purpose):** Add/remove users to/from a group manually. Manually managed groups are recommended only for testing purposes that require less permissions.

You can enter text in the **Search** field to display a list of all user groups whose names start with the entered text.

- The search results are displayed as a list of possible matches in real-time while text is being entered.
- Select the desired user group name from the list of possible matches for subsequent action.
- The search match is case insensitive.

Creating a dynamically managed user group

> The following procedure is not applicable to Dynamic User Groups.

Procedure

1. Click **+Add**.
2. Enter a user group name in the **Name** field.
3. (Optional) Click **Add Description** to add a description for the user group.
4. Click the **Dynamically Managed (Most Common)** option.
5. Set rules and/or attributes as per your requirements. The following are the available rule options:
    - Custom LDAP Attribute
        - msExchPoliciesIncluded
        - msExchMailboxGrid
        - mailNickname

    Default LDAP Attribute

        - samAccountName
        - userPrincipalName

    Default User Attribute

- email_address
- distinguished_name
- last_name
- display_name
- first_name
- User Group
- Custom User Attribute

User Group DN

- User Group GUID
- User Group Name

6. For each rule, select between local and LDAP users. You can include or exclude a sub-group by using the **User Group** filter criteria.
7. Add more rules by clicking the plus icon.
   You can set **ANY** or **ALL** conditional filters for the added rules.
8. Create a group of rules by clicking the hierarchical icon next to the plus icon.
9. Review the user group's rules and attributes in the text query displayed below the rules selection options.
10. In the **Results** section, review the user(s) details that match the configured criteria. When you add or modify a rule or an attribute you can observe that the matching users are displayed, if they exist.
11. Click **Save** to save the configured user group.

Creating a manually managed user group

1. Click **+Add**.
2. Enter a group name.
3. (Optional) Click **Add Description** to add a description.
4. Select the **Manually Managed (Limited purpose)** option.
5. In the **Search Users** field, type the email address of each user to be included in the group.
   As you type, the matching users are found and displayed, if they exist.
6. Select the users you wish to add to the group. You may search and add more users as required.
7. Click **Save**.

> Note: You can create a manually managed user group and then add this group to a dynamically managed user group. In such a scenario, editing the manually managed user group does not break the dynamically managed user group rule. You will not be able to delete a manually managed user group if it is added to a dynamically managed user group.

Creating a user group from one of the duplicate user groups

Starting from Neurons for MDM 127 the Administrator portal displays the number of duplicate user groups and the corresponding number of GUIDs to identify duplicate groups, when the "User Group Name" attribute is selected in the rule builder. Also, a table under this rule displays the list of the duplicate user groups and their details such as User Group Name, GUID, Source and distinguished name (DN).

Procedure

1. Log in to the Ivanti Neurons for MDM Administrator portal.
2. Go to **Users**, **User Groups**.
3. Click **+Add**. The Create User Group wizard opens.
    1. Specify the name in the **Name** field.
    2. Select **User Group Name** from the rule builder, select **is equal to**, select *one* of the duplicate group names.
    3. Click the **+** plus icon to add more rules.
    4. Select **User Group GUID**, **is equal to**.
    5. Copy and paste the GUID from the table that displays the list of duplicate user group names and GUIDs. The result displays the associated users who will be added to the new group.
    6. Click **Save**. The listed users are now added to the new user group that you created.

If you cannot perform tasks on the **Users Groups** page, it might be that you do not have the required permissions. You need one of the following **roles**:

- System Management
- User Management

Creating a user group by CSV file upload

The newly added function allows the administrators to create user groups and add users to the created groups using a CSV file.

Procedure

1. Log in to the Ivanti Neurons for MDM Administrator portal.
2. Go to **Users**, **User Groups**.
3. Click **+Add**.
4. Select **Import User Groups from CSV**. The Import User Group wizard opens.
    1. In the Download CSV section, click **Download CSV Template** to download the CSV template. Using the template, you can edit the file to create user groups and add the users to the new/existing user groups.
    2. After editing and saving the CSV file, click **Choose a file** to upload the CSV file.
    3. Click **Upload**. A confirmation on the successful upload is displayed.

Property	Description
CSV File Size Limitation	The maximum size of the CSV file for import is limited to 2MB.
CSV File Format Requirements	CSV files should contain exactly 2 columns: accountUid and groupName. • Both accountUid and groupName values are mandatory. • Records failing to meet these criteria will be discarded during import. Admins can download a sample CSV file from the import section for reference.
Error Handling During Import	If errors or failures occur during CSV import, an error file will be generated. • Admins can download this error file to review failed CSV rows and understand the reasons for failure. • The error file includes the specific CSV row that failed and provides an explanation for the failure.
Successful Import Conditions	Importing users to user groups is successful only when the user group is local and manually managed. • The user must exist in the system for the import to be successful.

Conditions for Creating an User Group and Adding an User with a sample CSV file

Sample CSV file details-

accountUid: test_user_1@org.com

groupName: test_group_1

Conditions	Description
Existing Group	If the group test_group_1 already exists, the user test_user_1@org.com will be associated with the group.
Non-Existing Group	If the group test_group_1 does not exist, a new group with the name test_group_1 will be created, and the user test_user_1@org.com will be associated with the group.
Non-Local Group	If the group test_group_1 exists but is not a local group, this record will be included in the error CSV file with the reason 'Group is not Local.'
Non-Manually Managed Group	If the group test_group_1 exists but is not a manually managed group, this record will be included in the error CSV file with the reason 'Group is not manually managed.'
Non-Existing User	If the user test_user_1@org.com does not exist, this record will be included in the error CSV file with the reason 'User not found.'
Non-Existing User and Group	If both the user test_user_1@org.com and the group test_group_1 do not exist, a new group with the name test_group_1 will be created, and this record will be included in the error CSV file with the reason 'User not found.'

6.3. User Settings

This section contains the following topics:

- Editing the default setting
- Adding a custom setting
- Deleting a custom setting
- Configuring the settings for new device registrations
- Configuring the device limit per user
- Configuring the device wipe limit
- User Settings
- Configuring the Self Service Portal authentication
- Setting the password complexity
- Defining the terms of service
- Configuring the User Invite reminder emails
- Configuring User Registration Confirmation emails
- Configuring User Work Schedule setting
- Configuring Admin Portal authentication setting

User settings define device registration options. There are several types:

- **Device Registration Setting**: Sets authentication by password, PIN, or both; Apple Enrollment type, and device ownership.
  - Previously, if you setup SAML auth/IdP, SAML authentication is used for both device registration and portal authentication.
  - **Platform Device Registration Settings** - Administrators can now control device enrollment at the operating system level by restricting specific Apple, Android, and Windows platforms from registering with the system. This new OS-level restriction setting is applied as a parent enrollment control, and when enabled for a platform, related registration restrictions for that platform are automatically disabled. This helps organizations enforce enrollment policies and prevent unsupported device platforms from being registered.

Device Limit Setting: Sets the number of devices a user can register.

- **Wipe Limit Setting**: Sets the limit for the maximum number of devices that can be wiped at a time.
- **Self Service Portal Authentication Setting:** Set the password authentication type for the self-service portal.
- **Password Complexity Setting**: Set password complexity and policy parameters for local accounts used for device registration, and access to Admin Portal and Self Service portals.
- **Terms of Service Setting**: Sets the terms of service displayed to the user for each device registration.
- **User Invite Reminder Setting:** Sets the dates and frequency to send User Invite reminder emails.
- **User Registration Confirmation Setting:** Controls the ability to send the User Registration Confirmation email. See Configuring and using registration confirmation emails for an overview of the solution and Configuring User Registration Confirmation emails below for specific user settings instructions.
- **User Work Schedule Setting:** Controls the ability to configure a user work schedule that blocks all communication from Sentry to managed devices during the prescribed non-working hours. Useful for locales with Right-to-Disconnect laws.

- **Admin Portal Auth Setting:** Controls whether Ivanti Neurons for MDM prompts the admin for password only, or password and PIN.

You can edit the default settings for the **All Users** group or add custom settings and assign them to other user groups.

Editing the default setting

Click the **Edit** link for the setting that has the lock icon. You cannot delete a default setting.

Adding a custom setting

Click the **Add setting for specific user groups** link.

Deleting a custom setting

Click the X icon.

Configuring the settings for new device registrations

You can configure minimum OS version, authentication type, and device ownership for new device registrations. The device enrollment URL generated in earlier versions of Ivanti Neurons for MDM will cease to work with the current version. The administrator will need to regenerate the device enrolment URL for device registration.

Allowlist device registration

The option to Allowlist device registration is available only in default user settings and not available for custom user settings. You can upload a CSV file using the template containing serial numbers and custom device attributes which are used to Allowlist a few devices. You can include one or more existing custom device attributes to create the Allowlist. This will enable you to assign attributes to device groups or spaces after registration.

To create custom attributes, go to **Admin >** Attributes. The iOS and macOS devices are not allowed to register via iReg if the Allowlist feature is enabled and the device serial number is not mentioned in the CSV file. If the CSV file contains a duplicate serial number, then the last entry in the CSV file would be considered and the custom device attributes associated with that entry would be considered for device assignment during registration.

If the **Device Allowlist** option is enabled, only the Allowlisted devices will be allowed to register with Ivanti Neurons for MDM. This feature is applicable only for devices which register via the web based registration process. This will not affect the devices that are already registered with Ivanti Neurons for MDM. After registration, if the device serial number is removed from the CSV file, the device will not be retired. The user mentioned in the CSV file is optional, and will be assigned only if the user is mentioned in the CSV file and is a valid user.

If you want to upload a new CSV file, you can delete the existing CSV file and upload the new file. Allowlisting is only supported with iReg and if the Go client is needed, then opt for zero-touch registration. For features like AppConnect and Threat Defense to function, the Go client should be installed on the system. Because we do not support in-app registration, the user can first register the device through iReg, and later, the MobileIron Go app can be pushed to the devices from the app catalogue. When user accepts installation of app, the device would be a managed device and all the features will continue to work post registration. Zero-touch configuration cannot be used on devices on which the AppConnect status is Active or Inactive. It can be used only when the AppConnect status is None. The AppConnect status remains as None until the Go client is launched on the device after registration through iReg.

Procedure

1. Log in to Ivanti Neurons for MDM.

2. Go to **Users** > **User Settings**.
3. Under **Device Registration Settings** click **+Add setting for specific user groups**.
4. Edit the default **Device Registration Authentication Type** setting or add a new one.
5. Enter a name in the **Name** field.
6. (Optional) Enter a description of the setting.
7. In the **OS Settings** section, define the minimum OS version for iOS, macOS, or Windows:
8. Select the **Enable Minimum Version** toggle button and select an OS version from the drop-down list.

> Enable Minimum Version setting is not applicable for DEP device registrations.

For **Android**:

- Enable **Minimum Security Patch** option (Android only) and specify the period by selecting the duration type from the following drop-down list options:
  - **days(s)**
  - **month(s)**
  - **year(s)**

  Enable **Manufacturer Allowlist/Blockedlist** option and select any of the following options:
  - **Create an Allowlist**- To only allow devices from these manufacturers to be registered.
  - **Create a Blockedlist**- To prevent devices from these manufacturers to be registered.
    To add a manufacturer:
    1. Click **Add manufacturer**.
    2. Type the name of the manufacturer in the **Manufacturer name** field.
    3. Click **Save**. The added manufacturer name is displayed in the table.

    > The manufacturer name is case sensitive. To edit or delete an added manufacturer name, click the **Edit** or **Delete** option for the manufacturer.

In the Apple Enrollment section, select the Apple Enrollment Type:

- **Device Enrollment**
- **User Enrollment** - By default, User Enrollment is applicable for iOS and iPadOS devices.
- (Optional) **Include macOS Device (macOS 10.15+)** - Select this option to make User Enrollment applicable for macOS devices as well.

In the **Registration Invitation Method (iOS and Android Only)** section, Enable **MAM only registration**.

> This option should be enabled for MAM-Only device registrations and when enabled, the users are redirected to Public App Store to download AppStation client app.

11. In the **Device Registration Authentication Type** section, select one of the following registration type options from the **Select Registration Type** drop-down. If you use Device Enrollment, make sure that your Device Enrollment configuration matches your choice.

- **Password Only**
- **PIN Only** When you select this option, the Bypass IdP Device Registration Authentication toggle button is locked.
- **Password and PIN**

> Users may still receive a PIN to complete account activation.

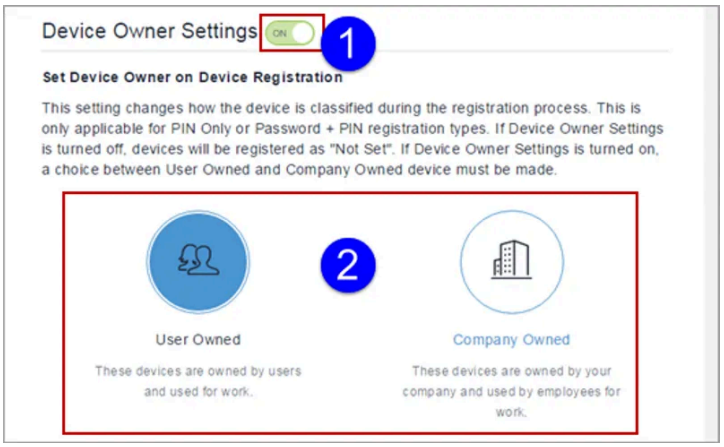
> This setting affects both normal registration and Device Enrollment registration.

For PINs, specify the following. During the device registration, a user can click **Resend PIN** if required.

- **PIN lifetime**: How long the PIN remains valid (1-30 days).
- **PIN length**: The number of characters (4-12).
- **Allow user to request a new PIN**: (when forgotten or expired).

Optionally, turn on **Device Owner Settings**, and then click **User Owned** or **Company Owned**. This setting changes how the device is classified during the registration process.

- If **Device Owner Settings** is turned ON and if the administrator has marked the device as User Owned, the user will be presented with the option to mark the device as User Owned or Company Owned during device enrollment and also from the self-service portal. For User Enrollment Enrolled devices, the default Device Owner Settings will be "User Owned" irrespective of the choice made by an administrator.
- For Supervised devices, device owner setting will be "Company Owned."



Click **+Add** for at least one user group to which you want to distribute the setting.

15. ([On-demand feature](#) for iOS and macOS devices only). Optionally, turn on the **Device Allowlist** option to allow device registration based on Allowlisted serial numbers.
16. Click **Next**. The User Setting Distribution page opens.
17. Select the user group distribution.
18. Click **Done**.
19. Send an invite to the users. For more information, see [Inviting Users](#).

Note the following points:

> If a user device is registered using PIN only option, the user receives a registration confirmation email with a PIN for authentication.

- A PIN is sent to the user's email ID.
- The user enters the PIN on the device registration page.
- If the PIN is correct, the user is directed to complete the registration process.

For users configured with SAML-based **Identity Provider** (IdP),Ivanti Neurons for MDMsupports PIN-based authentication while registering the device. The Device Registration Authentication Type should be PIN or PIN and Password. The PIN and Password feature acts as two-factor authentication for additional security. In this case, when such a user tries to register a device:

- A PIN is sent to the user's email ID.
- The user enters the PIN on the device registration page.
- If the PIN is correct, the user is redirected to the IdP's login page, where the user enters the IdP user name and password.
- If the IdP credentials are correct, the user is redirected to the device to complete the registration process.

Configuring the device limit per user

Procedure

1. Edit the default **Device Limit** setting or add a new one.
2. (Optional) Click **+ Add setting for specific user groups** to configure device limit for specific user groups.
3. Edit or assign a name to identify the setting.
4. Type an optional description of the setting.
5. From the **Maximum number of active devices** drop-down, select the active Apple devices limit.
6. From the **Maximum number of Apple watchOS devices to pair with an iPhone** drop-down, select the active Apple watchOS devices limit to pair with the iPhone.
7. (Optional) If **+ Add setting for specific user groups** is selected, click **Next** and select at least one user group for the distribution of this setting.
8. Click **Done**.

Configuring the device wipe limit

Procedure

1. Edit the default **Device Wipe Limit** setting.
2. Turn on the **Enable wipe limit for all users (including default roles)** option.
3. In the **Maximum number of devices a user can wipe at a time** field, type the maximum number of devices that can be wiped at a time. The default value is 1. You can set a maximum value of 200 as the device wipe limit.
4. Click **Done**.

Configuring the Self Service Portal authentication

Procedure

1. Edit the default **Self Service Portal Authentication** setting or add a new one by clicking **+ Add setting for specific user groups**.

2. Edit or assign a name to identify the setting.
3. Type an optional description of the setting.
4. Select a **Self Service Portal Authentication Type** from the drop-down. It can be one of the following options:
    - Password
    - Certificate
5. Click **Next**.
6. Select one or more user groups for which this configuration will be distributed.
7. Click **Done**.

Setting the password complexity

You can set password complexity and policy parameters for local accounts used for device registration, and access to Admin Portal and Self Service portals.

> The password length, characteristics, and policies set below define the security of a password.

This also defines the difficulty associated with a user selecting a valid password. If you use Local Account for your end users and would like secure passwords for access to the Admin Portal, consider using a PIN for device registration to ensure that password complexity does not interfere with device registration. Use the "Device Registration Authentication" Type setting to select the authentication mode for device registration under **User Settings > Device Registration Setting**.

Procedure

1. Edit the default **Password Complexity** settings.
2. Define the following password complexity settings:

Setting	What To Do
Minimum Password Length	Move the slider to specify the minimum length of a password to prevent the user from creating short and insecure passwords. Number ranges between 8 to 32.
Required characteristics	Specify the number of password characters that should be met when you select a password. The minimum number of characteristics that should be met is 3 (4 for Federal customers).
Required Special Characters (symbols)	Specify the number of non-alphanumeric characters a password should contain.
Required Uppercase Characters	Specify the number of uppercase alphabetical characters a password should contain.
Required Lower Case Characters	Specify the number of lowercase alphabetical characters a password should contain.
Required Numeric Characters	Specify the number of numeric characters a password should contain.
Password validations	
Allowed Numeric Sequence	Select the number of repeating number in a sequence. Example: 123.
Allowed Repeated Characters	Select the number of repeating alphabetical characters. Example: bbc.

3. Set the following password policies setting to customise behaviour.

Setting	What To Do
Retained Password History	Move the slider to select the number of new passwords that must be associated with a user account before an old password can be used. Number ranges between 3 to 36.
Password Expiration Period	Move the slider to select the password expiration duration in days. Number ranges between 30 to 365 days.
Inactivity Timeout	Move the slider to specify the time a user maybe inactive before an Admin Portal or a Self Service portal session time. Number ranges between 5 to 60(minutes).
Failed Logins Threshold	Move the slider to select the number of failed login attempts before the 5 minute account lockout takes effect. Number ranges between 2 to 5. When the failed attempts are within the threshold limit, a message is displayed to the user on the lockout and to attempt login later. When the failed attempts exceed the threshold limit, a message is displayed to the user on the lockout and to attempt login after a specified time (in minutes).

4. Click **Done**. If you have changed the Password Complexity default setting, older password of existing local account remains unchanged. On expiry, the user will be prompted to renew the password. For administrators, attempting to login to the Admin Portal, can contact Help Desk who can provide guidance for resetting password.

> In a device registration, the recommended approach is to use PIN-only registration mode.

Defining the terms of service

Procedure

1. Create a new **Terms of Service** setting.
2. Assign a name to identify the setting.
3. Type an optional description of the setting.
4. Select the **Prompt the user**... option.
5. Type a title and text to display.
6. Click **+Add** for at least one user group to which you want to distribute the setting.
7. Click **Save**.

> Once accepted, the terms of service cannot be deleted. However, you can turn off the prompts for new registration by clearing the **Prompt the user**... option.

Configuring the User Invite reminder emails

Administrators can drive device enrolments by using this setting to send User Invite reminder emails.

Procedure

1. Edit an existing **User Invite Reminder Setting** or add a new one.
2. Edit or assign a name to identify the setting.
3. Type an optional description of the setting.
4. Ensure the **User Invite Reminders** option is turned on.
5. In the Define Start and End Dates region, choose when you want to start and stop sending email reminders.

> The maximum number of emails that can be sent is 30. To reset this limit, the admin should re-send the invite.

6. In the Define Frequency region, choose how frequently you want to send email reminders.
7. Click **Next**.
8. Select a distribution for this configuration.
9. Click **Done**.

Configuring User Registration Confirmation emails

Administrators can send emails to new users who have completed registration.

Procedure

1. Edit an existing **User Registration Confirmation Setting** or add a new one.
2. Edit or assign a name to identify the setting.
3. Type an optional description of the setting.
4. Ensure the **Send a confirmation email upon successful User registration** option is turned on.
5. Click **Next**.
6. Select a distribution for this configuration.
7. Click **Done**.

Configuring User Work Schedule setting

Administrators can configure a user work schedule for users that blocks all communication from Sentry to managed devices during the prescribed non-working hours. This is useful for users in locales with Right-to-Disconnect laws.

Procedure

1. Select **Users**.
2. Select **User Settings**.
3. In the section, **User Work Schedule Setting**, select **+Add setting for specific user groups**.
4. Provide a name for the setting.
5. Turn on the setting.
6. Select the time zone.
7. Configure the hours during which Ivanti Neurons for MDM blocks the Exchange ActiveSync protocol, AppConnect-Enabled apps, and managed apps.
8. Click **Next**.
9. Configure the distribution, and then click **Done**.

Changes applied may take up to 1 hour and 15 minutes to take effect on the device.

Configuring Admin Portal authentication setting

Administrators can set the authentication type to authenticate user login. This setting controls whether the users will be prompted for password only or password and PIN.

Procedure

1. Edit an existing **Admin Portal Auth Setting** or add a new one.
2. Edit or assign a name to identify the setting.
3. Type an optional description of the setting.
4. In the **Admin Portal Authentication Type**, select any of the following options:

Option	Description
Password	Select this option to authenticate the login using password only. Users may still receive a PIN to complete account activation.
Password and PIN	Select this option to authenticate the login using password and PIN. When you select this option the following additional fields are displayed: • **PIN lifetime**: Select the minute duration of the lifetime of the PIN from the drop-down list. The minutes should be within the range of 1 to 15. • **PIN length**: Select the length of the characters of the PIN from the dropdown list. The range of the PIN length should be between 4 to 12. This option is applicable only for local accounts and not for LDAP Admin accounts.
Allow user to request a new PIN	Select this option to allow users to request a new PIN.

5. Click **Next**.
6. Select a distribution for this configuration.
7. Click **Done**.

For users configured with SAML-based **Identity Provider** (IdP), Ivanti Neurons for MDM supports PIN-based authentication to the administration portal. The Admin Portal Authentication Type should be PIN and Password. This feature acts as two-factor authentication for additional security. In this case, when such a user tries to log into the portal:

- A PIN is sent to the user's email ID.
- The user enters the PIN on the administration portal login page.
- If the PIN is correct, the user is redirected to the IdP's login page, where the user enters the IdP user name and password.
- If the IdP credentials are correct, the user is redirected to the administrator portal.

When logging into the administrator portal, a user can click **Forgot Password** to reset their password. In the next screen, the user can enter a new password and the PIN (prompted based on the preceding user authentication mode settings) sent to the user's email address. Click **Resend PIN** if required. The user must wait fifteen minutes between Forgot Password requests.

When this configuration is distributed to devices, consecutive unsuccessful log in attempt (default value: 5 attempts) by the user using password or PIN will result in account lockout and a message will be displayed to the user on the lockout.

6.4. User Branding

User branding enables you to customise the device registration process with names and logos that your users will recognise. You can customise the user-facing branding in the following ways:

- Set a custom host name for the registration URL
- Display your logo in the registration email and registration screen
- Display a custom favicon during registration activities

> Updating the above settings changes the value referred by **$**.

Licence: Gold

Prerequisite:

- Decide on the host name you want to use in your custom URL. It must meet the following requirements:
  - Contains no spaces
  - Contains no special characters

Obtain a logo file that meets the following requirements:

  - PNG format
  - 580 x 80 pixels

Obtain a favicon file that meets the following requirements:

  - PNG format
  - 64 x 64 pixels

Procedure:

1. Go to **Users > User Branding**.
2. Click **Customise** (upper right).
3. In the **Hostname** field, type a short name to use as the host name in your URL.
4. Click **Check Availability** to confirm that the host name you entered has not been used by someone else.
5. If the host name is not available, enter a different name.
6. Note the resulting registration URL under **URL Preview**.
7. Click **Next**.
8. Under **Logo**, click **Choose File** to upload the logo to be used in the registration email and registration screen.
9. Click **Next**.
10. Under **Favicon**, click **Choose File** to upload the favicon to be displayed in place of the Ivanti Neurons for MDM favicon during registration activities.
11. Click **Done**.

6.5. User Enrollment with Apple Business Manager

This section contains the following topics:

Applicable to:

- Unsupervised devices with iOS 13.0 through the latest version as supported by Ivanti Neurons for MDM.
- Devices with macOS 10.15or supported newer versions Ivanti Neurons for MDM.

Apple Business Manager is a place for IT teams to automate device deployment, purchase and distribute content, and manage roles in their organisations. Apple Business Manager implements User Enrollment - an enrollment option designed for companies implementing BYOD (Bring Your Own Device). User Enrollment is a modified version of the MDM protocol with a much greater focus on user privacy, implemented with a level of security that enterprises need.

User Enrollment allows the administrator to do the following:

- Install and remove managed applications
- Install and remove network configurations
- Install a partial VPN scoped to managed apps and accounts
- Require the usage of a password

Requirements for enabling User Enrollment

Below are the requirements for enabling User Enrollment. If any of them are not met, the enrolment type will be device enrolled.

- An unsupervised device with iOS 13.0 through the latest version as supported by Ivanti Neurons for MDM or a device with macOS 10.15or supported newer versions Ivanti Neurons for MDM.
- User setting for the Apple Enrollment Type field should be set as "User Enrollment."
- An Apple Business Manager account.
    - The Apple App Licence Account needs to be part of the same Apple Business Manager account.
    - Within Apple Business Manager, if you have an account listed in Locations, you need to have Apps and Books matched to the same location. You may need to add a new location (for example, West Coast).

Managed Apple ID - Managed Apple ID to be associated with each enrolled device.

- This Managed Apple ID provides authentication for MDM management and app licensing.
- When the MDM pushes down apps and media, necessary Apple licences are assigned to the Managed Apple ID associated with the device.
- As part of GDPR compliance, Managed Apple IDs are masked in the user list and user details pages considering the Apple ID to be user data.
- Managed Apple IDs were first utilised by Apple School Manager and are now utilised by Apple Business Manager for User Enrollment.

> The device's Managed Apple ID and Apps and Books Location token should be from the same Apple Business Manager account's Organisation.

If they are different, a notification is displayed in the Ivanti Neurons for MDM Admin Portal when the licence allocation fails for an app.

Microsoft Entra ID configured for Federated Authentication or an Apple ID created manually in Apple Business Manager with a validated domain.

- For instructions on using Federated authentication, see the **Apple Business Manager User Guide** on the Apple website. A login is required.

Device users who are synced to LDAP are to be assigned to a device management role and associated with a Managed Apple ID.

In the **Users** list page and the **Devices** list page, you can add the Managed Apple ID column to be displayed for all users. In the **Devices** list page, you can add the User Enrollment Enrolled column to display the status of User Enrollment devices. In addition, the user and device exports include these columns in CSV files.

Priority of registrations

- User Enrollment is supported via Go for iOS client and iReg. Apple no longer supports User Enrollment through Ivanti Go for iOS and iReg. **Account driven User Enrollment** is only available in the Work or School account of the device.
- Automated Device Enrollment and Apple Configurator registrations will always be device enrolled.
- If MAM configuration is applied to a device, MAM registration takes precedence over User Enrollment.
- If both auth-only and User Enrollment requirements are met, User Enrollment takes precedence.
- If you Re-enrol a device from Go for iOS client, the enrolment type will be the same as the type during the device registration irrespective of the change in the enrolment type in Ivanti Neurons for MDM. For example, if a device was user enrolled, change the type to Device Enrollment in Ivanti Neurons for MDM, and Re-enrol the device from the Go client, the device will still be user enrolled and not device enrolled.

Difference between standard MDM enrollment and User Enrollment

This section addresses the difference between standard MDM enrolment and User Enrollment with Apple Business Manager.

Standard MDM enrolment

The following list indicates what a Ivanti Neurons for MDM server can do in a standard MDM enrollment, but will not be able to do in User Enrollment mode.

The MDM server:

- Cannot erase the device.
- Does not see the personal apps the device user has installed on the device.
- Cannot convert user-installed apps into MDM-managed apps.
- Cannot clear the device passcode (i.e. unlock the device).
- Cannot set a long, complex device passcode requirement.
- Cannot configure a device-wide VPN or Wi-Fi proxy, or can it do any management of the mobile connectivity functionality.
- Cannot see device identifiers like the UDID, serial number, or IMEI.
- Cannot apply many device-wide restrictions (such as restricting the app content rating), block iCloud, and apply any the supervised restrictions.

User Enrollment with Apple Business Manager

In User Enrollment, the MDM server can still do everything needed to manage enterprise apps, accounts and data.

User Enrollment can:

- Install in-house apps or apps via user-based (Apple) Apps and Books licences.
  - The licences are applied on a first-come, first-served basis and are consumed by the Managed Apple IDs.
  - The licence consumed by an app installed on the User Enrolled device will be different from the licence consumed by the same app installed on the device enrolled device.
  - Check licence type for Apple Apps and Books applications in a user details page via the Licence Usage tab - the Enrollment Type is displayed as User Enrollment or Device Enrollment.

Enforce passcode payload settings. For example:

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

Query data related to enterprise-managed apps, certificates and profiles.

- Configure a per-app VPN for apps, mail, contacts, and calendars that have been installed by MDM.
- Enforce some restrictions, like managed open in, managed contacts, managed data on the lock screen and several others.

Enterprise data is stored in a separate Apple File System (APFS) volume, which is created at enrolment, and encrypted separately from device user data. This volume contains data stored by managed apps; enterprise Notes; enterprise iCloud Drive docs; enterprise Keychain entries; managed mail attachments and bodies; and calendar attachments. Un-enrolling from MDM destroys the volume and the keys.

All third-party apps can only be either a personal app or a managed app through Ivanti Neurons for MDM. The MDM service cannot start managing apps that the device user has already installed. In this case, the administrator will need to request the device user to delete the personal app before installing the app through MDM. The MDM service cannot start managing apps that the user has already installed. However, some system apps like Notes and Files will support both work and personal accounts.

User Enrollment for macOS devices

User Enrollment is supported for devices with macOS 10.15or supported newer versions Ivanti Neurons for MDM.

- Mobile@Work for macOS is not supported for macOS User Enrollment Enrolled devices.
  - Even if the app is distributed to the macOS User Enrollment Enrolled device, the app will not be pushed to the device from MDM.
  - Therefore, Mobile@Work features such as script management and app management for the Packager (MIP) apps are not supported for macOS User Enrollment Enrolled devices.

App dependency and behavioural changes in macOS User Enrollment Enrolled devices.

  - In macOS User Enrollment Enrolled devices, app dependency works on a best effort basis as the MDM is unaware of (cannot confirm) the installation status of prerequisite apps before distributing the main app.
  - Apps and configurations can be distributed to users and user groups that belong to macOS User Enrollment Enrolled devices. However, the apps always display the **Install** button instead of "Installed" because MDM cannot display the installation status of apps in macOS User Enrollment Enrolled devices.

- Installed apps are indicated as Requested Apps in **Devices > App Inventory** page as the macOS User Enrollment Enrolled devices do not notify the Ivanti Neurons for MDM server whether the apps are installed or not installed in the inventory report.

In the distribution filter for apps, User Enrollment Enrolled and Automated Device Enrollment Enrolled attributes can be used for custom distribution as required.

- User-based licences are supported using managed Apple IDs to install Apple Apps and Books applications. Device-based licences are not allowed. The app catalog only displays Apple Apps and Books applications.
- Not all configurations, policies and actions are allowed. See full list of configurations and policies listed following this procedure.
  - If unsupported configurations are distributed to a macOS User Enrollment Enrolled device, they will not be distributed or applied to the device and may display a message such as "Restrictions - this is not a valid request type."
  - Similarly, unsupported admin device actions will be informed in Ivanti Neurons for MDM UI.
  - Unsupported reports will not be sent by Ivanti Neurons for MDM.

The following are the configurations and policies unsupported to be distributed to macOS User Enrollment Enrolled devices:

- Passcode
- Tunnel
- Tunnel (On Demand)
- VPN configurations
- Office 365 Auto Account Creation
- macOS Kernel Extension Policy
- Privacy Preference
- macOS Restrictions
- Software Updates
- AirPrint
- MI Client Privacy
- FileVault 2
- FileVault Recovery Key
- Firewall
- System Policy Rule
- Certificate Preference
- System Policy Control
- System Policy Managed
- macOS AppStore Restrictions
- macOS Disk Burning Restrictions
- macOS Finder Settings
- Mobile@Work for macOS
- Mobile@Work for macOS Script
- Allowed Media Control

- Time Server
- Allowed Apps Policy

Difference between User Enrollment vs Device Enrollment

This section covers the difference between User Enrollment and device enrollment.

User Enrollment applies to devices with iOS 13.0 and macOS 10.15 through the latest version as supported. Devices lower than iOS 13.0 and macOS 10.15 will be considered “device enrollment” regardless of whether the device user has been enabled for User Enrollment or not.

> User Enrollment for Apple Business Manager does not allow for wipe or unlock. However, the user portal will still have those options available even though they will not work.

User Enrollment vs Device Enrollment			
Functionality	User Enrollment	MAM	Device Enrollment
Erase the device and see user's personal apps	✗	✗	✓
Convert managed to unmanaged or vice versa	✗	✗	✓
Clear device passcode, configure device-wide VPN or Wi-Fi proxy, or manage mobile functionality	✗	✗	✓
See device identifiers like serial number, IMEI	✗	✗	✓
Apply supervised restrictions	✗	✗	✓ (Supervised devices only)
Can install and configure apps and accounts	✓	✓	✓
Can configure a per-app VPN for apps, mail, contacts, and calendars that have been installed by MDM	✓	✗	✓
Can enforce some restrictions, like managed open in, managed contacts, managed data on the lock screen, and several others	✓	✗	✓
Can query data related to enterprise-managed apps, certificates and profiles	✓	✗	✓

Connecting Ivanti Neurons for MDM to Apple Business Manager

This section covers enabling User Enrollment for Apple Business Manager.

Prerequisites

- You must have an Apple Business Manager account. See **https://business.apple.com/**.
- You must request and install an Apple **MDM certificate** to manage iOS devices.

Creating local users to enable User Enrollment

This section covers creating local and LDAP users and setting the User Enrollment for unsupervised Apple devices. User Enrollment will not work on supervised devices or devices enrolled in Apple's Device Enrollment.

Creating a manually managed (static) user group

This is a one time procedure. If you have already created this group, skip to the "Creating users for User Enrollment" section.

Procedure

1. Go to **Users >** User Groups.
2. Create a manually managed (static) user group, such as User Enrollment Group, to add users with device registration type as User Enrollment.
3. Click **Save**.

Creating a device registration type setting

This is a one time procedure. If you have already created this group, skip to the "Creating users for User Enrollment" section. For User Enrollment Enrolled devices, the default Device Owner Settings will be "User Owned."

Procedure

1. Go to **Users >** User Settings.
2. In the Device Registration Setting section, click **+ Add setting for specific user groups**.
3. Create a new setting, such as UE Registration, for users with device registration type as User Enrollment.
4. In the Apple Enrollment section, select **User Enrollment** as the Apple Enrollment Type.
5. Click **Next**.
6. In the User Setting Distribution page, select the newly created user group, such as User Enrollment Group.
7. Click **Done**.

Creating a local user for User Enrollment

As a prerequisite, create a manually managed user group and a device registration setting for User Enrollment.

Procedure

1. Go to Users.
2. Click + **Add** > **Single User**.
   Enter the new user information and add it to the newly created user group, such as User Enrollment Group. For more information, see *Adding a user* in the Users topic.

Importing LDAP users to enable User Enrollment

Prerequisites

- As a prerequisite, set up a Ivanti Neurons for MDM connector to access LDAP resources.
- Ensure that the **Managed Apple ID** setting is set to **Pattern** (user email address). Ensure the pattern for Managed Apple ID is unique. Otherwise, the account will not be updated with the Managed Apple ID if the same Managed Apple ID exists in another account.

- (Optional) include "appleid" subdomain to avoid conflict with existing Apple IDs.
- You can import users from LDAP and invite them for User Enrollment. The imported LDAP users will have their Managed Apple IDs synced with Ivanti Neurons for MDM, which is a requirement for User Enrollment.

Procedure

1. Go to **Users**.
2. Click **+Add > Invite Users from LDAP**.
3. Click **Select Users** in the LDAP server entry.
4. In the Add LDAP Users page, enter the name of the user, group, or OU in the search field.
5. To add new users or groups, click **+Add** next to the entry you want to add.
6. Click **Done**.

Importing Entra ID users to enable User Enrollment

As a prerequisite, connect Ivanti Neurons for MDM with Microsoft Entra ID (Entra ID).

You can invite Entra ID users for User Enrollment. The imported Entra ID users will have their Managed Apple IDs synced with Ivanti Neurons for MDM, which is a requirement for User Enrollment.

Procedure

1. Go to **Admin >** Entra ID User Source.
2. Edit the settings.
3. Select **Enable this Entra ID**.
4. In the Managed Apple ID setting, select one of the following options:
    - **Pattern**
        - **User email address** - Ensure the pattern for Managed Apple ID is unique. Otherwise, the account will not be updated with the Managed Apple ID if the same Managed Apple ID exists in another account.
        - Alternatively, select **userUPN**.
5. (Optional), include "appleid" subdomain to avoid conflict with existing Apple IDs.
6. Select **Automatically invite users imported from Entra ID**. Users imported from Entra ID to Ivanti Neurons for MDM are automatically invited to register via email.
7. Click **Save**.

Device user instructions for registering using User Enrollment

This section addresses the actions the device user needs to take for registering Apple User Enrollment.

Procedure

1. On the iOS device you wish to register, open the invitation email that contains a link and text guiding the end user to a registration link such as mobileiron.com/go.
2. Open the registration link in Safari.
3. The login page displays. The device user is to log in using their local user or LDAP credentials.
   The registration page displays with a message saying the profile was downloaded.
   Tap Settings. The Settings page displays.

4. Tap Enroll in [Your Company Name].
5. The User Enrollment page displays.
6. Tap Enroll My [Your Device]. For example, tap Enroll My iPhone.
   If you tap Cancel and Delete Profile, you will have to start the registration process all over again.
   You will be presented with a login for either Apple or your Federated account. Enter the password for your Managed Apple ID. (The Managed Apple ID will be listed at the top of your login page.)
   You may be presented with the option to stay signed in, make a selection.
   A page displays the "Enrollment is Successful."

Using device logs for troubleshooting

To troubleshoot errors or issues for a User Enrolled device, start by reviewing the device logs.

Procedure

1. Go to Devices.
2. Click on the device to display the device details page. You can verify User Enrollment Enrolled and Registered Managed Apple ID fields.
3. Select the Logs tab.
4. In the Filters region, narrow the device logs using filters based on action names (such as Checkout, Device Name, Set Bootstrap Token, Get Bootstrap Token and so on), status, start date and end date.
5. In the Actions column, click the eye icon to display the device log details, such as Enrollment ID.
6. Click **OK**.

6.6. User Licences

Ivanti Neurons for MDM user-based licenses define the number of users you can register, the number of devices allowed per user license, the amount of content you can configure for distribution to devices, and which features are available. If you reach your limit for users, a red triangle displays on the Admin page. If you reach your limit for content, the service will prevent you from adding more and display a message to indicate that you have reached your limit.

To determine how many user licences you should plan for consider the following points:

- Each user licence purchased under the Secure UEM or Secure UEM Premium package allows registration of up to five devices.
- Once a user registers more than five devices, another user licence is claimed.
- There is no enforced limit to the number of user licences that a user can claim.
- Licences are released when devices are retired or wiped.

For example, when User1 registers her work phone on the first day of work, she claims a user licence. The following week, she registers two personal phones and a tablet under that same licence. When she registers another tablet, she now has five devices, so she claims a second user licence. When her personal phone is stolen, she wipes the device, which releases the second user licence.

Viewing the number of devices/ licenses for a user

Procedure:

1. Go to **Users**.
2. Click the link for the user.

The left pane lists user details, including licence usage.

6.7. Managing Users

This section contains the following topics:

- Adding an API user for Cisco ISE operations
- Assigning Roles to Users
- User Roles
- Finding and Filtering Users
- Assigning Users to User Groups
- Inviting Users
- Enabling and Disabling Users
- Managing Multiple Administrator Logins
- Changing a Password
- Sending a Message
- Removing Users from User Groups
- Deleting a User
- Exporting Users
- Assigning Custom Attributes to Users
- Removing Custom Attributes from Users
- Changing the User Locale
- Editing a Username
- Opting Out of Location Data Collection
- Timeout Information
- Opting Out of System Usage Analytics
- Device Registration by PIN Generation

6.7.1. Adding an API user for Cisco ISE operations

You can add an API user with the role "Cisco ISE Operations" that allows Cisco ISE to interact with the Cisco ISE APIs in Ivanti Neurons for MDM. After you create this user, you use this user's credentials from Cisco ISE to authenticate API calls into Ivanti Neurons for MDM. These APIs allow Cisco ISE to get device information; take actions on devices, for example, full wipe, corporate wipe, and pin lock; and send messages to devices.

> The API user will not be able to log into the Admin portal. This user is for enabling API usage only.

> Note: Only the Super Admin of a tenant is assigned the Cisco ISE Operations role by default. The Super Admin must explicitly choose the other users in the system who must possess this role and assign it to them. Users, that are assigned the Cisco ISE Operations role can, in turn, assign the role to other appropriate users in the system.

Procedure

1. Go to **Users** > **Users**.
2. Click **Add**.
3. Select **API User**.
4. Complete the resultant form with the user's information:
    - Email Address
    - Forename
    - Surname

> The Username field displays the email address you entered. In most cases, you should not edit this default. See **When to Edit a Username**.

If you want to change the display name for this user, edit the default text in the **Display Name** field.

6. Assign a password by entering it in the **Password** and **Confirm Password** fields.
7. Leave the **API Management Cisco ISE Operations** role selected in the **Assign Roles** section.
8. Click **Done** to add the user.

If you cannot perform tasks on the **Users** page, it might be that you do not have the required permissions. You need one of the following **roles**:

- System Management
- User Management

6.7.2. Assigning Roles to Users

You can give users access to Ivanti Neurons for MDM data and features by assigning **roles**. You can assign roles directly to users or to user groups. Assigning a role to a {{user group}} gives that role to all users in that group.

> The User Read Only role is not assigned to users by default.
> The Roles page and the associated options are hidden for tenants who have access to both Ivanti Neurons for UEM and Ivanti Neurons for MDM.

Users cannot assign the permissions that they do not already have. The permissions and roles that are not assigned to the users are not displayed for selection. In this case, an error message is displayed. When an Ivanti Neurons for MDM Administrator or a Partner Administrator attempts to assign roles to a Partner Administrator, Ivanti Neurons for MDM displays a message conveying that a Partner Administrator must perform this operation on the Service Provider Portal.

For more information about roles, see **Roles_Management.htm**.

Procedure:

1. Go to:
   - **Users > Users** *or*
   - Users > User Groups.

Select one or more users or user groups.

3. Click **Actions**.
4. From the Users details page or User Groups details page, click **Assign Roles** *or*
   From the User list or User Group list page, select **Append Roles**.
5. Select one or more of the following roles you want to assign:
   - System Management | Cross-Space
   - System Read Only | Cross-Space
   - User Management | Cross-Space
   - User Read Only | Cross-Space
   - LDAP User Import and Invite | Cross-Space
   - Device Management | Space-Specific
   - Device Read Only | Space-Specific
   - App & Content Management | Space-Specific
   - App & Content Read Only | Space-Specific
   - Device Actions | Space-Specific
   - Cisco ISE Operations | Cross-Space
   - Scheduled Task Management | Cross-Space
   - Common Platform Services (CPS) | Cross-Space
   - Low User Impact Migration Management | Cross-Space
   - Custom Device Enrollment | Cross-Space

- Edit Microsoft Graph | Cross-Space
- Send/Cancel Wipe | Cross-Space
- View Microsoft Graph | Cross-Space
- Manage Access Integration | Cross-Space

Click **Next**.

7. If the selected roles are Space bound, then select Spaces for all the Space bound roles.

> If there is only one Space (Default Space), the Specify Space step is skipped when assigning a Space-bound role.

The summary page displays the Space name for Space bound round as Default Space.
Review the summary of the roles to be assigned and click **Done**.

Giving helpdesk staff permission to use basic device actions

The helpdesk roles generally allow staff to view data. However, some organisations prefer to include the basic device actions:

- Force Check-in
- Lock
- Unlock
- Send Message
- Retire
- Wipe

Procedure

You can provide permission to the actions.

1. Go to **Users > Users*** or**** Users > User Groups**.
2. Select one or more users or user groups.
3. Click **Actions**.
4. From the User details page or User Group details page, select **Assign Roles** *or*
   From the User list or User Group list page, select **Append Roles**.
5. Select **Device Read Only**.
6. Select **Device Actions**.
7. Click **Done**.

> Ensure that you select Device Read Only before selecting Device Actions for the users to have the expected permissions.

6.7.3. User Roles

User roles determine the pages users can see in Ivanti Neurons for MDM and the things users can do. The following table lists the roles you can assign and what they mean.

Role	Description	Space-Specific
System Management	Allows an administrator to manage tenant-level settings such as MDM Certificates, App Catalog Settings and more.	No
System Read Only	Allows an administrator to view tenant-level settings such as MDM Certificates, App Catalog Settings and more.	No
User Management	Allows an administrator to add and remove users, assign roles and add users to user groups.	No
User Read Only	Allows an administrator to view users and user groups as well as the apps and content catalogues.	No
Device Management	Allows an administrator to manage device groups, configurations and policies as well as perform all device actions.	Yes
Device Read Only	Allows an administrator to view device groups, configurations and policies.	Yes
App & Content Management	Allows an administrator to add, distribute and remove Apps and Content.	Yes
App & Content Read Only	View data in Users, Apps, Content, including AppConnect tasks	Yes
Device Actions	Allows an administrator to initiate device actions, such as: • Force Check-in • Lock • Unlock • Send Message • Retire • Wipe Note: You must select Device Read Only before selecting Device Actions. Otherwise, users will not have the expected permissions.	Yes
LDAP User Import and Invite	Allows an administrator to register LDAP Users and send invitation(s) to register device(s)	No
Cisco ISE Operations	Allows an administrator to invoke API(s) required for Cisco ISE integration.	No
Scheduled Task Management	Allows an administrator to create and manage Scheduled Task(s) for various administrative operations.	No
Common Platform Services (CPS)	Allows an administrator to use Common Platform Services.	No
Low User Impact Migration Management	Allows an administrator to manage Low User Impact Migration settings.	No

Role	Description	Space-Specific
Custom Device Enrollment	Allows an administrator to enrol a device using custom device enrollment.	No
Edit Microsoft Graph	Allows an administrator to edit Microsoft Graph API settings used for Office 365 Apps protection.	No
View Microsoft Graph	Allows an administrator to view Microsoft Graph API settings used for Office 365 Apps protection.	No
Send/Cancel Wipe	Allows an administrator to send a Wipe command to a device or cancel an issued Wipe command before it is executed.	No
Manage Access Integration	Allows an administrator to manage Access integration.	No

For more information, see **Assigning Roles**

6.7.4. Finding and Filtering Users

This section contains the following topics:

Searching a user

Once you have added many users, it can be helpful to use filters or searches to quickly locate a user entry.

Procedure

1. Go to **Users**.
2. Type characters in the search box.

Using Advanced Search for users

You can use the Advanced Search option to search for users based on rules to identify and view the users with specific criteria. The rule options can be nested together using the ANY (OR) or ALL (AND) options. The users matching the rules are displayed below the section. The rules can be constructed using the following operators:

- begins with
- ends with
- contains
- does not contain
- does not begin with
- does not end with
- is less than
- is greater than
- is in range
- is equal to
- is not equal to

Starting from Neurons for MDM 127 the Ivanti Neurons for MDM Administrator displays the number of duplicate user groups and the corresponding number of GUIDs to identify duplicate groups, when the User Group Name attribute is selected in the rule builder. Also, a table under this rule displays the list of the duplicate user groups and their details such as User Group Name, GUID, Source and distinguished name (DN).

Procedure

1. From the Users page, click the **Advanced Search** link.
2. Click **Any** if the users need to match at least one of the rules, or Click **All** if the users need to match all the rules.
3. Create a rule that defines the search criteria, such as User Group, Custom User Attribute and Custom LDAP Attribute.
4. (Optional) Click + to create additional rules, if needed.
5. (Optional) Click **Save** to save the query.
6. Click **Search**. The list of users matching the search criteria are displayed in the page.

Loading the Search queries for users

Procedure

1. From the Users page, click the **Advanced Search** link.
2. Click the 'Folder' icon. The **Advanced Search** window is displayed. The list of the created Search queries are displayed in the **Load Query** section. The following details are displayed in this section:
    - **Query Name** - The name of the loaded query.
    - **Query Content** - Displays the content on the rules defining the search query.
    - **Actions** - Select the action to be performed on the query.
3. Click **Load Query** in the **Actions** column to view the list of users matching the criteria defined in the loaded query.
   To delete a loaded query, click the Delete icon.

Filtering Users

The Filters side navigation bar lists various sections that help you to search for a specific user from the entire list of users. The Manage Filters wizard contains the list of all the sections that you can select to display in the Filters navigation bar.

Procedure

1. Go to **Users**.
2. Click the relevant check boxes from the sections that are listed in the Manage Filters wizard. You can search from the following sections:
    - Administrators
    - Google Status
    - Invite Status
        - Completed (The user received it and responded.)
        - Expired (The user did not respond in time.)
        - Not Invited (You have not invited this user.)
        - Pending (Pending user response.)

    Password Expiration

        - Expires (users with password expiration option set to finite date.)
        - Never (users with password expiration option set to never.)
    - User Group (Select the {{user group}}s of interest.)
    - User Source
        - LDAP
        - Entra ID
        - Roster
        - Salesforce
        - Local
    - Sync
        - Direct Sync - Lists the users that were directly synced from the LDAP server

- No Sync - Lists the users that were removed from the LDAP server
- Indirect Sync - Lists the users that were indirectly synced from the LDAP server
- N/A

3. (Optional) Click **Restore Defaults** to restore the selection to the default filters. The Filters navigation bar displays the selected sections. If you clear all the check boxes from the Manage Filters wizard, the Filters side navigation bar displays all the sections.
4. Click anywhere outside the Manage Filters wizard to exit the wizard.
5. Click the x icon to close the Filters side navigation bar and click **Filters** to reopen the side navigation bar.

6.7.5. Assigning Users to User Groups

This section contains the following topics:

- Assigning users from the Users page
- Assigning users from the User Groups page

Assigning users to user groups is a great way to minimise the number of times you need to repeat tasks like:

- distributing apps
- assigning roles

Assigning users from the Users page

1. Go to **Users**.
2. Select the users you want to work with.
3. Click **Actions**.
4. Select **Assign to Group**.
5. Select the groups or click **Create New** to start a new group.
6. Click **Save**.

Assigning users from the User Groups page

1. Go to **Users > User Groups**.
2. Select the user groups you want to work with.
3. Click **Actions** (upper right-hand side).
4. Select **Assign Users**.
5. Type the email address of each user.
6. Click **Assign Users**.

6.7.6. Inviting Users

When you add a user, you have an opportunity to invite that user to enrol devices. In fact, this option is selected by default. The invited user receives an email message containing the information needed to enroll. You can also invite (or re-invite) a user from the **Users > Users** page.

Procedure

1. Go to **Users**.
2. Select the users you want to invite.
3. Select **Actions > Send Invite**. The Invitation Preview appears, along with an option to set device ownership to **UserOwned** or **Company Owned**.

4. Optionally, turn on **Device Owner Settings**.
5. Click **User Owned** or **Company Owned**. This setting changes how the device is classified during the registration process. This is only applicable for PIN Only or Password + PIN registration types. If **Device Owner Settings** is turned off, devices will be registered as "Not Set." For Supervised devices, device owner setting will be "Company Owned."
6. Click **Send**. If a PIN based device registration was performed, the user will receive a PIN to their registered email address. If a QR code based registration is set, the user will receive a QR code.
7. Click **Okay**.

> If the registration confirmation email feature is enabled as described in **Configuring and using registration confirmation emails**, then you will also see a reminder that the user will receive a registration confirmation email upon successful registration. To receive the email, the user needs to be part of the distribution list that you specify in **Configuring User Registration Confirmation emails** in **User Settings**.

For more information, see **Importing LDAP users**.

6.7.7. Enabling and Disabling Users

This section contains the following topics:

- Enabling and disabling local users
- Enabling and disabling LDAP users

The local and LDAP users can be in enabled or disabled status. Based on their status, you can create custom policies using the User Enabled condition and setting an action for the condition in the rule builder. For example, there can be a custom policy rule to retire the devices that belong to disabled local/LDAP users.

Enabling and disabling local users

By default, when a local user is created, the user is in enabled state.

Procedure

1. Go to **Users**.
2. Click the display name for the local user.
3. Click **Edit**. The **Authentication Required** window is displayed.
4. Enter your administrator password and click **Authenticate**.

> When multiple incorrect entries of the password are entered and if it crosses the 'Failed Logins Threshold limit' set in the 'Password Complexity Settings', the account will be locked and you will be logged out from the current session.

5. Select or deselect the **Enabled** option to enable or disable the local user respectively.
6. Click **Save**.

Enabling and disabling LDAP users

You can enable or disable LDAP users only for Microsoft Active Directory. In Microsoft Active Directory, when you open the properties for a user account, click the **Account** tab, and then either select or clear the check boxes in the **Account** options dialog box, numerical values are assigned to the **UserAccountControl** attribute. The value that is assigned to the attribute tells Windows which options have been enabled. After you assign a value to the UserAccountControl attribute, the user status will reflect after LDAP sync with Ivanti Neurons for MDM.

Following are the possible values you can assign:

- 512 - Enabled.
- 514 - Disabled.
- 66048 - Enabled, password never expires.
- 66050 - Disabled, password never expires.

View user accounts

Procedure

1.		Click **Start**.
	2.	Go to **Programs**.
3.		Go to **Administrative Tools**.
	4.	Click **Active Directory Users and Computers**.

For more information, see **https://support.microsoft.com/en-in/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-pro**.

You can view and edit the attributes by using either the Ldp.exe tool or the Adsiedit.msc snap-in. Only experienced administrators should use these tools to edit Active Directory. Both tools are available after you install the Support tools from your original Windows installation media.

6.7.8. Managing Multiple Administrator Logins

Multiple Ivanti Neurons for MDM admin portal sessions are supported so the administrator can view different pages of the portal at the same time. If you are an administrator, you can view your last login date to help you keep track of multiple logins.

View the last administrator login

Procedure

1. Click the **Account** `
2. View the **Last logged in:** entry.

6.7.9. Changing a Password

This section contains the following topics:

- Changing password from the Users tab
- Applying password to never expire
- Removing the password to never expire setting

> If a user has a System Management role, then only a Superuser or currently logged-in user can see the **Change Password** option.

You can change your Ivanti Neurons for MDM password. You can also change the password for another user if you have the permission.

Procedure

1. Click the Account icon (upper right).
2. 
   Select **Change Password** from the pull-down menu.
3. Enter your current password.
4. Enter your new password.
5. Enter your new password again.
6. To set the password to not expire, select **Set Password to Never Expire**.

> Setting the password to never expire overrides the **Password Expiration Period** defined under Users > User Settings > Password Complexity Setting.

7. Click **Done**.

> To reset local account password to expire, deselect **Set Password to Never Expire**. After the option is deselected, a pop-up window shows the previous password expiration date applied to the user.

Changing password from the Users tab

Procedure

1. Go to **Users**.
2. Click the display name for the user.
3. Click **Edit** (upper left). The **Authentication Required** window opens. Administrators (who are either local users or LDAP users) are required to authenticate by entering the administrator password before editing the user.
4. Enter your administrator password and click **Authenticate**.

> When multiple incorrect entries of the password are entered and if it crosses the 'Failed Logins Threshold limit' set in the 'Password Complexity Settings', the account will be locked and you will be logged out from the current session.

5. Enter the current password in the **Current Password** field.

> This field will not be displayed if you are changing the password for another user.

6. Enter the new password in the **Change Password** field.
7. Confirm the new password.
8. Click **Save** (upper left).

Applying password to never expire

1. Go to **Users**.
2. Select one or more users.
3. Click **Actions**.
4. Select **Assign Password Never Expire**. The **Set Local Account Password to Never Expire** window is displayed.
5. Click **Submit**.

Removing the password to never expire setting

1. Go to **Users**.
2. Select one or more users.
3. Click **Actions**.
4. Select **Remove Password Never Expire**. The **Remove Local Account Password Never Expire** window is displayed.
5. Click **Submit**. After this setting is removed, the previous password expiration date will be applied to the users.

6.7.10. Sending a Message

This section contains the following topics:

- Sending a message to users
- Sending a message to devices

You can send a message to any known user. Messages can be email or {{push notifications}}. Only users having enrolled devices can receive push notifications.

Prerequisites

- For iOS devices, ensure that Go client is installed.
- For macOS devices, ensure that Mobile@Work client is installed.

Sending a message to users

1. Go to **Users > Users**.
2. Select the users you want to message.
3. Click **Actions** (upper right-hand side).
4. Click **Send Message**.
5. If you do not want to send email, clear the **Send an Email message** check box.
6. If sending email, enter a subject and message text.
7. If sending a push notification, select the **Send a Push Notification** check box and enter message text.
8. Click **Send**.

Sending a message to devices

1. Go to **Devices > Devices**.
2. Select the devices you want to message.
3. Click **Actions** (upper right-hand side).
4. Click **Send Message**.
5. Optionally, click the device name link to go to the Device details page and click the **Send Message** icon.
6. If you do not want to send email, clear the **Send an Email message** check box.
7. If sending email, enter a subject and message text.
8. If sending a push notification, select the **Send a Push Notification** check box and enter message text.

> A push notification message can also include URLs which the users can access.

9. Click **Send**.
   When a push notification is sent to the user, the user will be able to see a bell icon on the device screen toolbar. Tapping the bell icon, the user can view the history of notifications received and can perform an action or delete a notification.

Available within both the **Devices** and **Users** pages, the admins can insert specific device or user attributes into messages that are then queued for end-user delivery.

6.7.11. Removing Users from User Groups

This section contains the following topics:

- Removing users from the Users page
- Removing users from the User Groups page

Removing a user from a user group means:

- any roles assigned to that group are removed from the user
- any apps assigned to that group are no longer available in the user's {{app catalog}}
- apps that were configured to be removable are removed from the user's devices

Removing users from the Users page

1. Select the user you want to work with.
2. Click **Actions** (upper right-hand side).
3. Select **Remove from Group**.
4. Select the groups.
5. Click **Remove**.

Removing users from the User Groups page

1. Click the user group to display its details.
2. Click **Edit**(upper right).
3. Click the **Remove** link next to the user you want to remove.
4. Click **Save** (upper right).

6.7.12. Deleting a User

This section contains the following topics:

- What happens when you delete a local user
- What about LDAP users?

Procedure

1. Go to **Users > Users**.
2. Select the entry for the user.
3. Click **Actions** (upper right-hand side).
4. Select **Delete**.

When an Ivanti Neurons for MDM Administrator or Partner Administrator attempts to delete a Partner Administrator, Ivanti Neurons for MDM displays a message conveying that a Partner Administrator must perform this operation on the Service Provider Portal.

> If a user has some devices associated with their account, first you must retire and delete the devices and then delete the user. If user has no devices the user information can be deleted when the user is deleted.

What happens when you delete a local user

- All information related to a deleted user is deleted from the system.
- Devices associated with the user are retired.
- Content uploaded by the user remains.
- No further device registrations are allowed for the user's account.

What about LDAP users?

- If the LDAP server has been disabled, an LDAP user cannot be permanently deleted. The next sync of LDAP data will restore a deleted LDAP user.
- If the LDAP server or group has been deleted, the LDAP users become local users and can be deleted.
- When a user is deleted from LDAP, it will not be deleted from Cloud. The sync status will switch to "NO_SYNC", but the user will not be removed.

6.7.13. Exporting Users

As an administrator, you can export a list of users from Ivanti Neurons for MDM.

> When the user device registration PIN is exported to a CSV file, the PIN will be masked as '' instead of the actual PIN for security reasons.

Procedure

1. Go to **Users > Users**.
2. Select one or more users from the list.
3. Click **Export to CSV**.

You will be prompted with a pop-up informing that the export report would take some time to process. After submitting the request, you must wait for the request to be completed and to submit another request. Once the report is ready, the you will be prompted with a message to either Download or Delete the generated report. You will also receive an email containing a link to download the report.

> The **Custom User** and **LDAP** attributes details can also be exported to a CSV file along with other details.

> When a user is added with any field value that contains either +,-,=, or @ characters, the user data in the exported CSV file will automatically prefix the field with a single quote (') and the pipe (|) symbol will be added with a backslash (\). This is done to prevent Excel injection vulnerability.

6.7.14. Assigning Custom Attributes to Users

You can assign custom user attributes such as Department to one or more users. Each attribute has a corresponding value that you can use for tasks like creating configurations and user groups. You can assign custom attributes to one or more users.

Procedure

1. Go to **Admin > System >Attributes** to create new custom attributes if required.
2. Go to **Users**.
3. Select one or more users.
4. Click **Actions**.
5. Select **Assign Custom Attributes**.
6. Select one of the following options:
    - Force assign (overwrite) all attributes even if any existing values are found.
    - Overwrite only if value is empty, and skip attributes with existing values.

Select the attributes you want to assign and enter their values (empty values are not allowed).

8. Click **Assign**.

Related topics:

- Attributes
- Variables

6.7.15. Removing Custom Attributes from Users

You can remove custom attributes from one or more users.

> Proceed with caution as this action is not reversible.

Procedure

1. Go to **Users**.
2. Select one or more users.
3. Click **Actions**.
4. Select **Remove Custom Attributes**.
5. Select the attributes you want to remove.
6. Click **Remove**.

Related topics:

- Attributes
- Variables

6.7.16. Changing the User Locale

By default, the user locale is set to the tenant locale. If required, you can change the locale for a single user.

Procedure

1. Go to **Users**.
2. Click the display name for the user.
3. Click **Edit**. The **Authentication Required** window is displayed.
4. Enter your administrator password and click **Authenticate**.

> When multiple incorrect entries of the password are entered and if it crosses the 'Failed Logins Threshold limit' set in the 'Password Complexity Settings', the account will be locked and you will be logged out from the current session.

5. Under the Locale field, click **Change**.
6. In the **Change User Locale** window, select the required locale from the **Change user locale to:** drop-down list.
7. Click **Done**.
8. Click **Save**.

6.7.17. Editing a Username

When you add a user, the text you enter for the email address is automatically listed for the username, as well. In most cases, you should leave the default username in place because:

- A username in the format of an email address is required.
- It is convenient to use the username **variable** in configurations, though the email address can also be used.

The only time to edit a username is in the rare event of a conflict with an existing username, because usernames must be unique across the entire device management system. A conflict might happen, for example, if two departments in an organisation sign up for the device management system.

If a username conflict happens

If you cannot add a user because of a username conflict, enter a different username using the format of an email address. The email address does not have to correspond to an actual email account. For example, you can change the following email address:

ksmith@mycompany.com

to

ksmith21@mycompany.com

If you edit the username, then any configurations that include the username as a variable will not work for this user. Create alternate configurations that use the email address variable, instead.

6.7.18. Opting Out of Location Data Collection

This section contains the following topics:

- For iOS devices
- For Android devices

If a privacy configuration is applied to enable the collection of location data, the device user can override the configuration.

For iOS devices

iOS device users can turn off location services to prevent sending location data to the device management system from the following setting:

Settings > Privacy > Location Services

For Android devices

Android device users can turn off the location setting to prevent collection of location data. The location of this setting varies by manufacturer. Android device users are also prompted to accept the request for location data.

6.7.19. Timeout Information

Inactivity timeout of the administrative portal is between 5 to 15 minutes and timeout is 24 hours.

Procedure

1. Go to **Users > User Settings**.
2. Edit the default **Password Complexity** settings.
3. In the Password Policies section, move the **Inactivity Timeout** slider to specify the time a user maybe inactive before an Admin Portal or a Self Service portal session time. Number ranges between 5 to 60(minutes).
4. Click **Done**.

6.7.20. Opting Out of System Usage Analytics

Anonymous product diagnosis and usage data are collected to help in product improvement.

If you wish to keep your usage data proprietary, you can opt out of sending system usage analytics.

Procedure

1. Click **Usage Data** link at the bottom of the page in the Ivanti Neurons for MDM administrative portal. The **Usage Data** window is displayed.
2. Clear the **Send out diagnostics and usage data** checkbox.
3. Click **Save**.

6.7.21. Device Registration by PIN Generation

This section contains the following topics:

- For Single or Multiple Users from the Users Landing Page
- For a Single User from User Details

You can generate Device registration PINs for users without sending an invite email, streamlining the device registration process.

For Single or Multiple Users from the Users Landing Page

1. Go to Users > Users.
2. Select the user(s) for whom you want to generate a registration PIN. You can select one or multiple users.
3. Click on the **Actions** button.
4. Select **Generate PIN** from the dropdown menu.
5. The generated PIN(s) will be displayed in the **REGISTRATION PIN** column.
6. To view the PIN(s), click on **View PIN**.

For a Single User from User Details

1. Go to Users > Users.
2. Click the username for whom you want to generate a registration PIN to open the user details.
3. In the User Information section, click on **Generate PIN**.
4. Click on **View PIN** to view the generated PIN.

> Ensure that you have the appropriate permissions to generate registration PINs for users. Generate PIN option is enabled only for users whose Device Registration status is 'Password & PIN.'

7. Devices

This section contains the following topics:

- Getting Started with Devices
- Device Groups
- App Inventory
- Managing Devices

7.1. Getting Started with Devices

This section contains the following topics:

- Managing devices
- Performing actions on a device
- Setting the time zone for a device
- Listing devices by criteria
- Displaying detailed device information
- Bulk assign or change users and custom attributes to devices
- Exporting devices to a CSV file
- Searching device logs

Each entry in the **Devices** page represents a mobile device that has been registered with Ivanti Neurons for MDM and lists important information about the device. The Devices list page displays devices with information such as:

- Name
- Email Address
- Phone No.
- OS
- Device Type
- Status
- Last Check-In
- Violation Count
- Space
- Legal Owner (for Shared iPads)

The Wi-Fi IP address is reported to the Ivanti Neurons for MDM server. Any changes to the IP address is reported at every check-in. GDPR-compliant IP address is available as an option in the device list page and in the device details page. This feature requires devices to be registered via Go 5.5 for iOS or later versions, and Go 72 or later versions for Android as supported by Ivanti Neurons for MDM.

> As new GDPR fields (such as IP Address and eSIM ID) are added over Ivanti Neurons for MDM releases, the admins who have configured GDPR already need to edit the GDPR profile if they want to hide the new fields.

The equipment identifier (EID) shows up as an iOS attribute when a device list is exported to spreadsheet (CSV) format. The EID and mobile EID (MEID) (when present) are prefixed by an EID string or MEID string, respectively.

> The Ivanti Neurons for MDM server cannot handle processing the same device with different client identifiers and registered across different tenants. The server can only handle the instance where it is the same device with different client identifiers and registered to the same tenant.

Managing devices

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Go to **Devices**.
3. Select one or more devices.
4. Select an action from the **Actions** drop-down list.

The following table lists the actions that are available on the Devices page:

Category	Action
Common	• Add to Group • AppConnect Unlock> • Assign Custom Attributes • **Assign to User** • Device Compliance Status Sync • Disable Remote Desktop • Enable Remote Desktop • Enable/Disable Bluetooth • **Force Check-in** • **Lock** • Remove Custom Attributes • Restart/Shutdown • Device Compliance Status Sync • **DeviceRetire** • **Send Message** • Set Ownership • **Unlock** • **Wipe**
iOS	• **Assign to Legal Owner** (Shared iPads only) • Reinstall iOS System Apps • Set Time Zone
macOS	• Set macOS Auto Admin Password • Set/Change Firmware Password • Set/Change Recovery Lock
Android	• Enter Kiosk Mode • Exit Kiosk Mode
Windows	Scripts and Actions via Ivanti Bridge

Performing actions on a device

The Actions menu (ellipsis button) lets you perform various actions on a selected device.

Procedure

1. Click a device name. The device details page opens.
2. Click the Actions (ellipsis) menu to perform one of the following device actions:
    - Change Device Name
    - Delete Device
    - Edit Group Membership
    - Enable/Disable Bluetooth
    - Scripts and Actions via Ivanti Bridge
    - Pull Ivanti Bridge Log
    - **Relinquish Ownership**
    - Request Debug Logs
    - Restart/Shutdown Device
    - Retire
    - Set Ownership
    - Set/Change Recovery Lock
    - Wipe
    - Device Compliance Status Sync

Setting the time zone for a device

Applicable to: iOS 14.0+ and tvOS 14.0+ devices

This action does not require Location Services. The time zone device action is also displayed in the device details page of a device. Time zone changes made in the device will also reflect in the Ivanti Neurons for MDM server.

> This device action triggers an error if the **Force automatic Date & Time** restriction is enabled in **iOS Restrictions configuration**.

Procedure

1. Select one or more devices.
2. Click **Actions** > **Set Time Zone** for the selected devices.
3. Enter the timezone string in the Olson Time Zone ID format. For example, Pacific/ Midway.
4. Click **Set Time Zone.**

Listing devices by criteria

You can use the Filters side navigation bar to search and view specific devices among the entire list of devices. Use the Space drop-down list to select all or specific spaces to view the devices and their related information. You can also search for devices using either the display version or the bundle version. The Devices page displays both bundle version and display version of devices.

When you navigate from the Device Group page and click the number that is listed under the **# of devices** column or from the **#Installed** column in the **App Inventory** page, a message is displayed indicating the name of the space for which the devices are listed in the page.

Displaying detailed device information

Click the link in the Name column of an entry to display the Device Details page. The Device Details page contains several tabs organising the following information:

- **Overview** - The following table lists all the details displayed on the Overview tab:
- **Configurations** - Displays the details of the applied configurations For more information, see **Working with Configurations**.

Section name	Description
General	• Device Location • Manufacturer • Wi-Fi MAC Address • WiFi-IP Address (Android devices) • Network Tethered - (iOS devices) • Has Battery - (Only for macOS 13.3+) • IP Address • Public IP Address - Displays the device's IP address for Android or ChromeOS. If the device connects to a VPN or proxy server, it shows the proxy WAN IP address. • Model Number - (macOS 13.3+ and iOS 16.4+) • Serial number • Alternative Serial Number (Android devices) - Manufacturer specific serial number applicable for Samsung devices in Device Admin or Device Owner mode. • Lock PIN - Administrators can remotely lock a managed device and generate a unique PIN to unlock it manually. Select **View** to display the PIN on the **Device Details** page for users with administrator privileges. Applicable for macOS devices only. • Storage Usage - Used (except Windows) and available internal storage on devices • Available Battery (Android) • Battery Status (Android) - Charging, Discharging, Full, and Not Charging • Battery Estimated Charge Remaining (Windows) • Battery Estimated Runtime (Windows) • Update Available (macOS) • Available Update Name (macOS) • OS Version • OS Build Version • Supplemental Build Version • Supplemental OS/Version Extra • Apple Silicon Device • Firmware Version • Device Source • Legal Owner • Multi-User Mode • Time Zone • Last Known Device Unlock Passcode • Security Lockdown Mode • System Update (Android devices)

Section name	Description
	• Zebra patch Version (Android devices) • Last Hotfix ID - (Windows devices) • Last Hotfix Installed On - (Windows devices) • MDM Enrollment Type • MDM Return to Service (iOS 27.0+ and visionOS 27.0+)
Settings	• Device Name • Device Identifier • Device GUID • Device Enrollment Device (Apple devices) • Device Enrollment Enrolled (Apple devices) • Automated Device Enrollment Enabled • Automated Device Enrollment Enrolled • User Enrollment Enrolled (Apple devices) • Registered Managed Apple ID (Apple devices) • Device Groups • Language • MDM Device Identifiers • Device Client ID • Client App version • Client App BundleID • Client Registered • EAS Device Identifiers • Activation Lock Enabled • Apple Declarative Management Enabled • Apple DDM App Enabled • Activation Lock Bypass Code • Terms of Service • Ownership • iTunes Account Active • Device Location Service Enabled • Quarantined • Sentry Blocked • Access Blocked • Compliance Action Blocked • APNS capable

Section name	Description

	• Supervised Mode (iOS and macOS devices) - Identifies a supervised device. Device remains in direct control of the IT team. The supervised mode enables additional device capabilities (for example, field service deployments, retail point-of-sale devices), "loaner" devices used in hospitality and services, and devices shared among students in a classroom lab.
	• Wipe PIN - Click **View** to display the PIN.
	• Managed macOS Admin user (macOS devices)
	• Local macOS Admin Password (macOS devices) - Select **View**, to see the **Admin Password**, **Password Last Rotated**, **Next Rotation**, and **Reason** information about enrolled and managed devices using Automated Device Enrollment.
	After the admin views the password, it might take up to another hour (next check-in) for the password to rotate from the displayed **Next Rotation** time.
	• Device Encryption Status (macOS devices)
	  ◦ FileVault Encryption Enabled
	  ◦ Personal Recovery Key Used
	  ◦ Institutional Recovery Key Used
	• Bootstrap Token Available
	• System Integrity Protection Enabled
	• Firmware Password
	  ◦ Password
	  ◦ Change Pending
	  ◦ Command Status
	  ◦ Allow Option ROMs
	• Recovery Lock
	  ◦ Password
	  ◦ Recovery Lock Enabled
	• Mobile@Work for macOS Script
	• Firewall Settings (macOS devices)
	  ◦ Firewall Enabled
	  ◦ Block All Incoming
	  ◦ Stealth Mode
	• Application Firewall Status (macOS devices)
	• Firewall Status (Windows devices)
	• Last backup to iCloud (iOS devices)
	• Passcode Lock Grace Period (iOS devices)
	• Android ID
	• Android Security Patch Level (Android devices)
	• Kiosk Mode (Android devices)

Section name	Description
	• Android SafetyNet Attestation Type (Android devices) • Android Enterprise Capable (Android devices) • Android Work Enabled (Android devices) • Samsung SAFE Capable (Android devices) • Android Work Managed Devices (Device Owner) Enabled • Android Work Profile on Company Owned Device Enabled • Anti-phishing native status • Anti-phishing status • Anti-phishing VPN status • Android Managed Device with Work Profile • Android Work Profile on Company Owned Device Lock Enabled • Help@Work Available • Zebra Capable • Secure Apps Status • Secure Apps Encryption Status • Secure Apps Encryption Mode • FCM Enabled • MTD activation status
Windows Information Protection (Windows devices) **Telephony**	• WIP • App Locker Configured • EDP Mandatory Settings **Device Service Subscriptions** • Phone number • Mobile Technology • IMSI • ICCID • IMEI • IMEI 2 - (Only on Android devices with dual SIM port. Applicable on Android 8.0 or higher) • MEID • Device Location • Carrier • Home MCC • Home MNC • Current Country Name • Home Country Name

Section name	Description
	• Mobile Technology • Roaming • Current Operator • Current MCC • Current MNC • Data roaming • Voice roaming • EID - (applicable for supported Android devices) **SIM Service Subscriptions** - (applicable for supported iOS devices) For supported iOS devices, these properties are displayed for multiple eSIM active service subscriptions. • Carrier Setting Version • Carrier Setting Network • Current MCC • Current MNC • EID • ICCID • IMEI • Data Preferred • Voice Preferred • Label • Label ID • Phone Number • SIM Slot • Is Roaming • Subscriber Carrier Network **SIM Service Subscriptions** - (applicable for supported Android devices) For supported iOS devices, these properties are displayed for multiple eSIM active service subscriptions. • Carrier Setting Version • Current MCC • Current MNC • ICCID • Data Preferred • Voice Preferred • Subscription ID • Phone Number

Section name	Description
	• SIM Slot • Is Embedded • Managed
Azure Device Compliance	• Azure Device Identifier • Azure Device Compliance Status • Azure Client Status Code • Azure Device Compliance Report Time • Azure Intune Device User UPN
Google BeyondCorp Device Compliance	• Device Identifier • Compliance Status • Compliance Report Time • User
Battery Information	• Battery Level - Displays current battery charge level as reported by the Android OS • Battery Health Status - As reported by the Android, Mac, iOS, and iPad devices. • Battery Charging Status - As reported by the Android OS • Battery Health Percentage (OEM Specific) - Battery health in percentage for supported device manufacturers such as Zebra devices • Battery Manufacture Date (OEM) - Battery manufactured date for supported device manufacturers such as Zebra devices • Battery Charge Cycles (OEM) - Number of cycles completed in total for supported device manufacturers such as Zebra devices
Device Component Health (applicable for iOS 27.0+ and macOS 27.0+ Supervised Devices)	• **Baseband**: Indicates the Baseband health status of the device. • **Camera**: Indicates the Camera health status of the device. • **Display**: Indicates the Display health status of the device. • **Face ID**: Indicates the Face ID health status of the device. • **Near Field**: Indicates the Near Field Communication (NFC) health status of the device. • **Touch ID**: Indicates the Touch ID health status of the device. • **Ultra Wideband**: Indicates the Ultra Wideband health status of the device.

- **Installed Apps** - Displays the details of the applications that are installed on the device. The installation date of the current version of the installed app is displayed under the **App Reported Date** column. Search the installed apps for the device as follows:
- App Name
- Bundle or Package ID

> The app installation date of the devices coming out of quarantine is the date when the device is removed from quarantine.

> In the case of Android Enterprise devices, you can also view the installed apps usage details sorted by Day, Week, Month, or Year. To view these details, you must have selected the **Enable App usage data collection** option available in the **Configuration Setup** section, and then you can select **App Usage - Day**, **App Usage - Week**, **App Usage - Month**, **App Usage - Year** options to view the app usage details.

- **Available Apps** - Displays the details of the applications that are available for the device. Search the available apps for the device as follows:
- App Name
- Bundle or Package ID

In the **App Configurations** column, when you select the **Configuration Name**, you will be directed to the app catalog's **App Configuration** tab to review the app configuration options. If needed, you can modify the app configurations for the device on the **App Configurations Summary** page. For more information about configuring an app, see App Configuration.

In the **App Configurations** column, when you select the **Configuration Name**, you will be directed to the app catalog's **App Configuration** tab to review the app configuration options. If needed, you can modify the app configurations for the device on the **App Configurations Summary** page. For more information about configuring an app, see App Configuration.

> Make sure to remember the specific app configuration's name and type for the assigned device on the **App Configurations** page.

> The **Status** column indicates the application installation status on the device. The App installation status is captured only for managed applications. The application installation status for unmanaged apps is displayed as Not Installed. You must convert the application to Managed to view the correct installation status.

- **AppConnect Apps** - Details of the installed AppConnect apps.
- **Policies** - Details of the applied policies. For compromised devices, check the violation reason in the Violation column. If the device has been rooted, the system displays the reason shown in the **Violation** column:

Priority (1 = highest)	Violation
1	Plugin compromised
2	Client tampered
3	Unknown device manufacturer: unknown
4	Suspicious folder detected: [path]
5	Suspicious binary found at: [path]
6	Folder /data is browsable OR Folder /data/data is browsable
7	Found /system/app/Superuser.apk
8	Package manager compromised
9	Suspicious app found: [package]

- **Certificates** - details of the installed certificates.
  For the usage of the certificate, check the Usage Type column. If the certificate is device specific, it displays the usage type as 'device'. If the certificate is user specific, it displays the usage type as 'user'.
- **Sentry** - Sentry information (ActiveSync associations)
- **Attributes** - Custom Attributes and Device attributes
- **Users** - Displays the list of active users for supervised MacOS device.

> **Users** tab is enhanced and shows the managed apple id as a hyperlink, clicking which redirects to user account details page in a Shared iPad device.

- **Logs** - View and customise device filters. You can do the following from the Filters:
  - Select the Action name to filter devices based on application actions.
  - Select Status.
  - Specify the Start Date and the End Date.
- **Hardware** - Hardware inventory details (system, motherboard, BIOS, hard drive, CD ROM, processor and physical memory)

Bulk assign or change users and custom attributes to devices

You can use the Bulk Assign via Upload icon to upload a CSV file to assign or change users and/ or custom attributes to devices in bulk.

Procedure

1. From the Devices page, click the **Bulk Assign via Upload** icon (next to the Actions button).
2. (Optional) Click **Download template** to save a CSV template file that you can edit and upload.
3. After the CSV file is ready, click **Choose File** to browse to the CSV file location or drag and drop the CSV file to the File data section.
4. Select one of the following options:
   - **Force assign (overwrite) all attributes even if any existing values are found**
   - **Overwrite only if value is empty, and skip attributes with existing values**

Click **Upload**.

Exporting devices to a CSV file

You can export the device details of a specific device using the **Export to CSV** option from the **Devices** page.

Procedure

1. Go to **Devices**.
2. Select all or multiple spaces to view the information related to specific spaces.
3. Click the devices count link. The Devices list page related to the selected space is displayed.
4. Click the **Export to CSV** option to export the devices list and related details to a CSV file. A pop-up message appears that the export report would take some time to process. Wait for the request to complete before you submit another request. Once the report is ready, you will be prompted with a message to either Download or Delete the report.
5. Click **Download**. You will also receive an email containing a link to download the report.

6. (Optional) Click **Delete** to delete the report.

Searching device logs

Procedure

1. Go to **Devices** > **Devices**, click the **Name** column link of an entry.
2. Click the **Logs** tab.
3. Use the Action, Status, Start Date, and End Date filters to narrow the displayed devices. You can do the following from the Filters:
    1. Select the Action name to filter devices based on application actions.
    2. Select Status.
    3. Specify the Start Date and the End Date.
4. The Device Details column displays the status of the application as follows:
   For all devices the status shows the following details:
    - App name, app version, bundle, or package ID
    - Status of installation
    - Any errors and reason for the error
      For example - appOrConfigName=Name:<app name>;Identifier=<bundleid>;iTunesStoreId:<itunesid>;Status:<status or error reason from Apple>version: <app version>

For Windows devices the status shows the following details:

- Include bundle ID or package ID, status, and errors
  For example -
- For type - application inventory and status - acknowledge - displays - appType
- For type - application inventory and status - sending - Does not display anything
- For type - install/uninstall and status - success/failure/sending - displays Include bundle ID or package ID, status, name, version, and errors

If you cannot see the **Devices** page, it might be that you do not have the required permissions. You need one of the following **roles**:

- Device Management
- Device Read Only

7.2. Device Groups

This section contains the following topics:

- Adding a device group
- Removing a device group
- Exporting devices to a CSV file
- Assign Custom Attributes to Device Groups

In the **Device Groups** page, you can create lists of devices that you want to treat in the same way. You can define and assign policies and configurations to the device groups. The following are the default device groups created by Ivanti Neurons for MDM:

- All Devices
- Android Devices
- Android Enterprise Devices
- iOS Devices
- Device Type (Apple)
- tvOS Devices
- macOS Devices
- visionOS Devices
- watchOS Devices
- Windows Devices

The details of the apps assigned to a specific device group is displayed under the **Apps** tab for the specific device group.

Adding a device group

> Adding a device group is not applicable to Dynamic User Groups.

Depending on the type of license you have, you can add a new device group based on rules to identify the devices with specific criteria. The devices matching the rules are displayed below the rule builder section. The rules can be nested together using the ANY (OR) or ALL (AND) options. The rules can be constructed using the following operators:

- begins with
- ends with
- contains
- does not contain
- does not begin with
- does not end with
- is less than
- is greater than
- is in range
- is equal to

- is not equal to
- is not blank
- is blank

The Ivanti Neurons for MDM Administrator displays a number of duplicate user groups and the corresponding number of GUIDs to identify duplicate groups, when the User Group Name attribute is selected in the rule builder. Also, a table under this rule displays the list of the duplicate user groups and their details such as User Group Name, GUID, Source and distinguished name (DN).

Bronze licence:

Rules can identify devices by the following criteria:

- Device Type
- OS - operating system (pre-populated)
- OS Version
- OS With Version
- User Group

Silver licence:

Rules can identify devices by the following criteria:

- Entra ID Enrolled
- Alternative Serial Number (Android Only - applicable for Samsung devices in Device Admin or Device Owner mode)
- Android Dedicated Device
- Android Enterprise Capable
- Android Managed Device with Work Profile
- Android SafetyNet Attestation Type
- Android Work Enabled
- Android Security Patch Level (Android devices)
- Android Work Managed Devices (Device Owner) Enabled
- Android Work Profile Enabled
- Android Work Profile on Company Owned Devices Enabled
- Anti-phishing native status
- Anti-phishing status
- Anti-phishing VPN status
- APNS Capable
- Apple Silicon Device
- Automated Device Enrollment Enabled
- Automated Device Enrollment Enrolled
- Azure Device Identifier
- Azure Device Compliance Status
- Azure Client Status Code

- Azure Device Compliance Report Time
- Baseband Health Status
- BitLocker Encryption
- Sentry Blocked
- Access Blocked
- Bootstrap Token Available
- Bulk Provisioned Type (Apple Configurator or None)
- Carrier
- Camera Health Status
- Client Last Check-in
- Client Registered
- Compliance
- Compliance Action Blocked
- Current Country Name (select the current country name from the drop down list)
- Current MCC
- Current MNC
- Custom Device Attribute
- Custom LDAP Attribute
- Custom User Attribute
- Data Roaming
- Device Name
- Device Registered
- Device Source
- Device Type
- Display Name
- Display Health Status
- Encryption Enabled
- Face ID Health Status
- Hard Drive Partitions
- Home Country Name (select the home country name from the drop down list)
- Home MCC
- Home MNC
- IMEI
- IMEI2 (only on Android devices with a dual SIM port and applicable for Android 8.0 or higher devices)
- Institutional Recovery Key Enabled
- IP Address
- Kiosk Mode

- Last Check-in
- MAM Only
- Manufacturer
- MDM Enrollment Type
- MDM Return to Service (iOS 27.0+ and visionOS 27.0+)
- Multi-User Mode (iOS 27.0+)
- MTD activation status
- NFC Health Status
- OS
- OS Build Version
- OS Edition
- OS Version
- OS With Version
- Ownership
- Phone No.
- Public IP Address (Android or ChromeOS devices)
- Personal Recovery Key Enabled
- Quarantined
- Recovery Lock Enabled
- Roaming
- Secure Apps Status
- Security Lockdown Mode
- Serial Number
- Status
- Supervised
- System Version
- Total Device Capacity
- Total Memory MB
- TPM Version
- Touch ID Health Status
- Unlock Token Available (iOS)
- User Enrollment Enabled
- User Group
- Ultra Wideband Radio Health Status
- Voice Roaming
- macOS Personal Recovery Key escrowed
- macOS Recovery Key Type

Procedure

1. Click **Add**.
2. Enter a name for the group.
3. Enter an optional description for the group.
4. Select the type of device group you want to create:
   - **Dynamically Managed**: Use rules to define which devices are in the group.
     - **Load from Advanced Search**: Select this option to open a library of your saved searches. Choosing a query will automatically populate the device group's name and rule criteria based on the selected search.

     > You can create and save these queries by navigating to **Devices** > **Devices** > **Advanced Search**. Any query saved there will automatically be available to load here.

   Manually Managed: Enter each user whose devices are to be included in the group.
5. For dynamically-managed groups:
   1. Create a rule that defines the group.
   2. **Example**: OS is iOS
      Click **+** to create additional rules, if needed.
   3. **Example**: Device is iPhone 5S
      Click **Any** if the devices need to match at least one of the rules.
   4. Click **All** if the devices need to match all the rules.
6. For manually-managed groups:
   1. Type the name of a user whose device you want to add.
   2. Select the device from the displayed list.
   3. Repeat steps a and b until all devices are displayed in the list.

Click **Save**.

Removing a device group

Procedure

1. Go to **Devices** > **Device Groups**.
2. Click the check-box for the device group you want to remove.
3. Click **Delete Device Group**.

Exporting devices to a CSV file

You can export the device details of a specific device group using the **Export to CSV** option from the **Device Groups** page.

Procedure

1. Go to **Devices** > **Device Groups**.
2. Select all or multiple spaces to view the information related to specific spaces.
3. Click the device group count link. The Devices list page related to the selected space is displayed.

4. Click the **Export to CSV** option to export the devices list and related details to a CSV file. A pop-up message appears that the export report would take some time to process. Wait for the request to complete before you submit another request.
5. Click **Download**. You will receive an email containing a link to download the report.
6. (Optional) Click **Delete** to delete the report.

If you cannot see the **Device Groups** page, it might be that you do not have the required permissions. You need one of the following roles

- Device Management
- Device Read Only

Assign Custom Attributes to Device Groups

Administrators can now assign custom attributes directly to device groups. Any device that becomes a member of a device group automatically inherits the configured custom attribute values, eliminating the need to manually assign attributes to individual devices after enrollment. Use device groups to automatically assign custom attribute values to devices that become members of the group.

Procedure

1. Go to **Devices** > **Device Groups**.
2. Select an existing group or create one.
3. In the Device Group details page, click **Attributes**.
4. Click **Add New**.
5. Choose the custom attribute and specify the required value.

7.3. Unmanaged Devices

This section contains the following topics:

- Blocking a device
- Unblocking a device
- Clearing a device from the device list

Licence: Silver

If you have set up Sentry email access control, any unregistered devices that access your email system are called unmanaged devices. You define whether unmanaged devices should have access to email by default when you set up a Sentry. You can then manually allow or block email access for these devices.

> The Unmanaged Devices page is updated every 5 minutes. Therefore, changes in management are not immediately reflected.

Blocking a device

Procedure

1. Select the device.
2. Select **Actions > Block**.

The device remains blocked until you select **Actions > Allow** or **Actions > Delete**.

Unblocking a device

Procedure

1. Select the device.
2. Select **Actions > Allow**.

The device continues to have access to email until you select **Actions > Block** or **Actions > Delete**.

Clearing a device from the device list

Procedure

1. Select the device.
2. Select **Actions > Delete**.

The next time the device attempts to access your email system, it will reappear on this list, and you will need to repeat any Block or Allow action you previously applied to the device.

7.4. App Inventory

This section contains the following topics:

- Filtering the display of apps
- Displaying the installed devices for an app
- Displaying the list of apps
- Displaying the installed Win32 or Win32 Store apps on a device
- Creating Custom View Permission
- Exporting an App Inventory

The app inventory is the list of apps detected on enrolled devices. As an administrator you can use this page to get information on the apps being used by enrolled devices. You can answer questions like:

- Which apps are most popular?
- Do iOS devices get their apps directly from the App Store?
- How many Android users have downloaded an optional {{in-house app}}?
- How many devices are using an outdated version of an app?

Filtering the display of apps

When you display the **Devices > App Inventory** page, all apps are listed. To narrow this list to certain apps, use the filters (left pane). For example, to narrow down the list to display only the private apps from Google Play, select **Private** under the **Source** section.

You can view app inventory across all or multiple space devices by selecting multiple spaces from the drop-down list. When you hover on the displayed apps, device counts are displayed. You can click on the count for an app to display all devices containing the app. Each app inventory record will be grouped by space.

You can search using either the App Name or Bundle/Package ID.

If you have selected multiple spaces, then hovering the **Total** value in the **# Installed** column displays the install count per device space.

Displaying the installed devices for an app

Click the **Managed**, **Unmanaged**, or **Total** number listed in the **# Installed** column.

Displaying the list of apps

Click the **# Requested** against the app in the app inventory to view the devices that requested the app. This is applicable only for MAM-Only devices.

Displaying the installed Win32 or Win32 Store apps on a device

The app inventory displays Win32 or Win32 Store apps on a device if the privacy configuration for that device allows for the collection of information for all apps on that device. You can configure the privacy policy for the device.

Procedure

1. Determine which privacy configuration applies to the desired device by following the directions in **Devices**.
2. Go to **Configurations**.
3. For the privacy configuration you noted in step 1:
    1. Select the configuration.
    2. Click Edit.
    3. Under **Collect App Inventory,** select **For All Apps on the Device**.
    4. Click **Done**.

> The Win32AppInventory CSP returns the list of all Win32 and Win32 Store apps installed on the device every 24 hours after the inventory scans run on the device.

Creating Custom View Permission

You can specify custom view permissions for users.

Procedure

1. Go to **Admin**.
2. Go to **Roles Management**.
3. Click **Add Custom Role**.
4. Select the **Space-Specific Role** option.
5. Enter the user name in the **Name** field.
6. From the **Devices** menu, click **App Inventory**.
7. Select the **View** checkbox.
8. From the **Devices** menu, click **Device Actions**.
9. Click **Save**.
10. Go to **Users** in the main menu.
11. Click the new user that you created.
12. Click **Assign Roles**.
13. Select the **app | Space-Specific** checkbox, click **Next**.
14. The **Summary** page displays the permissions that are assigned to the role you created.
15. Click **Done**.
16. Log in as the new user.
17. Click **Devices** from the main menu.
18. Click **App Inventory**.
19. The **App Inventory** page now displays only the permitted applications for the user.

Exporting an App Inventory

As an administrator, you can request App Inventory reports using the **Export to CSV** option.

Procedure

1. Go to **Devices > App Inventory**.
2. Select an inventory from the list.
3. Click **Export to CSV**.
4. Select one of the following options:

- **Export Apps to CSV** to export all the applications in the App Inventory.
- **Export Devices to CSV** to export a specific application as per the following table:

Option	Description
Bundle ID	Enter the Bundle/Package ID of the application.
Do you want to export	Select one of the following options: • Total Installed • Managed • Unmanaged • Requested (for MAM-Only devices)

5. Click **Export**.

The admin will be prompted with a pop-up informing that the export report would take some time to process. After submitting the request, the admin must wait for the request to be completed and to submit another request. Once the report is ready, the admin will be prompted with a message to either Download or Delete the report that has been generated. The admin will also receive an email containing a link to download the report.

If you cannot see the **App Inventory** page, it might be that you do not have the required permissions. You need one of the following **roles**:

- Device Management
- Device Read-Only

7.5. Managing Devices

This section contains the following topics:

- Deploying Windows devices
- Setup Apple Remote Desktop on macOS devices
- Device Registration (iOS, macOS, and Android)
- Device Registration (Windows 10+ PC and Microsoft HoloLens 2)
- Provisioning Package Enrolment with PIN
- Using Bulk Enrollment for Windows devices
- Changing Passcode Settings
- Changing the Device Name
- Finding and Filtering Devices
- Using Device Owner
- Managed Device with Work Profile
- Using Bulk Enrolment for Android
- Bulk Enrollment using CSV File Upload
- Using Samsung Knox Mobile Enrolment
- Enrolling Oculus devices
- Enabling Bluetooth on a Device
- Schedule iOS Update
- Re-install iOS System Apps
- Assigning a Device to a new user
- Reassigning an Android device
- Forcing a device to Check-in
- Locating a Device
- Locking a Device
- Managing Apple devices in lost mode
- Requesting debug logs
- Retiring a Device
- Relinquishing Ownership of a Device
- Wiping a Device
- Deleting devices
- Unlocking a Device
- Restarting or shutting down devices
- Clearing the Restrictions Password (iOS only)
- Deleting Sentry association for a device
- Assigning Custom Attributes to Devices

- Removing Custom Attributes from Devices
- Synchronising and fetching app feedback
- Setting firmware password
- Reissuing a new Personal Recovery Key
- Setting or changing recovery lock
- Apple Access Management
- Group Policy Enrollment

7.5.1. Deploying Apple Devices

Ivanti Neurons for MDM supports management for all your Apple devices. It is a comprehensive solution to provision, manage, update, and secure your fleet providing the end user with the best user experience.

This section contains the following topics:

- Installing your Apple MDM certificate
- Enrolling Apple Devices
- Ivanti Go for iOS Client
- Managing Applications for Apple Devices
- Managing Configurations
- Managing Software Updates
- Setting up iOS/iPadOS Devices
- Setting up watchOS Devices
- Supported device actions for watchOS Devices
- Setting up visionOS Devices
- Supported device actions for visionOS Devices
- Setting up macOS Devices
- Setting up TvOS devices
- Support for Declarative Device Management (DDM)

Installing your Apple MDM certificate

To manage Apple devices, start by requesting and installing an Apple MDM certificate to manage iOS devices. Renew the Apple MDM certificate once a year. (The Apple account used for creating the certificate receives a notification from the Apple site when the expiration date approaches.) Use the MDM Certificate page to add or renew this certificate.

Follow steps described in Install MDM Certificate

Enrolling Apple Devices

You can choose any one of the following method to enroll devices:

- Automated Device Enrollment
- Apple School Manager
- Apple Configurator

Ivanti Go for iOS Client

The next step is to select the enrollment type that your company allows for your devices. Ivanti Neuros for MDM currently supports:

- Device Registration (iOS, macOS, and Android)
- User Enrollment with Apple Business Manager
- Account driven User Enrollment

- Settings (Apple)

Managing Applications for Apple Devices

The App Catalog page in Ivanti Neurons for MDM serves as an interface for administrators to govern their app catalog efficiently. This functionality encompasses the orchestration of mobile applications available to end-users, spanning both public app stores and those earmarked for distribution through Ivanti Neurons for MDM.

Supported Apps:

The App Catalog page aggregates various types of apps, including Public AppStore apps, Custom Apps, in-house developed apps, AppConnect-enabled apps, GoClient for iOS, and M@W for macOS, streamlining the importation process for subsequent configuration and distribution.

On devices operating under Mobile Application Management (MAM)-Only configurations, iOS users are prompted to select an authentication certificate upon accessing the App Catalog. This authentication step is crucial for securing access to the listed apps and aligning with robust security practices.

> M1 chipset MacBooks from Apple offer specialized support for iPhone and iPad VPP apps within [Your Software Product]. Notably, only administrators have the authority to push supported iPhone and iPad VPP apps, restricting users from installing them directly from the App.

For detailed implementation instructions and configuration options, please refer to the comprehensive documentation available in the in the Admin guide and resources below:

- Managing Apps
- App Catalog Settings
- Set up Apple Apps and Books
- Apps@Work Corporate App Store
- MacOS AppStore Restrictions

Managing Configurations

Configurations are collections of settings that you as an administrator send to devices. For example, you can use configurations to automatically set up VPN settings and passcode requirements on the devices. The existing configurations for your system are listed in the Configurations page. You can select multiple configurations from the Configurations page and push them to multiple devices at once. These configurations can be pushed to devices specific to spaces and the devices in other spaces remain unaffected. Configurations can be pushed to either a single space or multiple spaces or all spaces at a time.

Most configurations in Ivanti Neurons for MDM are common to all platforms. For more details on how to work with configurations see Working with Configurations.

Some configurations are supported only by specific Platforms. You can review the list by platform supported on Configuration Types

Managing Software Updates

You can start by setting up the Software Update configuration for your iOS and macOS devices.

> When setting up a scheduled windows for the Software Update, the OS Update command will be pushed every hour to the device to make sure the update does not miss the window. As per Apple behavior every time the OS update command is received by the device a pop-up will notify the user to upgrade. User can defer up to three times. At the third time as per Apple behavior the Device will Force Upgrade.

MacOS devices have some specific rules that can be applied. See macOS Software Update Rules Configuration

OS Update Command for iOS

You can also send a one time command to update to one or more devices from the Device List or from the Device Page. See Schedule OS Update Command.

Setting up iOS/iPadOS Devices

The following configurations are supported for your iOS/iPadOS :

- **iOS/iPadOS Restrictions**
- **eSIM configuration**
  - **Preserve Data Plan**
- **Mobile Network Configurations**
- **Enable Lost Mode**
- **Configuring an iOS MDM Profile**
- **Single App Mode**
  - **Autonomous Single App Mode**
- **Shared iPad for Business**
- **Education Configuration**
- **iOS Custom Configuration**
- **Lock Screen Message**

Setting up watchOS Devices

You can now enroll Apple watchOS devices into Ivanti N-MDM while pairing with the iOS devices.

This feature currently supports: watchOS 10+.

ProcedureProcedure

1. You must enroll the iOS 17+ supervised device.
2. Assign the Apple Watch enrollment configuration to the iOS device.
3. You can now pair your Apple Watch to the iPhone.

> You can pair the Apple Watch after pushing the Watch configuration to the iPhone. You cannot enable Remote Management for an Apple Watch if the Watch configuration is pushed to the iPhone after the Apple Watch pairs with it.

The following configurations are supported for your watchOS devices:

- Cellular_Configuration
- Certificate configuration
- Certificate Transparency
- Identity_Certificate_Configuration
- iOS Restrictions
- Passcode_Settings
- Per-App_VPN_Configuration
- Wi-Fi_Configuration

Supported device actions for watchOS Devices

The following device actions are supported for your watchOS devices:

- Clear passcode
- Lock Apple watch
- Wipe Apple watch
- Unenroll Apple watch from Ivanti Neurons for MDM

> Unenrolling paired iOS device will reset the watch and unpairs from the iOS device.

Setting up macOS Devices

The following configurations are supported for your macOS:

- macOS Restrictions
- Configuring macOS Devices
- Working with Scripts and the Mobile@Work Client
- Configuring a macOS MDM Profile
- Setting Firmware Password
- Enable FileVault
  - FileVault Recovery Key
  - FileVault Options Configuration
- Platform and Extensible SSO
- Active Directory macOS
- Firewall
- Ethernet
- Office 365 Account Creation
- macOS System Extensions
- Media Disk Burning Restrictions
- Privacy Settings

Setting up TvOS devices

The following configurations are supported for your tvOS:

- Apple TV Configuration
- Apple TV Restrictions
- Conference Room Display
- AirPlay Mirroring

Setting up visionOS Devices

You can now enroll Apple visionOS devices into Ivanti Neurons for MDM.

This feature currently supports: visionOS 1.1+

You can enroll visionOS devices using one of the following methods:

- Account driven Device Enrollment
- Account driven User Enrollment
- Device Enrollment

The following configurations are supported for your visionOS devices:

- CalDAV Configuration
- CardDAV Configuration
- Certificate configuration
- Certificate Revocation Checking Configuration
- Certificate Transparency
- Creating DNS Proxy Configuration
- Encrypted DNS
- Email Configuration
- Exchange Configuration
- Google Configuration
- Identity Certificate
- iOS Restrictions
- LDAP Configuration
- Managed Domains
- Network Relay Configuration
- Per-app VPN Configuration
- Single Sign-On Configuration
- Subscribed Calendar Configuration
- VPN Configuration
- Web Content Filter
- Wi-Fi Configuration

Supported device actions for visionOS Devices

The following device actions are supported for your visionOS devices:

- Wipe Apple Vision Pro
- Retire Apple Vision Pro
- Unlock Apple Vision Pro

Support for Declarative Device Management (DDM)

Apple's Declarative Device Management is a modern management protocol that allows managed devices to proactively and autonomously apply their own management settings with less communication. Declarative Device Management is enabled on newly enrolled devices during enrollment or during check-in for already enrolled devices.

Declarative Device Management is automatically enabled on the following eligible devices:

- Computers with macOS 13 or later
- Devices with iOS 16 or iPadOS 16 or later
- Devices enrolled via User Enrollment support Declarative Device Management on iOS or iPadOS 15 or later.
- Apple TV devices with tvOS 16 or later
- Apple Watch devices with watchOS 10 or later
- Apple Vision Pro devices with visionOS 1.1 or later

Current supported Declarative Management Features:

- **Status Channels**:
  - Changes to the OS Version
  - Passcode compliance
  - Passcode present
- **Configuration**:
  - Declarative Management Configuration

Predicates in DDM Configurations

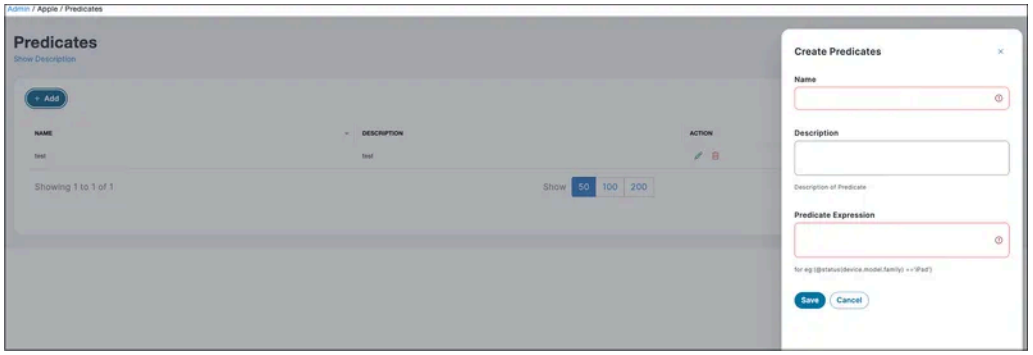
Predicates are expressions in Cocoa language that can provide flexibility and granularity to the activation of a configuration a device. The expression resides on the device and will be applied when the conditions on this predicate are met. We have added a new feature where you can create, save, and apply Predicates to any DDM configuration.

DDM configuration displays a new option in the Distribution page to apply a Predicate. You can find the Predicates already created from the dropdown list in this section.

Creating a Predicate

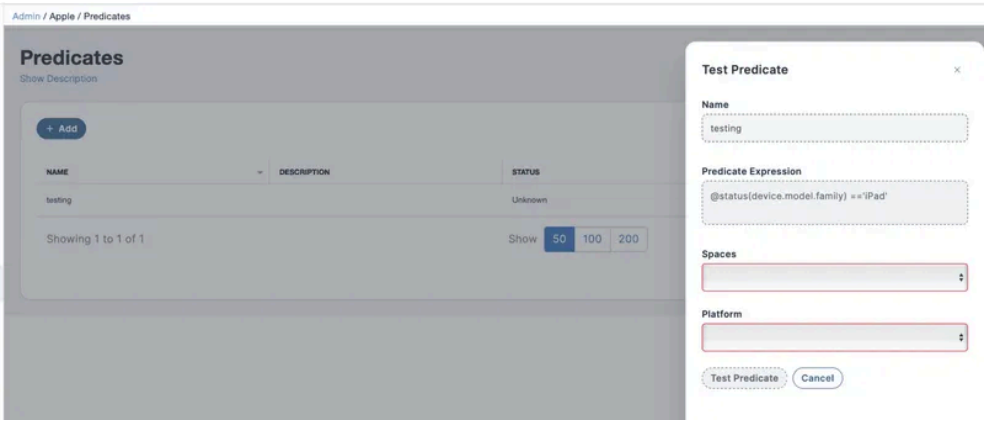
1. Go to **Admin** > **Apple** > **Predicates**.
2. Click **Add**. The Create Predicates window appears on the screen.
3. Enter the following information:
   - **Name** - Name of the predicate
   - **Description** - Add some relevant description

- **Predicate Expression** - Predicate expression. For example, @status(device.model.family) =='iPad'



4. Click **Save**. A dialog appears on the screen confirming the predicate creation.
5. Check the validity of the predicate syntax by refreshing the page and observing values in the STATUS field (with values: **Unknown**, **In Progress**, **Valid**, **Invalid**).
    1. Click **Test**. The **Test Predicate** window appears on the screen.
    2. Enter the following information:
        - **Name** - Default
        - **Predicate Expression** – Default
        - **Spaces** – Default Space
        - **Platform** – iOS/macOS
        - **Device Name** – Related to the predicate expression.

        > The **Device Name** field will appear beneath the **Platform** field only after the **Spaces** and **Platform** field details are selected from the dropdowns.

    3. Click **Test Predicate**.
    4. A dialog appears on the screen confirming the test predicate initiation.
    5. Refresh the page to find the status of predicate syntax.
        - For correct predicate expression, the status changes from **Unknown** > **In Progress** > **Valid**.
        - For incorrect predicate expression, the status changes from **Unknown** > **In Progress** > **Invalid**.
6. Repeat the procedure if you want to create multiple predicates using different Predicate Expressions.

7.5.2. Deploying Windows devices

This section contains the following topics:

- Overview
- Device Management
- Windows Device Enrollment and Registration
- Windows Update Management
- App Control
- Windows Device Management Configurations
- Windows Device Compliance
- Windows Apps and Hardware Inventory

Overview

Ivanti Neurons for MDM helps you to manage all Windows laptops and desktops including HoloLens 2 end-end device life cycle management: from configuration, enrollment, provisioning, securing, application, management, monitoring, software and OS updates, to retirement.

Device Management

Windows devices supported:

- Windows PC 10+
- Microsoft HoleLens 2

For more information about the Device Management and reporting functionality, see **Devices**

Windows Device Enrollment and Registration

Ivanti Neurons for MDM supports all standard device registration methods for Windows devices:

- Manual Registration
- Bulk Enrolment
- via SCCM and Ivanti EPM
- Windows Autopilot
- Entra ID Registration

For more information about the registration methods, see **Using Microsoft Azure**

For information on Multi-User Support, see **Using_Microsoft_Azure.htm#Multi**.

Windows Update Management

- Configuring and Scheduling Windows updates - To configure and schedule Windows updates, create a configuration using Configuration - **Software Updates**.

- Windows Update Management - You can view and approve the updates reported by Windows devices that you want to be updated using Windows Update Management. By using this feature, you can prevent the updates that are not necessary or not tested from being installed on the devices. For more information, see **Windows Update Management**.

App Management and distribution

Users can manage complete App life cycle (Import, configuration, schedule, distribution, update and removal) for Windows applications.

Supported App types:

- In-house
- MSB
- Public store

Supported App extensions:

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

For more details on managing Windows apps, see **App Configuration**. To automate app updates, see **Windows app scheduling** and **Working with Configurations**.

App Control

The App Control configuration allows you to categorise apps as Allowlist or Blockedlist at the device level. Apps that are already installed will not be visible and cannot be launched. Apps will still be visible in the App Store, but they cannot be downloaded or launched. Any device to which the App Control configuration is distributed will use this configuration and ignore any Allowed Apps Policy Settings. The App Control configuration supersedes any app-related policies that refer to the same app on the target devices.

For more details, see **App Control Configuration: Control Which Apps Are Installed Per Device**.

Windows Device Management Configurations

Support for Windows 10+ PC and Microsoft HoloLens 2 includes the following abilities:

- **Device Registration (Windows 10+ PC and Microsoft HoloLens 2)**
- **Passcode Configuration**
- **Exchange Configuration**
- **Configurations**
- **Devices**
- **Apps**
- **Windows app scheduling**
- **App Control Configuration: Control Which Apps Are Installed Per Device**
- **Windows Update Management**

- Device status reporting from Ivanti Neurons for MDM to Azure
- Configuring Windows Autopilot Profiles
- Pushing SyncML to Devices using Custom Configurations
- Policies
- Windows Restrictions
- Identity Certificates
- Windows Hello for Business
- Wi-Fi and VPN Profiles

> Configurations distributed to HoloLens devices that are not supported by this device type, will not be reported as configurations distributed under the Configurations tab in the Device Details.

Windows features (only supported for Windows PC):

- Ivanti Bridge
- Windows BIOS Configuration
- Windows BitLocker
- Windows Kiosk Configuration
- Windows Licence Configuration
- EMA Server Integration Configuration
- Printer Settings
- Remove Bloatware Configuration
- ADMX (GPO) Browser

Windows Device Compliance

Ivanti Neurons for MDM can be set up with Microsoft Azure for seamless enrollment of the users on their Windows desktop and Tablets devices running on Windows 10+. To configure Azure tenant integration to enable Windows Device Compliance, see Using Microsoft Azure.

Windows Apps and Hardware Inventory

Windows App Inventory

The App inventory is a list of apps detected on enrolled devices. Use this page to get information on the apps being used by enrolled devices. For more information, see App Inventory.

> The App Inventory displays Win32 or Win32 Store apps on a device if the privacy configuration for that device allows collecting the information of all apps on that device.

Configuring App inventory intervals

You can set Windows 10 app inventory collection intervals for multiple app source type inventories. The intervals are used when Privacy Configuration is set to collect all apps from the device.

For more information, see **Configuring app inventory intervals**.

Windows Hardware Inventory

You can enable the collection of hardware information from Windows 10+ devices. These details are retrieved using Bridge. For more information, see **Hardware Inventory**.

7.5.3. Setup Apple Remote Desktop on macOS devices

This section contains the following topics:

- Enabling Apple Remote Desktop on macOS devices
- Disabling Apple Remote Desktop on macOS devices

Enabling Apple Remote Desktop on macOS devices

The Apple Remote Desktop feature enables the screen sharing feature and lets you manage the devices remotely. The Apple Remote Desktop feature is available for supervised macOS 10.14.4+ devices.

Procedure

1. Go to **Devices**, select one or more supervised macOS devices.
2. Click **Actions** > **Enable Remote Desktop** action for the devices.
3. Click **Enable Remote Desktop** to confirm.

Disabling Apple Remote Desktop on macOS devices

Procedure

1. Go to **Devices**, select one or more supervised macOS devices.
2. Click **Actions** > **Disable Remote Desktop** action for the devices. The screen sharing feature is disabled and you cannot remotely manage the devices.

7.5.4. Device Registration (iOS, macOS, and Android)

This section contains the following topics:

- Installing the management profile manually
- Sending an invitation (iOS, macOS, and Android)
- Instructing end users to download the app (iOS and Android)

Most users start by registering a device. You can use any of the following approaches to start the registration process:

- Send an invitation to one or more end users (iReg registration)
- Instruct end users to download the Go (in-app registration)

> If iOS and macOS device MDM enrollment fails with the *Profile Installation Failed The SCEP server returned an invalid response.* error, the device user must re-initiate the device enrollment process from the beginning. This happens mostly when the device user takes longer time than expected to complete the iOS and macOS device MDM enrollment process after the profile is downloaded on the device. Please contact Ivanti support for further clarifications.

Ivanti Neurons for MDM supports the user-level management of a single user (local user or registered Active Directory (AD) user) on macOS devices. Administrators can manage devices for the users, apply device profiles and user profiles, and consequentially use App Store, app distribution, configurations, and policies (including Apps@Work, restrictions, security).

To manage macOS devices with AD user, the AD user needs to be the user that is logged in during registration. Any other non-registered user cannot view the registered-user specific profiles (for example, identity certifications, VPN). However, device-level configurations can be viewed and used by any logged-in user.

> The end user must have an account in Ivanti Neurons for MDM before you can start the device registration process. For LDAP users, that means a Connector and an LDAP server must be set up, and the user must be imported from the LDAP server. For local users, that means adding a user.

> The device enrollment URL generated in earlier versions of Ivanti Neurons for MDM will cease to work with the current version. The administrator will need to regenerate the device enrolment URL for device registration.

Installing the management profile manually

Applicable to:

- iOS 12.2 through the most recently released version as supported by Ivanti Neurons for MDM.
- macOS 11.0 through the most recently released version as supported by Ivanti Neurons for MDM.

iOS Device Registration

During in-app registration on iOS devices:

- During device registration using Go app a page with instructions to install the profile appears.
- Click the **Install Downloaded Profile** option and click Click **I Understand**.
- The downloaded profile is valid for a few minutes, after which re-registration is required.

macOS Device Registration

For macOS device registration in the self-service portal, a user must perform the following steps:

Procedure

1. Log in with their credentials.
2. In the Install Management Profile page, the profile is downloaded to the user's local system.
3. Double-click the downloaded profile to make it visible in the user's System Preferences.

> There is limited time for the user to install the profile before it becomes invalid.

4. Open **Profiles** in System Preferences. When the profile is downloaded to the device, users can view a web page having the Profiles link. Click **Profiles** to open the Settings app.
5. Click **Install** to install the management profile.
6. Continue and finish the installation procedure. Enter the system password when prompted.

Sending an invitation (iOS, macOS, and Android)

Start the registration process by sending an invitation. Ivanti Neurons for MDM provides the following ways to send end users an invitation to register a device:

- In the **Startup Wizard**
- When you **add one or more users**
- In the Users page (**Actions > Send Invite**)

> If the end users misplace the invite, you can share the URL that was listed in the invitation. Ensure that you add **/go** at the end of the URL.

End users who have an Ivanti Neurons for MDM account with a password do not need an invitation to start the registration process. You can send them the URL that is listed in the invitation.

Instructing end users to download the app (iOS and Android)

The Go application is available for Android and iOS devices. You can provide instructions to the end users on how to download the application from a public app store and start the registration process from the app. The email invitation contains the following information:

- A link to the registration page
- A one-time use PIN (if set by the administrator)
- Basic instructions for the next steps

If you have already set a password for the account, you can send the password to the corporate email address of the end user. If you are using LDAP for authentication, inform the end user that network credentials are required.

If the user does not complete installation of the MDM profile during registration, then Ivanti Neurons for MDM periodically sends push notifications to the device to prompt the user to complete the registration process.

The user can use either Username and Password or scan the QR code to begin the device registration from Go app. The details are as follows:

- **Username**: Email address
- **Password**: If specified in the **User Settings** and a temporary password is defined by the administrator
- **QR Code**: Generate the QR code from the Ivanti Neurons for MDM self-service portal. When you scan the QR code using the **Scan QR Code** option, a prompt appears on the screen requesting you to grant permission to access the camera on the device. After you grant permission, the camera scans the QR code and the device is registered. This option is supported for Android 9 and later, iOS 14 and later versions.

As an end user, if you receive a registration email on your mobile device, tap the link to start the registration process. If you receive the email on a laptop or desktop, enter the URL in a browser on your mobile device to begin the registration process.

If you do not yet have a password defined for your Ivanti Neurons for MDM user account or if your **User Settings** require a registration PIN, a one-time use PIN is included . After you enter the PIN, you are prompted to set a password for the account if the password does not exist.

> For Android Enterprise devices, when the registration is complete, any manually installed CA certificates to a work profile on company owned device or a work managed device are uninstalled.

Re-enrolling iOS devices

If you want to re-enroll your device you can do so as follows:

1. Launch the Go client on your device.
2. Go to **Settings** > **Troubleshoot** > **Re-enrol Device**. The re-enrollment process starts and displays a few prompts for confirmation.
3. Tap **Yes** on the prompts.

> If you tap **Cancel** during the profile installation, the enrollment process stops and the Ivanti Neurons for MDM server disables the device MDM.

To restart the re-enrolment process you must re-install the already downloaded profile. The downloaded profile is valid only for a few minutes after that you must perform the re-enrollment from Go client.

Re-registering Android devices

The admin can re-register a device by using the retire, wipe, or delete operations without manually clearing the existing active entry. This method is specifically more helpful for re-registrations where the new entry and existing entry belong to the same tenant. The Devices page displays the status of the device on the Ivanti Neurons for MDM administrative portal as follows:

- **Active** - device registration is successful
- **Retired** - device gets reset and retired status will be shown
- **Wiped** - device gets reset and wiped status will be shown
- **Reset** - device gets reset and will be in active status on the server until next registration

The Audit Trails page lists the device registration, re-registration, and retired statuses for Android devices. For more information, see **Working with Widgets**.

For Android 9.x and earlier versions, a single entry will be shown after re-registration. In case of Android 10.x and later versions, multiple entries will be displayed. However, only the latest entry will be active and older entries will be in a retired state.

7.5.5. Device Registration (Windows 10+ PC and Microsoft HoloLens 2)

This section contains the following topics:

Device registration process are of the following types:

- Manual registration
  - Invitation
  - End User registration
- Windows Autopilot
- With SCCM and Ivanti EPM via a Provisioning Package Enrollment with PIN. See **Provisioning Package Enrollment with PIN**.
- **Bulk Enrolment**

Manual registration

Most users start by registering a device. You can use any of the following approaches to start the registration process:

- Email invitation
- Direct users to the URL for your implementation
- The end **user must have an account** in Ivanti Neurons for MDM before you can start the device registration process. For LDAP users, that means a **Connector** and an **LDAP server** must be set up, and the user must be imported from the LDAP server. For local users, that means **adding a user**.
- The device enrollment URL generated in earlier versions of Ivanti Neurons for MDM will cease to work with the current version. The administrator will need to regenerate the device enrolment URL for device registration.

Sending an invitation

In most cases, you will start the registration process by sending an invitation. Ivanti Neurons for MDM provides the following ways to send end users an invitation to register a device:

- in the **Startup Wizard**
- when you **add one or more users**
- in the Users page (**Actions > Send Invite**)

If end users misplace the invite, receive it on a desktop or laptop, or fail to receive it for some reason, you can send them to the URL that was listed in the invitation. Just add **\go** to the end of your service URL.

End users who have an Ivanti Neurons for MDM account with a password set do not need an invitation to start the registration process. You can send them to the URL that would have been listed in an invitation.

Completing the end users registration process

Tell your device users how to complete the registration process. You can use the following instructions as a template and make any necessary changes:

Procedure

1. Open a browser on your Windows 10+ PC.
2. Navigate to mobileiron.com/go.
   You are redirected to a new page containing an enrolment URL.
3. Copy the enrolment URL to the clipboard.
4. Tap **add account** at the bottom of the **Settings** page.
5. Enter the email address associated with the invitation you received.

> If the user's Ivanti Neurons for MDM username does not match user's email address as entered in Ivanti Neurons for MDM, tell the user to enter the username when prompted for the email address.

Paste the Workplace server URL you copied into the next text field.

7. Tap **sign in**.
8. Enter your password in the next field.
9. Leave the other fields blank.
10. Tap **sign in**.
11. Click **done** in the **ACCOUNT ADDED** screen.
    The Workplace start screen shows that an account has been added.

Windows Autopilot

Windows Autopilot is a Microsoft feature that helps administrators to setup and pre-configure new devices to make them business ready. The Autopilot feature helps with a quick, reliable, and seamless provisioning of Windows Desktop or HoloLens2 devices. In addition, the Autopilot feature helps perform the following tasks:

- Automatically join devices to Entra ID (Entra ID)
- Auto-enroll devices into MDM services
- Create and auto-assign devices to configuration groups based on the profile of the device
- Customise the enrolment experience
- Apply configurations and policies
- Install essential applications

Ivanti supports all modes of Autopilot profiles:

- User Driven
- User Driven Pre-provisioned (former White Glove)
- Self-Deploying mode

For more information, see **Configuring Windows Autopilot Profiles**.

> For security and unauthorised use of the device, all Autopilot Windows devices can be locked to a tenant using the TenantLockdown CSP feature. To use this feature, the devices must be enrolled using the Autopilot option. This configuration is applied at the device level. See **TenantLockdown CSP**.

Entra ID Standard Registration

When users are added to the Entra ID tenant, they can directly enroll their devices via the Work Account.

Procedure

1. On a Windows device, go to **Settings > Accounts > Access work or school**.
2. Select Add Work or School account and then click **Connect**.
3. Provide email address from your work account.

The device gets automatically enrolled to Ivanti Neurons for MDM.

7.5.6. Local Admin Password Solution (LAPS)

The **Local Administrator Password Solution (LAPS)** automates the secure management of Windows devices passwords. LAPS enforces random, regular password changes and stores these passwords securely in a directory, reducing the risk of lateral movement in case of compromise.

Modern LAPS integrates with Azure and the latest Windows device management platforms, enabling secure password storage, retrieval, and policy configuration with Ivanti Neurons for MDM and the Azure portal. This ensures that administrator credentials remain protected and auditable across both legacy and cloud-managed Windows endpoints.

> To use LAPS with Ivanti Neurons for MDM, Azure administrators should ensure that the N-MDM app is added to their Azure tenant with the required LAPS permission (**DeviceLocalCredential.Read.All**).

> LAPS configuration can specify which local admin account it applies to by using the policy setting **Administrator Account Name**. If the account name specified in the config is not present on the device, the account name cannot be managed. However, when the **Administrator Account Name** is left blank, the policy defaults to the device's built-in local admin account, which is identified by its well-known relative identifier (RID).

> When the LAPS configuration is applied, the device's local administrator account password will be managed by the admin and the password will get generated in the Azure Active Directory.

Other features of LAPS

- Password storage in Azure - Local admin passwords can now be securely stored in the Azure device object.
- Password Retrieval – Administrators can retrieve the device passwords directly through Azure portal.
- Configurable Settings – LAPS Configurable Settings can be managed in Ivanti Neurons for MDM portal.
- On-Demand Password Rotation – Administrators can manually rotate device passwords from the Ivanti Neurons for MDM portal.
- Automatic Password Reset on Use – Passwords can be reset automatically once they are accessed.

Create LAPS Configuration

Prerequisites

- LAPS solution must be enabled for your devices. This solution is NOT available by default to all. Please reach out to the Technical Support team for assistance.
- Devices must be enrolled in Azure Device Operations (ADO).

Procedure

1. In your configuration management platform, initiate creation of the LAPS configuration.
2. **Set Required Parameters**:
    - **Backup Directory** - Select Backup the password to Microsoft Entra ID only.
    - **Local Admin Name** - Specify the administrator account name on your system (e.g., Admin).
3. **Configure Additional Settings** - Set these as per your organisation’s security policy. Default values will be used if not specified.
    - **PasswordAgeDays** - Number of days before the local admin password is rotated automatically.

- **PasswordComplexity** - Specify password complexity requirements (e.g., alphanumeric, special characters).
- **PasswordLength** - Set the desired length of the local administrator password.
- **PostAuthenticationActions** - Define any actions that should be performed after authentication.
- **PostAuthenticationResetDelay** - Set delay (in hours / minutes) to reset password after authentication.

4. **Distribute LAPS Configuration**
   - Assign the LAPS configuration profile to ADO-enrolled user/device.
   - Once you apply the configuration, a random local administrator password is created and securely stored in Microsoft Entra ID under:
     Devices → Manage Devices → Local administrator password recovery.
5. **Password Rotation**
   - Password is automatically rotated according to the value set in **PasswordAgeDays**.
   - You can review the Password rotation status in device logs.

Password Rotation

To force immediate rotation of the local administrator password, follow the steps below:

1. **Navigate to the Device** - Go to the device details page in your management console.
2. **Initiate Password Rotation**
   - Click on the three-dot menu (...).
   - Select **Rotate Administrator Local Password**.
   - Confirm the action when prompted. This will submit a password rotation request.
3. **Check-In and Confirmation**
   - The device processes the password change during the next force check-in.
   - Refresh the page in Microsoft Entra ID to view the updated password in the password recovery section.

7.5.7. Provisioning Package Enrolment with PIN

The admin can enroll the devices managed by SCCM or Ivanti Endpoint Manager to the Ivanti Neurons for MDM. The Deployment Package Tool allows organisations to streamline the transition of Windows devices to Ivanti Neurons for MDM Modern Management, without downtime or end user interruption. The seamless transition is achieved by downloading a unique deployment package from the Ivanti Neurons for MDM Console, then deploying it through the existing management tool or domain. Once the package is executed, it will silently enroll the endpoint into Ivanti Neurons for MDM for the ongoing management. The approach allows administrators to first easily migrate the devices, then have the flexibility to configure devices later over-the-air. When a device completes the silent enrollment into Ivanti Neurons for MDM, it is joined with MDM and is co-managed by the two management authorities. Once an administrator has configured the desired Windows experience within Ivanti Neurons for MDM, the legacy management platform can be decommissioned, leaving Ivanti Neurons for MDM as the single management authority of the device.

> There is an exception to this rule if a device is being transitioned from Microsoft Endpoint Manager (MEM) or formerly SCCM. The existing MEM Client continues to function in Coexistence Mode (opposed to Co-Management mode), until the MEM platform is decommissioned. When Coexistence Mode is enabled, the MEM Client automatically disables certain functionality in favor of Ivanti Neurons for MDM providing those workloads. For more information, see **Microsoft's Coexistence documentation**.

For more exact behaviours when using MEM and other 3rd Party Management platforms, Ivanti suggests to first test the Ivanti Neurons for MDM Deployment Package Tool in your environment.

Prerequisites

- User accounts must be imported on Ivanti Neurons for MDM using LDAP, Entra ID (Entra ID), Local User Upload, or other identity integrations
- All devices should have **Windows Configuration Designer** installed.
- Enable PIN based registration on . Ivanti Neurons for MDM
- Users should not have spaces in their username, this may cause a user device transition to fail.
- This tool can be deployed in environments that do not leverage the Entra ID.
- The main elements of Ivanti Neurons for MDM Modern Windows Management Suite does not require Entra ID. Co-management or coexistence may require certain workloads / configurations to be deployed upon silent enrollment, to avoid any impact during transition.
- Deployment Package is currently supported for SCCM and Ivanti Endpoint Manager only.

Procedure

1. Go to **Admin>Windows>Deployment Package**.
2. Select **User** or **User Groups** to generate PINs and click **Download Deployment Package** (.zip file).
3. The Deployment Package is given to the SCCM / Ivanti Endpoint Manager administrators to unzip and transfer the files to the respective devices managed by these admins. For information on how to perform this step, see **Packages and programs in Configuration Manager**.
4. After the transfer, administrators remotely trigger the setup.ps1 script on the devices. For information of triggering the script, see **Create and deploy scripts from the Configuration Manager**.
5. The devices are enrolled on Ivanti Neurons for MDM.

The PIN generated for the users are valid for 24 hours only. Once the PIN is expired, a new PIN has to be generated.

The file containing the PINs is deleted from the device post enrolment attempt is complete.

Enrolling SCCM devices to Ivanti Neurons for MDM

Procedure

1. Download all the deployment related files from the Ivanti Neurons for MDM for selected users.
2. Select accounts or groups that should be enrolled.
3. Deploy the Package files to client devices using SCCM:
    1. Verify if the required clients are present in SCCM. If the Windows-configuration-designer is not present on the client, the admin should push the designer and deploy it on the client.
    2. On the SCCM server, create a folder and copy the deployment zip file and extract the contents of the file.
    3. Create a .bat file that will copy the contents of the folder where the files are extracted to the client device.
    4. In SCCM, go to **Software Library > Application Management > Packages** and create a package to copy the contents of the folder to the client. Enter the destination folder to which you want to copy the contents.
    5. Deploy the package to the device or device location.
    6. Under the Monitoring section, you can monitor the deployment status and confirm that the files are copied to the client destination folder.
4. Execute the script to enroll a device:
    1. Go to **Software Library > Scripts** and create script.
    2. Enter a name to the script and import the PowerShell script **setup.ps1** from the unzipped folder.
    3. Approve the script and execute the script on target device.
    4. Select **Start now** and click **Save**. The Scheduled tasks starts executing the script. On successful execution, the status will become Green.
5. To verify the device enrollment, **Settings** > **Add or remove a provisioning package** > **Details**.

Enrolling Ivanti Endpoint Manager devices to Ivanti Neurons for MDM

Procedure

1. Download all the deployment related files from the Ivanti Neurons for MDM for selected users.
2. Select accounts or groups that should be enrolled.
3. **Case 1**: A device name is considered for enrolling the device with the same username - In this case, the email address is not a valid user email address. An email with device name concatenated with the AD domain is considered as the enrollment email address. The admin must set Account as LocalSystemAccount and use setup.ps1 as primary file to initiate the PowerShell execution.
   Case 2: A valid user email address is considered for enrolling the device and no restrictions on modifying files in the device location - Use the logged in user's email address for enrollment. To enable this enrollment, the admin must set Account as Current user account and use setup.ps1 as primary file to initiate the PowerShell execution.
   Case 3: A valid email address is considered for enrolling the device with restrictions on modifying files in the device location - Use the logged in user's email address for enrollment. This case has two sub-cases:
    - Using two scripts for enrollment - Create a distribution package with **setupEPMCopyContentsToTempFolderStep1.ps1** and run as Current User Account. The files are copied to a temporary location. Create another distribution package with

setupEPMCopyContentsToTempFolderStep2.ps1 and run as Local System Account.

> In case the device user has restrictions on modifying the folder containing package files - Copy the files to a temporary folder, check the user id and create a PowerShell package. The PowerShell package is executed by the **setupEPMCopyContentsToTempFolderStep2.ps1** script. After the installation, the temporary folder will be deleted.

Disable/Enable UAC

1. Update the registry entry to disable UAC control and reboot the machine
2. Execute the PowerShell package as Current user's account and using setup.ps1
3. Update the registry entry to enable UAC control and reboot the machine

Create PowerShell package:

1. Verify if the required clients are present in the Endpoint Manager.
2. Copy the files to C:\Program Files\LANDesk\ManagementSuite\LANDesk\files\. Create a sub-folder within this folder and extract files.
3. Create Package: **Distribution > Distribution packages > New > Windows > PowerShell**.

   > The admin can distribute the packages to different devices based on the level of restrictions set on devices.

4. In the Primary file section, enter the package name and upload setup.ps1 from the folder that has the copied files
5. Under the Additional files section, copy the remaining files (other than setup.ps1 script) using **Add**.
6. Select Current user's account under the Accounts section.
7. Click **Save**.

4. Create Scheduled task:
   1. Select the created package, right-click and select **Create Scheduled task(s)**. A Scheduled task is created.
   2. Drag the device and add it to the scheduled package section.
   3. On the Scheduled Package, right-click and select **Properties**.
   4. Verify the Package.
   5. Under Task type, select **Push**.
   6. Select **Start now** and click **Save**. The Scheduled tasks starts executing the script. On successful execution, the status will become Green.
5. To verify the device enrollment, **Settings** > **Add or remove a provisioning package** > **Details**. Alternatively, the admin can verify a device enrollment under the Diagnostic Logs of the device.

7.5.8. Using Bulk Enrollment for Windows devices

The Bulk Enrollment feature enables you to quickly register multiple Windows devices with Ivanti Neurons for MDM.

Prerequisites:

- User accounts must be imported on Ivanti Neurons for MDM using Entra ID (Entra ID) Premium Account.
- All devices should have **Windows Configuration Designer** installed.

Procedure:

1. Link the Ivanti Neurons for MDM and Entra ID tenants. See **Connecting Entra ID to UEM for Windows 10 Devices.**
2. Open the **Windows Configuration Designer** app and select **Provision desktop devices**. A New project window appears on the screen.
3. Enter the following details:
    - Name - A unique name for your project
    - Project folder - Location on the device where you want to save the project
    - Description - Optional description of the project

Click **Finish** to close the new project window and perform a sequence of steps.

5. **Set up device**
   Enter a unique name for your devices. The name can include a serial number (%SERIAL%) or a random set of characters.
6. Optionally you can enter a product key if you are upgrading the Windows, configuring the device for a shared use, or removing pre-installed software.
7. **Set up network**
   Optionally you can configure the Wi-Fi network devices to connect to when they first start. If the network devices are not configured, a wired network connection is required when the device is started first.
8. **Account Management**
   Select **Enroll in Entra ID**, enter a **Bulk Token Expiry** date, and then click **Get Bulk Token**.
9. Enter your Entra ID credentials to get a bulk token.
10. In the **Stay signed in to all your apps** page, click **No, sign in to this app only**.
    - Click Next when Bulk Token is fetched successfully and Create the Package.
    - A user with provisioning package is created in the Azure portal - User principal name (like package_0ea893a5-1e93-4d21-a6b1-dc788946fd1d@miwinqe.onmicrosoft.com). Copy the file (runtime ppkg tool) to a storage device.

> The Entra ID user for creating bulk token, and the package user should not have MFA enabled. To verify, you need to perform OOBE + Entra ID join on that user.

Recreate or synchronise the package user (created in Azure) to Ivanti Neurons for MDM.

Bulk enroll a device with a flash drive contained the provisioning package. You can also double-click on the existing device to perform post-OOBE experience. If the package failed to install in the first attempt, the second attempt also fails. Check if the new device is created in Ivanti Neurons for MDM and Entra ID belongs to the package user.

7.5.8.1. Ivanti Bulk Enrollment

Administrator can enroll multiple Windows devices with generic user (via ppkg) that starts with prefix **windows-bulkenroll**, and later do the user assignment.

Prerequisites:

- On the Ivanti Neurons for MDM, create a user account with prefix as **windows-bulkenroll**. For example, **windows-bulkenroll**-user1@abc.com, **windows-bulkenroll**-user2@abc.com.

Creating PPKG package with Windows Configuration Designer

1. Download and install the **Windows Configuration Designer**.
2. Create new project.
3. Click on **Provision Desktop**.
4. Enter the name of the project, and select a path.
5. In the **Set up device** section, enter device name.
6. In the **Set up network** section, enter network name (to setup network, if needed or can be disabled).
7. In the **Account Management** section, select **Enroll in Local Admin**. Enter **User name** and **Password**, and click **Next**.
8. In the **Add applications** section, click **Next**.
9. In the **Add certificates** section, select **Switch to advanced editor**, and click **Proceed** > **Yes**.
10. Go to **RuntimeSettings** > **Workplace Enrollments**. Enter **UPN** (same user created on Ivanti Neurons for MDM in the prerequisites section). Select the following options:
    - AuthPolicy: OnPremise
    - DiscoveryServiceFullUrl: https://login.mobileiron.com
    - Secret: Enter the Password

Click **File** > **Save**.

12. Click **Export** > **Provisioning Package**.
13. Click **Next** on subsequent screens, and click **Build**.
    The ppkg file is saved in the specified location.

Provision device in OOBE mode with ppkg

Provision the devices with the newly created ppkg package file from the above section. Once the device gets enrolled and checkin is successful, you will find the device entry on MDM server with the user that has prefix as **windows-bulkenroll**.

Assign Device to User

1. On the Devices page, click the user that has a prefix as **windows-bulkenroll**.
2. Click **Assign to User**. The Assign to User window opens.
3. Select or Search for the device from the list.
4. Select the required device.
5. Click **Assign to User**. The selected device will be assigned to the user.

When the user logs into the device for first time, the password change is must.

Assign to User option is available only for the Ivanti Bulk Enrolled devices.

Only device scope configurations and applications will work for the devices enrolled under this category. User scope configurations and applications are not supported.

7.5.9. Changing Passcode Settings

This section contains the following topics:

- Changing the assigned Passcode configuration
- Assigning a different Passcode configuration

Use the Passcode configuration assigned to a device to change the passcode settings. You can either:

- change the settings for the assigned configuration

OR

- assign a different Passcode configuration

Changes you make to the configuration will affect all devices that configuration is assigned to.

Changing the assigned Passcode configuration

Procedure

1. Go to **Devices**.
2. Find the entry for the device in the list.
3. Click the link in the **Name** column.

> If a Passcode configuration has been assigned, it will display in the Configurations tab.

In the Configurations tab, click the **Passcode Config** link.

5. Click **Edit**(upper right).
6. Make the changes.

Assigning a different Passcode configuration

Procedure

1. Make sure someone has created the configuration you need.
2. Go to **Devices**.
3. Find the entry for the device in the list.
4. Click the link in the **Name** column.

7.5.10. Changing the Device Name

Administrators can manually change a device's name (not using the Edit Device Name configuration).

Applicable to:

- iOS Supervised devices
- iOS Supervised devices
- macOS 10.10+ devices

Procedure

1. Go to **Devices**.
2. Find the entry for the device in the list.
3. Perform one of the following steps:
    - Add the **Device Name** column if not already added by clicking the Settings gear icon on the right and selecting **Device Name**.
    - Click the link in the **Name** column to go the device details page.
4. Next to the Device Name, click the **Edit** pencil icon.
5. Enter a new device name and click the tick icon.
6. In the Overwrite Device Name display box, review the notes and click **OK**.

The changed name will be pushed to the device the next time it checks in. This action cannot be undone.

> If a Default Device Name configuration was previously configured, this action will overwrite the name set in the configuration.

7.5.11. Finding and Filtering Devices

This section contains the following topics:

- Searching a device
- Filtering devices
- Using Advanced Search
- Loading the search queries

Searching a device

The Ivanti Neurons for MDM administrative portal displays the number of duplicate user groups and the corresponding number of GUIDs to identify duplicate groups, when the User Group Name attribute is selected in the rule builder. Also, a table under this rule displays the list of the duplicate user groups and their details such as User Group Name, GUID, Source and distinguished name (DN).

Procedure

1. Go to **Devices**.
2. Type device name in the **Search** field. All the devices that contain the characters are listed.

Filtering devices

The Filters side navigation bar lists various sections that help you to search for a specific device from the entire list of devices. The Manage Filters wizard contains the list of all the sections that you can select to display in the Filters navigation bar.

Procedure

1. Go to **Devices**.
2. Click the relevant check boxes from the sections that are listed in the Filters side navigation bar.
   Example:
   - From the **User Enabled** section, select **Yes** to display only those devices for which the users are in enabled state.
   - If you have assigned custom attributes to devices, you can filter devices based on those attributes by clicking the settings (cog) icon.
   - From the **Status** section, select **Retired** and **iOS** to display only retired iOS devices.

(Optional) Click **Restore Defaults** to restore the selection to the default filters. The Filters navigation bar displays the selected sections. If you clear all the check boxes from the Manage Filters wizard, the Filters side navigation bar displays all the sections.

4. Click anywhere outside the Manage Filters wizard to exit the wizard.
5. (Optional) Click the x icon to close the Filters side navigation bar and click **Filters** to reopen the side navigation bar.
   - If you use any of the stop words that are listed in the stopwords.txt file, which is part of the Apache SOLR server configuration, the words will not be indexed, as a result the entities that contain the stop words will not be displayed in the search results.
   - Examples of entities-devices, users, groups, attributes, applications, certificates, audit trails, content, and notification modules.
   - Examples of stop words-a, an, if, be, into, and so on.

Using Advanced Search

You can use the Advanced Search option to search for a device based on rules to identify and view the devices with specific criteria. The rules can be constructed using the applicable operators, including the "begins with", "ends with", "contains", "does not contain", "does not begin with", "does not end with", "is less than", "is greater than", "is in range", "is equal to", and "is not equal to" operators. The rule options can be nested together using the ANY (OR) or ALL (AND) options. The devices matching the rules are displayed below the section.

The Ivanti Neurons for MDM administrative portal displays the number of duplicate user groups and the corresponding number of GUIDs to identify duplicate groups, when the User Group Name attribute is selected in the rule builder. Also, a table under this rule displays the list of the duplicate user groups and their details such as User Group Name, GUID, Source and distinguished name (DN).

Procedure

1. From the Devices page, click the **Advanced Search** link. The Advance Search wizard opens.
2. Click one of the following options:
    - **Any**-if the devices must match at least one of the rules
    - **All**-if the devices must match all the rules

Create a rule that defines the search criteria. **Example**: APNS Capable is equal to Yes.

4. (Optional) Click **+** to create additional rules.
5. Click **Search**. The list of devices matching the search criteria are displayed.
    - For iOS 14.0+ devices, the eSIM ID (EID) of a device is available in the device details page. The eSIM ID (EID) allows the carriers to assign the SIM to a specific device. The eSIM ID (EID) field is GDPR-compliant.
    - As new GDPR fields (such as IP Address and eSIM ID) are added over Ivanti Neurons for MDM releases, the admins who have already configured GDPR must edit the GDPR profile if they want to hide the new fields.
    - Advance Search shows the status of the recovery lock of a device.

Loading the search queries

You can view the list of saved search queries.

Procedure

1. Click Advanced search and then click the folder icon. The list of the created search queries are displayed in the **Loaded Query** section and the following details are displayed:
    - **Query Name** - The name of the loaded query.
    - **Query Content** - Displays the content on the rules defining the search query.
    - **Actions** - Select the action to be performed on the query.
2. Click **Load Query** in the **Actions** column to view the list of devices matching the criteria defined in the loaded query.
3. Click **Delete** to delete a loaded query.

7.5.12. Using Device Owner

This section contains the following topics:

- Provisioning Android Enterprise Devices using a QR code or NFC Bump
- Provisioning Android Enterprise devices using client token

Licence: Gold

You can designate devices as company-owned or employee-owned after the devices have been registered. This designation helps manage policies that are based on whether a user has a personal device or a company owned device. With the proper licence, you can then use ownership in rules for creating device groups.

Starting with a new or factory-reset device, use the **Provisioner** app to provision device owner mode using one of the following options:

- NFC (Near Field Communication) bump
- QR code scan

An NFC bump involves tapping the master or template device against a new or factory-reset device to provision it.

A QR code scan involves tapping the screen of a new or factory-reset device, configuring a Wi-Fi network, and scanning the code when the device is ready to be provisioned.

While provisioning Device Owner mode using NFC or QR code, the provisioner app accepts an enrolment token. On registration, the enrolment token is sent to the server. If it is present in the server and the device is assigned to a user, the device is successfully registered.

The Go client will control the device once it is in Device Owner mode and locks itself to the screen until the device is registered with Ivanti Neurons for MDM to prevent users from leaving the provisioning process. Device Owner mode also supports Kiosk mode. For configuration information go to: **Lockdown & Kiosk Configuration**.

Important

- If you retire a device in Device Owner mode, the device will factory reset.
- All devices in Device Owner mode can optionally have all the system apps enabled.
- A device can only have one active device owner at a time.
- Only devices that are Android Enterprise capable are able to be provisioned into device owner mode.
- For Samsung Knox Standard devices that are in Device Owner mode, users will be prompted to activate Samsung ELM license. This prompt will also appear on Samsung devices that are in Device Owner mode when the Go client app is upgraded from a previous release to the most recently released version as supported by Ivanti Neurons for MDM. After activation, the serial number is displayed on the Device Details page, which would match with the Device > Settings > Serial Number field.

Provisioning Android Enterprise Devices using a QR code or NFC Bump

To provision Android Enterprise devices using QR code or NFC bump you will need to download and install the Provisioner app from Google Play on the master device.

Compatible Components

Provisioner version: 1.3.0.

Provisioner is compatible with or works with the following:

Item	Version
Android OS (on device to be provisioned)	• 5.0 - or supported newer versions is required, if using NFC. • 7.0 - or supported newer versions is required if using QR code. Device must be Android Enterprise capable.
Android OS (on master device)	5.1 - through the most recently released version. Device must have NFC for using NFC bump. It is not required for QR code.
UEM server product, enabled for Android Enterprise	One of the following: Ivanti Neurons for MDM, or Allow-labeled Ivanti Neurons for MDM.
Android client app	The latest client app version is automatically installed on the provisioned device by Provisioner.

Prerequisites

To provision an Android Enterprise device to be a work managed device, you need to:

- Ensure the required Android Enterprise-related configuration is defined and will apply to the registered device.

> The default Android Enterprise: Work Managed Device configuration must be enabled for the device.

Enable Android Enterprise on the server.

- Have an NFC-capable Android device (only if NFC is used) to serve as the master, with the Provisioner app installed.
- Have Android Enterprise-capable devices to provision.

To enable the Android beam for use with NFC bump:

Procedure

1. Go to **Settings** on the device.
2. Go to **Networks > Wireless Networks**.
3. In the **Connectivity section** select **Share & connect**.
4. Slide the **NFC** switch to **On**.
5. Slide the **Android Beam** switch to **On**.

> The steps to enable the Android beam and NFC may vary on different devices.

Provision Android Enterprise devices to become work managed devices

Procedure

1. Using the Android master device, download the Provisioner app from Google Play and install the app.
2. Launch Provisioner on the master device.
3. Select NFC or QR code for the Provisioning method.

4. Tap **App for Provisioning**, and choose the client app to be installed on the provisioned device:

Select this client app:	To register with this UEM server:
Go	Ivanti Neurons for MDM
At Work UEM	(Allow labeled) Ivanti Neurons for MDM

5. Fill out the remaining fields in the Provisioner app. Some fields may auto-populate if a supported Wi-Fi type is present. The Wi-Fi fields are not shown if QR code is selected. Use these guidelines:

Field	Value
Select app for provisioning	Go or At Work
Time Zone	Enter the time zone to be configured on the device
Locale	Enter the locale to be configured on the device
Enable All System Apps	Click the checkbox to enable all system apps
Wi-Fi Network SSID	Enter the Wi-Fi SSID the target device is to use
Wi-Fi Security Type	Enter the Wi-Fi security type
Wi-Fi Password	Enter the password for the Wi-Fi
Bulk Enrolment	The bulk enrollment feature is optional. To use the bulk enrollment, a hostname is required. Optionally, a username may be entered and the quick start option may be selected. To skip the bulk enrolment feature, these fields should be left blank.

6. Tap **Continue**.
7. If you selected **NFC**, tap **Continue**. The screen **Bump the devices!** appears on the master device. Continue with the **NFC Bump** section below.
8. If you selected **QR code**, the screen **Scan this QR code!** appears on the master device. Continue with the **QR Code** section below.

Use the steps below for NFC Bump

Confirm that the target device is displaying the Android Welcome screen.

9. Press the master device back-to-back with the target device to initiate an NFC transfer. If the NFC transfer succeeds, the target device may make a sound, and then proceed to download the client app. If a Wi-Fi connection cannot be established, or if the device is unable to download the client app, the device will automatically do a factory reset.

10. If you hear the sound or see a screen other than the Welcome screen, you can decouple the devices. This typically takes a few seconds. If the device is not encrypted, it will start the encryption process before continuing.
11. You can continue to provision additional devices by "bumping" the devices to the master device. The target device must be showing the Welcome screen, and the master device must be showing the "Bump the devices!"

Use the steps below for QR Code provisioning

Confirm that the target device is displaying the Android Welcome screen.

12. Tap the Android Welcome screen on the target device 6 times on the same place on the screen.
13. You will be prompted to configure a WiFi network so the setup wizard can download a QR code reader to the target device.
14. After the QR code reader is downloaded, the camera is launched.
15. Hold the target device a few inches above the master device until the QR code is scanned successfully. The setup wizard will then proceed to download the client app. If it is unable to download the client app, it will automatically do a factory reset.
16. You can continue to provision additional devices by scanning the QR code on the master device. The target device must have a camera ready to scan, and the master device must be showing the "Scan this QR code!"
17. The QR code can also be exported by tapping the Share icon. The options offered for exporting will vary by device.

Provisioning Android Enterprise devices using client token

You can provision an Android Enterprise device in Device Owner mode using a branded client token instead of using the NFC bump or QR code methods. This method enables you to sign on a device with a token which facilitates an automatic installation of the Go or At Work client and provisioning in Device Owner mode:

> Branded client tokens are supported on devices provisioned with Managed Google Play Accounts, using Android 6 or supported newer versions. For more details see the Android UEM Developers guide. https://developers.google.com/android/work/prov-devices#Key_provisioning_differences_across_android_releases.

Requirements to use this method:

- You must be enrolled with an Android Enterprise account.
- The device must be Android Enterprise-capable.
- The device must use Android 6 through the most recently released version.
- You must have a new or factory reset device.

Configure (for devices running Android 5.0+)

Procedure

1. In the Ivanti Neurons for MDM portal, Go to **Configurations**.
2. Click **+Add**.
3. Select **Lockdown & Kiosk: Android Enterprise**.
4. The **Create Lockdown & Kiosk: Android Enterprise Configuration** page is displayed.

Enter a configuration name and description.

5. Choose a Lockdown type.

Click **Work Managed Devices (Device Owner)**.

6. Android Device Owner Lockdown settings options are displayed.

Optionally, choose to

- Disable WI-FI or WI-FI settings
- Disable Camera
- Disable Bluetooth
- Disallow Bluetooth Settings
- Disable Screen Capture
- Mute Master Volume
- Disallow Apps Control
- Disallow Credentials
- Disallow Emergency Broadcasts
- Disallow Mobile Networks
- Disallow Tethering
- Disallow VPN
- Disallow Factory Reset
- Enable Factory Reset Protection

> You can optionally specify a list of authorised Google account IDs (an integer value) that can provision the device after factory reset or hover over the help icon to view help for retrieving authorised account IDs).

Disallow Modify Accounts

- Disable NFC (Outgoing Beam)
- Disallow Outgoing Calls
- Disallow Safe Boot
- Disallow Share Location
- Disallow Debugging features
- Ensure Verify Apps
- Disallow SMS
- Disallow Unmute Microphone
- Disable Auto Time
- Disable Auto Time Zone
- Disable Data Roaming
- Disable Wi-Fi Sleep
- Restrict Input Methods
- Restrict Accessibility Services
- Disable USB file transfer

- Disable external media
- Disable keyguard (no effect if PIN/Passcode is set)
- Keep screen on while connected to power
- Disallow create windows
- Skip first use hints

Under **Enable/Disable System Apps** section, you can optionally choose to enable to disable the following System Apps:

7. Optionally choose to enable **Kiosk Mode**.

Item	Version
Preset System Apps	
Built-In camera	Click the toggle button to turn **ON** or **OFF** the Built-In Camera app.
Built-In Phone	Click the toggle button to turn **ON** or **OFF** the Built-In Phone app.
System App Package Name	To enable or disable any other system app(s) other than the preset system apps, Click the +(plus) icon and add the system app package ID. To remove the system app, click the -(minus) icon.

The following settings are displayed:

- Enable Lock Task Mode
- Enter Kiosk automatically (on initial setup only)
- Disable Quick Settings
- Allow User to Access WiFi Settings
- Allow User to Access Bluetooth Settings
- Allow User to Access Location Settings
- Allow User to Delay Application Updates
- Allow User to Access Date and Time Settings
- Allow User to Access Mobile Network Settings
- Allow User to Select Language
- Enable Shared Device (select any of the following options)
  - Enable Login
  - Enable Logout (provide the Timeout setting in hours)

Optionally select the default or custom branding options from the drop-down list.

8. Optionally create a Kiosk Exit Pin to use to exit Kiosk mode.
9. Optionally, create an Allowlist of apps that will be available to users in Kiosk Mode.

Provision the device

Procedure

1. Power on the device and enter your WI-FI password. Your device may prompt you for a different password.
2. In the **Verify your account** screen enter your Android Enterprise token. Click **Next**.
3. On the **Google Services** screen click **Install**.
4. Accept the Terms and Conditions.
5. On the Setup work device screen click **Next**. The Go or At Work client downloads and installs on the device. The device now enters Device Owner mode.

Related topics

- Using Bulk Enrolment for Android
- Device Groups

7.5.13. Managed Device with Work Profile

Managed Device with Work Profile on Company Owned Device is a mode in which the Android Enterprise device is a corporate-owned device with personal data separate from the rest. This mode supports two profiles where you can deploy work apps inside the managed profile and have the user with their personal side. Managed Device with Work Profile on Company Owned Device mode is created by distributing a Managed Device with Work Profile configuration to a device that is provisioned in device owner mode.

For more information on Managed Device with Work Profile Lockdown Settings, see **Lockdown & Kiosk: Android Enterprise**.

> This mode requires Android 8.0 through the most recently released version.

App configurations, apps sharing widgets across profiles, client certificate aliases, and ID certificates can be applied to Managed Device with Work Profile.

The following configurations are applicable to Managed Device with Work Profile devices:

- Advanced passcode
- Always on VPN
- Certificate
- Identity Certificate
- Google account
- Passcode
- Samsung phone restriction
- Threat Defence
- Wi-Fi
- Default App Runtime Permissions
- SafetyNet Attestation
- Passcode
- Threat Defense Local Actions

7.5.14. Using Bulk Enrolment for Android

The bulk enrollment feature enables you to quickly register multiple Android devices with Ivanti Neurons for MDM.

Licence: Silver

Perform the following tasks before using bulk enrollment:

1. Install Android SDK, which includes the Android Debug Bridge (adb), on the computer used to register the devices.
   For more information about the Android Debug Bridge, see: **http://developer.android.com/tools/help/adb.html**.
2. Enable USB debugging.
   The procedure to enable USB debugging on Android devices varies depending on the Android release. See: **http://developer.android.com/tools/device.html** for information on enabling USB debugging.
3. Install the Go client on each device.
4. Connect the devices via USB cable to the provisioning computer to be used to register them.

The Go can be started and registered to a server using the Android Debug Bridge (adb) shell. The Android Debug Bridge is a tool that can be used from the command line in Windows, or in the Terminal utility in iOS. It enables you to communicate with a connected Android device. From the adb shell the command format is:

> 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

> The Registration Protocol (**mirp**) is used to encode relevant data for registration.

Valid keys and values are:

Key	Value
user password	User's email address that would have been typed into the username field if using iReg. Required. User's password
pin	Registration pin for the user
quickStart	**When set to TRUE:** the splash screen will show, but not as long. On the Welcome screen, when the spinner changes to the Continue button, the screen will automatically move on without having to tap Continue. Also, this streamlined provisioning flow occurs across all devices: • The privacy and shortcut prompts for the user are skipped. • On zebra devices, the client shall grant admin privileges to itself without a user prompt. Requires a minimum version of Zebra MX 4.3. **When set to FALSE:** the splash screen will show as usual and the user will need to tap Continue on the Welcome screen. Optional, defaults to FALSE.

> Use of a password, pin, or token is required to use bulk enrolment.

This example command specifies a server, user, password, pin, and quickstart:

am start -a android.intent.action.MAIN -d "mirp://ppp183.auto.mobileiron.com?user=miadmin@auto0001.mobileiron.com&password=P@$$W0R3&pin=12345&quickStart=true" -n com.mobileiron.anyware.android.qa/com.mobileiron.polaris.manager.ui.StartActivity

Sample bulk enrolment script

You can use this script as an example to use when designing your own bulk enrolment script. This sample script registers all devices attached to the provisioning machine with the same user and password.

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

Potential Error messages

Here are some potential errors that you may encounter using bulk enrollment.:

Error	Resolution
mirp scheme not found	Example command using a mirp scheme: am start -a android.intent.action.MAIN -d "xxxmirp://?
URL is invalid	Occurs if no data string is sent at all. Verify that the URL is correct.
No server information found	Server information missing or improperly entered.
No user information found	Verify that user key was entered.
No password/pin information found	Verify that a pin OR password key was entered.

> When there are multiple profiles created for Bulk Enrollment:

- A natively enrolled fully managed Android Enterprise device receives the custom attribute that was created with the first profile.
- When migrating devices, if the device is present in a bulk enrollment profile, the custom attributes defined for the migrating device in the bulk enrollment profile will be applied to the device on migration. This behavior is the same for the migrated fully managed Android Enterprise devices because it receives the custom attribute of the 1st profile.

Also, all the profiles created for that particular device are seen as active.

7.5.15. Bulk Enrollment using CSV File Upload

Bulk enrolment allows you to register multiple Android devices using device identifiers. You can upload the CSV file to add devices in bulk.

Procedure

1. In the **Devices** page, click **Bulk Enrolment** tab. The **Bulk Enrolment** page is displayed.
2. Click **Add**.
3. In the **Profile Name** text field, enter the name of the Profile. Optionally, click **+Add description** to provide a description for the CSV file.
4. In the **Upload CSV** section, click **Download CSV Template** to download the CSV template. Using the existing format, you can edit the file to add devices.

> Allows up to 200000 rows at a time in bulk enrollment CSV.

5. After editing and saving the CSV file, click **Upload CSV** to upload the CSV file. A confirmation on the successful upload is displayed.

> Rows with inadequate information may result in CSV upload failure. Each record should include at least the serial number and manufacturer information, or the IMEI value.

> To remove the added CSV file, click on the 'minus' icon. To choose a different CSV file to upload click on the **Choose a different file** link.

6. Optional: Select **Assign custom attributes without token** to bulk enroll all types of devices without generating a token. This option is not selected by default.

Bulk enrollment without token can also be applied when the IMEI or the combination of Serial number and Manufacturer (with or without custom attributes) is provided in the uploaded CSV file. But the registration of the device depends on the correctness in the attribute values uploaded in the CSV file. The following table explains the scenarios on the outcome based on the attribute value combination entered for bulk enrollment:

Scenario	**Entered Attribute values**			**Device registration status**
	IMEI	**Serial Number**	**Manufacturer**	
1	Correct	Incorrect	Incorrect	Device is registered
2	Incorrect	Correct	Correct	Device is registered
3	Incorrect	Incorrect	Correct	Device is not registered
4	Incorrect	Correct	Incorrect	Device is not registered

> The manufacturer name is case insensitive.

7. In the **Select User** field, you must select a user.
   The enrolment token is displayed in the Enrolment Token column. To refresh the enrollment token, click **Refresh**.
   The expiry date of the token is displayed in the **Token Expiry** section. To extend the token expiry period, click **Extend**. In the **Extend Upto** field, enter the number of days to extend the token.

> The number of days specified should be within the range 7 to 999. Default token expiry is within 7 days.
> This page will not be displayed if you have selected the option, **Assign custom attributes without token**.

8. Click **Done**.

After the upload, the following details of the uploaded CSV file are displayed in a table in the **Bulk Enrollment Profiles** page.

Setting	Description
Profile Name	The name of the Profile.
Description	Some description about the profile.
Last modified	The latest date of modification done in the CSV file.
TYPE	For Self-Maintained Profiles → Self-Maintained
No of Devices	The number of devices in the bulk enrolment.
Associated User	Name of the associated user.
Username	Specifies the user associated with the device. Required when Device-to-User Mapping is enabled. The user must exist in Ivanti Neurons for MDM.
Actions	You can perform any of the following action: **Download Existing Inventory** - Click this button to download details of all the devices available in the profile. **View** - Click this link to view the details of profiles uploaded in bulk for registration. **Edit** - Click this button to edit the profile details. This option is available only when single device option is selected. **Delete** - Click this link to delete the profile. In the confirmation window, click **Yes** to confirm the deletion of the uploaded profile.

> Token generated while uploading CSV should be used for the registration. Entering the wrong token redirects to normal IReg flow where the ID/password should be entered.

Actions

When viewing the Bulk Enrollment profiles from the View Profile details section, you can perform other tasks from the Actions tab, which is present on the View Profile details page.

- **Add More Devices** - Use this option to add more devices to a profile. You need to provide either **IMEI Number** or **Serial Number**, or both, **Manufacturer**, and optionally the **Custom Attributes** information and then click **Save**.

- **Modify Configuration** - Use this option to modify an existing configuration. You can add **Ivanti specific keys**, make changes to **Pre-Defined Android System Extras** or **Custom Android System Keys** and then click **Update**.
- **Generate QR code** - Use this option to generate a QR code for Bulk Enrollment of profiles.
- **Refresh Token** - Use this option to refresh a token or extend the validity of a token. The validity can be set in the range of 7 to 999 days or it can be set to **Never expires**.
- **Change Associate User** - Use this option to change an associated user. You need to search and select the user from the **Change Associate User** popup, and click **Apply**.
- **Edit** - Use this option to edit devices from the selected profile. You need to select the devices and click the **Edit** button.
- **Delete** - Use this option to delete devices from the selected profile. Once you select the devices and click the Delete button, a confirmation pop-up appears on the screen. Click **Delete**.

Self-Maintained devices have different device statuses. You can find more details **Using Samsung Knox Mobile Enrolment**.

7.5.16. Device_to_User_BulkEnrollment

File not found!

7.5.17. Using Samsung Knox Mobile Enrolment

Samsung Knox Mobile Enrollment enables administrators to register qualified Samsung devices to Ivanti Neurons for MDM. Using Knox Mobile Enrollment, a device can be shipped directly from an approved reseller to an end user and the Go Android client will automatically download with enrollment data pre-populated. For details, see the **Samsung Knox Mobile Enrollment for Android Enterprise**.

Requirements

- Device list by IMEI
- CSV file containing a list of devices containing an IMEI or serial number, and optionally a username and enrollment password.
- Ivanti Neurons for MDM (current release).
- Samsung Knox account approved for mobile enrollment
- Samsung supported devices. A list of Samsung supported devices is available **here**.

7.5.18. Enrolling Oculus devices

Ivanti Neurons for MDM can now manage the Quest for Business devices (Oculus devices). Currently, Meta supports Oculus for Business (OFB) and Quest for Business (QFB) devices for MDM. You need to perform some basic tasks on the Meta console to make the devices MDM-ready and then register for Ivanti Neurons for MDM.

You can enroll the Oculus device fleet in the Device Manager under the Meta Workplace console. You need to log in to the Oculus Business Workplace using the credentials shared on your registered email. On the Home page, All Devices information will be displayed under the Device Fleet section. The Device Fleet section provides an overview of all the devices available under Device Management. These details include the Device Name, Device Status, OS (Operating System), Model, etc.

This section contains the following topics:

- Prerequisites to enrolling Oculus devices
  - Setting up an MDM app in the Device Manager
  - Setting up the Oculus device

Register an OFB device with MobileIron Go

  - On Ivanti Neurons for MDM Console
  - On Go client

Prerequisites to enrolling Oculus devices

Setting up an MDM app in the Device Manager

The Devices / Headsets are provisioned and updated to at least **v28** of **Oculus for Business**. On the Meta Console, the administrator must set up an MDM in the Device Manager and map the Oculus devices to this specific MDM service.

Procedure

1. On the **Oculus Business Workplace** home page, select **Apps**.
2. Under the **App Library**, click on the third-party MDM app that you want to install, and then click **Update**.
3. Select the appropriate MDM for the app from the list under **Mobile Device Management** and then click **Update App**.
4. Click the Oculus Device headset on which you want to install the MDM. The device information will appear on the screen.
5. Under the **About** tab, scroll down to **Mobile Device Manager**.
6. Click the **Edit** button next to the **MDM Authority** option.

> By default, the Oculus Device Manager option will be selected. You need to select the MDM Authority App and select **MobileIron Go** from the MDM Authority App list.

Click **Save**. The Device automatically resets and then you need to set up the Oculus device using the setup app.

Setting up the Oculus device

You can add Oculus Quest 2 Headset devices using the Device Setup app. This app must be shared with the required users so that the users can download and install the app on their Android devices.

Procedure

1. Under the **Device Fleet** section, click **Unconfigured Devices**.
2. Click **Get Setup App**. The **Send Download Link** page appears on the screen.
3. Select one or more team members from the list or click **Add recipient** to select from the list.
4. Click **Send Link**. The selected users will receive an email with a link to install the **Device Setup** app.
5. Click the **Download Device Setup App** link in the email to install the **Device Setup App** on your Android device.

> After downloading, this app will not appear in the App Store of your device. You need to get it from the Downloads section of your device and install it.

Open the **Oculus for Business** app from your Android device.

7. Power ON the Oculus devices by pressing the power button for 2 seconds.
8. Turn on Bluetooth and place your Android device close to the Oculus devices until the setup is complete.
9. Search for Oculus devices using Bluetooth of your Android device.
10. Once the required Oculus device is found, you need to connect it to a Wi-Fi network to complete the setup.
11. Click **Enter Wi-Fi Information** and provide the Network Name and Password and then click **Save**. Now, the Oculus device is connected to the Wi-Fi network.
12. Click **Start Setup**. A notification appears on the screen that the setup is in progress, and you should not close the app or handle the headsets during the setup.
    A confirmation appears on the screen. You can continue to search for more devices using the **Find More Devices** button.

Registering an OFB device with MobileIron Go

On Ivanti Neurons for MDM Console

An OFB device can be registered with MobileIron Go on Ivanti Neurons for the MDM console. However, the Work Managed Device Non-GMS mode (AOSP) configuration (under **Configurations**) must be distributed to these OFB device groups.

On Go client

An OFB device can be registered on the MobileIron Go client. You need to perform the following tasks to register the OFB device:

- After completing the setup using the OFB Setup app, continue with the on-screen instructions on the OFB headset and complete the device setup.
- The MobileIron Go app launches automatically and you need to provide the login credentials and complete the registration by following the MDM instructions.

Now, the device is provisioned in DO mode and is set to be managed by the MDM.

7.5.19. Enabling Bluetooth on a Device

Applicable to:

- iOS 11.3+
- macOS 10.13.4+

You can enable or disable Bluetooth on a device.

Procedure

1. Navigate to the device in the **Devices page**.
2. Perform one of the following actions:
    - Select the devices from the list.
    - Click the device name to display the Device details page.
3. From the **Actions** menu, click **Enable/Disable Bluetooth**.
4. Click **OK**.

The changes will be pushed to the device(s) the next time it checks in.

7.5.20. Schedule iOS Update

Applicable to:

- iOS 9.0+ Supervised Device Enrollment devices
- iOS 10.3+ Supervised devices.

Schedule an iOS device to update to the latest iOS version available to it. The **Device** > **Actions** menu option **Update OS Version** for Supervised iOS devices displays a list of only those iOS versions which are applicable to the device.

Procedure

1. Navigate to the device in the **Devices page**.
2. Click the device name to display the Device details page.
3. From the **Actions** menu, click **Update OS Version**.
4. On the **Update OS Version** wizard, review the iOS version and select the OS version from the **Update to version** drop-down list.

> If you enter an equal or older version, an error message appears indicating that the target iOS version should be greater than the current version.

5. Click **Update**.

The iOS device will be scheduled to update to the latest iOS version available to it when the device checks in. If the device has a passcode, after MDM sends the update to the device, the device queues the update and the user is prompted to enter their passcode in order to start the installation. For more information, see **Software_Updates**.

7.5.21. Re-install iOS System Apps

Applicable to:

- iOS 11.3+ devices.

Re-install deleted iOS system apps on iOS devices.

Procedure

1. Navigate to the **Devices page**. Alternatively, you can click the name of the device and perform this action from the Device Details page.
2. Select one or more iOS devices.
3. From the **Actions** menu, click **Re-install iOS System Apps**.
4. On the Re-install iOS System Apps display box, select one or more available system apps to be installed on the devices.
5. Click **Re-install Apps**.

The apps will be installed on the selected and compatible iOS devices when the devices check in. System apps installed in this manner will not be considered managed apps. If there are no compatible devices selected, you will get a message that the system apps will not be installed on those devices.

For more information, see **Software_Updates**.

7.5.22. Assigning a Device to a new user

An existing registered device may need to be re-provisioned for a new user, if there has been a role change for the user, or if the previous user's relationship to the company has changed. These steps help to avoid retiring and re-registering the device.

Procedure:

1. Navigate to the device in the **Devices page**.
2. Click the device name to display the Device details page.
3. Click **Assign to user**  icon.

> Alternatively, you can select a device from the **Devices** page, and click **Assign to user** option from the **Actions** menu.

Start to enter the users name in the **Search User**... field.

5. Select the desired user.
6. Click **Assign to user**.
   The device will be provisioned for that user.

> You may notice that in user-based and licence-based scenarios, you can assign a device to a user who has exceeded the assigned device limit. This is because the intent of the device limit feature is to limit the registration of devices in support of Bring Your Own Device (BYOD) scenarios.

In both device-based and user-based licences, enforcing the device limit is inconsequential. For device-based licences, the cost to the end customer does not change because the total number of devices in the system does not change. For User-based licences, the lack of this check actually benefits the customer. For example, consider five users, U1 through U5 with 5 devices each. With user-based licensing, this would consume five licences. If instead, two of the devices from U4 and U5 are moved to U1 and U2, then licence consumption goes DOWN, from five to three.

7.5.23. Reassigning an Android device

The administrator can transfer the ownership of an Android device from one user to a different user. During the reassignment process, the device's management profile will be reconfigured or remapped from the current user to new user in Android Enterprise mode. The reassignment can be done on all Android Enterprise devices except the Android Management API (AMAPI) devices and cannot be done on Google Domain Android Enterprise devices.

> The device reassignment can be done only with the devices in same mode. For example, a device in Work Managed Device mode can be reassigned to another user in the same mode.

The device reassignment process will have the following statuses:

- Initiated
- Success
- Failed
- Pending

You can view the last reassignment status of a device under the **Device Details** page → **Overview** tab → **Last Reassignment Status**.

Procedure

1. Go to **Devices**.
2. Select one or more devices from the list.
3. From the **Actions** list, click **Assign to user**.
4. Alternatively, you can click on any device name. The **Device Details** page opens. Click the **Assign to User** icon to get the Assign to user screen and select the required user.
5. Click **Assign to user**. The selected options will be validated to check if the selected devices can be reassigned to the selected users or not.
   After successful validation and reassignment, a confirmation message appears on the screen.

> If you have selected a maximum number of 10 devices, then the "Assignment initiated" message appears on the screen. If you have selected 11 or more devices, then "Validation is in progress" pop up appears on the screen.

> Android Device Reassignment is an innovative solution built uniquely with focus on eliminating data-left-overs from the previous registered user and is only available in SUEM-Premium SKU.

7.5.24. Forcing a device to Check-in

Devices need to contact Ivanti Neurons for MDM (check in) to provide and receive information. Check-ins are scheduled at regular intervals. You can also prompt a device to check in on demand. Forcing a device to check in can speed up the process of applying configurations, updating policies, etc.

Procedure

1. Go to **Devices > Devices**.
2. Select the devices.
3. Click **Actions**.
4. Select **Force Check-in**.
5. Optionally, click the device name link to go to the Device details page and click the **Force Check-in**  icon and click **OK**.

> If there is a failure at device end while processing the configuration installation command during a check-in, Ivanti Neurons for MDM will not retry to install the configuration to the device during the later check-ins automatically. Administrator needs to retry installing the configuration manually from the device details page of the device. To do so, go to the Configuration tab, select the error configuration and click **Retry Install**.

7.5.25. Locating a Device

If you have enabled the Locate feature for a device, you can display the last known location for that device. You must edit the privacy configuration to enable collection of Location data and apply the configuration to the device to enable this feature. The device must also support this feature, and users must agree to share their location data.

Procedure

1. Navigate to the device in the Devices page.
2. Click the link in the **Name** column.
3. In the **Overview** tab, click on the link under **Device Location**.

The following details are displayed on the page:

Field name	Description
Last located on	Displays the date and time when the device was last located.
Coordinates	Displays the latitude (north-south position) and longitude (east-west position) of the device.

You can also find the device location map displayed in the page.

7.5.26. Locking a Device

You can trigger the screen lock on a device. Locking works somewhat differently on different devices.

Procedure

1. Go to **Devices > Devices**.
2. Select the device.
3. Click **Actions**.
4. Select **Lock**.
5. Alternatively, click the device name link to go to the Device details page and click the **Lock**  icon and click **OK**.
6. For AppConnect Android apps, the Lock command locks the user out of the container and also locks the device. The users can log back in to the device and the AppConnect app using the device passcode and the AppConnect passcode respectively.
7. For iOS 7 devices, you can enter a display message and phone number (optional).
   These options can give device users information about why the device has been locked and the number to call to get it unlocked.
8. For macOS devices, the user is prompted to enter a 6-digit PIN as passcode to access the device. To proceed with the screen lock, the device user needs to:
   1. Enter the PIN.
   2. Select the check box to confirm locking the device.
   3. Click **Yes, send lock command**.

> In macOS, user can add optional lock screen message and phone number during device lock passcode setting.

9. For ChromeOS devices, when you perform a Lock operation, a pop up window "Locking a device may require the user to enter a passcode to access the device." appears on the screen. Click **Lock** and the device status will be updated to **Disable sent**, and the updated device status will be visible after periodic device sync.

Alternate Methods of Locking a Device:

- A device user can perform the lock action from the Self Service Portal.
- An Administrator can perform the lock action from the Administrator Portal.

7.5.27. Managing Apple devices in lost mode

This section contains the following topics:

- Enabling lost mode
- Performing lost mode actions
- Disabling lost mode

Applicable to: iOS 10.3+ Supervised devices

You can place a supervised device in lost mode through Ivanti Neurons for MDM. This means you report the device as lost to Apple servers, allowing you to retrieve the last recorded location of the device, as well as disable lost mode if the device is found.

Enabling lost mode

You can report a lost device to Apple servers by placing the device in lost mode. After you have placed a device in lost mode:

- If the device is retired, you cannot disable lost mode.
- If the device is wiped, you cannot locate or track the device.

Procedure

1. Go to **Devices**.
2. Select the checkbox for the device.
3. Select **Actions** > **Common** > **Enable Lost Mode**.
4. Alternatively, navigate to the **Device Details** page by selecting the device name link. Click the action icon of the device and select **Enable Lost Mode**.

Performing lost mode actions

After the lost mode is enabled, you can perform the following actions from the Lost Device Mode section:

- Push Message/Phone Number to iPhone
  - Enter a message to be displayed on the locked screen of the lost device.
  - Enter a contact number to be displayed on the locked screen of the lost device. If someone finds the device, they can call the number to report it.

Lock Device

- **Refresh Device Location**

> If the device is wiped, you will not be able to locate the device.

- **Play Lost Mode Sound**

> Sound will play until the device is removed from lost mode or a user disables the sound on the device.

- **Refresh location**
  The **Refresh Location** option is added to **Lost mode** to view device location. The following details are displayed:

- **Latitude**: The latitude of the device location.
- **Timestamp**: The time and date Timestamp from the payload is displayed.
- **Longitude**: The longitude of the device location.

Disabling lost mode

If a device in lost mode is retrieved, or the lost mode was enabled in error, you can disable lost mode.

> If the lost device is retired from Ivanti Neurons for MDM, disabling lost mode will not work.

Procedure

1. Go to **Devices**.
2. Select the checkbox for the device.
3. Select **Actions** > **Common** > **Disable Lost Mode**.
4. Alternatively, navigate to the **Device Details** page by selecting the device name link and select **Lost Device Mode: Enabled** > **Disable Lost Mode**.

7.5.28. Managing Android devices in Lost Mode

This section contains the following topics:

- Enabling Lost Mode
- Disabling Lost Mode

Enabling Lost Mode

Applicable to: Android 8+ devices

You can place multiple Android devices simultaneously in Lost Mode through Ivanti Neurons for MDM. This means you can report a lost device to Ivanti Neurons for MDM by placing the device(s) in Lost Mode, which allows you to show a custom message, phone number, and footnote on the screen, along with an option to play a sound.

> This functionality supports only Fully Managed devices including Non-GMS devices.

Procedure

1. Go to **Devices**.
2. Select the checkbox for the device(s).
3. Select **Actions > Enable Lost Mode**.
4. ⋮ Alternatively, click on the device name link to go to the Device details page and click the icon. Select **Enable Lost Mode**.
5. Enter a lock screen message or phone number or both to be displayed on the locked screen of the lost device(s). Admins can also select the footnote and **Play Lost Mode Sound** options. If someone finds the device(s), they can call the number to report it.

> Either a message or phone number must be entered in the respective fields to activate the **Enable Lost Mode** option.

> The Lost Mode sound will play for 5 minutes unless the phone is unlocked, the call button is pressed, or the Admin disables Lost Mode within that time. To replay a sound, re-enable Lost Mode on the device(s).

6. Select **Enable Lost Mode** to place the Android device(s) in Lost Mode.

Activating Lost Mode will disable the following actions:

- Unlock
- Enter/Exist Kiosk
- Force Logout for shared Kiosk
- Assign to User
- Send Message
- Set Ownership

> Once the lost mode is enabled in a device, Lost Mode option in server will be disabled.

Disabling Lost Mode

If a device(s) in Lost Mode is retrieved, or the Lost Mode was enabled in error, you can disable Lost Mode.

> If the lost device(s) is wiped from Ivanti Neurons for MDM, disabling Lost Mode will not work.

Procedure

1. Go to **Devices**.
2. Select the checkbox for the device(s).
3. Select **Actions > Disable Lost Mode**.
4. Alternatively, click on the device name link to go to the Device details page and select **Lost Device Mode: Enabled > Disable Lost Mode**.

> In the **Details** section, **Disable Lost Mode** becomes visible only after **Enable Lost Mode** is activated. Once **Disable Lost Mode** is activated, the **Lost Device Mode: Enabled** field, which includes the **Disable Lost Mode** option disappears.

> Devices that were previously in Kiosk mode will need to be re-entered into Kiosk after Lost Mode is disabled.

7.5.29. Requesting debug logs

You can send a request to iOS, macOS, and Android work managed devices to retrieve debug logs for troubleshooting device issues. Using the "Request debug logs" command in the Devices page, the actions and success or failure of an event is captured in the debug logs.

This feature requires the following clients:

- iOS devices require Go 5.3.0 for iOS or supported newer versions. For devices that are migrated from Ivanti EPMM to Ivanti Neurons for MDM, this feature requires Mobile@Work 12.2.0 for iOS or supported newer versions.
- macOS devices require Mobile@Work 1.5 for macOS or supported newer versions.
- Android work managed devices require Go 65 for Android or supported newer version.

Procedure

1. Go to **Devices > Devices**.
2. Select the device and click the device name link to go to the Device details page.
3. Click the ⋮ icon.
4. Select **Request debug logs** and click **OK**.

When the request is sent and when the logs are ready at the device, a notification is sent to the admin and is displayed in device logs. The device logs can also be downloaded by clicking the link.

7.5.30. Apple_Enhanced_Logging

File not found!

7.5.31. Retiring a Device

Retiring a device ends its relationship with Ivanti Neurons for MDM. You might retire a device if:

- the user left the company
- the user has replaced the device
- you need to undo the management tasks you have completed (start over)

Procedure

1. Go to **Devices > Devices**.
2. Select the device.
3. Click **Actions** (upper right-hand side).
4. Select **Retire**.
5. Optionally, click the device name link to go to the Device details page and click the ⋮ icon.
6. Select **Retire** and click **OK**.

> When you perform a Retire operation on a device which is in Active state, the device will be retired immediately.

7.5.32. Relinquishing Ownership of a Device

Applicable to Android devices in Work Profile on Company Owned Device mode.

Relinquishing ownership of a device in Work Profile on Company Owned Device mode removes the work profile and retires the device from Ivanti Neurons for MDM, without affecting personal apps and data. The end user can then use the device as a personal device, with full access to all device controls and settings.

> The device needs to be removed from Google Zero Touch or Knox Mobile Enrollment portal.

You might relinquish ownership of a device if:

- the user left the company
- the user has replaced the device

Procedure

1. Go to **Devices > Devices**.
2. Select the device.
3. Click **Device details page** and click ⋮ icon.
4. Select **Relinquish Ownership**.

7.5.33. Wiping a Device

Wiping a device removes all the data and returns the device to factory default settings.

Procedure

1. Go to **Devices > Devices**.
2. Select the device.
3. Click **Actions** (upper right-hand side).
4. Select **Wipe**.
5. Alternatively, click on the device name link to go to the Device details page and click the ⋮ icon. Select **Wipe** and click **OK**.
6. By default, the **Preserve Data Plan** option is selected.
   (Optional, applicable to iOS 11.3+ devices) Select the **Skip Proximity Setup** option.
7. Select the **Return to Service** option to automatically re-enroll after the data is erased, so that you don't have to re-enroll the device manually after a wipe. Applicable only for iOS 17+ devices enrolled in DEP mode.
   1. Select the **Wi-Fi Configuration** from the dropdown menu. The user needs to deactivate all activation locks. Applicable only for iOS 17+ devices enrolled in DEP mode.
   2. (optional) Select the **Preserve Apps** option, if you want the devices to return to service with the existing apps preserved. Only the apps that are installed using Ivanti N-MDM with high priority will be preserved. Applicable only for iOS 26+ devices.
8. For macOS devices, you can send a 6-digit PIN to the device as passcode. On the device, the user is prompted to enter the PIN to access the device. To proceed with the wipe action, the device user needs to:
   1. Enter the PIN.
   2. Select the check box to confirm the device wipe action.
   3. Click **Yes, wipe this device**.
9. For ChromeOS devices, when you perform a Wipe operation from the **Device Details** or **Device Listing** page, a pop up window "Wiping a device returns it to factory settings, which can result in a loss of data on the device. The Wipe action differs by platform." appears on the screen.
   1. Select the "I understand that Wipe cannot be reversed" check box to confirm the device wipe action.
   2. Click **Wipe** to wipe the device.

The device status changes to "**Wipe Sent**." The updated device status will be visible after a periodic device sync.

On Android Enterprise devices, you can perform the **Wipe** device action even after the device reboots and remains locked.

Android devices that are in the **Wipe Pending** state can be deleted using the **Delete Device** option present on the **Device Details** page. Once a device is deleted, it loses connection to the server and becomes non-compliant. So the user must re-enroll the device after performing the factory reset.

7.5.34. Deleting devices

After you retire a device, you can delete it. Deleting it removes it from all pages. You can delete a device only if its status is Retired, Retire Pending, Wiped, or Wipe Pending.

Procedure

1. Go to Devices >Devices. The devices list appear on the screen.
2. Select the device you want to delete.
3. Click **Actions**.
4. Under the **Common** section, select the **Delete Devices** option. A pop up appears on the screen.
5. Select the "I understand that Delete cannot be reversed" option, and then click **Delete device(s)**.
6. Alternatively, you can delete a device by following the steps below:
    - Go to **Devices** >**Devices**.
    - Under the **User Display Name** column, click any link. The **Device Details** page appears on the screen. Click **Device Details**. A pop up appears on the screen, and if you acknowledge the warning and click **OK**, the specific device will be deleted.

Deleting multiple devices

You can delete multiple devices by selecting all the devices you want to delete.

Procedure

1. Go to **Devices > Devices**.
2. Select the devices from the available device list.
3. Click **Actions** tab, under the **Common** heading select the **Delete Devices** option.
4. On the **Delete Device(s)** window:
    1. Select the **I understand that Delete cannot be reversed** check box.
    2. Click on **Delete valid device(s)**, to delete the selected devices.

7.5.35. Unlocking a Device

This section contains the following topics:

- Unlocking Android devices
- Unlocking AppConnect for Android apps
- Unlocking an iOS device
- Unlocking ChromeOS devices

To unlock a device:

You can clear the screen lock on a device. Unlocking works somewhat differently on different devices.

Procedure

1. Go to **Devices > Devices**.
2. Select the devices.
3. Click **Actions**.
4. Select **Unlock**.
5. Alternatively, click the device name link to go to the Device details page and click the **Unlock** icon and click **OK**.

Unlocking Android devices

When an Unlock command is received, the Android app attempts to reset the passcode. In the Device Admin and Device Owner modes, the unlock code is reset, whereas in the Profile Owner and Company Owned Personal Enabled modes, the work profile unlock code is reset.

Unlock command provides an option for the administrator to set the unlock code with a combination of alphanumeric characters. The default option, which sets the unlock code to '0000' can be performed on multiple devices. However, the new option, Custom unlock code for Android, can be performed on one device at a time. The minimum number of characters should be 6 and maximum should be 8. This option is available under the **Actions** tab, as well as in the **Device Details** page. When you select the Unlock option from **Actions** tab or from the **Device Details** page, you can see the following two options.

- Default
- (Android only) Provide an unlock code - You can provide an Unlock code from this section and click **Unlock**.
    - Skip passcode reset prompt on device - Select to skip resetting the passcode if the passcode configuration is pushed to a device.

After setting the unlock code, the administrator can find the unlock code in the **Audit Trials** page and **Device Logs** page.

> The Directboot unlock works only for default unlock option, '0000' unlock code. The custom unlock code for direct boot is not supported.

Unlocking AppConnect for Android apps

For AppConnect apps, the **AppConnect Unlock** command helps to unlock containers that have been locked due to users trying to log in multiple times with incorrect passcodes. This unlock does not unlock the device.

Unlocking an iOS device

When an Unlock command is received, the iOS app removes the passcode from the device. If the **passcode configuration** specifies that a new passcode is required, then the device user will be prompted to set a new passcode that complies with the rules defined in the passcode configuration. The user must make this change within 60 minutes or the app will force the user to set the new passcode.

Unlocking ChromeOS devices

When a ChromeOS device is selected and the **Unlock** option is clicked, a pop up window appears on the screen - "Unlocking may clear an existing passcode to enable a user to access the device. Unlocking differs by platform." Click **Unlock** and the device status will be updated to "Unlock Sent", and the updated status will be visible after periodic device sync.

7.5.36. Restarting or shutting down devices

This section contains the following topics:

- Restarting a device
- Shutting down a device

Applicable to: Android 7.0+ (managed devices), iOS 10.3+ supervised, tvOS 10.3+ supervised, macOS 10.13+, and Windows 10+ devices.

Administrators can restart or shutdown an iOS supervised device individually from the device details page or in bulk from the devices list page.

Restarting a device

Procedure

1. Go to **Devices**.
2. Navigate to the device.
3. Click the link in the **Name** column.
4. Click the **Actions** button.
5. Click **Restart/Shutdown device**.

> Unsupported devices cannot be restarted.

6. Read the displayed warning.
7. (Optional) Select the option to clear the passcode of the device on restart. If the passcode is not cleared, the device will require a passcode and will not be connected to Wi-Fi after the restart.
8. Select **Restart Device** if not already selected.
9. If you still want to restart the device, click **Send to Device**. Otherwise, click **Cancel**.

> For Android devices, administrators can view the information on when the device was restarted under **Uptime** in the Device Details page.

You can restart multiple supported devices from **Devices** list page. To do so, select the devices, click **Actions >Restart/Shutdown Device,** and follow the instructions on the screen.

Shutting down a device

Procedure

1. Go to **Devices**.
2. Navigate to the device.
3. Click the link in the **Name** column.
4. Click the **Actions** button.
5. Click **Restart/Shutdown device**.

> Unsupported devices cannot be restarted.

6. Read the displayed warning.
7. Select **Shutdown Device**.
8. If you still want to shutdown the device, click **Send to Device**. Otherwise, click **Cancel**.

You can shutdown multiple supported devices from **Devices** list page. To do so, select the devices, click **Actions >Restart/Shutdown Device,** and follow the instructions on the screen.

7.5.37. Clearing the Restrictions Password (iOS only)

You can clear a Restrictions password set by users on supervised iOS 8 devices. This action is available for active devices only.

Procedure

1. Go to Devices > Devices.
2. Select the entry for the device.
3. Select Actions > Clear Restrictions Password.
4. Confirm the action when prompted.

7.5.38. Deleting Sentry association for a device

Sentry association is made to devices for App Tunneling or ActiveSync-enabled email system which controls email access to devices. If required, any device that is associated with Sentry can be removed from its association as follows:

Procedure

1. Go to **Devices.**
2. In the **Name** column, click on the device link of the device for which you want to delete the Sentry association.
3. Click on the **Sentry** tab.
4. In the **Actions** column, click **Delete**.

7.5.39. Assigning Custom Attributes to Devices

You can assign custom device attributes such as internal ID to one or more devices. Each attribute has a corresponding value that you can use for tasks like creating configurations and device groups. After you create custom attributes, you can assign them to devices. For more information about managing attributes, see **Attributes**.

Procedure

1. Log in to the Administrative portal.
2. Go to **Devices**.
3. Select one or more devices.
4. Click **Actions**.
5. Select **Assign Custom Attributes**.
6. Select one of the following options:
    - Force assign (overwrite) all attributes even if any existing values are found.
    - Overwrite only if value is empty, and skip attributes with existing values.

Select the attributes you want to assign and enter their values (empty values are not allowed).

8. Click **Assign**.

> The **Custom Device Attributes** with their values can be exported to CSV format from the **Device Details** page.

7.5.40. Removing Custom Attributes from Devices

Proceed with caution as this action is not reversible. To remove custom attributes from one or more devices:

Procedure

1. Go to **Devices**.
2. Select one or more devices.
3. Click **Actions**.
4. Select **Remove Custom Attributes**.
5. Select the attributes you want to remove.
6. Click **Remove**.

7.5.41. Synchronising and fetching app feedback

You can send a request to an app installed on Android devices to get the details of the current app configuration status of the app. When a request is sent, you receive app configuration feedback report for the device.

Procedure

1. Go to **Devices**.
2. Click on the device for which you want to send the request.
3. Click **Actions**.
4. Select **Sync and fetch App feedback**. The request is sent to sync and fetch the app configuration feedback. The App Feedback Last Sync field beside Client Last Check-in field will get updated.
5. In the **Installed Apps** tab, click **View Details** link for the app in the **App feedback** column. The **App Feedback** Window is displayed.
   Key - Provides detailed information and provides placement of reported settings (in the Managed app config of the app) based on the feedback received from apps.
   Time Stamp - Time and date of the Key.
   Severity - Specifies the severity of the key. Example: 'Info', 'Error'.
   Message - Type of message received from app config feedback. Example: 'Failure'.
   Data - Details of the data received from app config feedback.

Viewing app config feedback from the App Catalog

You can view app configuration feedback report for the particular app from the App Catalog.

Procedure

1. Go to **Apps > App Catalogue**.
2. Select a app for which you wish to view the details.
3. Click the **App Config Feedback** tab. The **Device Count** column displays the number of devices (hyperlink) for each key of the app configuration feedback report.
4. Click on the number of devices hyperlink to view the details of the devices. For example, by clicking on hyperlink 5, displays the details of 5 devices. The following details are displayed for the combination of 'Key' and 'Severity', which is displayed above the table:
   Email Address - specifies the username. Clicking the username link navigates to **Installed Apps** tab under **Devices> Device Detail**.
   Device Type - specifies the device model.
   OS - Android OS version number.
   Serial Number - Serial number of the device.
   Time Stamp - Time and date it was last updated.
   Message - Type of message received from app config feedback. Example: 'Failure'.
   Data - Details of the data received from app config feedback.

You can view the app config feedback error notifications for the Android device by clicking the bell icon (top right) or in the **Dashboard > Notifications** page. Clicking the notification link navigates to **App Config Feedback** tab and view the app feedback report.

The app config feedback report will be removed and will not be displayed when the device is wiped or retired. Background job that runs every 24 hours purges data older than 7 days.

7.5.42. Setting firmware password

Applicable to: macOS 10.13 or supported newer versions.

The administrator can set or update the firmware (EFI) password for a macOS device. A firmware password prevents starting up of the macOS device from any internal or external storage device other than the startup disk selected by the device user. As a result, it also blocks the ability to use most startup key combinations.

Procedure:

1. Go to **Devices**.
2. To set or change the firmware password for a single device:
    1. Click the user name the device is associated with to view the device details page.
    2. In the General section, expand **Firmware Password** and click **Set Password** or click **Set/Change Firmware Password** from the device Actions menu.
    3. The following information is displayed in this section:
        1. **Password:** Password or a list of probable passwords.

            > When an admin sets the firmware password, the command is sent to the device. If the device does not respond in time, the password is stored temporarily and displayed in this field. The new password will not take effect until there is an acknowledgment from device and the device gets restarted. Till then, all probable passwords are displayed. After the device is restarted and the password change is acknowledged, then all the unwanted passwords are cleared.

        2. **Change Pending -** Indicates if the password change is pending.
        3. **Command Status -** Indicates if the password change was success or failure.
        4. **Allow OptionROMs -** Indicates whether option ROMs are to be enabled. By default, it is set to No.

To set or change the firmware password for more than one device:

1. Select the devices.
2. From the Actions menu, click **Set/Change Firmware Password**.

Enter the current and the new passwords.

If it's the first time, the current password can be left blank.

To reset the password, leave new password field blank.

5. Click **Save**.

> Only devices with supported macOS versions will be updated with new password. Unsupported devices will be skipped.

7.5.43. Reissuing a new Personal Recovery Key

Applicable to: macOS devices with Mobile@Work for macOS 1.66 or supported newer versions.

When migrating from other MDM solutions to Ivanti Neurons for MDM, administrators can request the OS to reissue a new Personal Recovery Key (PRK) upon enrolment if a PRK was previously issued prior to enrolment. This enables the key to be stored in Ivanti Neurons for MDM.

You can view the Audit Trails log entries for the PRK activities as follows:

1. Go to **Dashboard > Audit Trails**.
2. In the Type filter, select **Personal Recovery Key**.PRK entries will be displayed in the Device Management category and activities such as "Personal Recovery Key viewed."

Prerequisite

Distribute the following configurations to the devices before performing this procedure:

- Mobile@Work for macOS configuration.
- FileVault Recovery Key configuration.

Procedure

1. Contact **Support** to request the script to generate new PRK on the device.
2. Create a device custom attribute with the name "deviceprk" which is used in the script.
3. Upload the script to the repository in **Admin > Scripts and Files > All Scripts**. While doing so, select the "deviceprk" custom attribute.
4. Create a dynamic device group for devices for which PRK was not retrieved from the old MDM solution. Select the device group rules as follows: "**Platform=macOS** and **Encryption Enabled is equal to Yes** and **macOS Personal Recovery Key escrowed is equal to No** and **macOS Recovery Key Type is equal to Personal**."
5. Create a Mobile@Work for macOS Script configuration in which you can select the PRK script from the repository. Distribute the configuration to the new device group.
6. Schedule the script to run once a day or as desired. This script will ask for user password on every run. By default, the timeout period for the script execution is 60 seconds. It is recommended to extend the timeout period in the corresponding Mobile@Work for macOS configuration by setting the **Max Run Time** field to 300 seconds.

- The decrypted key is available from the device details page of a device in the Device Encryption Status section. Click **View** next to the FileVault Encryption Enabled field.
- On obtaining the PRK, the device moves out of the device group. Hence, the script configuration will not be applicable anymore and will be deleted from the device.
- After the MDM retrieves the recovery key of a device using the script, the script will be uninstalled from the device.

Related topics:

- **Attributes**
- **All Scripts**

- Device Groups
- Mobile@Work for macOS
- FileVault Recovery Key

7.5.44. Setting or changing recovery lock

Applicable to: macOS 11.5+

The administrator can set or change recovery lock for device reboot for macOS device running on Apple silicon. A recovery lock prevents starting up of the macOS devices in recovery mode, unless the passcode is entered.

Procedure:

1. Go to **Devices**.
2. To set or change the recovery lock for reboot:
    1. Click the user display name the device is associated with to view the device details page. Perform one of the following steps:
    2. In the **Overview** section, expand **Recovery Lock** and click **Set Password** or click **Change Password**. Or Click the **Actions** ellipsis and click **Set/Change Recovery Lock**.
    3. In the **Set/Change Recovery Lock** dialogue box do the following:
        1. **Current Password**: Enter the current password here. Keep it empty if you are setting it for the first time.
        2. **Password**: Enter the password you want to set.
        3. **Confirm Password**: Re-type the password you want to set.

Click **Set/Change Recovery Lock**.

> In Overview, **Recovery Lock Enabled** shows the status of the Recovery Lock passcode.

> Administrators can also clear the passcode by removing the existing passcode and click **Set/Change Recovery Lock**.

7.5.45. Apple Access Management

Prerequisites:

- Verify and lock the domain on Apple Business Manager or Apple School Manager.
- Configure at least one MDM server from the Apple Business Manager or Apple School Manager organisations, where managed apple IDs are present in the Ivanti Neurons for MDM.

Signing-in to Managed Apple ID allows organisations to control which Apple services and features users can access.

In Apple Business Manager or Apple School Manager, **Allow Managed Apple Account on** setting controls where users can sign in with their Managed Apple IDs. The administrators can configure this setting to restrict sign-in to managed or supervised devices, or allow it on any of the devices.

- **Any device** (default): Users can sign in with their Managed Apple IDs on any device, regardless of whether it's managed by an MDM solution.
- **Managed devices only**: Users can only sign in on devices managed by an MDM solution that supports the Get Token endpoint.
- **Supervised devices only**: Users can only sign in on devices that are supervised (and managed) by an MDM solution that supports the Get Token endpoint.

These settings are a part of the broader "Access Management" for Apple Services within Apple Business Manager and Apple School Manager.

> With enhanced security, restricting sign-in to managed or supervised devices can improve data security by ensuring that work-related data is only accessible on controlled devices.

Managed Apple Account Login will fail if zero or multiple Device Enrollment MDM server organisations are present in the **Device Enrollment** tab and the administrator sets the **Allow Managed Apple Account on** setting present under **Access Management** > **Apple Services** is set to "Supervised Devices Only" or "Managed Devices Only" in Apple Business Manager or Apple School Manger.

> The devices will fail to log in if the **Managed Apple** account is not present in the Ivanti Neurons for MDM Device Enrollment MDM server.

7.5.46. Group Policy Enrollment

Windows 10/11 devices can be enrolled in Ivanti Neurons for MDM using a group policy. Creating a group policy will automatically enroll all devices that are hybrid-joined to Azure AD.

ProcedureTo enroll devices with a group policy

	1.	Ensure your devices are hybrid-joined to Azure AD. For more information, see Microsoft's documentation: Hybrid Azure AD joined devices.
	2.	Create a group policy object. For more information, see Microsoft's documentation: Configure the auto-enrollment for a group of devices.
	3.	Create a security group that includes the devices you want to enroll. For more information, see Microsoft's documentation: Active Directory Security Groups.
	4.	Link the group policy object to the security group. For more information, see Microsoft's documentation: Link the GPO to the Domain.

User experience

When a user logs into the device using credentials in Azure AD, Microsoft finds the Azure AD based MDM configuration that belongs to their organisation. The device is enrolled in Ivanti Neurons for MDM and can receive policies and commands.

8. Apps

This section contains the following topics:

- App Catalogue
- Apps@Work
- iOS Apps@Work AppStore Features
- Viewing App Details
- App Configuration
- Assigning Custom Attributes to Apps
- Managed Configurations for Android
- Managing Google Play Apps
- Deleting Apps from the App Catalogue
- Upgrading In-House Apps
- Finding the Package Name for an Android App
- Categories
- Distribution Filters
- Exclude or Distribute apps
- Reviews
- Apple Apps and Books
- Catalogue Settings
- Deploying app dependencies
- Deploying Divide Productivity with Android Enterprise
- Setting up the Provisioner app
- Managing Windows Applications
- Ivanti Bridge

8.1. App Catalogue

This section contains the following topics:

- Licensing for app features
- Switching between list and grid view
- Adding Google Play Store app for Android Enterprise
- Adding an app from a public store
- Adding an in-house app
- Delegating device permissions for Android Enterprise In-house apps
- Displaying the provisioning profile status for iOS in-house apps
- Updating provisioning profile for iOS in-house apps
- Deploying in-house apps to Google Play
- Adding a web app for Android Enterprise devices
- Adding a web app for iOS devices
- Using Advanced Search
- Exporting Apps to a CSV file

Use the App page to manage your app catalog. The app catalogue lists the mobile apps you have made available for your users. These include apps that users can download from public app stores and apps you intend to distribute using Ivanti Neurons for MDM (in-house apps). AppConnect-enabled apps, GoClient for iOS, and M@W for macOS are also available as business apps on the App Catalog page, thereby simplifying the process of importing them for configuration and distribution. In MAM-Only devices, iOS users will be prompted to select the certificate to authenticate access to these apps when they open the app catalog.

M1 chipset MacBooks by Apple supports iPhone and iPad VPP apps. Only the administrator can push the supported iPhone and iPad VPP apps. This option is not available for users to install from App .

For the Ivanti Neurons for MDM tenants with Android devices, if Android Enterprise is not enabled by the end of March 2021, administrators will not be able to search for apps with the names. Communication on this change is displayed with a banner message when accessing the App page. This banner message continues to be displayed till Android Enterprise is enabled on these tenants and until the 'Don't show this again' checkbox option is not selected.

- Silent App Install method is not available for public macOS apps. The macOS apps can also be deployed through Apple Apps and Books via device-based licences and through the Silent App Install method on enrolments.
- While uploading the Go app to Ivanti Neurons for MDM server, if there is a need for you to select the **Convert to managed app** option, then you also need to enable the **Install on Device** option.
- App Catalog and app installation are not supported for Sonim XP5s devices.
- Android does not allow apps with active admin privileges to be uninstalled. To uninstall such an app, go to **Device Settings > Security > Device Administrators** and disable the Device Administrator privileges. Then, uninstall the app.
- If an Android Enterprise app is installed manually using the Android Enterprise Play Store on the device, and if the administrator later undistributes the app, then the app must uninstalled manually as well.
- In-house Android apps cannot be uploaded if the app is compressed or obfuscated.
- Public apps are not supported on Shared iPads.

- Due to a limitation from Apple, for Business-to-Business (B2B) iOS apps available in the App Catalog, descriptions and screenshots of the apps are not available in the **Details** tab.
- When you search for an app in the App Catalog or Admin portal, the search results will be based on **App Name**, **Comment**, **Description**, **Display Version**, and **What's New**. If the searched app data matches with any of these fields, it will be displayed as a search result.

Licensing for app features

The following App Catalogue features require additional licensing:

- Silent app install/uninstall: Silver licence
- Per-app configuration: Gold licence
- AppConnect custom configuration: Gold licence
- Android Enterprise custom configuration: Silver license

If an Android device is in kiosk mode:

Only in-house apps can be installed while the device is in Kiosk Mode. You can install public apps, but the device must exit Kiosk Mode before those apps can be installed. Also, you can limit the apps available for use on devices in Kiosk Mode to only the apps that are approved or whitelisted by your company. On devices using Android 4.1, If an approved app launches an app not included on the Allowlist, that app will launch and then be quickly minimised. On devices using Android 5.0, the unapproved app launched from an Allowlisted app will remain available.

Switching between list and grid view

Click the List or Grid icon on the right side of the App Catalogue screen.

Adding Google Play Store app for Android Enterprise

- You can add an app from the Google Play Store to the App Catalog and make it available to the users. To add an app from Google Play Store in Android Enterprise, it is required to approve an app to be included in the app catalog.
- The Google Play Store layout for Android Enterprise devices has a home page for migrated devices which is managed from Core and has a quick link to Ivanti Neurons for MDM that displays all the applications that are managed from Ivanti Neurons for MDM. When you migrate Android Enterprise devices from Core to Ivanti Neurons for MDM, only the applications that are common between Core and Ivanti Neurons for MDM App Catalog are listed in the work profile Google Play Store of the device. You can click on the Ivanti Neurons for MDM button to view the list of all the applications that are available from Ivanti Neurons for MDM App Catalog.

The Google Play Store layout for Android Enterprise devices has a home page for migrated devices which is managed from Core and has a quick link to Ivanti Neurons for MDM that displays all the applications that are managed from Ivanti Neurons for MDM. When you migrate Android Enterprise devices from Core to Ivanti Neurons for MDM, only the applications that are common between Core and Ivanti Neurons for MDM App Catalog are listed in the work profile Google Play Store of the device. You can click on the Ivanti Neurons for MDM button to view all the applications that are available in Ivanti Neurons for MDM App Catalog.

Prerequisite

- You must enable Android Enterprise to access and add Google Play store applications to the App Catalog.

ProcedureProcedure

1. Go to **Apps > App Catalogue**.
2. Click **Add** (top left).

> Select Google Play from the drop-down list to search for an app in the Google Play Store. Google Play iFrame is displayed when Android Enterprise is enrolled.

3. Search for the app in the Search field and click on the app.
4. Click **Done**.

> An approved app can later be unapproved by clicking **UNAPPROVED**.

Option	Description
Approval Settings	
Keep approved when app requests new permissions	Allows users to install updated app
Revoke app approval when this app requests new permissions	**Removes the app from the store until it is re-approved.**
Approval Settings	
Add Subscriber	Enter the email address to add subscribers to email notifications when the apps you have approved request new permissions.

Adding an app from a public store

You can add an app from a public store to the app catalogue and make it available to the users.

Procedure

1. Go to **Apps > App Catalogue**.
2. Click **Add**.
3. Choose the app you want:
4. Select the public app store.
5. Enter the name of the app.
6. Select the app from the list.
7. Click **Next**.
8. Describe the app for users:
9. Add or remove categories.
10. Enter an optional description.
11. Click **Next**.
12. Define app distribution:
13. Select a distribution option.

14. Expand the **Advanced Options & App Configuration** section.
15. Use the following guidelines to complete the options:

Setting	What To Do
Install on Device	Select this option to start installation immediately after registration. The user will be prompted to confirm installation of the app except under the following conditions: • The device is a supervised iOS device for new app installs and app updates. • The device is a iOS non-supervised device for app updates. • The users who have enrolled in the Apps and Books program. • The device is a Samsung Knox device and the silent installation option below has been selected. For iOS public apps, when installed for the first time in the device, the App Catalogue displays 'Reinstall' button that allows the user to install the app again. The reinstallation is performed if app version on device is different from the version on iOS app store.
Do not show app in end user App Catalogue	Select this option if you do not want the user to see the app in the app catalogue on the device.
Set App Install Priority	Select High, Medium or Low to set the priority of the app installation during user onboarding. Only high priority apps gets installed during user onboarding.
Suspend app repush after a set number of failed attempts (iOS only)	Switch the toggle switch to ON to suspend the re-push of the app after a set number of failed re-push attempts using the following settings: **Stop repush after** - Enter the number of failed re-push attempts after which the re-push should be stopped. The values entered should be within **1** to **999**. **failed attempts and try again after** - Enter the number of hours required after the failed re-push to action the re-push again. The values entered should be within **3** to **48** hours.
(Android only) Silently install on Samsung Knox devices	This option does not apply to public apps.
(iOS and macOS only) Enable Per-App VPN for this app	Select this option to use a **Per-App VPN configuration** with this app. Select the Per App VPN configuration to be used from the drop-down list. For macOS, select Tunnel Per App VPN configuration only.
(iOS only) Prevent backup to iCloud and iTunes	Select this option to keep data related to this app from being backed up to iCloud and iTunes.
(iOS only) Remove apps on un-enrolment	Select this option to remove this app once the device is no longer managed by Ivanti Neurons for MDM.
(iOS only) AppConnect Custom Configuration	For AppConnect-enabled app, enter the keys and values that specify your custom configuration preferences. See the documentation for the app for available keys.
iOS 7+ Managed App Settings	Enter keys and values defined for this app as an iOS 7+ managed app. See the documentation for the app for information on supported keys.

> **Android Enterprise** apps will have different options.

Click **Next**

4. Select a promotion option:
5. Click **+ Add Description** to enter a brief description of the configuration.

- Not Featured
- Featured List
- Featured Banner
- If you select Featured Banner specify the following details:
    1. **Title** - Specify the application title
    2. **Description** - Specify the application detail
    3. **Banner style** - Select a banner colour

6. Optionally, change the distribution of the configuration.
7. Click **Done** to save the app configuration.
8. Click **Done**.

> When you search for a Windows app in the App Catalog, you can search the app that matches closely by using the **App Name** or **AppStore ID** options from the drop down list:

- **App Name** - Select this option and provide the App Name
- **AppStore ID** - Select this option and provide the AppStore ID

The Windows Store app search supports Win32 store apps.

Make sure the Winget tool is available on the device to manage the Win32 Store apps.

Adding an in-house app

You can upload an in-house app to the app catalogue with the following file formats. A large file could take several minutes to upload. The number of in-house application versions is limited to 100. If that number is exceeded, the Ivanti Neurons for MDM system purges the oldest versions of the application. The status of the application upload and purge is listed and is visible from the Audit Trails page.

MIP app inventory returned by Mobile@Work may be incorrect for few apps. Mobile@Work may fail to detect the installation status of apps that are not installed in default location. For such apps, adding the detection script will help in identifying the right state of the app on the device. Mobile@Work determines the presence of the app if the exit code of the detection script is 0. For any other exit codes, the app will be determined as not installed. Based on the apps detected, Mobile@Work prepares the inventory report for the device.

- IPA (iOS)
- MIP (Packager macOS app)
- PKG (macOS)
- APK (Android)
- APPX, APPXBUNDLE, EXE, and MSI (Windows)

> For applications such as PKG with scripts or DMGs having PKG with scripts, the Mobile@Work for macOS can only detect a successful install request. It will not report if the app has been deleted or if the scripts that were installed were removed. Therefore, the Ivanti Neurons for MDM server will be unable to resend an install command. If the connection is disconnected while downloading the apps, retry the app installation by doing a check-in. For MIP apps, even if the app is removed from the device installed by PKG or DMG having PKG with script in it, Mobile@Work will not the install the MIP app if the entry of the PKG exists in the receipts folder of the client device.

Procedure

1. Go to **Apps > App Catalogue**.
2. Click **Add** (top left).
3. Under **Select the platforms to upload file**, choose your platform category (e.g., **Apple Apps**) and select the specific OS (e.g., iOS or macOS from the dropdown of Apple Apps).

> If a user selects a platform and attempts to upload a conflicting file type (e.g., selecting Apple but uploading an .apk), the system will trigger a "Not a valid file format" error.

4. Drag the app file to the dotted box, or click **Choose File** to select it from your file system and click **Confirm**.
5. Click **Next** (lower right).
6. Describe the app for users and configure prerequisite apps:
7. Add categories.
8. When adding a macOS package, if the package file contains more than one app (for example, Microsoft Office and Cisco AnyConnect packages), then the selected primary apps will be used to identify that the package is installed. Per-app VPN, if configured, will be applied to these apps.
9. Enter an optional description.
10. **MSI product code**: When uploading the MSI apps, the product code of the MSI app is auto-populated in this field.

> You must select the "I have checked the MSI product code" option to ensure the correct GUID is populated.

Override URL: Enter an optional App Source URL Override to allow downloading the app from a different source or to allow obtainment of large files, such as Microsoft Office installation media, from a local network (HTTP and HTTPS). This option requires access to a secure internal network and manual synchronisation of an alternate server on which the apps are stored. Do not enter a value unless you have established the necessary infrastructure. You can edit this value while editing the app settings for the specific app.

- For iOS apps, the app Override URLs must be in HTTP or HTTPS format only.
- For Android and macOS apps, the app Override URLs must be in HTTPS format only.
- For macOS apps, the URL should end with the extension, which is .pkg.

6. **Command Line** (Windows 32-bit MSI apps only): Enter an optional Command Line switch to specify additional information that are not part of the package while deploying the MSI files. For example, to write installation logs to an output file, you can enter "/log output.txt" in this field. This creates the output.txt file in the C:\Windows\System32 folder. By default, the Command Line option /qn for silent installation is auto-populated during MSI app upload.

> The package name of the MSI app to be uploaded should not be added as part of Command Line arguments. If added, the upload will be restricted until the app's package name is removed from the Command Line arguments. A list of all the supported Command Line options is provided under the additional link. This link will be visible in the app's View and Edit mode.

.EXE for Win32: Installed through Bridge using the Admin PowerShell mode. The Bridge functionality will be automatically used, if available.

- Update version to maintain consistency between the **Display Version** and **Bundle Version**
- Installer (.EXE) location
- Installer command line parameters: argument to silently run the file (for example, /SILENT or /VERY SILENT) is mandatory
- Installer run as user: to install using user's credentials, select 'Run as User' option

For Win32 Store apps: Installed through Bridge using the Admin PowerShell mode.

9. For Packager macOS apps, configure prerequisite apps (optional). See Understanding Packager in-house macOS apps for an overview of prerequisite app functionality.
10. **Launch URL**: Enter the custom URL for launching the app in AppStation. Required only when adding non-AppConnect apps for distribution in a MAM-only deployment with AppStation and is applicable only for iOS apps.
11. Configure **app delegation**.

> Once you delegate a prerequisite app and it becomes a prerequisite app for the app from the non-default space, you cannot un-delegate that app unless you remove the prerequisite relationship first.

Click **Next**.

13. Click **Next**.
14. (Optional) Add screenshots of the app.
15. (Optional) Add or replace icons for the app (iOS, MacOS, and Windows apps).
16. Click **Next**.
17. For Packager macOS apps, define or select installation scripts to run before and/or after app installation. Select one or both of the following scripts by typing in the search box or clicking the link to see the list of scripts. Click **Next**.
18. You can create the scripts in the **Admin > Scripts and Files > All Scripts** page. If you upgrade the app, you can choose to copy the scripts from the older app and run the scripts for the upgraded app. If you skip this section, you can configure scripts by editing the app later.

- **Pre Install Scripts** - Enter the script name to select the script to run before app installation. The pre-install scripts will be run or retried until the script execution success status is received from the client. Only after that, is the app install command sent. You can view the script run status in the device details page in the **Logs** tab.
- **Post Install Scripts** - Enter the script name to select the script to run after app installation.
- **Uninstall Scripts**: Enter the script name that server sends to a device when it detects that an app is no longer distributed to the device.
- **Detection Scripts**: Enter the script name that server sends to a device to detect an app. The result of the detection script of the app overrides the default inventory result of the app on the device. Irrespective of whether the App is distributed to the device or not, the detection script of all apps will be sent to the device to evaluate the existence of the apps on the device.
  A sample detection script is shown below:

```
#!/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
```

Define app distribution:

12. Select a promotion option:
13. Select a distribution option.
14. Expand the **Advanced Options & App Configuration** section.
15. Use the following guidelines to complete the options:
16. Click **Next**.

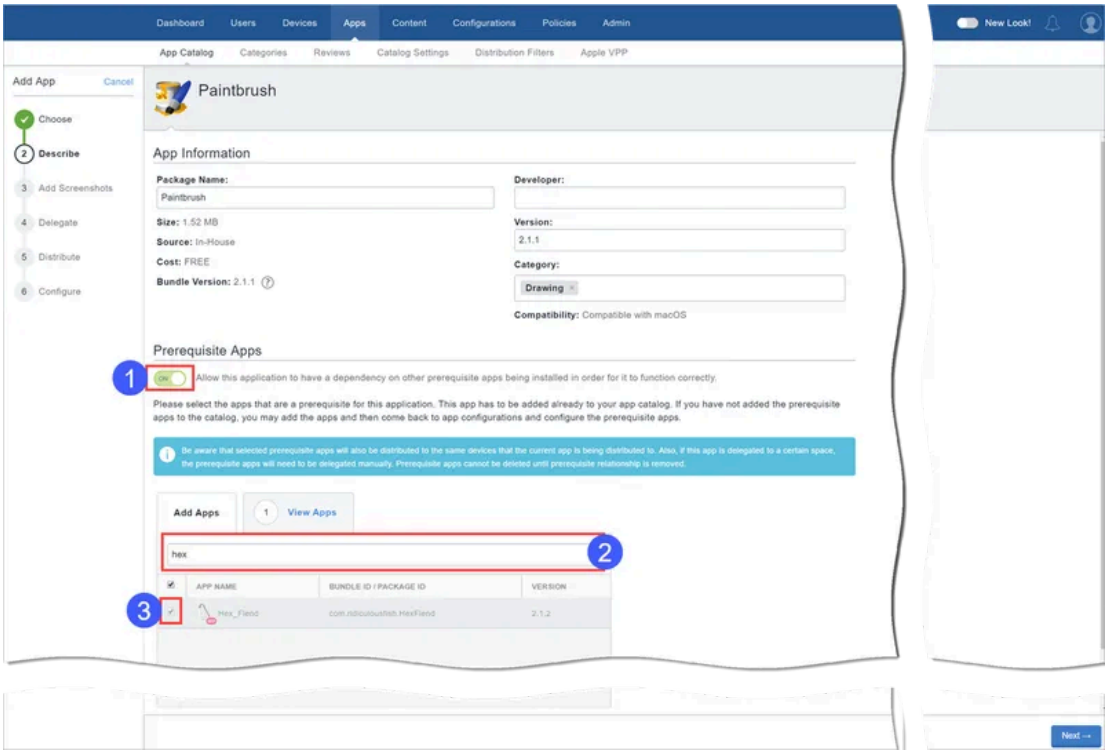
Setting	What To Do
Install on Device	Select this option to start installation immediately after registration. The user will be prompted to confirm installation of the app except under the following conditions: • The device is a supervised iOS device. • The device is a Samsung Knox device and the silent installation option below has been selected.
Do not show app in end user App Catalogue	Select this option if you do not want the user to see the app in the app catalogue on the device.
Set App Install Priority	Select High, Medium or Low to set the priority of the app installation during user onboarding. Only high priority apps gets installed during user onboarding.
Suspend app repush after a set number of failed attempts (iOS only)	Switch the toggle switch to ON to suspend the re-push of the app after a set number of failed re-push attempts using the following settings: **Stop repush after** - Enter the number of failed re-push attempts after which the re-push should be stopped. The values entered should be within **1** to **999**. **failed attempts and try again after** - Enter the number of hours required after the failed re-push to action the re-push again. The values entered should be within **3** to **48** hours.
(Android only) Silently install on Samsung Knox devices	Select this option if you do not want the user prompted to confirm installation on Samsung Knox devices.
(iOS and macOS only) Enable Per-App VPN for this app	Select this option to use a Per-App VPN configuration with this app. Select the Per App VPN configuration to be used from the drop-down list. For macOS, select Tunnel Per App VPN configuration only.
(iOS only) Prevent backup to iCloud and iTunes	Select this option to keep data related to this app from being backed up to iCloud and iTunes.
(iOS only) Remove apps on un-enrolment	Select this option to remove this app once the device is no longer managed by Ivanti Neurons for MDM.
(iOS only) AppConnect Custom Configuration	For AppConnect-enabled app, enter the keys and values that specify your custom configuration preferences. See the documentation for the app for available keys.
iOS 7+ Managed App Settings	Enter keys and values defined for this app as an iOS 7+ managed app. See the documentation for the app for information on supported keys.

17. Click **Done**.

- Not Featured
- Featured List
- Banner

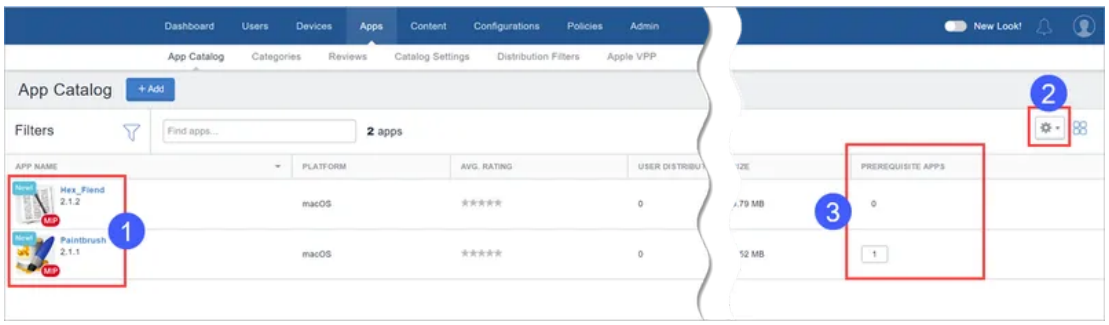
Understanding Packager in-house macOS apps

When importing Packager in-house macOS apps, the admin can enable, 1, the Prerequisite Apps feature to search for, 2, and select, 3, prerequisite apps that must be installed on clients before the app the admin is importing can be installed.



Once imported, the Packager macOS in-house app appears in the app catalog with the MIP badge displayed, 1, below. You can then use the column settings, 2, to add the PREREQUISITE APPS column, 3, to see at a glance the apps with dependencies, that is, that have prerequisite apps.

- You can search for and select MIP, non-MIP, and public apps (Apps and Books and macOS App Store public apps) as prerequisite apps.
- Users need to accept Apps and Books licence for Apps and Books prerequisite apps to install silently.
- For non-Apps and Books public prerequisite apps, administrators need to explicitly distribute the public apps and the user has to install the public apps. The public apps (Apps and Books and non-Apps and Books apps) have to be imported into the App Catalog in order to show up in the prerequisite apps list. The Source column indicates the type of prerequisite app.
- MDM check-in is required to install a non-MIP in-house app that has non-MIP prerequisite apps.
- Users need to manually install public non-Apps and Books prerequisite apps.
- If the Apps and Books token is removed or if the licence is exhausted, then the Apps and Books apps selected as the prerequisite apps, and thereby the main app, are not installed. The administrator has to follow a best practice to inform the users in advance in any of these cases for Apps and Books apps.

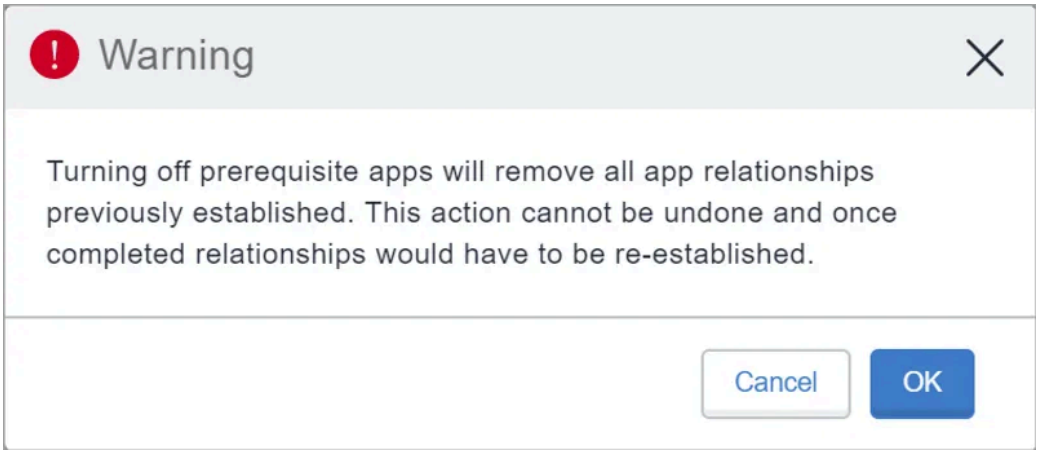


Prerequisite apps are also available as independent apps for download by the user when they are distributed explicitly. If the user tries to uninstall a prerequisite app:

- Make sure that the prerequisite app installs again in the next device check-in.
- The prerequisite app is uninstalled if there are no dependent main apps installed on the same device.
- If the prerequisite app is not distributed explicitly, then the prerequisite app will be uninstalled along with the main app.
- If the prerequisite app is distributed explicitly, then the prerequisite app stays on the device.
- If the prerequisite app has a dependent app, then the prerequisite app stays on the device.

Turning off the Prerequisite Apps feature

When interacting with apps with dependencies and prerequisite apps, for example, when updating, deleting, or delegating such apps, you will encounter system prompts informing you about how the app's dependency or prerequisite status may impact the actions you seek to perform. For example, when you try to turn off the Prerequisite Apps feature for an app, the following prompt appears:



- If you turn off the Prerequisite Apps feature for an app, details about the prerequisite apps are cleared. This includes automatic delegation and un-delegation of prerequisite apps from sub-spaces.
- In Apps@Work, the install button does not appear for dependent apps whose prerequisite apps are not already installed on the harbouring client.
- On the user devices, when a user tries to install an in-house app with dependencies, the prerequisite apps will be installed (if not already installed) first followed by the main app, which may take a few minutes. The list of dependent apps are displayed to the user along with the status of their installations.

Delegation and un-delegation of prerequisite apps from spaces

- Prerequisite apps tied to an app (the main app) are automatically delegated when the main app is delegated to a subspace.
- If the main app is un-delegated from a sub-space, the prerequisite apps are also un-delegated where prerequisite apps are not explicitly distributed. However, the prerequisite apps that are tied to more than one main app are not un-delegated.
- If the prerequisite apps are explicitly delegated, then they are not automatically un-delegated.

Delegating device permissions for Android Enterprise In-house apps

Delegated permissions can be assigned to in-house apps that can be applied to Android Enterprise managed devices and AMA devices.

Procedure

1. Go to **Apps > App Catalogue**.
2. In the **App catalog**, select an app to which you wish to delegate device permissions.
3. Click the **App Configurations** tab.
4. In the Delegated Permissions (In-house Android Enterprise app), select the required permissions for the apps:

> Only COSU deployment uses AMAPI. Refer to the AMAPI section for more information.

   - **Configure third-party app runtime permissions**
   - **Hide and suspend third-party apps**
   - **Manage certificates**
   - **Manage app configurations**
   - **Manage blocking app-uninstallation**
   - **Manage Enabling System apps**
   - **Manage Certificate Selection** (not supported in AMAPI mode)
   - **Manage Retention of Un-Installed apps** (not supported in AMAPI mode)
   - **Manage Network Log Collection**(supported in only one app at a time)
   - **Manage Security Log Collection** (supported in only one app at a time)
   - **Manage Installation of existing apps** (not supported in AMAPI mode)
   - **Install and remove packages** (not supported in AMAPI mode)

Install and remove packages option is available on all supported Android Device Owner mode devices (7.0 or later). Other delegated permissions are applicable only to Android 8.0 or later.
Configure the distribution options, selecting from **Everyone with App**, **No One**, or **Custom**.

6. Click **Save**.

Displaying the provisioning profile status for iOS in-house apps

Display provisioning profile status on the App Catalogue page for the iOS in-house apps. The tool tip next to the profile name displays the number of days for expiry of the profile. This status can be useful to check when the provisioning profiles are expiring for the in-house apps.

The status is useful for troubleshooting apps that are not installing due to profile being expired. The apps would install but would not open or launch if there is no appropriate provisioning profile.

Procedure

1. Go to **Apps > App Catalogue**.
2. Click the gear icon on the top right to display the columns.
3. Select **Provisioning Profile** to display the column for the list of apps on the App Catalog page.

The Provisioning Profile details are also available on the app details page under the Provisioning Profile Settings section.

Updating provisioning profile for iOS in-house apps

Provisioning profile is applied to a specific iOS in-house app. The Provisioning Profile details of an app are available on the app details page. A Provisioning Profile which is not expired is required in an iOS in-house app to launch on the device. If it is expired, you can update a provisioning profile by uploading the profile in the app details page.

Procedure

1. Go to **Apps > App Catalogue**.
2. Click on the app for which the provisioning profile update is required. The app details page is displayed.
3. Click **Edit**.
4. In the **Provisioning Profile** section, click **Choose File**.
5. Select the provisioning profile file (.mobileprovision file extension) to be uploaded and click **Save**.

Deploying in-house apps to Google Play

Upload your in-house apps to the Google Play Private channel and import them into Ivanti Neurons for MDM for deployment to Android Enterprise enabled devices.

Procedure

1. Log into Goople private apps console: **https://play.google.com/apps/publish**.
2. Click **All Applications** in the left menu.
3. Click **Create new application** and enter a name for the application.
4. Click **Upload APK** to upload the .apk file you generated.
5. Click **Store Listing**:
   - Enter a short description and a full description.
   - Upload screenshot for all tabs.
   - Upload a high resolution icon.
   - Upload a feature graphic icon (graphic.png).
   - Enter the required information for Categorisation, Contact details, and Privacy policy.
   - Complete the questionnaire for an app rating.
6. Click **Pricing & Distribution**.
   If all the required information has been entered Ready to Publish is displayed a the top of the page.
7. Go to the Apps tab In the Ivanti Neurons for MDM.
8. Click **Refresh Available Catalogs** to sync your private apps.

> It may take several hours to publish your app.

Adding a web app for Android Enterprise devices

A web app is a link to any website, which gets installed on the device as a shortcut. Web apps behave in a similar manner as any other app, which means the web app can be distributed on the same criteria as an app. It appears in the app catalogue and can be installed by users as any other app. However, web apps can have only a single version, and the silent install is not supported. Web apps use web clips and get installed on device as configurations, but behave as apps.

Set up a web clip as an app in the app catalog to make the web app available in the app catalog for the users. The web clip can be defined as a configuration, but a configuration can only be distributed by an administrator. Users can choose to install the web app on their devices or opt out, whereas users have no option to opt out of a web clip configuration.

In Android Enterprise, a web app is an embedded form of web app that runs over Google Chrome inside the Work Profile. It can be combined to a VPN or SSO solutions in Android Enterprise. After a web app is created, the app works like any other Android app, which you can distribute as required. Web apps require Chrome to be installed on Work Profile on Company Owned Device in order to run.

> If there are any issues with using this feature, administrators can contact **Support**.

Procedure

1. Go to **Apps > App Catalogue**.
2. Click **+ Add**.
3. Select **Google Play** from the drop-down list to search for an app in the Google Play Store. Google Play iFrame is displayed if Android Enterprise is enrolled.
4. Click **Web Application**.
5. Describe the app for users:
    1. App title or name.
    2. App URL.
    3. Display type for the web app.
    4. Upload icon, which can be a 512px square PNG or JPEG image.

Click **Create**. Wait for the app to be published to iFrame. It can take a few minutes. You can close it and return later.

7. After the web app is published, import the app to app catalog for distribution. Click the web app icon.
8. Scroll down and click **Select**.
9. Add categories and an optional description.
10. Click **Next**.
11. Select one of the following options for App Delegation:
    - Delegate this app to all Spaces.
    - Do not delegate this app to all Spaces.

Click **Next**.

13. Select a distribution option for the application.
14. Click **Finish**.

After adding a web app, you can edit the web app whenever required. To do so:

1. In the **App Catalog** page, click the name of the existing web app.
2. Click **Edit** to edit the web app fields.

Adding a web app for iOS devices

A web app is a link to any website, which gets installed on the device as a shortcut. Web apps behave in a similar manner as any other app, which means the web app can be distributed on the same criteria as an app. It appears in the app catalogue and can be installed by users as any other app. However, web apps can have only a single version, and the silent install is not supported. Web apps use web clips and get installed on device as configurations, but behave as apps.

Set up a web clip as an app in the App Catalog to make the web app available in the app catalog for the users. The web clip can be defined as a configuration, but a configuration can only be distributed by an administrator. Users can choose to install the web app on their devices or opt out, whereas users have no option to opt out of a web clip configuration.

> If there are any issues with using this feature, administrators can contact **Support**.

Procedure

1. Go to **Apps > App Catalogue**.
2. Click **+ Add** (top left).
3. Click **Web apps**.
4. Describe the app for users:
    1. App Name.
    2. App URL.
    3. Platform Type.
    4. App Icon.
    5. Add or remove categories.
    6. Full Screen - Select to display the web app as a full screen application.
    7. Removable - Select to make the web app removable.
    8. Click **Next**.

Select one of the following options for App Delegation:

- Delegate this app to all Spaces.
- Do not delegate this app to all Spaces.

Click **Next**.

7. Select a distribution option for the application.
8. Click **Finish**.

Editing a web app

After adding a web app, you can edit the web app whenever required.

Procedure

1. In the **App Catalog** page, click the name of the existing web app.
2. Click **Edit** to edit the web app fields.

Slow Rollout Distribution

The Slow roll out setting lets administrators to automatically roll out new version of applications to devices gradually. The option Use slow roll out distribution method, is available when you roll out the subsequent release of the application. The Ivanti Neurons for MDM administrative portal lets you edit applications even when the slow roll out is paused.

Once the slow rollout is set for one release, it is applicable for the subsequent releases with the same percentage that you set for the last release. You can pause the distribution of an application if the distribution is set to 100%. However, if you set the distribution target to 100%, you must manually set the distribution target percentage for the next version as the UI resets the percentage to 0%.

Procedure

1.	**Go to App Catalog, Apps, select one of the distribution mode options.**
2.	**Select the option Custom % of devices in selection summary (Slow Rollout).**
3.	**From the Slow rollout settings, drag the slider in Specify distribution target%.**
4.	**Click Confirm, and then click Done. The status of the latest app version is displayed. The App Catalog page indicates the SLOW ROLL OUT status in the table.**

If you cannot perform tasks on the **App Catalog** page, it might be that you do not have the required permissions. You need the App & Content Management role.

Using Advanced Search

You can use the Advanced Search option to search for an app based on rules to identify and view the apps with specific criteria. These rules can be constructed using the applicable operators, including the "equals", "is less than", "is greater than", "is equal to", and "is not equal to" operators. The rule options can be nested together using the ANY (OR) or ALL (AND) options. The apps matching the rules are displayed below the section.

> The custom attributes values used in Search are case sensitive.

Procedure

1. From the App Catalog page, click the **Advanced Search** link. The Advance Search wizard opens.
2. Click one of the following options:
    - **Any**-if the apps must match at least one of the rules
    - **All**-if the apps must match all the rules

To create a rule that defines the search criteria, select one of the following options and select the appropriate associated action:

- AppConnect Enabled
- Average Rating
- Bundle ID
- Category
- Cost

- Custom Attributes
- Date added to the AppCatalog
- Date Modified
- Device Distribution
- Device Group Distribution
- Device type
- Group Distribution
- Minimum OS version
- Name
- OS Platform
- Provisioning Profile
- Size
- Source
- User Distribution
- User groups Name
- Version

4. (Optional) Click **+** to create additional rules.
5. Click **Search**. The list of apps matching the search criteria are displayed.

Loading the search queries

You can view the list of saved search queries.

Procedure

1. Click Advanced search and then click the folder icon. The list of the created search queries are displayed in the **Loaded Query** section and the following details are displayed:
   - **Query Name** - The name of the loaded query.
   - **Query Content** - Displays the content on the rules defining the search query.
   - **Actions** - Select the action to be performed on the query.
2. Click **Load Query** in the **Actions** column to view the list of apps matching the criteria defined in the loaded query.
3. Click **Delete** to delete a loaded query.

Exporting Apps to a CSV file

You can export the apps using the Export to CSV option from the App Catalog page.

Procedure

1. Go to Apps > App Catalogue.
2. Click **Export to CSV** to export the app list and related details to a CSV file.

> Only the apps listed in the selected space are included, with all paginated results compiled into a single file.

> Using filters or search results will export only the relevant apps.

3. A pop-up message appears with **Continue** and **Cancel** buttons stating that the export process has started, and a report will be available shortly.
4. Click **Continue** and wait for the request to complete before you submit another request.
5. A message appears stating that the **App Catalog - CSV report is finished** with **Download** and **Delete** buttons.
6. Click **Download** to download the report.
7. (Optional) Click **Delete** to delete the report.

> The **Export to CSV** option will be re-enabled only after either the **Download** or **Delete** option is selected.

> If there are multiple versions of an app, then one entry per app version is seen.

Related topics

- User Roles
- Deleting Apps from the App Catalogue
- Deploying app dependencies

8.2. Declarative Device Management (DDM) App Management

Overview

Declarative Device Management (DDM) App Management introduces support for Apple's declarative management framework for application deployment and lifecycle management on iOS and iPadOS devices. Instead of relying on continuous command delivery and periodic pulling, DDM enables devices to apply declarations locally and proactively report state changes.

With DDM, the server sends a declaration to the device only once. The device then applies the configuration, monitors its state, and reports status changes back to the server. This device-driven approach reduces server communication, improves scalability, and provides more timely status updates for application deployments.

DDM App Management currently focuses on core application management capabilities for supported Apple devices.

DDM App Management Workflow

In a DDM workflow, the server delivers the desired state to the device, and the device becomes responsible for maintaining and reporting that state.

When an application is assigned to a DDM-enabled device:

1. The server sends an application declaration to the device.
2. The device processes the declaration locally.
3. The device installs, updates, or maintains the application based on the assigned configuration.
4. The device continuously monitors application state.
5. Any installation status or state change is immediately reported back to the server.

This declarative model provides near real-time visibility into application deployment progress without requiring periodic status pulling.

Enable DDM App Management

DDM App Management is enabled through User Settings and is assigned to specific user groups.

To enable DDM App Management:

1. Go to **Users** > **User Settings**.
2. Under **Apple DDM Setting**, click **+Add** setting for specific user group. The **Apple DDM Setting** page opens.
3. Enter a name and toggle the **Enable DDM App Management** slider.
4. Click **Next**. The User Setting Distribution page opens.
5. Select the user group that will use DDM App Management.
6. Click **Done**.

After DDM is enabled for a user group, all supported applications assigned to users in that group are processed through DDM App Management. The DDM configuration is tenant-wide but applied through user-group assignments, enabling organizations to gradually roll out DDM to selected users or groups.

Supported enrollment methods

DDM App Management supports iOS / iPadOS devices enrolled using:

- iReg/ Managed Ivanti Go client
- Add Device Enrollment Profile
- Account driven Device Enrollment

Supported application types

DDM App Management supports the following application types:

- Public applications
- VPP applications (Only for Device Enrollment)
- iOS in-house applications.

The application assignment and deployment workflow remains largely unchanged from traditional N-MDM deployments. Existing application distribution processes continue to work while benefiting from DDM's enhanced status reporting capabilities.

8.2.1. DDM App Management Settings

In general, App Management includes the following settings:

- Prevent backup to iCloud
- Do not install app on newly enrolled devices
- Mobile
- DNS Proxy
- Managed app config
- Business apps – Apps@Work, Email+, etc.
- Per app VPN
- Network relay
- Webcontent filter
- Allow Appstore updates

In addition to the above listed settings, DDM App Management introduces several capabilities that are available only for DDM-managed devices.

App Version Pinning

App Version Pinning allows administrators to deploy and maintain a specific application version across DDM-managed devices.

When Version Pinning is enabled:

- Devices install the specified application version.
- Automatic upgrades to newer versions are prevented.
- Applications remain on the assigned version until a new version is explicitly selected by an administrator.

This capability enables tighter control over application version consistency and staged upgrade deployments.

Procedure

1. Go to Apps > App Catalogue.
2. Click an app from the displayed list. The **App Details** page opens.
3. Under the **App Configurations** tab, click **Apple App Settings**.
4. Click on any of the listed existing settings.
5. Click **Edit**.
6. Under the **Pin app version to a device** section, select the **Pin app version** option.
7. From the **Select app version** list, select the required app version.

> If the device has an existing version of the app, you cannot replace it with an older version.

8. Click **Update**.

Automated App Store Update Controls (Automatic App Update)

Administrators can configure how App Store updates are handled for managed applications. This capability provides greater control over application update behaviour and helps organizations align updates with internal validation and rollout processes.

Allow Downloads via Cellular

DDM introduces a dedicated setting to control application downloads and updates over cellular networks.

Procedure

1. Go to Apps > App Catalogue.
2. Click an app from the displayed list. The **App Details** page opens.
3. Under the **App Configurations** tab, click **Install on Device**.
4. Click on any of the listed existing settings.
5. Click **Edit**.
6. Under the **Allowed downloads over cellular** section, select one of the following options:
    - **Store Settings** – Default option. The device uses the settings for the corresponding store when downloading apps.
    - **Always On** – App download is allowed even if the device has no Wi-Fi connectivity.
    - **Always Off** – App download is not allowed if the device has no Wi-Fi connectivity.
7. Click **Update**.

Application Installation Workflow

The process for distributing applications remains similar to traditional N-MDM app management.

Administrators

- Assign apps
- Distribute apps
- Install apps

However, DDM changes how deployment status is communicated. Rather than relying on server pulling, devices report application state changes as soon as an action is completed. This provides more accurate and timely information about installation progress and deployment results.

Status Reporting and Monitoring

One of the primary benefits of DDM App Management is proactive status reporting.

With DDM:

- Devices monitor application state locally.
- Installation and update events are detected immediately.
- State changes are automatically reported to the server.
- Deployment information becomes available without waiting for scheduled polling intervals.

This provides administrators with faster visibility into:

- Application installation progress
- Successful installations

- Application update completion
- Application state changes
- Deployment failures

Real-time reporting improves troubleshooting and provides a more responsive application management experience.

Requirements

DDM App Management is supported only on:

- iOS 26 or later
- iPadOS 26 or later
- Managed Ivanti Go client 126 or later

Devices that do not meet these requirements continue to use traditional N-MDM app management.

> Once a device is processed via DDM app management, disabling or updating this policy distribution does not revert the device to MDM app management. To return the device to MDM app management, remove the policy assignment and re-register the device.

8.3. Apps@Work (iOS, Android, Windows, and macOS)

Apps@Work is an enterprise app storefront that facilitates the secure distribution of software and apps. Apps@work is available for iOS, Android, macOS and Windows devices. Apps@Work corporate appstore is integrated into Ivanti Go app and Mobile@Work clients for iOS, Android and macOS. For Windows devices it is a native standalone application. This section contains the following topics:

- iOS Apps@Work
- Android Apps@Work
- macOS Apps@Work
- Windows Apps@Work

iOS Apps@Work

The Apps@work native appstore is deployed automatically with the Go client. No action from the administrator is required. The Apps@work tab is displayed on the Go client task bar. End user can go to this tab to view and install their company approved apps. For more information, see iOS Apps@Work AppStore Features.

The iOS Apps@Work end user notifications for app updates are enabled by default. If you want to change the settings see the **Notifications** topic in Catalogue Settings.

Existing Customers with iOS Apps@Work Webclip

The customers who have the legacy iOS Apps@Work webclip deployed, will not get the Native Integrated AppCatalogue by default. If you would like to transition to the iOS Apps@Work Native catalog and remove the Apps@work webclip from the devices, perform the following steps:

Pushing the configurations

The administrator must push the App Catalog for Native Client configuration to the devices to make Apps@Work available in a Native Appstore experience from Go client application. For more information, see Working with Configurations.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Go to **Configurations** > Filter and select **Client Services**. All the client configurations are listed.
3. Select **App Catalog for Native Client**. The App Catalog for Native Client configuration page opens.
4. Click the **Edit Distribution** icon. The Edit Distribution page opens.
5. Select one of the following options:
    - **All Devices**
    - **No Devices** - if you do not want to distribute to any devices
    - **Custom** - lets you select Devices, Device Groups, Users, User Groups
6. After the configuration is distributed the user must upgrade the Go client version to 83 or above. Apps@Work tab is now visible in the Go app client.

The configuration cannot be pushed for devices that are registered using iReg because Go client is unavailable on the device. You must install the Go app client to get the native app catalog. For more information, see **Device Registration (iOS, macOS, and Android)**.

Remove iOS Apps@Work Webclip

For customers who have Apps@Work Webclip distributed to their devices and have already migrated to Apps@Work Native experience they can remove iOS Apps@Work webclip.

Procedure

1. Go to **Configurations**.
2. Filter the Configuration – **Apple App Catalog** .
3. Click **Edit**.
4. From **Distribution** select **Distribution to No Devices**.
5. Click **Save**.

Android Apps@Work

The Apps@work native appstore is deployed automatically with the MI Go client. No action from the administrator is required. The Apps@work tab is displayed on the Mi Go client task bar. End user can go to this tab to view and install their company approved apps. For more information, see **Admin - Android Enterprise**.

macOS Apps@Work

macOs Apps@work is integrated into the macOS Mobile@Work client. Once device has registered into Ivanti Neurons for MDM the client will switch and display as Apps@Work. For newly created tenants the Apple App Catalog Webclip configuration will not be pushed to macOS devices. If required the administrator can distribute the Apps@work Webclip configuration to macOS devices. For more information, see **Configuring macOS devices**.

Distributing macOS apps

- Ivanti supports macOS apps distribution via Apple MDM protocol and using the Mobile@Work app. Administrators can choose to use one or both of the following approaches:
  - Apple's MDM protocol - Administrators can upload only specific PKG formats (distribution format) as in-house apps and can also distribute apps from Mac App Store (Apple's Apps and Books licensing support is included). However, this approach does not allow administrators to distribute DMG and other PKG formats.
  - Mobile@Work for macOS app - As a way to distribute apps to users, administrators can use MobileIron Packager (MIP) app to convert any PKG, DMG or .app files to a MIP file. Upload the MIP file into Ivanti Neurons for MDM as an in-house app

You can download the utility from the **software downloads site**.

- Administrators can use Mobile@Work to distribute in-house apps that are in the DMG, PKG or .app format. For apps that are only available in the Mac App Store, administrators can continue to use Apple's native MDM capabilities, which includes Apple Apps and Book licences capabilities. For more information, see **Configuring macOS devices**.

Windows Apps@Work

Apps@Work is a stand alone native app that can be downloaded from the Microsoft Store or can be push directly from Ivanti Neurons for MDM. It enables use of Windows public and in-house apps on Windows 10+ devices in Ivanti Neurons for MDM. Apps@Work is installed silently on supported Windows 10+ devices.

For more information, see **App Configuration**.

Using Windows Apps@Work

Apps@Work enables use of Windows public and in-house apps on Windows 10 devices in Ivanti Neurons for MDM. Apps@Work is installed silently on supported Windows 10 devices.

Apps@Work Certificate Authentication

To use Certificate Authentication with Windows Apps@Work:

1. Go to **Admin > Windows > Apps@Work Certificate Authentication**.
2. Toggle the setting to **ON**.

> Toggle the setting to **OFF** enforces the use of username and password.

> SAML is not supported for Apps@Work for Windows.

To configure an app for Apps@Work:

1. Select a Windows app.
2. Click the **App Configuration** tab.
3. Click **Install on Device**.
   Windows In-house app configuration can be set to the silent install flag or install using Apps@Work. Public apps cannot be set to silent install.
4. Optionally, choose to display or hide apps in Apps@work catalogue.
   This option applies to in-house apps only.
5. Click the **Promotion** tab.

> Apps@Work currently does not support the banner promotion so the available options are **Featured** and **Not Featured**.
>
> Only the **Promotion** option is displayed for public apps.

8.4. iOS Apps@Work AppStore Features

The Apps@Work tab has the following features:

- Access Apps@Work tab from the Go application
- Search
- Installing an app - Button States
- Featured Applications and Banner
- Application Update Notification
- Settings-My Devices

Access Apps@Work tab from the Go application

Procedure

1. Log in to Go app from your iOS device.
2. Tap the **Apps@Work** icon. Two default tabs are available-All Apps and Categories.

3. Tap the **All Apps** tab. The All Apps tab lists all the apps in an alphabetical order.
4. Tap the **Categories** tab. The Categories tab displays only the categories that have any applications in it as follows:
    - Each category displays the number of applications present in it.
    - The MyApps row under the Categories tab is a list item that contains all the installed applications. The MyApps row will always be the first category and the rest of the categories are listed alphabetically.
    - When no applications are installed the MyApps list displays None.
    - When you click on a category, all the applications that are specific to the category are listed with the Install option. Click **Install** to install each application individually or you can click **Install All** to install all the applications in the category. You will be prompted to permit the installation for each application.

Search

Procedure

1. Log in to Go app from your iOS device.
2. Tap the **Apps@Work** icon.
3. Tap the search (lens) icon to search for the following:
    - **New Releases**-displays a list of newly released apps appears when no text is typed in the search bar

    - Type any text and the search field will dynamically predict and display the matching applications.
    - The search result count is displayed as a sub-heading
    - You can also tap the **Install** button to install an application without navigating to the details page.


Installing an app - Button States

Since the app installation requires the server to process the request and push the application to the device, the install button will not display the progress in real-time. The install button changes states from Install > Requested > Installed.

Procedure

1. Log in to Go app from your iOS device.
2. Tap the **Apps@Work** icon.
3. Tap **Install** and the status notifications appear as follows:
    - An alert message appears, for the first time, indicating that an installation is requested.
    - Tap the Requested button. An alert message appears.

    > The Installed status is not a button.



Featured Applications and Banner

The Featured tab is visible based on the configuration pushed by the administrator. The Featured tab is the default landing page when no updates are available.



Procedure

1. Log in to Go app from your iOS device.
2. Tap the **Apps@Work** icon.
3. Tap the **Featured** tab.
    - The Featured App Banner displays one application in the banner.
    - The Featured App contains a list of all the featured applications.



Application Update Notification

The end user receives a notification on the device when any application updates are available. The notification contains the number of applications that have updates available. When user clicks on the notification, Apps@Work opens.

Procedure

1. Log in to Go app from your iOS device. The Apps@Work icon displays the count of applications that have pending updates.
2. Tap the application update notification, you will be redirected to the All Apps tab in Apps@Work. The following indications are displayed:
    - The Updates Available sub-section under the All Apps tab displays the count of the applications that are available for update.
    - A red dot icon is displayed for every application that requires an update.



Settings-My Devices

Procedure

1. Log in to Go app from your iOS device.

2. Tap the **Settings** icon.
    - The My Devices tab is available under Settings.
    - My Devices is now listed as a line item under Authenticate.

8.5. iOS Go Advanced Features

Key-Value Pairs (KVPs) are simple application settings made up of a key (the name of the setting) and a value (the configuration you want to apply). In Ivanti Go for iOS, organizations use KVPs to enable or disable features and adjust app behavior without requiring an app update.

When Ivanti Go runs on organization managed iPhones or iPads, it reads these KVP settings at startup or during a check-in. The app applies the updates immediately, ensuring that configuration changes are delivered quickly, consistently, and to the correct users.

Using KVPs in Ivanti Go App configurations

KVPs for customizing violation messages are supported on Ivanti Go app. You can configure KVPs within the Ivanti Go app settings to customise application.

Procedure

1. Open the **Ivanti Go app** in your AppCatalog.
2. Select **Configurations**.
3. Click **Add** to create a new **Apple App Configuration**.
4. Add your KVPs manually:
    - In the **Key** column, enter the configuration key you want to customise.
    - In the **Value** column, enter the value you want enforced on devices.
5. (Optional) Upload an existing *.plist* file containing predefined KVPs you wish to apply.
6. **Save** the configuration.
7. The updated KVPs will be applied to devices during their next check-in.

Adding a plist to a specific iOS App (for Multiple Key-Value Pairs)

Administrators can configure multiple Key-Value Pairs (KVPs) for an iOS app using app serial numbers, bundle identifiers, version details, or other metadata. This can be done efficiently by uploading a .plist file through the Ivanti Neurons for MDM console.

Procedure

1. Go to **Apps**.
2. Open **App Catalogue**.
3. Select and open the **Specific iOS app** you want to configure.
4. Go to the App Configurations tab.
5. Select **Apple Managed App Configuration**.
6. Click the **+Add** button.
7. Enter a **Name** for your configuration.
8. Click **Use .plist**.
9. Select **Choose one of these options**.
10. Browse to your plist file, select it, and click **Open**. The system will automatically populate the configuration table with the key value pairs from the plist.

11. Choose the user group(s) or device group(s) that should receive the configuration.
12. Click **Distribute this App Config**.
13. Click **Save** to complete the process.

> The uploaded file must have a .plist extension. If you manually created the file (example, in a text editor), ensure that the extension is changed from *.txt* to *.plist* before uploading.

Launching Ivanti Go in Single App Mode during registration

This feature enables administrators to use key-value pairs during device registration to automatically launch the Ivanti Go for iOS in Single App Mode (SAM). When a device begins enrollment, the configured key-value pairs trigger Ivanti Go to open immediately. During this process, the user is presented with a message indicating:

Please wait while your device is being configured.

To activate this behavior, the Single App Mode configuration must be installed and explicitly targeted to the Ivanti Go for iOS before or during the registration workflow. Once enrollment is successfully completed, Single App Mode is automatically exited. The device is then released to the end user for normal operation, ensuring secure setup without restricting post registration use.

This capability supports Ivanti Mobile@Work environments, providing a secure registration flow for supervised iOS devices.

Setting up Zero Touch activation

To enable Zero Touch Activation for Ivanti Go, complete the following steps:

1. Set up a group that includes only devices where *Client Registered = No*.
2. Create a Single App Mode (SAM) configuration for the Ivanti Go application. Assign this configuration only to the device group created in *Step 1*.
3. Add the zero_touch_activation key value pair (KVP) to the Ivanti Go app configuration. Target the same device group used in the previous steps.

configuration.

Key	Value	Type	Description
zero_touch_activation	True	Boolean	When the value is set to true, the Ivanti Go app recognizes that it is running in Single App Mode (SAM) through the SAM configuration. The SAM configuration launches the Ivanti Go app, while this value acts as an additional setting that enables the app to function correctly in SAM mode. After successful enrollment, the device exits Single App Mode and becomes available to the end user for normal use.

Enabling the Return to Service Button in Ivanti Go (iOS 18+)

The **Return to Service** feature allows the device to automatically re-enroll once data is wiped, reducing the need to manually re-enroll the device after a wipe.

Administrators can enable or disable the Return to Service button using a configurable Key Value Pair (KVP). When the KVP is deployed to Ivanti Go as part of the app configuration:

- The Return to Service option becomes visible to the end user.
- The user can initiate the reset process directly from Ivanti Go.
- The device performs an Apple managed Return to Service reset.
- Management profiles and required apps remain intact.
- The device completes its re-provisioning flow and becomes ready for reuse.

This feature is supported on Ivanti Go for iOS, iOS 18 and later devices enrolled in DEP mode.

configuration.

Add the following KVP to the Ivanti Go managed app configuration in Ivanti Neurons for MDM:

Key	Value	Description
ReturnToServiceEnabled	true	Enables the **Return to Service** button in Ivanti Go. When set to false or omitted, the feature remains hidden.

Disabling screenshot protection on the SAML authentication screen

The Ivanti Go for iOS include built in screenshot protection to enhance security during device registration. By default, the registration with SAML authentication screens block:

- Screenshots
- Screen recordings
- Screen sharing

This protection ensures that sensitive authentication data - such as usernames, passwords, and SAML based login content cannot be captured or shared without authorization.

Administrators can disable screenshot protection on managed devices using a KVP configuration. When this configuration is applied, the Ivanti Go app will allow screenshots and recordings only on the SAML Authentication screen, while maintaining all other security mechanisms throughout the app.

configuration.

To disable screenshot protection for the SAML authentication screen, apply the following KVP to the Ivanti Go app configuration in your MDM:

Key	Value	Description
SCREENSHOT_PROTECTION_DISABLED	True	Disables screenshot, screen recording, and screen sharing protection on the SAML Authentication screen. When omitted or set to False, protection remains enabled by default.

KVPs for customizing policy violation messages

These KVPs enable administrators to customise the messages sent to end users when Policy Violations are detected.

These KVPs for customization describes the KVPs and violation types available to administrators to customise Ivanti Go for iOS app behavior. These KVPs define app behavior such as providing detailed notifications to device users and export contacts from Ivanti Go for iOS.

The violation types are not mutually exclusive. If there are a set of violations, then a list of messages will be shown in the Ivanti Go for iOS.

Key Value Pairs (KVP)	Default Messages
compliance.message.COMPROMISED	• Your device has been compromised because it has been jailbroken. Please properly return your device to a non-jailbroken state or contact your administrator for help resolving this issue.
compliance.message.DATA_PROTECTION_DISABLED	• Corporate access has been disabled for data protection. Please contact your administrator for help resolving this issue.
compliance.message.OUT_OF_ CONTACT	• Your iOS device is out of contact. Please contact your administrator for help resolving this issue.
compliance.message.APPS	• Your device is missing apps that are required and/or it has apps that aren't allowed. Please add/remove necessary apps or contact your administrator for help resolving this issue.
compliance.message.MDM_DISABLED	• Your device is out of compliance because MDM capability has been deactivated. Please re-enroll your device, or contact your administrator for help resolving this issue.
compliance.message.ROAMING	
compliance.message.generic	• Corporate access has been disabled for an unspecified reason. Please contact your administrator for help resolving this issue.
compliance.message.header	Your device is out of compliance for the following reason(s): When the violation type is CUSTOM or CUSTOM_NOTIFY_ONLY, the system displays standalone messages without a header.
compliance.message.CUSTOM	An action may be required on your device. Please contact your admin as needed.
compliance.message.CUSTOM_NOTIFY_ONLY	Your device is out of compliance, and a notification has been sent. Please refer to the notifications tab or your email for details.

If the violation types list does not include any violation with a mapped message, but it includes at least one violation without a mapped message, then display the default message:

- Corporate access has been disabled for an unspecified reason. Please contact your administrator for help resolving this issue.

If the messages list contains at least one violation message, display the following header above the list:
Your device is out of compliance for the following reason(s):

If you do not want to change a default message, do not include a key-value pair (KVP) for it. Only define KVPs for the messages you intend to modify.

Configure default browser and email clients using Managed App Configuration

Key Value Pairs (KVP) enable administrators to configure which browser and email client **Ivanti Go** uses when opening web links and composing emails via Managed App Configuration.

As an administrator, you can use Managed App Configuration KVPs to control how links are handled within the **Support** tab:

Key	Value	Type	Description
default_browser	safari, edge, chrome, firefox, brave, opera, webatwork, duckduckgo	String	Browser Ivanti Go uses to open web links in the Support tab. http/https links are redirected to the configured browser's scheme. **Default if not configured**: system default browser.
Allow_browser_fallback	true, false	Boolean	**Behavior when default browser is not installed**: **True**: Falls back to default system browser. **False**: Link not opened, user sees "<Browser> not installed" alert. **Default if not configured**: True
restrict_log_sharing_to_email	true, false	Boolean	Whether log/support sharing is restricted to email only (using default_email). Auto-attaching logs works with Email+ and Native mail Works with **allow_email_fallback**. **True**: sharing to email only. **False**: standard sharing options available. **Default if not configured**: false.
default_email	nativemail, outlook, gmail, yahoo, citrixmail.emailplus, spark, protonmail	String	Email Client Ivanti Go uses to compose mails from mailto links in Support tab. mailto is transformed into the client's composing URL **Default if not configured**: Default mail application . Dual role in link resolution and log sharing when default_email client is not installed.
Allow_email_fallback	True, False	Boolean	**Behavior when default email is not installed**. **True**: Email composition falls back to the default mail application if the configured email client is not installed, and log sharing can use an alternate delivery method. **False**: Email composition is blocked, and users see a "**Not Installed**" alert if the configured email client is unavailable. Log-sharing restrictions are enforced with no fallback option. **Default if not configured**: true. (fallback behavior is enabled)

8.6. Viewing App Details

You can drill down from the App Catalog to app details about any of the apps in the catalog. In the app details page, the details on the apps such as Display Version (for example, 1.5.0),Bundle Version (for example, 1.5.0.42) and Minimum OS Version required (for example, 5.0 for Android) are displayed.

Apps that do not meet the version specified in the Minimum OS Version Required field are not displayed in Apps@Work catalog. Therefore, such apps are not available to be distributed to the devices. The Minimum OS Version Required field is also displayed as part of the **Audit Trails** for the apps.

Procedure

1. Click **Apps**.
2. Click **App Catalogue**.
3. Select the app.

The App Details window appears.

> For iOS in-house apps, you can check the **Provisioning Profile Expiration Date** on the app details page.

> App Information shows **Allow app installation on M1 devices upon distribution** as an option for all iOS and iPadOS VPP apps. The administrator must enable the option **Allow app installation on M1 devices upon distribution** for only iOS or iPad VPP applications that can be installed on M1 macOS device. Only after enabling this option, the administrator can see M1 macOS devices during application installation. The Managed app configuration is supported for iOS VPP applications on M1 Mac devices.

> For iOS and macOS App Store apps, including Business-to-Business, **Sync new version** checks and synchronise app updates from the App Store. The updated app version displays within 12 to 24 hours based on the app sync schedule.

> A toggle button for **Prerequisite Apps** is added in Device details. Administrators can select this option and add apps as prerequisites of a main app.

Once an app is distributed to different devices, the app distribution status can be viewed under the **Devices Summary** tab. The Device Summary tab also has information about the number of eligible devices, number of devices on which the app got installed, number of devices on which the app installation is pending, and number of devices on which the app installation failed. The device count in these boxes is based on devices that have Required App Installation, so admins can track the initial deployment on mandatory apps.

For general application count (including user installed applications), please use the App Inventory search.

> Apps excluded from the device have Pending distribution state.

The following table lists the reasons for app installation failure on iOS / OSX apps:

Reason	Description
AppAlreadyInstalled	"App Already Installed."
AppStoreDisabled	"The app store is disabled."
CouldNotVerifyAppID	"Could not verify the App ID."
Failed	"The app installation has failed with unknown error."
ManagedButUninstalled	"The app is managed, but has been removed by the user. When the app is installed again (even by the user), it will be managed once again."
ManagementRejected	"The user declined the conversion of an unmanaged app to a managed app."
NotAnApp	"The InstallApplication command is rejected due to an invalid application identifier which resolves to an asset other than an app."
NotSupported	"The app is not supported."
Other	"Reason for newly added errors."
PurchaseMethodNotSupported	"For iOS 7 and later, the app can't be installed due to an invalid purchase method (applicable only to VPP apps)."
UserInstalledApp	"The user has installed the app before the managed app installation could take place."
UserRejected	"The user rejected the offer to install the app."
UpdateRejected	"The user rejected the offer to update the app."

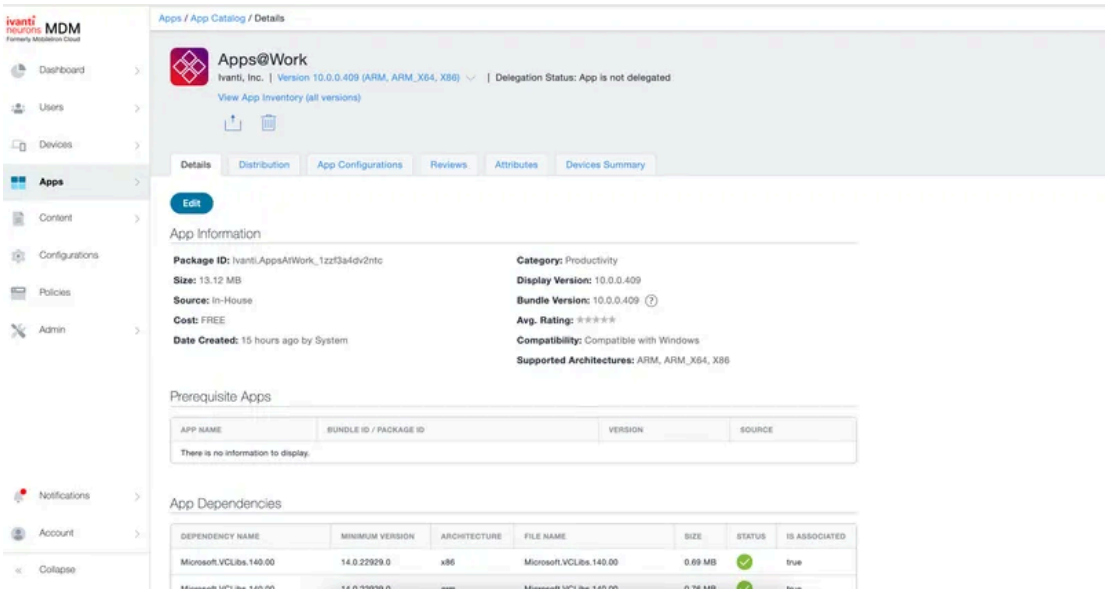
The following table lists the reasons for app installation failure on Android apps:

Reason	Description
USER_INSTALLED	"Already installed on device (outside of MDM)."
UNSUPPORTED	"Not supported"
USER_REJECTED_INSTALL	"User rejected the install of the application."
ERROR_INSTALL	"Error detected when trying to install; failed."
UNRECOGNISED	"Item is not found or is no longer tracked (for example, error / uninstalled from device and removed from tracking)."
UNSUPPORTED_INSTALL	"Updated for 3.0 Android client/22.0.0 server: specific status to track install vs uninstall is necessary."
HIDDEN	"During quarantine, the HIDDEN/UNINSTALLED status will be sent. Unquarantine should revert it back to installed."
OTHER	"Reason for newly added errors."

> For Windows devices, if the app is set to install silently in the App Configurations, then the Devices Summary displays the number of eligible, installed, pending, or failed devices for the app.

Viewing app inventory information from app details page

To view app inventory information, click the **View App Inventory (all versions)** to view in **Devices > App Inventory** a filtered list by bundle ID of that app.



8.7. App Configuration

This section contains the following topics:

- Licensing for app features
- Configuration steps common to multiple apps
- Hide and Suspend Apps (Android only)
- Configuring Network Relay
- Configuring Cellular 5G Slicing
- Distributing Application using Web Content Filter Configuration
- Distributing Application using DNS Proxy
- Clearing App Cache for Android Enterprise Devices

App configuration enables you to customise the installation, promotion, and distribution of each app you deploy to your users' devices. The apps can be your own in-house apps, apps from a public store, or Ivanti Neurons for MDM apps. You have the flexibility to deploy the apps to many different users and groups with unique names and configurations specifically tailored to each recipient. The number of in-house application versions is limited to 100. If that number is exceeded, the Ivanti Neurons for MDM system purges the oldest versions of the application. The status of the application upload and purge is listed and is visible from the Audit Trails page.

> When you change the values for the app configuration of an app in the app catalog or in the managed app configuration profile, one or two device check-ins are necessary for the device to receive the new configuration values.

Licensing for app features

> The following features require additional licensing:

- Silent app install/uninstall: Silver licence
- Per-app configuration: Gold licence
- AppConnect custom configuration: Gold licence

Multiple application packages require good group management as future device types could not be defined by the Windows OS. In such a case the only way of installing a proper version of the app is for the admin to use the correct group to the correct application.

Configuration steps common to multiple apps

Do these steps first and then proceed with configuration steps for each app you want to deploy. You can design multiple configurations of the same app and give each configuration a unique name. Each configuration can have its own distribution and promotion levels to fit your deployment strategy. The number of in-house application versions is limited to 100. If that number is exceeded, the Ivanti Neurons for MDM system purges the oldest versions of the application. The status of the application upload and purge is listed and is visible from the Audit Trails page. You can deploy an application to a maximum of 100 Users, Users Group, Device or Device Group at once. You can select an app to add to the App catalog. Ivanti Neurons for MDM has an asynchronous process to Send Install/Update Request command for iOS apps. When you use the Send Install/Update Request command, the Ivanti Neurons for MDM administrative portal displays a message that the:

- process will continue to run in the background

- process is complete
- status whether the process is successful or if there are any errors

Procedure

1. Go to **Apps > Apps Catalogue** and click **+Add**.
2. Use the pull-down menu to select either the App Store, Google Play or your In-House app store and choose an app to add to the catalog.
   Depending on your licensing agreement, you might also have apps available to add to your catalog.
3. Optionally, edit the Category of the app.
4. Optionally, add a brief description of the app in the **Description** field.
5. Click **Next**.
6. Choose a distribution level for this configuration of the app:
   - **To everyone** - The app is added to all the user compatible devices.
   - **To no one** - The app is staged for distribution at a later date.
   - **Custom Distribution** - Select any of the following options:
     - **User/User Groups** - The app is distributed to only the users or user groups you choose.
       Click the **Users** tab to select the user(s).
       Click the **User Groups** tab to select the user group(s).
     - **Device/Device Groups** - The app is distributed to only the devices or device groups you choose.
       Click the **Devices** tab to select the device(s).
       Click the **Device Groups** tab to select the device group(s).
7. Click **Next**.

Configuring installation options

You can select the installation configuration options.

Procedure

1. Click **Install Application configuration settings** or click the **+** icon to add another configuration to view the **Configuration Setup** page.
2. Enter a name for the configuration in the **Name** field.
3. Optionally, enter a brief description of the installation configuration in the **Description** field.
4. Select the **Device Installation Configurations** option.
5. Select one of the following options:
   - **Require installation on device**
   - **Install only once at device registration**
6. Select the **Do not require a specific app version** option to avoid downgrading an already installed app to a lower version. This option is available only for modern apps.
7. Select the following options:
   - **Silently install on Samsung Knox workspace and Zebra devices** (Android Only)
   - **Do not show app in end user App Catalog**.

- **Do not install app on newly enrolled devices**: Existing devices will not be impacted and will still display the app in the device app catalog.
  - For any newly enrolled devices in this distribution, the app will not be listed or pushed.
  - If the admin triggers a send install/update command, the command will be sent to the device.
- **Defer App Update by**: You can use this option to delay the new app version installation. This setting delays the automatic installation of new app versions based on the configured duration.
- **App Update Mode** (supported for AMAPI devices as well). (Android Only)
  Use this option to update an app to the latest version using one of the following three modes:
  - **Default**: This mode is selected once you select the App Update Mode option. In this mode, the update happens within 24 hours from the time of app availability.
  - **Postpone for 90 days**: If you select this update mode, you can postpone the app updates for 90 days. After 90 days, the apps are updated automatically based on other settings made in Managed Google Play configuration.
  - **High Priority**: If you select this update mode, and the user's device is online, the app gets updated immediately after it is available on the Google Play Store.
- **Set App Install Priority** - see the Configuring app priority topic for more details

> On Android devices, the app updates are allowed using the Auto Update option even without selecting the Silent Install option. Administrator can control app updates on apps which are not mandatory or the apps which are self-installed by the user.

- **Do Not Update While App is in Use**: Select this option to prevent an application from being updated while the user is actively using the application. When this option is enabled:
  - Application updates are deferred while the application is running in the foreground.
  - User can continue using the application without interruption.
  - Pending update is installed automatically when the application is closed or moved to the background.

Remove Applications When Distribution Is Removed (Android)
For managed Google Play applications, Ivanti Neurons for MDM automatically removes applications from Android devices when the application is no longer assigned to the device.
Applications are removed in the following scenarios:

- The application distribution is changed to To no one.
- The application is deleted from the App Catalogue.
- The device is excluded from the application distribution.

You may encounter additional configuration options, depending on the chosen app. These options may include the ability to add multiple Key and Value pairs. In such cases, click **+ Add** to enter Key and Value pairs. For more information, see **Adding an app from a public store** in App Catalogue.

9. (macOS 11+) Select the options to install and configure the apps as managed apps:
   - **Install as Managed App**
   - **Convert to as Managed App**

     > In macOS 12.0+, Managed App support is available on user enrolled devices.

Hide and Suspend Apps (Android only)

For Android devices in the following modes, **work profile**, **fully managed device**, **fully managed device with work profile**, and **work profile on company-owned device**, you can now hide or suspend apps after installation.

Procedure

	1.	**Install one or more apps on the device for which you want to apply the Hide or Suspend action.**
	2.	**Create an App Control Configuration and add the managed apps to Hide or Suspend list.**
	3.	**Apply the changes to the device.**

If an app is present in both Hide and Suspend lists, then the app will be hidden because the Hide list will be prioritized.

Configuring app priority

You can define the order in which apps are received on the device when it is first registered (specifically, within the first 20 minutes after registration date and time) and required apps are being pushed to install. You can prioritise downloading of specific apps before other apps. For example, prioritising the download of Tunnel and Email apps before other non-critical apps. This feature is applicable for public and private apps. Prerequisite apps are pushed before dependent apps.

This feature is supported on iOS (except AppStation for iOS), Android (except Android for Enterprise), macOS (in-house PKG apps and Apple Apps and Books apps), and Windows devices.

This feature is available for new registration devices. By default, all apps are set to Medium priority. During this process, the user can select to manually install any app in the catalogue even though that app will compete for resources to install and may queue before high priority apps.

In the case of Windows apps, the Bridge app has the highest priority than other apps.

See the previous section, "Configuring installation options" for the procedure to set the priority of an app using the **Set App Install Priority** option. You can set High, Medium, or Low priority for an app. Apps with same priority will be installed in no particular order. App priority is not used during app updates, when the user has already installed the app.

Selecting Apple Application Management Configuration settings

These settings will apply to this app only and will override any global settings selected in the **Apps > Catalog Settings**. To select **Apple App Management** settings.

Procedure

1. Click **Apple Apps settings** or click the **+** icon to add another configuration to view the **Configuration Setup** page.
2. Enter a name for the configuration in the **Name** field.
3. Enter a brief description of the configuration in the **Description** field.
4. Select or deselect one or more of the following options from the **Apple Management Settings**:

- **Prevent backup to iCloud and iTunes.**
- **Remove apps on un-enrolment**
- (iOS 14.0+) **Allow removal and offloading of this app** - You can deselect this option to prevent a user from removing and offloading a managed app.
- (Optional) Add an **Apple Managed App Configuration**

5. Click **Update**.

Selecting App Promotion levels

You can set the level of promotion for the app.

Procedure

1. Click **Promotion distribution configuration settings** or click the **+** icon to add another configuration to view the **Promotion configuration** page.
2. Click **Edit**.
3. Enter a name for promotion distribution configuration settings in the **Name** field.
4. Optionally, enter a brief description of the configuration in the **Description** field.
5. Select the level of promotion you want the app to receive, **Not Featured**, **Featured List**, or use **Feature Banner**. If **Not Featured** is selected the app will not be listed.
6. If you select Featured Banner specify the following details:
    1. **Title** - Specify the application title
    2. **Description** - Specify the application detail
    3. **Banner style** - Select a banner colour
7. Click **+ Add Description** to enter a brief description of the configuration.
8. Optionally, change the distribution of the configuration.
9. Click **Done** to save the app configuration.

Configuring AppTunnel traffic rules

Use the AppTunnel configuration to define traffic rules to allow access to services using Sentry.

For information about adding an AppTunnel configuration, see "Adding an AppTunnel configuration" in the *AppConnect Guide for Ivanti Neurons for MDM*.

Configuring Managed app

Procedure

1. Click the **+** icon to open the configuration page.
2. Click **+ Add Description** to enter a brief description of the configuration.
3. Click **+ Add** to enter a Key and Value.
4. Choose a distribution level.
5. Click **Next**.

Configuring a VPN for each app using Per App VPN

Procedure

1. Click the **+** icon to open the configuration page.
2. Enter a name for the VPN for this app in the **Name** field.
3. Click **+ Add Description** to enter a brief description of the configuration.
4. Click the **Enable Per-App VPN for this app** option and select an available Per-App VPN configuration.
5. (Optional) For macOS apps, enter **Designated Requirement** string in the format, identifier "\%s\". For example, identifier "com.google.Chrome". Use this field to enable a multiple package macOS app to use a Per-App VPN like Tunnel.
6. Choose how to **Distribute this App Config**.
7. Click **Next**.

Using Apple Managed App Configuration

Using the Apple Managed App Configuration, specific settings can be configured for the installed managed app. An application might have some configuration parameters implemented or restricted by the developer. For applications with such restrictions your configuration options might be limited. You can configure Apple managed apps.

Procedure

1. Go to **Apps > App Catalogue**.
2. Select an app.
3. Click the **App Configurations** tab.
4. Click **Apple Managed App Configuration** or click the **+** button.
   In the Apple Managed App Configuration there are some default configuration settings in place.
5. Click **Add** to add another configuration, if needed. Optionally, click the name of the configuration to edit the configuration.
6. Under **Configuration Source** select any of the **Source Type** options

- **AppConfig Community** - This option is available only for those apps that have an app configuration specification available in the community repository. If this option is available, it is selected by default.
- **Use .xml spec** - Select this option to upload the schema for the app to push a particular version of app configuration. Click **Choose File** to upload the .xml file. Ensure that the .xml file contains the bundle ID and the version. An error message will be displayed if the bundle ID in the file does not match with the bundle ID of the app.
- **None** - Select this option if you do not want to apply any schema for the app. This option is selected by default if the **AppConfig Community** option is not available.
  The uploaded .xml file is displayed in the **Configuration Source** section. Click the Delete icon to delete the uploaded .xml file.

7. In the **Apple Managed App Settings**, you can set the configuration options to enter key value pairs.

- Click **Add** to add the key value pairs to the managed app configuration to retrieve the registration name identity by Go client during iReg or Apple Device Enrollment.
  You can select the data types (String, Integer, Boolean, Long Float, Double, Date, String Array, Integer Array, Double Array, Float Array, Long Array) for the key value pairs.

> Add the following key value pairs to the managed app configuration to retrieve the registration name identity by Go client during iReg or Apple Device Enrollment:

Key	Value	Type
registration.username	$	STRING
registration.token	$	STRING
registration.token.expirationSeconds	$	STRING
registration.url	$	STRING

Add the following key value pairs to the managed app configuration to retrieve the registration name identity by mac agent (Mobile@Work) during iReg or Apple Device Enrollment:

Key	Value	Type
ClientRegistrationUrl	$	STRING
Token	$	STRING
TokenExpiresAt	$	STRING

If the end user terminates the Ivanti Go application, click **Edit** to set the application to do one of the following:

Key	Value	Type
To display default notification use the following values:		
enableAppTerminationNotification	True/False OR 1/0	Boolean OR String
To Display a custom notification use the following values:		
appTerminationNotificationMessage	Custom notification	String
enableAppTerminationNotification	True/False OR 1/0	Boolean OR String

- **Use .plist** - .plist files contain multiple key value pairs to be uploaded in bulk. Click **Choose File** to upload the .plist file. The validated plist data will be displayed in the **Apple Managed App Settings** table.

plists with nested dictionaries are invalid.

8. Click **Update** to save your entries.

Configuring Network Relay

To make your app's network traffic more private and secure without connecting to VPN. For more information see, Network Relay Configuration.

1. Click the **Network Relay + icon** to open the configuration page.
2. Enter a name for the **Network Relay** for this app in the Name field.

3. Click + **Add Description** to enter a brief description of the configuration.
4. Click the **Enable Network Relay** for this app option and select an available **Network Relay configuration**.
5. Choose how to **Distribute** this App Config.
6. Click **Next**.

Configuring Cellular 5G Slicing

Cellular 5G network slicing support allows individual managed apps (for all iOS apps) to be assigned to a network slice which may provide specific network capabilities and characteristics to optimise the app experience. The assignment is done using the new **CellularSliceUUID** app attribute in either the MDM app installation command or declarative app configuration. The string value of the network slice to put into the key needs to be provided by the supporting carrier.

> 5G network slicing will not be used if either the specific app or the entire device is configured to use a VPN.

ProcedureProcedure

1. Go to **Apps > Apps Catalog > App Configurations > Cellular 5G Slicing** and click **Add**.
2. Under the **Configuration Setup** section, update the following fields:
   - Name
   - Select the **Enable 5G network Slicing** option
   - Choose the **DNN** or **App Category** (as per the network provider)
3. Choose a distribution level for this configuration of the app:
4. Click **Save**.

Distributing Application using Web Content Filter Configuration

You can use the Web Content Filter configuration to distribute an application instead of a DNS proxy server. After you create the Web Content Filter configuration, you can add the configuration to an application for distribution. For more information about Web Content Filter configuration, see Web Content Filter.

Procedure

1. Go to Apps > App Catalogue.
2. Select an app.
3. Click **Next**.
4. Select the delegation option and click **Next**.
5. Select the distribution options and click **Next**.
6. Select **Web Content Filter configuration** and click the **+** icon.
7. Specify the **Name**.
8. Select the **Enable Web Content Filter for this app** checkbox.
9. Select the Web Content Filter from the drop-down menu.
10. Choose a distribution level for this configuration of the app:
    1. **To everyone** - The app is added to all the user compatible devices.
    2. **To no one** - The app is staged for distribution at a later date.

3. **Custom Distribution** - Select any of the following options:
    - **User/User Groups** - The app is distributed to only the users or user groups you choose.
      Click the **Users** tab to select the user(s).
      Click the **User Groups** tab to select the user group(s).
    - **Device/Device Groups** - The app is distributed to only the devices or device groups you choose.
      Click the **Devices** tab to select the device(s).
      Click the **Device Groups** tab to select the device group(s).

11. Click **Next**.
12. Click **Done**. The selected app is distributed to the specific users through the Web Content Filter configuration.

Distributing Application using DNS Proxy

You can use the DNS Proxy configuration to distribute an application. After you create the DNS Proxy configuration, you can add the configuration to an application for distribution. For more information about DNS Proxy Configuration, see **Creating DNS Proxy Configuration**.

Procedure

1. Go to Apps > App Catalogue.
2. Select an app.
3. Click **Next**.
4. Select the delegation option and click **Next**.
5. Select the distribution options and click **Next**.
6. Select **DNS Proxy Configuration** and click the **+** icon.
7. Specify the **Name**.
8. Select the **Enable DNS Proxy for this app** checkbox.
9. Select the DNS proxy from the drop-down menu.
10. Choose a distribution level for this configuration of the app:
    1. **To everyone** - The app is added to all the user compatible devices.
    2. **To no one** - The app is staged for distribution at a later date.
    3. **Custom Distribution** - Select any of the following options:
        - **User/User Groups** - The app is distributed to only the users or user groups you choose.
          Click the **Users** tab to select the user(s).
          Click the **User Groups** tab to select the user group(s).
        - **Device/Device Groups** - The app is distributed to only the devices or device groups you choose.
          Click the **Devices** tab to select the device(s).
          Click the **Device Groups** tab to select the device group(s).
11. Click **Next**.
12. Click **Done**. The selected app is distributed to the specific users through the DNS Proxy configuration.

Cloning App Configuration Settings

You can clone the Configuration Settings of a Managed app so that the same settings can be applied on other devices. You can even rename and make some changes to the cloned settings.

Android

You can clone Configuration Settings on Android devices.

Procedure

1. Go to **Apps > App Catalogue**.
2. Select an app from which you want to clone the configuration settings.
3. Click **App Configurations**.
4. Under the **App Configurations Summary** section, you will find the list of configurations (**Managed Configurations for Android**, **Install on Device**, **Promotion**, **Delegated Device Permissions**, and **Google Play Release**) available for Android devices.
5. Click on any of the available configurations.
6. Under **Actions**, click **Clone** to begin the cloning process.
7. By default, the cloned configuration name will be <Copy of the Cloned Configuration name>. However, you can modify the name by entering a name of your choice in the **Name** box.
8. (Optional) Enter some text about the cloned setting in the **Description** box.
9. Click **Continue**.

A confirmation window appears indicating that cloning the app configuration settings is complete. You can view the cloned version under the App Configurations Summary and within the cloned app.

iOS

You can clone Managed app Configuration Settings on iOS devices.

Procedure

1. Go to **Apps > App Catalogue**.
2. Select an app from which you want to clone the configuration settings.
3. Click **App Configurations**.
4. Under the **App Configurations Summary** section, you will find the list of configurations (**Install on Device**, **Apple App Settings**, **Promotion**, **AppConnect Custom Configuration**, **App Tunnel**, **Apple Managed App Configuration**,and **Per App VPN**) available for iOS devices.
5. Click on the required configuration that you want to clone.
6. Under **Actions**, click **Clone** to begin the cloning process.
7. By default, the cloned configuration name will be <Copy of the Cloned Configuration name>. However, you can modify the name by entering a name of your choice in the **Name** box.
8. (Optional) Enter some text about the cloned setting in the **Description** box.
9. Select a configuration source from the **Source Type** list.
10. Under the **Apple Managed App Settings** section, enter **Key**, **Value**, and select **Type** from the list.
    For information about the **Key**, **Value**, and **Type**, see **Using Apple Managed App Configuration**.
11. Click **Continue**.
    A confirmation window appears indicating that cloning the app configuration settings is complete. You can view the cloned

version in the **Apple Managed App Configuration** section.

Windows

You can clone App Configuration Settings on Windows devices:

Procedure

1. Go to **Apps > App Catalogue**.
2. Select an app from which you want to clone the configuration settings.
3. Click **App Configurations**.
4. Under the **App Configurations Summary** section, you will find the **Install on Device** and **Promotion** configurations.
5. Click on the required configuration that you want to clone.
6. Under **Actions**, click **Clone** to begin the cloning process.
7. By default, the cloned configuration name will be <Copy of the Cloned Configuration name>. However, you can modify the name by entering a name of your choice in the **Name** box.
8. (Optional) Enter some text about the cloned setting in the **Description** box.
9. Click **Continue**.

A confirmation window appears indicating that cloning the app configuration settings is complete. You can view the cloned version under the App Configurations Summary and within the cloned app.

Choosing Windows 10 apps for your in-house catalogue

Choose the apps to add to your in-house app catalogue. The in-house, Microsoft Store, and Microsoft for Business apps are supported for Windows 10. Windows 10 enforces compliance directly on the device based on the apps you choose to allow or disallow.

> The Windows 10 check-in interval is once every 60 minutes by default. You may want to perform a forced device check-in to get an update of the device and app status.

These actions are supported:

- Uploading new apps
- Silent installation
- Installing manually from Apps@Work
- Adding a new version of the app
- Deleting an app

These formats are supported:

- APPX
- APPXBUNDLE
- MSI wrapped Win32 - pre-bundled Win32 app
- MSIX (supported on RS5 and above Windows 10 devices)
- .EXE (using bridge)

The **Ivanti Neurons Agent** app is available on the **App Catalog** for **Windows** devices. The admin can deploy the **Ivanti Neurons Agent** app as an in-house app and this app can be distributed accordingly on the Windows devices.

Configure Windows 10 apps

Procedure

1. Click **Devices** on the main navigation bar.
2. Select a Windows 10 device that you have enrolled in Ivanti Neurons for MDM.
3. Click **Apps > App Catalog**.
4. Select an app.
5. Use the **Actions** pulldown menu to add the app or delete the app from your catalog.
   Optionally add a new version of the app.
   - Click the **Actions** pulldown menu.
   - Select **Add New Version**.
   - Go to the catalogue and select a new version of the app.
   - Click **Update and Save** to view the App information screen.
6. Use the **Version** pulldown menu to choose which version to use.
7. Click **Edit** to begin making changes to the details.
   - Edit the **Category** if needed.
   - Enter a **Description** if needed.
   - Add screenshots if needed.
8. Click **Save**.
9. Click the **Distribution** tab and click **Edit** to begin making changes to the distribution level.
10. Click **Save**.
11. Click the **App Configurations** tab to view a summary of the current configuration.
12. Enter a description of the app if needed.
13. Click **Install on Device** in the App Configurations summary page.
    Silent installation is the default and cannot be changed.
14. Click **Promotion** in the left navigation pane then click **Promotion distribution configuration settings** to change the promotion level.
    - Click **Edit** to make changes to the promotion level settings.
    - Enter a name for the configuration.
    - Enter a description for the configuration.
    - Select a promotion level.
    - Click **Update** to save your changes.
15. Click the **Reviews** tab to view information on reviews.
    Export the review data to a spreadsheet if needed.

Editing Windows 10 app configuration settings

Procedure

1. Click **Policies > Configuration**.
2. Click **+Add**.
3. Select **Windows App Control** to view the **Create Windows App Control Configuration** screen.
4. Enter a **Name** and **Description** for the configuration.
5. Define the app type as:
    - Allowed (Allowlisted) - Only these apps are allowed. These apps are installed silently if not already present on the device.
    - Disallowed (Blockedlisted) - If present on the device, these apps will be blocked if launched.
6. Specify the Rule definitions for the App Type and App Identifier.
7. Click **Lookup Apps** to view the **Search Windows 10 Apps** screen.
8. Enter the name of the app to search the Windows Store.
9. Select the app from the choices displayed to add it to the App Identifier.
10. Optionally use the App Type pulldown menu to set a path define in the App Identifier to allow or disallow apps using the specified path or block all apps installed in that path.
    App Type **Publisher/PFN Equals** applies to Windows 10+ devices and supports PFN. **EXE/Win32 Equals**.
11. Click **Next**.
12. Select a distribution level.
    - **All Devices**.
    - **No Devices**.
    - **Custom** - to enter the users or groups to receive the app.
13. Click **Done**.
14. You can edit the Rule definitions to select an App Type and specify an App Identifier.
    - Click the **Actions** pulldown menu.
    - Select **Add New Version**.
    - Select a new version of the app.
    - Click **Update and Save** to view the **App information** screen.

Configuring Reboot device after install option for Windows

You can configure a device to reboot after an app installation using the **Reboot device after install** option.

Procedure

1. Go to **Apps > App Catalogue**.
2. Select any Windows-specific app from the list.
3. Go to **App Configurations > Install on device > Install Application configuration setting**.
4. Click **Edit** and set the **Reboot device after install** option to ON.
5. Select one of the following schedule options at which you want to reboot the device:

Setting	What To Do
Right after Installation	Select this option to reboot the device soon after you install the application.
At specific time during the day	Select this option to reboot the device at a specific time of the day after you install the application.
After few mins	Select this option to reboot the device after **15**, **30**, **60**, or **120** minutes after you install the application.

6. Click **Update**.

The device will be rebooted at the scheduled time.

> In the case of public apps and Microsoft Store for Business (MSB) apps, you need to set the **Silently install on Windows devices** setting to ON from the **App Configurations** section.

Installing apps using Apps@Work

To install an app using Apps@Work:

1. Click the **Apps@Work** app.
   Your administrator email address and server URL are pre-filled in the Apps@Work login dialogue.
2. Enter your password and click Sign In to display the apps page.
3. Select an app to install. You will not be able to install apps with dependencies on prerequisite apps if those prerequisite apps are not already installed on the client.
   For Apps@Work for iOS devices, you can optionally click the **Install All** button to install all apps. This option is available in **New Releases**, **Featured Apps** and **Categories** screens.

> Apps and Books apps will not be installed if the Apps and Books app licence is not previously accepted.

4. Click **Update and Save** to view the **App information** screen.

App Installation and Updates for Android Enterprise Devices

Administrators can publish an app to the catalog for general access and simultaneously deploy it to a specific device for immediate use. This allows users to receive the app directly, while it also stays available in the catalog for others to install as needed.

To install apps and updates

1. Navigate to **Apps> Apps Catalog**.
2. Choose the app you want.
3. Click **Actions** on the **Details** screen. The **Send Install/Updates Request** is displayed.
4. Click Send Install/Updates Request. The **Send Install/Updates Request** dialog box is displayed.
5. Perform the following under **Send Install & update notifications to devices for this application**:
   - Select **Send request for new application (applies to devices that don't yet have the app installed)** checkbox to install the new application.

- Select **Send request for updates (applies to devices that have the app installed but an update is available)** checkbox to update an installed application.

6. Perform the following under **Select Users to Send Request**:
   - Click **Everyone** to distribute the configuration to all compatible users. The app appears in their App Catalog.
   - Click **Custom** to define the user group or user who sees the application in the App Catalog.

> The **Send Install /Update Request** distribution is part of the app distribution process. The settings you choose on the **Distribution** screen decide which devices will receive the app.

A confirmation window appears indicating that installation of the app is complete.

Changes from new installs or updates are shown in **Dashboard** > **Audit Trails**.

> For Public and Private apps **Send request for updates (applies to devices that have the app installed but an update is available)** is disabled. Only **Send request for new application** requests are allowed.

Related topics:

- App Catalogue

Clearing App Cache for Android Enterprise Devices

The **Clear App Cache Request** allows administrators to remotely clear cached data for a selected application that is installed on Android Enterprise devices using Ivanti Neurons for MDM. This action helps resolve common app issues, such as slow performance, unexpected errors, or outdated temporary data, without uninstalling or reinstalling the app. The request clears only the app's cache and preserves user data, app settings, and configurations. Administrators use this feature to quickly restore normal app behavior while minimizing disruption to end users.

Procedure

1. Navigate to Apps> Apps Catalog.
2. Select and open the app.
   The app **Details** page appears.
3. Click the action menu (⋮) on the app **Details** page.
4. Select the **Clear App Cache Request** option.
   The **Clear App Cache Request** pane appears.
5. Perform one of the following actions in the **Select Users to Send Request** section to distribute the app cache clear request:
   - Select **Everyone** to send the request to all compatible devices that have the app installed.
   - Select **Custom** to send the request to specific users, user groups, devices, or device groups.
6. (Optional) Search for an existing distribution list under **Other Distribution Filter Options**.
7. (Optional) Select **+ Add Distribution Filter** to create a distribution filter in the **Create Distribution Filter** pane.

> Use this option to send the **Clear App Cache Request** to a specific set of devices, such as DO or EPO mode devices.

8. Click **Send**.

9. Click **OK** in the **Clear App Cache** confirmation dialog-box.
   Ivanti Neurons for MDM displays a notification that lists the number of devices that received the **Clear App Cache Request**.

After completing the **Clear App Cache** request, all app details (version, name, platformAppId, displayVersion, and bundleVersion) are logged in the **Audit Trails** page.

8.8. Assigning Custom Attributes to Apps

After you create custom attributes, you can assign them to one or more applications. Each attribute has a corresponding value that you can use for tasks such as creating application groups. For more information about managing attributes, see **Attributes**.

Create and assign a custom attribute for an individual application

You can assign a custom attribute to a single application.

Procedure

1. Log in to the Administrative Portal.
2. Navigate to **Apps** > **App Catalog**.
3. Select an application and click **Attributes**.
4. Click **+Add New** select a value from the **Attribute Name** drop-down menu.
5. Specify the attribute value in the **Value** field.
6. Click **Save**. The custom attribute is added to the application.

Assign custom attribute to multiple applications

You can assign custom attributes to one or more applications. When you select multiple applications, the custom attribute is applied to every version of the application. You can select a specific application, go to the Attributes tab and change the custom attribute details for a specific application version.

Procedure

1. Log in to the Administrative Portal.
2. Navigate to **Apps** > **App Catalog**.
3. Select check boxes for one or more applications.
4. Click **Actions**.
5. Select **Assign Custom Attributes**. The Assign Custom Attributes to Apps wizard appears.
6. Select one of the following options:
    - Force assign (overwrite) all attributes even if any existing values are found.
    - Overwrite only if value is empty, and skip attributes with existing values.
7. Select the check boxes for one or more attributes.
8. Specify the value in the Value fields (empty values are not allowed).
9. Click **Assign**. The custom attribute is assigned to all the versions of the selected applications.
10. (Optional)If you want to change the custom attribute for a single application version, select the application version from the version drop-down and click Edit.

> The **Custom Apps Attributes** with their values can be used for creating reports and for exporting to CSV format from the **Device Details** page.

8.9. Managed Configurations for Android

This section contains the following topics:

- Using Android Enterprise Managed Configurations
- App Restrictions and Permissions for in-house apps
- Setting up Gmail with Android Enterprise

If Ivanti Neurons for MDM is Android Enterprise enabled, then the Android Enterprise configuration is available to use per app.

Using Android Enterprise Managed Configurations

1. Click **Apps**.
2. Click **App Catalogue**.
3. Select an app for which to configure the Android Enterprise configuration.
4. Click **App Configurations**.
5. Click **Managed Configurations for Android**.
6. Provide a name for the configuration.
7. Optionally, provide a description.
8. Use the Managed Configurations fields to configure managed configurations behaviours:
9. Use the **Tunnel Configuration Settings** to integrate the Tunnel app directly with Ivanti Go app for Android devices. Select the **Enable Tunnel Configuration** option to apply this setting. With this enhancement, administrators can enable Tunnel capabilities through Ivanti Go and configure secure connectivity using existing Tunnel configurations. The feature is available for newly enrolled Android devices. To ensure a seamless transition, the standalone Tunnel app continues to be supported. However, devices with the standalone Tunnel app installed will not display the integrated Tunnel experience in Ivanti Go. After the standalone Tunnel app is removed, the integrated Tunnel functionality becomes available within the Go app. Only one Tunnel configuration can be applied to a device at a time.

Setting	Description
Blocks apps from sharing widgets across profiles	Enable to block apps from sharing widgets across profiles only if the app is not silently installed. Leave disabled to allow trusted apps deployed in the Android Enterprise profile to display widgets on the home screen so users can access information without having to log in.
Blocks the user from uninstalling the app	Enable to block the user from uninstalling the app (public, private or in-house) after Ivanti Neurons for MDM silently installs the app.
Minimum version code	Set a minimum version code required for the app to override the default update behaviour. If the version code of the app currently installed on the device is less than the specified minimum version code then the app is updated immediately to the latest version.
Auto-launch on install	Select this option if you want to launch an app automatically after installation. This functionality is available only if the app is newly installed on the device and not for a version update. In the case of Work Profile and Work Profile on Company-Owned devices, Go app should be active and in the foreground. Due to limitations on Android 10+, only one app will auto-launch if the user pushes multiple apps in the case of Work Profile and Work Profile on Company-Owned devices.

10. The administrator can control the app configuration fields which can be sent to devices or which should not be sent. In general, the default values are set when pushing the configurations to different devices. Under the Managed Configurations section, within **Push to device** setting, select **Push all settings** or **Only push settings with values defined**.

Managed Configurations

Each Android Enterprise app configuration displays Certificate-enable button for each text field and when clicked, the text field is replaced by a drop-down list of certificates. When configured, these certificates are silently applied without any user interaction.

An existing certificate-enabled field can be changed to text-enabled by clicking the same button next to the field. A text-enabled field changed to certificate-enabled field can be changed back to text-enabled field by clicking on the same button. (Default drop-down fields cannot be changed back to text-enabled fields).

> If there are no ID certificates configured in the tenant and when switched from text to drop-down using the Certificate-enable button, only 'None' option is shown in the drop-down list.

Click **Manage Permissions** to select and configure runtime permissions for applications targeting API 23 or higher and Android 6.0+.

Only the dangerous permissions that are applicable to the specific application are listed for selection. The complete list of dangerous permissions (such as read your contacts, find accounts on the device, write call log, and so on) are listed at https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups.

11. The rights you can assign to each permission include:
    - The permissions are applied only when the application requests permissions.
    - The permissions are not applied if the users have previously accepted or denied permissions.
    - Auto grant
    - Auto deny. Use this setting with caution.
    - Default/Global

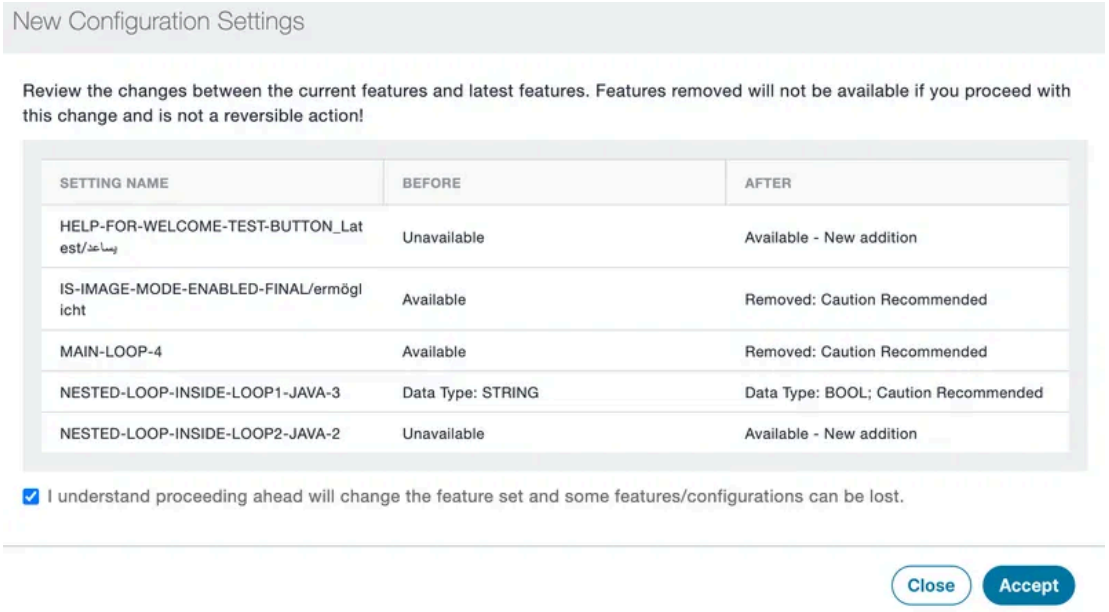
Configure the distribution options, selecting from **Everyone with App**, **No One**, or **Custom**.

12. Click **Save**.

New Configuration Settings

When an app version is updated and if there are any changes to existing configurations, the **Update to Latest Features** button appears after editing the Configuration Details page.

1. Click **Update to Latest Features**.
   A warning message appears on the screen indicating that moving to the latest features will prevent users from accessing the older versions of the application. The warning message recommends steps to integrate the latest version of the application seamlessly.
2. Click **Next**.
3. The **New Configurations Settings** window appears on the screen.



The **New Configuration Settings** window lists different settings that were existing with the configuration, and the status of each setting after the update. The New Configuration Settings window lists all the restrictions from the database, and the Google schema will list the following status:

- Added
- Removed
- Modified

Select the check box and click **Accept** to proceed with the update.
A confirmation message appears on the screen that the configuration has been updated successfully with the latest features. You can now distribute and save the configurations for changes to take effect.

App Restrictions and Permissions for in-house apps

The administrator can set some app restrictions and restrict or grant permissions for In-house apps. This functionality was available only for Public apps. But this functionality has been extended to the In-house apps now.

> The administrator must re-upload the In-house apps to have the **App Restrictions** and **Permissions** features available on their apps. It is recommended to delete the existing app before uploading a new version.

Procedure

1. Go to Apps > App Catalogue.
2. Select an **In-house** app from the list.
3. Click **App Configurations**.
4. Click **Manged Configurations for Android**.
5. Click **Add**.
6. The **App Restrictions** section appears on the screen.
   Enter the required values for the available restrictions.
7. Select **Manage Permissions**.
8. The **Select Permissions** window appears on the screen.
   Select the required permissions from the list and then click **Select**.
9. Under the **Runtime Permissions** section, set the values for the selected permissions.
10. Under the **Distribute this App Config** section, choose one of the following **App Distribution** options:
    - **Everyone with App**
    - **No One**
    - **Custom**
11. Click **Save**.
    The selected restrictions and permissions will be applied on the In-house apps.

Setting up Gmail with Android Enterprise

You can deploy Gmail to Android Enterprise devices if you have set up Ivanti Neurons for MDM for Android Enterprise. To setup Gmail with Android Enterprise

1. Go to **Apps > App Catalogue**.
2. Select Gmail app for which to configure the Android Enterprise configuration. The Configuration Setup section is displayed.
3. Provide a name for the configuration.
4. Optionally, provide a description.
5. Use the **Managed Configurations** fields to configure managed configurations behaviours:

> The **Expand all** and **Collapse all** options are available for nested or hierarchical restrictions only.

Setting	Description
Push to device	Push all settings - Select this option to enable all toggles, including those with no values Only push settings with values defined - Select this option to enable all toggles with defined values and disable the toggles for settings without values In many cases, the default settings are already available. However, the admin can select the required app config settings or edit the variables that must be sent to the devices.
Email address	Enter substitution variables to define the email address. Typically, you enter $emailaddress$. UEMs can use this field to pull user credentials from Active Directory.
Hostname or host	Enter the host name for the Active Sync server, such as hostname.company.com:443/path.
Username	Use the variable for the user's Active Directory username that can be specified as a direct username (janedoe) or templated value ($username$).
Authentication types	Select the list of strings containing the permitted authentications types.
SSL required	When selected, enables and requires SSL on port numbers used with hostname.
Trust All certificates	Select only if you want the app to automatically accept untrusted certificates. Use this option only for debugging or development when working in a test environment.
Login certificate alias	Enter the alias for the login certificate used for authenticating to the ActiveSync servers.
Allow unmanaged accounts	Select this option to allow users to add or remove any Exchange account other than the account specified in this managed configuration.
Default email signature	Enter the string comprising the default email signature to be appended to the bottom of all outbound email message text.
Default sync window	Enter the value from 0-5 that represents the time window for syncing with EAS (Exchange Active Sync).

Click **Next**.

7. Configure the distribution options, selecting from **Everyone with App**, **No One**, or **Custom**.
8. Click **Save**.

8.10. Managing Google Play Apps

You can define which binary from the Google Play app that should be deployed to specific groups or individuals. This deployment is applicable to Android enterprise deployments. The app developer must also Allowlist for your organisation to be able to deploy alpha or beta channel apps.

1. Click **Apps**.
2. In the **App Catalogue** select an app for which to configure the Google Play release configuration.
3. Click **App Configurations** tab.
4. Click **Google Play Release**.

> Google Release configuration is only applied for Android Enterprise apps. By default, Production option is applied if Google release configuration is not selected for newly added apps.

Click **Add**.

6. Provide a name for the configuration.
7. Optionally, provide a description.
8. Select an option from the drop-down list to select the binary that will be available to users and devices receiving this app. The options are:
   - Production
   - Alpha
   - Beta

   > Note: Production option is applied by default for apps which are already pushed to the device.
9. Configure the distribution options, selecting from **Everyone with App**, **No One**, or **Custom**.
10. **Custom** distributes the app within the user group along with device filter.
    Click **Save**.

Prioritising multiple release configuration

When multiple Google Release configurations are added, you can prioritise the order in which the Google Release configuration should be applied.

1. In **App Configurations**, click **Prioritise Configs**.

> Note: This button is displayed only when multiple configurations are listed

From the listed configurations, drag and drop the configuration that should be applied in priority to the top of the list.

3. Click **Update**.

> When the top prioritised configuration is deleted, the configuration that was earlier listed below gets the top priority.

8.11. Deleting Apps from the App Catalogue

You can delete public and in-house apps from the App Catalogue. You cannot delete prerequisite apps. You need to edit the apps to remove the prerequisite relationships before deleting such apps. If the app is installed on devices, it will be removed the next time those devices check in. Silent app install/uninstall is supported on Samsung and Zebra devices in Device Admin mode, or all devices in Device Owner mode.

In the case of in-house apps, a confirmation window appears on the screen. You need to select the acknowledgment that you want to continue with the Delete operation and click **Delete App**. When you try to delete multiple apps and some apps cannot be deleted, a window appears on the screen which contains information about the apps that cannot be deleted and the reason for that.

The following conditions apply when you try to delete one or more apps from the App Catalog:

- If one version of the in-house app cannot be deleted, then it is not possible to delete any version.
- If one version of the in-house app is a prerequisite app, then the app cannot be deleted and none of the versions can be deleted.
- When you select all or some of the in-house apps to delete them from the App Catalog, all the versions of the selected in-house apps will be deleted.
- An in-house app delegated from a Space cannot be deleted.

Procedure

1. Go to **Apps > App Catalogue**.
2. Click the link for the app.
3. Select **Actions > Delete from Catalog**.
4. Read the warning that explains what happens when you delete an app.
5. The warning explains that Apps and Books licences (iOS) and app reviews (all OSes) are also deleted.
   Select the "I understand the consequences of deleting an app" check box to proceed with the delete operation.
6. Click **Delete App**.

8.12. Upgrading In-House Apps

Use the following procedure to update an in-house app:

1. Go to **Apps > App Catalogue**.
2. Select the app to be upgraded.
3. Select **Actions > Add New Version**.
4. Drag and drop the app to the **Upload App** area or click **Choose File** to select it from your file system.
5. Select one of the following options based on what you want to do with the previous version of the app:
    - **Keep the description, screenshots, distribution, app prerequisites, and app configurations the same:** replaces the previous version in the app catalog.
    - **Change the description, screenshots, distribution, app prerequisites, or app configurations** : includes both versions in the app catalog.
6. Under **What's New**, enter text that explains to users what is different in the new version.
7. This text will be displayed on the device when the user selects the app for installation.
   If you chose to change descriptions, screenshots, or distribution options, complete those changes.
8. Click **Done**.

If you chose to keep older versions of the app in the catalog, only one entry will display under **Apps > App Catalog**. The pane on the far left will indicate the number of apps accounted for by the entry. If you later decide to delete the newer version, the older version will automatically replace it on installed devices.

Displaying a list of app versions

Admins are allowed to upload apps with the same version and different architectures.

ProcedureProcedure

1. Click the link for the app under **Apps > App Catalog**.
2. Click the **Version** tab.
   If there are multiple versions of the app in the catalog, a drop-down displays the versions. If multiple apps with the same version number but different architectures are uploaded, the drop-down displays the supported architecture details. The supported architectures for the apps are also displayed under **App Information**.

8.13. Finding the Package Name for an Android App

For public apps available on the Google Play Store:

1. Use a web browser to locate the app in Google Play Store.
2. Select the app.
3. Examine the URL displayed in the browser.

The package name is included in the URL after id= as shown below:

https://play.google.com/store/apps/details?id=<package name>

For in-house apps and other apps not available on the Play Store, try downloading **Package Name Viewer**, or a similar app on the Google Play Store.

8.14. Categories

This section contains the following topics:

- Adding a category
- Removing a category

Categories describe types of apps and help organise apps when users browse the app catalog. Every app must have at least one category assigned. A list of common app categories is available when you start using Ivanti Neurons for MDM. Use this page to manage app categories.

Adding a category

You can add new categories here, or when you add an app to the app catalog.

1. Click **Add** (bottom left)
2. Type the category name.
3. Categories are not case sensitive, so MINE is the same as Mine.
   Click **Save**.

Removing a category

- Click the X next to the category.

If you cannot perform tasks on the **App Categories** page, it might be that you do not have the required permissions. You need one of the following roles:

- App & Content Management

8.15. Distribution Filters

This section contains the following topics:

- Configuring the distribution filters
- Configuring the distribution filters for delegated administrator

Use Distribution Filters to limit the apps available for installation. Distribution filters enable you to display only the apps in the app catalogue that are applicable to the device.

Licence: Silver

These filters are available by default:

- **Android enterprise Enabled Apps** - limits app distribution to Android enterprise enabled devices only.
- **iPad Only Apps** - limits app distribution to iPad devices only.
- **iPhone Only Apps** - limits app distribution to iPhone devices only.

Configuring the distribution filters

1. Go to **Apps > Distribution Filter**.
   The default app filters and any created app filters are listed here.
2. Click **+Add** to access the **Create Distribution Filter** dialog.
3. Enter a name and description in the appropriate fields.
4. Select rule definitions. These rules can be constructed using the applicable operators, including the "contains", "is less than", "is greater than", "is in range", "is equal to", and "is not equal to" operators. The rules can be nested together using the ANY (OR) or ALL (AND) options. App distribution filters are as follows:
   - Access Blocked
   - APNS Capable
   - Android managed Device with Work Profile
   - Android Work Enabled
   - Android Security Patch Level (Android devices)
   - Android Work Managed Devices (Device Owner) Enabled
   - Android Work Profile on Company Owned Device Enabled
   - Client Last Check-in
   - Client Registered
   - Compliance
   - Compliance Action Blocked
   - Current Country Name
   - Current MCC
   - Current MNC
   - Custom Device Attribute
   - Custom LDAP Attribute

- Custom User Attribute
- Custom IDP Attribute
- Device Type
- Home Country Name
- Home MCC
- Home MNC
- IMEI
- IMEI2 (only on Android devices with a dual SIM port and applicable for Android 8.0 or higher devices)
- Kiosk Mode
- Manufacturer
- OS Version
- Ownership
- Phone #
- Roaming
- Secure Apps Status
- Supervised
- Sentry Blocked
- User Enrollment Enrolled
- Automated Device Enrollment Enrolled
- Automated Device Enrollment Enabled

5. Click **Create Distribution Filter**.
6. If needed, select a custom filter to update.
    1. Click **Edit** to display the **Update Distribution Filter** page.
    2. Enter a name and description in the appropriate fields.
    3. Use the pull-down menus to define rules for the filter.
    4. Click **Update Distribution Filter**.
7. Select an app.
8. On the App Detail page and select the **Distribution** tab.
9. Click **Edit**.
10. Choose an App Distribution option:
    - **Everyone**
    - **No one**
    - **Custom**

    > The Distribution Filter section is visible only if **Everyone** or the **Custom** distribution option is selected.

11. Choose a distribution filter option:
    1. Enter a filter name in the **Search the existing distribution filters**... field to locate a filter that has already been created.

2. Click **+Add Distribution filter** to add a new filter.

Distribution filters can be created or assigned to an app before it's added to the catalogue. Changes made to the Distribution Filters will impact the distribution of apps which are using that filter (in all Spaces).

When the filter is set and if the **Allow app installation on M1 Devices upon distribution** is enabled the result populates macOS M1 devices. iOS VPP app will be available for all mac devices if **Allow app installation on M1 Devices upon distribution** is enabled and the Distribution Filter is either **Everyone** or **Custom**. Distribution filters of macOS related attributes are not supported for iOS apps.

Configuring the distribution filters for delegated administrator

Delegated Administrator can manage and edit created filters that were added to individual apps during the distribution process in delegated Space. However, the Delegated Administrator cannot use distribution filters created in Default Space in any other space, but can use them for delegated apps.

Delegated Administrator can create, manage, and edit distribution filters in specific Space they have access to. The distribution filter is available only in the Space it was created it. App distribution filters cannot be delegated.

When a Delegated Administrator with App and System Management role adds an app using distribution filter in delegated Space can see the device details for devices in his Space and for the devices in other Spaces.

User with System management or System read only role will not be able to create, update, or delete distribution filters in any Space.

Delegated Administrator with App and Content manager role might not have access to the distribution filter. Due to which you cannot:

- Create apps using distribution filters. This happens when you are logged in as a Delegated Administrator and add an app.
- Delegated Administrator with only System Read-Only role or higher can add apps with distribution filter. A Delegated Administrator without System management role can add apps without distribution filter.

The Delegated Administrator can filter Delegation Status in App catalogue by selecting the following options:

- Delegated
- Not-Delegated

8.16. Exclude or Distribute apps

Exclude or distribute managed apps from a device without changing the app distribution configuration for in-house and public apps on iOS, macOS, and Windows devices. For all managed apps, these options are present in the **Actions** column of the **Available Apps** section for all devices.

Permissions

To exclude or distribute an application to or from a device, you need to have the following authorisations:

- Access device in space (partition)
- Access the available apps for the device.

Exclude

The exclude option for a selected app uninstalls and removes the associated data from the device. Follow the workflow to exclude a prerequisite app. A pop-up confirmation indicates that you are excluding a prerequisite app, resulting in the exclusion of the main app from the device.

If you exclude in-house apps with multiple versions, it then excludes all the undistributed app versions from the device. If you exclude an app from the device, it deletes from Apps@Work and Ivanti Go. If you exclude and delete an app from the App Catalog and add again, the app will no longer remain excluded for the device. If you exclude a managed app from the device, it should be visible in the **Devices** > **Devices** > **Available Apps** list for the administrator to distribute the app after excluding it.

Distribute

When the administrator triggers the **Send install** command from the app, the app will not install until the administrator decides to distribute it from the device's **Available Apps**. A new exclusion message appears for the devices that don't get the app. When the administrator distributes an available application, the next sync installs the distributed application on the device.

8.17. Reviews

This section contains the following topics:

- Viewing ratings and reviews
- Disabling ratings and reviews
- Deleting a review
- Exporting reviews to a CSV file

Reviews are the comments and ratings (stars) your users provide about apps in the app catalog. Reviews provide valuable information to you and to users who are considering installing an app. Use the **Reviews** page to view or delete ratings and reviews. You might delete a review or rating if it is old or inappropriate.

- Only device users can create and edit app ratings and reviews.
- Device users can edit, but not delete, their own ratings and reviews.
- Only administrators can delete app reviews.
- App ratings cannot be deleted. Ratings (stars) given to apps remain on the **Apps > App Catalog** page, even if you later disable the ratings and reviews feature for your users.

Viewing ratings and reviews

- Go to **Apps > Reviews** to read full user review comments and ratings (stars) for the apps you have distributed.
- Go to **Apps > App Catalog** and see the **Avg. Rating** column for the total number of reviews and the average rating.
- Go to **Apps > Apps Catalog**, click the **App Name**, and see the **Reviews** tab for ratings and reviews for a specific app.

Disabling ratings and reviews

1. Go to **Apps > Catalogue Settings**.
2. Uncheck **Enable Ratings and Reviews in the end user app catalog**.
3. Click **Save**.

Deleting a review

1. Go to **Apps > Reviews**.
2. Select the review.
3. Click the **Actions** button at the top right of the page.
4. Select **Delete**.
5. Click **Yes** in the **Delete Review** confirmation dialogue.

If you cannot perform tasks on the **Reviews** page, it might be that you do not have the required permissions. You need one of the following roles:

- Apps & Content Management

Exporting reviews to a CSV file

You can export the app reviews using the **Export to CSV** option from the **Reviews** page.

Procedure

1. Go to **Apps > Reviews**.
2. Click the **Export to CSV** option to export the review list and related details to a CSV file.
3. A pop-up message appears with **Continue** and **Cancel** buttons stating that the export process has started, and a report will be available shortly.
4. Click **Continue** and wait for the request to complete before you submit another request.
5. A message appears stating that the **Apps Reviews - CSV report is finished** with **Download** and **Delete** buttons.
6. Click **Download** to download the report.
7. (Optional) Click **Delete** to delete the report.

8.18. Apple Apps and Books

This section contains the following topics:

- Licence distribution of apps across multiple Apple Apps and Books accounts in a space
- Device-based and user-based licence distribution
- Using device-based licence option
- Using user-based licence option
- Adding an Apps and Books app to the catalogue
- Adding Apps and Books accounts
- Updating an Apps and Books secure token
- Updating the priority of an Apps and Books account
- Deleting an Apps and Books secure token
- Distributing licences for an Apps and Books app in the catalogue
- Viewing app licences per user
- Apps and Books licence usage notifications
- Viewing Apps and Books licence usage
- Revoking Apps and Books licence for an app
- Apps and Books behaviour for macOS and iOS devices
- Apps and Books licence entitlement when a device moves spaces

Licence: Silver

The **Apple Apps and Books** screen is available only if you have set up Apple Apps and Books in your app catalog settings. This screen shows the app licences that have been purchased for Apple devices via the Apple Apps and Books and how many have been used. Use this screen to:

- select the Apps and Books apps that will be included in your catalog
- distribute licences for Apps and Books apps

For more information about distributing apps with Apps and Books, see the Ivanti Community article, Ivanti Neurons for MDM: How to Distribute Apps with VPP.

> Apple Books may not be available in all countries or regions. In order to distribute licences for apps via Apple's Apps and Books you must enter the sToken provided by Apple.

Licence distribution of apps across multiple Apple Apps and Books accounts in a space

- If the same app exists in multiple Apps and Books accounts, then the licence will be distributed from the account in the order of priority of the accounts.
- If the same app exists in multiple Apps and Books accounts, and if the app licence in the Apps and Books account with higher priority is exhausted, then the app would be distributed a licence from the next prioritised account only if the user or the device is present in the licence distribution list of the next prioritised account.

- A licence will not be revoked and re-assigned on changing the priority of the Apps and Books accounts. The app would be distributed a licence from the first account. If the licences are exhausted in the first account, the app would be distributed a licence from the next prioritised account, and so on.
- A user has an option to revoke all licences of an app from the App Catalogue page. This action would revoke the licence of that app from all available Apps and Books accounts.
- Reserved licences have precedence over priority of the Apps and Books accounts.

Device-based and user-based licence distribution

Whether the licence for an app is Device-based or User-based depends on how you assign it. When assigning an app licence to a device, it becomes a device-based licence. When assigning an app licence to a user, it becomes a user-based licence.

A license is distributed when installing a Apps and Books app to a device, or when a token is issued for that app. If no licences are available for the app, the user has the option of installing and paying for the app themselves. If a user has already been assigned a user-based licence for the requested Apps and Books app, the app is installed using the existing user-based licence, rather than the Apps and Books licence.

> In the case of **Shared iPads**, Apps and Books are installed based on device-based licences regardless of whether device-based licences are selected or not.

Using device-based licence option

With device-based licences, the users need not enrol in Apps and Books. The required apps will install automatically. Corporate supervised devices do not need to deal with an IT owned Apple ID.

During device check-in, the device is identified by the serial number and the required app is installed if there are licences available. If no licences are available the app is not installed. If a licence for an app is reserved, then a device based licence assignment will not occur at app installation.

> Application updates for Apps deployed using Device based Apps and Books licensing are controlled by the administrator.

To control how an app will be updated, in **Apps> App Catalogue** navigate to the **App Configurations/Install On Device** tab. You will be able to select an immediate update that will occur at the next device check-in, or you can choose to have the app update automatically when new versions become available.

Important: Before assigning a device-based licence to a business to business (B2B) or productivity app, confirm the app is eligible for device-based licensing with the app developer.

Using user-based licence option

A user-based licence remains valid for that user if they have to move from one device to another in case the device is lost or stolen or the user upgrades to a new device. With user-based licences, the user must first enrol into Apple Apps and Books. Enrolling is a manual action that the end user must complete in the App Catalogue. Required Apps and Books apps won't be installed on the device until the user enrols in the Apps and Books.

If the app is a required Apps and Books app and the licence distribution is user-based:

- Required app install will not occur if the user is not enrolled in the Apps and Books program.
- Required apps may be installed if the user is enrolled in the Apps and Books program and a licence is available.

- If the user is enrolled in Apps and Books, but there are no licences available then the app will not be installed.

Adding an Apps and Books app to the catalogue

Procedure

1. Go to **Apps > App Catalogue**.
2. Select an app and click **Add to Catalogue**. Click **Next**.
3. Optionally, add a description of the app. Click **Next**.
4. Select a distribution option. Click **Next**.
5. Click the **App Configuration** tab.
6. Optionally, select **Install on device**. This configuration option installs the app without prompting the user on supervised iOS devices.
7. Select other configuration options if needed.

In the Apps and Books secure token info page, the following token details are displayed:

- Created date
- Location (if the token contains this information)
- Expiry date

Adding Apps and Books accounts

Ivanti Neurons for MDM allows adding multiple Apps and Books accounts by adding multiple Apps and Books secure tokens in a single space.

Perform the following steps to add a Apps and Books secure token in a space:

1. Go to **Apps > Apple Apps and Books**.
2. Click **+ Add Apps and Books sToken**.
3. Enter a name and choose a token file.
4. Optionally, deselect the **Automatically distribute Apps and Books apps to all users** option. This option is selected by default, in which case the All Users group is used to distribute the FCFS licences.
5. Optionally, select the **Clear all data from previous Apps and Books Licence** option to remove all app licences associated with this token.
6. Click **Save**.

After the account is added, a list of all added Apps and Books accounts is displayed in the table.

Updating an Apps and Books secure token

Procedure

1. Go to **Apps > Apple Apps and Books**.
2. Click the Apps and Books account name.
3. In the Token tab, click **Update sToken** (.stoken file).
4. Enter the token name and choose a token file.

5. Optionally, deselect the **Automatically distribute Apps and Books apps to all users** option. This option is selected by default, in which case the All Users group is used to distribute the FCFS licences.
6. Optionally, select the **Clear all data from previous Apps and Books Licence** option to remove all app licences associated with this token.
7. Click **Update**.

From the Token tab, click **Resync Apps and Books Licence Usage Information** to perform a full sync of all app and licence information from Apple Apps and Books service. This action is only necessary if the licence allocation information in Ivanti Neurons for MDM is not accurate. This inaccuracy may occur due to inconsistencies in Apple Apps and Books APIs.

Updating the priority of an Apps and Books account

Administrators can assign a priority for each Apps and Books account in a space depending on which the licences would be consumed. The priorities of the Apps and Books accounts are used to have a predictable licence distribution system and resolve conflicts when a user or a device is eligible to receive a licence from multiple Apps and Books accounts for the same app.

Procedure

1. Go to **Apps > Apple Apps and Books**.
2. Click **Edit Priority** against the required Apps and Books account name.
3. In the Edit Priority window, select a new priority.
4. Click **Save**.

Deleting an Apps and Books secure token

Removing a Apps and Books secure token is irreversible and destructive. When a token is removed:

- Apps that have reserved tokens will have their tokens removed.
- Apps that were paid for will remain in the catalogue and users can pay for them on their own.
- Apps that were installed by end users via the corporate Apps and Books account will need to transition to personal accounts if the users wish to use them. Users have a 30-day grace period to do so.

Procedure

1. Go to **Apps > Apple Apps and Books**.
2. Click the Apps and Books account name.
3. In the Token tab, click **Delete**.
4. In the Apps and Books Secure Token Delete window, select the **Yes, Delete the Apps and Books Secure Token** option to confirm.
5. Click **Delete**.

Distributing licences for an Apps and Books app in the catalogue

1. Select **Apps > Apple Apps and Books** from the main menu.
2. A list of Apps and Books accounts is displayed. Under each account, a list of apps purchased through the Apps and Books program is displayed.
   Select an app and click **Distribute Licences**.
3. Choose a distribution option, **First-come, first-served**, **Reserved**, or **Disallowed** in the Apps and Books Licences section.

Viewing app licences per user

You can view licence preference for your users by using the Licence Usage tab.

1. Click the **Users** tab
2. Select a user.
3. Click the **License Usage** tab.
   A list of apps is displayed with their Apps and Books Licence type and licence assignment details.

To view the licence usage for each app per user:

1. Go to **Users** in the Ivanti Neurons for MDM main menu.
2. Select a user.
3. The **Devices** tab is displayed by default.
   Click on the **License Usage** tab.
   A list of all the apps installed on the user's device is displayed including the licence status. The serial number for the device is listed in the Apps and Books Licence Type column for device based licences.
   - App name
   - Version of the app
   - Cost of the app
   - Date the app was assigned
   - Apps and Books licence type
   - Actions (Licence status.)
   - Platform Information for License details.

You can also view the Apps and Books licence usage for each app:

1. Go to **App > App catalog** in the Ivanti Neurons for MDM main menu.
2. Select an app.
3. Click on the **Apps and Books Licences** tab if present.
4. Click an account name. Only apps purchased through the Apps and Books program will be displayed in this tab.

A separate tab for each Apps and Books licence type is displayed.

Licence type and log	Description
First Come First Served (FCFS) - You have the option to select which user groups will receive this type of licence.	• User Requested Apps - Apps the user chooses to install. A User based Licence is the default • Required Apps - Apps that are required and are installed by Admin configuration using the **Install on Device** setting. These apps use Device based licences by default.
Reserved	Reserved licences have priority over FCFS licences. Here you can select the users or devices to have a Reserved licence for the app.
Disallowed	Enter the users who are not allowed to have a licence for this app. The user can still install the app, but they must purchase it.
Activity Log	Displays the user, the type of Apps and Books licence assigned to them, the date it was assigned, and the latest action taken on the licence.

To view the detailed licence usage for each app per device:

1. Go to **Devices** in the Ivanti Neurons for MDM main menu.
2. Select a device.
3. Click on the **Installed Apps** tab.
4. A list of all the managed apps installed to the selected device is displayed including the licence status.
    - App Name
    - Version of the app
    - Platforms supported
    - Source of the app
    - Size of the app
    - Apps and Books licence type
    - App reported (installed) date for iOS apps

Search the installed apps for the device as follows:

- App Name
- Bundle or Package ID

Apps and Books licence usage notifications

Apps and Books notifications help you track Apps and Books licence usage. The notifications thresholds are defined as:

- An information notification is issued when over 50% of the licences have been used.
- A warning notification is issued when 70 to 80% of the licences have been used.
- A Critical notification is issued when 90 to 100 % of the licences have used.
- Notifications are cleared when the usage drops below 50%.

To view licence information for each app:

1. Click **Apps > Apple Apps and Books**.
2. Licence Information is displayed including:
    - Name of the app.
    - Cost of the licence.
    - Number of licences available.
    - Number of redeemed licences.

Go to **Dashboard > Notifications** to view details of a licence notification.

3. The Notifications page is displayed.
   Click on the notification title to see the details. See Dashboard for the available notifications.

Apps and Books licence usage notifications

Trigger	Severity	Notification Type	Component Type
50% Redeemed	Info	Licence Usage	Apps and Books
70% Redeemed	Warn	Licence Usage	Apps and Books
80% Redeemed	Warn	Licence Usage	Apps and Books
90% Redeemed	Alert	Licence Usage	Apps and Books
100% Redeemed	Alert	Licence Usage	Apps and Books

Viewing Apps and Books licence usage

The licence usage details specific to a user is displayed in the licence usage table in the licence column.

1. Click an app.
2. Click the **License Usage** tab.
3. Enter a user name in the search field.

Revoking Apps and Books licence for an app

Apps and Books Licences are revoked when a:

- Device is inactive (retired or wiped).
- Apps and Books app is deleted.
- Device based licence is revoked when the device is retired.
- Apps and Books token is deleted.

To revoke a Apps and Books licence for an app:

1. Select the app under **Apps > App Catalog**.
2. Click the **Apple Apps and Books Licences** tab if present.
3. Perform one of the following tasks:

1. Click **Revoke All Licences** to revoke all licences from all users or devices.
2. Click the **Activity Log** tab. Use the **Actions** column to revoke individual licences on a per user or per device basis.

- For iOS devices, Apple allows a 30-day grace period for Apps and Books apps after the Apps and Books licence is revoked. Therefore, the Apps and Books app remains installable.
- For macOS devices, after the Apps and Books licence is revoked, the app still remains on the device.

To revoke a Apps and Books licence for a user:

1. Click an app.
2. Click the **License Usage** tab.
3. Click the **Revoke License** link for the user whose access to the license should be removed.

> Apps and Books licences are automatically revoked if the user is deleted or the user removes the MDM profile from the device.

Apps and Books Authentication Error Notifications

Some authentications errors might occur when using the Apple Apps and Books service. These Apps and Books Authentication errors notifications are:

Error Notification	Action
Invalid Authentication Token	Upload a valid Apps and Books sToken
Expired Token	Generate a new token online using your company's account
The sToken has been revoked	Upload a valid Apps and Books
Login required	Log into the Apps and Books service

Apps and Books behaviour for macOS and iOS devices

Apps and Books for iOS

Action	Device-based Licence	User-based Licence
Remove Apps and Books app from distribution for user	App is uninstalled on user's device	App is uninstalled on user's device
Un-Delegate Apps and Books app	App is uninstalled from all devices in non-default space(s)	App is uninstalled from all devices in non-default space(s)
Deleting Apps and Books app from default or custom space	App is uninstalled from all devices	App is uninstalled from all devices

Apps and Books for macOS

Action	Device-based Licence	User-based Licence
Remove Apps and Books app from distribution for user	App does not get uninstalled on user's device	NA
Un-Delegate Apps and Books app	App does not get uninstalled from all devices in non-default space(s)	NA
Deleting Apps and Books app from default or custom space	App does not get uninstalled from all devices	NA

Apps and Books licence entitlement when a device moves spaces

When a device moves to a new space, the Apps and Books licence that is assigned to the device or the device owner is revoked. A new Apps and Books licence is assigned depending on the availability in the new space.

The following are the Apps and Books licence entitlement scenarios:

Scenario	Entitlement
An Apps and Books licence is assigned to a device or a device owner in the source space and an Apps and Books licence for the same app is available in the destination space.	Assign a licence from the Apps and Books token in the destination space.
An Apps and Books licence is assigned to a device or a device owner in the source space and no Apps and Books licence for the same app is available in the destination space.	Revoke the licence from the Apps and Books token in the source space.
No Apps and Books licence is assigned to a device or a device owner in the source space and an Apps and Books licence for any installed Apps and Books app is available in the destination space.	Assign a licence from the Apps and Books token in the destination space.

If you cannot perform tasks on the **App Categories** page, it might be that you do not have the required permissions. You need one of the following **roles**:

- App & Content Management

8.19. Catalogue Settings

This section contains the following topics:

- Changing Apple App Management settings
- Setting Default App Store Region
- Enabling/disabling iOS app updates
- Enabling/disabling application ratings and reviews
- Uploading or updating an iOS/macOS Apps and Books sToken (Licence: Gold)
- Removing an iOS/macOS Apps and Books sToken from your Ivanti Neurons for MDM service

In the **Apps** > **Catalogue Settings** page, configure the preferences you want to apply across all the applications in your App Catalog. You can do the following:

- Include app updates during device check-in
- Prevent backup to iCloud and iTunes (iOS only)
- Set default app store region (Apple and Microsoft)
- Remove iOS apps when the device is un-enrolled
- Enable Ivanti Neurons for MDM "Ratings and Reviews"
- Upload iOS and macOS Apps and Books tokens (requires Gold license)

Changing Apple App Management settings

These settings will apply to all apps unless an app management configuration has been created for individual apps.

1. Select or clear one or more of the following check boxes:
    - **Update apps during device checkin** (selected by default)
    - **Prevent backup to iCloud and iTunes.**
    - **Remove apps on un-enrolment**

Click **Save**.

Notifications

1. Click the drop-down list under **Generate system notification when new app versions are available from Apple App store and Google Play Store**, and select one of the following options:
    - **Once a week**
    - **Once a day**

Click the drop-down list under **Generate End-User Notifications for new app updates available in AppCatalog**, and select one of the options:

- **Once a week**
- **Once a day**

Setting Default App Store Region

In the App Catalog settings, set default region for Apple and Microsoft app stores.

1. In the Default App Store Region section:
    - Select **Apple App Store Region**.
    - Select **Microsoft App Store Region**.
2. Select or clear the option to use the last selected App Store region as the default region for each administrator. If this option is selected, then the app store region will be set as whichever region was last selected by each administrator and it will override the previous settings. If this is the first time an administrator is using this feature, then the default app store regions will be set to the previous settings in this procedure.
3. Click **Save**.

Enabling/disabling iOS app updates

1. Select or clear **Update apps during device checkin.**
    - By default, this option is selected.
    - When cleared, any device checkin (including a force checkin by the admin) does not include app updates.
    - However, the user can manually update the app by clicking the Force checkin action on the device app catalogue.
    - New app installations and all other configurations and settings will be updated during the device checkin.

Click **Save**.

For a managed app, the admin can click the **Update** button on the app details page to manually update the app to the latest version from the App Store.

On a user's device, the user can click the **Force Checkin** button on the App Catalog menu to let the device checkin and let the app updates occur along with other configurations and updates.

These settings together allow end-users to choose when their apps get updated:

- Wait until connected to Wi-Fi to avoid data charges.
- Avoid being locked-out, at the wrong time, while the app updates.

Enabling/disabling application ratings and reviews

This will allow users to rate and review the applications and for other users to read those reviews.

1. Select or clear **Enable Ratings and Reviews in the end user app catalog**.
2. Click **Save**.

> The format of the Apps and Books sToken has changed. Instead of a character string in previous releases, it is now a character string stored in a text file in the vpptoken file format. Upload this file directly to the admin console for processing. The Apps and Books account page has been updated to display the Apps and Books organisation name and expiration dates.

Uploading or updating an iOS/macOS Apps and Books sToken (Licence: Gold)

1. Select **Add Apps and Books sToken**.
2. Enter a name for the sToken file in the **Alias Name** field.
3. Drag and drop the sToken file to the specified area or click **Choose File** to navigate to the sToken file.

4. Click **Save**, or if you are updating an sToken file click **Update**.
5. Go to the **Apple Apps and Books** page to view the apps associated with this token.

> If Apps and Books tokens were reserved for individual users in a previous release of Ivanti Neurons for MDM, you must verify that the tokens are still reserved for those users and reserve them again if needed.

Removing an iOS/macOS Apps and Books sToken from your Ivanti Neurons for MDM service

You can revoke an app that is no longer needed by a user, and reassign it as needed. If the app was deployed as a managed app with MDM for iOS/macOS, then you have the option of removing the app and all data immediately.

1. Select an app to remove.
2. Click **Delete**.
   A warning dialogue appears.
3. Optionally, you can give the user a 30-day grace period to:
   - Save their data.
   - Buy a personal copy of the app.
   - Transfer Apps they installed by this Apps and Books account to their personal accounts to continue use.

If you cannot perform tasks on the **Catalog Settings** page, it might be that you do not have the required permissions. You need the following **role**:

- App & Content Management

8.20. Deploying app dependencies

When you upload an in-house application bundle, Ivanti Neurons for MDM scans the application to identify dependencies. If any dependencies are found, it lists them in the third step of the Add App Wizard. For any application dependency, administrators can select to upload a dependency file. However, some applications might not install without uploading the dependency file.

The admin has an option to set app dependency when installing a particular app. In such a case, there can be one or more apps tagged with the main app. When a user tries to install the main app, the user will be notified about the dependent apps that will be installed with the main app.

> This feature is supported on iOS, Android, Windows, and macOS devices.

Note the following points about application dependencies and prerequisites:

- The administrator can set the dependent applications that are prerequisites before an application can be installed on a device. A prerequisite application can be an in-house, public, private(Android), or VPP application.
- The count of prerequisite applications are now displayed in the Prerequisite Apps column in the App Catalog page. You can mouse over the number to view the list of prerequisite applications.
- A prerequisite application is downloaded directly once the main application is triggered for installation.
- If a main application is delegated, the associated prerequisite applications are auto-delegated.
- You cannot delete a prerequisite application from the app catalog until the prerequisite relationship is removed.
- Multiple versions of an application can have different prerequisite applications.
- The Audit Trails page logs the addition, removal, and auto-delegation of prerequisite applications for iOS, Android, and macOS.
- If the administrator or end-user installs an application that has prerequisite applications, the prerequisite applications are installed before the main application is installed. If a device check-in takes place before all the prerequisite applications are installed, all the prerequisite applications are uninstalled.

> Although an application needs a dependency file, Ivanti Neurons for MDM does not require that you upload any of the files to deploy an app.

> For Samsung devices, the admin should add prerequisite apps to the Kiosk Mode Allowed Apps list. The prerequisite apps added to the Allowed apps list do not get added to the Blacklisted apps list.

> For non-Samsung devices, if the main app is added to the Kiosk Mode Allowed Apps list, the prerequisite app should run silently in the background. You can view the prerequisite app in kiosk mode only if the admin sets this app in kiosk mode.

> **Windows devices** - If the Bridge app is a prerequisite app that is not distributed, and the main app is a .exe that is distributed silently. When the dependency is removed, the Bridge app will be uninstalled, but the .exe fails after this step. Admin should make sure that the Bridge app is not undistributed by default.

> **Windows devices** - When the main app is non-silently distributed and the main app has a pre-requisite app with no distribution, the pre-requisite app installs first and is successful. However, in case the main app fails to install, then immediately the pre-requisite app uninstalls. Retry of failed main app happens only when the user triggers an install request.

Adding an in-house application

1. Go to **Apps > App Catalogue**.
2. Click **Add**.
3. Drag the app file to the dotted box, or click **Choose File** to select it from your file system and click **Confirm**.
4. Click **Next** (lower right). Ivanti Neurons for MDM scans the app for dependency files and lists them in the **App Dependencies** table.
5. Review the app information and verify that you selected the correct app.
6. Click on the Upload icon in the **Actions** column. The **Upload Dependency** window is displayed.
7. Click **Choose file** to browse and locate a local copy of the file and click **Upload**.
8. Ivanti Neurons for MDM scans optional packages for the app, if any and lists them in the Optional Packages table. If listed, click on the Upload icon in the Actions column. The Upload Optional package window is displayed.
9. Review the app information and verify that you have selected the correct app.
10. Click **Choose file** to browse and locate a local copy of the file and click Upload.
11. Click **Next**.
12. (Optional) Add screenshots of the app and click **Next**.
13. If the application requires other prerequisite applications.
    1. Select the option **On** from the **Prerequisite Apps** section.
    2. Search for the prerequisite application under the **Add Apps** tab.
    3. Select the applications.
    4. Click **Save**.
14. Define app distribution and click **Next**.
15. Define the App Configuration section and click **Done**.The next time the devices sync with Ivanti Neurons for MDM, the app is deployed in the device along with the dependent files.

> You can add additional dependencies by clicking the Add Dependencies button. When uploaded, these additional dependencies are also listed under the App Dependencies table. The admin can also manually add optional package with content only type. This type of package is not version dependent.

Adding a prerequisite app

You can add a prerequisite application to a main application. You can add different prerequisites for different versions of a main application. The App Catalog page provides you with the option to either keep the description, scripts, screenshots, distribution, app prerequisites, and app configurations the same as that of the existing application version or change the associated required applications. You cannot delete a prerequisite application without removing the association with the main application.

The Audit Trail page now displays the supported prerequisite applications in specific fields as follows:

The Prerequisite Applications section for the supported iOS, Android, and macOS applications in the Audit Trails page displays the following fields:

appVersionId

name

platformAppId

The prerequisite applications that are auto-delegated or undelegated containing the following fields are displayed:

dmPartitionDistributionType

dmPartitionDistributionReason

Procedure

1. Select an application from **App Catalog**.
2. Click **Edit**.
3. Scroll down to **App Delegation** and select the option **Delegate this app to all spaces**.
4. Click **Save**.

> If you delegate multiple applications, and choose to remove delegation from the main application, the prerequisite application is not removed from delegation automatically.

8.21. Deploying Divide Productivity with Android Enterprise

Divide Productivity is a PIM app you can deploy to Android Enterprise devices.

1. Go to **Apps > App Catalogue**.
2. Under **Business Apps**, click **Divide Productivity**.
3. Enter additional categories or a description.
4. Click **Next**.
5. Accept the displayed permissions.
6. Click **Next**.
7. Select a distribution option.
8. Expand **Advanced Options & App Configuration**.
9. Use the following guidelines to enable options:
10. Select a promotion option.

Setting	What To Do
Blocks the user from uninstalling the app	Select to prevent the end user from uninstalling the app when it has been silently installed.
Mail Address	Use variables to define the email address to associate with the app.
Password	Use variables to define the password for the email account. If you leave this field empty, the user will be prompted for the password.
Host	Enter the host name of the mail server to use. Enter the fully qualified domain name of the ActiveSync server. If you are using a Standalone Sentry, enter its fully qualified domain name (FQDN) instead. Example: mySentry.mycompany.com
Server Type	Select the type of mail server.
Username	Use variables to define the username for the email account.
Is SSL Required	Select if you want secure communication using https to the server that you specified in the Host field.
Trust All Certificates	Select only if you want the app to automatically accept untrusted certificates. Typically, you select this option only when working in a test environment.
Default Email Signature	Enter the default email signature for all emails. that the end user can change this at any time. Once the device user changes it, later changes to this field have no effect.
Email Max Attachment Size	Enter the maximum size to be allowed for attached files.
Enable Task	Select to synchronise tasks.
Login Certificate Alias	Enter the alias for the login certificate.
Smime Signing Certificate Alias	Not currently supported.
Smime Encryption Certificate Alias	Not currently supported.
Advanced Options	
Install on Device	Select to prompt the user to install the app.
Silently install on Samsung Knox devices	Select to install the app automatically on Samsung Knox devices.

Setting	What To Do
Do not show app in end user App Catalogue	Select if you do not want the app to appear in the app catalogue on the device.

11. Click **Done**.

8.22. Setting up the Provisioner app

This section contains the following topics:

- Provisioning Requirements
- Enable Android beam to use NFC bump
- Provision a corporate-owned device
- Register the device
- Verify the device registration status

Provisioner is a Ivanti Neurons for MDM app used to provision corporate-owned devices so that they can be registered as work managed devices and placed in Device Owner mode.

A company-managed device has a corporate profile only and no personal profile. The administrator is able to set over twenty lockdowns on the device, that can restrict device functions such as the camera, phone calls, SMS, networking, and more.

The Provisioner app is needed by the device that will initiate the configuration of the Android Enterprise target device with an NFC bump. To provision corporate-owned devices, install the Provisioner app onto a master device, and use the NFC (near field communication) bump to provision new devices. The bump is tapping the two devices together. The devices can be provisioned to use one of the client apps:

- Go to use with Ivanti Neurons for MDM
- At Work UEM, an unbranded client app, to use with Ivanti Neurons for MDM.

Provisioning Requirements

To provision a corporate-owned Android Enterprise device to be a work managed device:

- Corporate-owned native Android Enterprise-capable devices must be factory reset prior to provisioning.
- Android Enterprise configuration must be defined and applied to the Android device group.
- An NFC-capable Android device designated to serve as the master or as the template, with the Provisioner app installed.
- Android Enterprise-capable devices to provision.
- Provisioner app.
  Download the Provisioner app for Android from Google Play.

Enable Android beam to use NFC bump

Procedure

1. Go to **Settings** on the device.
2. Go to **Wireless & networks** and click **More**.
3. Select the **NFC** checkbox.
4. Click **Android Beam** and slide the switch to **On**.

> The exact steps may differ slightly for your device.

Provision a corporate-owned device

Procedure

1. Install the Provisioner app on the device to be used as the Android master device.
2. Launch Provisioner on the master device.
3. Select an app from the dropdown menu.
4. Enter the information requested by the Provisioner app. Some fields may auto-populate if a supported Wi-Fi type is present. Use these guidelines:

Field	Value
Select app for provisioning	Go (select for use with Ivanti Neurons for MDM) At Work UEM (unbranded client app; select for use with branded Ivanti Neurons for MDM).
Wi-Fi Network SSID	Enter the Wi-Fi SSID the master device is to use.
Wi-Fi Security Type	Enter the Wi-Fi security type
Wi-Fi Password	Enter the password for the Wi-Fi
Time Zone	Enter the local current time zone
Locale	Enter the locale

5. Click **Continue**.
   The **Bump the devices** screen is displayed on the master device.
6. With the target device turned on and displaying the Android Welcome screen, press the master device back-to-back with the target device to initiate an NFC transfer.
   If the NFC transfer is successful, the target device may make a sound, and then proceed to downloading the chosen client app. If the device is not encrypted, it will start the encryption process before continuing.
7. Continue to provision additional devices by bumping the devices. The target device must display the Welcome screen, and the master device must display the **Bump the devices** screen.

Register the device

Once the corporate-owned device has been provisioned using NFC bump, it will have the selected client app installed. Launch the client app and register the device.

Verify the device registration status

Procedure

1. Go to **Devices > Devices**.
2. Click the link for a device to view the details.
3. The status of the device is listed in the left pane.

8.23. Managing Windows Applications

Users can manage (Import, Configure, Schedule, Distribute, Update, and Remove) the complete app life cycle for Windows applications. The app distribution and app update processes are supported through the MDM console. For more details on managing Windows apps and other applications, see **App Configuration**, **App Insights**, and **App Catalogue**.

Supported app types

- In-house (Check options in **Adding an In-house app** from the section **App Catalogue**)
- MSB (Microsoft Store for Business integration)
- Public store (via native Microsoft Store Integration) Microsoft Store Region can be set in Apps > Catalog Settings. For more information, see **Adding an app from a public store** from the section **App Catalogue**.

Supported app extensions

- MSI
- MSIX
- APPX
- APPX bundles
- EXE (via **Ivanti Bridge**)

App Control

The App Control configuration controls the app installation per device. For more information, see **App Control Configuration: Control Which Apps Are Installed Per Device**.

Packages and Dependencies

The following different features are available:

1. Windows apps can be set as prerequisites for all types of applications. For information on how to set app prerequisites, see **Deploying app dependencies**.
2. The APPX and APPX bundles App Dependencies and Other Packages dependencies. On the **Viewing App Details** page, review the **App Dependencies and Other Packages** section.
3. Win32 apps support the selection of the correct product code (MSIs) and command lines and variables. A list of common command line options can be found **here**.

Scripts

Scripts are supported via Ivanti Bridge Client. For information on setting up the Scripts, see the **Ivanti Bridge**

Once Ivanti Bridge is installed on the devices, the scripts can be distributed as follows:

- At device level with the Scripts and Actions via Ivanti Bridge Action
- Via the Ivanti Bridge Configuration (go to Configurations > Bridge)

The **Check existing version on device** checkbox, available in the **Scripts and Files** tab for in-house MSI and EXE applications, and it controls how the app installs on Windows devices. When you enable this option, the device runs a check-in to verify whether the app

is already installed and to identify its version. Ivanti Neurons for MDM installs or upgrades the app only if it is not present or if the installed version is older than the required version. If the same or a newer version exists, the installation is skipped. This option requires that the app is installed on at least one device before you enable it.

Pre-install and post-install scripts and files

For .exe files and .MSI files

You can configure pre and post-PowerShell install scripts, registry scripts, and Windows executable (.exe) files and download other types of files for Windows apps at the App Details level.

When adding a new pre or post install script or file, the Ivanti Bridge screen appears. You can attach the script or file, add script argument and also provide a target location for the files. The pre-install script must be executed successfully on the device before sending the app installation command to the device. The pre and post install scripts and files will be executed / installed in the same order in which they were uploaded to the console. If the pre-install script download or installation fails, the app installation cannot proceed further.

If the post-install script fails, you can view the errors in the Device details page under the Device logs section. Also, you cannot revert the pre-install scripts / downloaded files and installed .exe files in case the post-install actions fail.

You can reorder the pre-install or post-install scripts and files using the Prioritize Scripts and Files option. This option will be available only if there are at least two or more scripts or files available. Using this option, you can drag and drop the files or scripts within their respective pre or post sections, and not from one section to another.

Installation behavior and configurations

Windows applications support the following features:

- Silent installations
- **Windows app scheduling**
- Reboot options

For more details on installation behavior options, see **App Configuration**

> MSI apps and EXE apps (installed using Bridge) support installations with user-less MDM sessions.

For example, in the following scenarios:

- The device was restarted, and no user is logged-in yet
- The user logged out from the Windows session
- The device was enrolled in Autopilot user-less (Self-deploying or Pre-provisioning) mode
- Applications are installed at the device level

> It allows installing the MSI apps in more efficient ways, for example, during Auto-pilot enrollment or during the night when nobody works on the Windows device. When simple repacking is used for EXEs in MSI, it can be installed, but not upgraded or deleted. The real MSI package has a connection with CSP. Other Application types will be installed after the user logs in.

Tunnel for Windows (Per-App VPN)

Tunnel is a stand-alone native Windows application. It is currently available in the Microsoft Store for distribution to devices. Creates a Per-App VPN Configuration. Sentry deployment is required. To configure the Tunnel app, go to **Configurations** > **+Add** > Search for Tunnel (choose the Configurations that support Windows devices). Select the Sentry profile and configure settings to start tunneling the app data via Sentry. To set up a Sentry Server, go to **Admin** > **Infrastructure** > **Sentry**.

App Inventory

Application and Software Inventory installed in your Windows Device fleet can be tracked at two levels:

- To check applications installed across your devices, go to **Devices** > **App Inventory**
- To check inventory at the device level, go to Devices > choose a device > click on Installed Apps

Administrators can set Windows application inventory collection intervals. Go to Admin > Windows > App Inventory Intervals The intervals are used when privacy configuration is set to collect all apps from the device. To configure the Privacy Configuration, go to Configurations > +Add > search for Privacy > Choose Collect apps Inventory For all apps on the device. Select app types to be collected.

Corporate App Catalog (Apps@Work)

Customers can enable a Corporate Catalog on Windows Devices using Apps@Work. Apps@Work is available and deployed via the App Catalog in Neurons for UEM. For more information, see **Apps@Work (iOS, Android, Windows, and macOS)**.

8.24. Ivanti Bridge

This section contains the following topics:

- Bridge supported file types
- Bridge setup
- Bridge Logs
- Bridge Last Check-in
- Bridge Service Failure Recovery

Ivanti Bridge unifies mobile and desktop operations for Windows 10 using a single console and communications channel. It extends UEM capabilities to managing PCs and allows organisations to take advantage of significantly reduced costs and increased efficiency while ensuring consistent security across PCs and mobile. By using Ivanti Bridge, enterprises have the ability to use a single protocol for Windows 10 Desktop devices as they do for supported Windows mobile devices, to send information to the legacy applications on the OS.

Ivanti Bridge allows IT to modernize Windows operations on UEM without giving up critical functionality. IT can apply policies and scripts already in place without requiring a systems image, domain join, or multiple channels of communication to the device.

With Ivanti Bridge, organisations can now:

- Have complete control over PCs with UEM
- Manage PCs remotely, over-the-air
- Reduce the need for imaging desktops
- Leverage GPO-based commands with PowerShell scripts deployed by UEM
- Easily edit and manage Registry
- Effortlessly deploy non-MSI wrapped Win32 apps and Win32 Store apps
- Gain File System visibility

> Ivanti Bridge is supported on Windows 11+ devices and ARM processors. Ivanti Bridge does not support Windows 10 Home desktop devices.

Bridge supported file types

Ivanti Bridge includes support for the following file types:

- PowerShell
  PowerShell scripts pushed to devices using Bridge support named arguments.
  64-bit PowerShell scripts are supported on 64-bit Windows 10 desktop devices.

> The Bridge timeout on the server-side for expecting a result after sending a PowerShell script to device is about 20 minutes. The timeout is logged as a Failure. However, the script on the device continues to work.

> The Bridge timeout on the device-side for expecting the process of a PowerShell script execution is about 60 minutes. After 60 minutes, the process will be killed, no output from the script is saved, and a new Failure is sent to the server.

> The server-side and device-side timeouts are logged as Failures. If the second timeout passes and the script generates some output, no output is logged on the server-side.

Registry

- VB Scripts
- .EXE for Win32 application deployment
- Win32 Store apps uses WinGet tool for installing and uninstalling the apps.

> If admins need to push Win32 (.EXE) files to a device (for example, as a Windows in-house app), the Bridge functionality will be automatically used if available. It is mandatory to enter an argument to silently run the file (for example, /SILENT or /VERYSILENT).
> The .EXE apps are installed through Bridge using the Admin PowerShell mode. For Windows devices, to install using user's credentials select 'Run as User' option.

> The admins should select the **Installer run as user** checkbox in **App Installer - Settings** to install the apps for a user. Do not select the check box if you want the apps to install at the system level.

Using Ivanti Bridge, the device can be augmented in following key areas.

- **Registry:** Reading, writing, and updating registry values.
- **Files:** Verifying, reading, and updating contents of a file.
- **Application Deployment:** Adding the ability to install .EXE-based applications to the desktop device. These applications can either reside on the Ivanti Neurons for MDM servers or on a Content Delivery Network (CDN) in the Cloud.

Bridge setup

Setting up Ivanti Bridge requires that admins complete the following steps in the following order:

1. Activating Bridge licenses
2. Installing the Bridge application
3. Uploading scripts to the devices for permanent or one time use to the devices

Activating Bridge licenses

Ivanti Bridge is part of the legacy Gold package and the current Secure UEM package.

Installing the Bridge application

After activating the Ivanti Bridge licenses, the Bridge mobile application can be installed as follows:

1. Go to **Apps > App Catalogue**.
2. Click **+Add**.
3. Click **Ivanti Bridge** in the Business Apps section.
4. Add details, customise, and distribute the Bridge mobile application to the required devices as per the procured licences.
   If you have enabled the **Silently install on Windows devices** option, Bridge mobile application will be silently installed and the Bridge service will start running on the devices.

Bridge app is added to the app catalog by default, and also distributed by default to all devices.

After importing the latest version of the Ivanti Bridge (2.1.419.0) into the tenant's catalog, the admin can view the newly aligned version of the app.

Uploading scripts to the devices

Administrators can upload scripts to the devices for permanent use by creating a new Bridge configuration:

1. Go to **Configuration > +Add**.
2. Select the **Ivanti Bridge for Windows Scripts and Actions Configuration** configuration.
3. Enter a name for the configuration.
4. Enter a description.
5. In the Configure Ivanti Bridge section, use one of the following two options to upload Scripts:
    - Select scripts from Scripts Library - Select one of the scripts available from the list.
    - Or
      Upload Scripts - Specify the settings as described in the table under step 7.
        - Enter the **Script File** category settings to specify an installation script to be pushed or executed on the devices.
        - (Optional) Enter the **UndoScript File** category settings to specify an uninstallation script to be pushed or executed on the devices. This is useful in scenarios such as device retirement or configuration deletion.
        - (Optional) Select the option **Configure Outlook** to configure Microsoft Outlook to a device using Bridge.

          Only supported on Outlook 2010 and 2013.

Click **Next**.

7. Select a distribution for this configuration.
   A force check-in will be done automatically for these device actions.

Category	Setting	What To Do
	Name	Enter a name that identifies this configuration.
	Description	Enter a description that clarifies the purpose of this configuration.
Script File	**All Versions (Windows 10+ Desktop)**	
	Script File	Select a valid script or executable file (.ps1, .reg, .exe). • The specified script file or executable file (.ps1, .reg, .exe) will be automatically executed. • Other file types will only be copied to the target folder.
	Script Arguments	Specify the list of arguments for the script file. • Note: For Win32 (.exe) files, enter an argument to silently run the file (for example, /SILENT or /VERYSILENT). This is mandatory.
	Target Folder	Specify the target folder for the script file. • If the target folder is not specified, then the value of the %TEMP% system environment variable is used as the target folder.
Undo Script File	**All Versions (Windows 10+ Desktop)**	
	Script File	Select a valid script or executable file (.ps1, .reg, .exe). • The specified script file or executable file (.ps1, .reg, .exe) will be automatically executed. • Other file types will only be copied to the target folder.
	Script Arguments	Specify the list of arguments for the script file. • Note: For Win32 (.exe) files, enter an argument to silently run the file (for example, /SILENT or /VERYSILENT). This is mandatory.
	Target Folder	Specify the target folder for the script file. • If the target folder is not specified, then the value of the %TEMP% system environment variable is used by default.

Uploading scripts to the devices for one-time use

Administrators can upload a script to the devices for one-time (ad hoc) use.

1. Go to **Devices > Devices**.
2. Click the device name link to go to the Device details page. This is a Windows 10 desktop device to which the one-time script will be pushed/executed.
3. Click the ⋮ icon and click **Script and Actions via Ivanti Bridge**.
4. Enter a name.
5. In the Script File section, specify a script to be pushed/executed on the device as described in the preceding table.

6. Click **Apply**.
   The script execution will be queued and may take a while to complete. Go to the Logs tab to check and view the status (output or failure messages). A force check-in will be done automatically for these device actions.

Bridge Logs

This feature allows you to pull Ivanti Bridge logs for individual devices for troubleshooting and diagnosing applications. The logs are sent at the next device check-in. You can wait for the next scheduled sync or perform a forced device check-in to get the logs quickly.

To pull logs from a device:

1. Go to **Devices > Devices**.
2. Click the device name link to go to the Device details page. This is a Windows 10 desktop device to which the one-time script will be pushed/executed.
3. Click the ⋮ icon and click **Pull Ivanti Bridge Log**. The **Pull Ivanti Bridge Log** window is displayed.
4. Select one of the following options:
   Single log - requests Ivanti Neurons for MDM to pull the most recent Bridge log on the device.
   All logs - requests Ivanti Neurons for MDM to pull all log (up to 30 days) on the device.
5. Click **Pull Log**. After a device has sent it to Ivanti Neurons for MDM, you can view the Bridge log from the Logs tab in the Device details page.

> Only logs sent using **All logs** option can be downloaded as zip file only.

Bridge Last Check-in

The Bridge Last Check-in column lists the Bridge service's last check-in date and time on the Devices page. The column can be added to the Devices page using the Customise Columns option and it is not visible by default.

To make this column visible, select **Devices** > **Customise columns** > select **Bridge Check-in**.

> The exported data will also have the Bridge Last Check-in details wherever applicable.

Bridge Service Failure Recovery

The Bridge Service Failure Recovery has been introduced in Bridge 2.1.14 version. By default, this version gets imported into the App Catalog for all the users. In some rare cases, the Bridge Service may fail without any known reason. In such cases, the support is available in Bridge 2.1.14 and later versions.

9. Content

Use the Content page to distribute content hosted by an external source. The content might includes files that users can download such as sales presentations, images, spreadsheets and documents.

This section contains the following topics:

- Managing Content
- Categories

9.1. Managing Content

This section contains the following topics:

- Distributing Hosted Content
- Deleting content

Hosted Content supports the distribution of downloadable content with external URLs. External URL should lead to a downloadable PDF or EPUB or IBOOK files only, and external URL must have these extensions.

Distribution of VPP Book licences are not supported, hence the distribution of Apple Books based oniTunes Store ID are not supported.

Use Books or Pages app on device to access the pushed content from Ivanti Neurons for MDM. You can access them in Library section.

iBook and EPUB content can be distributed to iOS 8+ iPad devices (Gold license). These formats are restricted to iPad because Apple supports in-house distribution of these formats only to iPad. This restriction does not apply to iOS 9 devices.

> Content previews are not available for these formats.

For **PDF** content, you have the option of pushing the document to the iBook app on iOS 8+ devices.

Distributing Hosted Content

Though you cannot upload new documents to Ivanti Neurons for MDM, you can provide a path (URL) where the content is hosted and distribute it to the device groups.

Procedure

1. Go to **Content > Hosted Content**.
2. Click **+ Add**.
3. Enter the following information:
    - Title
    - Author
    - Category
    - (Optional) Description
4. In the **Hosted Content Path** field, enter a URL for the file you would like to upload.
5. Click **Next**.
6. Make any necessary changes to the distribution.
7. Click **Done**.

To modify Hosted Content, the previous content has to be deleted, new Hosted Content has to be added and distributed.

To modify the settings other than the URL:

1. Go to **Content > Hosted Content**.
2. Click the link to the document in the **Name** column.

3. Click the Edit icon.
4. Make the required changes.
5. Click **Next**.
6. Make any necessary changes to the distribution.
7. Click **Done**.

Deleting content

1. Click the link to the document in the **Name** column.
2. Select **Actions > Delete This Document**.
3. Click the check box to confirm.
4. Click **Delete Document**.

When you delete a document:

- It is removed from the system.
- It is no longer available in the content catalogue.
- It is removed from devices that have downloaded it.

If you cannot perform tasks on the **Content** page, it might be that you do not have the required permissions. You need the following role:

- App & Content Management

9.2. Categories

This section contains the following topics:

- Adding a category
- Removing a category

> As part of the End of Support for Content announced April 15, 2017, the ability to add new Content has been disabled. Content currently uploaded can still be distributed to the Apple iBooks app and used.

Categories describe the types of content in the {{content catalogue}}. Categories help organise content so that users can easily find what they need. Each item added to the content catalogue must have at least one category assigned.

Adding a category

Procedure

1. Click **Add** (bottom left)
2. Type the category name. Categories are not case-sensitive.
3. Click **Save**.

Removing a category

You can click the X next to the category to remove a category.

If you cannot perform tasks on the **Content (Content)** page, it might be that you do not have the required permissions. You need the following role:

- App & Content Management

10. Configurations

Configurations are collections of settings that you send to devices. For example, you can use configurations to automatically set up VPN settings and passcode requirements on the devices. The existing configurations for your system are listed in the Configurations page.

This section contains the following topics:

- Working with Configurations
- Creating a User Self-Service Portal Configuration
- Custom Configuration
- Pushing SyncML to Devices using Custom Configurations
- Home Screen Layout Configuration
- App Control Configuration: Control Which Apps Are Installed Per Device
- App Notifications Configuration
- Exporting Configurations
- Prioritising Configurations
- Managing Configurations

10.1. Working with Configurations

This section contains the following topics:

- Filtering the display of configurations
- Adding a configuration
- Distributing the configuration
- Slow Rollout Distribution of configurations
- Pushing configurations to multiple devices
- Excluding configurations
- Pushing an excluded configuration
- Exporting configurations
- Importing configuration
- Editing a configuration
- Deleting configurations
- Schedule in-house application updates
- Windows Configurations Requiring an Active User Session

Configurations are collections of settings that you as an administrator send to devices. For example, you can use configurations to automatically set up VPN settings and passcode requirements on the devices. The existing configurations for your system are listed in the Configurations page. You can select multiple configurations from the Configurations page and push them to multiple devices at once. These configurations can be pushed to devices specific to spaces and the devices in other spaces remain unaffected. Configurations can be pushed to either a single space or multiple spaces or all spaces at a time.

There are many types of configurations available. They fall into the following basic categories:

- security
- user resources
- enterprise network access
- mobile network
- other (more configurations)

You can perform the following actions for most of the configurations:

- add
- edit
- clone
- delete
- exclude one or more configurations from a specific device
- push one or more excluded configurations to a specific device

Certain configurations have restricted actions:

- Some configurations cannot be added or cloned. iOS Activation Lock is an example of this type of configuration. Therefore, these configurations do not appear among the tiles listed when you add a configuration. These configurations are listed only in the

Configurations page.

- System-defined configurations cannot be edited or deleted. SCEP for iOS Enrolment is an example of this type of configuration.
- Some configurations can be marked as cannot be deleted or reinstalled from a device. These configurations cannot be excluded or pushed to the device.

Filtering the display of configurations

When you view the **Configurations** page, all configurations are listed. To narrow this list to certain configurations, use the filters (left pane) under OS and Configuration Type. For example, to narrow down the list to display only the macOS configurations, select **macOS** under the **OS** section.

You can view configuration across all or multiple space devices by selecting multiple spaces from the drop-down list. When you hover on the displayed configurations, a pop-up window with a list of spaces are displayed. You can click on a space to display the configuration details page.

Apply the **Supported** filter under **Apple DDM** to easily identify DDM-related configurations and enable better differentiation between configuration types.

To search for an existing configuration by its name, enter the configuration name in the **Search** field.

Starting from Ivanti Neurons for MDM release 81, global administrators can delegate space administrators to edit the Dynamically Generated Identity Certificate for All Devices and for the Custom distribution option.

Adding a configuration

This option is enabled only if a single space is selected in the drop-down list.

> You can distribute a maximum of 100 configuration files at once.

Procedure

1. Click **Add**.
2. Select the type of configuration you want to create.
3. Click **Next**.
4. If you do not want this configuration enabled immediately, clear the **Enable this configuration** option.
5. Select a distribution level for the configuration:
    - **All Devices** - distribute the configuration to all the available devices. To delegate configurations across spaces, select one of the following options:
        - **Do not apply to other spaces**.
        - To delegate configurations across spaces, select **Distribution Summary** > **Apply to devices in other Spaces**.
            - Select the **Allow Space Admin to Edit the Distribution** check box to allow the delegated space administrators to edit the distribution for the specific space.
    - **No Devices** - select this configuration for distribution at a later point in time.
    - **Custom** - define specific set of devices that will have this configuration sent to them. To delegate configurations across spaces, select one of the following options:
        - **Do not apply to other spaces**.

- **Distribution Summary** > **Apply to devices in other Spaces**.
  - Select **Allow Space Admin to Edit the Distribution** check box to allow the delegated space administrators to edit the distribution for the specific space.

> The administrator can use the Custom Distribution option to distribute Custom Configuration to Device, Device Groups, User and User Groups. The configuration assignment or distribution to User or User Groups is not available for the following configurations:

- Android Enterprise: Work Profile (Android for Work)
- Android Enterprise: Work Managed Device (Android for Work)
- Android Enterprise: Managed Device with Work Profile/Work Profile on Company-Owned device
- Android Work Managed Devices (Device Owner) for Work Managed Device Non-GMS mode (AOSP) devices

6. If your service has Spaces defined, specify whether the configuration should be applied to the other Spaces, and the priority.
7. Click **Done**.

> For configurations that issue a command to the device instead of installing a profile on the device, the configuration details will not list the configuration as applied to any devices.

Distributing the configuration

Global administrators can delegate space administrators to edit the Dynamically Generated Identity Certificate for All Devices and for the Custom distribution option. For the Dynamically Generated certificates, you can optionally select the **Allow this configuration to be available in all Spaces** option. This option makes Dynamically generated Identity Certificate available to all Spaces and can be used in Exchange, Wifi, VPN and any other applicable configurations including the managed App configurations. This option can be used in scenarios where Dynamically Generated Identity certificate only needs to be distributed to devices (in non default spaces) as part of associated configurations and not to be distributed as an individual configuration.

Procedure

1. Specify the settings fields using the information specified in the table for the individual configuration as applicable.
2. Click **Next**.
3. Select the **Enable this configuration** option.
4. (Optional) Select **Allow this configuration to be available in all Spaces**.
5. Select one of the following distribution options:
   - **All Devices**. Select one of the following options:
     - **Do not apply to other spaces**.
     - **Apply to devices in other Spaces**.
     - **Apply to all devices in other device spaces as highest priority**. (This is applicable only for Wi-Fi Configuration.)
     - **Apply to all devices in other device spaces as lowest priority**. (This is applicable only for Wi-Fi Configuration.)
       - Select **Allow Space Admin to Edit the Distribution** check box to allow the delegated space administrators to edit the distribution for the specific space.
   - **No Devices** (default)
   - **Custom** Select one of the following options:

- **Do not apply to other spaces**.
- **Apply to devices in other Spaces**.
- **Apply to all devices in other device spaces as highest priority**. (This is applicable only for Wi-Fi Configuration.)
- **Apply to all devices in other device spaces as lowest priority**. (This is applicable only for Wi-Fi Configuration.)
    - Select **Allow Space Admin to Edit the Distribution** check box to allow the delegated space administrators to edit the distribution for the specific space.

> Irrespective of spaces, Dynamically Generated Identity Certificate can be configured to all spaces, distributed to all devices, and applied to all devices in other device spaces.

6. Click **Done**.

Slow Rollout Distribution of configurations

When distributing configurations using **Custom** option, you can distribute the configurations using Slow Rollout process so that the configurations are rolled out in a timely schedule. You can schedule the slow rollout distribution in either manual or scheduled manner.

> The Slow Rollout Distribution is currently supported only for VPN and Wi-Fi configurations.

Procedure

1. Go to Configurations > Add.
2. Search for the required configuration.
3. Enter the details like **Name**, **Description**, etc. depending on the configuration, and click **Next**.
4. Select **Custom** as distribution option The **Slow Rollout Distribution** section appears on the screen.
5. Select **Use slow rollout distribution method**. The **Manual Rollout** and **Scheduled Rollout** options appear on the screen.
    - **Manual Rollout** - Using this option, you can manually set the percentage of distribution target. Only the specified percentage of distribution will be done. Alternatively, you can select **All devices in selection summary** to distribute the configuration to all devices.
    - **Scheduled Rollout** - Use this option to roll out distribution in four stages. For each stage, you can specify the rollout percentage, ensuring that each subsequent stage has a higher percentage than the previous one. The duration between stages must be at least one day and cannot exceed 30 days. The most recently saved configuration is automatically preloaded as an editable template for future configurations.
6. Select the desired groups to which the configuration has to be distributed.
7. Click **Done**.

You can view the details from **Configurations** > Newly created configuration > **Details**. From the Details page, you can Pause and Resume the rollout.

> When you create a new configuration with Scheduled Rollout, the percentages you have provided when creating the existing configuration are carried forward to the new one. You can edit the details or continue with the same percentages.

Pushing configurations to a device

If you want to reinstall any of the excluded configurations on a device, you can push the configurations.

Procedure

1. Go to **Devices** >**Devices**.
2. Click a device name to view the details page.
3. Go to **Configurations**.
4. Select the check-boxes to select the specific configurations to be pushed to the device.
5. Click **Push Profiles**.
6. To push a single configuration, click **Push** under the **Actions** column.

Pushing configurations to multiple devices

You can select multiple configurations from the Configurations page and push them to multiple devices at once.

Procedure

1. Log in to the Ivanti Neurons for MDM Administrator portal.
2. Go to **Configurations**.
3. Select the check-boxes to select the specific configurations.
4. Click **Actions**, select **Push selected configs** to devices. The Push Configurations wizard opens and all the configurations and their push statuses are displayed.
5. Click **Push valid configuration(s)**. The configurations are pushed to all devices in bulk. Configurations that are excluded for specific devices from the **Devices** > **Configurations** tab, are not pushed.

Excluding configurations

Some previously distributed configurations can be manually removed from a device by excluding them.

Procedure

1. Go to **Devices** >**Devices**.
2. Click a device name to view the details page.
3. Go to **Configurations**.
4. Select the check-boxes to select the specific configurations.
5. Click **Exclude Profiles**.

To exclude a single configuration, click **Exclude** under the **Actions** column. The selected configurations are now listed under the Excluded Configurations tab.

Pushing an excluded configuration

Procedure

1. Go to **Devices** >**Devices**.
2. Click a device name to view the details page.
3. Go to **Configurations** > **Excluded Configurations**.
4. Select one or more configurations to be pushed to the device.

5. Click **Push Profiles**.
6. To push a single configuration, click **Push** under the **Actions** column.

Exporting configurations

You can export the details of selected configurations or all configurations from selected spaces to individual files.

Procedure

1. Go to **Configurations**.
2. Select the check-boxes to select the specific configurations.
3. Click **Actions** > **Export selected configs with details**. If you want to export all configurations, select **Export all configs with details**.
   A set of YAML files are included in a .ZIP file. The report includes the details of all the existing configurations in the selected spaces.

Export all the configurations

Export your configuration files to send to support for use as a diagnostic aid. You can export a single configuration file to a Yaml format file or export all your configurations into a .zip file. You can export files from different areas of the Configuration page depending on which configurations you want to export.

Procedure

1. Go to **Configurations**.
2. Select the check-boxes to select the specific configurations.
3. Click **Actions** > **Export selected configs with details**. If you want to export all configurations, select **Export all configs with details**.
   A set of YAML files are included in a .ZIP file. The report includes details of all the existing configurations in the selected spaces.

Exporting a customised configuration

Procedure

1. Go to **Configurations**.
2. Click **+Add** to select a configuration.
3. Follow the steps to customise the configuration.
4. Click **Next**.
5. Choose a distribution level.
6. Click **Done**.
7. Select the configuration you just created from the list on the **Configuration** page.
8. Click the **Actions** pull-down menu and click **Export.**

A file with the name of the configuration and a timestamp _yyyymmdd.yaml is downloaded to your device.

Exporting an existing configuration

Procedure

1. Go to **Configurations**.
2. Select an existing configuration.
3. Click the **Actions** pull-down menu and click **Export**.
   A file with the name of the configuration and a timestamp _yyyymmdd.yaml is downloaded.

Importing configuration

You can import a YAML file that contains the configuration details. To edit a configuration you can edit the details in the YAML file select a configuration and import the file and the updated values appear in the configuration. If more then one configuration or space is selected, the Import button gets disabled. If an incorrect file type is selected, an error message appears. If you select a a YAML file that contains different details than the required details for a configuration, an error message appears.

Procedure

1. Go to **Configurations**.
2. Select a configuration, click **Import**, Click **Choose File**, select the YAML file, and click **Import**. The YAML file with the configuration details is imported.

Supported Whitelisted Configurations

- 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

Creating a configuration using YAML file

You can create a configuration from a YAML file. The distribution related specifications are not part of the YAML file. The distribution is by default set to No Devices.

Procedure

1. Go to **Configurations**.
2. Click **Import**, Click **Choose File**, select the YAML file, and click **Import**. The YAML file with the configuration details is imported. The Create configuration page opens displaying all the details that were added in the YAML file.
3. Select *one* of the distribution types:
    - **All Devices**
    - **No Devices**
    - **Custom**
4. Verify the details of the configuration and select *one* of the following Distribution Summary option:

> The distribution summary is not available for all the configurations.

    - **Do not apply to other spaces**
    - **Apply to devices in other spaces**
5. If the new name of the configuration matches the name of an existing configuration, an error message appears, click **OK**, click **Back** and edit the configuration name.
6. Click **Next** and then click **Done**.

Editing a configuration

You can open a configuration and directly edit the details of a configuration, or import a YAML file with all the necessary details. If more then one configuration or space is selected, the Import button gets disabled.

Procedure

1. Go to **Configurations**.
2. Select and open a configuration, click the edit (pencil) icon and edit the configuration.
3. Alternatively, from the edit configuration page click the **Import** icon, select the YAML file, and click **Import**. The Edit configuration page opens displaying all the details that were added in the YAML file.
4. Verify the details of the configuration and select one of the following Distribution Summary option:

> The distribution summary is not available for all the configurations.

   - **Do not apply to other spaces**.
   - **Apply to devices in other spaces**

     > The distribution is set to No Devices by default.

5. Click **Done**.

Deleting configurations

You can delete selected configurations.

Procedure

1. Select the check-boxes to select the specific configurations.
2. Click **Actions** > **Delete**.

Schedule in-house application updates

Ivanti Neurons for MDM automatically updates in-house applications when a device checks in. Administrators can now schedule in-house application updates based on the server time zone. The application updates only when the device checks in within the scheduled time. By default, the scheduling of application updates is disabled.

> This configuration is applicable only for updates and not for a new installation. You can use the Send install/update command to override the auto-update schedule for iOS applications. If auto update is enabled at the app level or catalog level, it will take precedence over the Scheduled App Configuration and the app will update immediately at check-in.

The configuration is applicable only for the following application types:

- iOS in-house applications.
- Android in-house applications that are only in DO mode.
- macOS applications that are of .pkg and .MIP formats.
- Windows applications.

Prerequisites

Ensure that the following prerequisites are met for the configuration to function as expected:

- The application must be managed for iOS and Android. For macOS, the application can be in either managed or unmanaged state.
- Ensure that the option Install on Device under Application Configuration is enabled.
- The device must be checked in during the scheduled time.

Procedure

1. Log in to the Ivanti Neurons for MDM administrator portal.
2. Go to **Configurations**.
3. Click **Add**. The Add Configuration page opens.
4. Search for **App Auto Update**. The Create App Auto Update Configuration page opens.
5. Specify a name in the **Name** field.
6. From the **Configuration Setup** section, select the **Timezone** from the drop-down list.
7. Select the **Start Time** from the drop-down list, and then select the **Duration** from the drop-down list.
8. Click **Next**.
9. Select the required user and device group and then click the checkbox **Enable this configuration**.
10. Click **Done**. The configuration is applied, the application will now update only at the specified schedule.

If you cannot see the Configurations page, it might be that you do not have the required permissions. You need one of the following roles:

- Device Management
- Device Read Only

Related topics:

- Spaces
- Prioritise Configurations

Windows Configurations Requiring an Active User Session

Some Windows configurations require an active user session (a user signed in to the device) before they can be provisioned. If no user is signed in, these configurations are applied after an MDM user signs in to the device.

The following configurations require an active user session:

- Passcode
- User Certificate (user-scoped identity certificate)
- Windows Firewall
- Exchange
- VPN
- Windows License
- Microsoft Defender for Endpoint
- Windows Settings (user scope)
- Bridge service-dependent configurations
- Modern/UWP applications

Bridge Service-Dependent Configurations

Configurations that require the Ivanti Bridge service are provisioned only when an active user session is available. Examples include Windows Desktop Restrictions, Browser Settings, Start Menu, Kiosk, BIOS, Windows Scripts, GPO, and other Bridge service-dependent configurations.

Exception: The following default Bridge scripts do not require an active user session and are sent to the device regardless of whether an MDM user is signed in:

- get-device-data.ps1
- get-bitlocker-status.ps1
- device-hardware.ps1

Modern/UWP Applications

Modern/UWP applications are provisioned only when an active user session is available. This includes:

- In-house applications packaged as .appx or .appxbundle
- Microsoft Store/UWP applications

Traditional MSI and EXE applications are not subject to this requirement.

> If a required user session is not available when a configuration is scheduled for deployment, the configuration is automatically provisioned after an MDM user signs in to the device.

10.2. Creating a User Self-Service Portal Configuration

As an enterprise user, you can use the Self-Service portal to manage your devices and certificates. The My Devices tab displays the devices that you have registered.

You can do the following tasks from the My Devices tab:

- Lock
- Unlock
- Retire
- Reset Secure Apps Passcode

You can perform the following tasks from the My Certificates tab:

- Upload Certificate

> You can distribute a maximum of 100 configuration files at once.

Procedure

1. Log in to the Ivanti Neurons for MDM administrator portal.
2. Click **Add**.
3. Search for **Create User Self-Service Portal Configuration**.
4. Click **Next**.
5. If you do not want this configuration enabled immediately, clear the **Enable this configuration** option.
6. Select a distribution level for the configuration:
    - **All Devices** - Distribute the configuration to all the available devices. To delegate configurations across spaces, select one of the following options:
        - **Do not apply to other spaces**.
        - To delegate configurations across spaces, select **Distribution Summary** > **Apply to devices in other Spaces**.
            - Select the **Allow Space Admin to Edit the Distribution** check box to allow the delegated space administrators to edit the distribution for the specific space.
    - **No Devices** - select this configuration for distribution at a later point in time.
    - **Custom** - define specific set of devices that will have this configuration sent to them. To delegate configurations across spaces, select one of the following options:
        - **Do not apply to other spaces**.
        - **Distribution Summary** > **Apply to devices in other Spaces**.
            - Select **Allow Space Admin to Edit the Distribution** check box to allow the delegated space administrators to edit the distribution for the specific space.
7. If your service has Spaces defined, specify whether the configuration should be applied to the other Spaces, and the priority.
8. Click **Done**.

For configurations that issue a command to the device instead of installing a profile on the device, the configuration details will not list the configuration as applied to any devices.

10.3. Custom Configuration

This section contains the following topics:

- Defining a Custom configuration
- Custom Configuration settings

Licence: Silver

Applicable to: iOS, macOS, Android, Windows

Description

Allows you to import and distribute a predefined configuration file.

The valid configuration file formats are as follows:

OS	Valid Configuration File Formats
iOS and tvOS	• .plist • .mobileconfig • .xml
macOS	• .plist • .mobileconfig
Android	.xml. Currently, this feature only supports .xml configuration files for Zebra devices.
Windows	SyncML.

Defining a Custom configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type "custom" in the search field, and then click the **Custom** configuration.
   The Custom Configuration details page appears.
4. Configure the settings on this page. Refer to the table in the section Custom Configuration settings for guidance on the values.
5. Click **Next** to configure the distribution settings.
6. (macOS devices) Select an additional option for the **Who does this configuration apply to** setting depending on your desired behavior for this configuration:
   - Device Wide (commonly used).
   - User Specific (current registered user).

Click **Done**.

Custom Configuration settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Choose OS	Click an OS icon to upload a configuration file that corresponds to the selected icon.
Choose File	This option appears after you have selected an OS. Drag a configuration file into the Drag and Drop box, or click the **Choose File** button to select a configuration file.

Custom CSP Configuration (Windows only)

You can create Custom CSP configuration on Windows devices only. When you select the Windows OS from Choose OS section, you will get two options:

Option 1 - CSP XML file - Select this option and follow the same process mentioned for the **Choose File** setting.

Option 2 - Custom CSP OMA-URI Schema Node

Procedure

1. Select the Custom CSP OMA-URI Schema Node option from the list. The Custom CSP Configuration section appears on the screen.
2. Under **ACTIONS**, click the + button to start creating the configuration with different OMA-URI fields.
3. The **Add Row** pop up window appears on the screen which has the following fields:
    - Description - Enter any general information about the setting
    - OMA-URI - Enter the OMA-URI that you want to use as a setting
    - Data type - Select a data type that you will use for this setting - DATE, FLOAT, BASE64, NODE, XML, BINARY, CHARACTER, TIME, BOOLEAN, INTEGER
    - Value - Enter a value that is associated with the selected data type
    - Access Type - Add, Delete, Exec, Replace, Get

Click **Save & Close** to close the window with the provided details. Click **Save & Add** another to create a new row.

5. Click **Next**.
6. Select the mode of distribution and click **Done**.

Related Topics

- Pushing SyncML to Devices Using Custom Configuration
- How to create a configuration

10.4. Pushing SyncML to Devices using Custom Configurations

You can create your own Synchronisation Markup Language (SyncML) configuration files or get them from a third party source to implement custom features by adding them to a custom configuration.

Supported platforms:

- Windows

Supported devices:

- Windows 10+
- Microsoft HoloLens 2

Procedure

1. Go to **Configurations**.
2. Click **+Add**.
3. Click **Custom Configuration** to display the **Create Custom Configuration** page.
4. Enter a name for the configuration.
5. Click the Windows OS icon.
6. Drag and drop the SyncML file in the interface or click **Choose File** to navigate to the file to select for uploading to the device.

> Ivanti Neurons for MDM does not perform any validation checks on the code in the file.

7. Click **Next**.

Custom SyncML Log

The SyncML commands sent to Windows device and SyncML responses on these commands from the device can be viewed under the Device Logs tab. This log information will be available after sending the **Windows Custom SyncML** configuration. When the system sends a Custom SyncML configuration, it has the "Installed" status always on the device "Configuration" tab for the configuration irrespective of the SyncML responses.

10.5. Home Screen Layout Configuration

The Home screen layout configuration defines a layout of apps, folders, and web clips for the Home screen.

This section contains the following topics:

- Defining a Home Screen Layout configuration
- Home Screen Layout Configuration settings

Licence: Silver

Eligible Devices:

- iOS9.3+ Supervised only
- tvOS Supervised Only

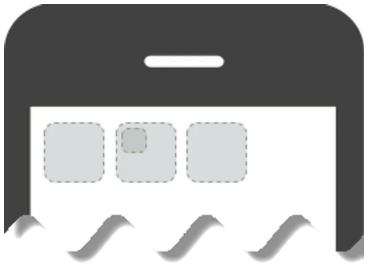
Defining a Home Screen Layout configuration

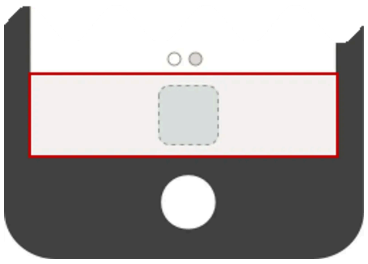
Procedure

1. Go to **Configurations** > click **+ Add**.
2. Type "home" in the search field, and then click the **Home Screen Layout** configuration. The Home Screen Layout Configuration details page opens.
3. Configure the settings on this page. Refer to the table in the section Home_Screen_Layout_Configuration_Settings for guidance on the values.
4. Click **Next** to configure the distribution settings. For shared iPad devices, select the **Device** channel or the **User** channel. For more information, see Working with Configurations.
5. Click **Done**.

Home Screen Layout Configuration settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Dock	Click the + icon to add an app or webclip to the dock of the home screen, shown highlighted here, and then follow the directions on the subsequent screens: You can manually add system apps by typing the Apple bundle ID (starting with 'com.apple'). For example, type 'com.apple.DocumentsApp' for adding 'Files' app.
Page 1	Click the ⊕ to add an app or webclip to the page area of the home screen, shown highlighted here, and then follow the directions on the subsequent screens: You can click Add Page to add another page to the phone display.







10.6. App Control Configuration: Control Which Apps Are Installed Per Device

The App Control configuration allows you to categorise apps as Allowlist or Blockedlist at the device level. Apps that are already installed will not be visible and cannot be launched. Apps will still be visible in the App Store, but they cannot be downloaded or launched. Any device to which this configuration is distributed will use this configuration and ignore any Allowed Apps Policy settings. This configuration supersedes any app-related policies that reference the same applications on the target devices.

This configuration supersedes any app-related policies that reference the same applications on the target devices. For Windows 10 devices, restrictions happen at the device level, therefore a configuration is the only way to enforce app rules.

The App Control configuration allows you to create a:

- **Allowedlist:** Only allow Apps that are explicitly added to this list. No other apps will be able to be installed on devices.
- **Blockedlist:** Disallow specific apps from being installed on devices.

Supported Devices

You can use the App Control configuration to Blockedlist or Allowlist different apps on the following devices:

- Android Work Profile on Company Owned devices
- iOS9.3+ Supervised only
- tvOS 11+
- Windows

Create App Control Configuration

Procedure

1. Select **Configurations**.
2. Click **+Add**
3. Enter **App Control** in the resultant **Choose Configuration** field, and then select the **App Control** configuration.
4. Enter name and description for the configuration.
5. Select an OS and then continue below at the section that applies to your OS.

Android Work Profile on Company Owned devices

Users can add up to 50 application IDs to the Allowlist or Blockedlist group.

Procedure

1. Select **Create a Allowedlist for Personal Apps** or **Create a Blockedlist for Personal Apps** to add the list of appropriate applications to be Allowlisted or Blockedlisted.
2. Enter the application ID (com.example.com) and click Add.
3. Click **Next** and select a distribution option.
4. Click **Done**.

iOS 9.3 supervised devices

Procedure

1. Choose whether to create an Allowedlist or Blockedlist.
2. Click **Add Apps**.
3. Choose the apps to Allowedlist or Blockedlist by clicking one or both of the following tabs:
    - Click **Add by Lookup** to search for and choose apps from the App Store or App Catalog.
    - Click **Add Manually** to choose apps by entering the Apple bundle ID (starts with "com.apple") for Apple System apps only.

Click the **Allowedlist** or **Blockedlist** tab to review the list of chosen apps to be Allowedlist or Blockedlisted.

5. (Optional) Select the **Include all Webclips** option.
6. Click **Next** and then choose a distribution option.
7. Click **Done**.

Windows devices

Procedure

1. Select **Allowed** or **Disallowed** to add the list of appropriate applications to be Allowlisted or Blockedlisted.
2. Under the **Rule Definition** section, select the **App Type** from the list.
3. Enter an identifier name in the **App Identifier** box to search for a specific app. You can also use the **Lookup Apps** link to open a new dialogue and search for Windows-specific app identifiers.
4. (Optional) Enter some description about the app in **App Description** box.
5. Use **+Add** link to add more rule definitions to Allowlist or Blockedlist the apps.
6. Click **Next** and select a distribution option.
7. Click **Done**.

10.7. App Notifications Configuration

Choose how users receive notifications from selected apps.

Applicable to: iOS 9.3+ Supervised devices.

Creating an App Notifications configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type notifications in the search field, and then click the **App Notifications** configuration. The App Notifications Configuration Setup page appears.
4. Name and describe the configuration.
5. Add apps by looking up in the App Store or manually by entering the Bundle ID.
6. Choose an app to which to apply the app notification settings.
7. Configure the notification settings. Here are the notifications you can select:
    - Allow Notifications
        - Show in Notification Centre
        - Sounds
        - Badge App Icon
        - Show on Lock Screen
        - (iOS 12.0+ Supervised) Show the critical alert when using CarPlay
        - (iOS 12.0+ Supervised) Allow critical alerts to be enabled (ignore "Do Not Disturb")
    - Unlock Alert Style
        - Banners
        - Modal Alert
        - None
    - (iOS 12.0+ Supervised) Grouping Type
        - Automatic
        - By app
        - Off
    - (iOS 14.0+) Notification Preview Type - Select a preview type to display in device notification message previews.
        - User Controlled - Display message previews as per user settings for the apps on the device.
        - Always - Display message previews.
        - When Unlocked - Display message previews only when a device is unlocked.
        - Never - Prevent apps from displaying message previews in Notifications.
8. Click **Next** to configure the distribution settings.
9. Click **Done**.

For more information, see **How to create a configuration**.

10.8. Exporting Configurations

Export your configuration files to send to support for use as a diagnostic aid. You can export a single configuration file to a Yaml format file or export all your configurations into a .zip file.

Procedure

Export Configuration

You can export files from different areas of the Configuration page depending on which configurations you want to export.

Export all the configurations:

1. Go to **Configurations**.
2. Select the check-boxes to select the specific configurations.
3. Click **Actions** > **Export selected configs with details**. If you want to export all configurations, select **Export all configs with details**.
   A set of YAML files are included in a .ZIP file. The report includes details of all the existing configurations in the selected spaces.

Export a customised configuration:

1. Go to **Configurations**.
2. Click **+Add** to select a configuration.
3. Follow the steps to customise the configuration.
4. Click **Next**.
5. Choose a distribution level.
6. Click **Done**.
7. Select the configuration you just created from the list on the **Configuration** page.
8. Click the **Actions** pull-down menu and click **Export.**

A file with the name of the configuration and a timestamp _yyyymmdd.yaml is downloaded to your device.

Export an existing configuration:

1. Go to **Configurations**.
2. Select an existing configuration.
3. Click the **Actions** pull-down menu and click **Export**.
   A file with the name of the configuration and a timestamp _yyyymmdd.yaml is downloaded.

10.9. Prioritising Configurations

If you select multiple device groups for a configuration, then multiple configurations of the same type might be assigned to a given device. When configurations of the same type are applied to the same device, the defined priority determines which configuration is applied. The configuration with the highest priority has the lowest number. For example, the configuration with priority 1001 has a higher priority than the configuration with priority 1002. The service assigns numbers automatically.

> Wi-Fi priority cannot be applied to the device and is exempted from the priority.

This option is available only if the page contains two or more configurations of the same type and if a single space is selected in the drop-down list. You can change the priority of configurations.

Procedure

1. Go to **Configurations**.
2. With no configuration selected, select **Actions > Prioritise configs**.
   If **Actions** is not displayed, then you do not have multiple configurations of a type that requires priorities.
3. Use the arrows to move the configurations so that the one that should have the highest priority appears at the top.

> A lock icon indicates that the configuration priority cannot be changed without editing the All Devices distribution setting in the configuration.

Click **Save**.

> Prioritisation can be done up to 400 configurations.

If you cannot see the Configurations page, it might be that you do not have the required permissions. You need one of the following roles:

- DeviceManagement
- DeviceReadOnly

10.10. Managing Configurations

This section contains the following topics:

- AppConnect Configurations
- Security Configuration
- User Resource Configurations
- Enterprise Network Access Configuration
- Mobile
- Other Configuration

10.10.1. Configuration Types

This section contains the following topics:

- Search a Configuration
- Security
- User Resources
- Enterprise Network Access
- Cellular Network
- More Configurations
- Device Sync Configuration

Search a Configuration

Use the search and filter capability on the **Choose Configurations** page to find the configuration you want to apply.

Procedure

1. Choose **Configurations**.
2. Choose one of the configurations listed or click the **+Add** button.
3. The **Choose Configuration** page is displayed
   Click one of the configurations listed or:
   - Enter the name of the configuration in the search box
   - Click a filter icon on the right of the search box to display configuration types compatible with platform.

Click a configuration button to access configuration setting options.

For more information, see **Working with Configurations**.

Security

Type	What It Does	For These Devices	Needs This Licence
Android Enterprise	Specifies Android Enterprise options	Android Enterprise	Silver
AppConnect Device	Specifies security settings AppConnect-enabled apps on devices	• Android • iOS	Gold
Apple PassKeys Attestation	Enable WebAuthn enterprise attestation for specific passkeys on Apple devices.	• macOS	
Entra ID (Azure Tenant)	By connecting Ivanti Neurons for MDM to the Entra ID, you can use the device compliance status of managed devices for conditional access to Microsoft 365 apps.	• iOS • Android	• For new customers:Secure UEM Premium • For existing customers: Platinum
Certificate	Establishes trust with servers	• Android • iOS • macOS • watchOS • visionOS • tvOS	
Certificate Transparency	Controls Certificate Transparency enforcement which can only appear in a device profile.	• iOS • macOS • tvOS • watchOS • visionOS	
Device Logging	Retrieves additional logs such as network and security logs from devices.	• Android Enterprise	
Disk Management Configuration	Defines the policies to manage external and network storage devices.	• Supervised macOS 15.0+	

Type	What It Does	For These Devices	Needs This Licence
Android Encryption	Prompts users to start encryption.	Android	
Encrypted DNS	Allows you to enhance security without needing to configure VPN.	• iOS • macOS • visionOS	Gold
External Intelligence Settings	Allow External Intelligence Integrations	• iOS 26.4+ • macOS 26.4+ • visionOS 26.4+	
Mobile Threat Defence	Protects managed devices from mobile threats and vulnerabilities affecting device, network and applications.	• Android • iOS	
Threat Defense Local Actions	Create and distribute a device configuration defining the local actions to be taken on supported Android devices when the Threat Defense-enabled client detects a threat.	Android	
FileVault 2	Provides ability to perform full XTS-AES 128 disk encryption on the contents of a volume.	macOS	Gold
FileVault Recovery Key	Determines settings for redirecting the FileVault recovery keys to a corporate server.	macOS	Gold
Identity Certificate	• Authenticates the device to servers. • Authenticates the device to network resources.	• Android • iOS • macOS • watchOS • visionOS	
iOS Activation Lock	Enables the Apple Activation Lock feature on supervised devices.	iOS	Silver
iOS Custom Configuration	Distributes an iOS configuration profile that was created by a different app.	iOS	
iOS Restrictions	• Locks down device features. • Enables device features.	• iOS	

Type	What It Does	For These Devices	Needs This Licence
		• watchOS • visionOS	
Intelligence Settings	Allows Apple Intelligence integrations.	• iOS 26.4+ • macOS 26.4+ • visionOS 26.4+	
Conference Room Display	Turns on the Conference Room Display mode on Apple TV.	tvOS 10.2+	
Keyboard Settings	Allows how devices manage keyboard behavior, input options, and related user experience settings.	• iOS 26.4+ • macOS 26.4+	
Lockdown & Kiosk: Android	• Locks down device features. • Re-enables device features. • Applies the kiosk feature.	Android	
Lockdown & Kiosk: Android Enterprise	• Defines features and apps that are restricted on Android Enterprise devices. • Applies the kiosk feature.	Android 5.0+	
Lockdown & Kiosk: Samsung Know Standard	• Defines features and apps that are restricted on Samsung Knox Standard devices. • Applies the kiosk feature.	Samsung Knox	
Local Administrator Password Solution Configuration	Allows administrators to automatically regenerate the local administrator password on managed macOS devices at set intervals	macOS	
macOS Firewall	Manages the Application Firewall settings that are accessible in the Security Preferences pane on macOS devices. The Administrator can enable the stealth mode by specifying a device that cannot be discovered by the ping command.	macOS 10.12+	Gold

Type	What It Does	For These Devices	Needs This Licence
macOS Restrictions	Determine which restrictions are enabled on macOS devices.	macOS	Gold
macOS AppStore Restrictions	Define which restrictions are enabled in macOS AppStore.	macOS	Gold
macOS Disk Burning Restrictions	Manage disk burning restrictions in macOS.	macOS	Gold
Mobile@Work for macOS	Create and distribute execution rules for Mobile@Work for macOS.	macOS	Gold
Mobile@Work for macOS Script	Create scripts to distribute to Mobile@Work for macOS.	macOS	Gold
Identity Preference	Identify an Identity Preference item in the user's keychain that references an identity payload included in the same profile.	macOS	Gold
Certificate Preference	Identify a Certificate preference item in the user's keychain that references a Certificate payload included in the same profile.	• macOS	Gold
Allowed Media Control	Configure mounting, unmounting, and eject options for physical media.	macOS	Gold
macOS Finder Settings	Manage settings of Finder app in macOS.	macOS	Gold
macOS Kernel Extension Policy	Controls restrictions and settings for loading user-approved Kernel Extensions.	macOS	Gold
Active Directory (macOS)	Configure advanced options to bind macOS devices to an Active Directory (AD) domain in order to access software services that rely on AD for authentication and security.	macOS	Gold
Office 365 Auto Account Creation (macOS)	Configure user information and options to setup initial configuration for all Microsoft Office 365 applications.	macOS	Gold
Apple App Catalogue	Manages access to the Apple App Catalog via a web clip.	• iOS • macOS	
Managed Domains	Specifies trusted email and web domains.	• iOS 8+	Silver

Type	What It Does	For These Devices	Needs This Licence
		• visionOS 1.1+	
Passcode	• Makes a passcode mandatory. • Specifies passcode length and content. • Changes passcode requirements.	• Android • iOS • macOS • watchOS	
Privacy Preference (macOS)	Configure which applications are allowed to gain access to system services, system files, and system resources.	macOS	Gold
Authenticate	Provide password-less authentication for cloud services and/or desktop logins.	• macOS • Windows	
Privacy Configuration	Specifies whether location data is collected.	• iOS • Android • Windows	
Client Privacy Statement Information	Display privacy policy to the user in Go client.	• Android • Android Enterprise • iOS	
Ivanti Go Client Settings	Configure to collect data via MixPanel including device and usage information to troubleshoot and maintain the highest quality of services.	• iOS • macOS	
Safari Extension Settings Configuration	Manage Safari browser extensions from various domains.	• Supervised iOS 18.0+ • Supervised macOS 15.0+	
Siri Settings	Allows how devices access and use Siri settings.	• iOS 26.4+ • macOS 26.4+	

Type	What It Does	For These Devices	Needs This Licence
		• watchOS 26.4+ • visionOS 26.4+	
Services Configuration Files Configuration	The administrators can centrally manage and deploy configuration files for various system services.	macOS	
Software Updates	Creates and distributes rules for OS updates.	• iOS • macOS • Windows	
Software Update Settings Configuration	Creates and updates Software Update Enforcement settings.	• Supervised iOS 18.0+ • Supervised macOS 15.0+	
Time Server	Allow devices to connect to custom time servers.	macOS	Gold
Web Content Filter	Controls Safari content.	• Supervised iOS 7 • visionOS 1.1+	Silver
Windows_Firewall	The Windows Firewall configuration has various firewall restrictions. Based on the firewall restrictions applied by the administrator, the Firewall Status result in one of the following firewall statuses in the Security Preferences pane on Windows devices: • Firewall is on and monitoring. • Firewall has been disabled. • Firewall isn't monitoring all networks or some rules have been turned off. • Firewall is temporarily not monitoring all networks. • Not applicable.	Windows 10+	
Windows Information	Defines Windows Information Protection (WIP) settings to protect enterprise data.	Windows 10+	Gold

Type	What It Does	For These Devices	Needs This Licence
Protection			
Windows Restrictions	Determines which features are available on Windows 10+ devices.	Windows 10+	
Windows AI Management Configuration	Allows you to manage Windows AI settings and configurations.	Windows 10+	

User Resources

Type	What It Does	For These Devices	Needs This Licence
CalDAV	• sets up access to a CalDAV server (like Google Calendar)	• iOS • visionOS	
CardDAV	• sets up access to a CardDAV server (like Google Contacts)	• iOS • visionOS	
Email	• sets up access for POP/IMAP email (like Gmail)	• iOS • visionOS	
Exchange	• sets up access for ActiveSync-based email (like Outlook) for Android and iOS mobile devices • sets up Exchange Web Services (EWS)-based email for macOS devices • defines how much to sync to the device • defines security for email	• Android • iOS • macOS • visionOS	• Exchange via sentry is not supported on macOS • The Sync Past days emails flag is not applicable for macOS
Google	• Creates Google account configurations that connect iOS 9.3.2+ devices to Google accounts. • Specifies which app to use to make calls to contacts in the Google system.	• iOS • visionOS	
Font	• installs non-standard fonts necessary for proper display of documents	• iOS	
Subscribed Calendar	• sets up a subscription to an internet calendar	• iOS • visionOS	
Web Clip	• displays a shortcut (icon) to a web page	• iOS • macOS	
Content Caching	• provides content-caching service in order to enable local copies of the App Store software and • enables connected clients for faster software and app downloads.	• macOS	

Enterprise Network Access

Type	What It Does	For These Devices	Needs This Licence
AirPlay	• sets up access to alternate devices for media display	• iOS • macOS	Silver
AirPrint	• sets up wireless printing	• iOS • macOS	Silver
Always On VPN	• sets up access to a VPN server without user interaction	• Android 7.0 + • iOS 8+	• Gold for Android Enterprise • Silver for iOS
Default App Runtime Permissions	• sets the runtime permission configuration for apps deployed to Android enterprise devices.	• Apps built targeting Android API 23+ and running Android 6.0+ on Android enterprise devices.	
Education	• configures the Apple Education payload and the Classroom app for Leaders and Members.	• supervised iOS 9.3+	Gold
Global Proxy	• sets up devices to forward HTTP traffic to a proxy server	• supervised iOS 7 • supervised tvOS	Silver
LDAP	• sets up access to a corporate directory	• iOS • visionOS	
Tunnel	• defines a per-app VPN connection between a client and Sentry using Tunnel	• iOS 7+ • macOS 10.13+ • Windows 10+ • Android	
Bridge	• allows IT to modernise Windows operations on UEM without giving up critical functionality	• Windows 10+ desktop	Bridge license
macOS Server	• define a macOS Server account with the configured account types and relevant settings. Allows the user to activate File Sharing on the server.	• iOS 10+	
Per-app VPN	• sets up connections between specific apps and a VPN server	• iOS • watchOS • visionOS • tvOS	Silver

Type	What It Does	For These Devices	Needs This Licence
Network Relay Configuration	• adds configuration to define settings for network relays	• iOS • macOS • visionOS	
Single Sign-On	• sets up single sign-on for specified managed apps	• iOS • macOS • visionOS	
Multi-user Secure Sign-in	• sets up secure multi-user login via web clip	• iOS	
VPN	• sets up access to a VPN server	• Android • Windows • iOS • macOS • visionOS • tvOS	
VPN On Demand	• sets up access to a VPN server based on domains, host names, etc.	• iOS	
Wi-Fi	• sets up access to a wireless network	• Android • Windows • iOS • macOS • watchOS • visionOS • tvOS	

Cellular Network

Type	What It Does	For These Devices	Needs This Licence
APN	• sets up the mobile Access Point Name for the device	• iOS	
Mobile	• sets up mobile network access	• iOS • watchOS	
Cellular Private Network Configuration	• sets the payload to provide device information on private network deployments	• iOS	
iOS Telecom Presets Configuration	• sets default values for roaming restrictions • sets default values for personal hotspot restrictions	• iOS	

More Configurations

Type	What It Does	For These Devices	Needs This Licence
Apple TV	• defines language and locale for Apple TV	• supervised iOS 7	Silver
Default Device Name	• defines a default device name using variables	• supervised iOS 8	Silver
iOS Wallpaper	• installs a home screen and lock screen background	• supervised iOS 7	Silver
macOS Wallpaper	• Installs a home screen and lock screen wallpaper on the devices. Wallpapers can be changed by the user but not removed from a device once distributed		Not required
Migration Assistant Settings	Helps administrators and users to transfer data, apps, and settings during device setup or migration.	• macOS 26.4+	
Single App Mode	• restricts the device to use of the specified app	• supervised iOS 7 • supervised tvOS	Silver
Associated Domains Configuration	• The Associated Domains configuration is a dictionary that maps apps to their associated domains. • Associated domains can be used with features such as Extensible AppSSO, universal links, and Password AutoFill.	• macOS 10.15+	Gold
Screen Sharing Host Settings Configuration	• Enables administrators to securely control macOS screen sharing features across managed devices.	• macOS 14+	

Device Sync Configuration

Device Sync settings provide a list data points you can monitor on devices. Device Sync configurations cannot be edited. You can view a list of the settings checked.

Procedure

1. Go to **Configurations**.
2. Click **Device Sync Config**.The Details tab of the **Device Sync Config** page is displayed with a list of items checked.

Settings	Time between readings in minutes
Certificate List	
Device Information	60
Installed App List	60
Managed App List	60
Profile List	60
Provisioning Profile List	60
Restrictions	60
Security Information	60
iOS 9+	
Check for Updates	1440

Related topics

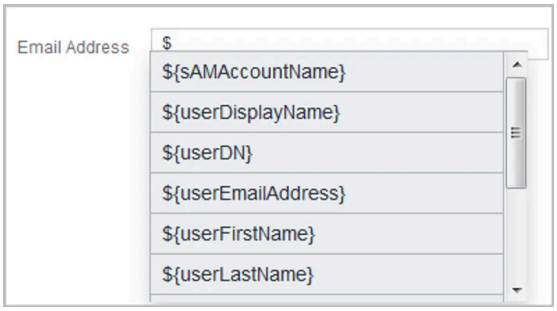
- Variables
- Working with Configurations

10.10.2. Variables

You can use variables in certain configuration fields to represent values specific to a given user. Any field that supports variables displays a list of supported variables if you type $ in the field. This section contains the following topics:

Supported user account variables

User Variables

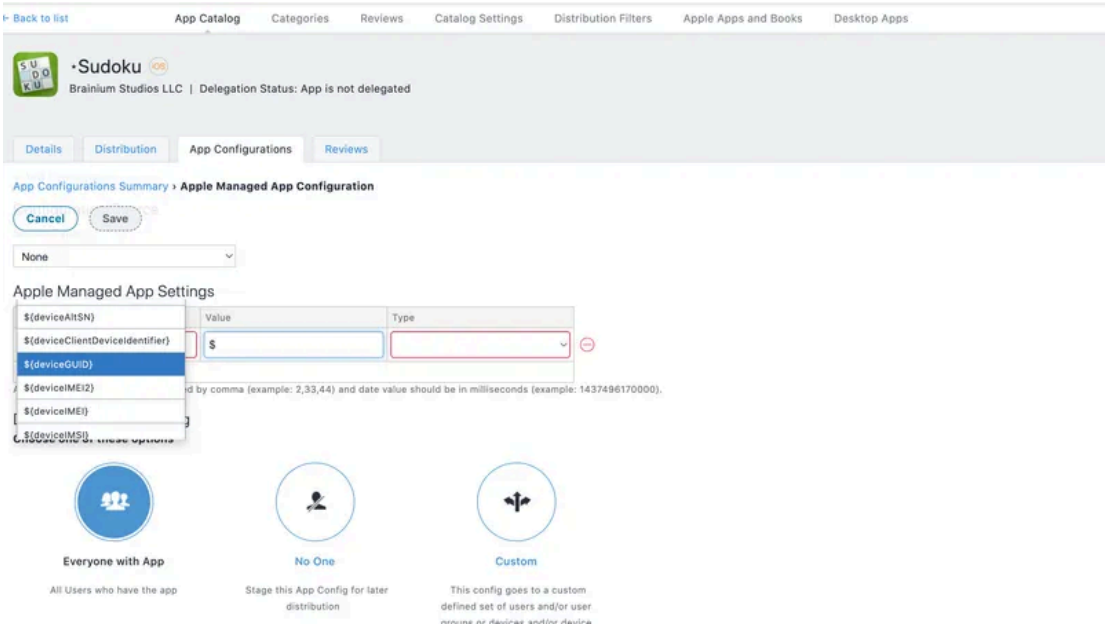


Variable key	Value description
$	department attribute (requires Entra ID)
$	Electronic Data Interchange-Personal Identifier
$	User's Managed Apple ID
$	sAMAccountName attribute (requires Active Directory)
$	Common Name (CN) attribute extracted from the distinguished name (requires LDAP)
$	Display name
$	Distinguished Name (requires LDAP)
$	The domain part of the email address (part after '@')
$>	The local part of the email address (part before '@')
$	Email address
$	Forename
$	Surname
$	Locale
$	Organisational Unit (OU) attribute extracted from the distinguished name (requires LDAP)
$	Kerberos Realm information (requires Active Directory)
$	The domain part of the login ID (the part after '@')
$	The local part of the login ID (the part before '@')
$	Login ID (email address format)
$	userPrincipalName attribute (requires Active Directory)

Supported device variables

Use device variables to specify information about a mobile device.

Device Variables


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

Variable key	Value description
$	Date client last checked-in (most recent checkin - either MDM or Client)
$	Alternative Serial Number
$	Identifier used by the client application
$	Globally unique device identifier
$	ICCID
$	IMEI2
$	IMEI
$	IMSI
$	Date device last checked-in (most recent checkin - either MDM or Client)
$	Internal device identifier
$	Identifier used for MDM
$	MEID
$	Model
$	Device name
$	Device phone number
$	Cluster unique device identifier
$	Serial Number
$	iOS UDID
$	Wi-Fi MAC Address

Email template variables

Variable key	Value description
$	Email body
$	Email subject

Time stamp variables

Variable key	Value description
$	Current timestamp (milliseconds since the epoch)

Policy template variables

Variable key	Value description
$	Policy name violated
$	Next Tiered Compliance Action (different than wait and retire) to be taken after send message
$	Count of days device has been in non-compliant state
$	Time stamp when policy violation was first triggered (UTC DD-MM-YYYY format)
$	Rule definition (query string the way it appears now)

Related topics:

- Attributes

10.10.3. AppConnect Configurations

This section contains the following topics:

- AppConnect Overview
- AppConnect Passcode

10.10.3.1. AppConnect Overview

AppConnect is a feature that containerizes apps to protect data on iOS and Android devices. Each AppConnect-enabled app becomes a secure container whose data is encrypted, protected from unauthorised access, and removable. Because each user has multiple business apps, each app container is also connected to other secure app containers. This connection allows the AppConnect-enabled apps to share data, like documents. Ivanti Neurons for MDM uses policies to manage the AppConnect-enabled apps.

For more information about AppConnect and how to configure and deploy AppConnect apps, see the *AppConnect Guide for Ivanti Neurons for MDM*.

Status of Secure Apps

From the **Devices > Devices** page, click a device to view the **Overview** page. On this page, users can check the status of secure apps with the following information:

- **Secure Apps Status** - Indicates whether AppConnect is enabled or disabled.
- **Secure Apps Encryption Status** - Indicates whether AppConnect passcode is enabled or disabled.
- **Secure Apps Encryption Mode** - Indicates the encryption mode (such as AES 256).

In addition, these fields can be used:

- As filters (left pane) to narrow the device entries displayed when users are trying to find/filter devices.
- As rules while creating a dynamically managed device group.
- As distribution filters, which refine the devices that apps will get distributed to based on defined rules.

For each secure app, administrators can review Container Policy and Configuration statuses (Installed, Applied, Sent, or Pending Install) in the **Configurations** tab of the device details page.

10.10.3.2. AppConnect Passcode

This section contains the following topics:

- Changing/Resetting a passcode
- Generating a one-time PIN for resetting a secure apps passcode for iOS devices

You can require an AppConnect passcode, also known as the secure apps passcode. With a single login with the AppConnect passcode, the device user can access all the secure apps. On the Admin Portal, you configure the rules for the AppConnect passcode. The AppConnect passcode is not the same as the passcode used to unlock the device.

Changing/Resetting a passcode

Users can change or reset the secure apps passcode in the Secure Apps Manager app for Android devices and in the Go for iOS app, provided it has been allowed in the AppConnect configuration. For iOS devices:

Procedure

1. Open the Go for iOS app.
2. Click **Secure Apps**.
3. Click **Authentication**.
4. Click **Change Secure Apps Passcode** and follow the instructions to change/reset the passcode.

For Android devices:

1. Open the Secure Apps Manager app.
2. Click **Change Passcode** in the options menu.
3. Click **Forgot Password** to reset the passcode.

Generating a one-time PIN for resetting a secure apps passcode for iOS devices

Administrators can configure Ivanti Neurons for MDM to allow iOS device users to reset their secure apps (AppConnect) passcode when they forget it. When you have configured this option, device users who registered with Ivanti Neurons for MDM using a user name and password can enter those credentials in Go 3.1.0 for iOS or supported newer versions to authenticate themselves and then reset their secure apps passcode. However, device users who have forgotten the password and PIN need a different mechanism for authenticating themselves.

Procedure

1. On Ivanti Neurons for MDM, the administrator turns on the **Secure Apps Passcode** option in the Default iOS AppConnect Configuration (or in any other iOS AppConnect Configuration).
2. The user generates a one-time PIN for a specific iOS device on the self-service user portal by clicking the **Reset Secure Apps Passcode** option and following the instructions. The one-time PIN is valid for 30 minutes.
3. In Go for iOS on a device, the user follows the instructions for resetting a forgotten secure apps passcode.
4. When prompted for his user credentials, the user enters his user name and the one-time PIN instead of the regular passcode.
5. The user resets his secure apps passcode.

10.10.4. Security Configuration

This section contains the following topics:

- Android Enterprise
- Editing the Android Enterprise default configuration
- Setting up Android Enterprise
- Android Work Challenge
- Certificate configuration
- Certificate Transparency
- Certificate Revocation Checking Configuration
- Create Autonomous Single App Mode Configuration
- Creating DNS Proxy Configuration
- Device Logging configuration
- Disk Management Configuration
- Android Encryption
- Encrypted DNS
- External Intelligence Settings
- Threat Defence
- FileVault 2
- FileVault Recovery Key
- FileVault Options Configuration
- Identity Certificate
- Apple Activation Lock Configuration
- iOS Custom Configuration
- Intelligence Settings
- Keyboard Settings
- iOS Restrictions
- Conference Room Display
- Lockdown & Kiosk: Android Device Admin Mode
- Setting up Kiosk Mode for Android
- Setting up Android shared device kiosk
- Lockdown & Kiosk: Android Enterprise
- Lockdown & Kiosk: Samsung Knox Standard
- macOS Firewall
- macOS Restrictions
- macOS AppStore Restrictions
- macOS Disk Burning Restrictions

- Allowed Media Control (Deprecated)
- macOS Finder Settings
- macOS Kernel Extension Policy
- Mobile@Work for macOS
- macOS Software Update Rules Configuration
- Certificate Preference
- Active Directory (macOS)
- Identity Preference
- Office 365 Auto Account Creation (macOS)
- Authenticate
- Apple App Catalogue
- Managed Domains
- Passcode Configuration
- Privacy Preference (macOS)
- Ivanti Go Client Settings
- Privacy Configuration
- Client Privacy Statement Information
- Safari Extension Settings Configuration
- Software Updates
- Software Update Settings Configuration
- Security Preferences Configuration
- Siri Settings
- Time Server
- Web Content Filter
- Windows Firewall
- Windows Information Protection
- Windows Restrictions
- Windows Desktop restrictions
- Desktop Settings for Windows 10
- Windows Hello for Business Configuration
- Windows AI Management Configuration
- Play Integrity (Previously SafetyNet Attestation)
- Advanced Android Passcode and Lock Screen
- Microsoft Defender for Endpoint
- Certificate-based authentication

10.10.4.1. Android Enterprise

Licence: Silver

An Android Enterprise configuration defines the **Android Enterprise** options enabled for supported devices. You can create alternate configurations for different groups of devices or just edit the default configuration. For a list of devices that support Android Enterprise, see the **Android** official page.

Android Enterprise settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Disable Screen Capture (Android 5.0 +)	Select to prevent devices from using the native screen capture feature.
Disable Apps Control (Android 5.0 +)	Select to prevent users from modifying apps in Settings or Launchers.
Disallow Config Credentials (Android 5.0 +)	Select to prevent users from setting up user credentials.
Disallow Cross Profile Copy / Paste (Android 5.0 +)	Select to prevent devices from copying and pasting to other Android Enterprise work profiles.
Disallow Modify Accounts (Android 5.0 +)	Select to prevent users from adding and removing accounts.
Disallow Outgoing Beam (Android 5.0 +)	Select to prevent users from using NFC to transfer app data.
Disallow Share Location (Android 5.0 +)	Select to prevent websites and apps from prompting the device user to share device location.
Restrict Input Methods (Android 5.0+)	Select to restrict input methods by designating a list of Allowed Package names. If there are no Allowlisted Packages, then only system input methods will be allowed. The input methods are not just restricted to the Work Apps, but to the entire device.
Restrict Accessibility Services (Android 5.0 +)	Select to restrict input methods by designating a list of Allowed Package names. If there are no Allowlisted Packages, then only system accessibility services will be allowed. The input methods are not just restricted to the Work Apps, but to the entire device.
Disable Caller ID (Android 6.0 +)	Sets whether Caller ID information from the work profile will be shown in the device for incoming calls.

Related topics

- Setting up Android Enterprise

10.10.4.2. Apple PassKeys Attestation

Use the Passkey Attestation configuration to configure the device to allow WebAuthn enterprise attestation for certain passkeys.

When the user uses a Passkey to authenticate and register their devices, the Apple Passkey Attestation configuration uses an Enterprise Managed Credential to attest the passkey with a corporate certificate. Supported credentials include SCEP, ACME, and Identity credentials.

The Passkey Attestation supports the following:

- Minimum supported operating system versions: macOS 14
- Supported enrollment methods: Device Enrollment
- Managed Apple Accounts are required to control syncing of passkeys.
- Can be used in conjunction with Access Management from ABM.

> Passkeys payload fails on Mac.

When creating a Passkey Configuration, you must first create an Identity Certificate Configuration, and link that to Passkey Configuration. Also, provide the following details in Security Passkey Attestation Configuration section:

Field	Description
Name	Name of the passkey.
Description	Any information about the configuration.
Attestation Identity Asset Reference • Attestation Identity Key is Extractable	Provide the asset reference identity that you have created to link to the Passkey Configuration. Select this option to confirm if the identity key is extractable.
Relying Parties	Enter the details for authenticated domains.

10.10.4.3. App Privacy Defaults

Use the **App Privacy Defaults** to define default privacy permissions for apps on supervised devices. Administrators can identify the privacy components an app uses, list the app and its components in the configuration, and set privacy defaults. When users launch the app, the app checks the configured privacy defaults and prompts users to grant permissions, while allowing them to defer or manage permissions later in device settings.

Applicable to:

- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- macOS 15.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **App Privacy Defaults** configuration.
3. In the **Name** field, enter text that identifies the configuration.
4. In the **Description** field, enter a description that clarifies the purpose of this file.
5. In the **Configuration Settings** pane, select **Add by Lookup**.
6. Enter the app name for which you want to configure **App Privacy Defaults** by selecting one of the following options:

- iOS Store
- App Catalogue
- visionOS Store
- OS X Store (macOS)

> You can select multiple apps.

7. (Optional) Select **Add Manually** to select an app.
8. (Optional) Enter the **Package Name** of the app.
9. (Optional) Click **Add App**.
10. Select **View App**.

The **View App** pane lists all the selected applications.

11. Click **Add Defaults** on each application to individually configure the App Privacy Defaults.

The **Add Defaults** pane appears.

12. Select the **Defaults** and **Restrictions** as per the following table:

Default	Restrictions
Camera	Select one of the following options: • Allow • None
Bluetooth	Select one of the following options: • Allow • None
Accessibility	Select one of the following options: • Allow • None
Dictation	Select one of the following options: • Allow • None
Microphone	Select one of the following options: • Allow • None
Location	Select one of the following options: • While Using • None • Always
Location Accuracy	Select one of the following options: • Approximate • Precise • None
Local Network	Select one of the following options: • Allow • None
Organization Justification	The **Organization Justification** prompt may display the organization name, app name, administrator-provided justification, and details for each component with a recommended privacy default. If the user selects **Allow**, the system applies to the recommended privacy defaults. If the user selects **Not Now**, consent prompts appear when the app accesses the specified components in the user's device.

13. Click **Save**.
14. Click **Next** to configure the distribution settings.
15. Select one of the distribution options to set up the **App Privacy Defaults** configuration. For more information about configuring distribution options, see **Working with Configurations**.
16. Click **Done**.

10.10.4.4. Editing the Android Enterprise default configuration

Global Administrators can allow space administrators to edit the distribution for any of the following Android Enterprise default configuration in custom space.

- Android Enterprise: Work Profile on Company Owned Device (Android for Work)
- Android Enterprise: Work Managed Device (Android for Work)
- Android Enterprise: Managed Device with Work Profile
- Android enterprise: AOSP

Edit the distribution for any of the above configurations

Procedure

1. In the Configurations tab, select the configuration to be edited.
2. Click on the Edit icon.
3. Click **Next**
4. Select any of the following distribution levels to edit and configure from the distribution page:
    - **All Devices**: Select one of the following options to distribute the configuration to all compatible devices:
        1. Do not apply to other spaces
        2. Apply to devices in other spaces.
    - **No Devices** (default)
    - **Custom**: Select one of the following options to distribute the configuration to all compatible devices or users:
        1. **User/User Groups**: Select the checkbox next to the users or user groups. Alternatively, you can type and search for the users or user groups.
        2. **Device/Device Groups**: Select the checkbox next to the devices or device groups. Alternatively, you can type and search for the devices or device groups.
           In the **Distribution Summary**, select one of the following options to enable or disable configurations across spaces:
            - Do not apply to other spaces.
            - Apply to devices in other spaces.

            > The checkbox **Allow Space Admin to Edit the Distribution** appears if you select the **Apply to devices in other Spaces** option, and it allows the delegated space administrators to edit the distribution for the specific space.

> If you edit the distribution option, you must select the checkbox "**I understand changing distribution of Android Enterprise-Device Mode Configuration can cause devices to retire or wipe if the configuration is removed from existing devices**."

5. Click **Done**.

When this configuration is applied to spaces, the Space administrators will be able to edit the distribution by clicking the distribute icon in custom space.

10.10.4.5. Setting up Android Enterprise

This section contains the following topic:

- Supported Devices
- Connecting Ivanti Neurons for MDM with Android Enterprise
- Getting Your Android Enterprise Credentials
- Adding your Android Enterprise MDM Token to Ivanti Neurons for MDM
- Synchronizing user between Ivanti Neurons for MDM and Google
- Active Directory/LDAP Users
- Local Users
- Deploying Android Enterprise to Supported devices
- Retiring Registered Devices
- Deploying the device
- Confirming Deployment
- Deploying Android Enterprise Apps
- Configuring Business Apps

Licence: Silver

Android Enterprise is a program offered by Google that enables mobility administrators to:

- Separate work and personal data
- Secure and manage enterprise apps
- Control system apps (such as Camera and Gallery)
- Centrally provision and configure apps in the Android Enterprise container
- Prevent data loss (screen capture)

You can configure Ivanti Neurons for MDM as the UEM server that manages Android Enterprise. Android Enterprise requires at least Android 3.0. There are two supported configurations of Android Enterprise, Device Owner and Managed Profile – Employee Owned.

Supported Devices

Ivanti Neurons for MDM currently supports Android Enterprise only on devices that are running Android 5.0 and have Android Enterprise enabled by the manufacturer. Android enterprise is required for Kiosk mode on devices running Android 5.0.

Prerequisite

If you have not already registered your domain with Google, you must first sign up for the program on the Google website:

https://admin.google.com.

During the process you will:

- Claim a domain (must match the domain for user email addresses)
- Receive a token
- Download a JSON client ID

Both items are required when you set up Android Enterprise on Ivanti Neurons for MDM.

After the process, you will receive an email containing instructions for verifying that you own the domain you claimed.

If the company has already used its domain name to sign up for Google Apps for Work, see https://support.google.com/work/android/answer/6174062 for information on enabling Android Enterprise.

Connecting Ivanti Neurons for MDM with Android Enterprise

Once you have signed up for Android Enterprise, set up Ivanti Neurons for MDM as the UEM server.

Getting Your Android Enterprise Credentials

Procedure

1. Go to **Admin > Android Enterprise**.
2. Click **Google Developers Console**.
3. Click the first displayed link to go to the Google Developers Console.
4. Select **Create a project** from the drop-down menu.
5. Enter a name for the project.
6. Accept the terms of service.
7. Click **Create**.
8. Click **API**.
9. Select **APIs**.
10. Type **emm** in the Search field to find the Google Play EMM.
11. Click the **Google Play EMM API** link.
12. Click **Enable API**.
13. Click **Credentials**.
14. Select **Service account**.
15. Click **Create** to save the JSON file.

Adding your Android Enterprise MDM Token to Ivanti Neurons for MDM

Procedure

1. Log into https://admin.google.com.
2. Click **Security**.
3. If you do not see Android Enterprise Settings, click **Show More**.
4. Select **Android Enterprise Settings**.
5. Under **Manage enterprise mobility management provider**, copy the MDM token.
6. Return to the Ivanti Neurons for MDM portal.
7. Click **Done**.
8. In box 2, paste the MDM token you just copied.
9. In the **Domain** field, enter the domain you claimed with Google.

10. Click **Choose File** and upload the JSON file you downloaded.
11. Click **Connect**.
    The message **Connected to Google** displays when the connection is successful.
12. In box 3 click **Authorise** to indicate that you want to give Ivanti Neurons for MDM access to your Google user data.
13. Click **Accept**.
    The message **Connected to Users** displays in the Ivanti Neurons for MDM portal.

Synchronizing user between Ivanti Neurons for MDM and Google

Before you deploy Android Enterprise to Android users managed by Ivanti Neurons for MDMIvanti Neurons for MDM, each user must have a corresponding record on the Google Admin Portal. The steps required for synchronizing the user information between Ivanti Neurons for MDM and the Google Admin Portal depend on whether you have set up an integration with your organisation's directory services (AD/LDAP).

Active Directory/LDAP Users

If you have set up an AD/LDAP integration with Ivanti Neurons for MDM, then you must use Google Apps Directory Sync set up an AD/LDAP integration with the Google Admin Portal. See **https://support.google.com/a/answer/106368?hl=en** for more information.

Local Users

If you created only local users in Ivanti Neurons for MDM and do not intend to integrate it with a directory service, then complete the following steps to synchronise those users with the Google Admin Portal:

Procedure

1. Log into the Google Admin Portal at **https://admin.google.com**.
2. Click **Users**.
3. Click the **Add user** or **Add multiple users** icon in the lower right corner.
4. For each Ivanti Neurons for MDM user that will use Android Enterprise, add a Google user with the same username and email address as the Ivanti Neurons for MDM user.
5. In the Ivanti Neurons for MDM portal for each Ivanti Neurons for MDM user that was just added to the Google Admin Portal:
   a. Click the username link in the Users tab to display the user's details.
   b. Select **Sync the User with Google User Directory**.
   c. Click **Sync with Google User Directory**.
   d. Confirm that Google Status is listed as Enabled.

Deploying Android Enterprise to Supported devices

Two configurations are required for deploying Android Enterprise:

- The Android Enterprise: Work Profile on Company Owned Device configuration enables Android Enterprise.
- A Lockdown & Kiosk configuration defines the Android enterprise restrictions to apply.

Retiring Registered Devices

In BYOD scenarios, moving from Device Admin to Android Enterprise Work Profile on Company Owned Device does not require a retire and re-enrol of devices. A device wipe or retire is required only for moving from Device Admin to Device Owner mode.

When you select a device enrolled in Device Owner / Enhanced Profile Owner / Company-Owned Personally Enabled modes for Retire action, a pop-up appears on the screen indicating that the "Retire command is not supported for devices which are organisationally owned."

Deploying the device

Procedure

1. In the Ivanti Neurons for MDM portal, go to **Configurations**.
2. Click **Android Enterprise: Work Profile**.
3. Click **Edit**.
4. Click **Next**.
5. Select **All Devices** or **Custom**.
6. If you selected **Custom**, search for and select the device groups that should receive the Android for Work settings.
7. Click **Done**.
8. Click **Back to list** (upper left corner).
9. Click **+Add**.
10. Click **Lockdown & Kiosk: Android Enterprise**.
11. In the **Name** field, enter text that identifies the configuration.
12. Under **Choose Lockdown Type**, select **Work Profile**.
13. Select the lockdown settings you want to apply to the target devices.
14. Click **Next**.
15. Select **All Devices** or **Custom**.
16. If you selected Custom, search for and select the device groups that should receive the Android Enterprise settings.
17. Click **Done**.

> You cannot make changes to the resulting profile once it has been deployed. Instead, you need to create a new Android Enterprise configuration and deploy it.

Confirming Deployment

You can confirm that Android Enterprise has been deployed in the following ways:

- Under **Users > Users**, find the entry for a user, and then check that the **Google Status** is **Enabled**.
- Under **Devices > Devices,** click the link for a device, and then check that status for **Android Enterprise** is **Enabled**.

Google Status for a user should be listed as **Enabled**. If it is not Enabled, then the user will not be able to register devices.

> For enterprises that are not GSuite subscribers, managed Google Play Accounts method allows users to be enrolled with Android Enterprise. If Android Enterprise was set up as managed Google Play Accounts, then the user is not shown as **Google Status: Enabled** until after an Android Enterprise device is registered. See **Managed Google Play Accounts** for more information about managed Google Play Accounts.

Deploying Android Enterprise Apps

Any app developed for Android Enterprise may include options that you can configure through Ivanti Neurons for MDM.

Procedure

1. In the Ivanti Neurons for MDM portal, go to **Apps >App Catalog**.
2. Find the app in the Google Play Store.
3. Click the app entry.
4. Accept permissions on behalf of Android Enterprise users.
5. Click **Next**.
6. Select a distribution option.
7. Expand **Advanced Options & App Configuration**.
8. Use the following guidelines to complete the options:
9. Click **Next**.

Setting	Description
Install on Device	Select this option to start installation immediately after registration. The user will be prompted to confirm installation of the app except when the device is a Samsung Knox device and the silent installation option below has been selected.
Do not show app in end user App Catalogue	Select this option if you do not want the user to see the app in the app catalogue on the device.
Silently install on Samsung Knox devices	Select this option if you do not want the user prompted to confirm installation on Samsung Knox devices.
Set App Install Priority	For Android Enterprise apps you can prioritize downloading of specific apps before other apps. For example, you can prioritise the download of Tunnel and Email apps before other non-critical apps. The following are the available priority level options: • **High** • Medium (selected by default) • **Low** This setting is applicable for In-House, Public, Private, and Web apps. The in-house apps are installed via the client and the public and private are installed via Google. The app priority is applied only to those apps that are installed via the same channel.
Install only when connected to Wi-Fi	Select this option to install the app only when the device is connected to the Wi-Fi.
Install only when charging	Select this option to install the app only when the charging of the device is in progress.
Install only when idle	Select this option to install the app only when the device is in idle (not actively used by the user).
Auto-launch on install	Select this option to launch an app automatically after installation. This functionality is available only if the app is newly installed on the device and not for a version update.

10. Select a promotion option.
11. Click **Done**.

Configuring Business Apps

Android Enterprise apps are available in the Business Apps section of the app catalog, including the following apps:

- Divide Productivity
- Email+
- Tunnel
- GMail

10.10.4.6. Android Enterprise: Work Managed Device Non-GMS mode (AOSP)

Ivanti Neurons for MDM supports Device Owner registration of Work Managed Device Non-GMS mode (AOSP) devices without the need for Google Mobile Services (GMS). It is a system configuration and administrators cannot add the configuration. Admins can distribute or undistribute it.

Procedure

1. Log in to Ivanti Neurons for MDM with user credentials.
2. Search Configurations for Android Enterprise: Work Managed Device Non-GMS mode (AOSP).
3. Edit the configuration and distribute it to the appropriate device groups. For example: Android Devices.
4. Click **Done**.

10.10.4.7. Android Work Challenge

This section contains the following topic:

- Creating the Android Work Challenge configuration:
- Configuration Setup settings

Licence: Silver

An Android Work Challenge configuration defines secure passwords for users to access the Work Profile data and apps. Requires Android Enterprise Work Profile.

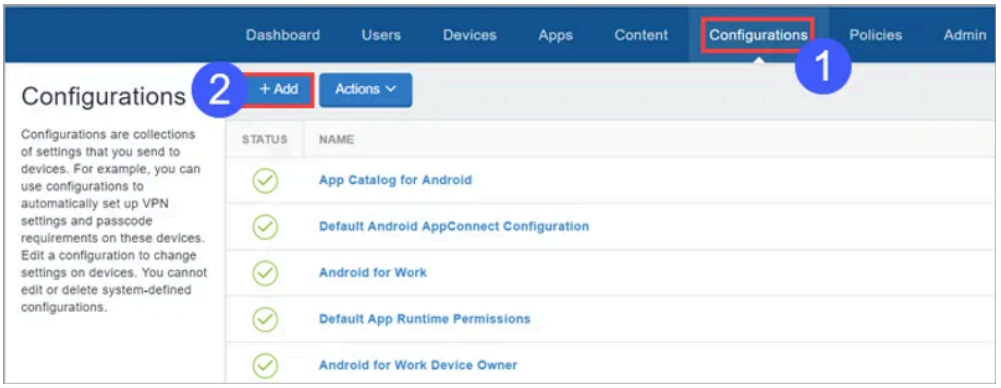
Implementation notes:

- Administrators can apply a device password policy and a work profile password policy independently.
- Ivanti Neurons for MDM does not send this configuration to clients earlier than Android 7.0 because such devices do not support this feature.
  Ivanti Neurons for MDM only sends this configuration to devices with an Android Enterprise Work Profile.

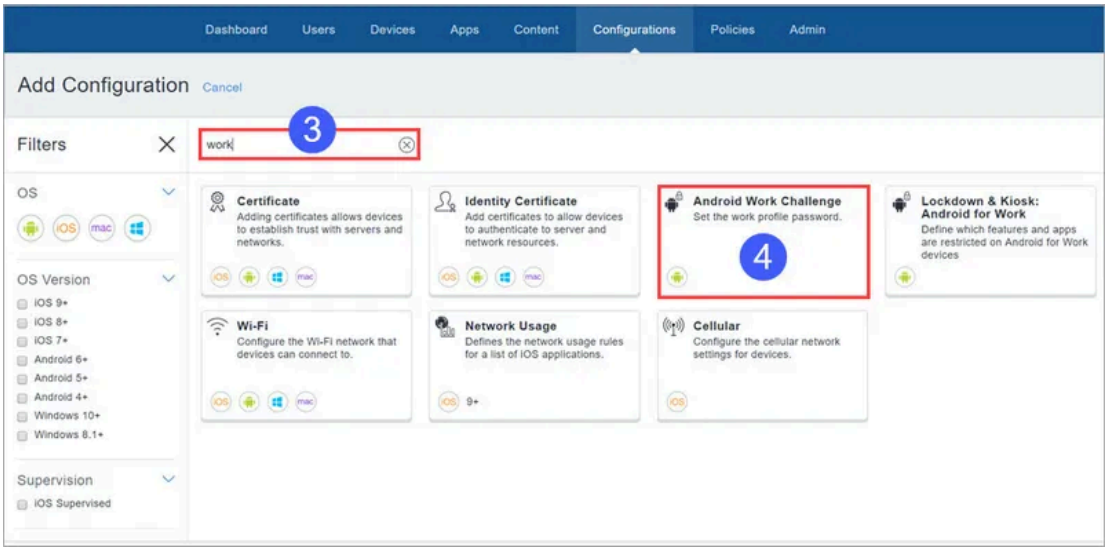
Creating the Android Work Challenge configuration:

Procedure

1. Click **Configurations**.

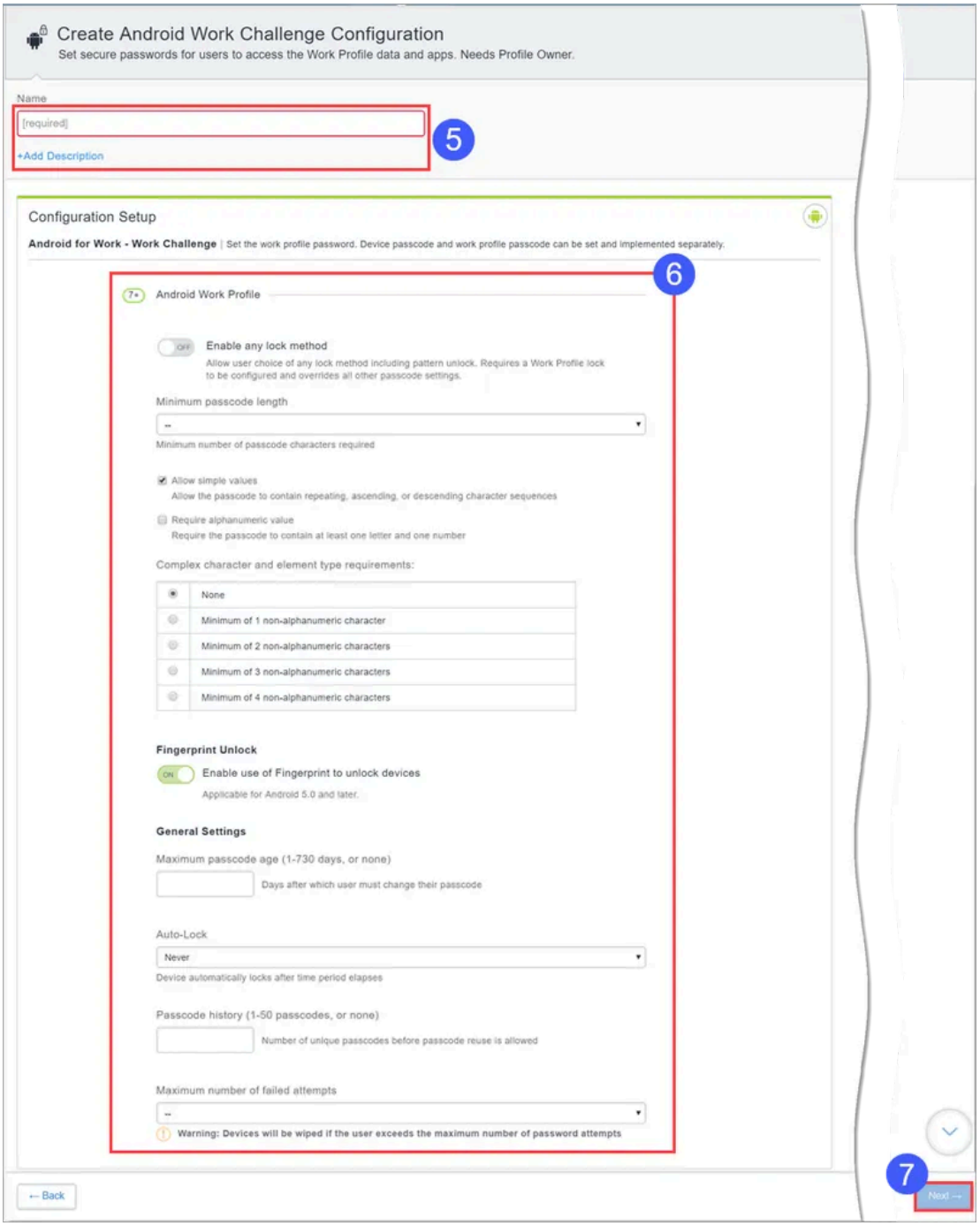


Click **+Add**.



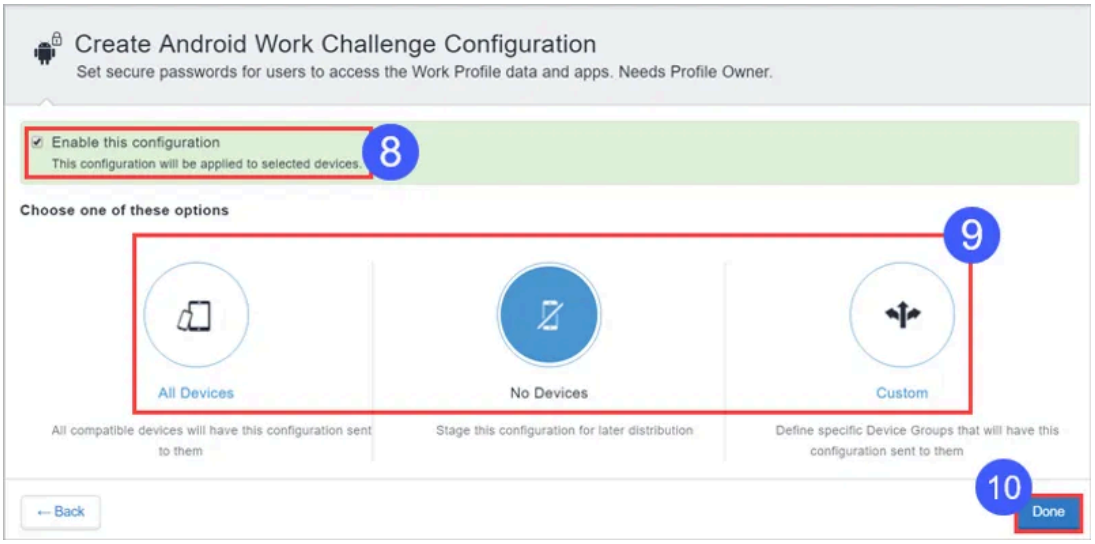
Type "Work Challenge" in the search field.

4. Select the **Android Work Challenge** configuration.



Enter a name for the configuration, and, optionally, a description.

6. Use the Configuration Setup fields to create the configuration. Refer to **Configuration Setup settings** for details on the settings.
7. Click **Next →**.



Enable the configuration if desired.

9. Configure distribution settings, to all devices, no devices, or to a custom set of devices.
10. Click **Done**.

Configuration Setup settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Enable any lock method	Allow user choice of any lock method, including pattern unlock. Overrides all other passcode settings.
Minimum passcode length	Select a minimum passcode length, from 4 to 16 characters.
Allow simple values	Enable to allow the passcode to contain repeating, ascending, or descending character sequences.
Require alphanumeric value	Enable to require the passcode to contain at least one letter and one number.
Complex character and element type characteristics	Configure complex character and element type requirements, ranging from: • None • Minimum of 1 non-alphanumeric character • Minimum of 2 non-alphanumeric characters • Minimum of 3 non-alphanumeric characters • Minimum of 4 non-alphanumeric characters
Fingerprint unlock	Enable to allow users to unlock their devices with their fingerprint.
Maximum passcode age	Configure a maximum password age, from none to 730 days.
Auto-lock	Select a time period after which the device auto-locks. Times range from never to fifteen minutes.
Passcode history	Specify the number of unique passcodes required before passcode reuse is allowed, ranging from none to 50 passcodes.
Maximum number of failed attempts	Select the maximum number of failed attempts. **WARNING: Ivanti Neurons for MDM wipes devices for which the user exceeds the maximum number of password attempts!**

10.10.4.8. Certificate configuration

A certificate configuration identifies a certificate to be distributed to devices. Certificates enable devices to establish trust with server and network resources. Starting with release 76 we support only v3 certificates.

As an administrator, you can now generate Ivanti Neurons for MDM certificate for smart card logon and custom object IDs (OIDs). You can generate certificates for the following authentication options:

- Client Authentication - enabled by default
- IPSEC – optional, admin can enable
- Smart Card Logon – optional, admin can enable
- Custom OIDs - optional, admin can enable

> This feature is only applicable for the following certificate authorities (CA):

- Local Certificate Authority
- Intermediate Certificate Authority
- External Certificate Authority - configure the application policies of CA template in NDES server to support IPSEC , Smart Card Logon and custom OIDs
- On-premise SCEP Certificate Authority

Distributing the configuration

Starting from Ivanti Neurons for MDM release 91, global administrators can delegate space administrators to edit the Certificate Configuration for All Devices and for the Custom distribution option. For the certificate config, you can optionally select the Allow this configuration to be available in all Spaces option. This option makes Certificate config available to all Spaces and can be used in Exchange, Wifi, VPN, Per-App VPN and any other applicable configurations. This option can be used in scenarios where certificate config is only needed to be distributed to devices (in non default Spaces) as part of associated configurations and not to be distributed as an individual configuration.

Procedure

1. Enter a name in the Name field.
2. Upload the certificate file.
3. Click **Next**.
4. Select the **Enable this configuration** option.
5. Select one of the following distribution options:
    - **All Devices**. Select one of the following options:
        - **Do not apply to other spaces**.
        - **Apply to devices in other Spaces**.
            - Select **Allow Space Admin to Edit the Distribution** check box to allow the delegated space administrators to edit the distribution for the specific space.
    - **No Devices** (default)
    - **Custom** Select one of the following options:

10.10.4.9. Certificate Transparency

Applicable to: iOS 12.1.1, macOS 10.14.2, tvOS 12.1.1, watchOS 10.0+, visionOS 1.1+, and supported newer version.

Controls Certificate Transparency enforcement which can only appear in a device profile. You can include multiple certificates and disable domains as needed.

Creating a Certificate Transparency configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **certificate** in the search field, and then click the **Certificate Transparency** configuration.
4. Enter a name and describe the configuration.
5. Specify the **Domains that will be disabled**. Click **+ Add Domain** to add more than one domain. A leading period can be used to match subdomains, however a domain matching rule must not match all the domains within a top level domain. For example, ".example.com" and ".example.co.uk" are allowed while ".com" and ".co.uk" are not allowed. Wildcard domains are not supported.
6. Specify **Certificate Hash** after selecting an algorithm (SHA 256). Click **+ Add** to add more than one certificate hash.
7. Click **Next** to configure the distribution settings.
8. Click **Done**.

To generate the data specified by the Hash key in the subjectPublicKeyInfo dictionary, use the following command for a PEM-encoded certificate:

```
openssl x509 -pubkey -in example_certificate.pem -inform pem | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

If your certificate is DER-encoded, use the following command:

```
openssl x509 -pubkey -in example_certificate.der -inform der | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

For more information, see **How to create a configuration**.

10.10.4.10. Certificate Revocation Checking Configuration

This configuration allows the administrators to check an array of certificates revoked from a device. Administrators can specify a certificate authority (CA) which allows the configuration to enable revocation checking for all the certificates which are linked to that CA.

Applicable to: iOS 14.2+ and visionOS 1.1+

Procedure

1. Go to Configurations > +Add.
2. Type certificate in the search field, and then click the Certificate Revocation Checking configuration.
3. Enter a Name and Description of the configuration.
4. Select algorithm as SHA 256 and enter the Hash of the root certificate.

> In Hash, you have to enter a Base64 encoded (binary) SHA-256 hash of the certificate's public key. See **Apple documentation** for the available trusted root certificates for Apple operating systems. You can add multiple root certificates in this configuration.

5. Click Next.
6. Select Enable this configuration option.
7. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
8. Click Done.

10.10.4.11. Create Autonomous Single App Mode Configuration

The Autonomous Single App Mode configuration lets you ensure that only specific applications run on a device. Even if the user attempts to launch a different application, the configuration launches only the specific application.

Procedure

1. Go to **Configurations** > **Add** > **Autonomous Single App Mode**.
2. Use the following guidelines to define the app and related settings.
3. Click **Next**.

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Configuration Setup	**Bundle Identifier** - (Required) The unique bundle identifier. If two dictionaries contain the same BundleIdentifier value but a different TeamIdentifier value, this will be considered an error and the profile won't be installed.
	Team Identifier - (Required) The developer's team identifier, used when the app was signed.

4. In the **Distribution** screen, select the groups to receive this configuration.
5. Click **Done**.

10.10.4.12. Creating DNS Proxy Configuration

As the Ivanti Neurons for MDM administrator, you can configure DNS Proxy settings using the DNS Proxy Configuration for users of iPhone and iPad devices. You can use the DNS Proxy payload to specify the application that provides the DNS proxy network extension and other vendor-specific values.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Go to **Configurations**
3. Type **DNS** in the search field, and click **DNSProxy Configuration**.
4. Enter a name and describe the configuration.
5. Enter the following DNS Proxy Configuration settings:
    - App Bundle Identifier (Required).
    - Provider Bundle Identifier.
    - Provider Configuration (Key-Value).
6. Click **Next**.
7. Select the **Enable this configuration** option.
8. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom

Click **Done**.

10.10.4.13. Device Logging configuration

The Device Logging configuration allows you to enable network and security logs for Android devices.

Creating a Device Logging configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. In the search field, type **Device Logging** and select the configuration.
4. Enter a name and describe the configuration.
5. Under the **Configuration Setup** section, select one or both options:
    - Enable Network Logging
    - Enable Security Logging

> For information on supported Android versions for Security and Network logging, refer to the tables under **Security Logging matrix** below.

Click **Next** to configure the distribution settings.

7. Click **Done**.

Security Logging matrix

Device type	Supported Android versions
Work Managed Devices and Work Managed Device Non-GMS mode (AOSP)	7, 8, 9, 10, 11, 12, 13
Managed Devices with Work Profile	8, 9, 10
Work Profile	NA
Work Profile on Company Owned Device	11, 12, 13

Network Logging matrix

Device type	Supported Android versions
Work Managed Devices and Work Managed Device Non-GMS mode (AOSP)	8, 9, 10, 11, 12, 13
Managed Devices with Work Profile	8, 9, 10
Work Profile	12, 13
Work Profile on Company Owned Device	12, 13

After installing the Device Logging Configuration on the device, the user gets a notification which has info about the Device management and Network logging. Click **OK** to acknowledge the notification.

Requesting Debug Logs

Procedure

1. Log in to the Ivanti Neurons for MDM.
2. Go to **Devices** > **Device details**.
3. From the **Overview** section, click on the three vertical dots button next to the **Force Checkin** button.
4. Select **Request Debug Logs**.
5. Select one of the following two options:
    - Exclude Bug report - When you select this option and click Next, a confirmation window appears on the screen. Click **Request Debug Logs**. Users do not have to provide any consent for this option, and these logs would exclude bug report for the selected Android devices.
    - Include Bug report - When you select this option and click Next, a confirmation window appears on the screen. Click **Request Debug Logs**. Users must provide consent for sharing the bug report. In the case of Android devices, users will be prompted to submit the device logs, to include bug report.

10.10.4.14. Disk Management Configuration

Ivanti Neurons for MDM Disk Management configuration settings define the policies for effectively managing data in external and network storage devices.

Applicable to: macOS 15.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Disk Management** configuration.
3. Configure the **Disk Management** settings as per the following table:

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Disk Management	
External Storage	Select one of the following values from the drop-down list: • **Allowed**: Allows reading and writing of the storage. • **Read Only**: Allows to read the storage. • **Disallowed**: It doesn't allow access to the storage.
Network Storage	Select one of the following values from the drop-down list: • **Allowed**: Allows reading and writing of the storage. • **Read Only**: Allows to read the storage. • **Disallowed**: It doesn't allow access to the storage.

4. Click **Next** to configure the distribution settings.
5. Select one of the distribution options to set up the **Disk Management** configuration. For more information about configuring distribution options, see **Working with Configurations**.
6. Click **Done**.

10.10.4.15. Android Encryption

An encryption configuration defines device encryption requirements for Android devices in Device Admin mode. Device encryption ensures that sensitive corporate data cannot be accessed by known jailbreak or root exploits. Encryption stores the device's data in an unreadable form so that anyone who might steal the device cannot access the data.

Enabling encryption prompts the device user to encrypt the device and requires setting a device passcode. The passcode is what decrypts the data so that you can read it. Device encryption is automatically enabled on Android enterprise (work profile or managed devices) or iOS devices when a passcode is set. The device cannot be used while it is being encrypted. Once encryption is on, turning it off requires a factory reset of the device.

Encryption settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Enable Device Encryption	Select the setting to turn on encryption for all encryption-capable Android devices that receive this configuration.

> Android Encryption Configuration is deprecated for Samsung devices in Device Admin mode on Android 11. This encryption is supported by default on Android Enterprise devices when a device passcode is set.

For more information, see **How to create a configuration**.

10.10.4.16. Encrypted DNS

Licence: Gold

Applicable to:

- iOS 14.0 or supported newer versions.
- macOS 11.0 or supported newer versions.
- visionOS 1.1 or supported newer versions.

Configure Encrypted DNS that will allow you to enhance security without needing to configure VPN.

This section contains the following topics:

- Encrypted DNS configuration
- Encrypted DNS configuration settings

Encrypted DNS configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **DNS** in the search field, and then click the **Encrypted DNS** configuration.
4. Enter a name and describe the configuration.
5. Enter the Encrypted DNS configuration settings.
6. Click **Next**.
7. Select the **Enable this configuration** option.
8. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
9. Click **Done**.

Encrypted DNS configuration settings

Use the settings in the following table to configure Encrypted DNS. For more information about these settings, see Apple documentation.

Setting	Description
DNS Settings	A dictionary that defines a configuration for an encrypted DNS server.
DNS Protocol	Specify the encrypted transport protocol used to communicate with the DNS server. Select one of the following protocols: • HTTPS • TLS
Server URL	The URI template of a DNS-over-HTTPS server, as defined in RFC 8484. This URL must use the https:// scheme, and the hostname or address in the URL will be used to validate the server certificate. If no Server Addresses are provided, the hostname or address in the URL will be used to determine the server addresses. This key must be present only if the DNS Protocol is HTTPS.
Server Addresses	An unordered list of DNS server IP address strings. These IP addresses can be a mixture of IPv4 and IPv6 addresses. Click **Add** to add one or more server addresses.
Supplemental Match Domains	A list of domain strings used to determine which DNS queries will use the DNS server. If this array is not provided, all domains will use the DNS server. Click **Add** to add one or more domains.
Prohibit users from disabling DNS Settings	Prohibits users from disabling DNS settings. This key is only available on supervised devices.
Demand Rules	An array of rules defining the DNS settings. If rules are not present, the system always applies the DNS settings. Click **+ Add Demand Rules** to add one or more sets of demand rules.
Network	The action to take if this dictionary matches the current network. Select one of the following actions: • **Connect:** Apply DNS Settings when the dictionary matches. • **Disconnect:** Do not apply DNS Settings when the dictionary matches. • **Evaluate Connection:** Apply DNS Settings with per-domain exceptions when the dictionary matches.

Evaluate Connection	This network option has the following settings:
	• **Domain Action** - The DNS settings behaviour for the specified domains. Select one of the following actions:
	  ◦ **Never Connect** - Do not use the DNS Settings for the specified domains.
	  ◦ **Connect if Needed** - Allow using the DNS Settings for the specified domains.
	• **Domains** - The domains for which this evaluation applies. Click **+ Add** to add one or more domains.

Rules	Click **+ Add** to add one or more rules to match the following parameters with the corresponding specified values.
DNS Domain Match	An array of domain names. This rule matches if any of the domain names in the specified list matches any domain in the device's search domains list.

Setting	Description
DNS Server Address Match	An array of IP addresses. This rule matches if any of the network's specified DNS servers match any entry in the array.
SSID Match	An array of SSIDs to match against the current network. If the network is not a Wi-Fi network or if the SSID does not appear in this array, the match fails. Omit this key and the corresponding array to match against any SSID.
Interface Type Match	An interface type. If specified, this rule matches only if the primary network interface hardware matches the specified type. Select one of the following types: • Ethernet • WiFi • Mobile
URL String Probe	A URL to probe. If this URL is successfully fetched (returning a 200 HTTP status code) without redirection, this rule matches.

For more information, see **How to create a configuration**.

10.10.4.17. External Intelligence Settings

Use the **External Intelligence Settings** to configure External Intelligence integrations on supervised devices. This configuration helps administrators apply consistent, policy-based settings that control how devices connect and use supported external intelligence services.

Applicable to:

- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- macOS 15.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **External Intelligence Settings** configuration.
3. Configure the **External Intelligence Settings** configuration as per the following table:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Allow External Intelligence Integrations	Select the checkbox to enable External Intelligence Integrations. Toggle the **Push to Device** button to enable External Intelligence Integrations on supervised devices.
Allow External Intelligence Integrations Sign-In	Select the checkbox to enable External Intelligence Integrations Sign In. Toggle the **Push to Device** button to enable External Intelligence Integrations Sign In on supervised devices.
Allow External Intelligence Workspace IDs	Enter the Workspace IDs to enable External Intelligence. Toggle the **Push to Device** button to enable External Intelligence for the entered Workspace ID on supervised devices.

4. Click **Next** to configure the distribution settings.
5. Select one of the distribution options to set up the **External Intelligence Settings** configuration. For more information about configuring distribution options, see Working with Configurations.
6. Click **Done**.

10.10.4.18. Threat Defence

Applicable to:

- Go for iOS client version 3.2.0 or supported newer versions.
- Go for Android client version 52 or supported newer versions.

Ivanti Neurons for MDM includes the ability to distribute activation tokens to enable Threat Defense technology integrated into Go for Android and iOS clients. Threat Defense protects managed devices from mobile threats and vulnerabilities affecting device, network and applications.

When this configuration is enabled in Ivanti Neurons for MDM and applied to the devices, the Threat Defense libraries are enabled on the Go clients. The Threat Defense service can be deactivated by removing the licence token and resending the licence configuration to the client.

Threat Defense monitors:

- On the device level: system parameters, configuration, firmware, and libraries to identify suspicious or malicious activity.
- On the network level: network traffic and suspicious connections to and from mobile devices.
- On the app level: leaky apps (potentially placing enterprise data at risk) and malicious apps, through risk assessment and code analysis.

Latest documentation

For the latest Threat Defense instructions, see the *Ivanti Neurons for MDM Threat Defense Solution Guide* in Product Documentation site at **Ivanti Neurons for MDM product documentation**.

10.10.4.19. FileVault 2

Licence: Gold

FileVault 2 provides the ability to perform full XTS-AES 128 disk encryption on the contents of a volume.

When you Enable FileVault 2, the following settings are available for configuration:

Category	Settings
FileVault User Settings	• Enable FileVault at SetupAssist **Default**: False • If true, and the payload is installed after enrolling with Ivanti Neurons for MDM in Setup Assistant, it requests the Setup Assistant to enable FileVault at setup time. Also, the system ignores all other keys in this payload, except for ShowRecoveryKey. **Prerequisite**:- Before you enable the file vault in the setup assistant, ensure that the **Await Device Configuration during Device Enrollment Setup** is enabled in the Device Enrollment Profile. • Defer enabling FileVault until the designated user logs out ◦ Always prompt user to enable FileVault ◦ Maximum number of times a user can bypass enabling FileVault Do not request enabling FileVault at user logout time
Output Path	Enter the path to the location where the recovery key and computer information plist will be stored.
Personal Recovery Key	• Create a personal recovery key • Display the personal recovery key to the user after FileVault is enabled This option is visible only when **Create a personal recovery key** is enabled. By default the option is disabled. • Enable Institutional Recovery Key: Using Keychain - if no certificate information is provided in this payload the keychain already created at /Library/Keychains/FileVaultMaster.keychain will be used. Select one of the following options: ◦ Upload Certificate ◦ Certificate ◦ Use keychain on the Users System
Rotate FileVault Key after __ days	The admins can configure periodic rotation of FileVault keys for macOS devices to mitigate security risk of the deployed devices. Admins can set the rotation interval in terms of days. Only Personal Recovery Keys are rotated.

10.10.4.20. FileVault Recovery Key

Licence: Gold

FileVault Recovery Key configuration determines redirecting and escrowing the FileVault recovery keys to a corporate server.

> Exclude and Re-push of File Vault Recovery Key configuration is disabled as a macOS device stops sending recovery key on re-pushing the configuration.

You can set the following options:

Setting	Description
Name	Enter a name that identifies this configuration.
Description	(Optional) Enter a description that clarifies the purpose of this configuration.
Configuration settings for macOS <10.13	
Store Recovery key to Ivanti Neurons for MDM Tenant	Select to enable Ivanti Neurons for MDM to store the keys on your tenant. When needed, the key can be decrypted from the Device Details page.
Redirect URL to Server	Enter the following settings: • Enter **Redirect URL** to which FDE recovery keys should be sent instead of Apple. The URL must begin with https://. • Select a Certificate from the dropdown list. Only PKCS1 format certificate is supported.
Configuration settings for macOS 10.13+	
Location	(Required) Enter a short description of the location where the recovery key will be escrowed. This text will be inserted into the message the user sees when enabling FileVault.
Device Key	(Optional) Enter a string to be included in the help text if the user appears to have forgotten the password.

10.10.4.21. FileVault Options Configuration

This configuration allows administrators to enable or disable FileVault and destroy FileVault key when the system goes into standby.

Applicable to: macOS 10.7+

Procedure

1. Go to **Configurations** > **+Add**.
2. Type FileVault in the search field, and then click the FileVault Options configuration.
3. Enter a Name and Description of the configuration.
4. In Configuration Setup, select the required options:
    - Destroy FileVault key when system goes into standby mode
    - Do not allow disabling Full Disk Encryption
    - Do not allow enabling Full Disk Encryption
5. Click Next.
6. Select Enable this configuration option.
7. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
8. Click Done.

10.10.4.22. Identity Certificate

This section contains the following topics:

- Identity certificate settings
- Distributing the configuration

An identity certificate configuration defines a certificate authentication mechanism for mobile devices. Identity certificates are X.509 certificates (.p12 or .pfx). Also, the identity certificates can be generated dynamically using the Certificate Authority as a source. Before beginning, you should already know how you plan to distribute certificates to your mobile devices. You should also have configured any necessary certificate authority.

> Starting from release 91, the Device Identity certificate for Apple devices is automatically renewed within 30 days of expiry. iOS devices receive renewed MDM certificates from Ivanti Neurons for MDM as part of the regular device check-in flow. However, iOS devices need to be re-enrolled with Ivanti Neurons for MDM when they are offline long enough for the MDM certificate to expire before a check-in that would have renewed the certificate before expiration.

- SHA-1 certificates are deprecated while creating the identity certificates. You can choose other algorithms. While updating the certificates, if the older certificates use SHA-1, the same SHA-1 algorithm can be used. If the older certificates use an algorithm above SHA-1, then switching to SHA-1 is not allowed.
- After configuring an identity certificate, you can click **Test Configuration and continue** to issue and verify the validity of the test certificate. An error may display by performing this test for a new or an existing dynamically generated identity certificate configuration if the subject name is the same as the local certificate authority. When this error message is displayed you should modify the identity certificate subject name which should be different from the local certificate authority subject name. For existing identity certificate configurations that are modified with the subject name, the certificates are re-issued and the configurations are re-pushed.
  If you have setup the option to create a configuration without issuing test certificate for **Dynamically Generated** certificate distribution, click **Continue**.
- Certificates will be re-issued implicitly.
- When Identity certificates are assigned to Android apps, the user's app gets Identity certificates without prompting the users to grant the permission (rather than app) to use the certificate. It includes all apps like Email+, Gmail, etc.
- Email+ can be configured with a user provided identity certificate and pushed and assigned as an app configuration to Android Enterprise devices. It is applicable only to Work Profile on Company Owned Device and Device Owner modes.

Identity certificate settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.

Certificate Distribution	Select the type of certificate distribution to set up:
	• **Single File**: Upload an existing certificate for distribution to devices.
	• **Dynamically Generated**: Create certificates on request using a local or external certificate authority.
	• **User provided**: Create labels for the type of certificates to be uploaded by the user. When created, the user will be able to see the created labels (options) in the self-service portal, and upload certificates corresponding to these labels.
	• **Derived Credential:** Specify one of the following usages for the derived credential:
	  ◦ Authentication
	  ◦ Encryption
	  ◦ Signing
	  ◦ Decryption
	• **SCEP Config**: Specify how to request a certificate from a SCEP server. Select one of the following configurations:
	  ◦ Apple Config
	  ◦ Windows Config
	  Your selection determines which options display in the rest of the form.

Allow All Apps to access Private Key (macOS 10.10+) Single File	**Applicable to:** Single file, Dynamically Generated, User Provided, and SCEP Apple Config identity certificates. (Optional) For PKCS#12 certificates, enable the **Allow All Apps to access Private Key** option to allow all apps access to the private key. For example, this key can be used in cases where a password is requested from the user to allow access to a certificate used for VPN.
Identity Certificate data	Drag the certificate file to the dotted box, or click **Choose File** to select it from your file system.
Password	Enter the password protecting the PKCS#12 certificate file. This password is used for installation without prompting.
Dynamically Generated	
Source Create configuration without issuing test certificate	Select the local certificate authority from the drop-down. You should have already created this CA under **Admin >** Certificate Management. Select the check box to create a configuration without issuing test certificate.

Setting	What To Do
Windows only - Target Certificate Store **User Provided**	Admins can now select the Target Certificate Store on Windows devices.
Certificate Display Name	Enter the name of the certificate. This certificate name is unique for a tenant and the user will be able to see the name in the self-service portal while uploading the certificate.
Delete the Private Key	Select this option to delete the private key of the certificate after *n* (1-30) days. You can also use the APIs provided by Ivanti Neurons for MDM for these operations. Refer to the Ivanti Neurons for MDM *API Guide* for more information about the APIs. If you try to use this certificate in any configuration (for example, to authenticate an application or to push a WiFi or a VPN configuration) after its private key has been deleted, the task will fail. Ensure that the task is performed before the private key is deleted.
Delete the Private Key after Days	Select the number of days (1-30) after which private keys of the certificate are cleared. Default value is 2 days.
Derived Credential	
Derived Credential Usage	Select any of the following options: • **Authentication** - To specify that the derived credential is used for authentication. • **Encryption** - To specify that the usage of the derived credential is for encryption. • **Signing** - To specify that the derived credential is used for signing. • **Decryption** - To specify that the usage of the derived credential is for decryption.
Brand	Select the Derived Credential Provider that you use from the following options: • **Entrust** • **Intercede** • **Purebred** To add custom derived credential providers that you use, see **Derived Credential Providers**.
ACME Config - Applicable only to iOS/iPadOS16+ /macOS14+	
Client Identifier	A unique string identifying a specific device
Directory URL	(Required) The directory URL of the ACME server. The URL must use the https scheme.
Extended Key Usage	The value is an array of strings. Each string is an OID in dotted notation. For instance, [”1.3.6.1.5.5.7.3.2”, “1.3.6.1.5.5.7.3.4”] indicates client authentication and email protection. The device requests this field for the certificate that the ACME server issues. The ACME server may override or ignore this field in the certificate it issues.
Key Size	(Required) The valid values for KeySize depend on the values of KeyType and HardwareBound. See

Setting	What To Do
	those keys for specific requirements.
Key Type	(Required) The type of key pair to generate.
Subject	(Required) Enter an X.500 name represented as a comma-separated array of OIDs and values. Typically, the subject is set to the user's fully qualified domain name. For example, C=US,DC=com,DC=MobileIron,OU=InfoTech or CN=www.mobileiron.com. You can also customise the Subject by appending a variable to the OID. For example, CN=www.mobileiron.com-${{deviceGUID}}. For ease of configuration you can also use the $ variable to populate the Subject with the user's FQDN. Do not use the backslash character () in the subject name.
Subject Alternate Name	The Subject Alt Name that the device requests for the certificate that the ACME server issues. The ACME server may override or ignore this field in the certificate it issues.
Key Usage	This value is a bit field. Bit 0x01 indicates digital signature. Bit 0x10 indicates key agreement. The device requests this key for the certificate that the ACME server issues. The ACME server may override or ignore this field in the certificate it issues.
Hardware Bound	If the Hardware bound is set to true the private key is bound to the device, and only then the Key Type must be ECSECPrimeRandom and Key Size must be 256 or 384.
Attest	If true, the device provides attestations describing the device and the generated key to the ACME server. When Attest is true, Hardware Bound must also be true.
SCEP Config - Apple Config	
Identity Certificate (SCEP)	Select to specify a SCEP server.
Local Certificate Authority	Select to specify a local certificate authority that you have already created under **Admin > Certificate Management**. Select the local certificate authority from the drop-down that appears when you select this option.
URL	Enter the URL for the SCEP server.
CA Identifier	Enter the identifier provided by the certificate authority.
Subject	Enter an X.500 name represented as a comma-separated array of OIDs and values. Typically, the subject is set to the user's fully qualified domain name. For example, C=US,DC=com,DC=MobileIron,OU=InfoTech or CN=www.mobileiron.com. You can also customise the Subject by appending a variable to the OID. For example, CN=www.mobileiron.com-$DEVICE_CLIENT_ID$. For ease of configuration you can also use the $USER_DN$ variable to populate the Subject with the

Setting	What To Do
	user's FQDN. Do not use the backslash character (\) in the subject name.
Subject Alternate Name Type	Select RFC 822 Name, DNS Name,Uniform Resource Identifier or None, based on the attributes of the certificate template.
Subject Alternate Name Value	Enter the value for the corresponding type. If you type '$' as the first character, a drop-down list is displayed with possible custom LDAP and Entra ID attributes. Select the appropriate custom attribute from the list. If Entra ID value is used, only 'onPremisesImmutableId' is supported. Enter fn:base64tohex($)
NT Principal Name	Enter a subject alt name for Microsoft environment. This would usually be configured to include the user's UPN (user principal name).
Challenge	(Optional) Used as a pre-shared secret for automatic enrolment.
Retries	Select from the list to set the number of times that authentication will be attempted after the first time a status of 'pending' is returned.
Retry delay	Select from the list to set the number of seconds to wait before a retry.
Key size	Select 1,024, 2,048, or 4,096 bits.
Use as digital signature	Select if the certificate can be used for signing.
Use as key encipherment	Select if the certificate can be used for encryption.
CA Fingerprint SCEP Config - Windows Config	If your certificate authority uses HTTP, enter the hex string to be used as the fingerprint of the CA's certificate. MD5 fingerprints is supported. If you prefer, you can create a fingerprint from the certificate. Just drag and drop the certificate to the designated area or click **Create from Certificate** to select the certificate from your file system.
CA (Certificate Authority)	Select to specify a certificate authority that you have already created under **Admin > Certificate Management**. Select the certificate authority from the drop-down that appears when you select this option.
Subject	Enter an X.500 name represented as a comma-separated array of OIDs and values. Typically, the subject is set to the user's fully qualified domain name. For example, C=US,DC=com,DC=MobileIron,OU=InfoTech or CN=www.mobileiron.com. You can also customise the Subject by appending a variable to the OID. For example, CN=www.mobileiron.com-$DEVICE_CLIENT_ID$. For ease of configuration you can also use the $USER_DN$ variable to populate the Subject with the user's FQDN. Do not use the backslash character (\) in the subject name.

Setting	What To Do
Subject Alternate Name Type	Click **+ Add** to select RFC 822 Name, DNS Name, Uniform Resource Identifier or None, based on the attributes of the certificate template.
Retries	Select from the list to set the number of times that authentication will be attempted after the first time a status of 'pending' is returned.
Retry delay	Select from the list to set the number of seconds to wait before a retry.
Key Length	Select key size in 1,024, 2,048, or 4,096 bits.
Select usage	Select at least one option: • Use as digital signature - Select if the certificate can be used for signing. • Use as key encipherment - Select if the certificate can be used for encryption.
Validity	Select validity in days, months or years.
CA Thumbprint	If your certificate authority uses HTTP, enter the hex string to be used as the fingerprint of the CA's certificate. MD5 fingerprints is supported. If you prefer, you can create a fingerprint from the certificate. Just drag and drop the certificate to the designated area or click **Create from Certificate** to select the certificate from your file system.
Hash Algorithm Family	Select SHA-2 or SHA-3 algorithms.

When applying an Identity Certificate to a work profile on a device without setting a work challenge passcode, the device prompts for a device passcode, rather than a work challenge passcode.

Working with Configurations For more information, see Working with Configurations.

10.10.4.23. Apple Activation Lock Configuration

Licence: Silver

This section contains the following topics:

- Enabling the iOS Activation Lock
- Enable the iOS Activation Lock feature on supervised devices
- Enabling the macOS Activation Lock
- Enable the macOS Activation Lock feature on supervised devices
- Using the iOS Activation Lock bypass code
- Clearing the iOS Activation Lock bypass code

Activation Lock is an Apple feature designed to prevent anyone from using a lost or stolen device. After Find My is enabled, a mapping between iCloud account and a hardware identifier for this device is saved to Apple's activation servers. From that point, no one can disable Find My, erase the device, or reactivate it without entering the existing Apple ID and password. If someone other than the user wipes the device and then tries to re-activate and use it, they will be prompted for the Apple ID and password in Setup Assistant.

Disabling Activation Lock will not disable this feature on supervised devices if the end-user has enabled Find My Device. The Setup Assistant will prompt the user to take action when the device is reset or remotely wiped.

Activation Lock provides administrators with more options for deterring theft of supervised devices. However, most corporate administrators are likely to leave Activation Lock disabled because it is primarily a consumer feature. The following table summarises the options for corporate-liable deployments:

Device Type	Result
Corporate-liable and supervised	• Activation Lock is disabled for supervised devices by default. • Device users cannot turn on Activation Lock.
Corporate-liable and unsupervised	• Activation Lock will be enabled as soon as the end-user signs in to iCloud with their Apple ID and turns on Find My Device. • MDM servers, including Ivanti Neurons for MDM, cannot control Activation Lock on unsupervised devices. Device users can lock activation with their personal credentials, leaving you no recourse should they leave the company.

Enabling the iOS Activation Lock

Applicable to: iOS 7+ Supervised

This configuration will be applied to Supervised devices (iOS 7 and later) that have the Find My feature enabled. If an administrator or other user tries to Wipe, Activate, or disable Find My Device on the device, an Apple Activation Lock screen will be displayed. To proceed, iTunes credentials or a Bypass code must be entered.

The Bypass code for Supervised devices will be stored upon activation and can be viewed in device details. The Bypass code can be sent remotely using the "Clear Activation Lock" command for Supervised devices. However, the code must be entered manually when reactivating a device or turning off the Find My Device feature.

> You can only create one Activation Lock Configuration for all spaces.

Enable the iOS Activation Lock feature on supervised devices

Procedure

1. Enable the **Find My** feature on your device.
2. Go to **Configurations**.
3. Select the **Apple Activation Lock** configuration from the list of existing configurations.
4. Click **Edit**.
5. In the iOS 7+ Supervised section, click **Enable Activation Lock**.
6. Click **Done**.
7. Register the device.

Enabling the macOS Activation Lock

Applicable to: macOS 10.15+ Supervised

This configuration will be applied to Supervised devices with macOS 10.15 and later. Activation Lock on macOS only applies to Macs that have an Apple T2 Security Chip. On Supervised devices, whether upgraded or freshly installed, and on upgraded currently registered devices, Activation Lock is off by default. Enabling Find My does not automatically enable Activation Lock on these devices.

If an administrator or other user tries to Wipe, Activate, or disable Find My feature on the device, an Apple Activation Lock screen will be displayed. To proceed, iTunes credentials or a Bypass code must be entered. The Bypass code for Supervised devices will be stored upon activation and can be viewed in device details. The Bypass code can be sent remotely using the "Clear Activation Lock" command for Supervised devices. However, the code must be entered manually when reactivating a device or turning off the Find My feature.

> You can only create one Activation Lock Configuration for all spaces.

Enable the macOS Activation Lock feature on supervised devices

Procedure

1. Enable the Find My feature on your device.
2. Go to **Configurations**.
3. Select the **Apple Activation Lock** configuration from the list of existing configurations.
4. Click **Edit**.
5. In the macOS 10.15+ Supervised section, click **Enable Activation Lock**.
6. Click **Done**.
7. Register the device.

Using the iOS Activation Lock bypass code

When the device is wiped with the iOS Activation Lock enabled, the bypass code is retained on the Apple Activation server and in the Ivanti Neurons for MDM Admin interface.

Procedure

1. Go to **Devices**.
2. Select the device.
3. Click **Actions > Wipe**. It may take a few minutes before the device restarts.
4. When the device prompts you for the Apple ID and password, leave the **Apple ID** empty.
5. Enter the bypass code in the **password** field.
6. Click **Next**.
7. Proceed with the setup.

Clearing the iOS Activation Lock bypass code

When the iOS Activation Lock is cleared in the Ivanti Neurons for MDM Admin interface, the bypass code is removed from the Apple Activation server, but it is still present in the device details in the Ivanti Neurons for MDM Admin interface.

Procedure

1. Go to **Devices**.
2. Select the device.
3. Select **Configurations**.
4. Select **Apple Activation Lock**.
5. Click **Edit**.
6. In the iOS 7+ Supervised section, disable **Enable Activation Lock**.
7. Click **Done**.
8. Go to **Devices**.
9. Select the device.
10. Click **Actions > Wipe**. It may take a few minutes before the device restarts. The device can now be setup with the new user's AppleID and password.
11. Proceed with the setup.

The status of the clear iOS Activation Lock is displayed on the interface as follows:

Region	Result
Pending	• Server is sending the Clear Activation Lock code to Apple.
Sent	• Apple acknowledges receipt of the Clear Activation Lock code.
Failed	• The server was unable to send the code to Apple. • Apple has reported an error.

10.10.4.24. iOS Custom Configuration

An iOS custom configuration enables you to upload and distribute an iOS configuration profile that was created by a different app, such as Apple's iPhone Configuration Utility.

iOS Custom settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
File data	Drag and drop the configuration file or click **Choose File** to select it from your file system.

For more information, see **How to create a configuration**.

10.10.4.25. Intelligence Settings

Use the Intelligence Settings to configure Apple Intelligence settings on supervised devices. This declaration helps administrators apply consistent, policy-based controls that manage how devices access and use Apple Intelligence features.

Applicable to:

- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- macOS 15.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Intelligence Settings** configuration.
3. Configure the **Safari Settings** settings as per the following table:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Allow Apple Intelligence Report	Select the checkbox to enable Apple Intelligence Report. Toggle the **Push to Device** button to enable Apple Intelligence Report on supervised devices.
Allow Genmoji	Select the checkbox to enable Genmoji. Toggle the **Push to Device** button to enable Genmoji on supervised devices.
Allow Image Playground	Select the checkbox to enable Image Playground. Toggle the **Push to Device** button to enable Image Playground on supervised devices.
Allow Image Wand	Select the checkbox to enable Image Wand. Toggle the **Push to Device** button to enable Image Wand on supervised devices. This setting is not applicable for macOS devices.
Allow Personalised Handwriting Results	Select the checkbox to enable Personalized Handwriting Results Wand. Toggle the **Push to Device** button to enable Personalized Handwriting Results Wand on supervised devices. This setting is not applicable for macOS and visionOS devices.
Allow Visual Intelligence Summary	Select the checkbox to enable Visual Intelligence Summary. Toggle the **Push to Device** button to enable Visual Intelligence Summary on supervised devices. This setting is not applicable for macOS and visionOS devices.
Allow Writing Tools	Select the checkbox to enable Writing Tools. Toggle the **Push to Device** button to enable Writing Tools on supervised devices.
Force On-Device Only Dictation	Select the checkbox to enable On-Device Only Dictation. Toggle the **Push to Device** button to enable On-Device Only Dictation on supervised devices.
Force On-Device Only Translation	Select the checkbox to enable On-Device Only Translation. Toggle the **Push to Device** button to enable On-Device Only Translation on supervised devices. This setting is not applicable for macOS and visionOS devices.
Apps	
Calendar	
Allow Natural Language Editing	Select the checkbox to enable Natural Language Editing in Calendar and Reminders. Toggle the **Push to Device** button to enable Natural Language Editing in Calendar and Reminders on supervised devices.
Mail	
Allow Smart Replies	Select the checkbox to enable Smart Replies. Toggle the **Push to Device** button to enable Smart Replies on supervised devices.

Setting	What To Do
Allow Summary	Select the checkbox to enable Summary. Toggle the **Push to Device** button to enable Summary on supervised devices.
Notes	
Allow Transcription	Select the checkbox to enable Transcription. Toggle the **Push to Device** button to enable Transcription on supervised devices. This setting is not applicable for visionOS devices.
Allow Notes Transcription Summary	Select the checkbox to enable Transcription Summary. Toggle the **Push to Device** button to enable Transcription Summary on supervised devices. This setting is not applicable for visionOS devices.
Safari	
Allow Summary	Select the checkbox to enable Summary. Toggle the **Push to Device** button to enable Summary on supervised devices.

4. Click **Next** to configure the distribution settings.
5. Select one of the distribution options to set up the **Safari Settings** configuration. For more information about configuring distribution options, see **Working with Configurations**.
6. Click **Done**.

10.10.4.26. iOS Restrictions

iOS restrictions are settings that help the primary user of the device control what other users are allowed to do with iOS, watchOS, and visionOS devices. These settings are defined by Apple and managed by Ivanti Neurons for MDM.

During the distribution of this configuration to **Shared iPads**, you can select either the Device Channel or the User Channel. This is useful to distribute separate configurations and enforce restrictions that are applicable only to the device or the user channel.

The global administrators can delegate space administrators to edit the configuration for **All Devices and for the Custom distribution** option. For the iOS Restriction configure, you can optionally select the **Allow this configuration to be available in all Spaces** option.

> The distribution changes are applicable only to the specific space. All other spaces continue to inherit the default space distribution settings.

iOS restrictions settings

Category	Setting	What To Do
	Name	Enter a name that identifies this configuration.
	Description	Enter a description that clarifies the purpose of this configuration.
Device functionality	**iOS All Versions**	**Enable use of device features.**
	Allow screenshots and screen recording	Select to allow the device user to take screen captures using the built-in iOS screen capture feature.
	Allow remote screen observation (iOS 9.3 and later)	Select to allow user to observe remote screen.
	Allow force unprompted managed classroom screen observation (Supervised only - iOS 10.3+)	(Applicable for iPads only) Select to allow unprompted message on the screen when a supervised iPad is configured with managed classes.
	Allow automatic sync while roaming	Select to allow synchronisation of mail accounts while the device is outside of its home country.
	Allow Siri	Select to allow the personal assistant app on supported devices.
	Allow Siri while device is locked	Select to allow the personal assistant app to perform tasks even when the device is locked.
	Enable Siri profanity filter (Supervised only)	Select to enable the Siri profanity filter.
	Allow voice dialling	Select to allow users to dial a contact or number by talking to the device.
	Allow In-App Purchase	Select to allow users to make purchases through apps running on the device.
	Allow passbook while device is locked	Select to allow Passbook notifications to display while the device is locked.
	Allow lock screen Control Centre	Select to allow access to Control Centre from the lock screen.
	Allow lock screen	Select to allow notifications to be displayed on the lock screen.

Category	Setting	What To Do
	Notifications view	
	Allow lock screen Today view	Select to allow access to the Today view from the lock screen.
	Allow Open In from managed to unmanaged apps	**Requires Gold licence**. Select to allow documents in unmanaged apps and accounts to be opened in managed apps and accounts. Disabling this option prevents exchange of documents from managed to unmanaged apps and accounts. For example, you might want to keep enterprise documents from being opened with personal apps. You can also use this option (disable) together with a managed domains configuration to ensure that data downloaded from managed domains can only be opened in a managed app.
	Allow Open In from unmanaged to managed apps	**Requires Gold licence**. Select to allow documents in unmanaged apps and accounts to be opened in managed apps and accounts. Disabling this option prevents exchange of documents from unmanaged to managed apps and accounts. For example, you might want to keep users from sending personal documents using company email. You can also use this option (turn off) together with a managed domains configuration to ensure that data downloaded from unmanaged domains cannot be opened in a managed app.
	Require passcode on first AirPlay pairing	Select to require the Apple TV to display a passcode that the user must enter on the iOS device to authorise the initial pairing of the devices.
	Force Password on AirPlay incoming requests (tvOS up to 10.1)	Select to require the user to enter password for all incoming AirPlay requests. Default: Deselected
	iOS 26+	
	Apps Exempted from Rating Restrictions (applicable for iOS 26.1+) **iOS All Versions Supervised**	Enter the list of apps that you want to exempt from age-based rating restrictions only if their bundle IDs are included in the intersection of all exemption lists from multiple payloads and parental control apps like ScreenTime. Default: Selected
	Allow Apple Books	Select to allow access to the Apple Books app.
	Allow explicit sexual content in iBooks Store (iOS and tvOS 11.3 and later)	Select to allow users to download iBooks store material that has been tagged as erotica.

Category	Setting	What To Do
	Allow account modification	Select to allow users with supervised iOS 7 devices to add email accounts and make changes to email accounts that have already been configured.
	Allow app mobile data modification	Select to allow users to make changes to mobile data settings for apps.
	Allow Find My Friends modification	Select to allow users to make changes to the Find My Friends app settings.
	Allow pairing with non- Configurator hosts	Select to allow host pairing for iTunes synchronisation. In effect, enabling this option allows supervised devices to sync with iTunes on a Mac other than the supervision host. Disabling this option disables all host pairing with the exception of the supervision host. If no supervision host certificate has been configured, all pairing is disabled.
	Allow AirDrop	Select to allow use of AirDrop on the device. AirDrop is Apple's ad hoc Wi-Fi system that enables file sharing with nearby users. By restricting this feature, you ensure that sensitive documents are not leaked to unauthorised or unsecured devices.
	Allow Touch ID / Face ID to unlock device	Select to allow Touch ID or Face ID to unlock the devices.
	Allow Spotlight search to return Internet search results	Select to allow Spotlight search to return Internet search results.
	Allow app in single app mode	Enter comma separated list of bundle IDs for apps that can autonomously enter single app mode on iOS supervised devices. For example, you can specify custom exam apps for students. As soon as the student launches the app, the app enters single app mode to ensure that the student cannot use other resources while taking the exam. This feature applies to apps developed for autonomous single app mode. Supervision is established with Apple Configurator.
	iOS 8+	
	Allow Enterprise books to be backed up	Select to allow personal backup of iBooks, ePub, and PDF documents that were pushed to the device using MDM.
	Allow Enterprise books notes and highlights to be synced	Select to allow the notes and highlights added to Enterprise books to be synchronised to iTunes.
	Force Apple Watch wrist detection	Select to hide on-screen notifications unless someone is wearing the Apple Watch.

Category	Setting	What To Do
	iOS 8+ Supervised	
	Allow predictive keyboard	Select to allow users to enable iOS prediction of the word being typed, enabling users to tap one of three predictions to complete the word.
	Allow keyboard auto-correction	Select to allow use of auto-correction with Bluetooth keyboards.
	Allow keyboard spell check	Select to allow use of spell check with Bluetooth keyboards.
	Allow keyboard definition lookup	Select to allow definition lookup with Bluetooth keyboards.
	Allow modifying Touch ID fingerprints / Face ID faces	Select to allow Touch ID or Face ID settings to be changed.
	iOS 9+ Supervised	
	Allow keyboard shortcuts on iPads	Select to allow use of keyboard shortcuts on the iPad.
	Allow modification of wallpaper	Select to allow users to change wallpaper images.
	Allow pairing with Apple watch	Select to allow pairing of the iPhone with the Apple watch.
	Allow modification of device name	Select to allow user to change the name of the device.
	Allow modification of enterprise app trust setting	Select to allow user to change the enterprise app trust settings.
	iOS 9.3+ Supervised	
	Allow modification of notifications settings	Select to allow user to change notification settings.
	iOS 9.3.2+ Supervised	
	Allow diagnostic submission modification	Select to allow user to change settings related to submission of diagnostic data to Apple.
	iOS 10+ Supervised	

Category	Setting	What To Do
	Allow Bluetooth modification	Select to allow user to modify the Bluetooth setting on supervised devices. Useful in such cases as shared iPads used for the Classroom app for Education where Bluetooth is required to run the app.
	iOS 10.3+ Supervised	
	Allow dictation	Select to allow the user to talk to the iPhone or iPad instead of typing.
	iOS 11+ Supervised	
	Allow AirPrint	Select to allow AirPrint feature for wireless printing.
	Allow AirPrint Credential Storage	Select to allow keychain storage of username and password for the AirPrint.
	Allow Airprint iBeacon Discovery	Select to allow the user to set iBeacon discovery of AirPrint printers.
	Allow adding VPN configurations	Select to allow the user to create VPN configuration
	Force Airprint Trusted TLS Requirement	Select to allow trusted certificates for TLS printing communication. Default: Deselected
	Allow System App Removal	Select to allow the removal of system app.
	Allow modifying mobile plan settings	Select to allow users to modify mobile plan settings.
	Allow setting up new nearby devices	Select to allow users to setup new nearby devices.
	Automatically join Classroom classes without prompting	Select to allow users to automatically join classroom classes without any prompt. Default: Deselected
	Allow Classroom to lock an app and lock the device without prompting	Select to allow classroom to lock an app and the device without prompting the user. Default: Deselected
	Force the user to authenticate before passwords or credit card information can	Device owner must authenticate before passwords or credit card information can be auto filled in Safari browser and in applications. Default: False

Category	Setting	What To Do
	be autofilled in Safari and apps	
	iOS 11.3+ Allow pairing with Remote app (tvOS 11.3 and later)	Select to allow pairing the device with the Remote app.
	Allow incoming AirPlay requests (tvOS 11.3 and later)	Select to allow incoming AirPlay requests.
	iOS 11.3+ **Supervised** Allow USB restricted mode	Select to allow user to access USB restricted mode.
	Defer software updates for 30 days (for iOS 11.3, tvOS 12.2 and later with supervised devices only)	Select to enter the number of days by which you want to defer software updates. The default is 30 days, and the maximum is 90 days. Default: Deselected
	Require teacher permission to leave Classroom unmanaged classes iOS 12+ Supervised	Select to allow user to get the required teacher permission to leave classroom unmanaged classes.
	Force automatic Date & Time (iOS 12.0 & tvOS 12.2 and later)	Select to turn on the Date & Time "Set Automatically" feature. It cannot be turned off by the user. Default: False
	Allow modifying eSIM settings (iPhone XS, iPhone XS Max, & iPhone XR - iOS 12.1 and later versions)	Select to allow user to modify the eSim configuration on supported devices. This option also prevents users from adding or removing a cellular plan in Settings on their devices. Default: True
	iOS 12.2+ **Supervised**	

Category	Setting	What To Do
	Allow modifying Personal Hotspot settings	Select to allow the user to modify Personal Hotspot settings. Default: True
	iOS 13.0+	
	Allow Files Network Drive Access	Select to allow the user to connect to network drives in the Files app. Default: True
	Allow Files USB Drive Access **iOS 13.0+** **Supervised**	Select to allow the user to connect to any connected USB devices in the Files app. Default: True
	Allow Continuous Path Keyboard	Select to enable continuous path keyboard (swipe or trace typing). Default: True
	Allow Device Sleep	Select to enable device sleeping. Default: True
	Allow Find Device Allow Find My Friend Force WiFi Power On **iOS 13.4+**	Select to enable Find My Device in the Find My app. Default: True Select to enable Find My Friends in the Find My app. Default: True Select to enable WiFi power to be in the on state. Default: False
	Allow Guest Session for shared iPad	If false, temporary sessions are not available on Shared iPad. Default: True
	iOS 14.0+	
	Allow Apple Personalised Advertising	If false, limits Apple personalised advertising. This will prevent Apple from using the user's information for targeting ads. This may not reduce the number of ads received, but the ads will be less relevant to the user. Default: True
	iOS 14.0+ **Supervised**	
	Allow App Clips	If false, prevents a user from adding any App Clips, and removes any existing App Clips on the device. Default: True

Category	Setting	What To Do
	iOS 14.2+ Supervised	
	Allow NFC	If false, disables NFC. Requires a supervised device. Available in iOS 14.2 and later. Default: True
	iOS 14.5+	
	Allow Auto Unlock	Administrators can use the existing allow AutoUnlock restriction to manage this feature. If false, disallows auto unlock. Available in macOS 10.12 and later, and iOS 14.5 and later. Default: true
	Force on Device only Dictation	If true, disables connections to Siri servers for the purposes of dictation. Default: false
	iOS 14.5+ Supervised	
	Allow unpaired external boot to recovery	If true, allows devices to be booted into recovery by an unpaired device. Default: false
	Force WiFi to allowed networks only	If true, limits device to only join WiFi networks set-up via configuration profile. Default: false If the **Force WiFi to allowed networks only** restriction is enabled and WiFi configuration is not distributed to the device, the WiFi connection is lost.
	iOS 15+	
	Force on Device only Translation	If true, the device won't connect to Siri servers for the purposes of translation. Default: false
	Require Managed Pasteboard	If true, copy and paste functionality respects the allowOpenFromManagedToUnmanaged and allowOpenFromUnmanagedToManaged restrictions. Default: false
	iOS 15.2+	
	Allow Mail Privacy Protection	If false, disables Mail Privacy Protection on the device. Available in iOS 15.2 and later. When the Allow Mail Privacy Protection configuration is installed and enabled from the Ivanti Neurons for MDM administrative portal, the Protect Mail Activity toggle is enabled on the device and the following options are visible: • **Hide IP Address** - The email sender cannot link the email to your online activity or determine your location • **Block All Remote Content** - Prevents the email sender from seeing your email activities Default: true
	iOS 15.4+	

Category	Setting	What To Do
	Allow Apple TV's automatic screen saver (tvOS 15.4 and later)	If false, disables Apple TV's automatic screen saver. Available in tvOS 15.4 and later. Default: true
	iOS 16.0 till 26.0	
	Allow Background Security Improvements Installation	To disable the responses. The user cannot install background security improvements.
	Allow Background Security Improvements Removal **iOS 17.0+** **Supervised**	To block the user from being able to undo the responses. The user cannot remove background security improvements.
	Allow iPhone widgets on Mac devices	Select to allow the iPhone widgets to appear on Mac devices that uses the same AppleID of the iPhone for iCloud on both the devices.
	iOS 17.2+ **Supervised**	
	Allow Live Voice Mail	Select to enable live voicemail on the device.
	Force Preserve ESIM On Erase **iOS 17.4+** **Supervised**	Select to preserve the eSIM when the system erases the device due to too many failed password attempts or the Erase All Content and Settings option in **Settings** > **General** > **Reset**. The system doesn't preserve eSIM if **Find My** initiates to erase the device.
	Allow Marketplace App Installation Allow Auto Dim **iOS 17.5+** **Supervised** Allow Web distribution App Installation	Select to allow the users from downloading apps from alternative marketplaces. This Restriction when set to false, will prevent users from installing new alternative marketplace apps and apps installed from those marketplaces. Select to allow auto dimming option on iPads with OLED displays. This **allowWebdistributionAppInstallation** restriction when set to false, will prevent users from installing apps directly from new alternative websites. It is applicable for supervised devices only.

Category	Setting	What To Do
	iOS 18.0+ Supervised	
	Allow eSIM Outgoing Transfers	Select to allow the transfer of an eSIM to a different device from the device on which the restriction is installed.
	Allow Genmoji	Select to allow the creation of Genmojis.
	Allow Image Playground	Select to allow the use of image generation.
	Allow Image Wand	Select to allow the use of Image Wand.
	Allow iPhone Mirroring	Select to allow the iPhone to mirror in a macOS device.
	Allow Personalised Handwriting Results	Select to allow the system to generate text using the user's handwriting.
	Allow Writing Tools	Select to enable Apple Intelligence writing tools.
	Allow Apps To Be Hidden	Select to allow apps to be hidden.
	Allow Apps To Be Locked	Select to allow apps to be locked.
	iOS 18.1+ Supervised	
	Allow Call Recording	Select to allow call recording. Default: True
	Allow Mail Summary	Select to allow the creation of summaries of email messages manually. Default: True
	Allow RCS Messaging	Select to allow RCS messaging. Default: True On iOS 26 devices and cellular iPad models with iPadOS 26, RCS Messaging usage can be limited on devices that have their cellular plan associated with ICCID.
	iOS 18.2+ Supervised	
	Allow External Intelligence Integrations	Select to enable the use of external cloud-based intelligence services with Siri.
	Allow External Intelligence	Select to enable external intelligence providers to enter anonymous mode. If a user is already signed in to an external intelligence provider, applying this restriction will cause them to be

Category	Setting	What To Do
	Integrations Sign-In	signed out.
Applications	Allow Default Browser Modification	Select to enable default browser preference modification. The Ivanti Neurons for MDM settings allows you to set the default web browser.
	iOS All Versions	Enable access to applications on the devices.
	Allow installing apps	Select to enable the user to install applications from the Apple App Store. Deselect to disable the App Store and remove its icon from the Home Screen.
	Allow use of camera	Select to enable the user to operate the camera. Deselect to disable the camera and remove its icon from the Home screen. In iOS 26+ devices, if the apps are added to the exception list, the Allow Camera restriction won't be applied.
	Allow use of Safari	Select to allow use of the Safari web browser. Deselect to disable the Safari web browser, remove its icon from the Home screen, and prevent users from opening web clips.
	Enable autofill	Select to turn on the autofill feature for fields displayed in Safari.
	Force fraud warning	Select to prompt Safari to attempt to prevent the user from visiting websites identified as being fraudulent or compromised.
Safari	Enable JavaScript	Select to turn on Javascript support for Safari.
	Block pop-ups	Select to block pop-ups for Safari.
	Supervised only - Version 26+	
	Allow Safari History Clearing	Select to allow users to clear browsing history.
	Allow Safari Private Browsing	Select to allow to use private browsing.
	iOS All Versions Supervised	
	Allow removing apps	Select to allow users to remove apps from the device.
	Allow use of Game Centre	Select to allow access to Game Centre.
	Allow adding Game Centre friends	Select to allow users to add friends to Game Centre.

Category	Setting	What To Do
	Allow multiplayer gaming	Select to allow users to play games that include other users.
	Allow iMessage	Select to allow use of iMessage. On iOS 26 devices and cellular iPad models with iPadOS 26, the iMessage usage can be limited if the device is added to the denied list.
	Accept cookies	Select Never, Always, or From Visited sites.
	Allow FaceTime	Select to allow the user to run FaceTime if the camera is enabled. On iOS 26 devices and cellular iPad models with iPadOS 26, the Face Time can be limited if the device is added to the denied list.
	iOS 8+	
	Allow managed applications to use cloud sync	Select to allow managed apps to use cloud sync.
	Allow Activity Continuation	Select to allow activity continuation in apps supporting Handoff.
	iOS 8+ Supervised	
	Allow use of Podcasts	Select to allow use of Podcasts.
	iOS 9+	
	Allow trusting of new enterprise app authors	Select to allow user to access new enterprise apps.
	iOS 9+ Supervised	
	Allow App Store	Select to allow user access to the Apple App store.
	Allow automatic app download	Select to allow the app to download files, data, updates with prompting the user.
	Allow News app	Select to allow use of the News app.
	iOS 9.3+ Supervised	
	Allow iTunes Radio	Select to allow use of iTunes radio.
	Allow Apple Music	Select to allow use of Apple Music.
	Allow Listed App Bundle IDs	Select to allow only bundle IDs listed in the array to be shown or launchable. Include the value com.apple.webapp to allow all webclips.

Category	Setting	What To Do
	Blocked App Bundle IDs **iOS 13.0+** **Supervised**	Select to prevent bundle IDs listed in the array from being shown or launchable. Include the value com.apple.webapp to restrict all webclips.
	Allow use of iTunes Store	Select to allow use of the iTunes Music Store. Deselect to disable iTunes Music store and remove its icon from the Home screen.

Category	Setting	What To Do
iCloud	iOS All Versions	Enable access to iCloud services.
	Allow backup Allow document sync Allow Photo Stream	Select to allow the device to back up data via Apple's iCloud service. Select to allow documents to be synchronised via Apple's iCloud service. Select to allow photos to be synchronised to your other iOS devices via Apple's iCloud.
	Allowed shared Photo Streams(disallowing can cause data loss) Allow Keychain sync **iOS 9+** Allow iCloud Photo Library **iOS 15+ Supervised** Allow cloud private relay	Select to allow synchronisation of shared photos. Deselecting this option can result in loss of photos. Select to allow synchronisation of your keychain. Select to allow access to iCloud photo library. If false, disables iCloud Private Relay. Default: true

Category	Setting	What To Do
Security and Privacy	**iOS All Versions**	Enable security and privacy policies.
	Allow over-the-air certificate updates	Select to allow over-the-air updates of root certificates.
	Force limit ad tracking	Select to require use of the limit ad tracking feature.
	iOS All Versions Supervised	
	Allow configuration profile installation	Select to allow users to install configuration profiles and certificates interactively.
	Allow assistant user generated content	Select to allow Siri to query user-generated content from the web.
	iOS 8+ Supervised	
	Allow user to erase all content and settings in Reset UI	Select to enable the "Erase All Content And Settings" option in the iOS Reset UI on the device.
	Allow Screen Time	Select to allow screen time (Settings > Screen Time).
	Allow diagnostic data to be sent to Apple	Select to allow automatic submission of diagnostic data to Apple.
	Allow user to accept untrusted TLS certificates	Select to allow the device user to accept untrusted HTTPS certificates. If this option is not selected, then the device will automatically reject untrusted HTTPS certificates without prompting the device user.
	Force encrypted backups	Select to require encrypted backups via iTunes. Automatically selected due to SCEP requirements.
	Force user to enter iTunes Store password for all transactions	Select to force device users to enter their iTunes password for each App Store transaction. If this option is not selected, then the device user can make multiple transactions on a single authentication.
	iOS 9+	
	Treat AirDrop as unmanaged destination	Select to allow user access to AirDrop file sharing. Default: False
	iOS 9+ Supervised	
	Allow modification of device passcode	Select to allow user to change the passcode for the device.
	iOS 12+	

Category	Setting	What To Do
	Allow managed apps to write contacts to unmanaged contact accounts	Select to allow managed apps to write contacts to unmanaged contacts accounts. Default: False
	iOS 12+ Supervised	
	Allow autofill passwords	Select to allow users to use the AutoFill Passwords feature on iOS and be prompted to use a saved password in Safari or in apps.
	Allow nearby devices to share requests for a password Allow password sharing Allow unmanaged apps to read contacts from managed contact accounts iOS 18.3	Select to allow user's device to request passwords from nearby devices. Select to allow users to share their passwords with the Airdrop Passwords feature. Select to allow unmanaged apps to read from managed contacts accounts. Default: False
	Allow External Intelligence Workspace IDs	Enter allowed External Intelligence Workspace ID.
	Allow Notes Transcription Summary Allow Visual Intelligence Summary	Select to enable creation of summaries from Transcriptions. Default: True Select to enable creation of summaries from Apple's Visual Intelligence using images or visual content. Default: True

Category	Setting	What To Do
Content Ratings		Control access to apps and media.
	Allow playback of explicit music, podcasts & iTunes U media (iOS 13+ Supervised only and tvOS 11.3 and later)	Explicit content is marked as such by content providers, such as record labels, when sold through the iTunes Store.
	Ratings region	Select a region from the drop-down list to change the region associated with the rating selections for applications, TV shows and movies.
	Movies	Select a rating limit for movies stored on the device: • Do not Allow Movies • G • PG • PG-13 • R • NC-17 • Allow All Movies
	TV Shows	Select a rating limit for TV shows stored on the device: • Do not Allow TV Shows • TV-Y • TV-Y7 • TV-G • TV-PG • TV-14 • TV-MA • Allow All TV Shows
	Apps	Select a rating limit for applications on the device: • Do not Allow Apps • 4+ • 9+ • 12+ • 17+ • Allow All Apps

For more information, see **How to create a configuration**

10.10.4.27. Conference Room Display

Applicable to: tvOS 10.2 and supported newer version.

This configuration will turn on the Conference Room Display mode on Apple TV. Conference Room Display mode locks Apple TV into that mode, to prevent other types of usage.

Beginning with tvOS 10.2, you can set supervised Apple TV devices to Conference Room Display mode. Conference Room Display locks scoped Apple TV devices to a black wallpaper screen and downloads a default screen saver, unless a background image and screen saver are manually defined in the Apple TV device settings. This mode can also display a message as configured in the Conference Room Display configuration.

The Conference Room Display configuration can be deployed automatically and apps can install while devices are in this mode. A device set to Conference Room Display mode that reboots will automatically resume locked screen without first showing the Home screen.

> If an Apple TV device is running in Single App Mode or if Single App Mode is deployed with Conference Room Display, Conference Room Display will override Single App Mode. In addition, if an Apple TV device is connected to a network via Ethernet, Conference Room Display will not automatically display a Wi-Fi network to join for AirPlay sharing. This instruction can be displayed on the screen using the Custom Message field of the Conference Room Display configuration.

Creating a Conference Room Display configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **conference** in the search field, and then click the **Conference Room Display** configuration.
4. Enter a name and describe the configuration.
5. Specify the **Custom Message**. This is the custom message displayed on the screen in Conference Room Display mode.
6. Click **Next** to configure the distribution settings.
7. Click **Done**.

For more information, see **How to create a configuration**.

10.10.4.28. Keyboard Settings

Use the **Keyboard Settings** to configure keyboard settings on supervised devices. This declaration helps administrators apply consistent, policy-based controls that manage keyboard behavior, input options, and related user experience settings.

Applicable to:

- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- macOS 15.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Keyboard Settings** configuration.
3. Configure the **Safari Settings** settings as per the following table:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Allow Auto-Correction	Select the checkbox to enable Auto-Correction. Toggle the **Push to Device** button to enable Auto-Correction on supervised devices. This setting is not applicable for macOS devices.
Allow Definition Lookup	Select the checkbox to enable Definition Lookup. Toggle the **Push to Device** button to enable Definition Lookup on supervised devices.
Allow dictation	Select the checkbox to enable Dictation. Toggle the **Push to Device** button to enable Dictation on supervised devices.
Allow Math Keyboard Suggestions	Select the checkbox to enable Math Keyboard Suggestions. Toggle the **Push to Device** button to enable Math Keyboard Suggestions on supervised devices.
Allow Predictive Text	Select the checkbox to enable Predictive Text. Toggle the **Push to Device** button to enable Predictive Text on supervised devices. This setting is not applicable for macOS devices.
Allow Slide to Type	Select the checkbox to enable Slide to Type. Toggle the **Push to Device** button to enable Slide to Type on supervised devices. This setting is not applicable for macOS devices.
Allow Spell Check	Select the checkbox to enable Spell Check. Toggle the **Push to Device** button to enable Spell Check on supervised devices. This setting is not applicable for macOS devices.
Allow Text Replacement	Select the checkbox to enable Text Replacement. Toggle the **Push to Device** button to enable Text Replacement on supervised devices. This setting is not applicable for macOS devices.

4. Click **Next** to configure the distribution settings.
5. Select one of the distribution options to set up the **Safari Settings** configuration. For more information about configuring distribution options, see **Working with Configurations**.
6. Click **Done**.

10.10.4.29. Lockdown & Kiosk: Android Device Admin Mode

A Lockdown & Kiosk: Android Device Admin mode configuration disables certain features of Android devices and creates a Allowlist of apps that will be available to users in Kiosk mode.

> The Android Device Admin Mode Configuration is deprecated and not supported for devices on Android 8 and later versions. It is recommended to use Android Enterprise Lockdowns for Kiosk Lockdowns on Android 8 and later versions.

You can restrict the option to modify settings or apps when an Android device is in Kiosk mode.

- Add apps and select settings in the Create Lockdown & Kiosk: Android Device Admin Mode Configuration page.
- The option to change the settings using the Settings icon will be available in Kiosk mode.
- Select apps without choosing any settings configuration options and the settings icon will not be displayed in Kiosk mode.
- If you choose not to include any apps in the configuration, then the settings icon will be displayed.

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Lockdown Settings: Disable features for all Android devices.	
Disable Wi-Fi	Select to turn off access to wireless LANs.
Disable Camera	Select to turn off camera access.
Disable Bluetooth	Select to turn off Bluetooth features. Use caution when using this option. Ivanti recommends against disabling audio because hands-free Bluetooth access is disabled. Legal requirements for hands-free use of devices while driving is becoming more widespread.
Kiosk Mode Settings: Enables the device to be used as a kiosk, with operation restricted to a few specific apps. Kiosk mode settings will not be applied to a device with Android 8.0 and above. For such devices, the Kiosk Status in device details page reports UNSUPPORTED_ON_DEVICE as Kiosk Status.	
Enable Kiosk Mode	Select to configure **Kiosk Mode** on Android devices.
Disable Quick Settings	Select to disable Quick Settings in Kiosk mode.
Allow User to Access Wi-Fi Settings	Select to allow a user to change Wi-Fi settings and access preferred wireless networks.
Allow User to Access Bluetooth Settings	Select to allow a user to change the Bluetooth settings and pair additional Bluetooth devices.
Allow User to Access Location Settings	Select to allow a user access to the location settings.
Allow User to Delay Application Updates	Select to allow a user to delay application updates.
Kiosk Exit PIN	Enter the four-digit code that the end user must type in order to exit Kiosk Mode.
Create an Allowlist of apps: These apps will be available to users in Kiosk Mode by adding apps to the allowed apps list. Drag and Drop to arrange the apps in the order they should appear in the Kiosk Mode launcher. Adding an application to the list of allowed apps will not install the app on the device. Be sure to distribute each app to the appropriate users and user groups in the App Catalogue.	

Setting	What To Do
Built-In Apps	Click +Add to include listed native apps in the group of apps allowed in Kiosk Mode. If you have disabled Dialler or Camera in Lockdown settings above, they cannot be added to the Allowed Apps list.
App Catalogue	Click +Add to included listed apps from the app catalogue in the group of apps allowed in Kiosk Mode.
Other Apps	Click +Add to include the **package name** of an app that is not available on the Google Play Store.
Kiosk Mode Allowed Apps	Click X to remove an app from the group of apps allowed in Kiosk Mode. Drag and drop to change the order in which apps appear on kiosk devices.

> For Samsung devices with Knox Standard 4.0 or higher, the multi-user feature is automatically locked down in kiosk mode.

For non-Samsung devices, Kiosk mode is not supported on Android 8.0 or higher. Ivanti recommends using Android Enterprise lockdowns for Kiosk mode on Android 8.0 or later.

Related topics:

- **Setting Up Kiosk Mode for Android**
- **How to create a configuration**

10.10.4.30. Setting up Kiosk Mode for Android

This section contains the following topics:

- Launching Kiosk Mode remotely
- Exiting Kiosk Mode

Licence: Silver

Kiosk Mode for Android devices enables you to restrict use of a device to specific apps. You might use Kiosk Mode to set up devices for employees who will use only work-specific apps.

When preparing Android devices for Kiosk mode or Device Owner with Kiosk mode, you will need to **create an Allowlist of apps** that you want to be available to users in Kiosk Mode. For devices using Device Owner you can add apps to the allowed apps list by dragging and dropping to arrange the apps in the order they should appear in the Kiosk Mode launcher when configuring the app. See **Lockdown & Kiosk configuration** for more information.

Prerequisites

Before you configure Kiosk Mode for Android devices, ensure that you have performed the following tasks:

- Installed the Go on the devices.
- Configured the app catalogue with the apps that your kiosk configuration will need.
- Distributed the app catalogue to the devices that will run in Kiosk Mode.

> SonimXP5S devices do not support Kiosk mode.

- Installed the apps that your kiosk configuration will need.
- (Optional) Set up **Android kiosk branding**.

> Kiosk mode is supported on Android 5.1 and 6.0. Non- Samsung Knox must be placed in Device Owner mode to prevent the use of undesired applications.

Important: Some devices have features which can cause the device to draw over the screen or otherwise create an escape from Kiosk Mode. The People Edge feature of the Samsung Galaxy S6 Edge is an example of such a feature. We recommend that these types of features be turned off by an administrator before the device is deployed.

Procedure

1. Go to **Configurations**.
2. Click **+Add**.
3. Click **Lockdown & Kiosk: Android Device Admin Mode**.
4. In the **Create Settings** screen, complete at least the **Kiosk Mode Settings** section.
5. In the **Distribution** screen, select the device groups to receive this configuration.
6. Click **Done**.
7. For non-Samsung devices, continue with the following steps:
    1. Go to **Devices** >**Devices**.

2. Select the devices you want to enable for kiosk mode.
3. Select **ActionsForce Check-in**.
4. On the devices, tap the **Kiosk Mode** button.
5. Press the **Home** button on the device.
6. If a **Choose Launcher** dialog appears, tap **Go Kiosk Launcher** and select **Always**. This step is necessary to ensure that the proper launcher will be used for this feature. Otherwise, the user would be prompted to select a launcher.

Launching Kiosk Mode remotely

Procedure

1. Go to **Devices > Devices**.
2. Add the Kiosk Mode column to the display.
3. Select devices that have Kiosk mode enabled, but are not currently in Kiosk mode.
4. Select **Actions > Enter Kiosk Mode**.

Exiting Kiosk Mode

You can exit Kiosk Mode on the device if you set a PIN in the configuration.

Procedure

1. Tap the **Settings** icon.
2. Select **Exit Kiosk Mode**.
3. Tap in the **Kiosk PIN** field when prompted.
4. Enter the kiosk PIN.

You can exit Kiosk Mode for a specific device from the portal:

Procedure

1. Go to **Devices > Devices**.
2. Display the details for the device.
3. Select **Actions > Exit Kiosk Mode**.

You can also use the following methods to exit Kiosk Mode:

- Delete the configuration
- Disable the configuration
- Remove the device group from the configuration

10.10.4.31. Setting up Android shared device kiosk

For task-worker deployments, companies may offer dedicated Android devices that are customised for a specific user role. Depending on a user's profile different apps and configurations may be presented on a device. For example, a user in a technical role may have a specific set of apps presented for their use, while another user in a maintenance role may have access to a different set of apps.

The Android shared device kiosk mode acts an app filter for different groups of users who share devices. A user who is logged into the shared device kiosk is only able to view the apps appropriate for their role. One of the main advantages to the shared device kiosk is that you can allow different user groups access to different sets of apps from the same device. When a user logs out of a Android shared device kiosk mode, their apps and user data, including history, are cleared from the display of the next user who logs onto the device(if the app marked for is re-installation). The shared device kiosk is only available to Android Enterprise deployments with Managed Google Play accounts.

The shared device kiosk requires two types of users, a staging user and a shared kiosk user, and at least two policies that correspond to these users. The staging user is used to prompt the login screen to appear on a shared device. Also, the staging user is a special type of admin user who allows other users to login to the actual kiosk device. After the shared device kiosk user logs in successfully, then the staging policy is replaced by a shared kiosk policy. The kiosk user has access to the apps installed on the device according to the policy assigned to it. Although you can create multiple shared kiosk policies, there is only one kiosk policy active on a kiosk device at a time. When the kiosk user logs out of the shared kiosk, the device reverts to the staging user and, consequently, the staging policy.

The staging user only has the ability to access the login page. As a result, you need to create staging policy that is dedicated to this user. In contrast, the shared device kiosk users are able to access the set of apps that you define in their policy. (Naturally, you also need to install the permitted apps on the shared device kiosk devices.) The shared device kiosk policy allows you to create a filter of permitted apps from all the apps you have installed previously. You cannot directly upload apps into a Android shared kiosk policy. Often you want to dedicate a shared kiosk policy to a type of shared kiosk user, or user group, depending on your organisation. For example, a company may have day-shift and night-shift employees who have different roles and require access to separate set of apps. In this case, you need to create a day-shift policy and a night-shift policy.

For more information on enabling shared device kiosk, see **Lockdown & Kiosk: Android Enterprise**

10.10.4.32. Lockdown & Kiosk: Android Enterprise

Lockdown & Kiosk: Android Enterprise configuration disables certain features of Android Enterprise devices and creates an Allowlist of apps that will be available to users in kiosk mode.

This section contains the following topics:

- Lockdown Settings
- Work Profile
- Work Managed Devices (Device Owner and kiosk mode settings)
- Managed Device with Work Profile/Work Profile on Company Owned Device Lockdown Settings

Lockdown Settings

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Choose Lockdown Type	Select the type of lockdown settings you want to configure: • Work Profile • Work Managed Devices (Device Owner and kiosk mode settings) • Managed Device with Work Profile/Work Profile on Company Owned Device Lockdown Settings Work Profile on Company Owned Device Lockdown Settings is applicable only for Android 11+ devices. Only one type is allowed per configuration. The options displayed depend on the type you select. If a Work Managed Device (Device Owner) and a Managed Device with Work Profile on Company Owned Device configuration is distributed to the same device, the Managed Device with Work Profile takes precedence.

Work Profile

Disable certain features on Android Enterprise devices.

Setting	What To Do	For Devices
Disable Screen Capture	Select to turn off the ability to use the device's built-in screen capture feature.	• Android 5.0 +
Disallow Apps Control	Select to prevent a user from modifying applications in Settings or launchers.	• Android 5.0 +
Disallow Config Credentials	Select to prevent a user from configuring user credentials.	• Android 5.0 +
Disallow Cross Profile Copy Paste	Select to prevent copy/paste of information between profiles.	• Android 5.0 +
Disallow Modify Accounts	Select to prevent a user from adding or removing accounts.	• Android 5.0 +
Disallow Outgoing Beam	Select to prevent a user from using NFC to transfer the app data.	• Android 5.1+
Disallow Share Location	Select to prevent a user from revealing the device location to apps.	• Android 5.0 +
Disallow Debugging Features	Select to disable debugging features on devices. By default, this option is turned on.	• Android 5.0 +
Ensure Verify Apps	Select to allow application verification features on devices. By default, this option is turned on. When this option is turned off, the device goes back to its default behaviour which may vary from device to device.	• Android 5.0 +
Disable Unknown Sources on Device	Select to prevent the device from installing apps from unknown sources. This setting, to take effect on the device, is dependent on an expected Google Play update to enable this feature.	• Android 5.0 +
Restrict Input Methods	Select to restrict Allowlisted IME package names by designating a list of Allowlisted package names via the **Package Name** field. The devices will have both Allowlisted package input methods and the default system input methods available to use. The user can switch between default system input methods and Allowlisted packages input methods. For Android 10+, Allowlisting is applicable for IME apps on the work profile side only. For	• Android 5.0 +

Setting	What To Do	For Devices
	older Android versions, Allowlisting is applicable for IME apps device wide (both inside and outside the work profile).	
Restrict Accessibility Services	Select to restrict accessibility services for work apps by designating a list of Allowlisted package names via the **Package Name** field. If there are no Allowlisted packages, then only system accessibility services will be allowed.	• Android 5.0 +
Disable unknown sources inside work profile	Select to disallow download from unknown sources within the work profile.	• Android 5.0 +
Enable/Disable System Apps	Select to enable and disable system applications to be deployed by designating two lists of package names via the **System App Package Name** fields. Use this feature to manage access to system applications that are not published in Google Play. Adding an app to the app catalog and also to a system apps list is not supported.	• Android 5.0 +
Disable Caller ID	Sets whether caller ID information from the work profile will be shown in the device for incoming calls.	• Android 6.0 +
Disable Contact sharing via Bluetooth	Select to prevent the device from sharing contacts with other devices via Bluetooth.	• Android 6.0 +
Disable Contact sharing via Search	Select to prevent the users from searching for work contacts from the personal phone dialler.	• Android 7.0 +
Disallow auto-fill	Select to disallow autofill	• Android 8.0+
Disallow work app notifications in personal profile	Select to restrict work profile notifications.	• Android 8.0+
Disallow printing	Select to restrict printing from all apps.	• Android 9.0+
Disallow share into Profile	Select to prevent users from sharing personal data into a work profile on the device.	• Android 9.0+

Setting	What To Do	For Devices
Allow Access to work profile calendars	Select any of the following options to allow all apps or select a set of apps on the personal side to access the calendar information present in the work profile: • **All Apps on Personal Profile** - allow all apps to access the calendar information present in the work profile • **Only the following apps on Personal Profile**- In the text field below, enter the bundle IDs of the apps separated by a comma. Only these selected apps on the personal side will be allowed to access the calendar information present in the work profile. The app on the personal side should implement specific APIs to be able to access a shared calendar.	• Android 10.0+
Enable Cross profile Allowlisting of Apps	Select the checkbox to enable users to share information from specific apps from within the work profile to the personal side of the device. In the **Allowlisted Apps** field, type the Package IDs of the apps to be Allowlisted, separated by commas. By default, this option is disabled.	• Android 11.0+
Enable 5G Network Slicing	Select to provide a 5G network slicing option on work profile of the company-owned devices. By default, this option is disabled.	• Android 12.0+
Disallow Sharing Admin Configured Wi-Fi	Select to prevent users from sharing Wi-Fi configurations set by the administrator.	• Android 13.0+
Disable AI Assist	Select to prevent users from AI Assist features. By default, this option is disabled.	• Android 15.0+

Work Managed Devices (Device Owner and kiosk mode settings)

Disable certain features on work managed devices (Device Owner) for Android 5.0 +.

Setting	Description
Disable Wi-Fi	Select to turn off access to wireless LANs.
Disable Wi-Fi Settings	Select to turn off access to wireless settings.
Disable Camera	Select to turn off camera access.
Disable Bluetooth (Android 8.0+)	Select to turn off Bluetooth features. Use caution when using this option. Ivanti recommends against disabling audio because hands-free Bluetooth access is disabled. Legal requirements for hands-free use of devices while driving is becoming more widespread.
Disallow Bluetooth Settings (Android 8.0+)	Select to turn off access to Bluetooth settings.
Disable Screen Capture	Select to turn off the ability to use the device's built-in screen capture feature.
Disable Network Reset	Select to prevent resetting network. (Applicable to Android 7.0+ devices and not supported in Work Profile on Company Owned device mode).
Mute Master Volume	Select to mute master volume.
Disallow Apps Control	Select to prevent a user from modifying applications in Settings or launchers.
Disallow Credentials	Select to prevent a user from configuring user credentials.
Disallow Emergency Broadcasts	Select to prevent emergency broadcasts.
Disallow Mobile Networks	Select to turn off access to mobile networks. This cannot be disabled if Wi-Fi is disabled.
Disallow Tethering	Select to turn off tethering as an option for using the internet connection of one device to provide internet access to another device.
Disallow VPN	Select to turn off VPN connections.
Disallow Factory Reset	Select to prevent users from returning the device to factory defaults.
Enable Factory Reset Protection	Select to allow users from returning the device to factory defaults. You can optionally specify a list of authorised Google account IDs (an integer value) that can provision the device after factory reset, or hover over the help icon to view help for retrieving authorised account IDs.
Disallow Modify Accounts	Select to prevent a user from adding or removing accounts.
Disallow NFC (Outgoing Beam)	Select to prevent a user from using NFC to transfer app data.
Disallow Outgoing Calls	Select to prevent a user from making outgoing calls.
Disallow Safe Boot (Android 6.0+)	Select to prevent a user from rebooting a device into safe boot mode.
Disallow Share Location	Select to prevent a user from revealing the device location to apps.

Setting	Description
Disallow Debugging Features	Select to disable debugging features on devices. By default, this option is turned on.
Ensure Verify Apps	Select to allow application verification features on devices. By default, this option is turned on. When this option is turned off, the device goes back to its default behaviour which may vary from device to device.
Disallow SMS	Select to prevent a user from sending and receiving SMS messages.
Disallow Unmute Microphone	Select to prevent a user from unmuting the device's microphone.
Disallow Auto Time	Select to prevent a user from enabling automatic time changes.
Disallow Auto Time Zone	Select to prevent a user from enabling automatic device time adjustment with time zone changes.
Sync time with server (Android 9.0+) Set timezone (Android 9.0+) Disable Data Roaming Disable Wi-Fi Sleep	Select to allow devices to sync time with the Ivanti Neurons for MDM servers first time on registration and thereafter once every 24 hours after each check-in. This option will be available only if the **Disable Auto-Time** is selected. Specify timezone string in Olson Time Zone ID format (for example, Pacific/Midway). Select to turn off data exchange while the device is roaming. Select to keep Wi-Fi on while the device is in Sleep mode.
Restrict Input Methods	Select to restrict Allowlisted IME package names by designating a list of Allowlisted package names via the **Package Name** field. The devices will have both Allowlisted package input methods and the default system input methods available to use. The user can switch between default system input methods and Allowlisted packages input methods. For Android 10+, Allowlisting is applicable for IME apps on the device side only. For older Android versions, Allowlisting is applicable for IME apps device wide.
Restrict Accessibility Services Disable USB file transfer Disable external media	Select to restrict accessibility services for work apps by designating a list of Allowlisted package names via the **Package Name** field. If there are no Allowlisted packages, then only system accessibility services will be allowed. Select to disable USB file transfer. Select to disable external media.
Disable keyguard (no effect if PIN/Passcode is set)	Select to disable the keyguard. This option has no effect if a password, PIN, or pattern is currently set. If a password, PIN or pattern is set after the keyguard is disabled, the keyguard stops being disabled.
Keep screen on while connected to power.	Select to keep the screen ON when connected to power. The screen may dim but does not turn off while the device is connected to a power source.

Setting	Description
	This setting will only take effect if auto-lock or inactivity timeout in the passcode configuration is not used to set a timeout.
Disallow create windows	Select to prevent apps from displaying certain types of overlay windows, such as alerts and toasts.
Skip first use hints	Select to enable the system recommendation for apps to skip the user tutorial and other introductory hints on first start-up.
Disallow unknown sources on device	Select to disallow user from installing apps from unknown sources.
Set lock screen message (Android 7.0+)	Select to set the lock screen message to be displayed on the device. Type the lock screen message (maximum of 256 characters) in the text field. By enabling this option, the user is blocked from setting the message in Settings and the message that is set by the admin is displayed to the user. If the admin does not provide any lock screen message after enabling 'Set lock screen message', the user is blocked from setting the message in Settings, but no message is displayed to the user.
Set screen brightness	Select to set brightness of your device's screen. • Manual - Select to enter a number manually (0 to 255) • Adaptive - Select to allow the device to set the brightness It is recommended to enable the "Disallow config brightness" option before setting the screen brightness of your device.
Set screen timeout	Select to set screen timeout duration (in seconds). It is recommended to enable the "Disallow config screen timeout" option before setting the screen brightness of your device.
Set screen orientation	Select to set screen orientation. You can set the screen orientation to 0, 90, 180, or 270 degrees from the drop down list. By default, this option is not selected. For Go app 89 and later versions, you must select this option and set the value to 0 to keep the device in Portrait mode in Kiosk.
Enable/Disable System Apps	Select to enable and disable system applications to be deployed by designating two lists of package names via the **System App Package Name** fields. Use this feature to manage access to system applications that are not published in Google Play. Adding an app to the App Catalog and also to a system apps list is not supported.
Android 8.0+	
Disallow auto-fill	Select to disallow the user from using auto-fill services.
Disallow Bluetooth Sharing	Select to disallow the user from sharing outgoing Bluetooth on the device.
Disable backup service	Select to disable the backup service.
Android 9.0+	

Setting	Description
Disallow printing	Select to disallow the user to print.
Disallow airplane mode	Select to disable flight mode on the entire device.
Disallow ambient display	Select to disallow the ambient display for the user.
Disallow config brightness	Select to disallow the user from configuring the brightness. It is recommended to define the "Set screen brightness mode" mode before selecting this option.
Disallow config date time	Select to disallow date, time and timezone configuration.
Disallow config location	Select to disallow the user from disabling location providers.
Disallow config screen timeout	Select to disallow the user from changing screen off timeout. It is recommended to define the "Set screen timeout" value before selecting this option.
Android 12.0+	
Enable USB for charging only	Select to enable the USB port for charging only.
Android 13.0+	
Set Minimum Required Wi-Fi Security	Use this option to set minimum required Wi-Fi security: • No minimum security required – Select this option if no minimum security is required • Personal Network Based Security – Select this option to block personal Wi-Fi networks such as WEP, WPA/WPA2/WPA3, etc. • Enterprise EAP Network Based Security – Select this option to block EAP protocol-based Wi-Fi networks • Enterprise 192 Network Based Security - Select this option to block EAP corporate-based Wi-Fi networks All the existing devices that do not meet the minimum criteria will be disconnected. Device details will show the Minimum Required Wi-Fi Security level (if available) under the **General > Wi-Fi Security Level**.
Disallow Sharing Admin Configured Wi-Fi	Select to prevent the users from sharing Wi-Fi configurations set by the administrator.
Android 15.0+	
Disable AI Assist	Select to prevent the users from AI Assist features. By default, this option is disabled.
Kiosk Mode Settings: Kiosk mode applies additional restrictions to the	

Setting	Description
devices including limited access to apps via a customised launcher.	
Enable Kiosk Mode	Select to configure **kiosk mode** on Android devices. • When a user logs into the Shared Kiosk mode and logs out, the username remains available with Go client for future logins. In shared Kiosk mode, the Go client preserves recently used seven usernames. • The shared kiosk mode supports IDP Authentication now. So, if Ivanti Neurons for MDM is configured with IDP, then the Shared Kiosk mode can be used with IDP Authentication.
Enable Lock Task Mode	Select to enable lock task mode on Android devices. Whenenabled,thedevicescandisplaykeyguard,statusbarandsafemode. This option is disabled by default. The following are the additional settings displayed when lock task mode is enabled for Android 9 or supported newer versions: **Settings icon** - Allows apps to have access to system functions that are dependent on the Device Settings app. Allowing Device Settings helps to avoid the Lock Task Mode violations in scenarios such as Bluetooth pairing from an app. It is recommended to keep this setting enabled for specific apps. **System Info** - Displays the date/time, connectivity, battery and vibration mode on the status bar. This option is disabled by default. **Keyguard** (Enabled by default) - Enables the keyguard during lock task mode. **Global Actions** (Enabled by default) - Enables the menu that is displayed when the user long-presses the power button. If this option is disabled, the user may not be able to power off the device. **Home button** - Enables the home button. This option is disabled by default. When enabled, the following sub-options are displayed: • **Overview Button** (Disabled by default) - Enables the Overview button and the Overview screen during lock task mode • **Notifications** (Disabled by default) - Enables notifications during lock task mode. This includes notification icons on the status bar, heads-up notifications, and the expandable notification shade. If Home Button option is not enabled, the user will not be able to use the multi window feature.
Enter Kiosk automatically (on initial setup only)	Select to automatically allow kiosk mode when the configuration is applied.
Maintain Kiosk Mode After Policy Updates	Select to automatically return the device to kiosk mode after a lockdown policy update is applied. This setting helps maintain uninterrupted kiosk operation and reduces the need for manual intervention following policy changes. Previously, updating a lockdown policy could cause the device to exit kiosk mode. When enabled, the device automatically re-enters kiosk mode after the updated policy is processed.

Setting	Description
Disable Quick Settings for Android 5 devices	Select to disable Quick Settings in kiosk mode for devices running on Android 5.
Disable Quick Settings for Android 6+ and all Samsung devices	Select to disable Quick Settings in kiosk mode for Android Enterprise devices from version 6 through the most recently released version and for all Samsung devices. Disabling this setting does not block notification icons and sounds on the device.
Allow User to Access Wi-Fi Settings	Select to allow a user to change Wi-Fi settings and access preferred wireless networks.
Allow User to Access Bluetooth Settings	Select to allow a user to change the Bluetooth settings and pair additional Bluetooth devices.
Allow User to Access Location Settings	Select to allow a user access to the location settings.
Allow User to Delay Application Updates	Select to allow a user to delay application updates.
Allow User to Access Date and Time Settings	Select to allow a user to access date and time settings.
Allow User to Access Mobile Network Settings	Select to allow a user to access mobile network settings.
Allow User to Select Language	Select to allow the user to access language settings.
Enable Shared Device	In a shared device kiosk, the device is shared among multiple end users. This option enable a device for sharing while the device is in kiosk mode: • **Enable Login**: This option is for a kiosk admin user. When a device is configured with this option, the user login screen will be displayed, allowing an end user to log in to the shared device kiosk. Enable Login option will be visible if and only if user is created as Android Enterprise Device Account user (staging user). Select Use domain substitution and enter the domain appropriately. This option checks the username for domain suffix. If the domain suffix is missing, the system automatically appends the domain suffix to the username. • **Enable Logout**: When a device is configured with this option, the logged in end user will have access to the Allowlisted apps. This user can see the option to log out, but cannot exit kiosk. When a user logs out of the shared device kiosk, another user can login to the shared device kiosk and view the apps as configured by the admin. • Apps appear with a Recycle icon, which is used for enforcing reinstallation of an app on every login. This option can be used for those apps that are locally cache data. User can exit kiosk mode if admin provides the exit kiosk PIN. • **Timeout**: Specify the timeout duration in hours. For example, when the timeout duration is configured for 2 hours and the end user fails to logout of the shared device kiosk, the logout action will be automatically performed on the device

Setting	Description
	after 2 hours. The **Timeout** field is displayed only when the **Enable Logout** option is selected and it is optional. You can also logout end users from shared kiosk mode by clicking the **Sign out Android Enterprise kiosk** option in the device details page.
Allow FIDO Auth (Requires Google Chrome app on device)	Select this option to use the FIDO-authentication for users when using the shared kiosk. Allow users to use FIDO-Keys for logging into the device. Google Chrome is the only supported browser and it must be available on the device for FIDO-authentication to be available in shared kiosk.
Allow user to configure brightness and auto rotate Enable Multi Window	Select to allow user to configure brightness and auto rotate. Select to allow the display of more than one app at the same time with Samsung devices (Device Owner kiosk). To allow multi window in lock task mode, the following lock task mode options should also be enabled: • **Home Button** • **Overview Button**
Enable Inactivity Protection	Select to enable the inactivity protection in Kiosk mode. If selected, the default value is 30 seconds until which the Kiosk screen will remain active. You can set any value between 30 and 3600.
Kiosk Branding	Select the default or custom branding options from the drop-down list.
Kiosk Exit PIN	Enter the 6-digit PIN that the user must type to exit the Kiosk mode. The PIN must have a minimum of 6 digits and a maximum of 10 digits. This PIN applies to all the devices in kiosk mode. Previously, the Kiosk PIN length was 4 digits. The user can continue to use the 4-digit PIN even after upgrading from a previous version to Ivanti Neurons for MDM 82. However, if there are any configuration changes, the PIN length must be set as per the new requirement (i.e., min 6 digits and max 10 digits). The Go app will protect the device against brute force attacks. For more information, see Go for Android documentation.
Enable Single App launcher Kiosk	Select to use the Kiosk mode to keep an app in foreground on GMS and non-GMS devices. You need to select an app from the App Catalog or enter a package ID.
Allow User Access to Ivanti Agent Settings	Select to access **Ivanti Agent Settings** while the device remains in **Single App Kiosk Mode**. Previously, the admin had to exit kiosk mode to access agent settings. After the setting is enabled and distributed to devices, users can open the Ivanti agent settings page by pressing and holding the Volume Up and Volume Down buttons simultaneously.

Setting	Description
	The feature is supported only on Android devices enrolled in Work Managed Device mode.
Enable Driver Safety **Create an Allowlist of apps:** These apps will be available to users in kiosk Mode by adding apps to the allowed apps list. Drag and Drop to arrange the apps in the order they should appear in the kiosk Mode launcher. Adding an application to the list of allowed apps will not install the app on the device. Be sure to distribute each app to the appropriate users and user groups in the App Catalogue.	Select to enable the Driver Safety icon for all the apps under the Kiosk Mode Allowed Apps section. Click the Driver Safety icon to disable the app If the speed crosses the limit.
Built-In Apps	Click +Add to include listed native apps in the group of apps allowed in kiosk mode. Under settings for the Kiosk Mode Allowed Apps, the following options are available: • **Clear app user data**: Enabling this option lets all the application data to be automatically cleared without any prompts when the user logs out of the kiosk. Select Enable Shared Device in the Kiosk mode settings for this option to be available with the applications. ◦ App data is not cleared for Google Chrome and webview package, even if they are added in the app whitelist with clear user data enabled. This is because Kiosk might crash if app data is cleared for these 2 packages. ◦ App data is not cleared for System apps for which app launcher is not available (both inside and outside kiosk). • **Make hidden**: Enabling this option allows the application to be accessible by other apps but is not available in the Kiosk launcher. If you have disabled Dialler or Camera in Lockdown settings above, they cannot be added to the Allowed Apps list.
App Catalogue Other Apps	Click +Add to included listed apps from the app catalogue in the group of apps allowed in kiosk Mode. Click +Add to include the package name of an app that is not available on the Google Play Store. For Samsung devices, admins should Allowlist the following dialler/system packages to make them functional in Kiosk mode for enabling dialler functionality in Kiosk mode. • Call – com.samsung.android.incallui

Setting	Description
Kiosk Mode Allowed Apps **Create an Allowlist of apps:** These apps will be available to users in kiosk Mode by adding apps to the allowed apps list. Drag and Drop to arrange the apps in the order they should appear in the kiosk Mode launcher. Adding an application to the list of allowed apps will not install the app on the device. Be sure to distribute each app to the appropriate users and user groups in the App Catalogue.	• Phone – com.samsung.android.dialer (should be Allowlisted and the admin should select hide option for this package to avoid issues with two dialler options for the user) • Call – com.sec.phone • Call Setting – com.samsung.android.app.telephonyui • Assisted Dialing – com.sec.providers.assisteddialing • Call Log Backup/Restore – com.android.calllogbackup • Dialler Storage – com.android.providers.telephony • Phone – com.android.server.telecom • Phone – com.android.phone • Smart Call – com.samsung.android.smartcallprovider • WiFi Calling – com.sec.unifiedwfc Click X to remove an app from the group of apps allowed in kiosk mode. Drag and drop to change the order in which apps appear on kiosk devices. **Add Folder** - You can use this option to create a folder under this section and move one or more apps to this folder. You can create folders up to two levels. The apps that are copied to one folder cannot be copied to another. Only 25 apps are supported within a folder.

Built-In Apps	Click +Add to include listed native apps in the group of apps allowed in kiosk mode. Under settings for the Kiosk Mode Allowed Apps, the following options are available:
	• **Clear app user data**: Enabling this option lets all the application data to be automatically cleared without any prompts when the user logs out of the kiosk. Select Enable Shared Device in the Kiosk mode settings for this option to be available with the applications.
	  ◦ App data is not cleared for Google Chrome and webview package, even if they are added in the app whitelist with clear user data enabled. This is because Kiosk might crash if app data is cleared for these 2 packages.
	  ◦ App data is not cleared for System apps for which app launcher is not available (both inside and outside kiosk).

Setting	Description
App Catalogue	• **Make hidden**: Enabling this option allows the application to be accessible by other apps but is not available in the Kiosk launcher. If you have disabled Dialler or Camera in Lockdown settings above, they cannot be added to the Allowed Apps list. Click +Add to included listed apps from the app catalogue in the group of apps allowed in kiosk Mode.
Other Apps	Click +Add to include the **package name** of an app that is not available on the Google Play Store. For Samsung devices, admins should Allowlist the following dialler/system packages to make them functional in Kiosk mode for enabling dialler functionality in Kiosk mode. • Call – com.samsung.android.incallui • Phone – com.samsung.android.dialer (should be Allowlisted and the admin should select hide option for this package to avoid issues with two dialler options for the user) • Call – com.sec.phone • Call Setting – com.samsung.android.app.telephonyui • Assisted Dialing – com.sec.providers.assisteddialing • Call Log Backup/Restore – com.android.calllogbackup • Dialler Storage – com.android.providers.telephony • Phone – com.android.server.telecom • Phone – com.android.phone • Smart Call – com.samsung.android.smartcallprovider • WiFi Calling – com.sec.unifiedwfc
Kiosk Mode Allowed Apps Enable Single App launcher Kiosk	Click X to remove an app from the group of apps allowed in kiosk mode. Drag and drop to change the order in which apps appear on kiosk devices. **Add Folder** - You can use this option to create a folder under this section and move one or more apps to this folder. You can create folders up to two levels. The apps that are copied to one folder cannot be copied to another. Only 25 apps are supported within a folder. Select to use the Kiosk mode to keep an app in foreground on GMS and non-GMS devices. You need to select an app from the App Catalog or enter a package ID.
Create an Allowlist of apps: These apps will be available to users in kiosk Mode by adding apps to the allowed apps list. Drag and Drop to arrange the apps in the order they should appear in the kiosk Mode launcher.	

Setting	Description
Adding an application to the list of allowed apps will not install the app on the device. Be sure to distribute each app to the appropriate users and user groups in the App Catalogue.	
Built-In Apps	Click +Add to include listed native apps in the group of apps allowed in kiosk mode. Under settings for the Kiosk Mode Allowed Apps, the following options are available: • **Clear app user data**: Enabling this option lets all the application data to be automatically cleared without any prompts when the user logs out of the kiosk. Select Enable Shared Device in the Kiosk mode settings for this option to be available with the applications. ◦ App data is not cleared for Google Chrome and webview package, even if they are added in the app whitelist with clear user data enabled. This is because Kiosk might crash if app data is cleared for these 2 packages. ◦ App data is not cleared for System apps for which app launcher is not available (both inside and outside kiosk). • **Make hidden**: Enabling this option allows the application to be accessible by other apps but is not available in the Kiosk launcher. If you have disabled Dialler or Camera in Lockdown settings above, they cannot be added to the Allowed Apps list.
App Catalogue Other Apps	Click +Add to included listed apps from the app catalogue in the group of apps allowed in kiosk Mode. Click +Add to include the **package name** of an app that is not available on the Google Play Store. For Samsung devices, admins should Allowlist the following dialler/system packages to make them functional in Kiosk mode for enabling dialler functionality in Kiosk mode. • Call – com.samsung.android.incallui • Phone – com.samsung.android.dialer (should be Allowlisted and the admin should select hide option for this package to avoid issues with two dialler options for the user) • Call – com.sec.phone • Call Setting – com.samsung.android.app.telephonyui • Assisted Dialing – com.sec.providers.assisteddialing • Call Log Backup/Restore – com.android.calllogbackup • Dialler Storage – com.android.providers.telephony • Phone – com.android.server.telecom • Phone – com.android.phone • Smart Call – com.samsung.android.smartcallprovider

Setting	Description
	• WiFi Calling – com.sec.unifiedwfc
Kiosk Mode Allowed Apps	Click X to remove an app from the group of apps allowed in kiosk mode. Drag and drop to change the order in which apps appear on kiosk devices. **Add Folder** - You can use this option to create a folder under this section and move one or more apps to this folder. You can create folders up to two levels. The apps that are copied to one folder cannot be copied to another. Only 25 apps are supported within a folder.
Enable Single App launcher Kiosk **Create an Allowlist of apps:** These apps will be available to users in kiosk Mode by adding apps to the allowed apps list. Drag and Drop to arrange the apps in the order they should appear in the kiosk Mode launcher. Adding an application to the list of allowed apps will not install the app on the device. Be sure to distribute each app to the appropriate users and user groups in the App Catalogue. Built-In Apps	Select to use the Kiosk mode to keep an app in foreground on GMS and non-GMS devices. You need to select an app from the App Catalog or enter a package ID. Click +Add to include listed native apps in the group of apps allowed in kiosk mode. Under settings for the Kiosk Mode Allowed Apps, the following options are available: • **Clear app user data**: Enabling this option lets all the application data to be automatically cleared without any prompts when the user logs out of the kiosk. Select Enable Shared Device in the Kiosk mode settings for this option to be available with the applications. ◦ App data is not cleared for Google Chrome and webview package, even if they are added in the app whitelist with clear user data enabled. This is because Kiosk might crash if app data is cleared for these 2 packages. ◦ App data is not cleared for System apps for which app launcher is not available (both inside and outside kiosk). • **Make hidden**: Enabling this option allows the application to be accessible by other apps but is not available in the Kiosk launcher. If you have disabled Dialler or Camera in Lockdown settings above, they cannot be added to the Allowed Apps list.
App Catalogue Other Apps	Click +Add to included listed apps from the app catalogue in the group of apps allowed in kiosk Mode. Click +Add to include the **package name** of an app that is not available on the Google Play Store.

Setting	Description
	For Samsung devices, admins should Allowlist the following dialler/system packages to make them functional in Kiosk mode for enabling dialler functionality in Kiosk mode. • Call – com.samsung.android.incallui • Phone – com.samsung.android.dialer (should be Allowlisted and the admin should select hide option for this package to avoid issues with two dialler options for the user) • Call – com.sec.phone • Call Setting – com.samsung.android.app.telephonyui • Assisted Dialing – com.sec.providers.assisteddialing • Call Log Backup/Restore – com.android.calllogbackup • Dialler Storage – com.android.providers.telephony • Phone – com.android.server.telecom • Phone – com.android.phone • Smart Call – com.samsung.android.smartcallprovider • WiFi Calling – com.sec.unifiedwfc
Kiosk Mode Allowed Apps	Click X to remove an app from the group of apps allowed in kiosk mode. Drag and drop to change the order in which apps appear on kiosk devices. **Add Folder** - You can use this option to create a folder under this section and move one or more apps to this folder. You can create folders up to two levels. The apps that are copied to one folder cannot be copied to another. Only 25 apps are supported within a folder.

For Samsung devices with Knox Standard 4.0 or higher, the multi-user feature is automatically locked down in kiosk mode.

Managed Devices with Work Profile

Disable certain features on managed device with work profile for Android 8.0+.

Certain features can be disabled for work profile on company owned devices (applicable for Android 11+ devices).

Setting	Description
Managed Device Lockdown Settings	
Disable Wi-Fi	Select to turn off access to wireless LANs.(Not applicable to Android 11+ devices)
Disable Wi-Fi Settings	Select to turn off access to wireless settings.
Disable Camera	Select to turn off camera access.
Disable Bluetooth	Select to turn off Bluetooth features. Use caution when using this option. Ivanti recommends against disabling audio because hands-free Bluetooth access is disabled. Legal requirements for hands-free use of devices while driving is becoming more widespread.
Disallow Bluetooth Settings	Select to turn off access to Bluetooth settings.
Disable Network Reset	Select to prevent resetting network (applicable to devices on Android 7.0 and later versions).
Mute Master Volume	Select to mute master volume. (Not applicable to Android 11+ devices)
Disallow Emergency Broadcasts	Select to prevent emergency broadcasts.
Disallow Mobile Networks	Select to turn off access to mobile networks. This cannot be disabled if Wi-Fi is disabled.
Disallow Tethering	Select to turn off tethering as an option for using the internet connection of one device to provide internet access to another device.
Disallow VPN	Select to turn off VPN connections. (Not applicable to Android 11+ devices)
Disable Factory Reset	Select to prevent users from returning the device to factory defaults. (Not applicable to Android 11+ devices)
Enable Factory Reset Protection	Select to allow users to return the device to factory defaults. You can optionally specify a list of authorised Google account IDs (an integer value) that can provision the device after factory reset, or hover over the help icon to view help for retrieving authorised account IDs.
Disallow Outgoing Calls	Select to prevent a user from making outgoing calls.
Disallow Safe Boot (Android 6.0+)	Select to prevent a user from rebooting a device into safe boot mode.
Disallow Debugging Features	Select to disable debugging features on devices. By default, this option is turned on.
Ensure Verify Apps	Select to allow application verification features on devices. By default, this option is turned on. When this option is turned off, the device goes back to its default behaviour which may vary from

Setting	Description
	device to device.
Disallow SMS	Select to prevent a user from sending and receiving SMS messages.
Disallow Unmute Microphone	Select to prevent a user from unmuting the device's microphone.
Disallow Auto Time	Select to prevent a user from enabling automatic time changes.
Disallow Auto Time Zone	Select to prevent a user from enabling automatic device time adjustment with time zone changes.
Disable Data Roaming	Select to turn off data exchange while the device is roaming.
Sync time with server (Android 9.0+)	Select to allow devices to sync time with the Ivanti Neurons for MDM servers first time on registration and thereafter once every 24 hours after each check-in. This option will be available only if the **Disable Auto-Time** is selected.
Set timezone (Android 9.0+)	Specify timezone string in Olson Time Zone ID format (for example, Pacific/Midway).
Disable Wi-Fi Sleep	Select to keep Wi-Fi on while the device is in Sleep mode. (Not applicable to Android 11+ devices)
Restrict Input Methods	Select to restrict input methods for work apps by designating a list of Allowlisted package names via the **Package Name** field.(Not applicable to Android 11+ devices) The devices will have both Allowlisted package input methods and the default system input methods available to use. The user can switch between default system input methods and Allowlisted packages input methods. In Android 10+, the input methods are applicable only for the device side, else they are restricted to the entire device.
Restrict Accessibility Services	Select to restrict accessibility services for work apps by designating a list of Allowlisted package names via the **Package Name** field. If there are no Allowlisted packages, then only system accessibility services will be allowed. In Android 10+, the input methods are restricted to Work Apps only, else they are restricted to the entire device.
Disable USB file transfer	Select to disable USB file transfer.
Disable external media	Select to disable external media.
Disallow Unknown Sources on device	Select to prevent the device from installing apps from unknown sources. This setting, to take effect on the device, is dependent on an expected Google Play update to enable this feature.
Set lock screen message (Android 7.0+)	Select to set the lock screen message to be displayed on the device. Type the lock screen message (maximum of 256 characters) in the text field. By enabling this option, the user is blocked from setting the message in Settings and the message that is set by the admin is displayed to the user.

Setting	Description
	If the admin does not provide any lock screen message after enabling 'Set lock screen message', the user is blocked from setting the message in Settings, but no message is displayed to the user.
Set screen brightness	Select to set brightness of your device's screen. • Manual - Select to enter a number manually (0 to 255) • Adaptive - Select to allow the device to set the brightness It is recommended to enable the "Disallow config brightness" option before setting the screen brightness of your device. If the user is allowed to make changes, these settings will be reset to the admin defined settings on next check-in. This setting is not supported on devices with Android 11 and later versions for Work Profile on Company Owned Device mode.
Set screen timeout	Select to set screen timeout duration (in seconds). It is recommended to enable the "Disallow config screen timeout" option before setting the screen brightness of your device. If the user is allowed to make changes, these settings will be reset to the admin defined settings on next check-in. This setting is not supported on devices with Android 11 and later versions for Work Profile on Company Owned Device mode.
Set screen orientation	Select to set screen orientation. You can set the screen orientation to 0, 90, 180, or 270 degrees from the drop down list. This setting is not supported on devices with Android 11 and later versions for Work Profile on Company Owned Device mode.
Disallow auto-fill (Android 8.0+)	Select to disallow auto-fill. (Not applicable to Android 11+ devices)
Disallow Bluetooth Sharing (Android 8.0+)	Select to disallow the user from sharing outgoing Bluetooth on the device.
Disable backup service (Android 8.0+)	Select to disable the backup service. (Not applicable to Android 11+ devices)
Disallow printing (Android 9.0+)	Select to restrict printing from all apps.(Not applicable to Android 11+ devices)
Disallow aeroplane mode (Android 9.0+)	Select to disable flight mode on the entire device.
Disallow ambient display (Android 9.0+)	Select to disallow the ambient display for the user. (Not applicable to Android 11+ devices)
Disallow config brightness (Android 9.0+)	Select to disallow the user from configuring the brightness (Not applicable to Android 11+ devices). It is recommended to define the "Set screen brightness mode" before selecting this option.

Setting	Description
Disallow config date time (Android 9.0+)	Select to disallow date, time and timezone configuration.
Disallow config location (Android 9.0+)	Select to disallow the user from disabling location providers.
Disallow config screen timeout (Android 9.0+)	Select to disallow the user from changing screen off timeout. (Not applicable to Android 11+ devices) It is recommended to set the "Set screen timeout" values before selecting this option.
Disallow system error dialogues (Android 9.0+)	Select to disallow system error dialogs.(Not applicable to Android 11+ devices)
Disable Screen Capture (Android 11.0+) **Android 12.0+**	Select to turn off the ability to use the device's built-in screen capture feature. When selected, screen capture is disabled on the personal side of the device.
Enable USB for charging only	Select to enable the USB port for charging only.
Android 13.0+	
Set Minimum Required Wi-Fi Security	Use this option to set minimum required Wi-Fi security: • No minimum security required – Select this option if no minimum security is required • Personal Network Based Security – Select this option to block personal Wi-Fi networks such as WEP, WPA/WPA2/WPA3, etc. • Enterprise EAP Network Based Security – Select this option to block EAP protocol-based Wi-Fi networks • Enterprise 192 Network Based Security - Select this option to block EAP corporate-based Wi-Fi networks All the existing devices that do not meet the minimum criteria will be disconnected. Device details will show the Minimum Required Wi-Fi Security level (if available) under the **General > Wi-Fi Security Level**.
Disallow Sharing Admin Configured Wi-Fi	Select to prevent users from sharing Wi-Fi configurations set by the administrator.
Work Profile Lockdown Settings	
Disable Screen Capture	Select to turn off the ability to use the device's built-in screen capture feature.
Disallow Apps Control	Select to prevent a user from modifying applications in Settings or launchers.

Setting	Description
Disallow Config Credentials	Select to prevent a user from configuring user credentials.
Disallow Cross Profile Copy Paste	Select to prevent copy/paste of information between profiles.
Disallow Modify Accounts	Select to prevent a user from adding or removing accounts.
Disallow NFC (Outgoing Beam) (Android 5.1+)	Select to prevent a user from using NFC to transfer app data.
Disallow Share Location	Select to prevent websites and apps from prompting the device user to share device location.
Disallow Debugging Features	Select to disable debugging features on devices. By default, this option is turned on.
Ensure Verify Apps	Select to allow application verification features on devices. By default, this option is turned on. When this option is turned off, the device goes back to its default behaviour which may vary from device to device.
Disable unknown sources inside work profile	Select to disallow download from unknown sources within the work profile.
Enable/Disable System Apps	Select to enable and disable system applications to be deployed by designating two lists of package names via the **System App Package Name** fields. Use this feature to manage access to system applications that are not published in Google Play. Adding an app to the app catalog and also to a system apps list is not supported.
Disable Caller ID (Android 6.0 +)	Sets whether caller ID information from the work profile will be shown in the device for incoming calls.
Disable Contact sharing via Bluetooth (Android 6.0+)	Select to prevent the device from sharing contacts with other devices via Bluetooth.
Disable Contact sharing via Search (Android 7.0+)	Select to prevent the users from searching for work contacts from the personal phone dialler.
Disallow auto-fill (Android 8.0+)	Select to disallow auto-fill. (Not applicable to Android 11+ devices)
Disallow work app notifications in	Select to restrict work profile notifications.

Setting	Description
personal profile (Android 8.0+)	
Disallow printing (Android 9.0+)	Select to restrict the printing from all apps. (Not applicable to Android 11+ devices)
Disallow share into Profile (Android 9.0+)	Select to prevent users from sharing personal data into a work profile on the device.
Restrict input methods (Android 10.0+)	Select to restrict Allowlisted IME package names by designating a list of Allowlisted package names via the **Package Name** field (Not applicable to Android 11+ devices). The devices will have both Allowlisted package input methods and the default system input methods available to use. The user can switch between default system input methods and Allowlisted packages input methods. The input methods will apply for IME apps installed on the work profile side. Even if the apps installed on the device side are Allowlisted for this lockdown, those will not be available for apps to use on the work profile side.
Allow Access to work profile calendars (Android 10.0+)	Select any of the following options to allow all apps or select a set of apps on the personal side to access the calendar information present in the work profile: • **All Apps on Personal Profile** - allow all apps to access calendar information present in the work profile • **Only the following apps on Personal Profile**- In the text field below, enter the bundle IDs of the apps separated by a comma. Only these selected apps on the personal side will be allowed to access the calendar information present in the work profile. The app on the personal side should implement specific APIs to be able to access a shared calendar.
Enable Cross profile Allowlisting of Apps (Android 11.0+)	Select the checkbox to enable users to share information from specific apps from within the work profile to the personal side of the device. In the **Allowlisted Apps** field, type the Package IDs of the apps to be Allowlisted, separated by commas. By default, this option is disabled.
Enable Maximum Profile Timeout (Android 11.0+)	Select to set a maximum time window the work profile can be turned off before Ivanti Neurons for MDM suspends personal apps on the device. You can set a time between 72 and 8,760 hours. 8,760 hours is one year of time. Default value is set to 72 hrs if the option is selected. The device user sees a message prompting to turn on the work profile to enable suspended apps. Available for Android 11+ devices in Work Profile on Company Owned Device. If the profile is turned off for longer durations, personal apps are suspended on the device.
Enable 5G Network Slicing (Android 12.0+)	Select to provide a 5G network slicing option on Work-Profile of the company-owned devices. By default, this option is disabled.
Disable AI Assist (Android 15.0+)	Select to prevent users from AI Assist features. By default, this option is disabled.

For more information, see **How to create a configuration**

10.10.4.33. Lockdown & Kiosk: Samsung Knox Standard

A Lockdown & Kiosk: Samsung Knox Standard configuration disables certain features of Samsung Knox Standard devices and creates an Allowlist of apps that will be available to users in Kiosk mode.

> Samsung KNOX Standard Configuration is deprecated and not supported on devices with Android 9 and later versions.

Lockdown settings

Setting

What To Do

Name

Enter a name that identifies this configuration.

Description

Enter a description that clarifies the purpose of this configuration.

Samsung Knox Lockdown Settings: Disable certain features on Samsung Knox devices only.

Disable Wi-Fi

Select to turn off access to wireless LANs.

Disable Camera

Select to turn off camera access.

Disable Bluetooth

Select to turn off Bluetooth features.

Allow Bluetooth Audio-only

Select to turn on Bluetooth audio features only.

Disable Mobile Data

Select to turn off exchange of data when one device touches another.

This cannot be disabled if Wi-Fi is disabled.

Disable GPS

Select to turn off GPS.

Disable Phone Dialler

Select to turn off the phone app.

Disable SD Card

Select to turn off SD card access.

Disable Google Backup

Select to turn off backups to Google servers.

Disable Copy/Paste

Select to turn off access to copy/paste functions.

Disable NFC

Select to turn off NFC (Near-field Communication) data exchange when the device touches another device.

Disable Microphone

Select to turn off app access to the device microphone.

Disable Screen Capture

Select to turn off the ability to use the device's built-in screen capture feature. Turning on this option does not allow screen captures of Go. Such screen captures are disallowed.

Disable Bluetooth Tethering

Select to turn off Bluetooth tethering as an option for using the internet connection of one device to provide internet access to another device.

Disable USB Debug

Select to turn off the USB debugging feature.

Disable USB Tethering

Select to turn off USB tethering as an option for using the internet connection of one device to provide internet access to another device.

Disable Wi-Fi Tethering

Select to turn off Wi-Fi tethering as an option for using the internet connection of one device to provide internet access to another device.

Disable Native Browser

Select to prevent users from accessing the Android browser.

Disable YouTube

Select to prevent users from accessing YouTube.

Disable Factory Reset

Select to prevent users from returning the device to factory defaults.

Disable OTA Upgrade

Select to turn off over-the-air upgrades of the device firmware.

Warning: Do not disable **Disable Setting Changes** if **OTA Upgrade** is enabled. **Disabling Setting Changes** when **OTA Upgrade** is enabled can result in a non-functional device because setting changes are required for upgrade.

Disable Voice Roaming

Select to turn off access to voice calls while the device is roaming.

Disable USB Media Player

Select to turn off the USB media player.

Disable Google Play

Select to turn off access to Google Play.

Disable Data Roaming

Select to turn off data exchange while the device is roaming.

Disable Unknown Sources

Select to disable installing apps from anywhere but the Google Play Store, except for the Go app.

Disable Device Admin Privileges Removal

Select to prohibit users from turning off device admin privileges from Go.

Disable Setting Changes

Select to turn off access to the device Settings app.

Warning: Do not disable **Disable Setting Changes** if **OTA Upgrade** is enabled. **Disabling Setting Changes** when **OTA Upgrade** is enabled can result in a non-functional device because setting changes are required for upgrade.

Kiosk Mode Settings: Kiosk Mode applies additional restrictions to the devices including limited access to apps via a customised launcher.

Applicable to Android versions up to 8.1. For Android versions 9.0, use Android Enterprise Managed Device Kiosk configuration.

Enable Kiosk Mode

Select to configure **Kiosk Mode** on Android devices.

Allow User to Access Wi-Fi Settings

Select to allow a user to change Wi-Fi settings and access preferred wireless networks.

Allow User to Access Bluetooth Settings

Select to allow a user to change the Bluetooth settings and pair additional Bluetooth devices.

Allow User to Delay Application Updates

Select to allow a user to delay application updates.

GPS Location Settings

Select one of the following GPS location settings:

- Disable Location
- Enable Location
- Allow User to Select

Kiosk Exit PIN

Enter the four-digit code that the end user must type in order to exit Kiosk Mode.

Create an Allowlist of apps: These apps will be available to users in Kiosk Mode by adding apps to the allowed apps list. Drag and Drop to arrange the apps in the order they should appear in the Kiosk Mode launcher.

Adding an application to the list of allowed apps will not install the app on the device. Be sure to distribute each app to the appropriate users and user groups in the App Catalogue.

Built-In Apps

Click +Add to include listed native apps in the group of apps allowed in Kiosk Mode.

If you have disabled Dialler or Camera in Lockdown settings above, they cannot be added to the Allowed Apps list.

App Catalogue

Click +Add to included listed apps from the app catalogue in the group of apps allowed in Kiosk Mode.

Other Apps

Click +Add to include the **package name** of an app that is not available on the Google Play Store.

Kiosk Mode Allowed Apps

Click X to remove an app from the group of apps allowed in Kiosk Mode. Drag and drop to change the order in which apps appear on kiosk devices.

> Using Kiosk mode on Android 4.4 or supported newer versions, Samsung devices that support multiple users, will automatically lock down the multi-user feature while in Kiosk mode.

For more information, see **How to create a configuration**

10.10.4.34. Local Administrator Password Solution Configuration

The **Local Administrator Password Solution (LAPS)** configuration settings enable Ivanti Neurons for MDM administrators to automatically regenerate the local administrator password on managed macOS devices at set intervals. For more information on LAPS, see Local Admin Password Solution (LAPS).

Applicable to: macOS devices that are enrolled and managed using Automated Device Enrollment.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Local Administrator Password Solution (LAPS)** configuration.
3. Configure the **LAPS** settings as per the following table:

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
OS Platform	Select macOS from the dropdown.
Rotation Interval	Select one of the following options from the dropdown list to define the automatic rotation of passwords: • No Rotation (**default**) • 15 Days • 30 Days • 60 Days • 90 Days • 120 Days • 180 Days
Rotation After Viewing Interval	Select one of the following options from the dropdown list to automatically rotate the passwords after viewing it from the **Device Details** page: • 1 to 24 Hours • 36 Hours • 48 Hours The default value is set to **2 Hours**.

4. Click **Next** to configure the distribution settings.
5. Select one of the distribution options to set up the **Local Administrator Password Solution (LAPS)** configuration. For more information about configuring distribution options, see Working with Configurations.
6. Click **Done**.

10.10.4.35. macOS Firewall

Licence: Gold

macOS Firewall manages the Application Firewall settings that are accessible in the Security Preferences pane on macOS devices.

Applicable to: macOS 12.3+

- **Allow built-in software to receive incoming connections** - If true, allows the built-in software to receive incoming connections.
- **Allow downloaded signed software to receive incoming connections** - If true, allows downloaded signed software to receive incoming connections.

Applicable to: macOS 12.0+

- **Enable logging** - If true, enables logging
- **Specify the type of logging**
  - **Throttle**
  - **Brief**
  - **Detail**

Applicable to: macOS 10.12+

When you click **Enable Firewall**, you can select one or more of the following options:

- **Block All Incoming** - Select to prevent all sharing services from receiving incoming connections on macOS devices, such as screen sharing or file sharing. The following system services may still receive incoming connections:
  - configd, which implements DHCP and other network configuration services
  - mDNSResponder, which implements Bonjour
  - racoon, which implements IPSec
- **Enable Stealth Mode** - Select to prevent macOS devices from responding to probing requests. Managed macOS devices still answer incoming requests for authorised apps, while ignoring unexpected requests, such as ICMP (ping).
- **Applications** - The list of applications with connections controlled by the firewall. Select specific apps for which you want to receive incoming connections on macOS devices.

Select **Add+** to add a row to the list of apps. Select the cell under **Bundle ID** to select the app whose incoming connections you want to explicitly allow. Select the check box in the **Allow Connections** cell to allow incoming connections from the selected app.

> The configuration must exist in a system-scoped profile. If more than one profile contains this configuration, then the most restrictive union of settings will be used.

> The **Automatically allow signed downloaded software** and the **Automatically allow built-in-software** options are not supported. However, both the options will be forced ON when this configuration is available.

> The Administrator can enable the stealth mode by specifying a device that cannot be discovered by the ping command.

10.10.4.36. macOS Restrictions

Licence: Gold

macOS restrictions determine which restrictions are enabled on macOS devices.

You can set the following features to be enabled or disabled on macOS devices:

macOS Version	Features
macOS 10.11+	• Allow Camera • Allow iCloud Document Sync **Supervised only:** • Allow Spotlight Internet Results
macOS 10.11.2+	
	• Allow Definition Lookup
macOS 10.12+	• Allow iCloud Keychain Sync • Allow Back to my Mac • Allow Find my Mac • Allow sharing to Notes, Reminders, or LinkedIn • Allow Bookmark Sync • Allow macOS mail iCloud Service • Allow macOS iCloud Calendar Service • Allow macOS iCloud Address Book Service • Allow iCloud Reminder Service • Allow Auto Unlock **Supervised only:** • Allow Apple Music
macOS 10.12.4+	
	• Allow Finger Print for Unlock
macOS 10.13+	• Allow iTunes File Sharing • Allow Content Caching • Allow modification of Wallpaper **Supervised only:** • Allow AirPrint • Allow AirPrint iBeacon Discovery

macOS Version	Features
	• Force AirPrint Trusted TLS Requirement • Allow AirDrop • Allow Game Centre
macOS 10.13.4+	**Supervised only:** Defer software updates for a range of days (30 to 90 days). Default: 30 days.
macOS 10.14+	
macOS 10.14.4+	**Supervised only:** Allow nearby devices to share requests for a password • Allow Screenshots • Allow remote screen observation **Supervised only:** • Allow automatically to join classroom • Allow classroom to request permission to leave classes • Allow classroom to lock an app and lock the device without prompting • Allow force unprompted managed classroom screen observation
macOS 11.0+	
macOS 11.3+	**Supervised only:** Allow to force delay App Software Updates Enforced Fingerprint timeout Default: 48 hours Prerequisite: Touch ID must be configured on the device
macOS 11.3+	**Supervised only:** • Enforced Software Update Major OS Deferred Install Delay

macOS Version	Features
	• Enforced Software Update Minor OS Deferred Install Delay • Enforced Software Update Non OS Deferred Install Delay • Force Delayed Major Software Updates
macOS 12+ **macOS 13.0 till 26.0**	• allowCloudPrivateRelay: If you set the Private Relay ON in a macOS device, the network traffic is encrypted so that the internet activity is private and secure. This restriction requires a supervised device. • Allow iCloud Photo Library Supervised only: • Allow Erase Content and Settings
macOS 14.0+	• Allow Background Security Improvements Installation: To disable the responses. The user cannot install background security improvements. • Allow Background Security Improvements Removal: To block the user from being able to undo the responses. The user cannot remove background security improvements. • Allow Universal Control: ◦ If **True**, the configuration lets you use the input devices of the primary device to control the secondary display device. ◦ If **False**, you can add a secondary display device but cannot control it with the primary input devices. Supervised only: • Allow UI Configuration Profile Installation: If False, the configuration does not allow the installation of profile, configuration, or certificates on the macOS device. • Allow USB Restricted Mode: If True, the configuration locks the device from using remotely connected input devices. The Allow Accessories to Connect options are greyed out on the device.
	• Allow ARD Remote Management Modification ◦ If False, prevents modifying the Remote Management Sharing setting in System Settings. ◦ Default: true • Allow Bluetooth Sharing Modification ◦ If false, prevents modifying Bluetooth setting in System Settings. ◦ Default: true • Allow Cloud Freeform ◦ If false, disallows iCloud Freeform services.

macOS Version	Features
	◦ Default: true • Allow File Sharing Modification ◦ If false, prevents modifying File Sharing setting in System Settings. ◦ Default: true • Allow Internet Sharing Modification ◦ If false, prevents modifying Internet Sharing setting in System Settings. ◦ Default: true • Allow Local User Creation ◦ If false, prevents creating new users in System Settings. ◦ Default: true • Allow Printer Sharing Modification ◦ If false, prevents modifying Printer Sharing setting in System Settings. ◦ Default: true • Allow Remote Apple Events Modification ◦ If false, prevents modifying Remote Apple Events Sharing setting in System Settings. ◦ Default: true • Allow Siri ◦ Default: true • Allow Startup Disk Modification ◦ If false, prevents modification of Startup Disk setting in System Settings. ◦ Default: true • Allow Time Machine Backup ◦ If false, prevents modification of Time Machine settings in System Settings. ◦ Default: true Supervised only: • Allow account modification ◦ If false, prevents account modification. ◦ Default: true • Allow modifying Device Name ◦ If false, prevents changing the Device Name. ◦ Default: true • Allow modifying TouchID fingerprints ◦ If false, prevents from modifying Touch ID fingerprints. ◦ Default: true

macOS Version	Features

macOS 15.0+	Supervised only:
	• Allow Genmoji
	  ◦ Select to allow the creation of Genmojis.
	  ◦ Default: true
	• Allow Image Playground
	  ◦ Select to allow the use of image generation.
	  ◦ Default: true
	• Allow iPhone Mirroring
	  ◦ Select to allow the iPhone to mirror in a macOS device.
	  ◦ Default: true
	• Allow Writing Tools
	  ◦ Select to enable Apple Intelligence writing tools.
	  ◦ Default: true

macOS 15.1+
 	
macOS 15.2+
	Supervised only:
	• Allow Mail Summary
	  ◦ Select to allow the creation of summaries of email messages manually.
	  ◦ Default: true
	• Allow Media Sharing Modification
	  ◦ Select to allow the modification of Media Sharing Settings.
	  ◦ Default: true

	Supervised only:
	• Allow External Intelligence Integrations
	  ◦ Select to enable the use of external cloud-based intelligence services with Siri.
	  ◦ Default: true
	• Allow External Intelligence Integrations Sign-In
	  ◦ Select to enable default browser preference modification. The Ivanti Neurons for MDM settings command to set the default browser preference will still work when this is applied.
	  ◦ Default: true

macOS Version	Features

macOS 15.3	**Security and Privacy**:
	• Allow External Intelligence Workspace IDs
	  ◦ Enter allowed External Intelligence Workspace ID
	• Allow Notes Transcription Summary
	  ◦ Select to enable creation of summaries from Transcriptions.
	  ◦ Default: true

10.10.4.37. macOS AppStore Restrictions

Licence: Gold

macOS AppStore Restrictions define which restrictions are enabled in macOS AppStore.

You can set the following options:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Configuration Setup	
macOS Version	**Features**
10.9+	Restrict app installations to admin users.
10.10+	• Restrict app installations to software updates only. • Disable app adoption by users. • Disable software update notifications.
10.11+	Restrict App installation to MDM-installed apps and software updates.

Distributing the configuration

Procedure

1. Set the options using the preceding table.
2. Click **Next**.
3. Select the **Enable this configuration** option.
4. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom

Click **Done**.

10.10.4.38. macOS Disk Burning Restrictions

Licence: Gold

macOS Disk Burning Restrictions manage disk burning restrictions in macOS. You can configure the **macOS Finder Settings** to enable or disable disc burning options from the Finder app on macOS.

You can set the following options:

Setting	**What To Do**
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Configuration Setup	
Setting	**What To Do**
Allow Disk Burning	• ON • OFF • Require Authentication

Distributing the configuration

Procedure

1. Set the options using the preceding table.
2. Click **Next**.
3. Select the **Enable this configuration** option.
4. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom

Click **Done**.

10.10.4.39. Allowed Media Control (Deprecated)

Licence: Gold

Allowed Media Control configuration manages mounting, unmounting, and eject on logout for various physical media in macOS.

You can set the following options:

Setting	What To Do
Name Description	Enter a name that identifies this configuration. Enter a description that clarifies the purpose of this configuration.
Configuration Setup	
Mount control for media types	
Turn on the mount control for each media type and set the mount settings. If you turn off the mount control, then OS default setting will apply.	
Media Type	**Mount Settings**
• CD • DVD • BD	• Read-only with authentication • Deny Mount • Eject Media
• Blank CD • Blank DVD • Bland BD • DVD-RAM • Disk Image • Internal Hard Disk • External Hard Disk • Network Disk	• Read-only • Deny Mount • Eject Media • Authenticate
• External Hard Disk includes USB HDD, USB Flash Drive storage, and SD-Cards. • Read-only media such as CD, DVD, and BD are mounted as read-only by default.	
Unmount control for media types	
Turn on the unmount control for each media type and set the unmount settings. If you turn off the Unmount control, then OS default setting will apply. Exercise caution when you set Deny Unmount setting for media types.	
Media Type	**Mount Settings**
• CD • DVD • BD • Blank CD	• Deny Unmount • Authenticate

Setting	What To Do
• Blank DVD • Bland BD • DVD-RAM • Disk Image • Internal Hard Disk • External Hard Disk • Network Disk	
Eject on logout settings	
Media types to be ejected automatically when the user logs out.	
Media Type	
• CD • DVD • BD • Blank CD • Blank DVD • Bland BD • DVD-RAM • Disk Image • External Hard Disk • Network Disk	

Distributing the configuration

Procedure

1. Set the options using the preceding table.
2. Click **Next**.
3. Select the **Enable this configuration** option.
4. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom

Click **Done**.

10.10.4.40. macOS Finder Settings

Licence: Gold

macOS Finder Settings manage settings of Finder app in macOS.

You can set the following options:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Configuration Setup	
Setting	**What To Do**
Disable Disc burn support in Finder	• Turn ON • Turn OFF

Distributing the configuration

Procedure

1. Set the options using the preceding table.
2. Click **Next**.
3. Select the **Enable this configuration** option.
4. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom

Click **Done**.

10.10.4.41. macOS Kernel Extension Policy

Applicable to: macOS 10.13.2 or supported newer versions.

Controls restrictions and settings for loading user-approved Kernel Extensions.

Creating a macOS Kernel Extension Policy configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **kernel** in the search field, and then click the **macOS Kernel Extension Policy** configuration.
4. Name and describe the configuration.
5. Select the **Allow User Overrides** option to allow users to approve additional kernel extensions not explicitly allowed by the following configuration.
6. In the Allowed Team Identifiers and Kernel Extensions section, click **+ Add** to add allowed team identifiers and kernel extensions. A kernel extension is the bundle identifier of a package. For each team identifier, you can add several validly signed kernel extension names in the pop-up window.
7. Click **Add**.
8. Click **Next** to configure the distribution settings.
9. Click **Done**.

For more information, see **How to create a configuration**

10.10.4.42. Mobile@Work for macOS

This section contains the following topics:

- Mobile@Work for macOS configuration and scripts execution workflow
- Creating a Mobile@Work for macOS configuration
- Enabling User Onboarding for macOS devices
- Creating a Mobile@Work for macOS Script configuration
- Perform a clean uninstall of Mobile@Work for macOS
- Applying Scripts via macOS Mobile@Work

Ivanti Neurons for MDM allows you to create your own macOS shell scripts, which you can then upload to Ivanti Neurons for MDM and run on managed macOS devices. For information about creating, uploading, and managing the scripts repository, see **All Scripts**.

A macOS device user can initiate the device to be retired using Mobile@Work for macOS 1.1 or later. The retire option is available when you click **Uninstall** from the About Mobile@Work screen. In Ivanti Neurons for MDM, you can verify the status of the device in the **Devices** page and on the device details page.

Mobile@Work for macOS 1.5 or later opens Apps@Work immediately after registration without waiting for the MDM registration to complete.

In Mobile@Work for macOS, click on an application tile to display the App Details page for that application. The page includes app description, screen shots, ratings and reviews.

Mobile@Work for macOS notifies the Ivanti Neurons for MDM server if the Packager in-house macOS apps are installed or not installed in the inventory report.

Prerequisites

In the **App Catalog**, the Mobile@Work for macOS client is available as a business app. Before you can run shell scripts on macOS devices, instruct the users to register their devices with Ivanti Neurons for MDM using Mobile@Work for macOS.

Procedure

1. Download the Mobile@Work for macOS application. It is available as a PKG file at **https://support.mobileiron.com/support/CDL.html**. See **this Ivanti customer forums article** for information on getting credentials for the download site.
2. Upload the PKG file for Mobile@Work for macOS to a secure server. This server must be accessible to device users.
3. Share the URL of the installation file for Mobile@Work for macOS with the device users via an e-mail or a message.
4. Instruct the users to:
    1. Download and install Mobile@Work for macOS on their device.
    2. Register the devices with Ivanti Neurons for MDM using Mobile@Work for macOS.

Mobile@Work for macOS configuration and scripts execution workflow

Procedure

1. Set up and distribute a Mobile@Work for macOS configuration.

2. Set up and distribute a Mobile@Work for macOS Script configuration to upload the script to Ivanti Neurons for MDM. The scripts are encrypted and signed using a signed certificate, which is unique per tenant. The key to decrypt the script is sent to the device along with download URL to the script, which is encrypted and signed.
3. Ivanti Neurons for MDM executes the scripts on macOS devices using Mobile@Work for macOS. Mobile@Work for macOS polls Ivanti Neurons for MDM periodically to check whether there are any scripts awaiting execution. If there are scripts in the queue, Mobile@Work downloads and runs the scripts on macOS devices according to settings you define on Ivanti Neurons for MDM.
4. Mobile@Work for macOS returns the script execution results to Ivanti Neurons for MDM, which are shown in the device logs. You can check the device logs from the device details page of the macOS device, in the **Logs** tab.

Creating a Mobile@Work for macOS configuration

A default system configuration for the Mobile@Work for macOS configuration is available. However, it is not distributed to any devices by default.

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **work** in the search field, and then click the **Mobile@Work for macOS** configuration.
4. Name and describe the configuration.
5. Enter **Max Run Time** in seconds to specify how long a script can run. The default value is 60 seconds.
6. Enter **Max Response Size** in kilobytes (KB) to specify the maximum response size limit of the output of the script that is returned to Ivanti Neurons for MDM. This is the stdout or stderr data that is returned when running the script. The default value is 1 KB.
7. Enter **Check-in Frequency** in minutes to specify how often the Mobile@Work for macOS app must check-in with Ivanti Neurons for MDM. The default value is 15 minutes.
8. (Optional) You can enable user onboarding for macOS devices using the Enabling User Onboarding for macOS devices section.
9. Click **Next** to configure the distribution settings.
    1. Choose a distribution level:
    2. **To everyone** - The app is added to all the user compatible devices.
    3. **To no one** - The app is staged for distribution at a later date.
    4. **Custom Distribution** - Select any of the following options:
        - **User/User Groups** - The app is distributed to only the users or user groups you choose.
          Click the **Users** tab to select the user(s).
          Click the **User Groups** tab to select the user group(s).
        - **Device/Device Groups** - The app is distributed to only the devices or device groups you choose.
          Click the **Devices** tab to select the device(s).
          Click the **Device Groups** tab to select the device group(s).
10. Click **Done**.

Enabling User Onboarding for macOS devices

You can enable user onboarding for macOS devices during the automated Device Enrollment process as follows:

- As soon as the Device Enrollment is completed, Mobile@Work for macOS (version 1.68 or later is required) is pushed to the device along with the profiles, configurations and apps.
- The Mobile@Work for macOS client and other apps are pushed to the devices only if:
  - The apps are either in-house PKG apps or Apple Apps and Books public apps.
  - The silent installation setting for the apps is set to true. The setting is available from the **Apps** > app details > **App Configuration** > **Install on device** page.
  - The priority for the apps is set to High. By default, the priority of the Mobile@Work for macOS client app is set to high (and it cannot be modified), **without which the user onboarding process may fail**.
  - The apps are configured to be distributed to the devices, user groups, or device groups.
- After Mobile@Work for macOS is installed and registered, the macOS device enters the kiosk mode (user has no control of the device) until the remaining profiles, configurations, and apps are configured and installed. The progress is displayed in steps.

For Mobile@Work for macOS 1.73 or later versions as supported by Ivanti Neurons for MDM, the following additional features are supported:

- The user onboarding process is completed soon after the Device Enrollment is completed for a device. The user onboarding process does not start after the time window to trigger user onboarding is expired (typically 20 minutes after device registration) even if an administrator enables user onboarding in the Mobile@Work configuration. This prevents a device from entering the user onboarding kiosk mode when the device is in regular usage.
- The user onboarding process is displayed in steps in the Mobile@Work for macOS client. Configurations will be installed as part of the first step.
- High-priority apps will be installed initially. Each high-priority app will be counted as one step. Packager apps are not counted as part of the steps.
- Remaining apps will continue to be installed in the background even after user onboarding is complete. Applications are marked as installed after the installation is initialised on a device or after the application is actually installed on the device.
- After user onboarding, you can go to the device details page to verify the configurations and apps pushed to each device. More information is available in the logs.

Procedure

1. Create a Mobile@Work for macOS configuration using **Creating a Mobile@Work for macOS configuration**.
2. Select the **Enable User Onboarding** option.
3. Enter the following details:
   - **User Onboarding Timeout Value** - Enter the approximate time that the device will take to install the app and configurations during the initial device setup. By default, the user onboarding process on a macOS device times out in 120 seconds, which you can modify as required.
   - **User Landing Page URL** - Provide a landing page URL to be displayed to the user after onboarding is completed.
4. Click **Next** to configure the distribution settings.
5. Click **Done**.

Creating a Mobile@Work for macOS Script configuration

You can create and distribute multiple Mobile@Work for macOS Script configurations to the devices. Using this configuration, you can select a script from the repository (**Admin > Scripts and Files > All Scripts**) to distribute to Mobile@Work for macOS.

You can schedule script executions on devices with Mobile@Work for macOS 1.66 or later versions. If you schedule a script execution to run on devices with Mobile@Work for macOS client versions earlier than 1.66, then the script is executed only once. If the Mobile@Work for macOS client is upgraded from 1.4 to 1.66, then all the macOS client configurations will be redistributed to the devices.

Prerequisites

- Go to **Admin > Scripts and Files > All Scripts** to upload and manage scripts that can be used in this configuration and distributed to devices.
- Configure and distribute the Mobile@Work for macOS configuration on devices. Otherwise, the Mobile@Work for macOS Script configuration will be in the Error state.

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **work** in the search field, and then click the **Mobile@Work for macOS Script** configuration.
4. Name and describe the configuration.
5. In the **Select Script** field, enter the name of the script to find and select the script from the drop-down list.
6. In the Script Input section, the script input labels and script variables associated with the script are displayed. If you need to override them, enter alternate script variables (for example, {$userWorkEmailAddress}) and their alternate default values (for example, john.doe@company.com).
7. In the Script Execution section, select one of the following scheduling options:
    - Execute Once On Deployment
    - Recurring Execution
8. If you choose Recurring Execution, specify the following details:
    - Timezone to use - Select Device's Local Time or UTC Time. The script will be executed at the time selected in this field.
    - Execution Starts on - Select the start date.
    - Execution Ends on - Select the end date (greater than or equal to the start date).
    - Execute Script - Select Daily or Weekly and enter the hours (in 24 hours format), minutes, and days as applicable.
9. Click **Next** to configure the distribution settings.
10. Click **Done**.

Perform a clean uninstall of Mobile@Work for macOS

If you have enabled the option **Remove apps on un-enrollment(Applicable to managed apps only)** during installation of Mobile@Work for macOS and if you initiate the device to be retired from the Ivanti Neurons for MDM administrator portal, then the Mobile@Work for macOS application and the uninstall script is just deleted from the device. To avoid the processes and scripts from running in the back end, ensure that during device registration of new users or retirement of existing users, you deselect the following option from the Ivanti Neurons for MDM administrator portal to ensure that the uninstall script runs and deletes the associated processes and scripts from the back end.

Procedure

1. Log in to the Ivanti Neurons for MDM administrator portal.

2. Go to **Apps** > **Mobile@Work** > **App Configurations** > **App Configurations Summary list** > **Apple App Settings** >**Apple Application Management configuration settings**.
3. From the **Configuration Setup** page deselect the following option:
    - **Remove apps on un-enrolment (Applicable to managed apps only)**.

Applying Scripts via macOS Mobile@Work

Scripts via macOS Mobile@Work allow administrators to remotely deploy and run shell scripts on managed macOS devices. This helps automate tasks, apply fixes, enforce policies, and streamline configuration without requiring user intervention, ensuring consistent and efficient device management at scale.

Prerequisites:

- Devices must be running macOS.
- Mobile@Work for macOS must already be installed on the devices.
- Ensure that the Mobile@Work for macOS configuration is properly created, distributed, and assigned. For more details, see **Creating a Mobile@Work for macOS configuration**.

> You cannot apply Scripts via macOS Mobile@Work if the device does not have the Mobile@Work client installed and configured, or if the device platform does not support script execution. Ensure the macOS client is active and that you select only supported macOS devices.

Procedure

1. Log in to the Ivanti Neurons for MDM administrator portal.
2. Go to **Devices** and select the list of macOS devices for which you want to execute the script.
3. In the **Devices** page, navigate to **Actions** > **macOS** > **Scripts via macOS Mobile@Work**.
   The **Scripts via macOS Mobile@Work** pane appears.
4. To apply the scripts, in the **Select Script** field, enter and select the script name.
   For more information on creating a script, see **All Scripts**.
5. Select **OK** to execute the script on the devices.

Related topics:

- **Admin > Scripts and Files > All Scripts**
- **How to create a configuration**

10.10.4.43. macOS Software Update Rules Configuration

Administrators can configure the software update policy of a device by defining the **macOS Software Update Rules**.

Applicable to: macOS 10.7 till 26.0.

1. Go to Configurations > +Add.
2. Type macOS in the search field, and then click the macOS Software Update Settings configuration.
3. Enter a Name and Description of the configuration.
4. Select the required configurations from **macOS Software Update Rules**.
5. Click Next.
6. Select Enable this configuration option.
7. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
8. Click Done.

macOS Software Update Rules

Admins can select from the list of rules as follows:

> Users cannot change these settings when these rules are applied on the device.

- Allowing pre-release software installation.
- Automatically:
    - Check for updates
    - Download new updates when available
    - Install macOS updates
    - Install app updates from app store
    - Install system data files and security updates.
- Restrict App installations to admin users.
- Option to add URL of the software update catalogue (unsupported on macOS 11+).

10.10.4.44. Certificate Preference

Applicable to:

- macOS 10.12 through the most recently released version as supported by by Ivanti Neurons for MDM.

Identify a Certificate preference item in the user's keychain that references a Certificate payload included in the same profile.

This configuration is used to bind a certificate to either an email address or a URL. After you bind a certificate to an email address, the Mail app will use it for that email account. If an SSL Certificate for a website is not trusted, adding a Certificate preference will ensure that the browser does not prompt you with a warning message when you try to access the website.

> The administrators must have a Certificate. For more information on adding and distributing a certificate, see **Certificate configuration**.

Creating an Certificate Preference configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **preference** in the search field, and then click the **Certificate Preference** configuration.
4. Name and describe the configuration.
5. In the Configuration Setup section, in the **Name** field, enter an email ID or a name for which a preferred certificate is requested.
6. In the **Certificate UUID** field, select a certificate.
7. Click **Next** to configure the distribution settings.
8. Click **Done**.

Related topics:

- **Identity Preference**
- **Certificate configuration**
- **How to create a configuration**

10.10.4.45. Active Directory (macOS)

Applicable to: macOS 10.9 or supported newer versions.

Configure advanced options to bind macOS devices to an Active Directory (AD) domain in order to access software services that rely on AD for authentication and security.

This section contains the following topics:

- Creating an Active Directory configuration
- Active Directory settings

Creating an Active Directory configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **privacy** in the search field, and then click the **Active Directory** configuration.
4. Name and describe the configuration.
5. Enter the settings as described in the following Active Directory settings table.
6. Click **Next** to configure the distribution settings.
7. Click **Done**.

Active Directory settings

Setting	What To Do
Active Directory Settings - Basic	
Hostname	(Required) Enter the host name, which is the Active Directory domain to join.
Username	Enter the user name of the account used to join the domain.
Password	Enter the password of the account used to join the domain.
AD Organisational Unit	Enter the organisational unit (OU) where the joining computer object is added.
AD Mount Style	Select one of the following options to indicate the network home protocol to use: • AFP • SMB
Active Directory Settings - Advanced	
Enable ADCreateMobileAccountAtLogin key	Enable or disable the ADCreateMobileAccountAtLogin key. Additional option: Create mobile account at login.
Enable ADWarnUserBeforeCreatingMA key	Enable or disable the ADWarnUserBeforeCreatingMA key. Additional option: Warn user before creating mobile account.
Enable ADForceHomeLocal key	Enable or disable the ADForceHomeLocal key. Additional option: Force local home directory.
Enable ADUseWindowsUNCPath key	Enable or disable the ADUseWindowsUNCPath key. Additional option: Use UNC path from AD to derive network home location.
Enable ADAllowMultiDomainAuth key	Enable or disable the ADAllowMultiDomainAuth key. Additional option: Allow authentication from any domain in the forest.
Default user shell	Enter the default user shell such as /bin/bash.
Map user UID to attribute	Select to map the user UID to the specified attribute.
Map user GID to attribute	Select to map the user GID to the specified attribute.
Map group GID to attribute	Select to map the group GID to the specified attribute.
Preferred Domain Server	Prefer this domain server.
Namespace convention	Select one of the following user account naming conventions: • Domain (default) • Forest
Packet Signing	Select one of the following packet signing options: • Allow (default) • Disable • Require

Setting	What To Do
Packet Encryption	Select one of the following packet encryption options: • Allow (default) • Disable • Require • SSL
Allow administration by specified Active Directory groups	Select to allow administration by specified Active Directory groups. Click **Add** to add one or more groups.
Restrict Dynamic DNS	Select to restrict dynamic DNS updates to the specified interfaces (for example, en0, en1, etc). Click **Add** to add one or more interface names.
Change Password Interval	Specify how often (in days) a change of the computer trust account password is required. The zero value is disabled.

For more information, see **How to create a configuration**

10.10.4.46. Identity Preference

Applicable to: macOS 10.12 or supported newer versions.

Identify an Identity Preference item in the user's keychain that references an identity payload included in the same profile.

On a macOS device, an Identity Preference allows you to choose the identity (key-value pair) you want to use with a website. Once you have pushed an Identity Preference (which consists of the URL and identity) to the device, it is listed in **Keychain access > All Items** (the "Kind" will be "Identity Preference"). The next time you try to connect to that URL from Safari, the device will present the configured certificate.

Ivanti Neurons for MDM creates a default system Identity Preference configuration with a payload for the AppStore URL and the certificate to use.

While accessing the macOS App Catalog using Safari on macOS 10.12 and later versions, the user will get a system password prompt to cache the identity certificate. Users need to select 'Always allow' for the first time to avoid subsequent prompts while accessing the macOS App Catalog.

Safari with macOS version less than 10.12 and other browsers will show certificate and system password prompts while accessing the macOS App Catalog on a new browser session from macOS devices.

Creating an Identity Preference configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **preference** in the search field, and then click the **Identity Preference** configuration.
4. Name and describe the configuration.
5. In the Configuration Setup section, in the **Name** field, enter an email ID, a DNS host name, or a name that uniquely identifies the service.
6. In the **Certificate UUID** field, select a certificate.
7. Click **Next** to configure the distribution settings.
8. Click **Done**.

Related topics:

- Certificate Preference
- How to create a configuration

10.10.4.47. Office 365 Auto Account Creation (macOS)

Applicable to:

- Supported macOS devices.
- Recommended Microsoft Office 365 apps versions to be 16.13.x or later.

Configure user information and options to setup initial configuration for all Microsoft Office 365 applications.

This section contains the following topics:

- Creating an Office 365 Auto Account Creation configuration
- Office 365 Auto Account Creation settings

Creating an Office 365 Auto Account Creation configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **office** in the search field, and then click the **Office 365 Auto Account Creation** configuration.
4. Name and describe the configuration.
5. Enter the settings as described in the following Office 365 Auto Account Creation settings table.
6. Click **Next** to configure the distribution settings.
7. Click **Done**.

Office 365 Auto Account Creation settings

Setting	What To Do
Office Activation Email Address	Enter the user email address.
Office Auto SignIn	Select to suppress first-run windows. Only prompts user for required information such as O365 authentication.
Default to local Open/Save	Select to force the open/save panel to 'On My Mac' instead of 'Online Locations'.
Show what's new on Launch	Select to display new feature information at the launch.
Visual Basic Macro Execution state	Select one of the following options: • Disabled with warnings • Disabled without warnings • Enabled without warnings
Disable Visual Basic External Dylibs	Select to disable Visual Basic external dependencies.
Allow Visual Basic To Bind System	Select to allow the macros to use a DECLARE to bind to the system() OS API. This API allows the macros to execute arbitrary external processes and pass them arbitrary data on the command line.
Disable Visual Basic To Bind To Popen	Select to allow the macros to use a DECLARE to bind to the popen() OS API. This API allows the macros to execute arbitrary external processes and pass them arbitrary data on the command line.
Disable Visual Basic Mac Script	Select to allow the macros to invoke the Apple Script Visual Basic API.

For more information, see **How to create a configuration**

10.10.4.48. Authenticate

Applicable to:

- macOS 10.13 and supported newer version.
- Windows 10 and supported newer version.

Use the Authenticate configuration to provide password-less authentication for cloud services and/or desktop logins. Each device will have only one Authenticate configuration.

Prerequisites

- Zero Sign-On licence is required.
- Ivanti Neurons for MDM should be registered with Access (Access profile should be configured).
- After configuring the Authenticate configuration, you cannot de-register Access profile as the Access profile will be referenced by the Authenticate configuration.
- If the Access profile has any changes, re-distribute the Authenticate configuration to the macOS devices. For Windows devices, copy and use the new CLI values in the new apps.

Creating an Authenticate configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **auth** in the search field, and then click the **Authenticate** configuration.
4. Name and describe the configuration.
5. Select a **Desktop Identity Certificate** from the drop-down list.
6. Select one or both of the following OS option(s):
    - macOS
    - Windows
7. For macOS:
    1. In the Custom Data region, click **+ Add** to add keys and string values for custom data to be pushed to the devices.
    2. Click **Next** to configure the distribution settings.
    3. Click **Done**.
8. For Windows 10 devices, this configuration helps in generating Command-Line arguments for the Authenticator MSI app for Windows as follows:
    1. Click **Done** to complete the Authenticate configuration.
    2. From the **Configurations** page, view the Authenticate configuration to copy the displayed command line text. This text is required when distributing the Authenticate app for Windows devices.

> When the Authenticate configuration is applied to Windows devices, the configuration stays in Pending Install state. You can ignore this as there will be no impact on the functionality.

For more information, see **How to create a configuration**

10.10.4.49. Apple App Catalogue

Applicable to: iOS and macOS

The Apple App Catalogue configuration manages access to the Apple App Catalogue via a web clip. Starting from Ivanti Neurons for MDM release 83, you can transition to Apps@Work native experience from Go application. For newly created tenants the Apps@work Webclip configuration is not distributed by default for iOS devices that are installed through iReg or client. The administrator has to manually distribute the webclip config to the devices that are registered through iReg or client.

> The Apps@Work webclip search result displays only 10 applications on iOS and iPad devices even if the search request has rows parameter as more than 10.

Procedure

Admins can edit the distribution of this system-defined configuration as follows:

1. Go to **Configurations**.
2. Click **Apple App Catalog**.
3. Click **Edit Distribution**.
4. Select one of the following distribution options:
    - All Devices - all compatible devices will have this configuration sent to them.
    - No Devices - disable access to Apple App Catalogue or stage this configuration for later distribution.
    - Custom - define specific device groups that will have this configuration sent to them.

Click **Save**.

10.10.4.50. Managed Domains

Licence: Silver

A managed domain configuration enables you to specify which domains are trusted for Mail and Safari on iOS 8+ and visionOS 1.1+ devices. Once the configuration is applied to the device, domains that are not specified in the configuration will be highlighted (untrusted) in Mail and Safari on the device. Use this configuration combined with a **restrictions configuration** to control the data downloads allowed in Safari.

Managed domains settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Managed Email Domains	Click **+Add** to enter a domain, as in mycompany.com.
Managed Web Domains	Click **+Add** to enter a domain, as in mycompany.com.

For more information, see **How to create a configuration**

10.10.4.51. Passcode Configuration

One of the first things you set up in Ivanti Neurons for MDM (using the startup wizard) is a passcode configuration. This configuration defines settings for the screen lock feature on devices.

Passcode settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Allow simple values	Restricts whether the PIN or Password contains ordered characters or digits. **For iOS, macOS, watchOS, and Android:** Select to allow pin or passcodes that are less secure because they contain repeated, ascending, or descending character sequences. Examples: 1111, 1234, abcd. Note: Deselecting this option for Android devices will enforce passcodes with complex PINs. For example, users cannot configure repeated, ascending, or descending character sequences. **For Windows 10+**: Select to allow passcodes that are less secure because they contain repeated or ascending numeric sequences. Examples: 1111, 1234
Require alphanumeric value	Requires the passcode to contain at least one letter and one number. **For iOS and Android**: Select to ensure that passcodes include letters and numbers. **For Windows 10+**: Select to ensure a strong password based on Microsoft's standard.
Minimum passcode length Minimum number of complex characters	Select a number from the list to set a minimum passcode length. **For Windows 10 Desktop**: Local accounts will enforce minimum passcode length 6. **For iOS and Android**: Select a number from the list to set a minimum number of characters that are not numbers or letters. **For Windows 10+**: Local accounts will enforce 3 complex characters.
Maximum passcode age	Enter a number to the number of days after which the device user must reset the passcode. If you do not want to set the a passcode age, then leave this field blank.
Auto-Lock	Select an interval from the list to define how long the device can stay idle before it automatically sets the screen lock.
Any Lock Method	**Android only**. Allows user choice of any lock method, including pattern unlock. The passcode settings above will not be applied to this device.
Passcode history	Enter a number to set the number of unique passcodes a user must enter before reusing a passcode. For example, if you set this field to 4, then the user must set 4 passcodes before being able to reuse the first passcode.
Grace period for device lock	Select an interval from the list to set the amount of time between the appearance of the lock screen and the point at which the device user needs to enter a passcode to unlock the device.
Maximum number of failed attempts	Select a number from the list to set the number of times the device user can consecutively enter the wrong passcode before the device is reset and wiped. **Warning:** Devices will be wiped if the user exceeds the maximum number of password attempts. Use caution with this option.

Setting	What To Do
(macOS Only) Enable Passcode Regular Expression (macOS 14+)	Specify the expression string that matches with the password to determine whether it matches with the policy.
(macOS Only) Language	Specify the language of the Description.
(macOS Only) Description	Describe the password complexity. For example, numbers, special characters, string, and so on.
(macOS Only) Enforce passcode rule at next login	Select to enable macOS to prompt the user to change the password to make the password compliant with the password policy next time the user logs in. By default, this option is not selected. Applicable for macOS 10.13 and later versions.
(macOS Only) Minutes until failed login reset	Specify the minutes before the login is reset after the maximum number of unsuccessful login attempts is reached. Ensure that the Maximum number of failed attempts number is set to enable this field. Available in macOS 10.10 and later.
SmartLock	**For Android 5.0 devices except in Android enterprise work profiles:** **For Android 6.0 or later:** Allows or disallows a user to choose the SmartLock feature to unlock a device. The SmartLock feature automatically unlocks a device in certain circumstances such as the user's proximity to the device, device at a location, or when the device is paired with a trusted device.
Fingerprint Unlock	**For Android 5.0 devices except in Android enterprise work profiles:** **For Android 6.0 or later:** Allows or disallows the user to choose Fingerprint to unlock a device.
Lock Screen Notifications (for Android Enterprise only)	**Enable Notifications for Work Managed Devices (for Device Owner)** Allow or disallow notifications on the lock screen for work managed devices **Enable Unredacted Notifications for Work Profile** **For Android 6.0 or later:** Allow or disallow unredacted notifications on the lock screen for work profile devices. After you enable this setting, you will receive the notification but the content appears as 'Content hidden by policy'. You can view the content (mail/ push notification) only from the app.

For more information, see **How to create a configuration**

10.10.4.52. Privacy Preference (macOS)

Applicable to: macOS 10.14 or supported newer versions.

Configure which applications are allowed to gain access to system services, system files and system resources. This configuration controls the settings on a macOS device under System Preferences > Security & Privacy > Privacy.

Creating a Privacy Preference configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **privacy** in the search field, and then click the **Privacy Preference** configuration.
4. Name and describe the configuration.
5. Navigate to one of the applications listed on the page. See **Apple documentation** for related information.
    1. For macOS 10.14+, the applications and settings available for configuration include:
        - Accessibility - Specifies the policies for the app via the Accessibility subsystem.
        - Address Book - Specifies the policies for contact information managed by the Contacts.app.
        - Apple Events - Specifies the policies for the app sending restricted AppleEvents to another process.
        - Calendar - Specifies the policies for calendar information managed by the Calendar.app.
        - Camera - A system camera. Access to the camera cannot be given in a profile; it can only be denied.
        - Microphone - A system microphone. Access to the microphone cannot be given in a profile; it can only be denied.
        - Photos - The pictures managed by the Photos app in ~/Pictures/.photoslibrary.
        - Post Event - Specifies the policies for the application to use CoreGraphics APIs to send CGEvents to the system event stream.
        - Reminders - Specifies the policies for reminders information managed by the Reminders app.
        - System Policy (All Files) - Allows the application access to all protected files, including system administration files.
        - System Policy (Admin Files) - Allows the application access to some files used in system administration.
    2. For macOS 10.15+, the applications and settings available for configuration include:
        - File usage - Allows a File Provider application to know when the user is using files managed by the File Provider.
        - Listen Event from all processes - Allows the application to use CoreGraphics and HID APIs to listen to (receive) CGEvents and HID events from all processes. Access to these events cannot be given in a profile; it can only be denied. Uncheck the Allowed option.
        - Access Media Library - Allows the application to access Apple Music, music and video activity, and the media library.
        - Screen Capture of the system display - Allows the application to capture (read) the contents of the system display. Access to the contents cannot be given in a profile; it can only be denied. Uncheck the Allowed option.
        - Recognise and send speech data to Apple - Allows the application to use the system Speech Recognition facility and to send speech data to Apple.
        - Access files in the user's Desktop folder - Allows the application to access files in the user's Desktop folder.
        - Access files in the user's Documents folder - Allows the application to access files in the user's Documents folder.

- Access files in the user's Downloads folder - Allows the application to access files in the user's Downloads folder.
- Access files on network volumes - Allows the application to access files on network volumes.
- Access files on removable volumes - Allows the application to access files on removable volumes.

6. For each application you want to configure, click **Actions > Add**.
7. Enter the values for the following identity dictionary keys:
   - Identifier - Name of the settings. For example: "us.zoom.ZoomPresence."
   - Identifier Type - Select either Bundle ID or Path. For example: "Bundle ID."
   - Code Requirement - Specify the value for Bundle ID or Path. For example: "identifier "us.zoom.ZoomPresence" and anchor apple generic."
   - Static Code (True or False)
   - Allowed (True or False)
   - Comment
8. Click **Save**.
9. (Optional) Under any application, click **Actions > Delete** to remove any existing privacy preference settings.
10. Click **Next** to configure the distribution settings.
11. Click **Done**.

For more information, see **How to create a configuration**

10.10.4.53. Privacy Configuration

A privacy configuration defines whether:

- location data is collected on the device and sent to the device management system
- administrators are allowed to wipe the device
- app inventory is collected for all apps or just those that appear in the app catalogue

Privacy settings

> Device Wipe action and collecting Inventory for all apps on device is not applicable for User Enrolled devices.

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Collect Location Data	Select to enable collection of location data. View device location in the **Devices** page. • For iOS devices, the location displayed for a device is based on the network location only. • F or Android devices, the location is based on both network location and GPS location (if available). • For Windows devices, the location is based on the latitude and longitude values obtained during a device checkin. When location collection is enabled on a device, the current location is updated every 4 hours. Location data is removed from the device management system when the device is retired or the privacy configuration is disabled or removed. Device users can **turn off collection of location data on the device**.
Disable Device Wipe Action	Select to prevent administrators from wiping the device. Consider selecting this option for devices that are owned by the user (employee owned).
Prompt user to enable location services	Select to allow the users to optionally enable the ability to allow or disallow the use of location services including locating the devices, Wi-Fi and MTD, as needed. In the case of fully managed devices, this can be auto granted if the administrator chooses to disable the option.
Collect App Inventory	Select **Collect App Inventory** to collect information on all apps installed on the device, regardless of whether an app is present in the app catalog. Select **For Apps on the Device that are in the App Catalog** to collect information on only those apps installed on the device and present in the app catalog. Select **For All Apps on the Device** to collect information on all apps on the device. This option is applicable to Windows 10+ devices. The following app source type inventories are displayed and selected by default. • **Enable Non App Store Inventory** - for In house apps(Universal apps) pushed through MDM or installed by end-user directly on device by manually unpacking the app and installing it locally. • **Enable App Store Inventory** - for the apps installed from Microsoft Store manually or via Apps@work store-front. • **Enable System Inventory** - for the apps reported as pre-installed along with Windows 10 OS by Microsoft. • **Enable Win32 inventory** - for the system 32 based apps like apps like MSI, EXE, Win32 Store apps, and so on that are installed by pushing through MDM or installed directly on device by the end-user. You can optionally select only those app source type inventories to collect information on selective apps. MDM-installed apps appear in the App Inventory, even if you don't select Non App Store or Win32 app inventory. The.EXEs inventory is also collected when the Privacy configuration is using the default configuration to collect App Inventory only for AppCatalog. The inventory must be

Setting	What To Do
	collected consistently for all apps when collecting only for the AppCatalog apps. The inventory for Modern, MSI, and EXE apps available in the App Catalog; will be pulled only when at least one app belonging to each of these variants is distributed.
Settings for Android Enterprise devices (7.0+) Configure the settings given below to set the privacy policy to Android Enterprise devices.	
Organisation name	Enter the name of the organisation managing the device.
Organisation colour	Select the organisation colour that should be displayed in the background of the user's screen.
Short message **Long message** **Keep Go app screens hidden**	Enter a short message that should be displayed when the user attempts to use a function that is locked down by the administrator. Enter the long message that should be displayed when the user clicks on the short message. This message provides more details on the restriction given to the user. Select True or False from the list. • **True** - During remote share, Ivanti Go app screens will not be visible. • **False** - During remote share, Ivanti Go app screens will be visible for any assistance with troubleshooting and also to view the documentation.

For more information, see **How to create a configuration**

10.10.4.54. Client Privacy Statement Information

Applicable to: Android, Android Enterprise, and iOS devices or supported newer versions.

Configuration to distribute the Privacy Statement information to the usersin Go clients. This is a system-defined configuration that can be edited to configure only the distribution settings.

The information displayed to the user includes the details configured as part of the following configurations:

- Privacy
  - Collecting location data
  - Collecting app inventory
  - Android 7.0+:
    - Organisation name
    - Organisation colour
    - Short message
    - Long message
- Client Privacy
  - SLC - Significant Location Change to periodically wakeup the device
  - Minimum Location based Wakeups Interval
  - Enable MixPanel status
- Mobile Device Management - MDM Access Rights (Not applicable to User Enrolled devices)
  - Device Lock and passcode removal
  - Device erase
  - Network Information (phone/SIM numbers, MAC Addresses)

10.10.4.55. Ivanti Go Client Settings

Configure the collection of anonymous end-user data, including device and usage information, to help identify product issues and ensure high service quality. This setting also enables support contact configuration options.

Creating a Ivanti Go Client Settings configuration

Applicable to:

- Mobile@Work for macOS 1.67 or supported newer versions.
- Go for iOS 3.5.0 or supported newer versions.
- Mobile@Work for Android 12.9.0.0 or supported newer versions.
- Go for Android 122 or supported newer versions.

Procedure

1. Go to **Configurations** > **Add Configuration** > **Ivanti Go Client Settings**. The **Create Ivanti Go Client Settings Configuration** page appears.
2. Enter a name for the configuration in the **Name** box.
3. Enter a **Description** of the configuration.
4. Under **Location based Wakeups**, select the **Enable SLC** option. The significant-change location service offers a more power-friendly alternative to deliver location updates to the MobileIron Go for iOS app only when the user's position changes by a significant amount, after a minimum of 15 minutes (default interval). If this service is enabled, then on location change the Go app wakes up in the background and checks in.
5. Under **Data Collection via Analytics for Clients**, select the **Enable Analytics** option if it has been disabled. By default, this option is enabled.
6. Click **Next** to configure the distribution settings.
7. Click **Done**.

Configure Setup for Support Tab

Applicable to:

- Mobile@Work for macOS 1.67 or supported newer versions.
- Go for iOS 3.5.0 or supported newer versions.
- Mobile@Work for Android 12.9.0.0 or supported newer versions.
- Go for Android 122 or supported newer versions.

Procedure

1. Go to **Configurations** > **Add Configuration** > **Ivanti Go Client Settings**. The **Create Ivanti Go Client Settings Configuration** page appears.
2. Enter a name for the configuration in the **Name** box.
3. Enter a **Description** of the configuration.
4. Under **Platform** option, select the respective platform.
5. In the **Configure Setup for Support Tab** section, click **Enable Support Tab**.

> **Enable Support Tab** field is only applicable for iOS devices.

> You can enable the **Support Tab** from Go for iOS version is 118.0.0 or above and Go for Android version is 124 or above. Devices with earlier versions will not display or support this feature.

In the **Support Contact Configuration** section, provide the following details:

- **Tab Name** - Enter the name of the tab displayed in the Ivanti app navigation. The default value is 'Support'. (Maximum length: 10 characters)
- **End User Instructions** - Enter the instructions on how to use the support contacts. (Maximum length: 40 characters)
- **Add Contacts** - Click **+Add** to add the contacts. (Maximum contacts: 5)
  - **Name** - Enter the contact name. (Maximum length: 20 characters)
  - **Enter Phone Number** - Enter a valid phone number. (With country calling code)
- **Add URL** - Click **+Add** to add the URLs. (Maximum URLs: 5)
  - **URL Name** - Enter the URL name. (Maximum length: 20 characters)
  - **Enter URL** - Enter a valid URL.
- **Additional Information** - Enter any additional support-related messages you want to display here. (Maximum length: 120 characters)
- **Email Address** - Enter the email where you can send emails for support. (Maximum length: 40 characters)

  > You must enter a valid email address in the format alias@domainname.com

- Support Ticketing System URL - Add a “Raise a Support Ticket” button to the Support tab in the Ivanti Go for iOS app. Enable the toggle to display the button on the Support tab, and enter the appropriate URL in the provided field to redirect users to your support system.

  > This URL is used in the Ivanti Go **Support Tab** to redirect users to the designated support system. For improved security, it is recommended to use URLs beginning with *https://* rather than *http://*.

Click **Next** to configure the distribution settings.

8. Click **Done**.

For more information, see **Configurations**.

10.10.4.56. Siri Settings

Use the **Siri Settings** to configure Siri settings on supervised devices. This configuration helps administrators apply consistent, policy-based controls that manage how devices access and use Siri features.

Applicable to:

- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- macOS 15.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Siri Settings** configuration.
3. Configure the **Safari Settings** settings as per the following table:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Enabled	Select the checkbox to enable Siri. Toggle the **Push to Device** button to enable Siri on supervised devices.
Allow Siri	Select the checkbox to enable the **Siri AI** specific features. Toggle the **Push to Device** button to enable the **Siri AI** specific features on supervised devices.
Allow User Generated Content	Select the checkbox to enable User Generated Content. Toggle the **Push to Device** button to enable User Generated Content on supervised devices. This setting is not applicable for macOS and visionOS devices.
Allow While Locked	Select the checkbox to enable While Locked. Toggle the **Push to Device** button to enable While Locked on supervised devices. This setting is not applicable for macOS and visionOS devices.
Force Profanity Filter	Select the checkbox to enable Force Profanity Filter. Toggle the **Push to Device** button to enable Force Profanity Filter on supervised devices. This setting is not applicable for visionOS devices.
Force reduce sensitive content	Select the checkbox to force Siri to reduce sensitive content. Toggle the **Push to Device** button to force Siri to reduce sensitive content on supervised devices.

4. Click **Next** to configure the distribution settings.

5. Select one of the distribution options to set up the **Safari Settings** configuration. For more information about configuring distribution options, see **Working with Configurations**.
6. Click **Done**.

10.10.4.57. Services Configuration Files Configuration

The **Service Configuration Files** configuration administrators to centrally manage and deploy configuration files for various system services on enrolled devices. Additionally, administrators can ensure that service settings remain consistent and resistant to unauthorised modification by delivering files to secure, service-specific directories in a tamper-resistant environment.

Applicable to: macOS devices

Before you begin:

- You can upload various configurations in a *ZIP* file format. For more information about adding a file, see **Files**.
- All files in the expanded archive are set to *-r–r–r– unix* file permissions. Any links in the archive will be restricted to referencing files within the service-specific location.
- The files in the zip archive need to mirror the folder structure and configuration files that the service expects to be present starting at the root of the file system. The service uses only the files the declaration provides and ignores the ones in its default directories.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Service Configuration Files** configuration.
3. Configure the **Service Configuration Files** settings as per the following table:

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Select file	Enter the file name.
Choose Service Type	Select one of the **Service Types** from the dropdown list: • SSHD • SUDO • PAM • CUPS • HTTP_D • BASH • ZSH

4. Click **Next** to configure the distribution settings.
5. Select one of the distribution options to set up the **Service Configuration Files** configuration. For more information about configuring distribution options, see **Working with Configurations**.
6. Click **Done**.

10.10.4.58. Software Updates

Applicable to:

- iOS 10.3 till 26.0 and tvOS 12.0 till 26.0 supervised devices
- macOS devices
- Windows 10+ devices

Create and distribute rules for OS updates.

This section contains the following topics:

- Configuring software updates for iOS/tvOS devices
- Configuring software updates for Non-DEP and DEP macOS devices
- Configuring software updates for Windows devices
- Software Updates Enforcement using Declarative Device Management

Configuring software updates for iOS/tvOS devices

Procedure

To allow iOS/tvOS devices to have OS updates sent to them if they are in supervised mode:

1. Go to **Configurations**.
2. Click **+ Add**.
3. Click **Software Updates**.
4. Click **iOS/tvOS** to view the Configuration Setup section.
5. Select the **Allow OS updates to be automatically installed on supervised devices** option.
6. Select one of the following options:
    - Update to latest version
    - Update to specific version - For example, enter iOS version number as 11.3.0.
7. Select one of the following installation actions:
    - Default
    - Download Only
    - Install ASAP
8. Select the following time options for the updates to happen:
    - Start Time
    - End Time
    - Timezone
9. Click **Next**.
10. Select the **Enable this configuration** option.
11. Select one of the following distribution options:
    - All Devices

    - No Devices (default)
    - Custom
12. Click **Done**.

- When installing a specific version of OS update for iOS devices, you must select a version that is available for the device. If you select an invalid or an unavailable version, software update of the device will be ignored.
- If the device has a passcode, after MDM sends the update to the device, the device queues the update and the user is prompted to enter their passcode in order to start the installation.
- Enable `enforcedSoftwareUpdateDelay` in **iOS Restrictions** to make sure the manual scan on devices for software updates will not delete the specific versions downloaded by this configuration.

Configuring software updates for Non-DEP and DEP macOS devices

Device Enrollment profile is part of Apple Business Manager that enables customers to purchase devices in bulk and automatically enroll the devices in MDM during activation. For more information, see **Device Enrollment**.

The following procedure helps you send OS updates to Non-DEP and DEP macOS devices.

Procedure

1. Go to **Configurations**.
2. Click **+ Add**.
3. Click **Software Updates**.
4. Click **macOS** to view the Configuration Setup section.
5. Select the **Enable macOS Software Updates** option.
6. Select the type of updates for the device. For each of these updates, you can also select updates that do not require restart.
    - OS Updates
    - Critical Updates
    - Configuration Data Updates
    - Firmware Update
    - Non Critical Updates

    > Admin can manage (install/schedule) non critical macOS updates by enabling **Enable Non Critical Updates**. This option is disabled by default for the existing tenants and needs to be enabled by admin explicitly post upgrade if required.

    > In **OS updates**, Administrators can update the device to a specific version of macOS.

    > All macOS updates can be configured with actions as follows:

        - Default
        - Notify Only
        - Install Later
        - Install Force Restart

- Download Only
- Install ASAP

Priority

Default - Low

Possible values - Low, High

- Max User Deferrals
  Possible value - Integer
  Only supported when Install Later option is selected.

7. Select the following time options for the updates to happen:
   - Start Time
   - End Time
   - Timezone
8. Click **Next**.
9. Select the **Enable this configuration** option.
10. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
11. Click **Done**.

Configuring software updates for Windows devices

Procedure

To configure your Windows installation update schedule:

1. Go to **Configurations**.
2. Click **+ Add**.
3. Click **Software Updates**.
4. Click **Windows** to view the Configuration Setup section.
5. Enter the following options depending on the version of your Windows devices.
6. Click **Next**.
7. Select the **Enable this configuration** option.
8. Select one of the following distribution options:
   - All Devices
   - No Devices (default)
   - Custom

Click **Done**.

Software updates for Windows 10+ devices

- Update Sources - Select one of the following sources:
  - Enterprise WSUS
  - Microsoft Update and/or Enterprise WSUS

Driver Update Source

- Feature Update Source
- Other Update Source
- Quality Update Source
- URL to Enterprise WSUS Server
- Alternate intranet Microsoft update server
- Allow Updates from 'Trusted Publishers' - Limit sources for updates to trusted publishers only.
- Auto Update Strategy - Select one of the options from the pull-down menu.
- Scheduled Installation Day - Set the frequency of updates.
- Scheduled Installation Time - Select an installation time for updates.
- Allow updates to be downloaded automatically over metered connections - Enable or disable the option.
- Do not allow update deferral policies to cause scans against Windows Update - Enable or disable the option.
- Engaged restart deadline - Select the number of days to restart deadline.
- Snooze engaged restart deadline - Select the number of days to snooze the engaged restart deadline.
- Engaged restart transition schedule - Select the number of days to restart transition schedule.
- Update/Fill empty content URLs.
- MO App download limit - Select one of the following options:
  - Do not ignore MO download limit for apps and their updates
  - Ignore MO download limit (allow unlimited downloading) for apps and their updates
- MO update download limit - Select one of the following options:
  - Do not ignore MO download limit for OS updates
  - Ignore MO download limit (allow unlimited downloading) for OS updates
- Manage preview builds - Select one of the following options:
  - Disable Preview builds
  - Disable Preview builds once the next release is public
  - Enable Preview builds
- Auto-restart warning notification schedule for updates - Select the minutes to be taken to auto-restart warning notification.
- Restart warning reminder - Select the hours to set the restart warning reminder.
- Automatic update schedule - Select the frequency of automatic updates.
- Auto-restart notification for updates - Turn on the auto-restart notification for updates.
- Product version - Enter the product version as listed on the Windows Update version page (URL: aka.ms/WindowsTargetVersioninfo). For example, "Windows 11" or "11" or "Windows 10".
- Target release version - Enter the target release version on the Windows Update version page.

- Active Hours Start – If you enable this option, a PC will not restart automatically after updates during active hours. Outside of active hours, the PC will attempt to restart.
- Active Hours End – If you enable this option, the PC will not restart automatically after updates during active hours. Outside of active hours, a PC will attempt to restart.
- Active Hours Max Range – Enable this option to indicate the maximum number of hours from the start time that users can set their active hours.
- No Update Notifications During Active Hours – The update notification options are below.
  - Default Windows Update notifications
  - Turn off all notifications, excluding restart warnings
  - Turn off all notifications, including restart warnings
- Disable Updates for Drivers – Enable this option to exclude drivers with Windows quality updates. If you disable or do not configure this option, Windows Update will include updates with a driver classification.
- Quality Updates Deadline – The number of days before quality updates are automatically installed on devices is independent of active hours.
- Quality Updates Deadline Grace Period – The minimum number of days from update installation until automatic restarts for quality updates.
- Feature Updates Deadline Grace Period – The number of days until feature updates are automatically deployed on devices, independent of active hours.
- Feature Updates Deadline Grade Period – The minimum number of days until feature updates are automatically deployed on devices, independent of active hours.
- Don't auto-restart until end of grace period – When enabled, devices will not automatically restart outside of active hours until the deadline and grace period have passed, even if an update is ready to restart. When disabled, an automatic restart may be attempted outside of active hours if the update is available for restart prior to the deadline.

Software updates for pre-Windows 10.0.14393 devices

The following settings will not work if Telemetry Restriction is disabled on a device:

- Pause Upgrade/Updates - Turn on to delay changes to a later date
- Defer Updates for - Choose to delay up to 4 weeks
- Defer Upgrades - Turn on to defer upgrades
- Defer Upgrades for - Choose to delay up to 8 months

Software updates for Windows 10.0.14393+ devices

- Branch to install updates from - Allows the IT admin to set which branch a device receives their updates from. Branch to install updates from field contains the following options:
  - Windows Insider build – Fast
  - Windows Insider build – Slow
  - Release Windows Insider build
  - Semi-annual Channel (Targeted)
  - Semi-annual Channel
  - Release Preview of Quality Updates Only

- Canary Channel

Feature Updates (upgrades) - Supported only in Windows Professional, Windows Enterprise, and Windows Education.

- Pause updates
- Defer for - Choose to delay up to 180 days.

Quality Updates (updates) - Supported only in Windows Professional, Windows Enterprise, and Windows Education.

- Pause updates
- Defer for - Choose to delay up to 30 days.

Software updates for Windows 10.0.17083+ devices

- Feature Updates:
  - Feature update uninstall period - Select the number of days to be taken to uninstall a feature update.

Software updates for Windows 10.0.17763+ devices

- Disable "Pause Updates" access by users
- Disable UXWU Access by users (Windows Update Scan, download and install)
- Update notification level - Select one of the following options:
  - Use the default Windows Update notifications
  - Turn off all notifications, excluding restart warnings
  - Turn off all notifications, including restart warnings
- Feature updates:
  - Deadline before auto-restart for update installation - Select the number of days for the deadline before auto-restart for update installation.
  - Engaged restart deadline - Select the number of days for the engaged restart deadline.
  - Snooze engaged restart deadline - Select the number of days to snooze the engaged restart deadline.
  - Engaged restart transition schedule - Select the number of days to restart transition schedule.

Software Updates Enforcement using DDM

The administrator can enforce Software Updates installation on iOS, macOS, and iPadOS devices using DDM.

Supported on:

- iOS 17+
- iPadOS 17+
- macOS 14+

Procedure

1. Create a **Software Update Enforcement** configuration from the Configurations section.
2. Perform a Force Check-in to ensure the Software Update Enforcement configuration is installed on the device.

When you open the device, you should see a notification about the required software updates with details like the version number, required by date, etc.

> If you do not want to enforce the software update, you need to set the configuration distribution option to **None**.

Distributing predicates for a Software Update Enforcement configuration

1. Create a Software Update Enforcement configuration.
2. Set the toggle switch “Activation with Predicates” to ON, and use + button to include the predicates (as needed).



To edit or delete a predicate, go to **Admin** > **Apple** > **Predicates**. You can find the list of predicates available in this page. Click **Edit** to make any changes to the existing predicate and save it. Similarly, to delete an existing predicate, select the predicate and click **Delete**.

> You cannot delete a predicate if it is associated with any configuration.

10.10.4.59. Software Update Settings Configuration

Ivanti Neurons for MDM enables the creation of Software Update Enforcement Settings and defines the behavior of updates to the end user for cadence and deferrals.

Applicable to:

- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- macOS 15.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Software Update Settings** configuration.
3. Configure the **Software Update Settings** settings as per the following table:

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
iOS 18+ Supervised and **macOS15+** Beta Enrollment Program Enrollment (Optional)	Select one of the following options: • **Allowed**: The user can enroll in any applicable beta programs associated with their logged in Apple Account. • **Always On**: The beta programs specified by the organisation are used, and the user is not able to enroll in a beta program using their logged in Apple Account. **Offer Program** - With Offer Program, you can enforce a required program. When enforcing, you can set the required versions for iOS and macOS devices. **Require Program** - The device automatically enrolls in this beta program. • **Always Off**: The device is not allowed to enroll in any beta programs. The system removes the device from any beta programs, if already enrolled.
iOS 18+ Supervised and **macOS15+ Supervised** Notifications Automatic Actions Download Install OS Updates	Select the **Notifications** checkbox and the **Show all software update enforcement notifications** checkbox to display all the software update enforcement notifications in the user's device. If you select the **Notifications** checkbox only, the device will display a single enforcement notification one hour before the enforcement deadline. If you do not select either of the check boxes, the device displays the notifications triggered to display all the software update enforcement notifications in the user's device. Select one of the following options: • **Allowed**: The user can turn “On” or “Off” for automatic downloads. • **Always On**: The automatic downloads are always “On” for the user. • **Always Off**: The automatic downloads are always “Off” for the user. Select one of the following options: • **Allowed**: The user can turn “On” or “Off” to automatically install OS updates. • **Always On**: The automatic installation of OS updates is always “On” for the user. • **Always Off**: The automatic installation of OS updates is always “Off” for the user.
Background Security Improvements	
Background Security Improvements	Select the **Background Security Improvements** checkbox to control the installation and rollback of updates. Select the following options:

Setting	Description
	• **Enable**: If selected, it offers **Background Security Improvements** installation to the user. • **Enable Rollback**: If selected, it offers **Background Security Improvements** rollback to the user.
iOS 18+ Supervised	
Recommended Cadence	Select one of the following options to show the software updates to the user when more than one update is available: • **All**: Shows all software update versions. • **Oldest**: Shows only the oldest (lower numbered) software update version. • **Newest**: Shows only the newest (highest-numbered) software update version.
Deferrals	You can choose to postpone the software updates for all supervised devices. You cannot postpone the **Background Security Improvements**.
Combined Period In Days	Set the days to postpone a major or minor system update on the device. Once configured, the major or minor software updates will appear after a specified number of days following their release. You can set any values between 1 and 90 days.
macOS 15+ Supervised	
Allow Standard User OS Updates	Select the **Allow Standard User OS Updates** checkbox to allow a user to perform OS updates. Select the **Allow standard user to perform Major and Minor Software Updates** checkbox to allow a standard user to perform minor and major software updates. Only the administrators can perform minor and major software updates if you do not select the checkbox.
Deferrals	
Major Update Period In Days	Set the days to postpone a major OS software update on the device. Once configured, the major software update will appear after a specified number of days following its release. You can set any values between 1 and 90 days.
Minor Update Period In Days	Set the days to postpone a minor OS software update on the device. Once configured, the major software update will appear after a specified number of days following its release. You can set any values between 1 and 90 days.
System Update Period In Days	Set the days to postpone a system OS update on the device. Once configured, the major software update will appear after a specified number of days following its release. You can set any values between 1 and 90 days.
Automatic Actions	
Install Security Update	Select one of the following options: • **Allowed**: The user can turn “On” or “Off” the installation of security updates. • **Always On**: The installation of security updates is always “On” for the user. • **Always Off**: The installation of security updates is always “Off” for the user.

4. Click **Next** to configure the distribution settings.

5. Select one of the distribution options to set up the **Software Update Settings** configuration. For more information about configuring distribution options, see **Working with Configurations**.
6. Click **Done**.

10.10.4.60. Security Preferences Configuration

Administrators can manage and control user changes to Firewall settings, Lock Messages and Password Changes on the device with the Security Preferences Configuration.

Applicable to: macOS 10.10+

Procedure

1. Go to Configurations > +Add.
2. Type Security in the search field, and then click the Security Preferences configuration.
3. Enter a Name and Description of the configuration.
4. Select the required configurations:
    - Disable changes to the firewall settings
    - Disable changes to the lock message
    - Disable changes to the password
5. Click Next.
6. Select Enable this configuration option.
7. Select one of the following channel options to apply the configuration:
    - Device channel (most common)
    - User channel (current registered user)
8. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
9. Click Done.

10.10.4.61. Time Server

Applicable to: macOS 10.12.4 and supported newer version.

Create Time Server configuration to allow devices to connect to custom time servers.

Creating a Time Server configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **time** in the search field, and then click the **Time Server** configuration.
4. Enter a name and describe the configuration.
5. Specify **NTP Server**.
6. Specify **Time Zone** string in Olson Time Zone ID format (for example, Pacific / Midway). To get the Olson Time Zone format, run the `"/usr/sbin/systemsetup -listtimezones` " command on the administrator's macOS device.
7. Click **Next** to configure the distribution settings.
8. Click **Done**.

For more information, see **How to create a configuration**

10.10.4.62. Web Content Filter

Licence: Silver

A web content filter configuration limits web access for iOS 7+, macOS 10.15+, and visionOS 1.1+ devices.

Web content filter settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Allowed websites	**Limited Adult Content:** Select this option if you want to block access to web sites based on iOS automatic filters. These filters attempt, with a high degree of accuracy, to block websites with inappropriate content. **Specific Web Sites Only:** Select this option if you want to manually list the accessible web sites. **Plug-in (iOS8 Supervised and macOS 10.15+ Only):** Select this option to use a third-party plug-in.
Permitted URLs	This option is available only if you selected Limit Adult Content. Enter the permitted URLs. Each URL must begin with either: • http:// • https:// Note: If you want to permit both http:// and https:// for the same site, include two separate URLs. All URLs for which the initial characters match the given permitted URL are accessible. Example: http://www.someCompanySite.com permits access to the following: • http://www.someCompanySite.com • http://www.someCompanySite.com/jobs These URLs are accessible even if the iOS automatic filters block them.
Use Deny List URLs	This option is available only if you selected Limit Adult Content. Enter the Blockedlisted URLs. Each URL must begin with either: • http:// • https:// Note: If you want to block both http:// and https:// for the same site, include a row for each URL. All URLs for which the initial characters match the given Blockedlisted URL are blocked. Example: http://www.someCompanySite.com blocks access to the following: • http://www.someCompanySite.com • http://www.someCompanySite.com/jobs These URLs are blocked even if the iOS automatic filters allow them.
Allowlisted bookmarks	This option is available only if you selected Specific Websites Only. Optionally enter the folder into which the bookmark should be added in Safari. Example: /Sales/Products/ If absent, the bookmark is added to the default bookmarks directory.
Filter Name	This option is a available only if you selected Plug-in. Enter text that will be displayed to identify this filter.
Identifier	This option is available only if you selected Plug-in. Enter the bundle ID of the plug-in providing the filtering service.

Setting	What To Do
Service Address	This option is available only if you selected Plug-in. Optional: Enter any server address necessary for use by the plug-in. Consult the documentation for the plug-in to determine if this value is necessary.
Organisation	This option is available only if you selected Plug-in. Optional: Enter any organisation string required by the plug-in. Consult the documentation for the plug-in to determine if this value is necessary.
Username	This option is available only if you selected Plug-in. Optional: Enter any username required by the plug-in service. Consult the documentation for the plug-in to determine if this value is necessary.
Password	This option is available only if you selected Plug-in. Optional: Enter any password required by the plug-in service. Consult the documentation for the plug-in to determine if this value is necessary.
Certificate	This option is available only if you selected Plug-in. Optional: Enter any certificate required by the plug-in service to authenticate the user. Consult the documentation for the plug-in to determine if this value is necessary.
Filter Webkit Traffic	This option is available only if you selected Plug-in. Select to include Webkit traffic in the filter.
Filter Socket Traffic	This option is available only if you selected Plug-in. Select to include socket traffic in the filter.
Custom Data	This option is available only if you selected Plug-in. Optional: Add any key/value pairs required by the plug-in service. Consult the documentation for the plug-in to determine if this value is necessary.

For more information, see **How to create a configuration**.

10.10.4.63. Windows Firewall

The Windows Firewall configuration allows you to configure Windows firewall profile settings as well as the desired set of custom rules to be enforced on the device. This configuration can be used to manage non-domain devices, and reduce the risk of network security threats across all systems connecting to the corporate network.

Configure Windows Firewall configuration

Procedure

1. Go to **Configuration > +Add**.
2. Select **Firewall** configuration.
3. Click on the **Windows** icon.
4. Enter a name for the configuration.
5. Enter a description for the firewall configuration.
6. In the Configuration Setup section, specify the remaining settings as described in the following table.

Setting	What To Do
Profiles	
Enable	Slide the switch to ON to enable the profile.
Type	Displays the type of profile. Example: Domain.
Default Inbound Action	Select a option for a default action that should be performed on inbound traffic. **Allow**: To allow the traffic **Block**: To block the traffic.
Default Outbound Action	Select the default action that should be performed on outbound traffic. **Allow**: To allow the traffic **Block**: To block the traffic.

7. To add Rules, click **+Add** and configure the following settings:

Setting	What To Do
Rules	
ON	Slide the switch to enable the profile.
Rule Name	Enter a name that identifies this rule.
Description	Enter a description that clarifies the purpose of this rule.
Direction	Select the direction of the traffic to which the rule should be applied: • **In**: For inbound traffic • **Out**: For outbound traffic • **Both**: Both directions.
Action	Select the action to be performed • **Allow**: To allow the traffic • **Block**: To block the traffic.
Profile	Select the profile(s) to which the rule should be applied: • **All** • **Domain** • **Private** • **Public**
App	Type the package family name (PFN) or full path to the app executable.
Protocol	Select any of the following protocol to which the rule should be applied: • **TCP** • **UDP** • **ICMP**
Local Address Ranges	Type the local IPv4/IPv6 address ranges or subnet masks.
Local Port Ranges	Type comma separated list of remote ports or port ranges. Example: 20,50,100-120.
Remote Address Ranges	Type the remote IPv4/IPv6 address ranges or subnet masks.
Remote Port Ranges	Type comma separated list of remote ports or port ranges. Example: 20,50,100-120.
Interface Types	Select any of the following interface type options: • **All** • **Remote Access** • **Wireless** • **Lan**

Setting	What To Do
	• **Mobile Broadband** The default option **All** is applied if no iterface type option is selected.

8. Click **Next**.
9. Select one of the following distribution options:
   - All Devices
   - No Devices (default)
   - Custom
10. Click **Done**.

10.10.4.64. Windows Information Protection

Licence: Gold

Applicable to: Windows 10+

A Windows Information Protection (WIP) configuration defines WIP settings to protect enterprise data. This configuration can be applied to devices enrolled under management. You can also view WIP details for a configured device on the overview page of that device.

Setting Up Windows Information Protection for Windows

Procedure

1. Go to **Configuration > +Add**.
2. Select the **Windows Information Protection** configuration.
3. Enter a name for the configuration.
4. Enter a description.
5. In the Configuration Setup section, specify the remaining settings as described in the following table.
6. Click **Next**.
7. Select a distribution for this configuration.

Category	Setting	What To Do
	Name	Enter a name that identifies this configuration.
	Description	Enter a description that clarifies the purpose of this configuration.
Enterprise Information	**All Versions (Windows 10+)**	
	Protected Domain Names	Specify the list of identities for which Data Protection policies are configured. Emails and other data associated with these identities will be considered enterprise and protected. • This is a list of domains separated by | with the first domain in the list considered the primary identity for the purposes of Windows UI. • For example: "domain1.com|domain2.co.uk"
	Network Domain names	Specify the list of domains that comprise the boundaries of the enterprise. Data from one of these domains that is sent to a device will be considered enterprise data and protected. • These locations will be considered a safe destination for enterprise data to be shared to. • This is a comma-separated list of domains. • For example: "mail.domain3.com, domain4.com"
	Cloud Resources	Contains a list of Enterprise resource domains hosted in the cloud that need to be protected. Connections to these resources are considered enterprise data. Specify one or more domain names with optional proxy addresses in brackets. • For example: "domainname1.com, domainname2 (10.0.0.1)". • If a proxy is paired with a cloud resource, traffic to the cloud resource will be routed through the enterprise network via the specified proxy server (on Port 80). • All proxy addresses specified in this field should also be entered in the following Internal Proxy Servers field.
	IP Range	Sets the enterprise IP ranges that define the computers in the enterprise network. Data that comes from those computers will be considered part of the enterprise and protected. These locations will be considered a safe destination for enterprise data to be shared to. This is a comma-separated list of IPv4 and IPv6 ranges. • This is a comma-separated list of IPv4 and IPv6 ranges. • Select the **IP Ranges are authoritative** option when the client must accept the configured list and not use heuristics to attempt to find

Category	Setting	What To Do
		other subnets.
	Neutral Resources	Specifies the list of domain names that can be used for work or personal resource.
	Proxy Servers	Specifies the comma-separated list of proxy servers. Any server on this list is considered non-enterprise. • For example: "157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59". • Select the **Proxy Servers are authoritative** option when the client must accept the configured list of proxies and not try to detect other work proxies.
	Internal Proxy Servers	Specifies the comma-separated list of internal proxy servers. • For example "157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59". • These proxies have been configured by the admin to connect to specific resources on the Internet. They are considered to be enterprise network locations. The proxies are only leveraged in configuring the EnterpriseCloudResources policy to force traffic to the matched Cloud Resources through these proxies.
Data Protection	**All Versions (Windows 10+)**	
	Enforcement Level	Choose one of the following enforcement levels: • Off - No protection (previously encrypted data will be un-encrypted). • Silent - Encrypt the data and and audit activities on the device after data is being protected. The user is not prompted on account of any negative data/app information. • Override - Similar to the Silent mode. In addition, if an app or data is being used incorrectly, the user is prompted to either proceed or cancel the operation the user is currently performing. • Block - Similar to the Silent mode. In addition, if an app or data is being used incorrectly, the operation the user is currently performing is blocked and the user is warned with the reason for blocking the operation. Note: Except in the Off mode, any data or app that was not supposed to use enterprise data or resources will be logged on the device. That data can be removed from the device using another configuration service provider (CSP).

Category	Setting	What To Do
	Data Recovery Certificate	Specify a recovery certificate that can be used for data recovery of encrypted files. • This is the same as the data recovery agent (DRA) certificate for encrypting file system (EFS). However, this certificate is delivered through MDM instead of through the Group Policy. You can also select one or more of the following options: • Allow User Decryption • Revoke On Unenrol • Show EDP Icons • Require Protection Under Lock (Windows 10 Mobile only)
RMS	**All Versions (Windows 10+)**	
	Allow Azure RMS	Specify whether to allow Azure Rights Management (Azure RMS) encryption for WIP.
	RMS Template ID	Specify TemplateID GUID to use for RMS encryption. The RMS template allows the admins to configure the details about who has access to RMS-protected file and how long they have access.
App Control	**All Versions (Windows 10+)**	
	Specify a collection of apps that are built under the **Apps > App Catalog** page with a value of WIP. Specify the rule definitions for the apps using the following set of parameters:	
	App Type	Select one of the following app types: • Publisher/PFN Equals - applies to Windows 10+ supporting PFN. • EXE/Win32 Equals - applies to Windows Desktop only.
	App Identifier	Select the app from the choices displayed to add it to the App Identifier. You can also click **Lookup Apps**.
	App Description	Enter a description for the app.

10.10.4.65. Windows Restrictions

Windows restrictions determine which features are enabled on Windows 10+ devices.

Windows Restrictions settings

Category	Setting	What To Do
	Name	Enter a name that identifies this configuration.
	Description	Enter a description that clarifies the purpose of this configuration.
Device Capabilities	**All Versions (Windows 10+)**	
	Disable Wi-Fi offloading	Select to prevent the device from accessing compatible networks to carry data intended for authorised wireless networks.
	Disable internet sharing	Select to prevent the device from accessing the internet by means of another wireless device.
	Disable location	Select to disable location services.
	Disable mobile data roaming	Select to disable data roaming when the device is in mobile mode.
	Disable bluetooth	Select to prevent the device from establishing Bluetooth connections.
	Disable VPN when roaming or on a mobile network	Select to prevent the device from establishing VPN connections when not on WiFi.
	Disable manual configuration of Wi-Fi	Select to prevent the user from manually configuring the Wi-Fi settings on the device.
	Disable Wi-Fi	Select to allow or deny WiFi connection.
Telemetry - Allow device to send diagnostic and usage telemetry data.	**Windows 10 only**	
	Telemetry level	Select one of the following telemetry levels of data reporting: • **Security** - Send information about the Connected User Experience, Telemetry Component Settings, the Malicious Software Removal Tool, and Windows Defender. • **Basic** - Send basic device information that includes quality-related data, app compatibility, app usage data, and data from the Security level. • **Enhanced** - Send more information that includes usage and performance of Windows, Windows Server, System Centre, and apps. Also includes advanced reliability data, and data from both the Basic and the Security levels. • **Full (Default)** - Send all data to identify and help fix the problems, plus data from the Security, Basic, and Enhanced levels.
Data Loss Prevention (DLP)	**All Versions (Windows 10+)**	

Category	Setting	What To Do
	Disable camera	Select to prevent the end user from using the camera app.
	Disable access to storage (SD) card	Select to prevent the device from accessing a storage card.
	Disable screen capture (Desktop only)	Select to prevent from capturing the screen using screen capture apps within the device.
	Disable USB mass storage (HoloLens only)	Select to prevent HoloLens from accessing mass storage devices.
Data Usage	**Windows 10+**	
	Cost of 3G Connections	Select one of the following options: • **Unrestricted** - Connection is unlimited and not restricted by usage charges and capacity constraints. • **Fixed** - Connection is restricted by usage charges and capacity constraints after a certain data limit. • **Variable** - Connection is charged on a per byte basis.
	Cost of 4G Connections	
Defender	**Windows 10+**	
	Disable Defender RealTime Monitoring functionality	Select to disable Windows Defender Realtime Monitoring functionality
DeviceGuard	**Windows 10+**	
	Disable virtualisation based security (VBS)	Select to prevent virtualisation based security from providing support for security services.
	Credential Guard with virtualisation-based security	Select one of the following options: • **Disabled** - Disable Credential Guard with virtualisation-based security. • **Enabled with UEFI lock** - Enable Credential Guard with virtualisation-based security with Unified Extensible Firmware Interface (UEFI) lock. • **Enabled without lock** - Enable Credential Guard with virtualisation-based security without UEFI)lock.
	Platform Security Level (Require Platform Security Features)	Select one of the following options: • **VBS with Secure Boot** - Select this option to enable virtualisation-based security with secure boot. • **VBS with Secure Boot and Direct memory Access** - Select this option to enable virtualisation-based security with secure boot and direct memory access (DMA).

Category	Setting	What To Do
Privacy	**Windows 10+**	
	Disable the Advertising ID	Select to disable Advertising ID.
Windows and Application	Disable to publish the activity feed by Apps/OS	Select to prevent Apps/OS to publish to the activity feed.
	All Versions (Windows 10+)	
	Disable Microsoft accounts for service other than email	Select to prevent the end user from using Microsoft accounts for authenticating to non-email services.
	Disable non-Microsoft accounts	Select to prevent the end user from configuring email using non-Microsoft accounts.
	Disable Cortana personal assistant	Select to prevent the end user from accessing Microsoft's personal assistant.
	Disable location-based search	Select to prevent searches from leveraging the device location.
	Disable developer unlock	Select to prevent the end user from enabling sideloading of apps. The default mode when a device is enrolled in MDM is SideLoad enabled.
	11+ Supported Editions only	
	Configuration of the Teams Chat Icon on the taskbar	Select one of the following options: • **Show:** Chat icon appears on the taskbar by default. Users can show or hide it in Settings. • **Hide:** Chat icon hidden by default. Users can show or hide it in Settings. • **Disabled:** Chat icon not displayed, and users cannot show or hide it in Settings. • **Not Configured:** Chat icon behaves according to the defaults for your Windows edition. Changes do not take effect until restart of the Windows device.
	Windows 10+ Supported Versions only	
	Disable automatic update of apps from Microsoft Store	Select to prevent automatic update of apps from the Microsoft Store.
	Disable the launch of all apps from Microsoft Store that came preinstalled or were downloaded	Select to prevent the end user from launching all pre-installed or downloaded apps from Microsoft Store. Supports only Enterprise and Education Windows editions.

Category	Setting	What To Do
Other Restrictions	Let apps run in the background **All Versions (Windows 10+)**	Select one of the following options: • **User in control**: allows the user to control the running of apps in the background. • **Force allow**: allows running apps in the background. • **Force deny**: prevents running of apps in the background.
	Disable ability to unenrol from UEM and delete the workplace account.	Select to prevent the end user from unenrolling from UEM and deleting company account image.
	Disable user from setting the device lock grace period (HoloLens only). **Windows 10+ Supported Versions only**	Select to prevent the user from setting the device lock grace period.
	Disable user to factory reset the device by using control panel and hardware key combination	Select to prevent the end user from setting the device lock grace period.
	Require users to connect to network during device set up (Autopilot profile is required)	Select this option to enable TenantLockdown to lock all the Windows devices that are enrolled using the Autopilot feature.
	Windows 10+ Supported Versions only	
	Disable user from making changes to the eSIM through the user interface.	Select this option to restrict the user from making any changes to the eSIM profiles.

10.10.4.66. Windows Desktop restrictions

Applicable to: Windows 10 Desktops

This section contains the following topics:

- Configure Windows Desktop restrictions
- Creating an Allowlist for removable storage devices

Administrators can control OS information on managed Windows 10 Desktop devices by restricting user access to the following areas on a device:

- Control Panel
- Task Manager
- File Explorer
- Registry Editor

The above functions enables a user to make a lot of changes to their device. Using this feature, administrators have the ability to restrict access to these system level controls and thereby secure the access.

This feature requires Bridge. See Ivanti Bridge for details.

Configure Windows Desktop restrictions

Procedure

1. Go to **Configuration > +Add**.
2. Select **Windows Desktop Restrictions** configuration.
3. Enter a name for the configuration.
4. Enter a description.
5. In the Configuration Setup section, specify the remaining settings as described in the following table.

Setting	What To Do
Task Manager	Select the **Deny access** checkbox for the setting for which the access should be denied.
Control Panel	
Registry Editor	
File Explorer **Removable storage** Access mode for Removable Storage	Select the **Restrict Capabilities** checkbox to restrict capabilities of File Explore. Example: Removal of map network drive. Click on the link provided to view the list of capabilities that are restricted. • **Restrict Read Access**: This prevents any access and is the most restrictive configuration. • **Restrict Write Access**: This allows limited access, but prevents unauthorised removal of data or the ability to add viruses, etc. to the device.

6. Click **Next**.
7. Select one of the following distribution options:
   - All Devices
   - No Devices (default)
   - Custom
8. Click **Done**.

> For the configuration to take complete effect, the device should be rebooted after applying the configuration.

Creating an Allowlist for removable storage devices

If you want to create an Allowlist of permitted storage devices, complete the following steps first:

- Attach the USB storage devices you want to allow to a PC.
- Open Device Manager and click on the USB controller.
- Look at the settings for each controller for device information.
- Store the device information to use when creating your Allowlist.

To create Allowlist for removable storage device:

Procedure

1. In the **Windows Desktop Restrictions** configuration page, click **+Add** under **Allowlisted Removable Storage** section.
2. In the **Add hardware IDs** window, enter the hardware ID for one or more devices that you wish to remove from the Allow list and block as storage devices.
3. Click **Add hardware IDs**. The list of Allowlisted hardware IDs are displayed under **Allowlisted Removable Storage** section.

> To edit or delete a hardware ID from the list, select the Edit or Delete option under the **Actions** column.
>
> For the configuration to take complete effect, the device should be rebooted after applying the configuration.

10.10.4.67. Desktop Settings for Windows 10

The Desktop Settings for Windows 10 configuration allows you to customise the desktop settings and push them to Windows 10 devices. Using this configuration, you can configure the following desktop settings:

- Desktop background image
- Lock screen image
- Upload a custom Screen Saver
- Desktop shortcuts

> This feature requires Bridge. See **Ivanti Bridge** for details.

Procedure

1. Under **Configuration**, click **+Add**.
2. Select **Desktop Settings for Windows 10** configuration. The**Desktop Settings for Windows 10** page is displayed.
3. In the **Name** field, type an appropriate name for the settings.
4. (Optional) Click the +**Add Description** link to add a description for the configuration.
5. In the **Configuration Setup** section, configure the following settings:

Setting	Description
File Delivery	Select any of the following file delivery options for Desktop Settings: • **Upload File** - Upload settings to Ivanti Neurons for MDM. • **Override URL** - Provide override URLs with the settings files to download.
Desktop Wallpaper Settings	Click **Choose File** to locate and upload a wallpaper image.: Supported file formats are BMP, JPG, JPEG, PNG.
Lock screen Wallpaper Settings (The Lock screen Wallpaper setting is **NOT** supported on Windows 10 Pro devices)	Click **Choose File** to locate and upload a wallpaper image. Supported file formats are BMP, JPG, JPEG, PNG.
Screen Saver Settings	Click **Choose File** to locate and upload a screen saver file. Upload only Windows compatible .SCR files. Select **Password protect for Screen Saver** if you want to set password to unlock the Screen Saver mode. Select a **Screen Saver Timeout** period (in minutes).
Desktop shortcuts	Click **Add Shortcut** to set up desktop shortcuts to add to device desktops. The **Add Shortcut** window is displayed. Fill out the table using the following options: • **Location** - Type the location where the shortcut is to appear on the Windows device. • **Target Path** - Type the local path, or UNC path or the drive letter to which the shortcut will lead. Target path can also be a URL. • **Arguments** - Type any argument to be used when opening the target file. • **Working Directory** - Type the folder path that contains files required by the target. • **Icon File** - Upload valid Windows .ico files. After configuring the options, click **Add Shortcut**.

6. Click **Next**.
7. Select one of the following distribution options:
   - All Devices
   - No Devices (default)
   - Custom
8. Click **Done**.

10.10.4.68. Windows Hello for Business Configuration

This configuration allows the administrators to set up Windows Hello in the devices. Setting up Windows Hello requires setting up a PIN to sign-in to the device.

Applicable to: Windows 10

ProcedureProcedure

1. Go to Configurations > +Add.
2. Type windows in the search field, and then click the Windows Hello for Business configuration.
3. Enter a Name and Description of the configuration.
4. Toggle the Enable/Disable Windows Hello for Business for Windows 10 Devices to On.

> The toggle is set to On by default. Disabling Windows Hello for Business does not remove the PIN from the devices.

5. Set the PIN Complexity.
6. Select the required configurations:
    - Requires a Trusted Platform Module (TPM) for Windows Hello for Business
    - Use Windows Hello for Business certificates as smart card certificates
    - Use of biometric gestures, such as face and fingerprint, as an alternative to the PIN gesture for Windows Hello for Business
    - Requires enhanced anti-spoofing for facial feature recognition on Windows Hello face authentication
    - Dynamic Lock
    - Enables users to sign in with a FIDO2 security key.
7. Click Next.
8. Select Enable this configuration option.
9. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
10. Click Done.

10.10.4.69. Windows AI Management Configuration

Ivanti Neurons for MDM allows the administrators to manage Windows AI settings and configurations. The Windows AI Management enhances creativity and productivity with the help of a powerful AI assistant. Use the **Windows AI Management** configuration to manage Windows AI features on enrolled Windows devices. This configuration allows administrators to control Microsoft Copilot, Windows Recall, and Microsoft Paint AI capabilities through Windows AI Configuration Service Provider (CSP) policies.

Administrators can disable selected AI capabilities, remove access to Copilot features, control Windows Recall behavior, and manage AI-powered image generation features in Microsoft Paint.

Applicable to: Windows 10+

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Windows AI Management** configuration.
3. Enter a **Name** and **Description** of the configuration.
4. In the **Configuration Setup** section, select from the following options: ### Copilot Settings

Setting	Description
Disable Windows Copilot	Prevents users from accessing Windows Copilot.
Disable Copilot Hardware Key	Disables the dedicated Copilot hardware key on supported devices.
Remove Microsoft Copilot App	Removes the Microsoft Copilot application from the device.

Recall Settings

Setting	Description
Disable AI Data Analysis	Disables AI-based data analysis used by Windows Recall.
Set Maximum Storage for Recall Snapshots (GB)	Specifies the maximum amount of storage that Windows Recall can use for storing snapshots.

Paint AI Settings

Setting	Description
Disable Image Creator	Disables the Image Creator feature in Microsoft Paint.
Disable Cocreator	Disables the Cocreator feature in Microsoft Paint.
Disable Generative Fill	Disables the Generative Fill feature in Microsoft Paint.

Microsoft has deprecated the **TurnOffWindowsCopilot** policy used by this configuration. As a result, this configuration no longer affects the Copilot app residing on devices.

> If you don't select the **Disable Windows Copilot** checkbox, the configuration will override the previous configuration selection on the device to enable Windows AI Management.

5. Click **Next** to configure the distribution settings.
6. Select one of the distribution options to set up the **Windows AI Management** configuration. For more information about configuring distribution options, see **Working with Configurations**.
7. Click **Done**.

10.10.4.70. Play Integrity (Previously SafetyNet Attestation)

Play Integrity (Previously SafetyNet) helps in assessing the security and compatibility of Android devices using Google's Play Integrity APIs. When configured, it allows you to analyze devices after a regular time interval in determining whether the device has been tampered or not.

> Play Integrity is now supported on all Android versions.

Procedure

1. In the **Configuration** tab, click **+Add**.
2. Select **Play Integrity** configuration. The **Play Integrity Configuration** page is displayed.
3. In the **Name** field, type an appropriate name for the Play Integrity Configuration.
4. Click the +**Add Description** link to add a description for the configuration. This field is optional.
5. In the **Configuration Setup** section, type the minimum time interval (in hours) that should be applied for assessing the security and compatibility check on devices. The value should be between 1 to 24.
6. Click **Next** and select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom

Click **Done**.

> When the Play Integrity and SafetyNet nonces will be sent to the device, Play Integrity nonce will be prioritized over the SafetyNet nonce.

10.10.4.71. Advanced Android Passcode and Lock Screen

Couldn't convert your doc.

10.10.4.72. Microsoft Defender for Endpoint

Microsoft Defender for Endpoint (MDE) configuration formerly known as Windows Advanced Threat Protection, allows customers to onboard and offboard devices to MDE service.

Procedure

1. Go to **Configuration > +Add**.
2. Select **Microsoft Defender for Endpoint** configuration.
3. Enter a name for the configuration.
4. Enter a description.
5. In the Configuration Setup section, specify the remaining settings as described in the following table.

Setting	Description
Onboarding or Offboarding Blob	Paste the onboarding or offboarding blob from the Microsoft Defender for Endpoint Security Centre site

6. Click **Next**.
7. Select one of the following distribution options:

- All Devices
- No Devices (default)
- Custom

8. Click **Done**.

10.10.4.73. Certificate-based authentication

Ivanti Neurons for MDMsupports certificate-based authentication which allows administrators to log in using digital certificates and a tenant-specified (vanity) hostname. When enabled and configured, the administrators can log in using the digital certificates instead of the basic authentication (username and password).

> This feature is disabled by default. Administrators should contact Support to enable this feature on their tenant(s). This feature is only available on NA3 cluster environments, and only if enabled by Support. Please ensure that you have your super admin username and password tested and ready, because once certificate-based authentication is enabled, these credentials will be the only ones you can use to log in until you have successfully configured your vanity domain.

Procedure

1. In the **Admin** tab, select **Vanity Host Configuration**.
2. In the Vanity Host Configuration page, configure the following options:
3. Click **Save**.
   It may take a few minutes for your vanity host to become accessible.

Setting	What To Do
Create Vanity Domain	Type the name of the vanity domain. This is the domain name that may more closely align with your corporate identity and into which you can log in using digital certificates.
Upload Trusted issuing CA certificates	Click **Choose File** to select and upload the CA certificate that issues certificates to your administrators. To enable the certificate revocation check, select **Enable certificate status validation settings for this certificate** (optional). This option is enabled by default. Deselect this option to disable certificate revocation. Click **Add More** to add more certificates. Ensure that the certificate format is .p7b, .pem, .der, .crt or .cer.
Certificate Attribute mapping	Certificate attribute mapping configures the mapping of the certificate identity elements to the account attributes of the admin. In the **From Certificate** field, select either of the following certificate elements: • **NTPrincipalName** • **RFC 822 Name** In the **To Variable** field, select any of the following account attributes of the admin: • **UserUPN** • **$UserEmailAddress** • **$EDIPI**

10.10.5. User Resource Configurations

This section contains the following topics:

- CalDAV Configuration
- CardDAV Configuration
- Google Configuration
- Email Configuration
- Exchange Configuration
- Font Configuration
- Subscribed Calendar Configuration
- Create a Web Clip Configuration
- Office 365 Installation
- Windows GPO Settings
- BitLocker Encryption Configuration

10.10.5.1. CalDAV Configuration

A CalDAV configuration defines access to a web calendar using the CalDAV internet standard.

CalDAV settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Hostname and Port	Enter the host name and port for the calendar server.
Principal URL	Enter the URL for accessing calendar services.
User	Enter the user name to use for access.
Password	Enter the password to use for access.
Use SSL	Select to use only the secure socket layer for communications between the device and the server.
Per-App VPN	**Prerequisite**: Configure Tunnel or any per-app VPN configuration before configuring per-app VPN in CalDAV configuration. From the drop-down menu, select the pre-configured per-app VPN configuration. **Applicable to**: iOS 14+

For more information, see **How to create a configuration**

10.10.5.2. CardDAV Configuration

A CardDAV defines access to a web address book using the CardDAV internet standard.

CardDAV settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Hostname and Port	Enter the host name and port for the address book server.
Principal URL	Enter the URL for accessing address book services.
Username	Enter the user name to use for access.
Password	Enter the password to use for access.
Use SSL	Select to use only the secure socket layer for communications between the device and the server.
Per-App VPN **iOS 10+**	**Prerequisite**: Configure Tunnel or any per-app VPN configuration before configuring per-app VPN in CardDAV configuration. From the drop-down menu, select the pre-configured per-app VPN configuration. **Applicable to**: iOS 14+
Communication Service Rules	Choose a default app to use to make audio calls to contacts within the CardDAV system.

For more information, see **How to create a configuration**

10.10.5.3. Google Configuration

Google account configuration connects iOS 9.3.2 and visionOS 1.1 or Android 6.0+ devices, or supported newer versions, to Google accounts. Android enterprise is required for Google accounts. The configuration can set up multiple Google email addresses and any other Google services the user enables after authentication.

Procedure

1. Go to **Configuration > +Add**.
2. Select the **Google Account** configuration.
3. Enter a name for the configuration.
4. Enter a description.
5. In the Configuration Setup section, specify the remaining settings as described in the following table:

Setting	What To Do
iOS 9.3.2+ , Android 6.0+	
Name	Enter a name that identifies this configuration.
Account description	Enter the display name of the account.
Account name	Enter the full name of the user for the account.
Email address	Enter the Google email address of the account.
Per-App VPN	**Prerequisite**: Configure Tunnel or any per-app VPN configuration before configuring per-app VPN in Google Account configuration. From the drop-down menu, select the pre-configured per-app VPN configuration. **Applicable to**: iOS 14+
iOS 10+	
Communication Service Rules	Choose a default app to use to make audio calls to contacts within the Google system by selecting any of the following options: • **From App Catalogue & System Apps**: Search for apps by typing the first few letters of the app name. • **Enter Bundle ID (for Apple system apps only)**: Type the System App Bundle ID. Bundle ID must begin with 'com.apple'.

6. Click **Next**.
7. Select one of the following distribution options:
   - All Devices
   - No Devices (default)
   - Custom
8. Click **Done**.

When a Google account configuration is applied to the device, Go client prompts the user to log in to Google.

For more information, see **How to create a configuration**

10.10.5.4. Email Configuration

An email configuration sets up POP or IMAP email on devices.

Email settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Account Description	Enter the text you want to use to identify this email account.
Account Type	Select IMAP or POP. If you select IMAP, you can also enter the path prefix. The internet service provider (ISP) can give you information on which type of account is available. A prefix is generally required when all IMAP folders are listed under the Inbox. ISPs that require prefixes usually provide information on the specific prefix to configure.
User Display Name	Enter the text you want to use to identify email account user. Note that the user can set this value on the device, as well.
Email Address	Enter a variable to specify the email address for the account.
Allow Move	Select if you do not want to prevent email from being moved from this account.
Enable S/MIME	Select to turn on support S/MIME encryption. Then, you can select signing and encryption certificates. Requires certificate caching. Make sure that caching is enabled in the Certificate Authority being used by Identity Certificate's configuration. **iOS 10.3+:** Select one of the following options for the **S/MIME signing** and **S/MIME encryption** fields: • Off • On • User Select **iOS 12.0+:** • Enable user to override S/MIME signing settings • Enable user to select S/MIME signing identity • Enable user to override S/MIME encryption settings • Enable user to select S/MIME encryption identity **Enable S/MIME per-message signing and encryption** if required.
Allow Mail Drop	Select to allow Mail Drop for this account. Mail Drop enables the user to send email with large attachments by storing the attachment in iCloud and placing a link to it in the email. For more information on Mail Drop go to: https://support.apple.com/
Per-App	The ability to associate a number of different per-app VPN profiles on Mail domains is supported by Apple. IMAP and POP3 email configurations are now supported over per-app VPN.

Setting	What To Do
VPN	**Prerequisite**: Configure Tunnel or per-app VPN configuration before configuring per-app VPN in email configuration. From the drop-down menu, **Select Per-App VPN config**.

Incoming Mail

Setting	What To Do
Mail Server and Port	The internet service provider (ISP) can give you this address.
User Name	Enter the user name for accessing the incoming mail server. This often the same as the email address. Your ISP can provide the format.
Authentication Type	Select the authentication type defined by the ISP.
Password	Enter the password for accessing the incoming mail server.
Use SSL	Select to use only the secure socket layer for communications between the device and the server.

Outgoing Mail

Setting	What To Do
Mail Server and Port	The internet service provider (ISP) can give you this address.
User Name	Enter the user name for accessing the outgoing mail server. This often the same as the email address. Your ISP can provide the format.
Authentication Type	Select the authentication type defined by the ISP.
Password	Enter the password for accessing the outgoing mail server.
Outgoing password same as incoming	Select if SMTP authentication uses the same password as POP/IMAP.
Use Only in Mail	Select if you want this configuration used only by the email client. Other apps that send email, including apps that send content using the native email client, are not able to use this configuration.
Use SSL	Select to use only the secure socket layer for communications between the device and the server.

10.10.5.5. Exchange Configuration

An Exchange configuration sets up ActiveSync-based email on Android, iOS, and visionOS devices and Exchange Web Services (EWS)-based email for macOS devices.

> The Exchange Configuration is deprecated by Samsung in Android 9. For Samsung devices on Android 9 and later versions, the Exchange Configuration is not supported in Device Admin mode.

Exchange settings

Setting	What to do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Exchange Host	If you are using **Sentry** to control email access, enter the Sentry server host name. Otherwise, enter the address of the ActiveSync server.*
Allow Move	**For iOS and Android:** Select if you do not want to prevent email from being moved from this account. **For Windows 10:** Not applicable.
Enable S/MIME	Select to turn on support S/MIME encryption. Then, you can select signing and encryption certificates. Requires certificate caching. Make sure that caching is enabled in the Certificate Authority being used by Identity Certificate's configuration. **iOS 10.3+:** Select one of the following options for the **S/MIME signing** and **S/MIME encryption** fields: • Off • On • User Select **iOS 12.0+:** • Enable user to override S/MIME signing settings • Enable user to select S/MIME signing identity • Enable user to override S/MIME encryption settings • Enable user to select S/MIME encryption identity **Enable S/MIME per-message signing and encryption** if required.
Sync Recent Email Addresses	Select to sync recently-contacted email addresses between the device and the server.
Use Only in Mail	Select if you want this configuration used only by the email client. Other apps that send email, including apps that send content using the native email client, are not able to use this configuration.
Use SSL	Select to use only the secure socket layer for communications between the device and the server.
Enable OAuth for exchange payload	iOS 12.0+ and macOS 10.14+: Select to enable authentication using OAuth. If this option is enabled, the following additional settings are available for email apps that support authentication using OAuth: • OAuth Sign In URL • OAuth Token Request URL
Domain	Enter the domain for this email account, unless you want the user to be prompted for it.
User	Enter a variable representing the email address for this account.*
Account Password	Enter the password for this account, unless you want the user to be prompted for it.
Email Address	Enter a variable representing the email address for this account.*

Setting	What to do
Past Days of Mail to Sync	Select the number of days of email to sync between the device and the server.
Per-App VPN	**Prerequisite**: Configure Tunnel or any per-app VPN configuration before configuring per-app VPN in Exchange Active Sync configuration. From the drop-down menu, select the pre-configured per-app VPN configuration. **Applicable to**: iOS 14+
Android and Windows	
Sync Calendar	**For Android and Windows 10:** Select to sync calendar items between the device and the server. **For Samsung devices:** This setting is not used (it is ON by default). **For Android Email+ app:** This setting is used.
Sync Contacts	**For Android and Windows 10:** Select to sync contacts between the device and the server. **For Samsung devices:** This setting is not used (it is ON by default). **For Android Email+ app:** This setting is used.
Sync Email	**For Android and Windows 10:** Select to sync email between the device and the server. **For Samsung devices:** This setting is not used (it is ON by default). **For Android Email+ app:** This setting is not used (it is ON by default).
Sync Tasks	**For Android and Windows 10:** Select to sync tasks between the device and the server. **For Samsung devices:** This setting is not used (it is ON by default). **For Android Email+ app:** Not applicable.
iOS 13.0+	
• Sync Calendar • Sync Contacts • Sync Mail • Sync Notes • Sync Reminders	Specify individual syncing of Outlook Exchange items such as Calendar, Contacts, Mail, Notes and Reminders. For each item, select or deselect the **Enable** and the **Allow User Override** options. Sync must be enabled for at least one of these items. If you disable syncing for one of the options but allow user to override, the user will still be able to enable it.
Identity Certificate	Select an identity certificate from the list if you want the device to authenticate to the server using a certificate. Certificates appear in this list only if already configured using an identity certificate configuration.
Android	
Use Certificate Based Authentication Only	Use the selected identity certificate as the only means of authenticating to the Exchange server.
Accept all SSL Certificates	Select to allow device users to set Android devices to accept all SSL certificates. This setting applies to Android Email+ and Samsung Knox Email. • Use caution when enabling this setting, as device users might unknowingly expose the device to attack.

Setting	What to do
	• This option needs to be enabled if the Sentry certificate is a self-signed or unknown certificate.
Exchange App Priority	Select the email client to be configured by default on Android devices - Android Email+ and Samsung Email. Email+ app are added in the app catalog for all tenants that have enabled the Exchange app priority.
iOS 10+	
Communication Service Rules	Choose a default app to use to make audio calls to contacts within the CardDAV system.
Windows 10+ Only	
Configure Outlook	Select this option to configure Microsoft Outlook to a device. This option is supported only if Bridge is enabled.

*Type $ to see a list of supported **variables**, if available, for this field.

10.10.5.6. Font Configuration

A font configuration enables you to provide additional TrueType or OpenType font files to iOS 7 devices. The following table describes the font settings:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Upload Fonts	Drag the font file to the dotted box, or click **Choose File** to select it from your file system. Font files must be .otf or .ttf files.

For more information, see **How to create a configuration**

10.10.5.7. Subscribed Calendar Configuration

A subscribed calendar configuration defines access to a public web calendar.

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
URL	Enter the URL for accessing the calendar.*
User	Enter the user name to use for access.*
Password	Enter the password to use for access.
Use SSL	Select to use only the secure socket layer for communications between the device and the server.

Type $ to see a list of supported **variables**, if available, for this field.

For more information, see **How to create a configuration**

10.10.5.8. Create a Web Clip Configuration

A web clip is a shortcut to a website or web page from an iOS device. Use a web clip configuration to create standard web clips on devices. You can add a web clip icon to your iOS device that will launch a specific website. Web Clips help you to quickly find and use bookmarks on the home screens of your devices. You can also control some of the parameters of the Mobile Safari viewing experience for the site.

> Delegation with custom distribution option is available for this configuration. For more information, see *Distributing the configuration* topic in **Working with Configurations**.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Click **Configurations**.
3. Click +Add.
4. Search and select the Web Clip configuration.
5. Configure the settings on this page. Refer to the table in the topic **Web Clip Configuration Settings** for guidance on the values.
6. Click **Next** to configure the distribution settings.
7. Select **Custom** and then select **Devices/ Device Groups**.
8. Click **Done**.

Web Clip Configuration Settings

The following table lists the Web Clip Configuration settings:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Label	Enter the text that you want to display below the shortcut on the device screen.*
URL	Enter the URL that the web clip will access.*
Removable	Select the check box to allow the device user to delete the web clip.
Icon	Drag the icon file to the dotted box, or click **Choose File** to select it from your file system.
Precomposed Icon	Select to eliminate the special effects added by more recent versions of Safari.
Full Screen	Select to display the web clip in full-screen mode instead of as content in a browser.
Ignore Manifest Scope	Select to allow navigation to an external website without displaying the Safari browser. This option has no effect when Full Screen is not selected.
Target Application Bundle Identifier	The application bundle identifier that specifies the application that opens the URL. **Example**: com.google.chrome.ios

> Type $ to see a list of supported **variables**, if available, for this field.

Related topics:

- **Multi-user Secure Sign-in for iOS**
- **How to create a configuration**

10.10.5.9. Office 365 Installation

Licence: Silver

Applicable to: Windows 10+

Setting up Office 365 Installation

The Office 365 installation is a configuration setting that can be applied to selected devices for installing or uninstalling Office 365. You can define the configuration settings in xml format by using Microsoft's Office deployment tool and then uploaded the file. After uploading the file(s), you can push the configuration options to selected device(s).

Procedure

1. In the **Configuration** tab, click **+Add**.
2. Select **Office 365 Installation**. The **Office 365 Installation** page is displayed.
3. In the **Name** field, type an appropriate name for the configuration.
4. Click the +**Add Description** link to add a description for the configuration.This field is optional.
5. In the **Configuration Setup** section, update the following fields:

Field name	Description
Configuration file for installing Office 365	Click the **Choose File** button to browse and select the configuration file in XML format that includes the defined settings for Office 365 installation. Example: <Configuration> <Add OfficeClientEdition="64" Channel="Current"> <Product ID="O365ProPlusRetail"> <Language ID="en-us"/> </Product> </Add> </Configuration> Ensure that the configuration file is in xml format and the green check mark is displayed after adding the configuration settings file.
Configuration file for uninstalling Office 365	Click the **Choose File** button to browse and select the configuration file in the xml configuration file in XML format that includes the defined settings for uninstalling Office 365. Example: <Configuration> <Remove All="TRUE"/><Display Level="None" AcceptEULA="TRUE" /> </Configuration> Ensure that the configuration file is in xml format and the green check mark is displayed after adding the configuration settings file.

6. Cick **Next**.
7. Select any of the following options to distribute the settings to device(s).

Option	Description
Enable this configuration	Selecting the check box allows this configuration to the selected devices. Deselecting the check box removes the configuration, if already applied to devices.
All Devices	Distributes the settings to all the devices.
No Devices	Withholds the settings to be distributed to device(s).
Custom	Distributes the settings for a defined device group. Select the check box next to the device type for which you wish to distribute the settings. You can alternatively search for device groups by typing the device group name in the **Search Device Groups** search field. If you wish to create a new device group, click the **Create New Device Group** link at the bottom of the page. See **Device Groups** for more information. As and when you select the device category, you can observe the details (**NAME**, **PHONE#**, and **DEVICE TYPE**) of the list of device users for the selected device category under the **Distribution Summary** section.

8. Click **Done** to push the setting to the selected devices.

10.10.5.10. Windows GPO Settings

Licence: Bridge

Applicable to: Windows Desktop

Setting up Windows GPO Settings

Group Policy Object (GPO) is a collection of settings defining the permissions that the device(s) are allowed or not allowed to do. It is a prerequisite to have a Bridge setup to manage GPO settings. See **Ivanti Bridge** for more details.

Contact the site administrator if the GPO metadata is not uploaded to the database. The GPO configuration is deployed to devices by PowerShell scripts over Bridge. Using the GPO Settings you can configure and push specific settings to device(s).

Procedure

1. In the **Configuration** tab, click **+Add**.
2. Select **Windows GPO Settings** configuration. The **Windows GPO Settings** page is displayed.
3. In the **Name** field, type an appropriate name for the Windows GPO Settings.
4. Click the +**Add Description** link to add a description for the configuration. This field is optional.
5. In the **Configuration Setup** section, click +**Add**. The **Add Windows Group Policy Object(GPO)** window is displayed.
6. Search and select a GPO by clicking the relevant component from the GPO hierarchy tree in the left pane. The GPO hierarchy tree represents the path of the policy settings. You can alternatively, search for a specific GPO settings by typing the name of the GPO settings in the search field.
   After you select a GPO setting, you can view the details of the selected GPO setting in the right pane.
7. In the **Setting Status** field, the following setting options are available:

Option	Description
Not Configured	Removes existing GPO settings.
Enabled	Enables the GPO settings.
Disabled	Disables the GPO settings.

8. In the **Settings Value** field, type an appropriate name to be given to the GPO.
   For adding additional settings value, click on the **+** icon. Some GPO settings may not require any additional Settings Value. Some may require additional data to be specified under the Setting Value in the form of text value. In such settings, select any value from the available drop-down values.

> This field is editable only when the **Enabled** option is selected under **Setting Status**.

9. Click **Save & Close** to save the GPO and close the window. If you wish to add another GPO, click **Save & Add another** to save and keep the GPO window open.
   The GPO setting that is added is displayed in the **Configuration Setup** section.

> You can edit or delete a GPO setting by clicking on the relevant icons in the **Actions** column.

OptionDescriptionEnable this configuration Selecting the check box allows this configuration to the selected devices. Deselecting the check box removes the configuration, if already applied to devices.**All Devices**Distributes the settings to all the devices.**No Devices**Withholds the settings to be distributed to device(s).**Custom**Distributes the settings for a defined device group. Select the check box next to the device type for which you wish to distribute the settings. You can alternatively search for device groups by typing the device group name in the **Search Device Groups** search field. If you wish to create a new device group, click the **Create New Device Group** link at the bottom of the page. See **Device Groups** for more information.

As and when you select the device category, you can observe the details (**name**, **phone#**, and **device type**) of the list of device users for the selected device category under the **Distribution Summary** section.

10. Click **Done** to push the GPO setting to the selected devices.

10.10.5.11. BitLocker Encryption Configuration

Licence: Bridge

Applicable to: Windows Desktop

This section contains the following topics:

- Setting up BitLocker Encryption
- Viewing BitLocker Settings

Setting up BitLocker Encryption

BitLocker Encryption is a feature that enforces encryption on hard drives and removable drives of the devices for data protection. It is a prerequisite to have a Bridge setup to manage BitLocker encryption. See **Bridge** for more details. BitLocker Encryption Configuration helps you in configuring encryption settings to device(s).

Procedure

1. In the **Configuration** tab, click **+Add**.
2. Select **BitLocker Encryption** configuration. The **BitLocker Encryption** page is displayed.
3. In the **Name** field, type an appropriate name for the BitLocker encryption.
4. Click the **+Add Description** link to add a description for the configuration. This field is optional.
5. In the Configuration Setup section, configure the following settings:

Setting	Description
Encryption method and type	Select the type of encryption algorithm based on the key size for encryption. The following options are available: • **AES-CBL 128 bit** • **AES-CBL 256 bit**
Encrypt all hardware drives	Click the toggle button to turn **ON** or **OFF** the setting to encrypt all the hardware drives. If any hardware drive is already encrypted on a device, editing this configuration will not be applied because encryption process is non-reversible through editing.
Select Drive(s)	Select the drive(s) that needs to be encrypted. Example: **C:** Click **+Add** to add more drives. This field will not be displayed if you have turned ON the **Encrypt all hardware drive** setting.
Hardware based encryption for drive types	Trusted Platform Module (TPM) is a chip on computer's motherboard that helps in tamper-resistant encryption. If you are using BitLocker encryption or device encryption on a computer with TPM, part of the key is stored in the TPM. You can choose the following hardware based encryption setting options from the drop-down list: • **Require TPM on startup** • **Require startup PIN with TPM** • **Do not use TPM** TPM option is only applicable to OS drives and for TPM version 1.2 and above. If you apply a hardware based encryption setting to a device, you cannot edit this setting to the device any longer. If a device is already set with a BitLocker configuration, then you cannot push a second bitlocker configuration with a different TPM option.
Select the following configuration checkbox options (optional): • **Deny write access to fixed drives not protected by BitLocker** • **Deny write access to removable drives not protected by BitLocker**	
Pre-encrypted Device Action	Select any of the following options to define the way to handle the drive that is not fully decrypted or already has a key protector. • Stop encryption - Stops the encryption if any of the selected drives are already encrypted. • Decrypt the selected drive which doesn't have recovery password store in Ivanti Neurons for MDM - Select this option to apply to only drives which does not have a recovery password in Ivanti Neurons for MDM.

Setting	Description
Recovery Options	Recovery option is used if a user forgets the password. You can retrieve it from the device details page. you can configure the following recovery options: • **Disable Recovery** • **Use password and store in AD** • **Use password and store in AD and MobileIron**
Restart interval	After the configuration is pushed to the device, it prompts for a restart. The encryption then begins after the restart. To configure the restart interval, from the drop-down list, select the time duration that the device should take to restart. The minimum restart interval is 1 minute and the maximum restart interval is 120 minutes (2 hours).
Restart Message	Type the restart message that should be displayed in the device. If applicable, the startup password or the startup PIN is also displayed to the user. The user can make a note of it to type it when prompted after restart.

6. Click **Next**.
7. Select any of the following options to distribute the settings to device(s).

Setting	Description
Enable this configuration	Selecting the check box allows this configuration to the selected devices. Deselecting the check box removes the configuration, if already applied to devices.
All Devices	Distributes the settings to all the devices.
No Devices	Withholds the settings to be distributed to device(s).
Custom	Distributes the settings for a defined device group. Select the check box next to the device type for which you wish to distribute the settings. You can alternatively search for device groups by typing the device group name in the **Search Device Groups** search field. If you wish to create a new device group, click the **Create New Device Group** link at the bottom of the page. See Device Groups for more information. As and when you select the device category, you can observe the details (**NAME**, **PHONE#**, and **DEVICE TYPE**) of the list of device users for the selected device category under the **Distribution Summary** section.

8. Click **Done** to push the setting to the selected devices.

Viewing BitLocker Settings

You can view the BitLocker Settings that is set for a device in the Device details page (**Devices>Devices>[Device name]**) under the **BitLocker Settings** section. By default, the details are hidden.

You can view the following details by clicking on the view (eye shaped) icon next to each field:

Setting	Description
Recovery Password	When this option is selected, the recovery password is generated by Windows and returned to Ivanti Neurons for MDM after pushing the BitLocker configuration. If the device goes through recovery mode, the user is prompted to type this password. The same recovery password should be used if multiple drives are encrypted. Recover password will only be posted if recovery option **Use password and store in AD and MobileIron** is selected.
PIN	Displays the startup 6-digit PIN. The PIN is displayed only if you have selected the option **Require Startup PIN with TPM** in the BitLocker configuration setup.
Startup Password	The startup password set for the device. The startup password is displayed only if you have selected the option **Do not useTPM** in the BitLocker configuration settings.
TPM version	Displays the configured TPM version.

Some fields might display **N/A** based on the settings configured in the BitLocker configuration setup.

- The status of encryption is displayed under Device encryption status in the Device Details page.
- The same Startup password or PIN will be used for all the drives of a device for which the BitLocker would be applied.
- If you are creating a configuration to encrypt a second drive of a device which already has a drive encrypted and recovery password saved, the earlier password will be overwritten. Hence, it is recommended that the Recovery Password option is used only for one drive in a device.

10.10.6. Enterprise Network Access Configuration

This section contains the following topics:

- AirPlay Configuration
- AirPrint Configuration
- Always-on VPN Configuration
- Default App Runtime Permissions
- Education
- Global Proxy Configuration
- LDAP Configuration
- macOS Server Configuration
- Network Relay Configuration
- Tunnel
- Setting Up AppTunnel
- Per-app VPN Configuration
- Single Sign-On Configuration
- Multi-user Secure Sign-in for iOS
- Android APN Settings Configuration
- VPN Configuration
- VPN On Demand
- Wi-Fi Configuration

10.10.6.1. AirPlay Configuration

Licence: Silver

An Airplay configuration sets up access to alternate devices for media display. The following table lists the Airplay settings:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Allow list	Enter the device ID of each permitted AirPlay destination. If you do not list an ID, then AirPlay destinations are not restricted. **Applicable to**: iOS 7.0+ and macOS 10.10+ (Supervised).
Device Settings	Enter the device ID (macOS) or device name (iOS) and password for each known AirPlay destination.

For more information, see **How to create a configuration**

10.10.6.2. AirPrint Configuration

Licence: Silver

An AirPrint configuration sets up wireless printing. The following table lists the AirPrint settings:

Settings	What to do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
AirPrint Settings	**IP Address:** Enter the IP address of the AirPrint printer. **Resource Path:** Enter the Resource Path associated with the AirPrint printer. This corresponds to the rp parameter of the _ipps.tcp Bonjour record. Examples: • printers/Canon_MG5300_series • printers/Xerox_Phaser_7600 • ipp/print • Epson_IPP_Printer. The resource path is case sensitive. **Port:** Enter the listening port of the AirPrint destination. If this is not specified, AirPrint will use the default port. For details on Apple standard ports, visit https://support.apple.com/en-us/HT202944 **Force TLS**: Allows you to enable the connection to be secured by Transport Layer Security(TLS). By default, it is disabled.

After installation of **AirPrint** configuration on the macOS, the printer details are pushed through the **AirPrint** configuration to the device. Users can view the autopopulated printer details by clicking System Preference > Printers & Scanners > +. In the **Add** screen, user must select **Default** and then select the required print profile. This adds the required printer to the **Printers & Scanners**.

For more information, see **How to create a configuration**

10.10.6.3. Always-on VPN Configuration

Licence:

- **Gold for Android Enterprise**
- **Silver for iOS**

The Always-on VPN configuration ensures that users are automatically connected to VPN (when available) without needing to take any action. This feature requires Android 7.0 + or iOS 8+, as well as a VPN provider that supports the IKEv2 protocol.

Always-on VPN settings for Android

Always-on VPN configuration is sent to Android Enterprise devices with Android 7.0 +. On Managed device with Work Profile (Android 8.0+), the VPN configuration is applied in the Work Profile.

> When a device is deployed in **COSU** mode with **AMA** as Device Enrollment type, and if an app with **Always-on** configuration is pushed to the device, then the **Always-on** configuration will also get pushed to the device.

To enable this configuration, select an app from the App Catalogue or enter a package name.

Always-on VPN settings for iOS

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Use same tunnel configuration for Mobile and Wi-Fi	Select to define one server-identifier pair for VPN connections, regardless of whether the connection is established over a mobile or a Wi-Fi network.
Server	Enter the host name or IP address of the VPN server.
Local Identifier	Identifier of the IKEv2 client in one of the following formats: • FQDN • UserFQDN • Address • ASN1DN
Remote Identifier	Remote identifier in one of the following formats: • FQDN • UserFQDN • Address • ASN1DN
Enable EAP	Select to enable extended authentication.
Machine Authentication	Available only if Enable EAP is not selected. Select one of the following: • Certificate • Shared Secret
EAP Authentication	Available only if Enable EAP is selected. Select one of the following: • Certificate • Username/Password
Shared Secret	Available only if Shared Secret was selected for Machine Authentication. Enter the shared secret for the connection.
Credential	Available only if Certificate was selected for Machine Authentication. Select the certificate to use. this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Account	Available only if Username/Password was selected for EAP Authentication. Enter the account ID for the VPN server.
Password	Available only if Username/Password was selected for EAP Authentication. Enter the password for the VPN server.

Setting	What To Do
Dead Peer Detection Interval	Select one of the following: • None (Disable) • Low (keepalive sent every 1 hour) • Medium (keepalive sent every 30 minutes) • High (keepalive sent every 10 minutes)
Encryption Algorithm	Select one of the following: • DES • 3DES • AES-128 • AES-256 • AES-128-GCM • AES-256-GCM • ChaCha20-Poly1305
Integrity Algorithm	Select one of the following: • SHA1-96 • SHA1-160 • SHA2-256 • SHA2-384 • SHA2-512
Diffie Hellman Group	Select the D-H key exchange group.
Lifetime In Minutes	Enter the SA lifetime (re-key interval) in minutes. Valid values are 10 through 1440.
Voice Mail	Select Allow traffic via tunnel to make voice mail exempt for Always-on VPN. Select Drop traffic to not make it an exemption.
Airprint	Select Allow traffic via tunnel to make Airprint traffic exempt for Always-on VPN. Select Drop traffic to not make it an exemption.
Mobile Services	Select Allow traffic via tunnel to make cellular services traffic exempt for Always-on VPN. Select Drop traffic to not make it an exemption.
Allow traffic from captive websheet outside the VPN tunnel	Select to allow traffic from captive web sheets outside the VPN tunnel.
Allow traffic from all captive networking apps outside the VPN tunnel	Select to allow traffic from all captive networking apps outside the VPN tunnel to perform captive network handling.

Setting	What To Do
Captive Networking App Bundle Identifiers	List the bundle IDs for captive networking apps whose traffic will be allowed outside the VPN tunnel to perform captive network handling. Captive networking apps may require additional entitlements to operate in a captive environment.

For more information, see **How to create a configuration**

10.10.6.4. Default App Runtime Permissions

Applicable to: Apps built targeting Android API 23+ and running Android 6.0+ on Android enterprise devices.

Administrators can set the runtime permission configuration for apps deployed to Android enterprise devices. Apps built targeting API 23 (or higher) and running Android 6.0 or later, are able to prompt users for permissions at runtime. The Default App Runtime Permissions configuration sets the default for these app runtime permissions. Ivanti Neurons for MDM creates this configuration by default. You can edit this default system configuration or create a new configuration based on your requirements.

The app-specific permissions take precedence over the general app permission configuration. In-house apps are subject to the global permissions. Setting the per-app permissions for in-house apps is not supported.

Setting global runtime permissions

Administrators can edit the default app runtime permissions and the distribution of this configuration as follows:

ProcedureProcedure

1. Go to **Configurations**.
2. Perform one of the following actions:
    - To edit the default system configuration, click **Default App Runtime Permissions** and click **Edit**.
    - To add a new configuration, click **Add > Default App Runtime Permissions**.

Enter a name for the configuration.

4. Enter a description.
5. In the Configuration Setup section, set one of the following default runtime permissions:
    - User Prompt (default option)
    - Auto Grant
    - Auto Deny (Use with caution)

Click **Next**.

7. Select the **Enable this configuration option**.

> Note: If you deselect this option, this configuration will not be applied to any devices. It will be removed from all devices if it was previously applied.

8. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom

Click **Done**.

Setting app-specific runtime permissions

Administrators can set the default runtime permissions for an individual application as follows:

Procedure

1. Go to **Apps**.
2. Click the name of the app.
3. Click **App Configurations > Android Enterprise**.
4. Click **Add** or click the configuration name to edit an existing configuration.
5. Set the configuration options such as a name, description, and restrictions.
6. In the Runtime Permissions section, click **Manage Permissions**.
7. Select the permissions in the displayed window and click **Select**.
   Only the dangerous permissions that are applicable to the specific application are listed for selection. The complete list of dangerous permissions (such as read your contacts, find accounts on the device, write call log, and so on) are listed at https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups.
   - The permissions are applied only when the application requests permissions.
   - The permissions are not applied if the users have previously accepted or denied permissions.

In the Runtime Permissions section, select one of the following default runtime permissions:

- Default/Global (default option)
- Auto Grant
- Auto Deny (Use with caution)

In the Distribute this App Config section, select one of the following distribution options:

- Everyone with App
- No One
- Custom

Click **Save**.

10.10.6.5. Education

Licence: Gold

Applicable to: Supervised iOS 9.3+

Configures the Apple Education payload and the Classroom app for Leaders and Members. The following table lists the Education settings:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Configuration Type	Select one of the following types: • Leader • Member
Enable this configuration	• Select this option to apply this configuration to selected devices. • Deselect this option to remove this configuration from all the devices if it was previously applied.
Distribute	Select one of the following distribution options: • All Devices • No Devices • Custom

For more information, see **How to create a configuration**

10.10.6.6. Global Proxy Configuration

Licence: Silver

A global proxy configuration sets up devices to forward HTTP traffic to a proxy server. The following table lists the Global proxy settings:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Type	Select **Manual** or **Auto**. If you select **Manual**, you need the proxy server host name and port, and optionally a username and password into the proxy server. If you select **Auto**, you can enter a proxy autoconfiguration (PAC) URL.
Hostname and Port	If you selected **Manual**, enter the hostname and port number for the proxy server.
User	(Optional) Username for accessing the proxy server.*
Password	(Optional) Password for accessing the proxy server.
PAC URL	(Optional) If you selected **Auto**, you can enter the URL of the PAC file that defines the proxy configuration. If you leave this setting blank, the device uses the web proxy autodiscovery protocol (WPAD) to discover proxies.
Allow direct connection if PAC is unreachable	(iOS 7 and later) Select to allow a direct connection if the device is unable to access the PAC file for any reason.
Allow bypassing proxy to access captive networks	(iOS 7 and later) Select to allow bypassing the proxy to display the login page for a captive network.

> Type $ to see a list of supported **variables**, if available, for this field.

For more information, see **How to create a configuration**

10.10.6.7. Global Proxy Configuration (Android)

> Applicable only for Android devices in Device Owner and AOSP modes.

A global proxy configuration sets up devices to forward HTTP traffic to a proxy server.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Click **Configurations**.
3. Click +Add.
4. Type **Global** in the search field, and then click **Global Proxy**:
   The Global Proxy Configuration details page appears.
5. Enter a name for the configuration in the **Name** box.
6. Optionally, you can add some description about the configuration.
7. From the **Platform** list, select **Android**. The Configuration Setup section is displayed.
8. Under Type, select **Manual** or **Auto**.
   - **Manual**
     - Enter the **Hostname** (Domain name/IP address) and **Port** details.
     - Under **Add Exclusions**, you can add multiple hostnames (domain names/wild cards) that must be under the exclusion list.
   - **Auto**
     - Enter the PAC URL.
9. Click **Next** to configure the distribution settings, and then click **Done**.

10.10.6.8. LDAP Configuration

An LDAP configuration sets up access to a corporate directory. The following table lists the LDAP settings:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Hostname	Enter the host name for the LDAP server.*
User	Enter the username for accessing the LDAP account.*
Password	Enter the password for accessing the LDAP account.
Use SSL	Select if you want to use SSL for the connection to the LDAP server.
Search Settings	Enter at least one entry for the account. Each entry represents a node in the LDAP tree from which to start searching. Click the + button to add a new entry, then edit the entry. An entry consists of the following values: Description: Explains the purpose of the search setting. Scope: **Select Base, Subtree,** or **One Level** to indicate the scope of the search. **Base** indicates just the node level, **Subtree** indicates the node and all children, **One Level** indicates the node and one level of children. Search Base: The conceptual path to the specified note (e.g., ou=people, o=mycorp).
Per-App VPN	**Prerequisite**: Configure Tunnel or any per-app VPN configuration before configuring per-app VPN in LDAP configuration. From the drop-down menu, select the pre-configured per-app VPN configuration. **Applicable to**: iOS 14+
iOS 10+	
Communication Service Rules	Choose a default app to use to make audio calls to contacts within the LDAP system.

> Type $ to see a list of supported **variables**, if available, for this field.

For more information, see **How to create a configuration**

10.10.6.9. macOS Server Configuration

A macOS Server configuration defines a macOS Server account with the configured account types and settings. This configuration allows the user to activate File Sharing on the server.

Applicable to: iOS 10+

Configuring macOS Server

Procedure

1. Go to **Configurations > +Add**.
2. Select the **macOS Server** configuration to display the **Create macOS Server Configuration** page.
3. Enter a name for the configuration.
4. Enter a description.
5. Enter **Host Name** to specify the server address.
6. Enter **User Name** to specify the user's login name.
7. (Optional) Enter **Password** for the user.
8. (Optional) Enter **Description** for the account.
9. (Optional) Under Configured Accounts, enter **Port** number to use when contacting the server for the Documents dictionary account. If no port number is specified, the default port number is used.
10. Click **Next**.
11. Select a distribution for this configuration.

10.10.6.10. Tunnel

Ivanti Tunnel enables VPN capability on iOS, Android, and Windows devices. Ivanti Tunnel interacts with the Unified Endpoint Management (UEM) platform, Standalone Sentry, and Access to secure access to enterprise resources from outside the enterprise network. The enterprise resource can be on premise or in the cloud. The UEM platforms are: Ivanti EPMM and Ivanti Neurons for MDM.

> The Per-App Configuration is deprecated for Android Enterprise devices. You need to use the Managed Configuration for Ivanti Tunnel from the App Catalog.

About Ivanti Tunnel configuration

Configurations for Ivanti Tunnel are created in a Unified Endpoint Management (UEM) platform. Ivanti Tunnel receives the configuration from the UEM client. The client for Ivanti EPMM is Mobile@Work, and the client for Ivanti Neurons for MDM is Go.

Latest documentation

For the latest Tunnel instructions, visit product documentation:

- Tunnel for Android, see **Ivanti Tunnel for Android Guide**
- Tunnel for iOS, see **Ivanti Tunnel for iOS Guide**
- Tunnel for macOS, see **Ivanti Tunnel for macOS Guide**
- Windows Tunnel, see **Ivanti Tunnel for Windows Guide**

> Ivanti Tunnel for Windows is deprecated and not supported with Ivanti Neurons for MDM now.

10.10.6.11. Setting Up AppTunnel

AppTunnel protects app data by providing app-by-app session security between each app container and the corporate network.

This section contains the following topics:

- Setting up Sentry to use AppTunnel with certificates
- Uploading Sentry certificates
- Setting up apps to use AppTunnel
- About the AppTunnel service name

Setting up Sentry to use AppTunnel with certificates

> When you first install Standalone Sentry, a self-signed certificate is also installed. Ivanti strongly recommends that you replace the default certificate with a publicly trusted third-party certificate.

Prerequisites

- AppTunnel depends on the latest supported version of Sentry. Complete the Sentry installation before starting the AppTunnel setup tasks.
- If you intend to use a SCEP identity:
  - Add a local or external certificate authority. A Connector installation is required.
  - Add an App Identity Certificate Configuration. This is the dynamic distribution you will use when you configure AppTunnel.

You can configure ActiveSync and/or AppTunnel using X.509 certificates for authentication to use Sentry servers that are assigned to a profile.

Procedure

1. Go to **Admin > Sentry**.
2. Click **+ Add Sentry Profile**.
3. Click **ActiveSync and/or AppTunnel with certificates**.
4. Click **Next**.
5. Use the guidelines in the following table to complete the **Global Settings** page.

Table: Global Settings for Admin > Sentry	
Setting	**What To Do**
Name	Enter a name that identifies this profile.
Description	Enter a description that clarifies the purpose of this profile.
External Hostname and Port	Enter the hostname and port for the Sentry.
Device Authentication Mode	
Use a single certificate for 2-factor auth	Select to use a single certificate for authentication. If you do not already have a certificate uploaded, you can do so in the area displayed below the selected option.
Select certificate	To upload a group certificate required for device authentication: 1. Click **Add**. The **Add Certificate** window is displayed. 2. Type the name of the certificate in the **Certificate Name** field. 3. Type the password protecting the PKCS12 file. 4. Click **Choose File** to upload the group certificate. Ensure that the file format is in .p7b, .p12, .pfx, .pem, .der, .crt or .cer file.
Enable certificate revocation list (CRL)	Select to validate the certificates presented by the device against the Certificate Revocation List (CRL) published by the CA.
Default Unmanaged Devices Behaviour	
Allow unmanaged devices to receive email and data	Select if you do not want to block data access for devices that are not managed by Ivanti Neurons for MDM.

6. Click **Next**.
7. In the **Sentry Server Configuration** page, configure the following fields:
8. Click **Next**.

Table: Sentry Server Configuration for Admin > Sentry	
Setting	What To Do
Listener protocol	Select any of the following protocol options: • **HTTPS Only** • **HTTP Only** • **HTTPS and HTTP**
Https Port **Http Port** **Sentry TLS Server Certificate/key**	Enter the Https port number. This field will not be displayed if the Listener protocol is selected as HTTP Only. Enter the Http port number. This field will not be displayed if the Listener protocol is selected as HTTPS Only.
Use Sentry's self-signed cert **Add** **Add second certificate**	Select to use a self-signed certificate created by the Ivanti Neurons for MDM service and sent to Sentry as a part of this profile. This certificate is used for communication between the Sentry and mobile devices. To upload your own certificate required for authentication: 1. Click **Add**. The **Add Certificate** window is displayed. You will be able to see this option only when you unselect the **Use Sentry's self-signed cert** option. 2. Type the name of the certificate in the **Certificate Name** field. 3. Type the password protecting the PKCS12 file. 4. Click **Choose File** to upload the certificate. Ensure that the file format is in .p12 file. 5. Click **Add**. All the uploaded TLS Server certificates (including those certificates uploaded from the Sentry main page and from other profiles) are displayed in the Sentry TLS Server Certificate/Key section. To select the TLS certificate required for authentication, click the radio button next to the certificate. Select to enable the second certificate. Once the primary certificate expires, Sentry automatically switches to the reserve certificate without admin intervention. Tunnel already stores both certificates and can match either, ensuring uninterrupted connectivity.
Protocols	Select the required incoming and outgoing protocols.
Cypher suites	Ciphers are used in the SSL-encrypted communication with the Sentry. Strong ciphers are generally preferred. Weak ciphers might be required for older devices. Strong ciphers are selected by default. Select any additional ciphers you want to use. At least one cipher must be selected.

9. Add at least one of the displayed services.
10. Click **Save**.

Once a Sentry is registered, it is displayed in the Sentry page under the Unconfigured Sentry Servers section. To assign a profile for the Sentry, click **Assign** in the **Actions** column.

Uploading Sentry certificates

Ivanti Neurons for MDM uploads TLS Server certificates and Group certificates when creating a Sentry profile. You can also upload these certificates from the **Sentry** page under the **Sentry Certificates** section.

Ivanti Neurons validates Sentry certificates upon upload, returning the following types of information depending on the conditions found in the certificates:

Condition	Information type
The leaf certificate does not contain a chain to any certificate authority or there is no certificate authority in the uploaded file.	Error
There is no root certificate authority available.	Warning
The root certificate authority has not signed off the intermediate certificate authority for the leaf certificate.	Warning

Ivanti Neurons for MDM also validates against the rules in **this article**.

Procedure

1. In the **TLS Server Certificates** section, click **Add**. The **Add Certificate** window is displayed.
2. Type the name of the certificate in the **Certificate Name** field.
3. Type the password protecting the PKCS12 file.
4. Click **Choose File** to upload the group certificate. Ensure that the file format is .p7b, .p12, .pfx, .pem, .der, .crt or .cer.
5. Click **Add**. The uploaded certificate is displayed on the table.
6. To delete the TLS Server certificate, click on the Delete icon in the **Actions** column.

> If the TLS Server certificate is used in any Sentry profile, you will not be able to delete the certificate. An error message will be displayed if the delete action is performed.

Add Group certificates

Procedure

1. In the **Group Certificates** section, click **Add**. The **Add Certificate** window is displayed.
2. Type the name of the certificate in the **Certificate Name** field.
3. Type the password protecting the PKCS12 file.
4. Click **Choose File** to upload the group certificate. Ensure that the file format is .p7b, .p12, .pfx, .pem, .der, .crt or .cer.
5. Click **Add**.

To delete the uploaded Group certificate, click on the Delete icon in the **Actions** column.

Edit the Sentry Root Certificate

As the administrator you have the option to edit the distribution of the Sentry Root Certificate configuration. You can also provide edit permission to the custom space administrator by delegating config to other spaces.

1. Go to **Configurations**.
2. Search for the **Sentry Root Certificate**.
3. Click the edit icon.
4. Select the checkboxes corresponding to the Devices or Device Groups to distribute the certificate. Alternatively, clear the checkboxes corresponding to the Devices or Device Groups.
5. Select one of the following options from the Distribution Summary section as applicable:
    - **Do not apply to other spaces**
    - **Apply to devices in other spaces**
6. (Optional) Click the checkbox **Allow Space Admin to Edit the Distribution**.
7. Click **Save**.
8. A warning message appears. Click **Yes** to confirm.

Setting up apps to use AppTunnel

For the latest Sentry instructions, visit **Product Documentation** and click Sentry. Select the document appropriate to your version of Sentry.

About the AppTunnel service name

An AppTunnel service defines the backend service that an AppConnect app tunnels to.

For the latest instructions, visit **Product Documentation** and select the documents appropriate to your versions of **Sentry** and **AppConnect**.

10.10.6.12. Per-app VPN Configuration

Licence: Silver

Applicable to: iOS, watchOS, visionOS, and tvOS devices

A Per-app VPN configuration defines the settings for virtual private network access for the following specific apps:

- Per-app VPN settings
- Psec (Cisco)
- Cisco AnyConnect
- Juniper SSL
- NetMotion VPN
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- Custom SSL
- Palo Alto Networks GlobalProtect

> Per-App VPN configuration is dependent on App configuration. Per-App VPN configuration is created during App Configuration setup. When Per-App VPN configuration is deleted or undistributed, App configuration malfunctions by disconnecting the App from the network.

Distributing the configuration

Starting from Ivanti Neurons for MDM release 91, global administrators can delegate space administrators to edit the Per-App VPN Configuration for All Devices and for the Custom distribution option. For the Per-App VPN Configuration, you can optionally select the Allow this configuration to be available in all Spaces option.

> The distribution changes are applicable only to the specific space. All other spaces continue to inherit the default space distribution settings.

Specify the configuration settings in the fields using the information from the following tables as applicable and then distribute the configuration:

For more information, see *Distributing the configuration* topic in Working with Configurations.

Per-app VPN settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Connection Type	Select the type of VPN to configure. The remaining settings depend on this selection.
Enable VPN On Demand	Select to use this configuration for domains and host names that establish a VPN on demand.
Enable iOS Rules (Applicable if Enable VPN On Demand is selected)	For iOS and macOS, you can set up: • Network rules that allow or disallow connections to, and allow or ignore, the networks that evaluate as true. • Connection rules allow when needed, or never allow, connections to the networks that evaluate as true. For network rules, you can specify the following types of parameters: • DNS Domain Match • DNS Server Address Match • SSID Match • URL String Probe • Interface Type Match For connection rules, you can specify the following types of parameters: • DNS Domain Match • DNS Server Address Match • SSID Match • URL String Probe • Interface Type Match • Domains • DNS Server • URL Probe
On demand match app enabled	Select to enable the per-app VPN on demand.
Enable 5G network slicing	Select **DNN** (Data Network Name provided by network provider) to tunnel, targeting to the specific cellular slice VPN. Select **App Category** (provided by network provider), to identify the type of cellular slice to be tunneled.
Domains	
Safari Domains (iOS)	An array whose entries must each specify a domain that triggers the VPN connection in Safari. Each entry is in the format www.apple.com.
iOS 14.0+ and macOS 11.0+	

Setting	What To Do
Associated Domains	Specify one or more associated domains. Connections to servers within one of these domains are associated with the per-app VPN.
Excluded Domains	Specify one or more excluded domains. Connections to servers within one of these domains are excluded from the per-app VPN.
iOS 13+ and macOS 10.15+	
Mail Domains	Click **+ Add** to enter one or more domains that will trigger this VPN connection in Mail. Each entry is in the format www.apple.com.
Contacts Domains	Click **+ Add** to enter one or more domains that will trigger this VPN connection in Contacts. Each entry is in the format www.apple.com.
Calendar Domains	Click **+ Add** to enter one or more domains that will trigger this VPN connection in Calendar. Each entry is in the format www.apple.com.
iOS 9 and later	
Provider Type (iOS 9+)	Select one of the following tunnel providers: • app-proxy - tunnels traffic at the app layer. See **Apple documentation** for an overview of App Proxy Provider. • packet-tunnel - tunnels traffic at the IP layer. See **Apple documentation** for an overview of Packet Tunnel Provider.

IPsec (Cisco)

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Machine Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Include User PIN	Select to prompt the user for a PIN.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. **If you select Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. **If you select Automatic,** then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Cisco AnyConnect

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Group	Enter the group to use to authenticate the connection.
User Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select Manual, then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select Automatic, then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Juniper SSL

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Realm	Enter the authentication realm to be used for authenticating the connection.
Role	Enter the authentication role to be used for authenticating the connection.
User Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select Manual, then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select Automatic, then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

NetMotion VPN

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
User Authentication	**Certificate** is the user authentication method to use. The following field is available: **Credential**: Select the identity certificate to use. User provided certificates are supported only for iOS devices.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy. Select the following options: • Enable VPN On Demand - Add domains or host names that establish a VPN on demand. • Enable iOS rules. • On demand match app enabled.
Safari Domains	Click **+ Add** to add Safari domains.
Provider Type (iOS 9.0+)	**packet-tunnel** is selected as the tunnel provider type by default. See Apple documentation for an overview of Packet Tunnel Provider.

F5 SSL

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
User Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select Manual, then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select Automatic, then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

SonicWALL Mobile Connect

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Login Group or Domain	Enter the login group or domain to be used for authenticating the connection.
User Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select Manual, then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select Automatic, then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Aruba VIA

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
User Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select Manual, then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select Automatic, then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Custom SSL

Setting	What To Do
Identifier	Enter the identifier for this custom SSL VPN in reverse DNS format (such as com.mycompany.myserver).
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Custom Data	Enter the key-value pairs that define the custom data for this VPN.
User Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select Manual, then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select Automatic, then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.
(iOS 9.0+) Include ProviderType in main and sub VPN dictionary	Choose to include the provider type while generating a plist (predefined configuration file).
Provide bundle identifier	Enter the bundle identifier for the VPN provider. You can maintain multiple apps Config for the same app with different Provider Bundle Identifiers.

Palo Alto Networks GlobalProtect

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.
Custom Data	Enter the key-value pairs that define the custom data for this VPN.
User Authentication	Certificate is the user authentication method. Select an identity certificate to use in the **Credential** field.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select Manual, then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select Automatic, then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

> Type $ to see a list of supported variables, if available, for this field.

Related topics:

How to create a configuration

10.10.6.13. Single Sign-On Configuration

Ivanti Neurons for MDM enables Extensible Single Sign-On (SSO) with the Extensible SSO and Extensible SSO Kerberos configurations. The implementation requires an app extension, such as Microsoft Authenticator, from the identity provider. With an Extensible SSO implementation, users need to only authenticate once when accessing enterprise resources. Users are not prompted to authenticate for subsequent logins. For information about setup information for the intended identity provider, see **Configure Identity Provider**.

This section contains the following topics:

- **Single sign-on account settings**
- **Extensible single sign-on account settings**
- **Extensible single sign-on Kerberos account settings**

Single sign-on account settings

Applicable to:

- iOS 7.0 through the most recently released version as supported by Ivanti Neurons for MDM.
- visionOS 1.1 through the most recently released version as supported by by Ivanti Neurons for MDM.

Use the following settings to configure Kerberos-based enterprise SSO for any managed app and Apple Safari browser on iOS devices.

> This configuration requires Tunnel and Sentry. For more information, see "Setting up single sign-on with Kerberos" in the *Tunnel for iOS Guide*.

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
User name	Enter the Kerberos principal name.
Kerberos realm name	Enter the Kerberos realm name.
Certificate	**For iOS 8 with Gold license:** Select the certificate to use to renew the Kerberos credential.
URL prefixes matches	List of URLs prefixes that must be matched in order to use this account for Kerberos authentication over HTTP.
Allowlist Applications for SSO	Add apps from the App Catalog to Allowlist them for SSO. For example, enter "Safari" to add Apple Safari. If no apps are Allowlisted for SSO using a configuration of this type, all apps that support iOS SSO can utilise SSO, including built-in iOS apps.

Extensible single sign-on account settings

Applicable to:

- iOS 13.0 through the most recently released version as supported by Ivanti Neurons for MDM.
- macOS 10.15 through the most recently released version as supported by Ivanti Neurons for MDM.
- visionOS 1.1 through the most recently released version as supported by by Ivanti Neurons for MDM.

Use the following settings to configure the SSO extension profile with the generic extension type to enable SSO for native apps and websites with various authentication methods.

> Extensible SSO does not work when the configuration is pushed in the user channel for macOS 10.15.x devices.

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Choose SSO type	Select one of the following SSO types: • **Credentials** ◦ Enter one or more **Host** names or domain names that can be authenticated through the app extension. Host or domain names are matched case-insensitively, and all the host/domain names of all installed Extensible SSO payloads must be unique. Hosts that begin with a "." are wildcard suffixes and will match all subdomains, otherwise the host must be an exact match. ◦ Enter the **Realm** name. This value should be properly capitalised. • **Redirect** ◦ Enter one or more **URL** prefixes of identity providers where the app extension performs SSO. The URLs must begin with http:// or https://, the scheme and host name are matched case-insensitively, query parameters and URL fragments are not allowed, and the URLs of all installed Extensible SSO payloads must be unique.
Extension Identifier	Enter the bundle identifier of the app extension that performs SSO for the specified URLs.
Team Identifier Custom Data Authentication Method (Applicable only for macOS 13+)	The team identifier of the app extension. This key is required on macOS and ignored elsewhere. Enter one or more custom data as key-value pairs. • Password • User Secure Enclave Key
Registration Token Screen Locked Behavior (applicable for iOS 15.0+ and macOS 12.0+) Denied Bundle Identifiers (applicable for iOS 15.0+	Enter the token. This field is enabled once you select one of the Authentication Methods. Select one of the following options: • **Cancel**: The system cancels authentication requests when the screen is locked. • **Do Not Handle**: The authentication request continues without SSO when the screen is locked. Add multiple bundle identifiers of apps that do not use the SSO provided by this extension. For example, *com.company.appname.www*.

Setting	Description
and macOS 12.0+)	

Applicable to: macOS 14.0 through the most recently released version as supported by Ivanti Neurons for MDM.

Setting	Description
Account Display Name	Enter a name for the account that displays in notifications and authentication requests.
Additional Groups	Enter the name of the groups that will not have administrator access.
Administrator Groups	Enter the name of the group that has administrator access.
Authentication Method	Select one of the authentication methods from the drop-down list: • Password • User Secure Enclave Key • Smart Card
Authorisation Groups	Enter the authorisation right for a group name.
Enable Authorisation	Select the checkbox to enable authorisation prompts for administrator groups, authorisation groups, or additional groups.
Enable Create User At Login	Select the checkbox to enable the creation of new users during login by using a password or smart card as an authentication method.
Login Frequency	The duration, in seconds, until the system requires a full login instead of a refresh. The default value is 64,800 (18 hours). The minimum value is 3600 (1 hour).
New User Authorisation Mode	Select one of the authorisation modes for a new user from the drop-down list: • Standard: The account is for a standard user. • Admin: The system adds the account to the local administrator's group. • Groups: The system automatically groups the new user under the administrator group, authorisation group, or additional group.
Token To User Mapping	Enter the account name and the full name of the new users to map them for authorisation.
User Authorisation Mode	Select one of the authorisation modes for a user from the drop-down list: • Standard: The account is for a standard user. • Admin: The system adds the account to the local administrator's group. • Groups: The system automatically groups the new user under the administrator group, authorisation group, or additional group.
Use Shared Device Keys	Select the check box to enable the same login and encryption keys for all users.

Applicable to: macOS 15.4 through the most recently released version as supported by Ivanti Neurons for MDM.

Setting	Description
Allow Device Identifier Attestation	Select the checkbox to include the device's UDID and serial number in Platform SSO attestations, allowing backend tracking of registered devices.

Applicable to: macOS 14.0 through the most recently released version as supported by Ivanti Neurons for MDM.

To view the Extensible single sign-on account settings, select the drop-down option as **Password** in the **Authentication Method** field.

Setting	Description
FileVault Policy	Enable the policy to view the following settings: • Attempt Authentication • Require Authentication Select the **Require Authentication** checkbox to enable additional configuration settings. • Allow Offline Grace Period • Allow Authentication Grace Period
Login Policy	Enable the policy to view the following settings: • Attempt Authentication • Require Authentication Select the **Require Authentication** checkbox to enable additional configuration settings. • Allow Offline Grace Period • Allow Authentication Grace Period
Unlock Policy	Enable the policy to view the following settings: • Attempt Authentication • Require Authentication Select the **Require Authentication** checkbox to enable additional configuration settings. • Allow Offline Grace Period • Allow Authentication Grace Period • Allow TouchID Or Watch For Unlock
Authentication Grace Period	Enter the amount of time after selecting one of the policies to use unregistered local accounts. If you select the **Allow Authentication Grace Period** checkbox in one of the policies, it becomes a mandatory field.
Offline Grace Period	Enter the amount of time after selecting one of the policies to use an offline local account password after a successful Platform SSO login. If you select the **Allow Offline Grace Period** checkbox in one of the policies, it becomes a mandatory field.
Non Platform SSO Accounts	Select **+ Add** to enter the list of usernames that are not subjected to FileVault, Login, or Unlock policies.

Extensible single sign-on Kerberos account settings

Applicable to:

- iOS 13.0 through the most recently released version as supported by Ivanti Neurons for MDM.
- macOS 10.15 through the most recently released version as supported by Ivanti Neurons for MDM.
- visionOS 1.1 through the most recently released version as supported by by Ivanti Neurons for MDM.

Use the following settings to configure an app extension that performs SSO with Kerberos extension.

> Extensible SSO Kerberos does not work when the configuration is pushed in the user channel for macOS 10.15.x devices.

Setting	Description
Basic Settings	
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
User name	Enter the Kerberos principal name.
Realm	Enter the Kerberos realm name.
Certificate	Select the certificate to use to renew the Kerberos credential.
URL Prefixes	List of URLs prefixes that must be matched in order to use this account for Kerberos authentication over HTTP.
Advanced Settings	
Allow Automatic Login	If false, passwords are not allowed to be saved to the keychain. By default, this option is enabled.
Delay User Setup	If true, doesn't prompt the user to setup the Kerberos extension until either the administrator enables it with the app-sso tool or a Kerberos challenge is received. This option is applicable to macOS 11 through the latest version as supported by Ivanti Neurons for MDM.
Require User Presence	If true, requires the user to provide Touch ID, Face ID, or their passcode to access the keychain entry.
Monitor Credential Cache	If false, the credential is requested on the next matching Kerberos challenge or network state change. If the credential is expired or missing, a new one will be created. This option is applicable to macOS 11 through the latest version as supported by Ivanti Neurons for MDM. By default, this option is enabled.
Cache Name	Enter the Generic Security Service (GSS) name of the Kerberos cache to use. This option is now deprecated.
Domain Realm Mapping	Enter the name of the realm as the key. The value is an array of DNS suffixes that map to the realm. Click **+ Add** to add one or more key-value pairs.
Default Realm	This property specifies the default realm if there is more than one Kerberos extension configuration.
Use Site Auto Discovery	If false, the Kerberos extension doesn't automatically use LDAP and DNS to determine its AD site name. By default, this option is enabled.
Site Code	Enter the name of the Active Directory site the Kerberos extension should use.
Replication Time	Enter the time, in seconds, required to replicate changes in the Active Directory domain. The Kerberos extension will use this when checking password age after a change. This option is applicable to macOS 11 through the latest version as supported by Ivanti Neurons for MDM. This option is now deprecated.
Credential Bundle ID ACL	Click **+ Add** to add a list of bundle IDs allowed to access the Ticket Granting Ticket (TGT) for authentication.

Setting	Description
Include Managed Apps in Bundle ID ACL	If true, the Kerberos extension will allow only managed apps to access and use the credential. This is in addition to the Credential Bundle ID ACL, if it is specified. This option is applicable to iOS 14 or supported newer versions of Ivanti Neurons for MDM.
Include Kerberos Apps in Bundled ID ACL	If true, the Kerberos extension allows the standard Kerberos utilities including Ticket Viewer and klist to access the use the credential. Available in macOS 12 and later.
Custom Username Label	Enter the custom user name label used in the Kerberos extension instead of "Username." For example, "Company ID." This option is applicable to macOS 11 through the latest version as supported by Ivanti Neurons for MDM.
Help Text	Enter the text to be displayed to the user at the bottom of the Kerberos login window. It can be used to display help information or disclaimer text. This option is applicable to iOS 14 and macOS 11 through the latest version as supported by Ivanti Neurons for MDM.
Credential Use Mode	This setting affects how the Kerberos Extension credential is used by other processes. Use one of the following: • Always (default) - The extension credential will always be used if the service principal name (SPN) matches the Kerberos Extension Hosts array. The credential will not be used if the calling app is not in credentialBundleIDACL. • When Not Specified - The credential will only be used when another credential has not been specified by the caller and the SPN matches the Kerberos Extensions Hosts array. The credential will not be used if the calling app is not in credentialBundleIDACL. • Kerberos Default - The default Kerberos processes for selecting credentials is used which normally uses the default Kerberos credential. This is the same as turning off this capability. (Optional) Select **Require TLS for LDAP**.
Preferred Key Distribution Centres	Add Preferred Key Distribution Centres. Click **+Add** to add a preferred KDC.
	Allow Platform SSO Auth Fallback - If True and if Use Platform SSO TGT is true, allows the user to manually sign in. Available in macOS 13 and later
	Perform Kerberos Only - If True, the Kerberos extension handles Kerberos requests only. Available in macOS 13 and later.
	Use Platform SSO TGT - If True, this configuration uses a TGT from Platform SSO instead of requesting a new one. Available in macOS 13 and later.
Configure Switch to Password mode	If True, allows the user to switch the user interface to Password mode. Available in macOS 15 and later.

Setting	Description
Configure Switch to Smart Card mode	If True, allows the user to switch the user interface to SmartCard mode. Available in macOS 15 and later.
Configure Start in Smart Card mode	If True, the user interface starts in SmartCard mode. Available in macOS 15 and later.
Identity Issuer Auto Select Filter	Filters the list of available Smart Cards. Available in macOS 15 and later.
Password Settings	
Allow Password Change	If false, disables password changes. This option is applicable to macOS 10.15 through the latest version as supported by Ivanti Neurons for MDM. By default, this option is enabled.
Password Change URL	Enter the URL to be launched in the user's default web browser when they initiate a password change. This option is applicable to macOS 10.15 through the latest version as supported by Ivanti Neurons for MDM.
Allow Password Complexity	If true, passwords must meet Active Directory's definition of "complex." This option is applicable to macOS 10.15 through the latest version as supported by Ivanti Neurons for MDM.
Minimum Password Length	Enter the minimum length (in characters) of passwords on the domain. This option is applicable to macOS 10.15 through the latest version as supported by Ivanti Neurons for MDM.
Password Expiry Notification	Enter the number of days prior to password expiration when a notification of password expiration will be sent to the user. This option is applicable to macOS 10.15 through the latest version as supported by Ivanti Neurons for MDM. The default value is 15 days.
Password Expiry Override	Enter the number of days that passwords can be used on this domain. For most domains, this can be calculated automatically. This option is applicable to macOS 10.15 through the latest version as supported by Ivanti Neurons for MDM. (This option is now deprecated)
Password Required Text	Enter the text version of the domain's password requirements. Only for use if pwReqComplexity or pwReqLength aren't specified. This option is applicable to macOS 10.15 through the latest version as supported by Ivanti Neurons for MDM.
Password History Count	Enter the number of prior passwords that cannot be re-used on this domain. This option is applicable to macOS 10.15 through the latest version as supported by Ivanti Neurons for MDM.

Setting	Description
Password Minimum Age	Enter the minimum age (in days) of passwords before they can be changed on this domain. This option is applicable to macOS 10.15 through the latest version as supported by Ivanti Neurons for MDM.
Allow Syncing Local Password	If false, disables password sync. This will not work if the user is logged in with a mobile account. This option is applicable to macOS 10.15 through the latest version as supported by Ivanti Neurons for MDM.
Password Requirement RTF data	RTF file formatted version of the domain's password requirements. Available in macOS 15 and later. Only for use if pwReqComplexity or pwReqLength are not specified.

For more information, see **How to create a configuration**

10.10.6.14. Network Relay Configuration

Ivanti Neurons for MDM enables Network Relay configuration for the payload you use for configuring relay settings for a device or an application without the need for VPN or tunnels to access private resources.

Applicable to

- iOS 17.0 through the most recently released version as supported by Ivanti Neurons for MDM.
- macOS 14 through the most recently released version as supported by by Ivanti Neurons for MDM.
- visionOS 1.1 through the most recently released version as supported by by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Network Relay** configuration.
3. Configure the **Network Relay** settings as per the following table:

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
HTTP/3 Relay URL	Specify a URL value to use as the HTTP field value for this configuration. Include either HTTP/2 Relay URL or HTTP/3 Relay URL, or it can include both.
HTTP/2 Relay URL	Specify a URL value to use as the HTTP field value for this configuration. Include either HTTP/2 Relay URL or HTTP/3 Relay URL, or it can include both.
Additional HTTP Header Fields	Specify the HTTP header field value for the corresponding header field name.
Certificate	Select one of the identity certificates that you have created from the drop-down list.
Raw Public Key	Specify the raw public keys to authenticate the server during a network connection.
+ Add	Select **+ Add** to add multiple network relay configuration.
Match Domains	Specify the list of domains to determine which connection to route through the servers in Relays.
Exclude Domains	Specify the list of domains to determine which connection to avoid through the servers in Relays.
Match FQDNs(supported on iOS 18.4+ and macOS 15.4+ devices)	Specify the list of Fully Qualified Domain Names (FQDNs), also known as hostnames, which should be routed through the servers contained in Relays. Any connection that matches this exact FQDN or hostname will use the relays. If no FQDNs and no 'MatchDomains' are listed, traffic to all domains, except those matching an excluded domain or excluded FQDN, will be routed to the relay servers.
Exclude FQDNs (supported on iOS 18.4+ and macOS 15.4+ devices)	Specify the list of Fully Qualified Domain Names (FQDNs), also known as hostnames, which should **NOT** be routed through the servers contained in Relays. Any connection that matches the FQDN exactly will not use the relay server. When 'MatchDomains' are also specified, any FQDN listed here in 'ExcludedFQDNs' should be a sub-domain of at least one MatchDomain. Otherwise, it will not have any effect.

4. Click **Next** to configure the distribution settings.
5. Select one of the distribution options to set up the **Network Relay** configuration. For more information about configuring distribution options, see **Working with Configurations**.
6. Click **Done**.

10.10.6.15. Multi-user Secure Sign-in for iOS

The Multi-user web clip allows users to log in and log out of iOS devices that are registered on Ivanti Neurons for MDM. When a user logs in for the first time, the profiles, apps, and configurations that are associated with that user are pushed to the device. When they have finished their work, they can open the web clip and select the "log out" function, which assigns the device to the Nobody User and removes the profiles, apps, and configurations associated to the user that had originally logged in, as long as the configurations and apps are not being distributed to the Nobody User. After a log out, the web clip resets so that the next user can log in and receive their custom configurations, apps and policies. Device supervision is not required to use the multi-user secure sign-in feature. See the Support knowledge base article, **Ivanti Neurons for MDM: Multi-user secure sign-in for iOS**, for a deeper look at the multi-user sign-in feature.

Applicable to: iOS devices (Not applicable to User Enrolled devices)

This section contains the following topics:

- Supported credentials
- Understanding the Nobody User
- Signing in to a device
- Signing out of a device

Supported credentials

User name and password must be used to log into the Multi-user secure web clip. PIN based registration is not supported with the Multi-user secure web clip.

Procedure

1. Go to **Configurations**.
2. Click **Multi-user Secure Sign-in for iOS**. You may need to use the search functionality to find it if there are multiple pages of configurations. This configuration is not accessed by selecting **+Add**.
3. Click **Edit Distribution**, or the associated icon to distribute the web clip to the appropriate Device Group.

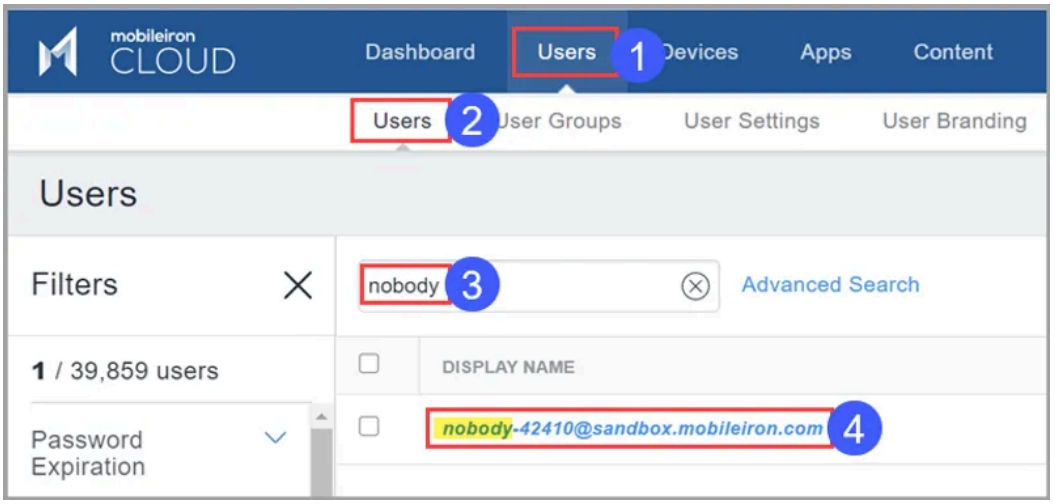
If you want to distribute it to a User Group, you can create a dynamic Device Group that is tied to a User Group.
4. Select one of the following distribution options, remembering that you must always distribute the web clip to the Nobody User, or the Device Group with which Nobody User is associated. This does not happen by default, so make sure that you are distributing it to the Nobody User.
    - All Devices
    - No Devices (default)
    - Custom

Click **Save**.

Understanding the *Nobody* User

When a device has been logged out through the web clip, it remains enrolled with Ivanti Neurons for MDM to a special user called the Nobody User. If you want to remove apps and configurations from the device when a User logs out, you must make certain that those apps and configurations are not distributed to the Nobody User. If you want certain configurations, such as Wi-Fi, to remain on the

device when a user signs out of the Secure Sign-In web clip, then you must ensure that those configurations are also distributed to the Nobody User.



This means that you must pay attention to User Groups and Device Groups to which you distribute apps and configurations. If you are distributing an app to Everyone, and you want it to be removed when a user signs out of the device, then the best practice is to create a User Group that does not include the Nobody User. Custom attributes make it much easier to create a group of users that are "multiusers," and another User group that consists only of the Nobody User. You can create a User Attribute from Admin > System > Attributes called "Multiuser owner" and then assign the value of "Yes" or "True" to the Nobody User. You can then create User Groups and Device Groups based on the value of the attribute.

Signing in to a device

A user can sign in to an iOS device and assign the device to self. After logging in, all relevant applications, policies, configurations, and certificates are pushed to the device.

> For security reasons, iDP user must re-authenticate every time they log in, even if they are already signed on to the device.

Signing out of a device

A user can sign out of his/her iOS device after usage. After signing out, the applications, policies, configurations, and certificates are removed from the device, leaving the device in the state that it was in prior to the user sign-in. Then, the device is available for sign-in by another user.

> Logout from all the Microsoft Apps before logging out from Multi-user Web Clip.

For more information, see **Multi User Sign-In Branding**

10.10.6.16. Android APN Settings Configuration

The Android APN Settings Configurations allow you to set the Access Point Name (APN) settings required on devices on a public network. This configuration is applicable to Android Enterprise Work Managed Devices and Managed Devices with Work Profile on Company Owned Device (on Android version 9.0 or supported newer versions).

Procedure

1. Go to **Configuration > +Add**.
2. Select **Android APN Settings** configuration.
3. Enter a name for the configuration.
4. Enter a description.
5. In the Configuration Setup section, configure the following options:
6. Click **Next**.

Setting	Description
Entry Name	Type the name of the Access Point settings.
Access Point Name	Type the name of access point.
Access Point Type	Select the type of access point from the following options: • **Default** • **DUN** • **IMS** • **Emergency** • MMS • **HIPRI** • **CBS** • **MCX** • **SUPL** • **FOTA** • **IA**
MVNO Type	Select the type of Mobile Virtual network Operator from the following options: • **None** • **SPN** • **IMSI** • **GID** • **ICCID**
Bearer	Select the type of bearer service used for data transmission from the following options: • **1xRTT** • **CDMA** • **EDGE** • **EHRPO** • **EVDO** • **EVDO A** • **EVDO B** • **GPRS** • **GSM** • **HSDPA** • **HASP** • **HSPAP** • **HSUPA** • **IDEN**

Setting	Description
	• **IWLAN** • **LTE** • **NR** • **TD_SCDMA** • **UMTS**
APN Protocol	Select the APN protocol required for the APN. The following are the available options: • **None** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP** (Point-to-Point Protocol) • **UNSTRUCTURED**
APN Roaming Protocol	Select the APN roaming protocol required for the APN. The following are the available options: • **None** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP** (Point-to-Point Protocol) • **UNSTRUCTURED**
Enable/Disable APN	Turn ON the APN configuration.
Carrier ID	Enter the numeric value of the Carrier ID.
Authentication Type	Select the type of authentication protocol from the following options: • **None** • **PAP** (Password Authentication Protocol) • **CHAP**(Challenge-Handshake Authentication Protocol) • **PAP or CHAP**
Username	Enter the login username.
Password	Enter the login password.
Confirm Password	Re-enter the password for confirmation.
Port Number	Enter the port number (numeric value between 1 to 65535).
Proxy Address	Type the proxy address.

Setting	Description
Mobile Country Code	Enter the mobile country code.
Mobile Network Code	Enter the mobile network code.
MMS Proxy Address	Type the MMS proxy address.
MMS Port Number	Enter the MMS port number (numeric value between 1 to 65535).
MMS Server Address (mmsc)	Type the MMS server address.

7. Select one of the following distribution options:
8. Click **Done**.

- **All Devices**
- No Devices (default)
- **Custom**

> You cannot add another APN configuration with same values for the following fields If there is an existing APN configuration with these values for the device:

- Mobile Country Code
- Mobile Network Code
- Access Point Name
- Proxy Address
- Port Number
- MMS Proxy Address
- MMS Port Number
- MMS Server Address
- Enable/Disable APN
- MVNO Type
- APN Protocol
- APN Roaming Protocol

The Android APN Settings Configuration overrides the APN settings if already configured in the device manually or by the network operator.

10.10.6.17. VPN Configuration

Applicable to:

- Android (Deprecated for Android Enterprise devices. You need to use the Managed Configuration for specific VPN from the App Catalog.)
- Windows
- iOS
- macOS
- tvOS
- visionOS

A VPN configuration defines the settings for virtual private network access.

> Delegation with custom distribution option is available for this configuration. For more information, see *Distributing the configuration* topic in **Working with Configurations**.

Procedure

1. Go to **Configurations** > **+Add**.
2. Select the **VPN** configuration.
3. Enter a **Name** for the configuration.
4. Enter a description.
5. Configure the VPN settings as per the following descriptions.
6. (iOS 9.0+ Only) In the Match Domains section, click **+ Add** to enter one or more matching domains (example: company.com). Proxy connection is used when the domain is one of these specified domains.
7. Click **Next**.
8. (macOS only) In the Distribute page, select one of the following distribution options:
    - Device channel - the configuration is effective for all users on a device, which is the typical option.
    - User channel - the configuration is effective only for the currently registered user on a device.
9. Select the remaining distribution options for this configuration.
10. Click **Done**.

VPN settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Connection Type	Select the type of VPN to configure. The remaining settings depend on this selection.

The protocols and their settings are listed as follows:

- **L2TP** (Not supported on Ivanti Go)
- **PPTP** (Not supported on Ivanti Go)
- **IPsec (Cisco)** (Not supported on Ivanti Go)
- **Cisco AnyConnect** (Supported on Ivanti Go)
- **Juniper SSL** (Not supported on Ivanti Go)
- **NetMotion VPN** (Not supported on Ivanti Go)
- Pulse Secure (Supported on Ivanti Go)
- **F5 SSL** (Not supported on Ivanti Go)
- **SonicWALL Mobile Connect** (Not supported on Ivanti Go)
- **Aruba VIA** (Not supported on Ivanti Go)
- **Custom SSL** (Not supported on Ivanti Go)
- **Palo Alto Networks GlobalProtect** (Supported on Ivanti Go)
- **KEv2 (Windows Only)** (Not supported on Ivanti Go)
- **IKEv2** (Not supported on Ivanti Go)

L2TP

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
User Authentication	Select the authentication method to use: **Password** or **RSA SecurID**.
Shared Secret	Enter the shared secret passcode if one is necessary for initiating the connection.
Send All Traffic	Select this option to use this connection for all network traffic. This option helps protect data from being compromised, particularly on public networks.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

PPTP

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
User Authentication	Select the authentication method to use: **Password** or **RSA SecurID**.
Encryption Level	Select a level of data encryption for the connection: **None, Automatic**, or **Maximum (128-bit)**.
Send All Traffic	Select this option to use this connection for all network traffic. This option helps protect data from being compromised, particularly on public networks.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

IPsec (Cisco)

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Machine Authentication	Select the authentication method to use: **Shared Secret/Group Name** or **Certificate**.
Group Name	Shared Secret/Group Name authentication. Specify the name of the group to use. If Hybrid Authentication is used, the string must end with â€œ[hybrid]â€.
Shared Secret	Shared Secret/Group Name authentication. Enter the shared secret passcode.
Use Hybrid Authentication	Shared Secret/Group Name authentication. Select to specify hybrid authentication, i.e., server provides a certificate and the client provides a pre-shared key.
Prompt for Password	Shared Secret/Group Name authentication. Specify whether the user should be prompted for a password when connecting.
Credential	*Certificate authentication* Select the identity certificate to use.
Include User PIN	*Certificate authentication* Select to prompt the user for a PIN.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional fields are available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Cisco AnyConnect

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Group	Enter the group to use to authenticate the connection.
User Authentication	Select the user authentication method to use: **Password** or **Certificate**. If you select **Certificate**, then the following field is available: **Credential**: Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Juniper SSL

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Realm	Enter the authentication realm to be used for authenticating the connection.
Role	Enter the authentication role to be used for authenticating the connection.
User Authentication	Select the user authentication method to use: **Password** or **Certificate**. If you select **Certificate**, then the following field is available: **Credential**: Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

NetMotion VPN

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
User Authentication	Select the user authentication method to use: **Password** or **Certificate**. If you select **Certificate**, then the following field is available: **Credential**: Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

F5 SSL

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.
User Authentication	Enter the user authentication method to use: **Password** or **Certificate**. If you select **Certificate**, then the following field is available: **Credential**: Select the identity certificate to use.
Proxy Setup	Select Manual or Automatic to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

SonicWALL Mobile Connect

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Login Group or Domain	Enter the login group or domain to be used for authenticating the connection.
User Authentication	Select the user authentication method to use: **Password** or **Certificate**. If you select Certificate, then the following field is available: **Credential**: Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Aruba VIA

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
User Authentication	Select the user authentication method to use: **Password** or **Certificate**. If you select **Certificate**, then the following field is available: **Credential**: Select the identity certificate to use.
Proxy Setup	Select Manual or Automatic to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Custom SSL

Setting	What To Do
Identifier	Enter the identifier for this custom SSL VPN in reverse DNS format (such as com.mycompany.myserver).
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Custom Data	Enter the key-value pairs that define the custom data for this VPN.
User Authentication	Select the user authentication method to use: **Password** or **Certificate**. If you select Certificate, then the following field is available: **Credential**: Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Palo Alto Networks GlobalProtect

Not applicable to Android devices.

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.
Custom Data	Enter the key-value pairs that define the custom data for this VPN.
User Authentication	Select the user authentication method to use: **Password** or **Certificate**. If you select Certificate, then the following field is available: **Credential**: Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

IKEv2 (Windows Only)

Setting	What To Do
Server	Enter the host name or IP address of the VPN server.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

IKEv2

Setting	What To Do
Server	Enter the host name or IP address of the VPN server.
Local Identifier	Identifier of the IKEv2 client in one of the following formats: • FQDN • UserFQDN • Address • ASN1DN
Remote Identifier	Remote identifier in one of the following formats: • FQDN • UserFQDN • Address • ASN1DN
Machine Authentication	Available only if **Enable EAP** is not selected. Select one of the following: • Certificate • Shared Secret
EAP Authentication	Available only if **Enable EAP** is selected. Select one of the following: • Certificate • Username/Password
Shared Secret	Available only if Shared Secret was selected for Machine Authentication. Enter the shared secret for the connection.
Credential	Available only if Certificate was selected for Machine Authentication. Select the certificate to use. this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Enable EAP	Select to enable extended authentication.
Account	Available only if Username/Password was selected for EAP Authentication. Enter the account ID for the VPN server.
Password	Available only if Username/Password was selected for EAP Authentication. Enter the password for the VPN server.
Dead Peer Detection Interval	Select one of the following options: • None (Disable) • Low (keepalive sent every 1 hour) • Medium (keepalive sent every 30 minutes) • High (keepalive sent every 10 minutes)

Setting	What To Do
Server Certificate Issuer Common Name	(Optional) - Common name of a server certificate issuer, causes the IKE server to send a certificate request based on the certificate issuer to the server.
Server Certificate Common Name	(Optional) - Common name of a server certificate used to validate the certificate sent by the IKEv2 server.
Use IP4 and IP6 subnets attributes	(Optional) Select to use IP4 and IP6 subnets attributes.
Enable IKEv2 Mobility and Multihoming Protocol (MOBIKE)	(Optional) The default setting is 0. MOBIKE (The ability to support multi-homed mobile devices when connected to both Wi-Fi and mobile links with multiple IP addresses) is enabled. It is enabled by default. Set to 1 to disable MOBIKE.
Enable Perfect Forward Secrecy (PFS)	(Optional) When set to 1 it enables PFS for IKEv2 connections. The default setting is 0.
Enable IKEv2 redirect	(Optional) The default setting is 0. The IKEv2 connection is redirected if a redirect request is received from the server. It is enabled by default. Set to 1 to disable IKEv2 redirect.
Enable NAT keepalive	Enables the Network Address Translation keepalive that prevents the deletion of NAT entries in the absence of any traffic when there is NAT between IKE peers.
NAT keepalive interval	If NAT keepalive is enabled, this is the time in seconds that keepalive packets will be sent for the device.
PPK	Enter the Post-quantum Pre-shared key (PPK) with VPN servers that support RFC 8784. If this key is present, the PPK Identifier must be present.
PPK Identifier	Enter the PPK identifier.
PPK Mandatory	Select one of the following drop-down options: • **Mandate**: The VPN connection will successfully establish if the server supports RFC 8784 or if it accepts the PPK identifier specified in the PPK Identifier. • **Non-Mandate**: The VPN connection will fail to establish if the server does not support RFC 8784 or it does not accept the PPK identifier specified in the PPK Identifier.
Encryption Algorithm	Select one of the following options: • **DES** • **3DES** • **AES-128** • **AES-256** (Default) • **AES-128 GCM** • **AES-256 GCM**
Integrity Algorithm	Select one of the following options: • **SHA2-256** (Default) • **SHA2-384**

Setting	What To Do
	• **SHA2-512**
Diffie Hellman Group	Select one of the following options: • **1** • **2** (Default) • **5** • **14** • **15** • **16** • **17** • **18**
Lifetime In Minutes	Enter the SA lifetime (re-key interval) in minutes. Valid values are 10 through 1440.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

*Type $ to see a list of supported **variables**, if available, for this field.

For more information, see **How to create a configuration**

10.10.6.18. VPN On Demand

Applicable to: iOS devices

A VPN On Demand configuration sets up access to a VPN server based on domains, host names, etc.

VPN On Demand settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Connection Type Enable VPN On Demand	Select the type of VPN to configure. The remaining settings depend on this selection. Select to use this configuration for domains and host names that establish a VPN on demand.
Enable iOS Rules (Applicable if Enable VPN On Demand is selected)	For iOS and macOS, you can set up: • Network rules that allow or disallow connections to, and allow or ignore, the networks that evaluate as true. • Connection rules allow when needed, or never allow, connections to the networks that evaluate as true. For network rules, you can specify the following types of parameters: • DNS Domain Match • DNS Server Address Match • SSID Match • URL String Probe • Interface Type Match For connection rules, you can specify the following types of parameters: • DNS Domain Match • DNS Server Address Match • SSID Match • URL String Probe • Interface Type Match • Domain Name • DNS Server • URL Probe
Provider Type (iOS 9+)	Select one of the following tunnel providers: • app-proxy - tunnels traffic at the app layer. See **Apple documentation** for an overview of App Proxy Provider. • packet-tunnel - tunnels traffic at the IP layer. See **Apple documentation** for an overview of Packet Tunnel Provider.
EnforceRoutes	When enabled, the VPN's non-default routes overrides any locally defined routes. • If IncludeAllNetworks is enabled, the system disregards the EnforceRoutes setting • Available in iOS 14.2 and later.

Setting	What To Do
ExcludeLocalNetworks	When enabled along with IncludeAllNetworks, all local network traffic routes outside of the VPN.
IncludeAllNetworks	When enabled, it routes all traffic through the VPN.

The protocols and their settings are listed as follows:

- IPsec (Cisco)
- Cisco AnyConnect
- Juniper SSL
- NetMotion VPN
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- Custom SSL
- Palo Alto Networks GlobalProtect

IPsec (Cisco)

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Machine Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Include User PIN	Select to prompt the user for a PIN.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. **If you select Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. **If you select Automatic,** then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Cisco AnyConnect

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Group	Enter the group to use to authenticate the connection.
User Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. **If you select Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. **If you select Automatic,** then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Juniper SSL

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Realm	Enter the authentication realm to be used for authenticating the connection.
Role	Enter the authentication role to be used for authenticating the connection.
User Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. **If you select Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. **If you select Automatic,** then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

NetMotion VPN

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
User Authentication	Certificate is the user authentication method. **Credential**: Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. If you select **Automatic,** then the following additional field is available: **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

F5 SSL

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
User Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. **If you select Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. **If you select Automatic,** then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

SonicWALL Mobile Connect

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Login Group or Domain	Enter the login group or domain to be used for authenticating the connection.
User Authentication Credential Proxy Setup	Only Certificate authentication is supported. Select the identity certificate to use. Select **Manual** or **Automatic** to configure a proxy. **If you select Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. **If you select Automatic,** then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Aruba VIA

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
User Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. **If you select Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. **If you select Automatic,** then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Custom SSL

Setting	What To Do
Identifier	Enter the identifier for this custom SSL VPN in reverse DNS format (such as com.mycompany.myserver).
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.*
Custom Data	Enter the key-value pairs that define the custom data for this VPN.
User Authentication	Only Certificate authentication is supported.
Credential	Select the identity certificate to use.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. **If you select Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. **If you select Automatic,** then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Palo Alto Networks GlobalProtect

Setting	What To Do
Server	Enter the IP address or host name for the VPN server.
Account	Enter the user account to be used for authenticating the connection.
Custom Data	Enter the key-value pairs that define the custom data for this VPN.
User Authentication	Certificate is the user authentication method. Select an identity certificate to use in the **Credential** field.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. **If you select Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. **If you select Automatic,** then the following additional fields are available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Type $ to see a list of supported variables, if available, for this field.

For more information, see How to create a configuration

10.10.6.19. Wi-Fi Configuration

Applicable to:

- Android
- Windows
- iOS
- macOS
- watchOS
- visionOS
- tvOS

This section contains the following topics:

Wi-Fi settings

- WEP, WPA/WPA2/WPA3, Any (Personal) settings
- WEP Enterprise, WPA/WPA2/WPA3 Enterprise, Any (Enterprise) settings
- iOS, macOS, and visionOS

Wi-Fi settings

A Wi-Fi configuration sets up access to a wireless network.

> A user can modify some of the Wi-Fi settings on the device. However, the MDM server may or may not receive information about the changes, which is based on the device OS. Therefore, the configurations will not be re-pushed automatically to the device to override the configuration on the device with the configuration on the server.

> Delegation with custom distribution option is available for this configuration. For more information, see *Distributing the configuration* topic in **Working with Configurations**.

> Some specific versions of Android devices may require administrators to enter domain and additional information to connect to a TLS, TTLS, PEAP, etc. (WPA2) networks. It is recommended to ensure changes to Wi-Fi configuration are made on selected devices before making these changes on a larger set of devices.

> Android 14.x devices registered on any Ivanti Neurons for MDM version earlier than 94 will have the Config status in “Pending Install” state. When you upgrade the Ivanti Neurons for MDM to 94 without editing the Wi-Fi configuration, the configuration status remains in "Pending Install" state. You must enable the Domain field for EAP_PEAP and update the Domain and Certs in configuration to update the status to “Installed” state.

Procedure

1. Go to **Configurations** > **+Add**.
2. Select the **Wi-Fi** configuration.
3. Enter a **Name** for the configuration.

4. Enter a description.
5. Configure the Wi-Fi settings as per the following descriptions.
6. Click **Next**.
7. (macOS only) In the Distribute page, select one of the following distribution options:
    - Device channel - the configuration is effective for all users on a device, which is the typical option.
    - User channel - the configuration is effective only for the currently registered user on a device.
8. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
9. Click **Done**.

The following table lists the Wi-Fi Settings:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description Service Set Identifier (SSID)	Enter a description that clarifies the purpose of this configuration. Enter the name of the wireless network these settings apply to. This field is case sensitive.
Auto Join Hidden Network	Select if devices should automatically join the corresponding Wi-Fi network. If this option is not selected, device users must tap the network name on the device to join the network. Select this option if the network access is not broadcast.
Disable Captive Network Detection (iOS 10+)	Administrators can enable or disable Wi-Fi Captive bypass mode. When Apple detects the presence of a captive portal, it opens a login screen to request access. You can disable the detection of captive portals, requiring the user to manually launch a web browser which triggers the portal login of the captive network. This new setting is useful when an ISE captive portal prevents the login screen from popping up, leading users to believe that their unconnected devices are actually connected to the Internet.
Proxy Setup	Select **Manual** or **Automatic** to configure a proxy. If you select **Manual,** then the following additional fields are available: • **Server and Port**: Enter the network address and port number for the proxy server.* • **Authentication**: Enter a valid user name if one is required for connecting to the proxy.* • **Password**: Enter a valid password if one is required for connecting to the proxy. To remove the added host name, click on the 'minus' icon. If you select **Automatic,** then the following additional field is available: • **Proxy Server URL**: Enter the fully-qualified URL for the proxy.

Setting	What To Do
Security Type	Select the security method required for accessing the network: • Any (Personal) • Any (Enterprise) • WEP • WEP Enterprise • WPA • WPA Enterprise • WPA2 • WPA2 Enterprise • WPA3 • WPA3 Enterprise WPA3/WPA3 Enterprise is applicable for iOS 13+. Windows supports WPA, WPA Enterprise, WPA2, and WPA2 Enterprise.

WEP, WPA/WPA2/WPA3, Any (Personal) settings

Setting	What To Do
Password	(Optional) Enter the password for accessing this network. Otherwise, the device user will be prompted for any password required for accessing the network.

WEP Enterprise, WPA/WPA2/WPA3 Enterprise, Any (Enterprise) settings

Setting	What To Do
Protocols	
Accepted EAP Types	Select the EAP types that can be used for accessing this network: • TLS • TTLS - In the Inner Identity field, select one of the authentication protocols such as OS Default, PAP, CHAP, MSCHAP, MSCHAPv2, and EAP • PEAP • LEAP (Not supported for AMAPI-enrolled devices) • EAP-SIM • EAP-AKA • EAP-FAST (Not supported for AMAPI-enrolled devices)
EAP-FAST	Select the EAP-FAST option that define authentication methods: • **Use PAC:** Select to use a proxy auto-config (PAC).. • **Provision PAC:** Select to allow a PAC to be provisioned. Otherwise, only a PAC already provisioned on the device can be used. This option is available only if you selected Use PAC. • **Provision PAC Anonymously:** Select to allow a PAC to be provisioned without authenticating the server. This option is available only if you selected Provision PAC.
Authentication	
Username	Specify the username required for network access. If you leave this blank, the device user will be prompted for it.
Use Per-Connection Password	Select to prompt the device user for a password for each connection. When the device rejoins the same network, the device user will be prompted to reauthenticate to join the network. This option is not supported for AMAPI-enrolled devices.
Password	(Optional) Enter the password for accessing this network. Otherwise, the device user will be prompted for any password required for accessing the network.
Identity Certificate	(Optional) Select the certificate to use for the identity credential. The **Identity Certificate** configuration defines each available identity certificate.
Authentication Certificate (Available for Windows devices only)	Select one of the following three Certificate Stores to pick a certificate and connect to a Wi-Fi network: • Machine or User: If this option is selected and the user is not logged in, the Authentication certificate will be picked from the machine store. If the user is logged in, the specific certificate will be picked from the user store. • Machine: If this option is selected, the Authentication certificate will be picked from the machine store. • User: If this option is selected, the Authentication certificate will be picked from the user store. By default, the User option is selected.

Setting	What To Do
Outer Identity Domain **Trust**	(Optional) For TLS, TTLS, PEAP, and EAP-FAST, select to allow device users to hide their identity. The user's actual name appears only inside the encrypted tunnel. This option can increase security because an attacker cannot see the authenticating user's name in the clear. Supported when EAP type is TLS and TTLS.
Trusted Certificates (Not supported for AMAPI-enrolled devices) Trusted Server Certificate Names	Select the checkboxes to select multiple certificates from the list. Click **+ Add** to enter the names of one or more trusted server certificates. (Optional) Select **Allow Trust Exceptions** to allow trust decisions to be made by the user in a dialog window.

iOS, macOS, and visionOS

Setting	What To Do
All Versions	
Network Type	Select if this network should be treated as: • standard • legacy hotspot • Passpoint
Proxy PAC fallback allowed	(Optional) Allows the device to connect directly to the destination if the PAC file is unreachable.
Setup Modes (Optional)	An array of strings that contain the type of connection mode to be attached. • System: WiFi is connected before the user logs in to the device. • Login Window: The WiFi is available after the user logs in to the device. Currently, setup modes work only when both System and Login Window modes are enabled.
Passpoint Settings	The settings in this section appear if you selected Passpoint for the Network Type.
Domain Name	Enter the domain name to be used for Passpoint negotiation.
Connect to roaming partner Passpoint networks	(Optional) Select to allow connections to roaming service providers.
Roaming Consortium Organisation Identifiers	(Optional) Enter the identifiers assigned by IEEE to the entities supported by this Wi-Fi profile.
Network Access Identifier Realm Names	(Optional) Enter the Network Access Identifier Realm names to be used for Passpoint negotiation.
MCC and MNC pair	(Optional) Enter the Mobile Country Code (MCC)/Mobile Network Code (MNC) pairs to be used for Passpoint negotiation. Each string must contain exactly six digits.
Displayed operator name	(Optional) Enter the network operator name to display.
Cisco QoS fast lane	The settings in this section apply to Cisco fast lane configuration. Settings include Allowlisting apps for L2 and L3 marking, and whether to Allowlist the audio and video traffic of built-in audio/video services such as FaceTime and Wi-Fi Calling.

Setting	What To Do
Restrict QoS marking	If unselected, then all apps will use L2 and L3 marking when the network supports Cisco QoS Fast Lane. If selected, then use the **Choose Apps** settings that appear to add the apps that you would like included for L2 and L3 marking. All apps not selected will not use L2 and L3 markings.
Enable QoS marking	Disables L3 marking and uses only L2 marking for traffic sent to the Wi-Fi network. When unselected, the system treats Wi-Fi as not associated with a Cisco QoS Fast Lane network.
Allowlist Apple audio/video calling	Specifies whether to Allowlist the audio and video traffic of built-in audio/video services such as FaceTime and Wi-Fi Calling.
Choose Apps	Use to add the apps that you would like included for L2 and L3 marking. All apps not selected will not use L2 and L3 marking.
iOS 10+	
Cisco QoS fast lane	The settings in this section apply to Cisco fast lane configuration. Settings include Allowlisting apps for L2 and L3 marking, and whether to Allowlist the audio and video traffic of built-in audio/video services such as FaceTime and Wi-Fi Calling.
Restrict QoS marking	If unselected, then all apps will use L2 and L3 marking when the network supports Cisco QoS Fast Lane. If selected, then use the **Choose Apps** settings that appear to add the apps that you would like included for L2 and L3 marking. All apps not selected will not use L2 and L3 markings.
Enable QoS marking	Disables L3 marking and uses only L2 marking for traffic sent to the Wi-Fi network. When unselected, the system treats Wi-Fi as not associated with a Cisco QoS Fast Lane network.
Allowlist Apple audio/video calling	Specifies whether to Allowlist the audio and video traffic of built-in audio/video services such as FaceTime and Wi-Fi Calling.
Choose Apps	Use to add the apps that you would like included for L2 and L3 marking. All apps not selected will not use L2 and L3 marking.
iOS 10.3+ Supervised	
Enable Wi-Fi Allowlisting	Determines which Wi-Fi networks the device is allowed to connect to. If multiple Wi-Fi configurations exist, the most restrictive will be applied.
iOS 14.0+ and macOS 15.0+	
Disable MAC Address Randomisation	In iOS 14.0+ and macOS 15.0+, Apple changed the default behavior for a device reporting its Wi-Fi MAC address to report a random address for new connections instead of the device's actual Wi-Fi MAC address. As a result, this feature may cause unexpected behaviour for enterprises using captive portals or filtering of MAC addresses. Administrators can **Disable MAC Address Randomisation** for a Wi-Fi network by editing the associated Wi-Fi configuration and turning on this option (by default, false). This will cause the Wi-Fi configuration to be re-

Setting	What To Do
	pushed to all devices. This option displays a privacy warning in the device Settings indicating that the network has reduced privacy protections. A device user can still manually turn this on or off through their device's settings.
Android 11+ MAC Address Randomisation	• Disabled: Wi-Fi is connected before the user logs in to the device. • Enabled - Auto: The Wi-Fi is available after the user logs in to the device. • Enabled - Non-persistent • Enabled - Persistent

> Type $ to see a list of supported **variables**, if available, for this field.

For more information, see **How to create a configuration**.

10.10.7. Mobile Network Configuration

This section contains the following topics:

- APN Configuration
- Mobile
- Cellular Private Network Configuration.htmCellular Private Network Configuration
- iOS Telecom Presets Configuration
- eSIM Configuration

10.10.7.1. APN Configuration

An APN configuration sets up the cellular Access Point Name for the device. For iOS 7, use the **Cellular configuration**, instead.

APN settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Access Point Name	Enter the name for the corresponding access point. The name is generally defined by the operator providing service.
Access Point User Name	Enter a user name authorised for this access point.*
Access Point Password	Enter the password corresponding to the user name entered.
Proxy Server and Port	Enter the IP address or URL and the port number of the APN proxy.
EnableXLAT464	Select the check box to enable the Access Point Name (APN). This option provides IPv4 services over an IPv6-only network.

Type $ to see a list of supported **variables**, if available, for this field.

For more information, see **How to create a configuration**.

10.10.7.2. Mobile

Applicable to: iOS 7.0+ and watchOS 10.0+

This section contains the following topics:

- Mobile settings for Default APN
- Mobile settings for Data APNs
- Controlling mobile network access while roaming
- Controlling mobile access

A cellular configuration sets up the cellular profile for a device. Configure the cellular network settings on devices running with iOS 7.0+ or watchOS 10.0+. Some companies have contracts with their mobile operators that grant them access to a unique Access Point Name (APN) for remote network access or for special billing plans. Consult your cellular operator for configuration parameters.

- No more than one mobile profile can be installed at any time.
- A cellular profile cannot be installed if an APN profile is already installed.

You can configure cellular settings for the following APN types from the **Configured APN Types** dropdown box:

- Default & Data APNs
- Default APNs
- Data APNs

For all the configurations, enter a name that identifies the configuration and an optional description.

Mobile settings for Default APN

Default APN Settings	What To Do
APN Name	Enter the name for the corresponding access point. The name is generally defined by the operator providing service.
APN Authentication Type	(Optional) Select one of the following: • CHAP (challenge handshake authentication protocol) • PAP (password authentication protocol)
User Name	(Optional) Enter a user name to be used for authentication.
Password	(Optional) Enter a password to be used for authentication.

Mobile settings for Data APNs

Data APN Settings	What To Do
APN Name	Enter the name for the corresponding access point. The name is generally defined by the operator providing service.
APN Authentication Type	(Optional) Select one of the following: • CHAP (challenge handshake authentication protocol) • PAP (password authentication protocol)
User Name	(Optional) Enter a user name to be used for authentication.
Password	(Optional) Enter a password to be used for authentication.
Proxy Server	Specify the proxy server.
Proxy Server Port	Specify the proxy server port.
10.3+	
Allowed Protocol Mask	Select IPv4, IPv6, or Both.
Allowed Protocol Mask in Domestic Roaming	Select IPv4, IPv6, or Both.
Allowed Protocol Mask in Roaming	Select IPv4, IPv6, or Both.

Controlling mobile access while roaming

You can limit the access of some or all of the managed apps to mobile data while the device is in a roaming state.

Procedure

1. Go to the **Configurations** tab in the Ivanti Neurons for MDM main navigation menu.
2. Click **+Add**
3. Enter **Network** in the search field, and then click the **Network Usage** configuration.
4. Select the **Disallow for all managed apps** checkbox to block managed apps from accessing cellular data when roaming or at all times.
5. Leave the checkbox deselected to be able to specify the managed apps by name or bundle ID to block from receiving mobile data.
6. Use the pulldown menus in the Apps field to search for an app by name or by bundle ID.

Controlling mobile access

You can limit the access of some or all of the managed apps to mobile data at any time. The apps can still be used on a limited basis, but they will not have access to mobile data.

Procedure

1. Go to the **Configurations** tab in the Ivanti Neurons for MDM main navigation menu.
2. Click **+Add**

3. Enter **Network** in the search field, and then click the **Network Usage** configuration.
4. Select the **Disallow for all managed apps** checkbox to block managed apps from accessing cellular data at any time.
5. Optionally, leave the checkbox unselected to specify the managed apps to block from receiving mobile data.
6. Use the pulldown menus in the Apps field to search for an app by name or by bundle ID.

For more information, see **How to create a configuration**.

10.10.7.3. Cellular Private Network Configuration

Ivanti Neurons for MDM enables the Cellular Private Network configuration payload to provide device information on private network deployments, including geographical location, preference over Wi-Fi, and network deployment type.

Applicable to

iOS 17.0 through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Cellular Private Network** configuration.
3. Configure the **Cellular Private Network** settings as per the following table:

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Cellular Data Preferred	Select the check box to enable and use cellular data over Wi-Fi.
NR Standalone	Select the check box if the cellular data network has NR 5G Standalone.
Data Set Name	Specify the Data Set Name that identifies with this configuration.
Version Number	Specify the Version Number for the data set to track the system updates.
GeoFences	Specify the Latitude, Longitude, and Radius for each Geo ID to deploy a private network in a geographical location. You can create a list of up to one thousand geofences for private networks.

4. Click **Next** to configure the distribution settings.
5. Select one of the distribution options to set up the **Cellular Private Network** configuration. For more information about configuring distribution options, see **Working with Configurations**.
6. Click **Done**.

10.10.7.4. iOS Telecom Presets Configuration

An iOS Telecom Presets configuration sets default values for roaming restrictions and hotspot restrictions.

iOS Telecom Presets settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Allow devices to use voice service while roaming	Select to enable voice roaming. Availability of voice roaming depends on the operator.
Allow devices to use data service while roaming	Select to enable data roaming. Enabling data roaming also enables voice roaming on the device.
Allow users to enable personal hotspot	Select to enable the personal hotspot feature. Availability of this feature depends on the operator.

For more information, see **How to create a configuration**.

10.10.7.5. Enhanced 5G Network Slicing Configuration

Ivanti neurons for MDM provides enhanced 5G network slicing configuration to set up 5G network slices for android which allows mobile network operators to allocate dedicated 5G network segments, or "slices," for grouping different applications with similar needs like low latency or high bandwidth in a specific slice for better optimisation of network resources. This enables MDM administrators and network providers to manage slices directly for better app performance.

Key Features

1. **Dedicated Network**: Instead of all applications sharing the single network slice, network slicing enables different apps to use their own network slice tailored to their specific requirements

2. **Customisation**: The admin can configure how apps are assigned to specific network slices according to their individual requirements—for instance, ensuring low latency for real-time communication apps or high bandwidth for streaming services like YouTube. A slice intended for high-performance gaming may prioritise low latency, whereas one for media streaming would be optimised for high bandwidth.

3. **Partner Involvement**: This feature often requires collaboration with network providers who define these slices and inform MDM admins about list of slices and its significance.

Creating an Enhanced 5G Network Slicing Configuration

Procedure

1. **Add Configuration**

- Navigate to **Configurations >> +Add**. The **Add Configuration** page is displayed.
- Enter **Enhanced Network Slicing** in the search bar to configure Enhanced Network Slicing. The **Create Enhanced Network Slicing Configuration** page is displayed.
- Click **+Add Description** to enter a description of the configuration.

2. **Configure Application**

- Under **Configuration Setup >> App Catalog**, enter the desired application name.
- Click **Add Manually** if the application is not available in the Play Store or App Store.
- Enter **Package ID** and select appropriate **Network Slice** from the drop down menu.
- Select the desired slice from **Select Slice** drop-down.
- Click **Add**. The application will now appear in the **Configure Network Slices** under the selected network slice.
- To remove an application, click **Remove** under the **Configure Network Slice** section.

3. **Distribute Configuration**

- Click **Next**, select or deselect the "**Enable this configuration**" check box, choose a distribution option (All Devices, No Devices, or Custom),
- Click **Done** to complete the configuration.

Enhanced Network Slicing Configuration for Lockdown & Kiosk

Creating a Enhanced 5G Network Slicing Configuration allows you to configure devices to operate in a restricted manner, ensuring that users only have access to specified applications and settings.

Under the following lockdowns, there is an "**Enable 5G network slicing**" checkbox:

- **Work Profile**- On employee-owned devices with a Work Profile configured using Android Enterprise version 12.0, the "Enable 5G Network Slicing" checkbox can be found under
  Configuration Setup > Work Profile Lockdown Settings.
- **Managed Device with work profile / Work Profile on Company owned devices** - Under Managed Device with work profile/ Work Profile on Company owned devices with Android 12.0 versions we have "Enable 5G network slicking" checkbox.

This is a legacy setting that permits the devices to use of 5G network slicing. Its correlation to the new Enhanced 5G Network Slicing configuration is as follows:

If any of the above lockdowns are applied to a device and the *Enable 5G network slicing* option is **not** selected, the *Enhanced 5G Network Slicing* configuration will fail with an error.

Examples

- **Case 1**: If device lockdown is not distributed and enhanced network slicing configuration is distributed, the enhanced configuration will activate.
- **Case 2**: If device lockdown is distributed but the 5G check box is not selected (false), the enhanced 5G network configuration will error out.
- **Case 3**: If enhanced network slicing is distributed first, followed by the device lockdown with the check box enabled, enhanced network slicing configuration will keep working. Otherwise, it will error out.

Configuration Details:

- If the device lockdown is distributed and the enhanced network slicing configuration is pushed /distributed, users must ensure that the Enable 5G network slicing check box is enabled to prevent errors.
- If the check box is not enabled and the configuration is sent, it will error out on the device.

10.10.7.6. eSIM Configuration

eSIM configuration configures mobile network on the devices with the RefreshCellularPlans Command. Administrators must obtain the eSIM carrier URL before mapping the mobile network to the device.

Applicable to: Android 15+, iOS, iPadOS, and Windows 11

Procedure for Android 15+ devices

1. Go to **Configurations** > **+Add**.
2. Type eSIM in the search field, and then click the **eSIM** configuration.
3. Enter a Name and Description of the configuration.
4. From the **Platform** list, select **Android**.
5. Under the **Configuration Setup** section, enter the **Carrier URL**.
6. **Auto Enable** - Select this option to download eSIM profile and enable on the device automatically. If this option is not selected, the eSIM profile will be downloaded, but will not enabled on the device automatically.

> This option is NOT available for devices in Work Profile mode.

7. Select and distribute the configuration using one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
8. Click **Done**.

EID for Android 13+ devices

The **Request EID** option is now available in the Device Details and Devices list page. This option is supported for eSIM-compatible devices on Work Profile, Work Managed Device, and Work Profile on Company Owned Device modes only. If a device is registered, the EID will be automatically picked for the registered device and displayed under the Device Details page. If not, this field will be enabled and you can request for the EID by clicking **Request EID**. You can also export EID using the **Export to CSV** option from the Devices list page.

> In the **Device Details** page, the **Request EID** option is available for Android 13+ devices with Ivanti Go R122 or later versions.

Preserve eSIM Data Plan (applicable for iOS 11+ Android 15.0+): When you attempt to wipe a device enrolled with an eSIM configuration, the **Wipe Device** action provides an additional option to preserve the data plan. If you select **Preserve eSIM Data Plan (applicable for iOS 11+ and Android 15.0+)** and then click **Wipe**, the existing eSIM data plan is retained while all other data on the device is erased. You can access this option from the **Device Details** page or by selecting the device, opening the **Actions** menu, and clicking **Wipe**.

Procedure for iOS and iPadOS devices

1. Go to **Configurations** > **+Add**.
2. Type eSIM in the search field, and then click the eSIM configuration.
3. Enter a Name and Description of the configuration.

4. Select **iOS/iPadOS**.
5. Type the Carrier URL.
6. Click **Next**.
7. Select Enable this configuration option.
8. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
9. Click Done.

Procedure for Windows 11 devices

1. Go to **Configurations** > **+Add**.
2. Type eSIM in the search field, and then click the eSIM configuration.
3. Enter a Name and Description of the configuration.
4. In the Choose OS section, click on **Windows**.
5. In the Configuration Setup section, type the Carrier URL in Server Name textbox (in FQDN format).
    - Is Discovery Server - Select to mark the server as discoverable.
    - Auto Enable - Select to enable the profile on the device once downloaded.
6. Click **Next**.
7. Select Enable this configuration option.
8. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
9. Click **Done**.

Reset eSIM to factory state (only for Windows 11 devices)

This option is available under the Device Details section of all devices. Clicking this option deletes all the eSIM profiles downloaded on the device.

Important Notes - Applicable only for Windows eSIM Configuration

- When a device is registered, the **Device Details** section now displays whether the device supports eSIM or not under **ESIM Capable**. For eSIM-capable devices, the respective eSIM identifier details are also shown under **ESIM Identifiers**.
- When an Ivanti Neurons for MDM enrolled device is wiped & re-enrolled; the old record of this device (with the status as Wiped) should be deleted from the Devices page to avoid provisioning issues with the eSIM configuration, onto this re-enrolled device.
- Repushing the same configuration to a device which already has downloaded the profiles, fails to download the profiles again. If the admin wants the device to download the profiles afresh, reset the eSIM module to factory state first and then push / repush of the eSIM configuration is recommended.

- When an eSIM configuration is provisioned successfully on a device; before retiring the device, admin should perform the eSIM wipe action, to ensure the downloaded eSIM profiles are erased from the device.
- Removal of the eSIM configuration will just delete the configuration from the device. If any eSIM profiles were discovered, downloaded, and activated on the device, such eSIM profiles will remain active until an eSIM wipe is performed.
- Performing an eSIM wipe action removes all the downloaded eSIM profiles from the device. However, the eSIM configuration which is in Installed state remains intact on the device. Admin needs to undistribute the eSIM configuration to remove the configuration from the device.

10.10.8. Other Configuration

This section contains the following topics:

- Associated Domains Configuration
- Android File Transfer Configuration
- Apple TV Configuration
- AirPlay Configuration
- AirPlay Mirroring
- Browser Settings
- Configuring Single App Mode for iOS
- Configuring an iOS MDM Profile
- Configuring a macOS MDM Profile
- Content Caching
- Creating an Android Shortcut
- Device Name Settings
- Ethernet Configuration (macOS)
- EMA Server Integration Configuration
- Device Wallpaper Configuration
- Lock Screen Message Configuration
- Create Screen Saver Configuration
- Configure User's Screen Saver
- macOS System Extension configuration
- MAM-Only
- Managed Google Play Configuration
- Migration Assistant Settings
- App Notifications Configuration
- Printer Settings
- Remove Bloatware Configuration
- Samsung Phone Restrictions Configuration
- Single App Mode Configuration
- Start menu and Taskbar
- System Update Configuration
- Windows Update Management
- Windows app scheduling
- Windows BIOS Configuration
- Windows BitLocker
- Windows Kiosk Configuration

- Windows Licence Configuration
- Software update recommendation cadence configuration

10.10.8.1. Associated Domains Configuration

Licence: Gold

The Associated Domains configuration is a dictionary that maps apps to their associated domains. Associated domains can be used with features such as Extensible AppSSO, universal links, and Password AutoFill.

The Associated Domains settings are as follows:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Application Identifier	(Required) The app identifier to associate the domains with.
Associated Domains	(Required) The domains to be associated with the app. Each string is in the form of "service:domain". Domains should be fully qualified hostnames, like www.example.com.
Enable Direct Download	If true, data for this domain should be downloaded directly instead of through a CDN. The entitlement value for this domain must be set to service:domain?mode=managed or this value will be ignored. Available in macOS 11 and later. **Default**: false

10.10.8.2. Android File Transfer Configuration

As part of Android 11, Google made significant changes in storage access on a device from apps, which also impacted how enterprises manage to send files to specific apps on these devices. With these changes in mind, many large enterprises face challenges in distributing files to devices and apps as devices are upgrading to Android 11 and beyond. Any approach that is dependent on specific APIs from hardware vendors limits enterprises in having the same approach across different devices from different manufacturers and OS versions.

Ivanti developed a file transfer solution that is agnostic for the Android version and hardware vendor. This solution relies on Android's standard *Content-Provider* capability. *Content-Provider* allows Ivanti's Go app to generate a unique on-device location for each file pushed via UEM.

The File Transfer Configuration is available for Android devices in Fully Managed device mode. Using this configuration, the administrator can provide an option to transfer files on the device to be shared between different allowed apps present on the same device. Other apps can use the files for whatever reason needed. An example use case is initializing app configuration using JavaScript or displaying corporate information using PDFs or videos. Every file uploaded into Ivanti's File Transfer configurations is downloaded by Ivanti Go when it receives the corresponding config and associated file. The file is securely stored within Ivanti Go.

Other apps cannot access this file arbitrarily.

Every downloaded file inside the app sandbox is referenced by a unique location, also referred to as *ContentURI* or *URI*. Custom Attributes are used to hold the ContentURI value on the server for every file on a device and can help administrators determine a file's availability on device, form dynamic device groups, and are required to communicate ContentURI to target app using managed app configuration, etc.

> For non-Ivanti apps, administrators should check with third-party app developers on their support for this approach which is commonly referred to as "Consuming FileProvider based ContentURI."

Prerequisites:

- Add a new device-based custom attribute to be used for File Transfer operation. For every File transfer configuration, a unique custom attribute should be created. Each custom device attribute can only store the contentURI (location of file) from device for one file per config.

Procedure

1. Go to **Configurations** > **Add Configuration** > **File Transfer**. The **Create File Transfer Configuration** page opens.
2. Enter a name for the configuration in the **Name** box.
3. Enter a **Description** of the configuration.
4. **Configuration Setup**
   In the **File to Transfer** section, select the files to be transferred using the Drag and drop option or browsing through the **Choose File** option. By default, the maximum limit of file size is 50 MB.
5. Select one or more of the following **Download to device** options (optional):
   - **Allow download over a metered network** - Select to continue downloading the file even on a metered network
   - **Require charging** - Select to make sure that the device is charging during the file transfer process
   - **Require device idle** - Select to keep the device idle during the file transfer process
6. Use one of the following two options to share a file with other apps

- **Transfer using Android Managed App Config**- Use this option only if the target app can consume Content URI using its Managed App Config.
- **Transfer using On-device Intent** - Intents are app-specific. To share a file using this option, see the target app's documentation and provide information in the intents section below. Intents allow Ivanti Go app to broadcast a message on the device once the file is available to be shared with the apps.

Transfer using Android Managed App Config

Procedure

1. In the **Choose an existing device based custom attribute to share this file with other apps** field, enter an existing attribute name, for example, **Custom-Filename**. For more information, see Assigning Custom Attributes to Devices.
2. The custom attribute name should be new, unique attribute solely used for this file transfer operation. Each custom device attribute can only store the contentURI (location of file) from device for one file per config.
   Provide access to the following apps and / or package names: You can select app names from the App Names selector and add Package Names.

> These will be the only authorised packages allowed to access the file.

- **App Names** - You can select app names from the App Names selector.
- **Package Names** - You can enter the Bundle IDs in this area, for example,Separate multiple package names with semicolons(;).

```bash
com.mobileiron.filetransfer.android3.
```

Click **Save**. The new File Transfer configuration appears on the Configurations page.

Configuring the target app

Procedure

1. Go to **Apps > App Catalog**.
2. Select the target app that will receive the file.
3. Navigate to **App Configurations > Managed Configurations for Android**.
4. Create a new configuration or use an existing configuration.
5. An app may have a setting such as "Manifest Info" or other properties where the administrator can define the substitution variable and communicate the location of the file to the target app. For Ivanti Velocity app as an example, in the App Configuration dialog box > **Fetch Configurations > Manifest Info** field, enter the substitution variable. For example, $Custom-File-Name$.
   Select your distribution.
6. Click **Save**.

Transfer using On-device Intent

Procedure

1. In the **Choose an existing device attribute to pass file path in intents extras** field, enter a new custom attribute name, for example, deviceIntentURI.
2. Custom Attributes are used to hold the location (URI / ContentURI) value on the server for every device and can help administrators determine a file's availability on device. For more information, see **Assigning Custom Attributes to Devices**.
   In the **Provide access to specific app or package name** field, enter the **App Name** or the **Package Name**, for example, Velocity.

> These will be the only authorised packages allowed to access the file.

3. In the Intents-Standard section, provide the following details:
   - **Operation Type** - From the drop-down list, select **Start Activity** / **Start Service** or other similar choice as per the app. Choose the right value for this field depending on the target app developer's guidance or refer to the target app documentation.
   - **Class Name** (Optional) - Choose the right value for this field depending on the target app developer's guidance or refer to the target app documentation.
   - **Action** - Set the action to:or similar, as per the app.

     Bash

     ```
     com.wavelink.nameofapp.action.INSTALL_CONFIG
     ```

   - **Category** - Enter values separated by a semicolon (;).
   - **Mime Type** (Optional) - In the administrator's host server, the custom.mobileconfig file should be set with a MIME type of application/configuration so that the MDM profile for the device is downloaded and installed on the device. Choose the right value for this field depending on the target app developer's guidance or refer to the target app documentation.
   - **Flags** (Optional) - Select the number of flags to be used. Choose the right value for this field depending on the target app developer's guidance.

Provide the **Intents-Extras** values under KEY, TYPE, and VALUE (optional). For more specific parameters, see the OEM app documentation. Choose the right value for this field depending on the target app developer's guidance or refer to the target app documentation.

5. Click **Save**.
6. In the Configurations page, select the new File Transfer Configuration and then select **Actions** > **Apply to Label**. The **Apply To Label** dialog box opens.
7. Select the suitable Label and then click **Apply**.
   Transferring /Sharing of file with other apps can only be verified by collecting logs from the target app or from the device.

Verifying file download status

Custom Attributes are used to hold the location (ContentURI) value on the server for every file on each device and can help administrators determine a file's availability on the device.

Procedure

1. Go to **Devices** > **Devices**.
2. Select a specific device the File Transfer configuration was deployed to.

3. In the Device Details page, select the device and then select **Actions** > **Force Device Check-in**.
4. Under the Configurations tab, check that the File Transfer configuration displays with the status as **Applied**.
5. Under the Custom Attributes tab, check that the name of the new custom attribute displays (for example, "Custom-File-Name$") with its related value. This provides the information about the storage location of the file on the device and showcases that file has been locally downloaded to the device available within the Ivanti Go app sandbox.
   Transferring /Sharing of file with other apps can only be verified by collecting logs from the target app or from the device.

10.10.8.3. Apple TV Configuration

Licence: Silver

An Apple TV configuration defines the language and locale for Apple TV.

The Apple TV settings are as follows:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Language	Enter the two-character language code to specify the UI language.
Locale	Enter the locale ID to specify the country/language combination for the UI.

For more information, see **How to create a configuration**.

10.10.8.4. AirPlay Mirroring

Licence: Gold

AirPlay Mirroring is a feature that gives you the ability to display the screen from an iOS device on a monitor using Apple TV. Apple TV and the iOS device must be connected to the same Wi-Fi network. This feature requires the following devices:

- iOS 7 and later devices - Supervised
- macOS 10.10 and later devices - Supervised
- Apple TV version - Supervised
- AirPlay

> Switching to include management of non-iOS devices cannot be reversed.

This section contains the following topics:

- Configuring Apple AirPlay
- Setting up AirPlay on the mobile device
- Setting up a monitor to work with Apple TV
- Connecting your iOS device to Apple TV

Configuring Apple AirPlay

For more information on AirPlay configuration settings, see AirPlay Configuration.

Procedure

1. Go to **Configurations**.
2. Click **+Add**.
3. Click **AirPlay**.
4. Enter a Name and Description of the configuration in the appropriate fields.
5. For all supported iOS versions, enter a Device Name and Password.
6. Click + **Add** to add another device, if needed.
7. Optionally, for Supervised iOS 7+ devices or macOS 10.10+ add device IDs to a Allow list.
8. Click **Next**.
9. Choose a distribution level.
10. Click **Done**.

Setting up AirPlay on the mobile device

Procedure

1. Setup Apple Configurator.
2. Go to **Devices > Devices**.
3. Click the name of an iOS device to display the Details page for that device.

4. Click the ⋮ icon.
5. Select **AirPlay Mirroring** to display the AirPlay mirroring dialogue.
6. Select an Apple TV device from the pulldown menu.
7. Enter a scan time in seconds to specify a time limit to search for the device you selected.
8. Enter the password for the Apple TV device.
9. Click **Send Request**.

Setting up a monitor to work with Apple TV

Procedure

1. On a monitor connected to Apple TV, go to **Settings > Profile**.
2. Select **Ivanti Neurons for MDM Apple Configurator**.
3. Click **Add Profile**.
4. Click the ⋮ icon.
5. Select **AirPlay Mirroring** to display the AirPlay mirroring dialogue.
6. Select an Apple TV device from the pulldown menu.
7. Enter a scan time in seconds to specify a time limit to search for the device you selected.
8. Enter the password for the Apple TV device.
9. Click **Send Request**.

Connecting your iOS device to Apple TV

Procedure

1. Connect the Apple TV device to a monitor.
2. Using the Apple TV remote, go to **Settings > Accounts > Home Sharing** to turn on Home Sharing.
3. **Connect iOS device** to the same Wi-Fi network as your **Apple TV device**.
4. Open the Remote app on your **iOS** device.
5. Enable **Home Sharing** from the **Remote Settings** screen.

10.10.8.5. Browser Settings

Using Browser Settings, you can configure settings and restrictions for Google Chrome, Mozilla Firefox, Microsoft Edge and Internet Explorer in Windows 10 Devices.

This feature requires Bridge. See **Ivanti Bridge** for details.

> Ensure that the browsers are installed in the device before applying the browser settings.

To configure browser settings:

1. Go to **Configuration > +Add**.
2. Select **Browser Settings** configuration.
3. Enter a name for the configuration.
4. Enter a description.
5. In the Configuration Setup section, specify the remaining settings as described in the following table.

Setting	What To Do
Browsers	Select the browser type for which settings are required: • **Chrome** • **Firefox** • **Microsoft Edge** • **Internet Explorer**
Browser settings	Configure the following options: **Allow Browsers**: • Allow saving of Passwords • Allow Safe Browsing mode • Allow outdated plugins to stay on the browser **Chrome and Firefox**: • **Allow deleting browser history** **Chrome and Internet Explorer**: • **Allow browser printing** • **New Tab Page URL** **Chrome Only**: • **Show apps shortcuts in Bookmark Bar** • **Show Home button** • **Allow synchronisation of data with Google** • **Continue running background apps when Chrome is closed** **Firefox only**: • **Allow install extensions** **Internet Explorer Only**: • **Allow downloading data from websites**
Browser favourites	Click **+Add**. The **Add Browser Favourite** window is displayed. Configure the following fields: • **Display Name**: Type the display name for the favourite • **URL**: type the URL of the browser favourite. Click **Add**. The details of added browser favourite is displayed in the page. In the **Actions** column, click the Edit icon to edit the setting. To delete the browser favourite, click the Delete icon. **Browser Favourites Folder Name**: Type the name of the browser favourites folder name where the favourites should be listed. You can also add browser favourite in a CSV format. To upload in CSV format: 1. Click Upload CSV file. Browse and choose the CSV file to be uploaded. 2. Click **Upload**. The details in the CSV file should be added in the following format: • First column (Display Name) should specify the display name of the favourite. Example: "shopping".

Setting	What To Do
	• Second column (URL) should specify the URL of the favourite. Example: "https://amazon.com".
Website Security	Configure the following website security settings: **All Websites (Chrome and Firefox)** • **Block Cookies** • **Block Javascript** • **Block Plugins** • **Block Popups** Specific Websites (Chrome Only) **Blockedlisted Websites (Chrome and Edge)**: Add the website that you wish to Blockedlist. Click **+Add**. The **Add Blockedlisted Website** window is displayed. In the **Website URL**, type the URL of the website that should be Blockedlisted. In the **Access** field, select **Block** to Blockedlist the website. The default option is **Allow**. Click **Add**.
Browser Extensions	**Allowed Extension Types (Chrome Only)**: Select any of the following options: • **Extension** • **User Script** • **Themes** • **Packaged App** • **Hosted App** • **Platform App** **Browser extension sources (Chrome only)**: Click **+Add** to add browser extension sources. After the browser extension sources are added, you can edit or delete the sources by clicking the relevant options in the **Actions** column. **Force-Install Extensions (Chrome Only)**: Click **+Add** to add force-install extensions. After the force-install extensions are added, you can edit or delete the sources by clicking the relevant options in the **Actions** column.

6. Click **Next**.
7. Select one of the following distribution options:
   - All Devices
   - No Devices (default)
   - Custom
8. Click **Done**.

10.10.8.6. Configuring Single App Mode for iOS

Licence: Silver

Single app mode restricts iOS devices to the use of the specified app. For example, you might want to set up devices that can only use a custom app your organisation has developed.

Procedure

1. Go to **Configurations > Add > Single App Mode**.
2. Use the following guidelines to define the app and related settings.
3. Click **Next**.

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Choose App	Select the method to use for selecting the app: • **From App Catalog & System Apps:** Select to search the Ivanti Neurons for MDM app catalog and system apps (pre-installed on Apple devices by default). • Enter the name of the app and select it when it displays in the apps list. • **Enter Bundle ID:** Select to enter the unique identifier for the system app you want to select. Use this option if you cannot find the system app using the **From App Catalog & System Apps** option.
Disable Touch	Select to disable the touch screen.
Disable device rotation	Select to disable device rotation sensing.
Disable volume buttons	Select to disable the device's volume buttons.
Disable ringer switch	Select to disable the device's ringer switch.
Disable sleep wake button	Select to disable the device's sleep/wake button (top right on device rim).
Disable auto lock	Select to prevent the device from going to sleep after an idle period.
Enable voice over	Select to enable the VoiceOver screen reader (accessibility feature).
Enable zoom	Select to enable Zoom (accessibility feature).
Enable invert colours	Select to enable the invert colours adjustment (accessibility feature).
Enable assistive touch	Select to enable AssistiveTouch (accessibility feature).
Enable speak selection	Select to enable Speak Selection (accessibility feature).
Enable mono audio	Select to switch from stereo to mono audio (accessibility feature).
Voice over adjustments	Select to allow device users to make VoiceOver adjustments.
Zoom adjustments	Select to allow device users to make Zoom adjustments.

Setting	What To Do
Invert colours adjustments	Select to allow device users to invert colours.
Assistive touch adjustments	Select to allow users to make AssistiveTouch adjustments.

4. In the **Distribution** screen, select the device groups to receive this configuration.
5. Click **Done**.

> If you have configured the Phone dialer as the app to be used, then the Home button works once the device enters single app mode.

10.10.8.7. Configuring an iOS MDM Profile

The iOS MDM configuration defines the access limits for Ivanti Neurons for MDM. There are two types of iOS MDM configurations:

- **iOS MDM - Bulk Provisioned:** For devices purchased by the enterprise and provisioned as part of a mass distribution.
- **iOS MDM - Individually Provisioned:** For devices provisioned one by one. Will not be applied to Supervised and User Enrolled devices.

Only one of each type is provided and allowed across all Spaces.

Edit an iOS MDM configuration

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Go to **Configurations**.
3. Select the iOS MDM configuration you want to edit.
4. Click the pencil (edit) icon to edit the configuration.
5. Use the following guidelines to make changes:
6. Click **Done**.

Setting	What To Do
MDM Access Rights	
Allow device lock and passcode removal	Uncheck to prevent enforcement of a passcode compliance configuration.
Allow device erase	Uncheck to prevent enforcement of a device wipe action.
Allow query of Network information (phone/SIM numbers, MAC addresses)	Uncheck to exclude the device from networking information reporting. If this option is unchecked, then the device list view and device detail view will show N/A for the network information that is no longer reported. Also, the roaming policy will not be enforceable for affected devices.
Profile Removal Password	
Password to remove Profile	Specify a password. The user will be prompted to enter the password while deleting a profile from the device.
ADD Required APP (iOS 15+)	
Add by Lookup	Enter the App name and search the app in the App store and select the required app. Only one can be added at a time. Selecting one app disables the other apps.
Add Manually	Enter the iTunes ID of the app.

Your changes apply only to the devices that are provisioned after you make the change.

10.10.8.8. Configuring a macOS MDM Profile

The macOS MDM configuration defines access limits for Ivanti Neurons for MDM. The macOS MDM configurations are individually provisioned, for devices provisioned one by one.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Go to **Configurations**.
3. Select the macOS MDM configuration you want to edit.
4. Click the pencil (edit) icon to edit the configuration.
5. Use the following guidelines to make changes:
6. Click **Done**.

Setting	What To Do
Allow device lock and passcode removal	Uncheck to prevent enforcement of a passcode compliance configuration.
Allow device erase	Uncheck to prevent enforcement of a device wipe action.
Allow query of Network information (phone/SIM numbers, MAC addresses)	Uncheck to exclude the device from networking information reporting. If this option is unchecked, then the device list view and device detail view will show N/A for the network information that is no longer reported. Also, the roaming policy will not be enforceable for affected devices.
Profile Removal Password	
Password to remove Profile	Specify a password. The user will be prompted to enter the password while deleting a profile from the device.

Your changes apply only to the devices that are provisioned after you make the change.

10.10.8.9. Content Caching

Licence: Gold

Applicable to: macOS 10.13.4 or supported newer versions.

Configure content-caching service in order to enable local copies of the App Store software and enable connected clients for faster software and app downloads.

Content caching configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **caching** in the search field, and then click the **Content Caching** configuration.
4. Enter a name and describe the configuration.
5. Enter the **content caching configuration settings**.
6. Click **Next**.
7. Select the **Enable this configuration** option.
8. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
9. Click **Done**.

Content caching configuration settings

Use the settings in the following table to configure content caching. For more information about these settings, see **Apple documentation**.

Setting	Description
Allow the system to purge content from the cache automatically (Available in macOS 10.15 or supported newer versions.	Allow the system to purge content from the cache automatically when it needs disk space for other apps (i.e. when free disk space runs low on the computer). By default, this option is enabled.
Allow personal caching	Cache the user's iCloud data. Clients may take some time (hours or days) to react to changes to this setting; it doesn't have an immediate effect. By default, this option is enabled.
Allow Shared caching	Cache non-iCloud content, such as apps and software updates. Clients may take some time (hours, days) to react to changes to this setting; it does not have an immediate effect. By default, this option is enabled.
Allow automatically activating the content cache	Automatically activate the content cache when possible and prevents it from being disabled.
Allow Auto-Enable Tethered Caching (Available in macOS 10.15.4 or supported newer versions	Automatically enable Internet connection sharing when possible and prevent disabling Internet connection sharing.
Disables Tethered Caching	Disables tethered caching. The Disables Tethered Caching option overrides the Allow Auto-Enable Tethered Caching option.
Cache Limit	The maximum number of bytes of disk space that will be used for the content cache. A value of 0 means unlimited disk space. Default value: 0
Data Path	The path to the directory used to store cached content. Changing this setting manually doesn't automatically move cached content from the old location to the new one. To move content automatically, use the Sharing preference's Content Caching pane. The value must be (or end with) /Library/Application Support/Apple/AssetCache/Data.
Allow display alerts (Available in macOS 10.15 or supported newer versions.	Content Caching displays exceptional conditions (alerts) as system notifications in the upper corner of the screen.
Keep device Awake (Available in macOS 10.15 or supported newer versions.	Prevents the computer from sleeping as long as Content Caching is on (System Preferences > Sharing > Content Caching is on).
Listen Ranges	An array of dictionaries describing a range of client IP addresses to serve.

Setting	Description
First IP address	First IP address of the clients in the Listen Ranges.
Last IP Address	Last IP address of the clients in the Listen Ranges.
IP Address Type	Select one of the following options: • IPv4 (default) • IPv6
Allow Listen ranges Only	The content cache provides content to the clients in the Listen Ranges only.
Allow Listen with Peers and parents	The content cache provides content to the clients in the union of the Listen Ranges, Peer Listen Ranges and Parents. By default, this option is enabled.
Allow Local subnets only	The content cache offers content to clients only on the same immediate local network. No content is offered to clients on other networks reachable by the content cache. If this option is enabled, the Listen Ranges will be ignored. By default, this option is enabled.
Log client Identity	The Content Cache logs the IP address and port number of the clients that request content.
Parents selection Policy	Select one of the following policy options: • First available • URL path hash • Round-robin (default) • Random • Sticky-Available
Parents	An array of the local IP addresses of other content caches that this cache should download from or upload to, instead of downloading from or uploading to Apple directly. Click **+ Add** to add one or more IP addresses.
Allow Peer local Subnets only	The content cache only peers with other content caches on the same immediate local network, rather than with content caches that use the same public IP address as the device. By default, this option is enabled.
Port	The TCP port number on which the content cache accepts requests for uploads or downloads. Set the port to 0 to pick a random, available port. Default value: 0
Public Ranges	An array of dictionaries describing a range of public IP addresses that the Ivanti Neurons for MDM servers should use for matching clients to content caches.
First IP address	First IP address of the servers in the Public Ranges.
Last IP Address	Last IP address of the servers in the Public Ranges.
IP Address Type	Select one of the following options:

Setting	Description
	• IPv4 (default) • IPv6

For more information, see **How to create a configuration**.

10.10.8.10. Creating an Android Shortcut

Shortcuts are only available in Kiosk Mode using an Allowlisted browser. The browser must be Allowlisted in the Lockdown and Kiosk configuration. The shortcuts will appear in the Ivanti Neurons for MDM Kiosk launcher.

Procedure

1. Go to **Configurations**. **> +Add**
2. Click **Android Shortcut** to display the **Create Android Shortcut Configuration** page.
3. Enter a name for the Configuration in the **Name** field.
4. Enter a description of the configuration in the **Description** field.
5. Enter a unique label for the shortcut in the **Label** field.
6. Enter a URL for the target of the shortcut in the **URL** field.
7. Optionally, drag and drop a file in the icon field or click **Choose File** to navigate to the file to choose an icon for the shortcut.
8. Click **Next**.

10.10.8.11. Creating Accessibility Settings Configurations

This configuration allows enterprises to restrict, make changes, or configure accessibility settings on Apple devices.

Procedure

1. Go to **Configurations**.
2. Click **+ Add**.
3. Click **Accessibility Settings Configurations**.
4. Configure the settings specified in the following table:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Select one of the Accessibility Settings **Accessibility Settings** Close View Far Point Close View Near Point Contrast Value	• **Accessibility Settings**: Use this to configure accessibility settings on the macOS devices. • **Accessibility Settings Restrictions**: Use this to restrict the changes to accessibility settings for iOS devices. **Configuration Setup** The minimum Zoom level in zoom settings The maximum zoom level in zoom settings Enable "Use Scroll Gesture" in zoom options Enable "Smooth Images" in zoom options Specify the value
	Select the check box - Enable the "Flash the screen" in Audio options
	Select the check box - Enable Mouse keys in the Mouse and Trackpad options
Cursor Size	Specify the value
	Select the check box - Ignore Built-in Trackpad
Mouse Driver Initial Delay	Specify the value
Mouse Driver Max Speed	Specify the value
Enable "Slow Key" in Keyboard options	Select the check box
Enable "Click Key Sound" for slow keys Slow Key Delay Specify the value in milliseconds Select the check box - Play Stereo Audio as mono Enable Sticky Keys in the Keyboard options Enable the beep when a modifier key is set for sticky keys	Select the check box Select the check box Select the check box Select the check box Select the check box Select the check box
Enable display pressed keys on screen for sticky keys	Select the check box

Setting	What To Do
Enable voice over	Select the check box
Enable invert colours in display accommodations	Select the check box
Accessibility Restrictions	**Configuration Setup**
Enable bold text	Select the check box
Enable increase contrast	Select the check box
Enable reduced motion	Select the check box
Enable reduced transparency	Select the check box
Accessibility text size app that support that supports dynamic text use	Select the option from the drop-down list
Enable touch accommodations	Select the check box
Enable voice over	Select the check box
Enable zoom	Select the check box

5. Select the distribution option and specify the required details as applicable.
6. Click **Done**.

10.10.8.12. Create Screen Saver Configuration

The Screen Saver configuration lets you add options such as Password, Idle Time, Module path and name.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Click **Configurations**.
3. Click +Add.
4. Type screen in the search field, and then click **Screen Saver**:
   The Create Screen Saver Configuration details page appears.
5. Configure the settings on this page. Refer to the table in the topic **Screen Saver Configuration Settings** for guidance on the values.
6. Click **Next** to configure the distribution settings, and then click **Done**.

Screen Saver Configuration Settings

Setting	What To Do
Name (mandatory)	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Prompt for password check box	Select the check box to prompt the device user for password when the screen saver is unlocked or stopped. (Available in macOS 10.13 and later).
Prompt for password delay	Specify the delay duration in seconds.
Login Window Idle Time	Specify the idle time after which the screen saver must appear in Seconds.
Path to the screen saver module	Specify the path of the screen saver module.
Name of the screen saver module (mandatory)	Enter the name of the screen saver.

For more information, see **How to create a configuration**.

10.10.8.13. Configure User's Screen Saver

The User's Screen Saver configuration lets you add options such as Password, Idle Time, Module path and name.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Click **Configurations**.
3. Click +Add.
4. Type screen in the search field, and then click **User's Screen Saver**:
   The Create User's Screen Saver Configuration details page appears.
5. Configure the settings on this page. Refer to the table in the topic **User's Screen Saver Configuration Settings** for guidance on the values.
6. Click **Next** to configure the distribution settings, and then click **Done**.

User's Screen Saver Configuration Settings

Setting	What To Do
Name (mandatory)	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Idle Time	Specify the idle time after which the screen saver must appear in Seconds.
Path to the screen saver module	Specify the path of the screen saver module.
Name of the screen saver module (mandatory)	Enter the name of the screen saver.

For more information, see **How to create a configuration**.

10.10.8.14. Device Name Settings

Licence: Silver

A default device name configuration enables you to create a new configuration that gets pushed down to the device at the registration or post-registration level and allows the device naming. The admin can define default device names for **supervised iOS 8 devices** only. You can use the following variables to construct the device name:

- Device Serial Number
- Device IMEI
- Device Model
- Ivanti Neurons for MDM Username (local users only)
- LDAP Organisational Unit (OU)
- LDAP Common Name (CN)

For example, you would enter $-$ for device names that begin with the device serial number and end with the user's organisation as defined in LDAP.

Default Device Name Settings (for iOS)

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Device Name	Enter the format for the default device name, including available device and LDAP attributes.* If the resulting device name exceeds 63 characters, it will be shortened to make sure it displays correctly on the device.
Description	Enter a description that clarifies the purpose of this configuration.

Type $ to see a list of supported **variables**, if available, for this field.

Device Name Settings (Android)

The Android device name can be retrieved by the Go app. When the admin generates the Device Details report, the actual device name, the actual device name is shown rather than the device model or manufacturer's name. In case the user changes the device name, the new name will be shown the next time the report is generated. The respective device name can be viewed under **Devices** > **Settings** > **Device Name**.

10.10.8.15. Device Wallpaper Configuration

Licence: Silver

The device wallpaper configuration defines a default wallpaper image for the Home screen and Lock screen of Android 7.0 devices in Device Owner mode or Company Owned Personal Enabled (COPE) devices (excluding Android 11 EPO mode devices).

Android wallpaper settings

To define a default wallpaper image for Android devices:

1. Go to **Configurations**.
2. Click **+ Add**.
3. Click **Device Wallpapers**.
4. Click on the Android icon to view the Configuration Setup section for Android and configure the following settings
5. Click **Next**

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Upload Android Wallpaper	
Use the same image for Home Screen and Lock Screen	Select to upload a single image for both the screens.
Home Screen	Drag and drop the image file or click **Choose File** to select it.
Lock Screen	Drag and drop the image file or click **Choose File** to select it.

6. Select one of the following distribution options:

- **All Devices**
- **No Devices** (default)
- **Custom**

7. Click **Done**.

> The uploaded image must be in .jpg or .png format.

iOS wallpaper settings

You can define a default wallpaper image for iOS devices.

> This setting is applicable only for supervised devices.

1. Go to **Configurations**.
2. Click **+ Add**.

3. Click **Device Wallpapers**.
4. Click on the iOS icon to view the Configuration Setup section for iOS and configure the following settings
5. Click **Next**.

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Upload iPhone Wallpaper	
Use the same image for Home Screen and Lock Screen	Select to upload a single image for iPhone.
Home Screen	Drag and drop the image file or click **Choose File** to select it.
Lock Screen	Drag and drop the image file or click **Choose File** to select it.
Upload iPad Wallpaper	
Use the same image for Home Screen and Lock Screen	Select to upload a single image for iPad.
Home Screen	Drag and drop the image file or click **Choose File** to select it.
Lock Screen	Drag and drop the image file or click **Choose File** to select it.

6. Select one of the following options:

- **All Devices**
- **No Devices** (default)
- **Custom**

7. Click **Done**.

> The uploaded images must be 1164H x 640W and in .jpg or .png format.

macOS wallpaper settings

To define a default wallpaper image for macOS devices:

1. Go to **Configurations**.
2. Click **+ Add**.
3. Click **Device Wallpapers**.
4. Click on the macOS icon to view the Configuration Setup section for macOS.
5. Enter the path to the desktop picture.
6. Click **Next**.
7. Select one of the following options:
    - **All Devices**
    - **No Devices** (default)

- **Custom**

8. Click **Done**

> You can change Wallpapers based on the restriction. If macOS restrictions configuration **Allow modification of Wallpaper** is enabled, then you can modify the wallpaper.

For more information, see **How to create a configuration**.

10.10.8.16. EMA Server Integration Configuration

The EMA Server Integration configuration allows Windows 10 devices to link to the configured Intel EMA server. To link devices to the configured Intel EMA server, you should provide the installation directory of the original EMA agent and upload the EMA agent .msh file from the new EMA server.

This feature requires Bridge. See **Bridge** for details.

Procedure

1. Go to **Configuration > +Add**.
2. Select **EMA Server Integration** configuration.
3. Enter the name for the configuration.
4. In the Configuration Setup section, click **Choose File** to select the EMA agent .msh file.

> The msh file is an agent policy file that can be downloaded from the EMA server.

5. In the Original **EMA Agent Installation directory** field, type the location where the original EmaAgent.exe file is installed.
6. Click **Next**.
7. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
8. Click **Done**.

10.10.8.17. Energy Saver Configuration

Ivanti Neurons for MDM enables Energy Saver configuration for the payload you use to configure energy-saver settings on Windows and macOS devices.

Applicable to:

- Windows 10 through the most recently released version as supported by Ivanti Neurons for MDM.
- macOS 10.7 through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Energy Saver** configuration.
3. In the Choose OS section, select **Windows** or **macOS** and click **Next**.
4. Click **+ Add Description** to enter a brief description of the configuration.
5. For Windows, configure the following **Energy Saver** settings:
    - **Device on Battery**
    - **Device is Plugged in**
6. Configure the following **Energy Saver** settings:
    - **Desktop AC power energy-saver settings**
    - **Schedule for the computer to start up or shut down settings**
    - **Laptop AC power energy-saver settings**
    - **Laptop battery power energy-saver settings**
7. Click **Next** to configure the distribution settings.
8. Select one of the distribution options to set up the **Energy Saver** configuration. For more information about configuring distribution options, see **Working with Configurations**.
9. Click **Done**.

Windows Energy Saver configuration

When a new Energy Saver configuration applies to a device or when the existing Energy Saver configuration settings are modified, users must reboot their devices for the changes to take effect.

Device on Battery

Use the following energy saver settings in the table when the device is using power from the battery:

Setting	Description
Battery Threshold to turn on Energy Saver	When the device is using battery power, enter the battery charge level to turn on the Energy Saver, you can enter values from 0 to 100. Enter a percentage value that indicates the battery charge level. For example, when set to 80, Energy Saver turns on when the battery has 80% charge or less available charge. If you don't enter a value, Ivanti Neurons for MDM doesn't change or update this setting. By default, the Windows will set it to 70%.
When Lid is closed	• **Take No Action**: The device stays on and continues to use battery power. • **Sleep**: The device goes into sleep mode and uses a small amount of battery charge. The computer is still on, and opened apps and files are stored in Random Access Memory (RAM). • **Hibernate Sleep State**: The device goes into hibernate mode. Opened apps and files are stored on the hard disk, and the device turns off. • **Shut down**: The device shuts down. Opened apps and files are closed without saving.
When Power button is selected	• **Take No Action**: The device stays on and continues to use battery power. • **Sleep**: The device goes into sleep mode and uses a small amount of battery charge. The computer is still on, and opened apps and files are stored in RAM. • **Hibernate Sleep State**: The device goes into hibernate mode. Opened apps and files are stored on the hard disk, and the device turns off. • **Shut down**: The device shuts down. Opened apps and files are closed without saving.
When Sleep button is selected	• **Take No Action**: The device stays on and continues to use battery power. • **Sleep**: The device goes into sleep mode and uses a small amount of battery charge. The computer is still on, and opened apps and files are stored in RAM. • **Hibernate Sleep State**: The device goes into hibernate mode. Opened apps and files are stored on the hard disk, and the device turns off. • **Shut down**: The device shuts down. Opened apps and files are closed without saving.
Turn on hybrid sleep	• **True**: Devices can go into Hybrid Sleep mode. Opened apps and files are stored in RAM and on the hard disk. It uses a small amount of battery charge. • **False**: Prevents devices from going into hybrid sleep mode.

Device is Plugged in

Use the following settings in the table when the device is using power from an external power source:

Setting	Description
Battery Threshold to turn on Energy Saver	When the device is plugged in, enter the battery charge level to turn on Energy Saver, you can enter values from 0 to 100. Enter a percentage value that indicates the battery charge level. For example, when set to 80, Energy Saver turns on when the battery has 80% charge or less available charge. If you don't enter a value, Ivanti Neurons for MDM doesn't change or update this setting. By default, the Windows will set it to 70%.
When Lid is closed	• **Take No Action**: The device stays on and continues to use external power source. • **Sleep**: The device goes into sleep mode and uses a small amount of external power source. The computer is still on, and opened apps and files are stored in RAM. • **Hibernate Sleep State**: The device goes into hibernate mode. Opened apps and files are stored on the hard disk, and the device turns off. • **Shut down**: The device shuts down. Opened apps and files are closed without saving.
When Power button is selected	• **Take No Action**: The device stays on and continues to use external power source. • **Sleep**: The device goes into sleep mode and uses a small amount of external power source. The computer is still on, and opened apps and files are stored in RAM. • **Hibernate Sleep State**: The device goes into hibernate mode. Opened apps and files are stored on the hard disk, and the device turns off. • **Shut down**: The device shuts down. Opened apps and files are closed without saving.
When Sleep button is selected	• **Take No Action**: The device stays on and continues to use external power source. • **Sleep**: The device goes into sleep mode and uses a small amount of external power source. The computer is still on, and opened apps and files are stored in RAM. • **Hibernate Sleep State**: The device goes into hibernate mode. Opened apps and files are stored on the hard disk, and the device turns off. • **Shut down**: The device shuts down. Opened apps and files are closed without saving.
Turn on hybrid sleep	• **True**: Devices can go into Hybrid Sleep mode. Opened apps and files are stored in RAM and on the hard disk. It uses a small amount of external power source. • **False**: Prevents devices from going into hybrid sleep mode.

macOS Energy Saver configuration

Desktop AC power energy-saver settings

Use the following settings to configure the macOS desktop device's AC power energy-saver settings:

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Start up automatically after a power failure	Enable the device to start up automatically after a power failure.
Put a hard disk to sleep after	Enable the checkbox to put the hard disk to sleep at fixed intervals between 1 and 180 minutes. A value of 0 minutes will never put the hard disk to sleep.
Turn display off after	Enable the checkbox to turn off the display at fixed intervals between 1 and 180 minutes. A value of 0 minutes will never turn off the display.
Dynamic Power Step	Select the checkbox to enable the dynamic power step.
Reduce Processor Speed	Select the checkbox to reduce processor speed.
Put the computer to sleep after	Enable the checkbox to put the computer to sleep at fixed intervals between 1 and 180 minutes. A value of 0 minutes will never put the computer to sleep.
Wake for network access	Select the checkbox to wake the computer for network access.
Wake for modem ring	Select the checkbox to wake the computer for the modem ring.

Schedule for the computer to start up or shut down settings

Use the following settings to configure the macOS devices for scheduled start up or shut down of the devices.

Turning off the device settings

Select the checkbox **Turn the device off** to shut down the devices at fixed intervals.

Setting	Description
Event Type	Select one of the event types from the drop-down list: • Sleep • Restart • Shut Down
When	Select one or more days of the week to schedule an event type.
At	Select the time to schedule an event type.

Starting or waking up the device settings

Select the checkbox **Start up or wake the device** to wake up the devices at fixed intervals.

Setting	Description
Event Type	Select one of the event types from the drop-down list: • Wake Up • Start Up / Wake
When	Select one or more days of the week to schedule an event type.
At	Select the time to schedule an event type.

Laptop AC power energy-saver settings

Use the following settings to configure the macOS laptop device's AC power energy-saver settings:

Setting	Description
Start up automatically after a power failure	Enable the device to start up automatically after a power failure.
Put a hard disk to sleep after	Enable the checkbox to put the hard disk to sleep at fixed intervals between 1 and 180 minutes. A value of 0 minutes will never put the hard disk to sleep.
Turn display off after	Enable the checkbox to turn off the display at fixed intervals between 1 and 180 minutes. A value of 0 minutes will never turn off the display.
Dynamic Power Step	Select the checkbox to enable the dynamic power step.
Reduce Processor Speed	Select the checkbox to reduce processor speed.
Put the laptop to sleep after	Enable the checkbox to put the laptop to sleep at fixed intervals between 1 and 180 minutes. A value of 0 minutes will never put the laptop to sleep.
Wake for network access	Select the checkbox to wake the laptop for network access.
Wake for modem ring	Select the checkbox to wake the laptop for the modem ring.

Laptop battery power energy-saver settings

Use the following settings to configure the macOS laptop battery power energy-saver settings:

Setting	Description
Start up automatically after a power failure	Enable the device to start up automatically after a power failure.
Put a hard disk to sleep after	Enable the checkbox to put the hard disk to sleep at fixed intervals between 1 and 180 minutes. A value of 0 minutes will never put the hard disk to sleep.
Turn display off after	Enable the checkbox to turn off the display at fixed intervals between 1 and 180 minutes. A value of 0 minutes will never turn off the display.
Dynamic Power Step	Select the checkbox to enable the dynamic power step.
Reduce Processor Speed	Select the checkbox to reduce processor speed.
Put the computer to sleep after	Enable the checkbox to put the laptop battery to sleep at fixed intervals between 1 and 180 minutes. A value of 0 minutes will never put the laptop battery to sleep.
Wake for network access	Select the checkbox to wake up the laptop battery for network access.
Wake for modem ring	Select the checkbox to wake the laptop battery for the modem ring.

10.10.8.18. Ethernet Configuration (macOS)

Licence: Gold

Applicable to: macOS 10.13+ or supported newer versions.

Administrator can configure Ethernet Interface in variations. The following payloads are available for configuring Ethernet:

- Global Ethernet
- First active Ethernet
- First Ethernet
- Second active Ethernet
- Second Ethernet
- Third active Ethernet
- Third Ethernet

> The different payload for configuring Ethernet are default fallback Global, First, First active, Second, Second active, Third, and Third active Ethernet interface. Apple has an existing known issue with install of First, First active, Second, Second active, Third, and Third active Ethernet interface.

Ethernet configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.
3. Type **Ethernet** in the search field, and then select **Ethernet** Configuration.
4. Enter a name and describe the configuration.
5. Choose the configuration setup from the drop-down list.
6. Enter the **Ethernet configuration settings**.
7. Click **Next**.
8. Select the **Enable this configuration** option.
9. Select one of the following channel options to apply the configuration:
    - Device channel (most common)
    - User channel (current registered user)
10. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
11. Click **Done**.

Ethernet configuration settings

Use the settings in the following table to configure Ethernet. For more information about these settings, see **Apple documentation**.

Setting	Description
Protocols	
Accepted EAP Types	Select the EAP types that can be used for accessing this network: • Transport Layer Security(TLS): The TLS is a protocol that establishes an encrypted session between two computers on the Internet. It verifies the identity of the server and prevents hackers from intercepting any data. • TTLS: In the **Inner Identity** field, select one of the authentication protocols such as OS Default, PAP, CHAP, MSCHAP, MSCHAPv2 and EAP. • PEAP • LEAP • EAP-SIM: In the **EAP SIM Number of RANDs** field, select number of rands from the drop-down list. • EAP-AKA • EAP-FAST: Select the EAP-FAST option that define authentication methods: ◦ **Use PAC**:Select to use a proxy auto-config (PAC). ◦ **Provision PAC**: Select to allow a PAC to be provisioned. Otherwise, only a PAC already provisioned on the device can be used. This option is available only if you selected Use PAC. ◦ **Provision PAC Anonymously**: Select to allow a PAC to be provisioned without authenticating the server. This option is available only if you selected Provision PAC.
Authentication	**Username**: Specify the username required for network access. If you leave this blank, the device user will be prompted for it. • Use Per-Connection Password: Select to prompt the device user for a password for each connection. When the device rejoins the same network, the device user will be prompted to reauthenticate to join the network. Every time connection is initiated, password is requested. • Prompt One time password when connected to network: Password is requested only once when the configuration is pushed to the device. Every connect and disconnect to network, will not request any password. **Password**: (Optional) Enter the password for accessing this network. Otherwise, the device user will be prompted for any password required for accessing the network. **Outer identity**: (Optional) For TTLS, PEAP, and EAP-FAST, select to allow device users to hide their identity. The user's actual name appears only inside the encrypted tunnel. This option can increase security because an attacker cannot see the authenticating user's name in the clear. **System Mode Credentials Source Identity**: System mode is used for computer authentication. Authentication using system mode occurs before a user logs in to the computer. System mode is commonly configured to provide authentication with the computer's X.509 certificate (EAP-TLS) issued by a local certificate authority.
Trust	**Trusted Certificates:** Select the checkboxes to select multiple certificates from the list. **Trusted Server Certificate Names**: Add the certificate name. • **Allow Trust Exceptions**: Allow trust decisions (via dialog) to be made by the user. • **Require TLS certificate** **Maximum TLS version allowed with EAP authentication**

Setting	Description
	Minimum TLS version allowed with EAP authentication **TLS Trusted Certificates: MobileIron Agent CA Certificate**

For more information, see **How to create a configuration**.

10.10.8.19. Google BeyondCorp Configuration

Ivanti Neurons for MDM can be integrated with Google BeyondCorp for conditional access. Ivanti Neurons for MDM sends device compliance status signal to Google BeyondCorp. This ensures that only compliant devices under N-MDM can access Google workspace applications.

Applicable to

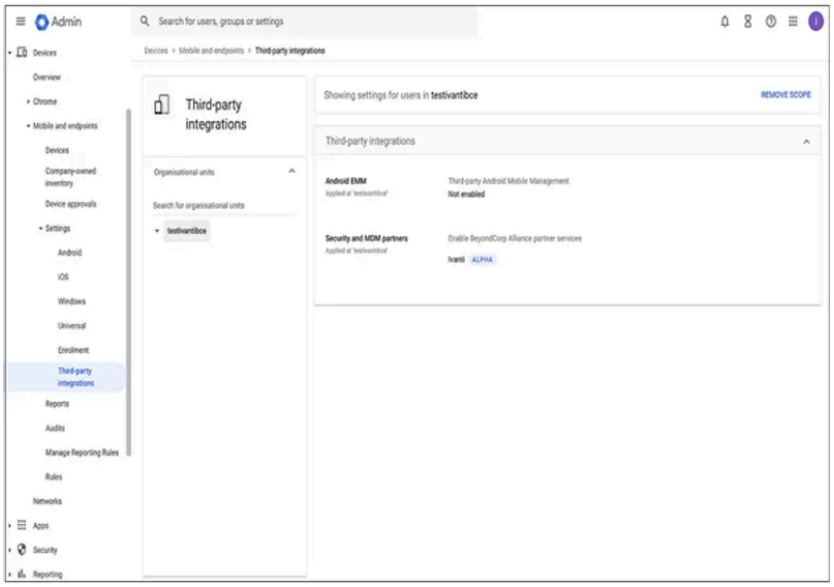
- iOS
- Android
- Windows

Prerequisites

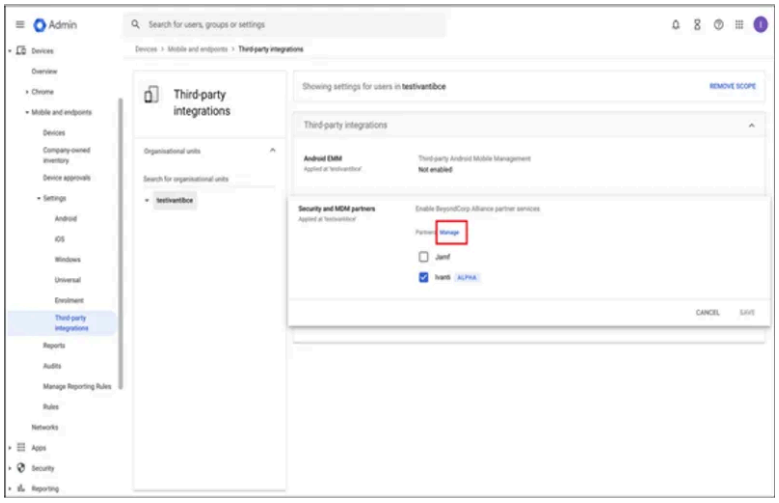
- For Ivanti Neurons for MDM, you must have an Ivanti Professional Plus / Premium license.
- For Google, you must have the BeyondCorp Enterprise, Google Workspace Enterprise or Cloud Identity Premium license.
- For Windows, you must have the following installed on the device:
  - Ivanti Bridge
  - Google Chrome

Procedure (Google)

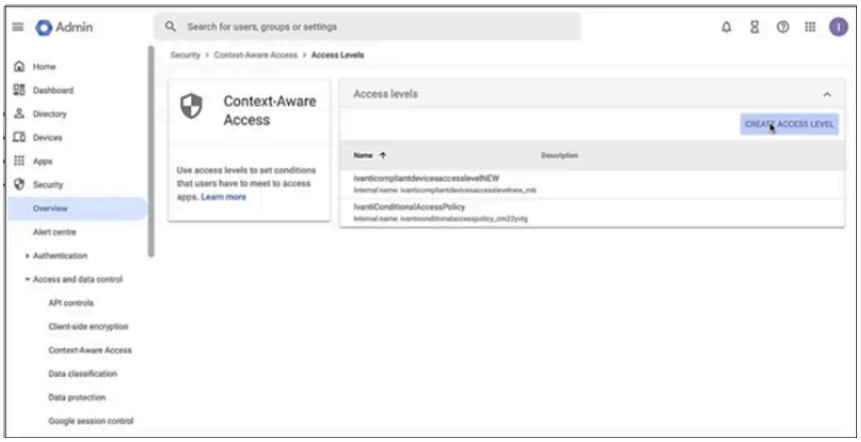
1. Login to the **Google Admin console** with admin credentials.
2. Go to **Devices** > **Mobile & Endpoints** > **Settings** > **Third-party integrations**.



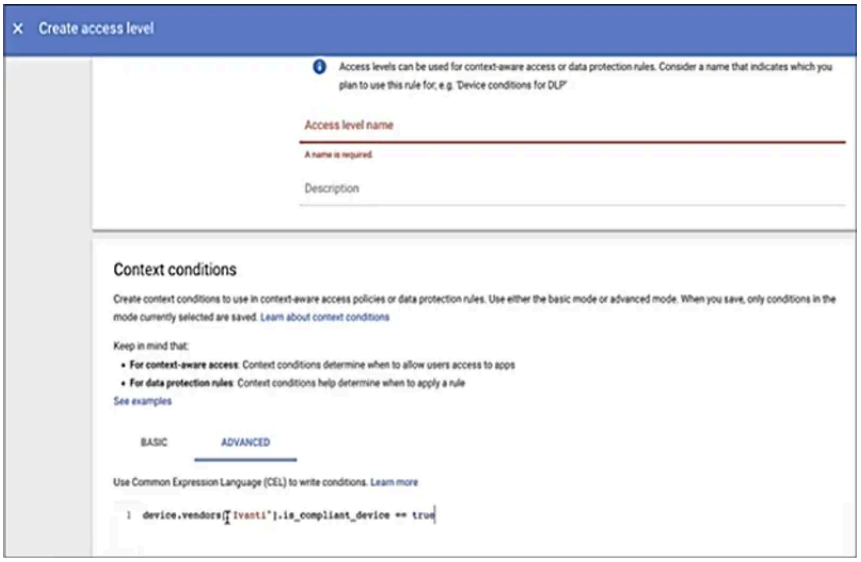
3. Click **Security and MDM partners** > **Manage**.



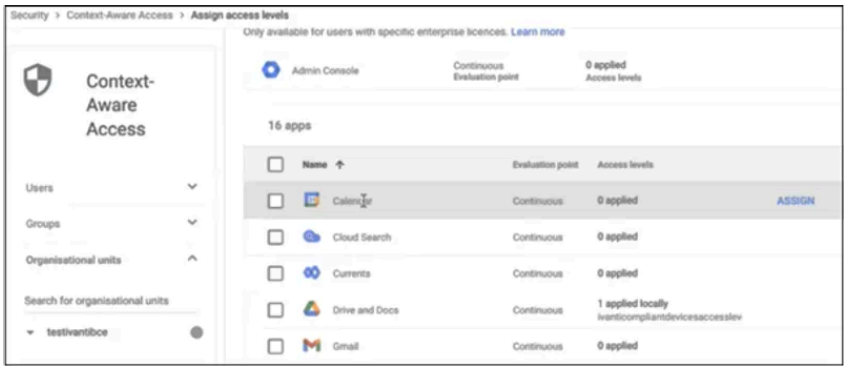
4. In the **Manage Partner Connections** window, select **Ivanti**.
5. Click **Open Connection**.
   You will be redirected to the Ivanti Neurons for MDM login page; enter the tenant admin credentials. Once you log in to the tenant, you will see that **Google BeyondCorp** is enabled and linked to your Google account automatically.
6. In the Google Admin Console, go to **Security** > **Context-Aware Access** > **Access levels**.



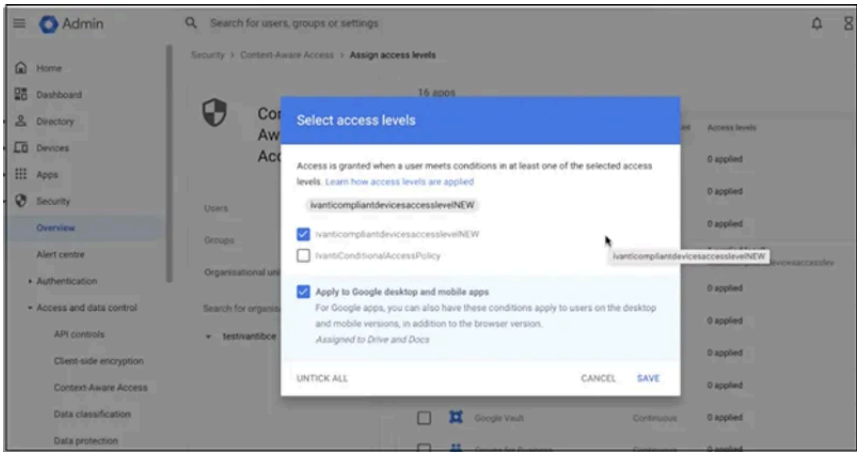
7. Click **Create Access Level**.
   In the Create Access Level window, under the Context conditions section, click **ADVANCED** and provide the required information.



8. Go to **Security** > **Context Aware Access** > **Access level**, select the application for which you would like to assign the policy.



9. Click **Assign**.
10. From the **Select access levels** window, select the policies you want to assign and click **Save**.



Once the above setup is complete, you can create the partner device compliance configuration using **Google BeyondCorp**.

Procedure (Ivanti Neurons for MDM**)**:

1. Go to **Configurations** > **Add Configuration**.

2. Select **Partner Device Compliance** configuration.
3. The Create Partner Device Compliance configuration page appears on the screen.
   Enter a name for the configuration.
4. Under the Choose Partner list, select **Google BeyondCorp**.
5. The Configuration Setup section appears on the screen. Make sure the Report Compliance Status for iOS and Android devices option is set to ON.
   Click **Next**.
6. Select **Enable this configuration**.
7. Select **Custom** as distribution option
8. Select **Users/User Groups** under the **Custom Distribution** Option.
9. Under the **Select below to distribute this configuration** section, select users/user groups from the list.
10. Click **Done**.

Google BeyondCorp server can uniquely identify each device through the app-managed configuration P-List.



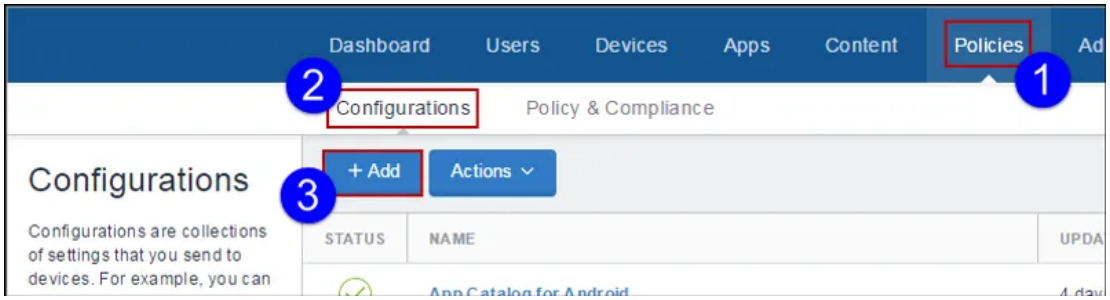
10.10.8.20. Lock Screen Message Configuration

Displays a message and asset tag info on the login and lock screens. This is for supervised devices using iOS 9.3 or supported newer versions.

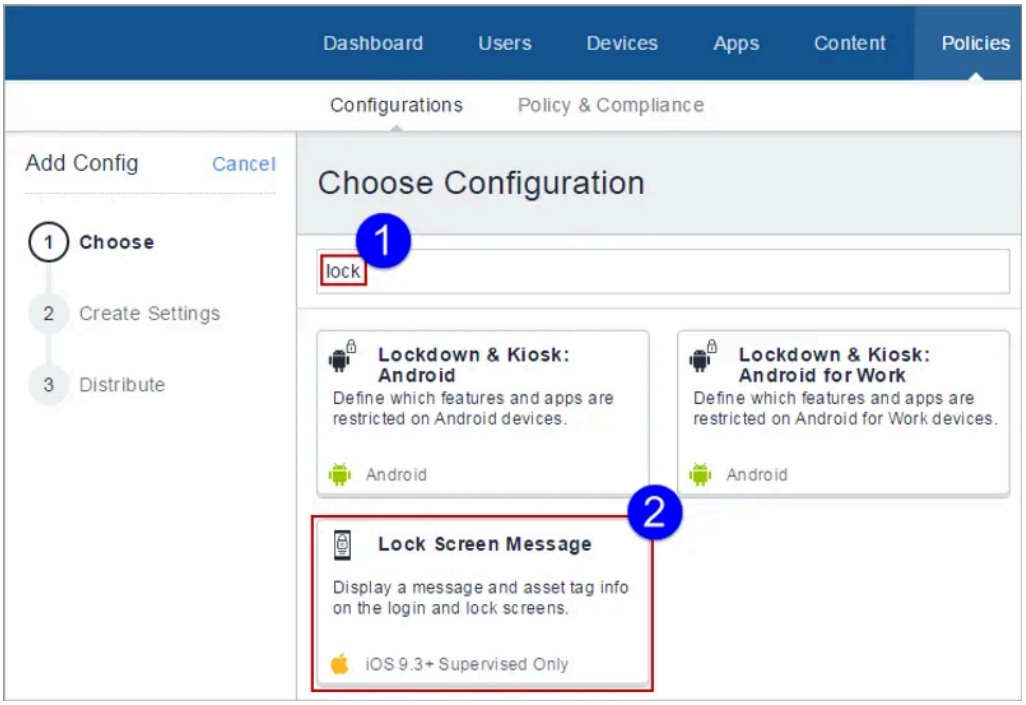
Creating a Lock Screen Message configuration

Procedure

1. Select **Configurations**.
2. Click **+ Add**.



Type **lock** in the search field, and then click the **Lock Screen Message** configuration:



The Lock Screen Message Configuration details page appears.
Configure the settings on this page. Refer to the table in the section Lock Screen Message Configuration Settings for guidance on the values.

5. Click **Next** to configure the distribution settings, and then click **Done**.

Lock Screen Message Configuration settings

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Lock Screen Footnote	This text appears on the login window and lock screen.
Asset Tag Information	This text appears at the bottom of the login window and lock screen.

For more information, see **How to create a configuration**.

10.10.8.21. Login Window Configuration - macOS

Procedure

1. Login to Ivanti Neurons for MDM.
2. Go to **Configurations** > **Add Configurations**.
3. Click (or Select) **Login Window**.
4. In the **Name** field, enter a name for the login window configuration.
5. Click **+ Add Description** to add details.
6. Under the **Configuration Setup** section, provide the following fields:
    - **Admin Host Info**: Enter the hostname or IP address or SystemVersion.
    - **Allow List**: List of user GUIDs or group GUIDs of users that the system allows users to log in. An asterisk ('*') string specifies all users or groups.
    - **Auto Login Password**: Enter the password for auto-login.
    - **Deny List**: The list of user GUIDs or group GUIDs of users that the system disallows logging in. This list takes priority over the list in the 'AllowList' key.
    - **Login Window Text**: Enter the login window text.
    - Select the checkbox for additional options like:
        - **Disable Console Access**
        - **Disable FDE Autologin (FileVault Disk Encryption)**
        - **Disable immediate Screen Lock functions**
        - **Hide administrator users when showing a user list**
        - **Show only network and system users**
        - **Hide Mobile Accounts**
        - **Show Network users**
        - **Disables the logout menu item**
        - **Disable power off when the user is logged in**
        - **Disable the restart menu item when the user is logged in**
        - **Disable Restart item**
        - **Show the name and password dialog**
        - **Show other users – managed**
        - **Show input menu**
        - **Disable the shutdown button**
        - **Disable the Sleep button**
        - **Disable the shutdown menu button**
7. Click **Done**.

10.10.8.22. macOS System Extension configuration

System Extension configuration allows installation of extension types like Driver Extension, Network Extension and Endpoint Security Extension, without kernel-level access.

Procedure

Applicable to: macOS 10.15+

1. Go to **Configurations** > **+Add**.
2. Type **extension** in the search field, and then click the **System Extensions** configuration.
3. Enter a **Name** and **Description** of the configuration.
4. Under **Allowed System Extensions**, **+Add** the **Allowed Team Identifiers** and **Allowed System Extensions**.
5. Under **Allowed System Extensions Types**, **+Add** the **Allowed Team Identifiers** and **Allowed System Types**.
6. Check **Allow user overrides** option.
7. Click **Next**.
8. Select **Enable this configuration** option.
9. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
10. Click **Done**.

> In macOS 12, RemovableSystemExtensions allows application to deactivate their system extension without administrator approval during application uninstallation.

10.10.8.23. MAM-Only

Ivanti Neurons for MDM allows you to specify iOS and Android devices as MAM-only and provides Mobile App Management (MAM) to such devices. A MAM-only deployment allows you to distribute and manage apps without having to manage the device itself.

MAM-Only Solution - Ivanti AppStation Alternative

As an alternate solution to Ivanti AppStation, Ivanti is offering a modern and flexible Mobile Application Management (MAM) solution using the Ivanti Go Client, available for both iOS and Android platforms.

The new MAM-Only solution introduces an integrated App Catalog along with Ivanti Neurons for MDM Web Clip functionality, which together fulfills the core use cases previously addressed by App Station in delivering a simplified, secure, and unified App Management experience for both users and administrators.

Key features

- **In-App App Catalog**: Hosts and distributes approved, managed apps directly within the Go Client.
- **App Configuration and Updates**: Supports application-level configuration and version updates, enforced through MAM policies.
- Ivanti Neurons for MDM **Requirement**: Ideal for BYOD and contractor scenarios where Ivanti Neurons for MDM enrollment is not feasible.

Using Web Clip for Ease of Access

- **Direct Access to App Catalog**: Deployment of Web Clips via Ivanti Neurons for MDM to provide a shortcut to the App Catalog or specific web-based enterprise apps.
- **Custom App shortcuts**: Allows users to quickly launch frequently used resources from their home screen.

Enhanced Admin and User Experience

- **Unified Interface**: Combines App Catalog, Web Access, and Compliance Messaging into one experience.
- **Simplified Administration**: No need to maintain separate solutions (i.e., App Station), reducing complexity and risk of configuration drift.

Flexibility and Customisation

- **Customise Catalog Views**: Customizing the App Catalog contents based on user roles, geo-location, or organisational unit.
- **Uses Existing Infrastructure**: Leverages your existing Ivanti Neurons for MDM / MAM investment (no separate infrastructure is required).

Support for dual role users

The Ivanti MAM-Only solution is designed to support modern work scenarios, including users with dual roles:

- **Full time employee - Org A**: Access enterprise apps via a Webclip (e.g., Apps@Work) deployed through Ivanti Neurons for MDM.
- **Contractor - Org B**: Use Ivanti Go Client in MAM-Only mode to securely access managed applications—without requiring device enrollment in Ivanti Neurons for MDM.

This enables seamless, role-based access to necessary apps without profile conflicts or device management overlap.

Migration Guidance

Ivanti strongly encourages App Station customers to plan and execute their transition to the Go Client-based MAM-Only solution. For step-by-step migration assistance, please refer to the following resources:

- Ivanti MAM-Only Solution
- **App Catalog Configuration in Go Client**
- **Create a Web Clip Configuration**

If you have questions or need migration assistance, please contact **Ivanti Support** or your Customer Success Manager.

10.10.8.24. Managed Google Play Configuration

Administrators can configure the automatic update setting that Google Play Store uses to update apps on the Android Enterprise device.

To configure auto-update settings:

1. Go to **Configuration > +Add**.
2. Select **Managed Google Play** configuration.
3. Enter a name for the configuration.
4. Enter a description.
5. In the Configuration Setup section, select an option to update apps from Google Play.

Setting	What To Do
User Defined	The device user can set the auto-update appsmaintenance window setting to define when the apps should be updated. 1. In the **Start Time** field, select the time to perform the app update. 2. In the **Duration** field, select the duration (in hours) within which the update should be performed. The minimum and maximum range is between 1 hour to 24 hours. The apps can be updated anytime between the start time to selected duration. For example, if the 'Start Time' is set as 6 PM and the 'Duration' is set for 12 hrs, the apps may be updated anytime from 6 PM to 6 AM.
None	Google Play Store never automatically updates apps on the device.
Wifi Only	Google Play Store automatically updates apps on the device but only using Wi-Fi, not mobile connections.
Always	Google Play Store automatically updates apps on the device using either Wi-Fi or mobile connections.

6. Click **Next**.
7. Select one of the following distribution options:

- All Devices
- No Devices (default)
- Custom

8. Click **Done**.

10.10.8.25. Migration Assistant Settings

Use the **Migration Assistant Settings** to configure Migration Assistant settings on supervised devices. This configuration helps administrators apply consistent, policy-based controls that manage how users transfer data, apps, and settings during device setup or migration.

Applicable to:

- macOS 15.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Migration Assistant Settings** configuration.
3. Configure the **Migration Assistant Settings** settings as per the following table:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Should Do Managed Migration	Select the checkbox to enable and manage Migration of devices. Toggle the **Push to Device** button to enable Migration of devices.
Excluded Accounts	Enter the account names that you want to exclude from migrating. Toggle the **Push to Device** button to enable exclusion of accounts.
Excluded Paths	Enter the path names that you want to exclude from migrating. Toggle the **Push to Device** button to enable exclusion of paths.
Required Paths	Enter the path names that you want to include in migration. Toggle the **Push to Device** button to enable inclusion of paths.
Should Migrate Security Privacy Settings	Select the checkbox to enable migration of Security Privacy Settings from devices. Toggle the **Push to Device** button to enable migration of Security Privacy Settings.

4. Click **Next** to configure the distribution settings.
5. Select one of the distribution options to set up the **Migration Assistant Settings** configuration. For more information about configuring distribution options, see **Working with Configurations**.
6. Click **Done**.

10.10.8.26. App Notifications Configuration

Using the Notifications configuration, administrators can schedule silent and visible notifications for iOS devices. The Notifications configuration can also be cloned, exported, or deleted.

Procedure

1. Go to **Configuration > +Add**.
2. Select **Notifications** configuration.
3. Enter a name for the configuration.
4. Enter a description.
5. In the Configuration Setup section, select one or both **Notification Scheduling** options:
    - Silent Notification Scheduling - Silent notifications are used to support background device&nbhyphen;management operations initiated by . They enable automated actions such as compliance checks, policy updates, and app updates without requiring user interaction. sends silent notifications to the device at the configured level.
    - Visible Notification Scheduling - Visible notifications are used when user awareness or action is required to maintain device compliance, security, or functionality. Visible notifications are triggered only after the specified interval, even if multiple actions or events occur during that period. A visible notification is shown on the device only if a silent notification has not been sent during the visible&nbhyphen;notification interval.
6. Click **Next**.
7. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
8. Click **Done**.

Visible Notification Content for MTD devices - Your device could be vulnerable to threats. Please launch the Ivanti Go application and check Threat Defense status.

Visible Notification Content for Non-MTD devices - To receive enhanced security features and ensure the latest protection measures, please launch the app on your device for a more secure user experience.

10.10.8.27. Printer Settings

Ivanti Neurons for MDM allows you to create printer profiles and add them to devices. This feature requires Bridge. See **Bridge** for details.

> When the printer profile is sent to the device, the printer must be active, otherwise the device cannot discover it.

To set Printer Settings configuration for a Windows device:

1. Go to **Configuration > +Add**.
2. Select **Printer Settings** configuration.
3. Enter a name for the configuration.
4. Select the **Windows** option.
5. In the **Configuration Setup** section, configure the following settings:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Windows Printer Settings	
Shared Printer	If the **Shared Printer** option is selected, the printer will be shared with other devices. Configure the following fields: **Name**: Enter the name of the printer configuration. **Description**: Enter a description of the printer. **Print Server**: Enter the IP address of the print server. **Shared printer name**: Enter the printer name.
Network-attached printer	When the **Network-attached** option is selected, the printer can be accessed only by devices within the attached network. Configure the following fields: **Name**: Enter the name of the printer configuration **Description**: Enter a description of the printer. **Print Name**: Enter the name of the printer in the network. **Printer host address**: Enter the host IP address of the printer. **Printer port number**: Select the port number of the network printer. **Printer driver name**: Enter the name of the printer driver. **Printer driver URL**: Enter the URL of the printer driver. For the Printer driver, upload a ZIP archive containing the required files. The ZIP archive must include the following files: • .inf file (driver information) • .cat file (catalog/signature) • Any additional driver binaries referenced by the INF (such as .dll, .sys, etc.)

6. Click **Next**.

7. Select one of the following distribution options:

- All Devices
- No Devices (default)
- Custom

8. Click **Done**.

To set Printer Settings configuration for a macOS device:

1. Go to **Configuration > +Add**.
2. Select **Printer Settings** configuration.
3. Enter a name for the configuration.
4. Select the **macOS** option.
5. In the **Create Printer Configuration** section, configure the following settings:

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Configuration Setup	Update the following fields to set-up printer for macOS devices: • Allow Local Printers • Default Printer Display Name • Footer Font Name • Footer Font size • User Printer List • + Add Printer

6. Click **Next**
7. Select one of the following distribution options:

- All Devices
- No Devices (default)
- Custom

8. Click **Done**.

10.10.8.28. Remove Bloatware Configuration

Remove Bloatware configuration allows you select the list of applications installed in devices which needs to be forcibly removed. It is a prerequisite to have a Bridge setup for this configuration. See **Bridge** for more details.

To run or uninstall apps:

1. In the **Configuration** tab click **+Add**.
2. Select **Remove Bloatware** configuration. The **Remove Bloatware Configuration** page is displayed.
3. In the **Name** field, type an appropriate name for the configuration.
4. Click the **+Add Description** link to add a description for the configuration.This field is optional.
5. In the **Configuration Setup** section, select the apps that should be removed or uninstalled. You can alternatively search for an app in the Search field using the App name displayed in Desktop-apps list.

> Before creating the **Remove Bloatware** configuration, you should fetch apps by going to **Apps>Desktop Apps>Fetch Apps**. If not, no applications will be available to search or choose from when creating the **Remove Bloatware** configuration.

The file types .appx,.appxbundles,.xap and .msi can be removed but not the file type .exe.

6. In the Advanced options, configure the following options:

Option	Description
Run this configuration every	Set the interval duration (in minutes) after which the configuration should run.
Run at Logon	Select the checkbox to run the configuration at logon.
Suppress force restart after uninstall	Select the checkbox to prevent force restart after uninstalling the app.

10.10.8.29. Safari Extension and Settings Configuration

Safari Extension

Ivanti Neurons for MDM enables the management of Safari Extensions on supervised iOS and macOS devices. The administrators can effectively manage Safari Extensions for standard and private browsing.

Applicable to:

- iOS 18.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.
- macOS 15.0 Supervised through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Safari Extension Settings** configuration.
3. Configure the **Safari Extension Settings** settings as per the following table:

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Extension ID	Enter the composed extension identifier. For example, "*Identifier (TeamIdentifier)*." Enter "*" for all extensions. To generate this string, use code sign *-dv <path_to_appex>*. The browser extension is located in the plug-ins folder inside the app bundle. The expected format is "*Identifier (TeamIdentifier)*." For extensions that are not available on macOS, the app developer should provide this information.
Extension State	Select one of the following options: • **Allowed**: The user can turn on or off the extension. • **Always On**: The extension is always "On" for the user. • **Always Off**: The extension is always "Off" for the user.
Private Browsing State	Select one of the following options: • **Allowed**: The user can turn on or off the extension in Private Browsing. • **Always On**: The extension is always "On" for the user even during Private Browsing. • **Always Off**: The extension will not be available.
Allowed Domains	Enter the domain or sub-domain values to grant the Safari Extension access. You can enter multiple domain or sub-domain values. The Allowed Domain settings are not applicable on the device if you enter "*" in the Extension ID field.
Denied Domains	Enter the domain or sub-domain values to restrict the Safari Extension access. You can enter multiple domain or sub-domain values. The Denied Domain settings are not applicable on the device if you enter "*" in the Extension ID field.

4. Click **+Add** to add multiple **Extensions**.
5. Click **Next** to configure the distribution settings.
6. Select one of the distribution options to set up the **Safari Extension Settings** configuration. For more information about configuring distribution options, see **Working with Configurations**.
7. Click **Done**.

Safari Settings

Ivanti Neurons for MDM enables the management of Safari Settings on supervised iOS and macOS devices. The administrators can effectively manage Safari Extensions for standard and private browsing.

Applicable to:

- iOS 26.0+, iPad 26.0+, macOS 26.0+, visionOS 26.0+ beta versions through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Safari Extension and Settings** configuration.
3. Click **Safari Settings**.
4. Configure the **Safari Settings** settings as per the following table:

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Configuration Settings	Select one of the following options to set the start page type: • **Start**: To use the default start page. Safari disables the existing homepage. • **Homepage**: To use the specified HomePage URL. Safari sets this as homepage. • **Extension**: To use the page specified by Safari Extension for which the identifier is ExtensionIdentifier. Safari disables the existing homepage.

5. Click **Next** to configure the distribution settings.
6. Select one of the distribution options to set up the **Safari Settings** configuration. For more information about configuring distribution options, see **Working with Configurations**.
7. Click **Done**.

Safari Privacy Settings

Safari Privacy Settings allow administrators to define default camera and microphone permissions for specific websites in Safari using Declarative Device Management (DDM). This feature helps organizations manage website privacy permissions centrally and provide a more consistent browsing experience on managed Apple devices.

Applicable to:

- iOS 27.0+ and macOS 27.0+ versions through the most recently released version as supported by Ivanti Neurons for MDM.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Safari Extension and Settings** configuration.
3. Click **Safari Privacy Settings**.
4. Configure the **Safari Settings** settings as per the following table:

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.

Configuration Settings	• **Add url**: Enter a url to apply the setting.
	• **+Add Defaults**: Specify the default values that you want to apply for this setting.
	  ◦ Camera - Allow/Deny
	  ◦ Microphone - Allow/Deny
	  ◦ Organization Justification (mandatory)

5. Click **Next** to configure the distribution settings.
6. Select one of the distribution options to set up the **Safari Settings** configuration. For more information about configuring distribution options, see **Working with Configurations**.
7. Click **Done**.

10.10.8.30. Samsung Phone Restrictions Configuration

Configurations

Samsung Phone restrictions configuration allows you to set call restrictions and exceptions in Samsung devices. These restrictions limits the phone numbers that users can make or receive.

Applicable to: All Samsung devices with Knox SDK 2.0+.

To configure Samsung Phone restrictions:

1. In the **Configuration** tab, click **+Add**.
2. Select **Samsung Phone Restrictions** configuration. The **Samsung Phone Restrictions Configuration** page is displayed.
3. In the **Name** field, type an appropriate name for the configuration.
4. Click the +**Add Description** link to add a description for the configuration.This field is optional.
5. In the **Configuration Setup** section, configure the following options:
   Option
   Description
   Incoming Calls
   Blocked numbers
   Click the Add icon to add numbers and Java regular expressions to define restrictions on incoming calls.
   Allowlisted numbers
   Click the Add icon to add numbers and Java regular expressions to define allowed numbers out of a larger set of blocked numbers for incoming calls.
   Note: This option will not have any effect if there are no blocked numbers.
   Outgoing calls
   Blocked numbers
   Click the Add icon to add numbers and Java regular expressions to define restrictions on outgoing calls.
   Allowlisted numbers
   Click the Add icon to add numbers and Java regular expressions to define allowed numbers out of a larger set of blocked numbers for outgoing calls.
   Note: This option will not have any effect if there are no blocked numbers.
6. Click **Done** to push the setting to the selected devices.

> Note: When the device is retired, all the call restrictions are removed from the device

For more information, see **How to create a configuration**.

10.10.8.31. Default Browser Configuration - iOS and visionOS

Configuration to change the settings of default applications on iOS and visionOS devices.

Prerequisites

- Applicable only for iOS (18.2+) and visionOS 2.2 versions.
- These apps are set on iOS devices in **Settings** - **Apps** - **Default Apps**.

Procedure

1. On the **Devices** page, register an iOS (18.2 +) device or a visionOS 2.2 device.
2. Navigate to **Configurations** > **Add Configuration** > **Default Application Settings** to set default browser on iOS devices.
3. Click **Configurations** > **Create Settings** > **Create Default Application Settings Configurations**
4. Under the Configuration Details section, provide the **Name** and **Description**.
5. Under Configuration Settings > Add App > Add by Lookup, search for the desired browser. The list of browsers is displayed.
6. Select the desired browser from the list.
7. In the **Create Default Application Settings Configuration** page, click **Custom** to distribute the configuration to a specific device or device groups or users or user groups.
8. Under **Choose one of these Custom Distribution option**, select the desired option to specify distribution of this configuration to either User / User Groups or Device / Device Groups.
9. Select the desired option under **All Available** to distribute this configuration.
10. Click **Done**.

10.10.8.32. Screen Sharing Host Settings Configuration

The **Screen Sharing Host Settings** configuration enables administrators to securely control macOS screen sharing features across managed devices using Ivanti Neurons for MDM. This feature allows specification of authorised users, authentication methods, and service restrictions to ensure compliant and secure remote access.

Applicable to: macOS 14.0 through the most recently released version as supported by Ivanti Neurons for MDM.

Before you begin: For seamless integration of the **Screen Sharing Host Settings** configuration, the user must enable '**Remote Management**' on their device. In your device, go to **Settings** > **Remote Management** > **Enable Remote Management**.

Procedure

1. Go to **Configurations** > **+Add**.
2. Search and select the **Screen Sharing Host Settings** configuration.
3. Configure the **Safari Settings** settings as per the following table:

Setting	Description
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Port Base	Enter the initial UDP port number to connect to the host. Screen sharing requires multiple connections, so the system increments this value by 1 for each additional connection. This doesn't change the port number that the system uses to initially establish a connection with a host, which is always TCP port 5900. **Minimum Port Base value**: 1024 **Maximum Port Base value**: 65535
Maximum Virtual Displays	You can use up to two virtual displays.
Prevent Copy Files From Host	Select the checkbox to prevent the users from copying files from the screen-sharing host.
Prevent Copy Files To Host	Select the checkbox to prevent the users from copying files to the screen-sharing host.
Prevent High Performance Connections	Select the checkbox to prevent the users from establishing high-performance connections to the host.

4. Click **Next** to configure the distribution settings.
5. Select one of the distribution options to set up the **Safari Settings** configuration. For more information about configuring distribution options, see **Working with Configurations**.
6. Click **Done**.

10.10.8.33. Single App Mode Configuration

Configurations

Licence: Silver

Single app mode restricts iOS devices to the use of the specified app. For example, you might want to set up devices that can use only a custom app your organisation has developed.

Single app mode configuration

Setting	What To Do
Name	Enter a name that identifies this configuration.
Description	Enter a description that clarifies the purpose of this configuration.
Choose App	Select the method to use for selecting the app: • **From App Catalog & System Apps:** Select to search the Ivanti Neurons for MDM app catalog and system apps (pre-installed on Apple devices by default). • Enter the name of the app and select it when it displays in the apps list. • **Enter Bundle ID:** Select to enter the unique identifier for the system app you want to select. Use this option if you cannot find the system app using the **From App Catalog & System Apps** option.
Disable Touch	Select to disable the touch screen.
Disable device rotation	Select to disable device rotation sensing.
Disable volume buttons	Select to disable the device's volume buttons.
Disable ringer switch	Select to disable the device's ringer switch.
Disable sleep wake button	Select to disable the device's sleep/wake button (top right on device rim).
Disable auto lock	Select to prevent the device from going to sleep after an idle period.
Enable voice over	Select to enable the VoiceOver screen reader (accessibility feature).
Enable zoom	Select to enable Zoom (accessibility feature).
Enable invert colours	Select to enable the invert colours adjustment (accessibility feature).
Enable assistive touch	Select to enable AssistiveTouch (accessibility feature).
Enable speak selection	Select to enable Speak Selection (accessibility feature).
Enable mono audio	Select to switch from stereo to mono audio (accessibility feature).
Voice over adjustments	Select to allow device users to make VoiceOver adjustments.
Zoom adjustments	Select to allow device users to make Zoom adjustments.

Setting	What To Do
Invert colours adjustments	Select to allow device users to invert colours.
Assistive touch adjustments	Select to allow users to make AssistiveTouch adjustments.

For more information, see **How to create a configuration**.

10.10.8.34. Software update recommendation cadence configuration

Administrators have an option to allow users to view and update the devices to highest numbered (most recent) release or lower numbered (oldest) release or both.

Applicable to: iOS and iPadOS14.5+ (supervised)

Procedure

1. Go to Configurations > +Add.
2. Type Software update recommendation in the search field, and then click the Software Update recommendation cadence configuration.
3. Enter a Name and Description of the configuration.
4. Select the required configuration setup from the drop-down:
    - Present both software update versions
    - Present the lower numbered (oldest) software update version
    - Present only the highest numbered (most recent) software update version
5. Click Next.
6. Select Enable this configuration option.
7. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
8. Click Done.

10.10.8.35. Start menu and Taskbar

You can define the Start menu layout for your users to define applications that are safe to use and remove applications that are not required. The Windows 10 and 11 versions support different features, as the Start menu layouts are different.

To set Start menu and Taskbar configuration:

1. Go to **Configuration > +Add**.
2. Select **Windows Start Menu & Task Bar** configuration.
3. Enter a name for the configuration.
4. Select the Windows-specific version.
5. **Windows 10 devices**:
   In the **Configuration Setup** section, configure the following settings:
   Setting
   What To Do
   Name
   Enter a name that identifies this configuration.
   Description
   Enter a description that clarifies the purpose of this configuration.**Select Golden Device**
   Select the Windows 10 device that has the apps provisioned in its Start menu and Taskbar.
6. Click **Fetch Start Menu Layout from Device** and configure the following options.
7. **Setting**
   What To DoStart menu and Taskbar Layout
   Select the any of the following options for hiding the list of apps.
   - None
   - Hide all apps list
   - Hide all apps list, and disable "Show app list in Start menu" in Settings app
   - Hide all apps list, remove all apps button, and disable "Show app list in Start menu" in Settings app

Start menu layoutCustomise Start menu
Click **Yes** to customise Start menu and layout parameters.**TaskbarCustomise Taskbar**Click **Yes** to customise Taskbar**Remove existing pinned Taskbar shortcuts before adding the custom ones**Click **Yes** to remove the existing pinned Taskbar shortcut before adding the custom Taskbar.**App Type**Specifies the type of app.**App**Specifies the ID of the app.**Restore**
Click the **Restore** link to restore the Taskbar from the original Golden device taskbar.
Click and drag the arrow icon in the row to move the position(up or down)the specific row.
Click the delete icon to delete the row.
Click the **Add New** button to add a new row.

8. **Windows 11 devices**
   In the **Configuration Setup** section, configure the following settings:
   Setting
   What To Do
   Name
   Enter a name that identifies this configuration.
   Description

Enter a description that clarifies the purpose of this configuration.**Select Golden Device**
Select the Windows 11 device that has the apps configured in the PINNED section of its Start menu.**Start Menu and Taskbar LayoutStart menu and Taskbar Layout**
Select one of the following options to view the search option in the taskbar:

- **Hide**
- **Search Icon**
- **Search Icon and Label**
- **Search Box (Default)**

Select the checkbox **Hide Task View** to hide the task view.**Most Used Apps**
Select one of the following options to configure the most used apps in the Start menu:

- **Don't enforce visibility of list of most used apps in Start.**
- **Force showing of list of most used apps in Start.**
- **Force hiding of list of most used apps in Start.**

The checkbox **Allow Pinning to Task bar** is selected by default.
Select the checkbox **Hide Recommended Section** to hide all the recommended sections.
Due to a vendor issue, the **Hide Recommended Section** checkbox will not have a visible impact on the device even after the user logs off or logs in. Currently, you can't hide the Recommended section.**TaskbarApp Type**
Select one of the following options to specify the type of app:

- **App User Model ID**
- **Desktop Application Link Path**

AppSpecifies the ID or path of the app.**Restore**
Click the **Restore** link to restore the Taskbar from the original Golden device taskbar.
Click and drag the arrow icon in the row to move the position (up or down) the specific row.
Click the delete icon to delete the row.
Click the **Add New** button to add a new row.

9. Click **Fetch Start Menu Layout from Device**.
10. After fetching settings from the Golden Device, all apps configured in the PINNED section of the start menu will be displayed for the administrator to review.
    Click **Next** and distribute the configuration to all the applicable device and user groups.

> Due to a vendor issue, when the configuration is undistributed, Pinned apps will remain as originally configured. However, when a new configuration is distributed, the previous layout will be overridden, and the new layout will be applied.

10.10.8.36. System Update Configuration

Administrators can limit device users from managing system updates on Android 6.0 devices or supported newer versions. This feature is applicable only to Android Enterprise devices.

To configure:

1. Go to **Configuration > +Add**.
2. Select **System Update** configuration.
3. Enter a name for the configuration.
4. Enter a description.
5. In the Configuration Setup section, configure the following options:

Setting	Description
Automatic	Silently apply the system update whenever new firmware is available.
Postpone	Postpones the installation of system updates for 30 days. After the 30-day period has ended, the system prompts the device user to install the update.
Windowed (Local Time)	Schedule a time period to silently apply the system update. Select the **Start Time** and **End Time** hours.
Manual OS Update (Android 10+) Not applicable or supported on Samsung and Zebra devices	Select to perform OS update manually on limited number of devices before rolling out the update for all devices. **Firmware File** - Select **Custom Attribute** or **HTTPS URL** option. Enter the following details: • Firmware location - If you have selected **Custom Attribute** as the Firmware File option, you need to provide the custom attribute that was used for File Transfer. Firmware file can be self-hosted or can be uploaded to Ivanti Neurons for MDM using the File Transfer configuration. Please refer to the **File Transfer Configuration** for details. Uploading files greater than 50 MB to Ivanti Neurons for MDM requires an add-on license. • Description (optional) • Fingerprint (mandatory) - To validate that the intended OS version is installed on the device. Fingerprint can be found in the OTA file by unzipping the OTA folder and opening the /META-INF/com/android/metadata file. Search for an entry similar to the one below: "post-build=google/xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxxxx:user/release-keys" In the above entry, **google/ xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxx:user/release-keys** is the fingerprint and TQ3A.230805.001.S1 is the build ID(Build ID is the 4th value from left in the values separated by '/' in fingerprint). • Checksum (optional) **Update Settings** → **OS Update Request** - The settings within this section are same for Zebra Firmware Configuration. Please refer to the *Zebra Firmware Configuration* section in this table. If you select **HTTPS URL** as the Firmware File option, you need to provide the following information: • Firmware Location - Enter the path from which the firmware can be downloaded without requiring any authentication. Description (optional) • Fingerprint (mandatory) - To validate that the intended OS version is installed on the device. • Checksum (optional) You will have the **Initiate Download Request** and **During Download Conditions** sections in addition to the "**OS Update Request**" section. The options available under the **Initiate Download Request** and **During Download Conditions** sections are same as they are under the **Zebra Firmware Configuration** section. Once system update in device starts after download, restarting the device in between an update aborts the update process.
Freeze Period	Freezes the system update for a specified period. This option is applicable for Android 9.0+ devices. Click **Add Freeze Period**. Select the **Start Date** and the **End Date** for the freeze period.

Setting	Description
	The freeze period cannot be more than 90 days and you can add multiple freeze periods. The next freeze period can be selected only after 60 days from the previous calendar end date. To delete a freeze period click on the Delete icon.
Zebra Firmware Configuration	Select **Configure Zebra OTA** to upgrade or update the operating firmware of the Zebra devices (running on Android version 8.0 or supported newer versions). This is applicable only to Device Owner modes. To configure Zebra OTA updates, you must enable Ivanti Neurons for MDM OTA service under **Admin>Firmware Management>Zebra OTA** and Zebra devices must be present on Ivanti Neurons for MDM. You must enter your Zebra credentials in the popup. To re-create your credentials, contact Zebra directly. When this option is selected, the list of registered Zebra devices are displayed. To select and apply the firmware to the device model: 1. In the **Action** column for the Zebra device, perform any of the following actions: ◦ **None**: No action will be performed for the device model. ◦ **Full Upgrade**. In the **Select Target Zebra Firmware** window, select the full upgrade firmware version to be applied to the device model. During the **Full Upgrade** process, only port 443 is needed. In the **Search** field, you can type the characters of a build ID to search for upgrades based on build ID. The build IDs are sorted and displayed in descending order (latest on top). The **Patch Upgrade** option will **NOT** be available for Android 11+ devices. 2. Configure any of the following options: **Initiate Download Request** - These conditions will be evaluated by the Go app. ◦ **Minimum required battery level**: Move the slider to set the minimum required battery level from the available range. ◦ **Require device to be charging** : Select this option to keep the device in charging mode during the process. ◦ **Download schedule** : Select this option to create a schedule to initiate download request and file download. ◦ The **Require device idle**, **Require charging**, and **Allow downloaded over metered network** are passed to Android Download Manager. Go app will add the download request to Android Download Manager in mentioned window with the above parameters. **Apply schedule for download** - Select the **Day(s) of the week** and the **Start time** and **End time** to schedule the download. Multiple days can be selected to schedule the download. For example, if Saturday and Sunday is selected with start and end time between 12:00 AM to 11:00 PM, the download is performed in the Zebra devices only during this time period for the selected day(s). In the Go app, the download begins as scheduled when the configuration is applied to the device. There is no download end time limit, and it may complete at a time beyond the scheduled end time. ◦ Apply schedule for update - Select the **Day(s) of the week** and the **Start time** and **End time** schedule the installation of the firmware update. The installation will be postponed if the device battery level is below 32. If no update schedule is configured, the installation begins immediately after the firmware download completes.

Setting	Description
	3. Configure any of the following options: **During Download Conditions**- These conditions will be evaluated by Download Manager. You can make the selection depending on criteria. ◦ **Require device idle** (Selected by default): Allows firmware updates on the device when the device is idle. ◦ **Require charging** (Selected by default): Allows firmware updates on the device when it is in charging mode. ◦ **Allow download over metered network** : Select this option to allow download in Wi-Fi mode. This option is deselected by default. ◦ The **Require device idle**, **Require charging**, and **Allow download over metered network** are passed to Android Download Manager. Go app will add the download request to Android Download Manager in mentioned window with the above parameters. **Allow download to continue outside of specified 'download schedule'** : Select this option to allow download outside of the specified download schedule. **OS Update Request** ◦ **Minimum required battery level** - Select this option to set the minimum battery level that must be available to request OS update. ◦ **Require device to be charging** - Select this option to keep the device in charging mode during the process. ◦ **Create schedule to start OS update on the device** - Select this option to set a schedule at which the OS update will start on the device. In the Go app, the download begins as scheduled when the configuration is applied to the device. There is no download end time limit, and it may complete at a time beyond the scheduled end time. Click **Apply**.
Samsung E-FOTA Configuration	Select **Configure Samsung E-FOTA** to upgrade or update the operating firmware of the Samsung devices (on Knox version 2.7.1 and above). This is applicable only to Managed Device with Work Profile on Company Owned Device modes. If there are no Samsung E-FOTA capable devices are registered, a message informing this information is displayed on the page. To configure Samsung e-FOTA updates, you must activate Samsung e-FOTA license under **Admin>Firmware Management>Samsung E-FOTA**.When this option is selected, the list of registered Samsung devices are displayed. To select and apply the firmware to the device model: 1. In the **Action** column for the Samsung device, perform any of the following actions: ◦ **Latest**: The latest firmware version is applied. This option is selected by default. ◦ **Force**: In the Select Target Samsung Firmware window, select the particular firmware version to be force applied (without user intervention) to the device model. When this action is performed, firmware downloading begins within fifteen minutes. ◦ **Target**: In the Select Target Samsung Firmware window, select the particular firmware version to be applied to the device model.

Setting	Description
	When performing the 'Force' or 'Target' actions, if there are no firmware listed for the device, a message informing this information is displayed on the page. 2. **Enable debug FW** (Optional): When the **Enable Debug FW** option is enabled, and the configuration is applied, the device is upgraded to a dummy firmware. The dummy firmware of the Samsung device firmware allows the admin to test the system update configuration behaviour on the devices, without actually modifying anything on the device. To upgrade to the actual firmware update, instead of the dummy firmware, the admin should ensure that the **Enable debug FW** option is disabled before applying the configuration 3. Click **Apply**.

6. Click **Next**.
7. Select one of the following distribution options:

- All Devices
- No Devices (default)
- Custom

8. Click **Done**.

Samsung E-FOTA Configuration (Decommissioned)

The Samsung E-FOTA configuration is decommissioned in July 2022. So, this configuration will not be available for new devices. The devices with the existing configuration can only deactivate this configuration.

10.10.8.37. Windows 10 Update Management

As an administrator, you can view and approve the updates reported by Windows 10 devices that you want to be updated using Windows 10 Update Management. By using this feature you can prevent unnecessary or untested updates from being installed in devices.

Update Management feature requires devices to be configured with **Software Updates** configuration with **Require update approval** option enabled. Only by applying this configuration to the devices, the devices report updates for installation and wait for approval.

Managing updates

1. Go to the **Admin>Windows Updates**. The following details of the updates are displayed in the page.
   Creation Date: The date when the update was created.**Title**: Describes the type of update along with the Knowledge Base article number.

> When clicked on the update, the description is displayed.

Classification: Classifies the type of update into one of the following categories:

- Critical Updates
- Definition Updates
- Driver Updates
- Security Updates
- Updates
- Upgrade
- Update Rollups

Distribution: The distribution performed for the update. For example, it display **All** when the update is distributed to all the devices.

> If the update is distributed to a certain specific number of groups, it displays the count of the distribution. For example, it displays 3 if the distribution is performed only to 3 groups.

2. In addition, you can view if an update has been distributed to the required devices or not. The following columns have numbers that indicate the number of devices present under different category of the updates:
   - Eligible devices
   - Installed devices
   - Failed devices
   - Reboot pending devices

When you click on any of these numbers, you will be directed to the filtered view on the Devices page to know the status of updates and perform the required actions.
Review the updates and select the update that you would like to distribute to the devices by clicking the check-box for the update.

3. Under **Actions**, click **Set Distribution**.
4. In the **Distribute Windows Update** window, select any of the following distribution options:
   All Devices: Distributes the updates to all the devices.

No Devices: Withholds the updates to be distributed to devices**Custom**: Distributes the updates for the specified device groups.

5. Click **Save**.

Searching and filtering updates

You can search and filter updates based on the following criteria:

- Knowledge base article ID
- Configured distribution

Filtering based on Knowledge base article ID:

1. In the **Windows 10 Update Management** page, type the Knowledge base ID in the quick search field(only the number in the Search field.
   Example: For KB4056892, type 4056892. The update that matches with the search criteria is displayed on the page.

> You can further look for additional information on the update by clicking **Support** and **More Information** link. The **Support** links to the Microsoft web page that provides product support information for the update and the **More Information** links to the Microsoft web page that displays more information on the update, such as the Knowledge Base article.

Filtering based on configured distribution:

In the **Windows 10 Update Management** page, select any of the following filtering options based on the configured distribution:

- **All**: Displays all the updates.
- **Configured**: Displays the list of updates that are distributed to devices.
- **Unconfigured**: Displays the list of updates for which the distribution is not specified.

> Configured and Unconfigured filters are based on the distribution performed and the distribution can also be **None**.

Viewing updates for a device

To view the detailed update information specific to a device:

1. Go to **Devices > Devices**.
2. Click a device name to view the details page.
3. Go to **Updates** tab. The updates for the device that are pending (update approved by the admin but not reported as installed on the device), failed, and installed are displayed.

> You can also see notifications about new Windows updates available in the Notifications page under Dashboard. The notification includes creation date of the notification, number of notifications available and the purpose of the notification. The Windows update notification is also visible in the top right corner of the Admin Portal.

10.10.8.38. Windows app scheduling

Windows Desktop apps can be large, adding extra and extended load on networks and servers during key use times for the enterprise. Windows app scheduling feature allows you to schedule a time to install apps, especially large apps, on devices during a time you choose.

To configure app scheduling:

1. Go to **Apps > App Catalogue**.
2. Click **Add** and select a Windows app and continue with the next steps in **Add App** wizard.
3. In step 5(Configure), click **Install Application configuration settings** to view the **Configuration Setup** page.
4. Select the **Schedule Installation** checkbox.

> **Schedule Installation** checkbox is displayed only when Silent installation is enabled.

5. Select a **Start Time** and a **End Time** to schedule the time to install apps.
6. Select a **Start Date** and a **End Date** to schedule the date to install apps.

> You can also select one of the following two actions that should be performed when the scheduled date is missed: **Install during next check-in** or **Do not install**.

7. Select an App Configuration distribution option: **Everyone with App**, **No One**, or **Custom**.
8. Click **Done**.

> Apps that need to be scheduled should not be added into Apps@Work.
> App scheduling is not applicable for Store apps since silent installation of Store apps is not supported.

10.10.8.39. Windows BIOS Configuration

Administrators can set Windows BIOS settings on Lenovo devices. At least one Lenovo device that supports BIOS settings must be enrolled to set this configuration.

To configure:

1. Go to **Configuration > +Add**.
2. Select **Windows BIOS** configuration.
3. Enter a name for the configuration.
4. Enter a description.
5. In the Choose device model section, select the device model from the drop down list.
6. In the Configuration Setup section, configure the following options:

> The list of settings vary depending on what is available for the specific device model that is enrolled. Please refer to the respective device website for more information.

Setting	What to do
AMT Control	Select any of the following options: • **Disable** • **Enable**
Adaptive Thermal Management AC	Select any of the following options: • **Balanced** • **Maximised Performance**
Adaptive Thermal Management Battery	Select any of the following options: • **Balanced** • **Maximised Performance**
Always On USB	Select any of the following options: • **Disable** • **Enable**
BIOSPasswordAtBootDeviceList	Select any of the following options: • **Disable** • **Enable**
BIOS Password At Reboot	Select any of the following options: • **Disable** • **Enable**
BIOS Password At Unattended Boot	Select any of the following options: • **Disable** • **Enable**
BIOS Update By End Users	Select any of the following options: • **Disable** • **Enable**
Bluetooth Access	Select any of the following options: • **Disable** • **Enable**
Boot Device List F12 Option	Select any of the following options: • **Disable** • **Enable**

Setting	What to do
Boot DisplayDevice	Select any of the following options: • **DisplayPort** • **Dock Display** • **HDMI** • **LCD**
BootMode	Select any of the following options: • **Diagnostics** • **Quick**
Boot Order Lock	Select any of the following options: • **Disable** • **Enable**
BootTimeExtension	Select any of the following options: • **1** • **10** • **2** • **3** • **5** • **Disable**
BottomCover Tamper Detected	Select any of the following options: • **Disable** • **Enable**
CPU Power Management	Select any of the following options: • **Automatic** • **Disable**
Computrace Module Activation	Select any of the following options: • **Disable** • **Enable**
Data Execution Prevention	Select any of the following options: • **Disable** • **Enable**
Ethernet LAN Access	Select any of the following options: • **Disable** • **Enable**
Ethernet LAN Option ROM	Select any of the following options: • **Disable**

Setting	What to do
	• **Enable**
Fingerprint Password Authentication	Select any of the following options: • **Disable** • **Enable**
Fingerprint Pre-desktop Authentication	Select any of the following options: • **Disable** • **Enable**
Fingerprint Reader Access	Select any of the following options: • **Disable** • **Enable**
Fingerprint Reader Priority	Select any of the following options: • **External** • **Internal Only**
Fingerprint Security Mode	Select any of the following options: • **High** • **Normal**
Fn Ctrl Key Swap	Select any of the following options: • **Disable** • **Enable**
FnKeyAsPrimary	Select any of the following options: • **Disable** • **Enable**
FnSticky	Select any of the following options: • **Disable** • **Enable**
IPv4 Network Stack	Select any of the following options: • **Disable** • **Enable**
IPv6 Network Stack	Select any of the following options: • **Disable** • **Enable**
Integrated Camera Access	Select any of the following options: • **Disable** • **Enable**

Setting	What to do
InternalStorageTamper	Select any of the following options: • **Disable** • **Enable**
Keyboard Beep	Select any of the following options: • **Disable** • **Enable**
Lock BIOS Setting	Select any of the following options: • **Disable** • **Enable**
Memory Card Slot Access	Select any of the following options: • **Disable** • **Enable**
Microphone Access	Select any of the following options: • **Disable** • **Enable**
Minimum Password Length	Select any of the following options: • 4 • 5 • 6 • 7 • 8 • 9 • 10 • 11 • 12 • **Disable**
NFFControl	Select any of the following options: • **Disable** • **Enable**
Nfc Access	Select any of the following options: • **Disable** • **Enable**
On By Ac Attach	Select any of the following options: • **Disable** • **Enable**

Setting	What to do
PasswordBeep	Select any of the following options: • **Disable** • **Enable**
PasswordCountExceededError	Select any of the following options: • **Disable** • **Enable**
Physical Presence For Tpm Clear	Select any of the following options: • **Disable** • **Enable**
Physical Presence For Tpm Provision	Select any of the following options: • **Disable** • **Enable**
Rapid Start Technology	Select any of the following options: • **Disable** • **Enable**
SecureBoot	Select **Enable**
Secure Roll Back Prevention	Select any of the following options: • **Disable** • **Enable**
Security Chip	Select any of the following options: • **Active** • **Disable** • **Enable** • **Inactive**
Smart Card Slot Access	Select any of the following options: • **Disable** • **Enable**
SpeedStep	Select any of the following options: • **Disable** • **Enable**
Startup Option Keys	Select any of the following options: • **Disable** • **Enable**
TXT Feature	Select any of the following options:

Setting	What to do
	• **Disable** • **Enable**
Total Graphics Memory	Select any of the following options: • **256 MB** • **512 MB**
TouchPad	Select any of the following options: • **Automatic** • **Disable**
TrackPoint	Select any of the following options: • **Automatic** • **Disable**
USB30 Mode	Select any of the following options: • **Automatic** • **Disable** • **Enable**
USB BIOS Support	Select any of the following options: • **Disable** • **Enable**
USB Port Access	Select any of the following options: • **Disable** • **Enable**
Uefi Pxe Boot Priority	Select any of the following options: • **IPv4 First** • **IPv6 First**
VTd Feature	Select any of the following options: • **Disable** • **Enable**
Virtualisation Technology	Select any of the following options: • **Disable** • **Enable**

Setting	What to do
Wake On LAN	Select any of the following options: • **AC Only** • **AC and battery** • **Disable** • **Enable**
Wireless LAN Access	Select any of the following options: • **Disable** • **Enable**
Wireless WAN Access	Select any of the following options: • **Disable** • **Enable**

7. Click **Next**.
8. Select one of the following distribution options:
   - All Devices
   - No Devices (default)
   - Custom
9. Click **Done**.

10.10.8.40. Windows BitLocker

As an administrator, you can bulk update of recovery key for a set of encrypted Windows 10 devices by uploading an Excel file with the device GUID and recovery password.

To upload the Excel file for the bulk update of recovery key:

1. Go to the **Admin>Windows BitLocker**.
2. Click **Download sample csv file** to download the sample CSV file to download and view an example of .csv file.
3. Create and add the records for the BitLocker recovery keys .csv file.
4. Click **Upload recovery passwords.**
5. Click **Choose File** to upload the .csv file you have created.
6. Click **Upload**. Uploading a new file with previously uploaded keys will overwrite the old entries.

> A maximum of 1000 records can be submitted in each upload. After a successful upload, you can view the individual keys in the device details of the specific device.

10.10.8.41. Windows Kiosk Configuration

Using Windows Kiosk configuration, you can configure single or multiple-app kiosk on Windows 10 devices. By applying this configuration, the kiosk users are restricted from accessing any features outside the kiosk apps. This configuration requires Windows Bridge to be enabled.

The following are 3 modes in which the configuration can be applied.

- Single Application
- Multiple Applications (fetch list of application from Windows device)
- Multiple Applications (select an existing layout from Start Menu configuration)

> Applications used for a Windows Kiosk configuration should be already present on a device before entering into a configured Windows Kiosk mode.

To configure Windows Kiosk configuration:

1. Go to **Configuration > +Add**.
2. Select **Windows Kiosk** configuration.
3. Enter a name for the configuration.
4. Enter a description.
5. In the Configuration Setup section, specify the remaining settings as described in the following table.

Setting	What To Do
Select Kiosk mode: Select any of the following 3 options.	
Single Application	Select this option to configure single application kiosk mode for a device. 1. In the **Select Windows Device (optional)** section, choose a Windows 10 device. Click **Fetch Apps from Device** to fetch the list of apps from a device. The device you select should be under your supervision and requires a check-in to successfully fetch app data. To skip these steps, select the **Skip this step. You can change your mind later if desired** checkbox. 2. Click **Add From Fetched App List** to add apps from the fetched list. 3. Select a single app by clicking the radio button in the **Name** column of the app. Click **Add New** to add a new app to the list. To delete an app from the list, click on the Delete icon.
Multiple Applications (Fetch list of Applications from Windows device)	Select this option to configure multiple applications kiosk mode for a device. 1. In the **Select Windows Device (optional)** section, choose a Windows 10 device. Click **Fetch Apps from Device** to fetch the list of apps from a device. The device you select should be under your supervision and requires a check-in to successfully fetch app data. To skip these steps, select the **Skip this step. You can change your mind later if desired** checkbox. 2. In the **Kiosk Apps and Start Menu Layout**, click **Add From Fetched App List**. The **Select Kiosk App** window is displayed. Select the app(s) from the fetched list and click **Use Selected App**. 3. In the Additional Allows Apps section, click **Add From Fetched App List**. The **Select Kiosk App** window is displayed. Select the app(s) from the fetched list and click **Use Selected App**. Additional allowed apps are the apps that are considered as dependencies for the selected apps in the **Kiosk Apps and Start Menu Layout**.Without 'allowed apps', the OS does not allow to run this application even when the application icon is displayed in Start Menu. 4. Click **Add New** to add a new app to the list. To delete an app from the list, click on the Delete icon. You can drag and move an app in the list to any position in the list. 5. In the **Multiple App Other settings**, select the required options: ◦ **Hide Power Button** ◦ **Hide User Tile** ◦ **Hide Taskbar** In Microsoft Windows 11, the multi app kiosk mode option "**Hide Taskbar**" is not supported.
Multiple Applications (Select an existing layout from Start Menu Configuration)	If you have created a Start menu layout configuration, you can import the configuration and use it to configure the multiple-application mode by selecting this option. 1. In the **Select Layout** section, Select a layout that has been previously setup as a Start Menu Configuration. Previously created configurations with applicable layout parameters are displayed in the drop-down list below.

Setting	What To Do
	2. In the Multiple App Other settings, select the required options: ◦ **Hide Power Button** ◦ **Hide User Tile** ◦ **Hide Taskbar** In Microsoft Windows 11, the multi app kiosk mode option "**Hide Taskbar**" is not supported.

6. Click **Next**.
7. Select one of the following distribution options:

- All Devices
- No Devices (default)
- Custom

8. Click **Done**.

> For the configuration to take complete effect, the device should be rebooted after applying or updating a Windows Kiosk configuration. Depending on applications for multi-app kiosk configuration, it might be required to reboot a device for the second time. Some icons may be missed on the first login, but the missing icons will be displayed on login after the second reboot.

Device has to be rebooted after applying, deleting or updating a Kiosk configuration. It can be done with Restart/Shutdown device command from the device action menu. Without reboot:

- Device is not entered into Kiosk mode automatically after applying a Kiosk configuration.
- Device does not exit from Kiosk mode automatically after deleting an applied Kiosk configuration.
- Device does not change the running Kiosk configuration.

If a device with an applied kiosk configuration receives an updated configuration, Windows OS on the device removes an existing kiosk user and recreates a new kiosk user with a new kiosk configuration. The session for the current user should be ended explicitly with reboot of the device.

It is preferable to configure with '.lnk' files for a multi-app kiosk configuration and '.exe' for a single-app kiosk configuration. An imported Start Menu configuration from a device uses the '.lnk' format. Start Menu items created manually for '.exe' applications sometime could be not displayed in Start Menu of multi-app kiosk configuring depending on '.exe' application.

For example, Windows Media Player can be added to Start Menu using one of the following '.lnk' files:

- %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Media Player.lnk
- %ALLUSERSPROFILE%\Microsoft\\Windows\Start Menu\Programs\Windows Media Player.lnk

If this app is added directly with any of the following '.exe' file, a corresponding icon will not be displayed, even the first '.exe' path is used internally in the above '.lnk' files:

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
- C:\Program Files\Windows Media Player\wmplayer.exe

For single-app kiosk configuration, you can add arguments to exe file. E.g. '%ProgramFiles%\Internet Explorer\iexplore.exe -k www.bing.com'. However, the icon for exe app with arguments are not displayed in the Start Menu in case of multi-app configuration.if you need an exe app with arguments in multi-app kiosk configuring, use '.lnk' file which can have arguments internally. '.lnk' does not work in case of a single-app kiosk configuration.

Dependencies in multi-app kiosk mode

Win32/64 applications could require dependencies added to Additional Allowed Apps' section in case of multi-app kiosk mode. 'Additional Allowed Apps' are not required for a single-app kiosk mode.

Example 1: For Windows Media Player app, the following dependencies are required in multi-app kiosk mode:

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\setup_wm.exe

The first dependency is the app binaries called from corresponding ".lnk" file. The second one is one-time wizard called from the first dependency.

Without 'Allowed Apps', OS does not allow to run this application even when the application icon is displayed in Start Menu.

Example 2: For Internet Explorer, its icon is displayed in Start Menu if it is configured with any item from the following list:

- %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 requires the following dependencies:

- 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

The first dependency is app binaries required for '.lnk' item only, the other dependencies for one-time wizard. Without the first dependency, OS blocks the app with the popup. Without other dependencies, the application is closed just after startup without any additional notifications from OS.

10.10.8.42. Windows Licence Configuration

The Windows Licence configuration upgrades the operating system on the device such as Windows 10 Pro to Windows 10 Enterprise. In addition, this configuration provides the capability to activate or change the product key of Windows 10 desktop devices.

To upgrade a Windows licence:

1. Go to **Configuration > +Add**.
2. Select **Windows Licence** configuration.
3. Enter a name for the configuration.
4. In the **Configuration Setup** section, type the Windows **Product Key**.
5. Click **Next**.
6. Select one of the following distribution options:
    - All Devices
    - No Devices (default)
    - Custom
7. Click **Done**.

11. Policies

Policies define requirements for devices, as well as what will happen if a device does not comply with requirements. Each policy consists of a rule and a compliance action (what happens if the rule is violated). Use the **Policies** page to select, set up, and distribute policies.

> With the automated device check-in process, please note the following changes:

- Devices checked-in during the last 90 days only will be evaluated.
- Only Forced Check-in command will be triggered on devices that were checked-in after 90 days and before one year.
- No action on devices that were not checked-in during the last one year.

This section contains the following topics:

- Working with Policies
- Custom Policy
- Monitoring and Controlling Allowed Apps
- Prioritising Policies
- Windows Hardware policy

11.1. Working with Policies

This section contains the following topics:

- Implement policies
- Compliance Actions
- Finding an existing policy
- Adding a policy
- Editing a policy
- Deleting a policy

Implement policies

Policies define requirements for devices, as well as what will happen if a device does not comply with requirements. Each policy consists of a rule and a compliance action (what happens if the rule is violated). Use the **Policies** page to select, set up, and distribute policies.

The following policy types are available:

Type	What It Does
Compromised Devices	Priority (1 = highest) Violation 1 Plugin compromised 2 Client tampered 3 Unknown device manufacturer: unknown 4 Suspicious folder detected: [path] 5 Suspicious binary found at: [path] 6 Folder /data is browsable OR Folder /data/data is browsable 7 Found /system/app/Superuser.apk 8 Package manager compromised 9 Suspicious app found: [package] Flags devices that have been jailbroken (iOS) or rooted (Android). To view the violation reason why the system flagged an Android device as compromised due to rooting: 1. Click the **Policies** tab 2. Click the **Compromised Devices** link. 3. Click the **Active Violations** tab. 4. Check the violation reason in the Violation column. To view the violation reason why the system flagged an Android device as compromised due to rooting: 5. Click the **Policies** tab. 6. Click the **Compromised Devices** link. 7. Click the **Active Violations** tab. 8. Check the violation reason in the **Violation** column. It will be one of the following reasons:
Data Protection/Encryption Disabled (macOS only)	Flags macOS devices that do not have a passcode or encryption enabled.
International Roaming	Flags devices that might be incurring international roaming charges. Status is refreshed when the device checks in. For iOS, the service uses the roaming flag as set and reported by iOS. The compliance action is triggered by the first violation only.
MDM/Device Administration Disabled	If the device is MDM-disabled, then it will not be evaluated for any other policies or delta processing of configurations or apps further during check-ins.
Out of Contact	Flags devices that have been out of contact with Ivanti Neurons for MDM for the specified time range. Choose the actions to take if the device has not checked in for a specified range of hours (2-3 to 23-24) or number of days.
MI Client Out of Contact (iOS only)	Flags Ivanti Neurons for MDM clients that have been out of contact with Ivanti Neurons for MDM for the specified time range.

Type	What It Does
	Choose the actions to take if the client has not checked in for a specified range of hours (2-3 to 23-24) or number of days. This is also applicable for devices registered via iReg. The policy marks a device as non-compliant if there is no client or if the client has not checked-in for a defined period of time.
Allowed Apps	Flags devices that violate rules about which apps are allowed or required.
Custom Policy	Creates a custom policy based on conditions and related actions you specify.

Compliance Actions

The following compliance actions are available:

Compliance Action	What It Does
Monitor	Flags the device in the Ivanti Neurons for MDM Devices page. By default, this action is turned on.
Block	Instructs Access and /or Sentry to block a device if the device tries to access a resource via Sentry or Access after the policy has been violated as of the last check-in details.

Send message to user	• Flags the device in the Ivanti Neurons for MDM Devices page.
	• Sends an email to the device owner.
	• In addition to the existing policies, the "**Use the Compliance Policy Email Template**" toggle is now available for the following policies as well:
	  ◦ Data Protection/Encryption Disabled
	  ◦ International Roaming
	  ◦ MDM/Device Administration Disabled
	  ◦ Out of Contact
	  ◦ MI Client Out of Contact
	  Sends a push notification to the device.

Quarantine	• Removes most configurations from the device. ◦ Exceptions: passcode configurations, Wi-Fi configurations for Wi-Fi-only devices, Restriction configurations (iOS). • Removes all apps installed by Ivanti Neurons for MDM. • Removes all content distributed by Ivanti Neurons for MDM, including iBook and ePub files. • Blocks access to Ivanti Neurons for MDM catalogs. • Suspends prompts for installing additional apps. • Blocks access to AppConnect-enabled apps. • Includes support for AppConnect-enabled apps. • If turned on, suspends personal apps on the personal side of the quarantined device to indicate that device user needs to address the compliance issues on the device to make it functional. Supported on Android 11+ Devices provisioned as a Work Profile on Company Owned Device.
Additional Quarantine Actions (Optional):	**Block New App Download** - Prevents download of any new apps to the device. **Quarantine Managed Applications** - Removes Ivanti Neurons for MDM managed apps from the device and enables the Block New App Downloads option to block the apps from being re-installed on the device. Select one of the following options: • **All Applications** • **Remove all apps except the following** - Remove all applications except the ones that are added to the application list. • **Designated Applications** - Add one or more apps by lookup or manually (using Bundle ID or Package Name). Click the **View Apps** tab to review the list of added apps. The Block App Store Access default quarantine action is no longer available. On certain devices, the Quarantine action will not remove the application from the device due to certain

Compliance Action	What It Does
	device limitations. By default, this option is selected (for all three: All Applications, Remove all apps except the following and Designated Applications) and cannot be de-selected. This blocks the apps from being re-installed on the device. **Remove configurations** - Removes Ivanti Neurons for MDM configurations from the device. Select one of the following options: • **All Configurations** • **Designated Configurations** - Select one or more configurations from the list or search for them. Click the **Selected Configurations** tab to review the list of selected configurations. **Push Designated Configurations** - Distribute designated configurations as part of custom compliance. This list contains configurations meeting the following criteria: • Enabled configuration • Non-system configuration • Quarantinable configuration • Configurations created in the current space or delegated from the default space For the list of non-quarantinable configurations, see **Non-quarantinable configurations.** **Remove Content** - Removes all content and media associated with the apps distributed by Ivanti Neurons for MDM from the device. **Suspend Personal Apps** - Suspend apps on the personal side of the quarantined device to indicate that device user needs to address the compliance issues on the device to make it functional. Supported on Android 11+ Devices provisioned as a Work Profile on Company Owned Device.

Finding an existing policy

You can use filters and the search feature in the Policies page to find one or more existing policies.

Procedure

1. Go to **Policies**.
2. To filter a list of policies that match certain criteria, click **Filters**.
3. Select one or more filter criteria.
4. To search for an existing policy by its name, enter the policy name in the **Search** field.

Adding a policy

Procedure

1. Go to **Policies**.
2. Click +**Add** (upper right-hand side).
3. Select a policy type.
4. Complete the settings.
5. Select the device groups you want to receive this policy.

> You can distribute to a maximum of 100 configuration files at once.

6. Click **Done**.

Editing a policy

Procedure

1. Go to **Policies**.
2. For the required policy, click the **Edit** (pencil) icon under the Actions column.
3. Make your changes.
4. Save the changes.

Deleting a policy

Procedure

1. Go to **Policies**.
2. For the required policy, click the **Remove** icon under the Actions column.
3. Click **Yes** to confirm.

If you cannot see the Policy page, it might be that you do not have the required permissions. You need one of the following **roles**:

- Device Management
- Device Read Only

For more information, see **Prioritise policies**.

11.2. Custom Policy

Policies

Licence: Platinum

Eligible devices: Android, iOS, macOS, Windows.

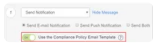
Allows you to create a custom policy based on device and user attributes, section criteria, values, and compliance actions you specify.

> Note: Even Android Security Patch level setting can be used when defining a custom policy.

Adding a custom policy

1. Go to **Policies**.
2. Click **+ Add**.
3. Select **Custom Policy**.
4. Provide a name for the custom policy.
5. Click **+ Add Description** to enter additional details if desired.
6. Use the Rule Builder to define conditions that trigger actions when the conditions evaluate as true. See Understanding_the_conditions_settings for guidance on creating the conditions. The Ivanti Neurons for MDM administrator displays the number of duplicate user groups and the corresponding number of GUIDs to identify duplicate groups, when the User Group Name attribute is selected in the rule builder. Also, a table under this rule displays the list of the duplicate user groups and their details such as User Group Name, GUID, Source and distinguished name (DN).
7. Select one of the compliance actions (see Default Actions below) to take when the specified conditions are met. Adding the action "**Wait**" in between other actions provides a way to allow device users to fix their device and get it back into compliance before additional actions are taken. As an example, you may want to send a warning message and wait 24 hours before applying a quarantine action.
8. Select the **Send a notification when the device comes back into compliance** option, which is turned off by default.

- **Send Email Notification** - Sends an email to the device user's email address notifying them when the device comes back into compliance.
  - Turn on the **Use the Compliance Policy Email Template** option to insert the message you configure here into the policy notification email template you configure as described in **Customising an email template** in **Branding Email Templates**. See **Configuring and using policy compliance notification emails** for an overview.

    
  - You can customise the messages by including optional substitution variables to provide recipients more details about policy violations and other relevant information. Click the following attribute types to display the complete list of variables:
    - Policy Attributes including $, $, and $.
    - User Attributes including $, $, and $.
    - Device Attributes including $, $, and $.
    - Custom Device/User/LDAP attributes that are created from the **Admin > Attributes** page.
- **Send Push Notification** - Sends a push notification to the device when the device comes back into compliance.

- **Send Both** - Sends both a push notification to the device and an email to the device user's email address notifying them when the device comes back into compliance. You can customise the messages by including optional substitution variables to provide recipients more details as described previously for the Send Email action.

9. Specify the following options from the table to notify the administrators and the registered device owners if the device owners violate the policy rules:

Option	Description
Subject	Enter the subject text. For example, "You have violated a policy!."
Body	Enter the message as needed. For example, "Action required!."
Send Email Notification to Admins only	Select this option to send email notification to administrators only.
CC to administrators	This textbox will not be available if you have selected the "Send Email Notification to Admins only" option.
Enter email addresses of administrators	Enter the e-mail ID of the administrators. Use a semicolon (;) as a separator to add multiple e-mail addresses.
Preview E-Mail	Click the **Preview E-Mail** button to view the e-mail address.

10. Click **Next** to save the policy details.

Default actions:

1. Click the **Yes** check box to affirm that you understand that if this policy has previously been triggered on a device, adding the tiered policy will reset the policy and any compliance actions that had previously been applied. The new custom policy takes effect upon the next device check-in. If you selected the Retire action, then click **Yes** to affirm that you understand that you cannot undo the action.

- **Monitor** - Currently always selected. Sentry version 9.0.0 or later is required to utilise the tiered compliance actions.
- **Do Nothing**
- **Send Notification**
- **Send Email** - Sends an email to the device user's email address notifying them that the device is out of compliance.
  - You can use the policy notification email template as described above.
  - You can customise the messages by including optional substitution variables to provide recipients more details about policy violations and other relevant information. This provides users of non-compliant devices with relevant information about the policy violation so they can take remedial actions. Click the following attribute types to display the complete list of variables:
    - Policy Attributes including $, $, and $.
    - User Attributes including $, $, and $.
    - Device Attributes including $, $, and $.
    - Custom Device/User/LDAP attributes that are created from the **Admin > Attributes** page.
- **Send Push Notification** - Sends a push notification to the device that the device is out of compliance.
- **Send Both** - Sends both a push notification to the device and an email to the device user's email address notifying them the device is out of compliance. You can customise the messages by including optional substitution variables to provide recipients

more details as described previously for the Send Email action.

- **Block** - Uses Sentry to block managed devices from accessing email and AppConnect-enabled applications. Sentry version 9.0.0 or later is required to utilise the block action.
- **Retire** - Retires the device. **This action cannot be undone**. For example, there can be a rule to retire the devices for all the disabled users by using the User Enabled condition.
- **Wait** - Delays action for a specified time period (hours or days) to allow users to remediate the violation before additional actions are taken if the device remains in a non-compliant state.
- **Quarantine** - Removes access to apps, content, and servers as per the following actions:

(Optional) Additional Quarantine Actions	Description
Quarantine Managed Applications	Removes Ivanti Neurons for MDM managed apps from the device and enables the Block New App Downloads option to block the apps from being re-installed on the device. Select one of the following options: • **All Applications** • **Designated Applications** - Add one or more apps by lookup or manually (using Bundle ID or Package Name). Click the **View Apps** tab to review the list of added apps. The Block App Store Access default quarantine action is no longer available. On certain devices, the Quarantine action will not remove the application from the device due to certain device limitations.
Block New App Downloads	Prevents download of any new apps to the device. Select one of the following options: • **All Applications** • **Designated Applications** - Add one or more apps by lookup or manually (using Bundle ID or Package Name). Click the **View Apps** tab to review the list of added apps. The Block App Store Access default quarantine action is no longer available. By default this option is selected (for both All Applications and Designated Applications) and cannot be de-selected. This blocks the apps from being re-installed on the device.
Remove Configurations	Removes Ivanti Neurons for MDM configurations from the device. Select one of the following options: • **All Configurations** • **Designated Configurations** - Select one or more configurations from the list or search for them. Click the **Selected Configurations** tab to review the list of selected configurations.
Push Designated Configurations	Distribute designated configurations as part of custom compliance. This list contains configurations meeting the following criteria: • Enabled configuration • Non-system configuration • Quarantinable configuration • Configurations created in the current space or delegated from the default space For the list of non-quarantinable configurations, see **Non-quarantinable configurations.** For more information, see the **Pushing a designated configuration** section after this procedure.
Remove Content	Removes all content and media associated with the apps distributed by Ivanti Neurons for MDM from the device.
Suspend Personal Apps	Suspend apps on the personal side of the quarantined device to indicate that device user needs to address the compliance issues on the device to make it functional. Supported on Android 11+ Devices provisioned as a Work Profile on Company Owned Device.
Default Quarantine Actions - these actions are always performed.	

(Optional) Additional Quarantine Actions	Description
Block App Store Access	Prevents the device from accessing app stores via Ivanti Neurons for MDM.
Block Content Store Access	Prevents the device from accessing content store via Ivanti Neurons for MDM.
Block AppConnect	Prevents the device from using AppConnect features.
Block AppTunnel	Prevents applications on the device from accessing content and servers via AppTunnel.
Block ActiveSync	Prevents the device from accessing email via the ActiveSync server.

2. Click **Next** to configure which devices the policy and actions will apply to.
3. Click **Done**.

The following table illustrates the quarantine behaviour on various Android devices when the Ivanti Neurons for MDM is the initiator of the quarantine action:

Devices	Quarantine behaviour
Samsung devices in Device Admin mode via the Go client app	• Uninstall both managed public and in-house apps • Remove certain profiles (excluding Mobile Threat Defense and others)
Non-Samsung devices in Device Admin mode via the Go client app MAM via the AppStation app	• Do not support uninstalling or hiding both managed public and in-house apps • Remove certain profiles (excluding Mobile Threat Defense and others)
Android Enterprise via the Go client app	• Hide both managed public and in-house apps • Remove certain profiles (excluding Mobile Threat Defense and others)

Pushing a designated configuration

Distribute designated configurations as part of custom compliance. Configure the Custom Policy to distribute a set of configurations when a device goes out of compliance. Reset the device to its previous state as part of remediation action when a device status changes from non-compliant to compliant status.

> An error occurs when an administrator tries to delegate a custom policy that has non-delegated configurations under the Push Designated Configurations tab.

The following are the behaviours when configurations are pushed via custom policies under certain conditions:

Condition(s)	Behaviour
Two configurations of same type are selected which have priority set	Configuration with the higher priority will be pushed to the device.
Two configurations of same type are selected which do not have priority set	Both configurations will be pushed to device. May result in unexpected behaviours.
When device already has a configuration of the same type which supports priority defined in the Custom Policy	The configuration defined in the Custom Policy will take precedence and will be pushed to the device. The one existing on the device will be removed irrespective of priority (even if its priority is higher than the one defined in custom policy).
When device already has a configuration of the same type which does not support priority defined in the Custom Policy	The configuration defined in the Custom Policy will be pushed to the device. Both configurations will be present on the device. May result in unexpected behaviours.
If the priority of a configuration is changed after the Custom Policy is created	On device check-in, the configuration with the highest priority will be pushed if it is part of the Custom Policy.
When both conditions are met: • Condition A: When a device with a violation has had a configuration pushed as part of a custom policy (and it took priority over a configuration of the same type already on the device). • Condition B: Violation has been re-mediated and device is no longer in quarantine	The configuration defined in the Custom Policy will be removed and the one of the same type on the device before quarantine will be pushed through the application of existing device groups, reverting the device back to its original state.

In the Quarantine action, if you select Remove Configurations along with Push Designated Configurations, note the following rules:

- Remove all configurations + Push Designated Configurations: In this scenario, all configurations from the device will be removed and the configurations selected under Push Designated Configurations will be pushed to the device.
- Remove designated configuration(s) (in one custom policy) + Push Designated Configuration(s) (in another custom policy) with common configuration(s) in the selection of both: As the configurations are selected in two different compliance policies, the most restrictive approach would be taken i.e. the configuration(s) will be removed from the device.

You can delegate a custom policy from the default **space** to a custom space. For a custom policy to be delegated, the configurations mentioned in the custom policy under the Push Designated Configurations tab need to be delegated to spaces.

On the **Devices** page, you can click the name of a device to visit the device details page. Under the Configurations tab, the Distribution Method column indicates the distribution method for a configuration pushed to the device. It can be either "Device Group" or "Compliance Action."

On the Configurations page, for each configuration, Ivanti Neurons for MDM displays a count of devices that received the configuration via device group and via compliance action.

Understanding the conditions settings

The following table describes some fields available to build rules:

UI Field	Description	Possible values	Supported Platforms
APNS Capable	This field indicates whether the device is APNS capable.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	iOS/macOS/Android
Anti-phishing native status	This field displays the anti-phishing native status	Possible operators are: • is equal to • is not equal to Possible values are: • Not Enabled • N/A • Enabled • Unknown	iOS/Android
Anti-phishing status	This field displays the anti-phishing status	Possible operators are: • is equal to • is not equal to Possible values are: • Not Enabled • N/A • Enabled • Unknown	iOS/Android
Anti-phishing VPN status	This field displays the anti-phishing VPN status	Possible operators are: • is equal to • is not equal to Possible values are: • Not Enabled • N/A • Enabled • Unknown	iOS/Android
Battery Information	This field has the following attributes: • Battery Level - Displays current battery charge level as reported by the Android OS • Battery Health Status - As reported by the Android OS	For information on possible values, see **Using Advanced Search**.	Android

UI Field	Description	Possible values	Supported Platforms
	• Battery Charging Status - As reported by the Android OS • Battery Health Percentage (OEM Specific) - Battery health in percentage for supported device manufacturers such as Zebra devices • Battery Manufacture Date (OEM) - Battery manufactured date for supported device manufacturers such as Zebra devices • Battery Charge Cycles (OEM) - Number of cycles completed in total for supported device manufacturers such as Zebra devices		
Baseband Health Status	This field indicates the Baseband health status of the device.	Possible operators are: • is equal to • is not equal to Possible values are OK or Error.	iOS 27.0+ Supervised Devices
Bootstrap Token Availabl e	This field indicates whether a bootstrap token is available for a device.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	macOS
Autopilot Enrolled	This field indicates whether device is Autopilot Enrolled or not.	• is equal to • is not equal to Possible values are Yes and No.	Windows
Bridge Last Check-in	This field indicates the bridge last check-in time of the client.	Possible operators are: • is less than • is less than or equal to • is greater than • is greater than or equal to • is in range • is not in range Enter the numerical value of bridge last check-in time. Select any of the following option for the duration:	Windows

UI Field	Description	Possible values	Supported Platforms
		• hours • days Example: Bridge Last Check-in is less than 12 hours ago.	
Camera Health Status	This field indicates the Camera health status of the device.	Possible operators are: • is equal to • is not equal to Possible values are: • OK • Error • Non-genuine (if it is not a genuine Apple component)	iOS 27.0+ Supervised Devices
Client Last Check-in	This field indicates the last check-in time of the client.	Possible operators are: • is less than • is greater than Enter the numerical value of last check-in time. Select any of the following option for the duration: • hours • days Example: Client Last Check-in is less than 12 hours ago.	iOS/macOS/Android
Client Registered	This field indicates the status of the client registered.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	iOS/macOS/Android
Compromised	This field indicates whether the device is rooted/compromised.	Possible operators are: • is equal to • is not equal to Possible values are: • jailbroken or rooted • not compromised	iOS/Android
Current Country Name	This field indicates the name of the current country corresponding to the Mobile Country Code (MCC) or Mobile Network Code (MNC) that the device reports to be currently connected.	Possible operators are: • is equal to • is not equal to Possible value is a drop down list value that indicates the home country name.	iOS/macOS/Android

UI Field	Description	Possible values	Supported Platforms
Current MCC	This field indicates the current mobile country code	Enter the attribute's value to be verified. Possible operators are: • is equal to • is not equal to	iOS/macOS/Android
Current MNC	This field indicates the current mobile network code	Enter the attribute's value to be verified. Possible operators are: • is equal to • is not equal to	iOS/macOS/Android
Custom Device Attribute	This field enables adding an existing custom device attribute as a condition of a rule to verify its value.	Enter the attribute's value to be verified. Possible operators are: • is equal to • is not equal to • contains • does not contain Value can be a string of ASCII characters, including Space and Unicode characters.	iOS/macOS/Android/Windows
Custom LDAP Attribute	This field enables adding an existing custom LDAP attribute as a condition of a rule to verify its value.	Enter the attribute's value to be verified. Possible operators are: • is equal to • is not equal to • contains • does not contain Value can be a string of ASCII characters, including Space and Unicode characters.	iOS/macOS/Android/Windows
Custom User Attribute	This field enables adding an existing custom user attribute as a condition of a rule to verify its value.	Enter the attribute's value to be verified. Possible operators are: • is equal to • is not equal to • contains • does not contain Value can be a string of ASCII characters, including Space and Unicode characters.	iOS/macOS/Android/Windows
Data Roaming	This field enables data roaming to be used as a condition of a rule to verify its value.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	iOS/Android

UI Field	Description	Possible values	Supported Platforms
		Default value is No if the supported device does not report info about this field.	
Device Type	This field represents the device model.	Possible operators are: • is equal to • is not equal to • begins with • ends with Possible value is a text value.	iOS/macOS/Android/Windows
Device Type (Apple)	This field represents the device model pretty name.	Possible operators are: • is equal to • is not equal to • begins with • ends with Possible value is a text value.	iOS/macOS
Display Health Status	This field indicates the Display health status of the device.	Possible operators are: • is equal to • is not equal to Possible values are: • OK • Error • Non-genuine (if it is not a genuine Apple component)	iOS 27.0+ Supervised Devices
Encryption Enabled	This field determines whether the device is encryption/data protection enabled.	Yes - Device is encryption/data protection enabled. No - Device is not encryption/data protection enabled.	iOS/Android/Windows
GUID	This field indicates the device GUID.	Possible operators are: • is equal to • is not equal to • begins with • ends with	iOS/macOS/Android/Windows
Face ID Health Status	This field indicates the Face ID health status of the device.	Possible operators are: • is equal to • is not equal to Possible values are OK or Error.	iOS 27.0+ Supervised Devices

UI Field	Description	Possible values	Supported Platforms
Home Country Name	This field indicates the name of the home country corresponding to the Mobile Country Code (MCC) or Mobile Network Code (MNC) that is programmed into the SIM or eSIM of the device.	Possible operators are: • is equal to • is not equal to Possible value is a drop down list value that indicates the home country name.	iOS/Android/ Windows
Has Failed Windows Update	This field determines whether the device is out of compliance with the latest update rules.	Yes - Device is not compliant with the latest update. No - Device is compliant with the latest update.	Windows
Home MCC	This field indicates the home MobileCountry Code.	Enter the attribute's value to be verified. Possible operators are: • is equal to • is not equal to	iOS/macOS/Android
Home MNC	This field indicates the home MobileNetwork Code	Enter the attribute's value to be verified. Possible operators are: • is equal to • is not equal to	iOS/macOS/Android
IMEI	This field indicates the IMEI number of the first SIM slot.	Possible operators are: • is equal to • is not equal to • begins with • ends with	iOS/Android/ Windows
IMEI2	This field indicates the IMEI number of the second SIM slot.	Possible operators are: • is equal to • is not equal to • begins with • ends with	Android
IMSI	This field indicates the IMSI number of the SIM card.	Possible operators are: • is equal to • is not equal to • begins with • ends with	Android/Windows
Institutional	This field indicates if the Institutional Recovery Key is enabled or not on the	Possible operators are: • is equal to	macOS

UI Field	Description	Possible values	Supported Platforms
Recovery Key Enabled	device.	• is not equal to	
Last Check-in	This field allows you to set conditions related to the last check-in time of the managed device via MDM channel.	Possible operators are: • is less than • is greater than • is blank Enter the numerical value of last check-in time. Select any of the following option for the duration: • hours • days Example: Last Check-in is greater than 12 hours ago.	iOS/macOS/Android/Windows
Last Hotfix ID	This field allows you to set conditions related to the last hotfix ID	Possible operators are: • is equal to • is not equal to • is less than • is less than or equal to • is greater than • is greater than or equal to • contains • does not contain • begins with • does not begin with • ends with • does not end with	Windows
Last Hotfix Installed On	This field allows you to set conditions related to the hotfix that was last installed.	Possible operators are: • is less than • is greater than	Windows
Locator Services Enabled	This field indicates whether the device has a device locator service (such as Find My iPhone) enabled.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	iOS

UI Field	Description	Possible values	Supported Platforms
Manufacturer	This field allows you to set conditions related to manufacturer of the device.	Possible operators are: • is equal to • is not equal to Possible values are: • Samsung • NOKIA • HTC • LGE • Apple Inc	iOS/macOS/Android/Windows
MTD activation status	This field represents the MTD activation status	Possible operators are: • is equal to • is not equal to Possible values are: • N/A • Error • Pending • Protected	iOS/Android
MDM Managed	This field determines whether the device is MDM/Device admin enabled.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	iOS/macOS/Android
MDM Enrollment Type	This field indicates the enrollment type of the device.	Possible operators are: • is equal to • is not equal to Possible values are: • User • Device • Supervised • None	iOS 27.0+, macOS 27.0+, tvOS 27.0+, visionOS 27.0+, and watchOS 27.0+
MDM Return to Service	This field indicates the device status for MDM return to service with app preservation.	Possible operators are: • is equal to • is not equal to Possible values are True or False.	iOS 27.0+ and visionOS 27.0+
Multi-User	This field indicates if the device (iPad) uses multi-user mode.	Possible operators are: • is equal to	iOS 27.0+

UI Field	Description	Possible values	Supported Platforms
Mode		• is not equal to Possible values are Yes or No.	
Near Field Health Status	This field indicates the NFC health status of the device.	Possible operators are: • is equal to • is not equal to Possible values are OK or Error.	iOS 27.0+ Supervised Devices
OS	This field represents the OS type of the device.	Possible operators are: • is equal to • is not equal to Possible values are: • macOS • Android • iOS • Windows • visionOS	iOS/macOS/visionOS/Android/Windows
OS Build Version	This field represents the OS build version of the device.	Possible operators are: • is equal to • is not equal to • is less than • is less than or equal to • is greater than • is greater than or equal to • contains • does not contain • begins with • does not begin with • is not blank • is blank • ends with • does not end with	iOS/macOS/visionOS/Android/Windows
OS Version	This field represents the OS version of the device.	Possible operators are: • is equal to • is not equal to • is less than • is less than or equal to	iOS/macOS/visionOS/Android/Windows

UI Field	Description	Possible values	Supported Platforms
		• is greater than • is greater than or equal to • is in range • is not in range Possible value is text.	
OS With Version	This field represents the OS and the OS version of the device	Possible operators are: • is equal to • is not equal to • is less than • is less than or equal to • is greater than • is greater than or equal to • is in range • is not in range Possible value is text.	iOS/macOS/visionOS/Android/Windows
Ownership	This field indicates the ownership type of the device.	Possible operators are: • is equal to • is not equal to Possible values are: • user owned • not set • company owned	iOS/macOS/Android/Windows
Personal Recovery Key Enabled	This field indicates if the personal recovery key is enabled or not.	Possible operators are: • is equal to • is not equal to	macOS
Passcode Compliant With Profiles	This field indicates whether is device is passcode compliant with profiles.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	iOS/macOS/Android
Personal Hotspot	This field indicates whether Personal Hotspot feature is enabled on the device.	Possible operators are: • is equal to	iOS

UI Field	Description	Possible values	Supported Platforms
Enabled		• is not equal to Possible values are Yes and No. The Personal Hotspot setting is only available on certain carriers.	
Phone No.	This field indicates the device phone number.	Possible operators are: • is equal to • is not equal to • contains • begins with • ends with	iOS/Android/Windows
Public IP Address	This field indicates the public IP address. If the device uses a VPN connection or a proxy server to connect to Ivanti Neurons for MDM, it displays the proxy WAN IP address.	Possible operators are: • is in range • is not in range • is not blank • is blank	Android/ChromeOS
Roaming	This field indicates the roaming status of the device.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	iOS/Android/Windows
Security Lockdown Mode	This field indicates whether the lockdown mode is enabled or disabled for a device.	Possible operators are: is equal to is not equal to Possible values are True or False.	iOS 27.0+ and macOS 27.0+
Sentry Blocked	Indicates whether the device is blocked by Sentry.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	iOS/macOS/Android/Windows
Status	This field indicates the registration status.	Possible operators are: • is equal to • is not equal to The default possible value is 'Active.' In custom policies, it restricts the device state to Active by removing all other potential values because policy evaluation occurs when the device checks in for Active, Retire-pending, and Wipe-	iOS/macOS/Android

UI Field	Description	Possible values	Supported Platforms
		pending statuses, and these devices will have their policies evaluated upon check-in.	
Serial Number	This field indicates the device serial number.	Possible operators are: • is equal to • is not equal to • begins with • ends with	iOS/macOS/Android/Windows
Supervised	This field indicates whether the device is supervised.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	iOS/macOS
Supplemental Build Version	This field represents the supplemental build version of the device.	Possible operators are: • is equal to • is not equal to • is less than • is less than or equal to • is greater than • is greater than or equal to • contains • does not contain • begins with • does not begin with • ends with • does not end with • is not blank • is blank	iOS/macOS
Supplemental OS/Version Extra	This field represents the supplemental OS build version of the device.	Possible operators are: • is equal to • is not equal to • is less than • is less than or equal to • is greater than • is greater than or equal to • contains • does not contain	iOS/macOS

UI Field	Description	Possible values	Supported Platforms
		• begins with • does not begin with • ends with • does not end with • is not blank • is blank	
Touch ID Health Status	This field indicates the Touch ID health status of the device.	Possible operators are: • is equal to • is not equal to Possible values are: • OK • Error • N/A (if it is a iPhone)	iOS 27.0+ Supervised Devices
User Enabled	This field indicates whether the user is enabled.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	iOS/macOS/Android/Windows
User Group	This field represents the user group.	Possible operators are: • is equal to • is not equal to	iOS/macOS/Android/Windows
Ultra Wideband Health Status	This field indicates the Ultra Wideband health status of the device.	Possible operators are: • is equal to • is not equal to Possible values are OK or Error.	iOS 27.0+ Supervised Devices
Voice Roaming	This field indicates whether voice roaming is enabled on the device.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No. The voice roaming setting is only available on certain carriers. Disabling voice roaming also disables data roaming. Default value is not equal to if the supported device does not report info about this field.	iOS

UI Field	Description	Possible values	Supported Platforms
Access Blocked	Indicates whether the device is blocked by Access.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	iOS/macOS/Android/Windows
Compliance	Indicates whether the device is compliant or not.	Possible operators are: • is equal to • is not equal to Possible values are In Compliance and Out of Compliance.	iOS/macOS/Android/Windows
Compliance Action Blocked	Indicates whether the device is blocked or not.	Possible operators are: • is equal to • is not equal to Possible values are Yes and No.	iOS/macOS/Android/Windows

Non-quarantinable configurations

The following table shows the list of configurations that are non-quarantinable:

OS	Non-Quarantinable Configurations
Android	• Android App Catalogue • Android Encryption • Android enterprise • Android Enterprise App • Android Zebra • Anti-phishing Protection • Android Work Challenge • Device Passcode • File download • Lockdown & Kiosk: Android Device Admin Mode • Lockdown & Kiosk: Samsung Knox Standard • MAM Only • Managed Device with Work Profile/Work Profile on Company Owned Device • Work Managed Devices (Device Owner) • Samsung Phone Restrictions • SafetyNet Attestation • Work Profile on Company Owned Device
iOS and macOS	• Anti-phishing Protection (iOS) • App Notifications (iOS) • AppStation Sites (iOS) • Filevault Recovery Key (macOS) • Filevault 2 (macOS) • Global Proxy (iOS and tvOS) • Home Screen Layout (iOS and tvOS) • iOS App Control • iOS Restrictions • iOS Software Updates (iOS) • macOS Firewall • macOS Software Updates • MAM Only (iOS) • MI Client Privacy (iOS/macOS) • Network Usage (iOS) • Office 365 Account Creation (macOS) • Single App Mode (iOS and tvOS) • System Policy Control (macOS)

OS	Non-Quarantinable Configurations
	• System Policy Managed (macOS) • System Policy Rule options (macOS) • Time Server (macOS) • Web Content Filter (iOS)
Windows	• Windows App Control • Windows RestrictionsDDF (Data Definition File) • Windows Firewall • Windows Network Proxy • Windows Restrictions • Windows Update
All	• Active Directory • Client Services • Mobile Device Management • Mobile Threat Defense Activation • Mobile Threat Defense Local Actions • Passcode • Privacy • Privacy Statement • ServiceConnect • Sync

If you cannot see the Policy page, it might be that you do not have the required permissions. You need one of the following **roles**:

- Device Management
- Device Read Only

11.3. Monitoring and Controlling Allowed Apps

Licence: Silver

To control which apps are installed on devices, you create an Allowed Apps policy. This policy also supports MobileIron Packager (MIP) in-house macOS apps. The policy contains the following information:

- {{Allowlist apps}}
- {{Blockedlist apps}}
- {{required apps}}
- {{compliance actions}}

If an app is both required and Blockedlisted, then the evaluation of the app against the required list takes precedence. For example, if an app A1 is present in both in the required list and the Blockedlist, then the apps policy evaluation for this device behaves as follows:

- Device will be compliant if A1 is installed on the device.
- Device will be non-compliant if A1 is not installed on the device.

Supported Devices

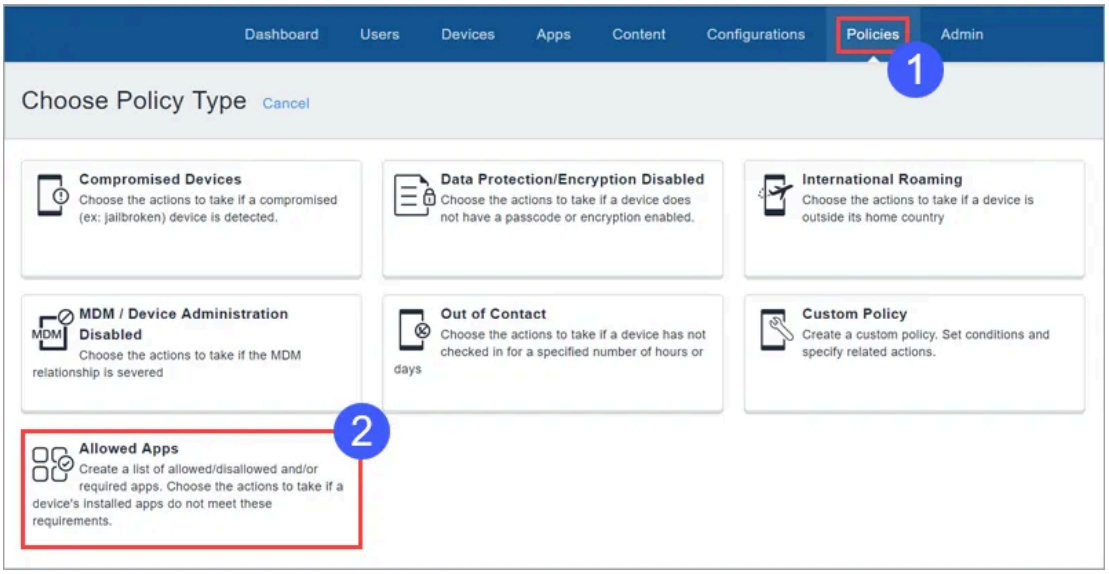
- Android 4.2 or supported newer versions
- iOS 8.0 or supported newer versions
- macOS 10.12 or supported newer versions
- Windows 10 or supported newer versions

Prerequisites

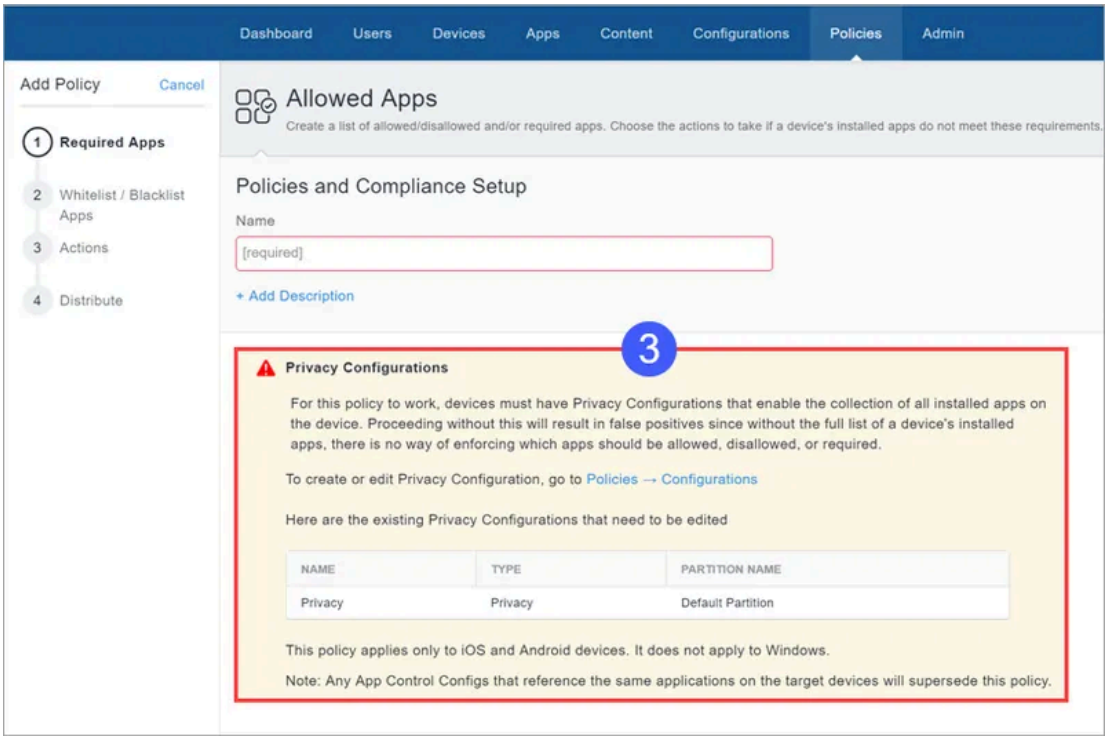
- The privacy configuration assigned to a device must allow collection of app information in order for an Allowed Apps policy to work correctly. Check the privacy configurations assigned to the devices to which you will apply the Allowed Apps policy.

If you are not sure which configurations are affected:

1. Go to **Policies**.



Click **Allowed Apps**.



3. Under **Privacy Configurations**, note the configurations that need to be edited.
4. Go to **Configurations**.
5. For each privacy configuration you noted:
    1. Select the configuration.
    2. Click **Edit**.
    3. Under **Collect App Inventory,** select **For All Apps on the Device**.
    4. Click **Done**.

Creating an Allowed Apps policy

Prerequisites

- Enable Android Enterprise to access Google Play Store and to add new applications to allowed apps policy.

Procedure

1. Go to **Policies** and click **+ Add**.

2. Click **Allowed Apps**.

3. In the **Name** field, type a name for this policy.
4. In the **Description** field, type optional text that explains the purpose of the policy.
5. Choose the apps to Allowlist or Blockedlist by clicking one or both of the following tabs:

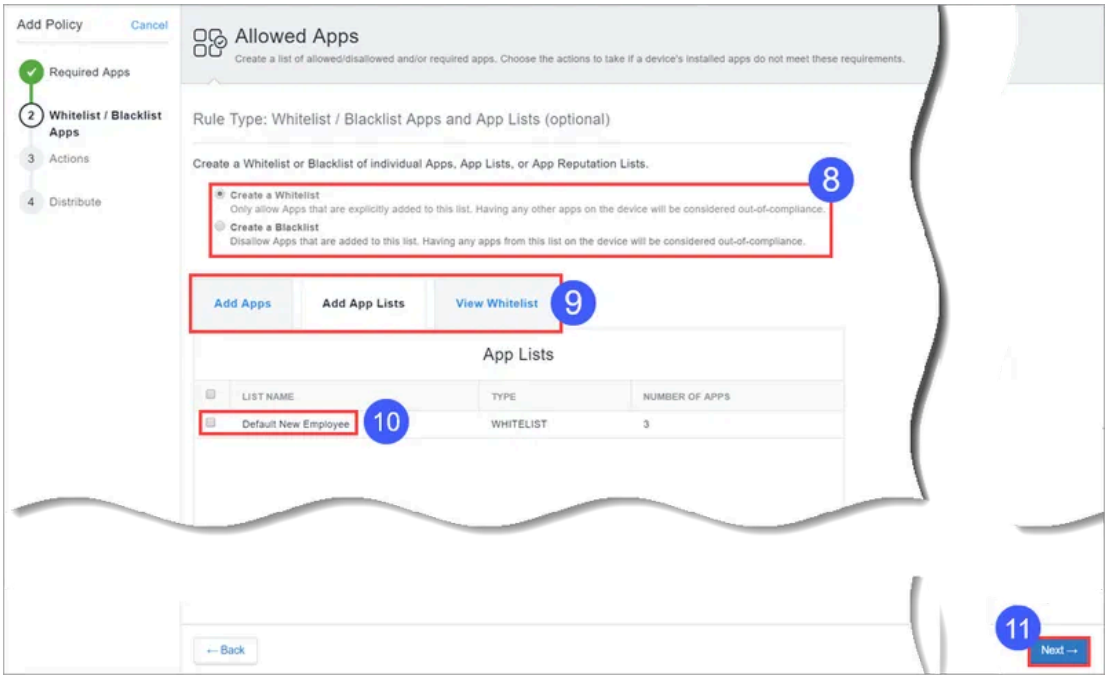
- Click Add by Lookup to search for and choose apps from the App Store or App Catalogue.
  Ensure to enable Android Enterprise to access Google Play Store.
  
- Click **Add Manually** to choose apps by entering the bundle ID for Android, Windows, iOS or macOS system apps.

Select the **Add App Lists** tab and then select the desired required apps lists.

6. Use the resultant fields to select the required apps or apps lists.
7. Click **Next**

> Click the **View Required List** tab for a list of apps you have selected so far.

8. Select whether to create a Allowlist or a Blockedlist.



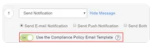
9. Use the **Allowlist/Blockedlist Apps and App Lists** section to select apps and apps lists.

> You cannot have both an Allowlist and a Blockedlist for a device simultaneously. Creating an Allowlist means all other apps are Blockedlisted.

10. Use the resultant fields to select the required apps or apps lists.
    - Select the **Add App Lists** tab and then select the desired apps lists.
11. Click **Next**.

> Click the **View Allowlist or Blockedlist** tab for a list of apps you have selected so far.

12. Select the actions to take when a device is out of compliance:

Action	What To Do
Monitor	Currently always selected. Sentry version 9.0.0 or later is required to utilise the tiered compliance actions.
Do Nothing	Select to take no action if the device is out of compliance.
Send Notification	
Send Email	Select to send an email to the device user's email address notifying them the device is out of compliance. • Turn on the **Use the Compliance Policy Email Template** option to insert the message you configure here into the policy notification email template you configure as described in **Customising an email template** in **Branding Email Templates**. See **Configuring and using policy compliance notification emails** for an overview.  • You can customise the messages by including optional substitution variables to provide recipients more details about policy violations and other relevant information. This provides users of non-compliant devices with relevant information about the policy violation so they can take remedial actions. Click the following attribute types to display the complete list of variables: ◦ Policy Attributes including $, $, and $. ◦ User Attributes including $, $, and $. ◦ Device Attributes including $, $, and $.
Send Push Notification	Select to send a push notification to the device that the device is out of compliance.
Send Both	Select to send both a push notification to the device and an email to the device user's email address notifying them the device is out of compliance. You can customise the messages by including optional substitution variables to provide recipients more details as described previously for the Send Email action.
Wait	Select to delay action for a specified time period to allow users to remediate the violation before additional actions are taken if the device remains in a non-compliant state.
Block	Uses Sentry to block managed devices from accessing email and AppConnect-enabled applications.
Quarantine	Select to remove access to apps, content, and servers as per the actions in the following table. Remove all apps action is not allowed.
Send a notification when the device comes back into compliance	
Send Email	Sends an email to the device user's email address notifying them when the device comes back into compliance. • You can use the policy notification email template as described above. • You can customise the messages by including optional substitution variables to provide recipients more details about policy violations and other relevant information. Click the following attribute types to display the complete list of variables:

Action	What To Do
	◦ Policy Attributes including $, $, and $. ◦ User Attributes including $, $, and $. ◦ Device Attributes including $, $, and $. ◦ Custom Device/User/LDAP attributes that are created from the **Admin > Attributes** page.
Send Push Notification	Sends a push notification to the device when the device comes back into compliance.
Send Both	Sends both a push notification to the device and an email to the device user's email address notifying them when the device comes back into compliance. You can customise the messages by including optional substitution variables to provide recipients more details as described previously for the Send Email action.

The Allowed Apps policy supports **tiered compliance actions** if you have a Platinum licence.

(Optional) Additional Quarantine Actions	Description
Quarantine Managed Applications	Removes Ivanti Neurons for MDM managed apps from the device and enables the Block New App Downloads option to block the apps from being re-installed on the device. Select one of the following options: • **All Applications** • **Designated Applications** - Add one or more apps by lookup or manually (using Bundle ID or Package name). Click the **View Apps** tab to review the list of added apps. The Block App Store Access default quarantine action is no longer available. On certain devices, the Quarantine action will not remove the application from the device due to certain device limitations.
Block New App Downloads	Prevents download of any new apps to the device. Select one of the following options: • **All Applications** • **Designated Applications** - Add one or more apps by lookup or manually (using Bundle ID or Package name). Click the **View Apps** tab to review the list of added apps. The Block App Store Access default quarantine action is no longer available.
Remove Configurations	Removes Ivanti Neurons for MDM configurations from the device. Select one of the following options: • **All Configurations** • **Designated Configurations** - Select one or more configurations from the list or search for them. Click the **Selected Configurations** tab to review the list of selected configurations.
Remove Content	Removes all content and media associated with the apps distributed by Ivanti Neurons for MDM from the device.
Suspend Personal Apps	Suspend apps on the personal side of the quarantined device to indicate that device user needs to address the compliance issues on the device to make it functional. Supported on Android 11+ Devices provisioned as a Work Profile on Company Owned Device on company owned device.
Default Quarantine Actions - these actions are always performed.	
Block App Store Access	Prevents the device from accessing app stores via Ivanti Neurons for MDM.
Block Content Store Access	Prevents the device from accessing content store via Ivanti Neurons for MDM.
Block AppConnect	Prevents the device from using AppConnect features.
Block AppTunnel	Prevents applications on the device from accessing content and servers via AppTunnel.
Block ActiveSync	Prevents the device from accessing email via the ActiveSync server.

Click **Next**.

14. Configure the distribution.
15. Click **Done**.

For more information about setting higher or lower priorities to an Allowed Apps policy, see **Prioritize policies**.

11.4. Prioritising Policies

The Allowed Apps policy supports a priority, similar to Configurations. A priority is used to determine which policy of the same type is distributed to multiple device groups, and the case where the same device appears in those multiple device groups. For example, a policy priority is useful to determine policy distribution in the case where:

- "Required App A" needs to be distributed to Device Group 1,
- "Required App B" needs to be distributed to Device Group 2, and
- The user's device is a member of both device groups.

You can prioritise policies as follows:

1. Go to **Policies > Policy & Compliance**.
2. Select **Actions > Prioritize policies**. If **Actions** is not displayed, then you do not have multiple policies requiring priorities.
3. Use the arrows to list priorities from highest (top) to lowest (bottom). A lock icon means the policy's priority cannot be changed without editing the All Devices distribution setting within the policy.
4. Click **Save**.

11.5. Windows Hardware policy

Couldn't convert your doc.

12. Admin

The admin section helps you manage users, devices, and configurations from the Ivanti Neurons for MDM portal. The following sections contain the list of all the tasks you can perform as an administrator:

- System
- Infrastructure
- Settings (Apple)
- Work with Windows Devices
- Setup with Microsoft Azure
- Connect with Google Apps
- Work with ChromeOS Devices
- Firmware Management
- Tenant Suspension
- Manage Scripts and Files
- Branding
- Adding management of non-iOS devices

12.1. System

This section contains the following topics:

- Attributes
- Device Cleanup Settings
- GDPR Profiles
- Notification emails
- Roles Management
- Spaces
- Support Administrators
- Admin > System Use Notification

12.1.1. Attributes

Use the Attributes page to do the following tasks:

- Manage the types of information you can record for users, devices, and apps.
- View the standard types of information that Ivanti Neurons for MDM tracks.

Custom user attributes include information such as Department or an internal ID. Each attribute has a corresponding variable that you can use to build groups or distribute configurations.

> While creating user rule group criteria, if the custom attributes have a number value, Ivanti Neurons for MDM does not support integer operations.

Creating custom attributes

You can create custom attributes from the Ivanti Neurons for MDM administrative portal.

Procedure

1. Log in to the Administrative Portal.
2. Navigate to **Admin** > **System** > **Attributes**.
3. Under **Custom Attributes**, click **+Add**
4. In the **Attribute Name** field, enter text that will represent the attribute.

> The text you enter will be used to create the corresponding variable in the **Usage** field.

Select any the type of attribute from the following **Attribute Type** options.

   - **User**
   - **Device**
   - **App**
   - **IDP** (for more information, see User Provisioning with SCIM or Connect Ivanti Neurons for MDM with Entra ID User Source)

If the Attribute type is Device, select one of the following **Data Type** options:

   - **Numeric**
   - **Text**

7. **Preserve attribute** (Optional): This option can be used only when the attribute type is **Device**. Select this option to preserve the custom attribute even when a wipe / retire operation is performed on a device.
8. Click **Add**.
   The created custom user attribute is displayed under **Admin Added** section in the Attributes page.

> The custom attributes combination $ + $ + $ + ${Static String} is supported in any order.

Renaming a custom attribute

Renaming a custom attribute will rename all references of that custom attribute that are used in the following entities:

- Custom Policy
- User group
- Device group
- App Distribution Filter
- Spaces

> References of the custom attribute in any other entities such as configurations, invitation email templates, email and push messages in policy compliance actions, and so on will not be updated.

Procedure

1. Under **Admin Added**, click **+Edit** next to the attribute you want to rename.
2. In the **Attribute Name** field, enter a new name that will represent the attribute.

> The text you enter will be used to create the corresponding variable in the **Usage** field.

Click **Save**.

Deleting a custom attribute

Deleting a custom attribute will remove its values from all the associated users or devices. It cannot be reversed.

Custom attributes cannot be deleted if the attribute is used in any of the following entities:

- Custom Policy
- User group
- Device group
- App Distribution Filter
- Spaces

Remove the custom attribute from the entities before attempting to delete the custom attribute.

If the attribute you want to delete does not have references to any of the above entities, clicking **Delete** next to the attribute will display a pop-up to confirm the action. Confirm the action and click **Delete**.

> The field names of the following custom attributes are sorted in the applicable rule builders:

- Custom LDAP Attribute
- Custom User Attribute
- Custom Device Attribute
- Custom IdP Attribute
- Custom App Attribute

Viewing the system attributes

System attributes are pre-defined attributes for you to use in your configurations as variables. The complete list is provided in the **System Attributes** section of the **Admin** > **System** > **Attributes** page. System attributes include the following types of attributes:

- User Attributes
- Device Attributes
- Email Template Attributes
- System Attributes
- Timestamp Attributes
- Entra ID Custom User Attributes
- Policy Attributes

User attributes

Use user attributes to specify information about users.

Key	Description
$	department attribute (requires Entra ID)
$	Electronic Data Interchange-Personal Identifier
$	User's Managed Apple ID
$	sAMAccountName attribute (requires Active Directory)
$	Common Name (CN) attribute extracted from the distinguished name (requires LDAP)
$	Display name
$	Distinguished Name (requires LDAP)
$	The domain part of the email address (part after '@')
$>	The local part of the email address (part before '@')
$	Email address
$	Forename
$	Surname
$	Locale
$	Organisational Unit (OU) attribute extracted from the distinguished name (requires LDAP)
$	Kerberos Realm information (requires Active Directory)
$	The domain part of the login ID (the part after '@')
$	The local part of the login ID (the part before '@')
$	Login ID (email address format)
$	userPrincipalName attribute (requires Active Directory)

Device attributes

Use device attributes to specify information about a mobile device.

Key	Description
$	Date client last checked-in (most recent checkin - either MDM or Client)
$	Alternative Serial Number
$	Identifier used by the client application
$	Globally unique device identifier
$	ICCID
$	IMEI2
$	IMEI
$	IMSI
$	Date device last checked-in (most recent checkin - either MDM or Client)
$	Internal device identifier
$	Identifier used for MDM
$	MEID
$	Model
$	Device name
$	Device phone number
$	Cluster unique device identifier
$	Serial Number
$	iOS UDID
$	Wi-Fi MAC Address
	Phone Number 2
	ICCID 2

When you create a custom attribute and refer this attribute in a Managed app config, If the attribute value is updated, the attribute referenced in the managed app config also gets updated and the managed app config will be re-pushed to the device.

When the Custom or Device attributes are updated and the configuration is pushed to a device, the Android Kiosk branding configuration should be updated as well.

App attributes

Use app attributes to specify information about applications and create custom application groups.

Key	Description
$	Date application was added to the AppCatalog
$	Name of the application
$	Application operating system
$	Application bundle or package ID
$	Describes the source from where the application was imported
$	Describes if an iOS or macOS application is VPP or not

Email template attributes

Key	Description
$	Email body
$	Email subject

Time stamp attributes

Variable Key	Description
$	Current timestamp (milliseconds since the epoch)

Policy template attributes

Key	Description
$	Policy name violated
$	Next Tiered Compliance Action (different than wait and retire) to be taken after send message
$	Count of days device has been in non-compliant state
$	Time stamp when policy violation was first triggered (UTC DD-MM-YYYY format)
$	Rule definition (query string the way it appears now)

Related topics:

- Assigning Custom Attributes to Users
- Assigning Custom Attributes to Devices
- Removing Custom Attributes from Users
- Removing Custom Attributes from Devices
- Variables

12.1.2. Device Cleanup Settings

Device cleanup automates device life cycle for unused devices. You can retire devices that have been out of contact for a number of days that you specify. You can delete devices that have been retired for a number of days that you specify. The Audit Trails page captures the Retire Device, Delete Device, and Delete Wiped Device settings.

The following table provides information about the Android devices that support device cleanup settings:

Mode	Retire if Out of compliance	Delete Retired	Force Retire or Retire Pending	Delete Wiped	Delete Wipe Pending
Android Work Profile (Profile Owner)	**YES**	**YES**	**YES**	**NO**	**NO**
Device Admin/ Work Profile on Company Owned Device	**YES**	**YES**	**YES**	**YES**	**YES**
Work Managed Device / Android Managed Device with Work Profile	**NO**	**NO**	**NO**	**YES**	**YES**

Prerequisites

You must have System Management Role permissions to access this setting.

Retire Devices

Procedure

1. Go to **Admin** > **System** > **Device Cleanup**. The Device Cleanup page opens.
2. Select **Retire Device**.
3. Use the **Retire Devices** table to specify the details.
4. Click **Show not checked-in device list**. Shows the list of devices that are not checked in for specified number of days.
5. Click **Retired Devices Now**, alternatively, you can schedule the device retirement.
6. The Ivanti Neurons for MDM administrative portal will retire the specified devices.
7. Click **Save** to save your setting.
8. (Optional) If you update the values you can click **Reset** to reset the settings back to the initial settings.

Retire Devices

Field	Description
Select Platforms	Select the required platform on which the device cleanup settings should be applied. This option is currently available only on **Retire Device** and **Retire the Retire Pending Device** settings.
Retire Devices That Have Been Not Checked-In More Than (Days)	Days: 30 days is default, 365 days is maximum number of days allowed.
Maximum Devices to Retire in Each Session	Select 100, 500, or 1000 (Default - 100).
Automatically Retire Devices on a schedule	Select the check box to retire devices based on a preset schedule.
Retire Schedule Configuration	Select one of the following options to set the frequency of retirements: • **Daily -** Set to retire devices everyday. • **Weekly -** Specify the day of the week to schedule the retirement. • **Monthly -** Set to retire devices the first day of every month.

Delete Retired Devices

Procedure

1. Go to **Admin** > **System** > **Device Cleanup**. The Device Cleanup page opens.
2. Select **Delete Retired Device**.
3. Use the **Delete Retired Devices** table to specify the details.
4. Click **Show retired devices list**. Shows the list of devices that are retired for the specified number of days.
5. Click **Delete Retired Devices Now**, alternatively, you can schedule the device deletion.
6. The Ivanti Neurons for MDM administrative portal will delete the specified devices.
7. Click **Save** to save your setting.
8. (Optional) If you update the values you can click **Reset** to reset the settings back to the initial settings.

Delete Retired Devices

Field	Description
Delete the Devices That have Been Retired More Than (Days)	Days: 30 days is default, 365 days is the maximum number of days allowed.
Maximum Retired Devices to Delete in Each Session	Select 100, 500, or 1000 (Default - 100)
Automatically Delete Retired Devices on a schedule	Select the check box to retire devices based on a preset schedule.
Delete Schedule Configuration	Select one of the following options to set the frequency of deletion: • **Daily -** Set to delete devices everyday. • **Weekly -** Specify the day of the week to schedule the deletion. • **Monthly -** Set to delete retired devices the first day of every month.

Delete Wiped Devices

Procedure

1. Go to **Admin** > **System** > **Device Cleanup**. The Device Cleanup page opens.
2. Select **Delete Wiped Device**.
3. Use the **Delete Wiped Devices** table to specify the details.
4. Click **Show wiped devices list**. Shows the list of devices that are retired for the specified number of days.
5. Click **Delete Wiped Devices Now**, alternatively, you can schedule the wiped devices deletion.
6. The Ivanti Neurons for MDM administrative portal will delete the specified devices.
7. Click **Save** to save your setting.
8. (Optional) If you update the values you can click **Reset** to reset the settings back to the initial settings.

Delete Wiped Devices

Field	Description
Delete Devices That have Been Wiped More Than (Days)	Days: 30 days is default, 365 days is the maximum number of days allowed.
Maximum Wiped Devices to Delete in Each Session	Select 100, 500, or 1000 (Default - 100)
Automatically Delete Wiped Devices on a schedule	Select the check box to delete wiped devices based on a preset schedule.
Delete Wiped Schedule Configuration	Select one of the following options to set the frequency of deletion: • **Daily -** Set to delete wiped devices everyday. • **Weekly -** Specify the day of the week to schedule the deletion. • **Monthly -** Set to delete wiped devices the first day of every month.

Delete Wipe Pending Devices

Procedure

1. Go to **Admin** > **System** > **Device Cleanup**. The Device Cleanup page opens.
2. Select **Delete Wipe Pending Device**.
3. Use the **Delete Wipe Pending Devices** table to specify the details.
4. Click **Show wipe pending devices list**. Shows the list of devices that are due to be wiped for the specified number of days.
5. Click **Delete Wipe Pending Devices Now**, alternatively, you can schedule the pending devices for deletion.
6. The Ivanti Neurons for MDM administrative portal will delete the specified devices.
7. Click **Save** to save your setting.
8. (Optional) If you update the values you can click **Reset** to reset the settings back to the initial settings.

Delete Wipe Pending Devices

Field	Description
Delete the Devices That have Been Wipe Pending More Than (Days)	Days: 30 days is default, 365 days is the maximum number of days allowed.
Maximum Wipe Pending Devices to Delete in Each Session	Select 100, 500, or 1000 (Default - 100)
Automatically Delete Wipe Pending Devices on a schedule	Select the check box to delete wiped devices based on a preset schedule.
Delete Wipe Pending Schedule Configuration	Select one of the following options to set the frequency of deletion: • **Daily -** Set to delete wipe pending devices everyday. • **Weekly -** Specify the day of the week to schedule the deletion. • **Monthly -** Set to delete wipe pending devices the first day of every month.

Retire the Retire Pending Devices

Procedure

1. Go to **Admin** > **System** > **Device Cleanup**. The Device Cleanup page opens.
2. Select **Retire the Retire Pending Device**.
3. Use the **Retire the Retire Pending Devices** table to specify the details.
4. Click **Show retire pending device list**. Shows the list of devices that are due to be retired for the specified number of days.
5. Click **Force Retire the Retire Pending Devices Now**, alternatively, you can schedule the pending devices to retire.
6. The Ivanti Neurons for MDM administrative portal will retire the specified devices.
7. Click **Save** to save your setting.
8. (Optional) If you update the values you can click **Reset** to reset the settings back to the initial settings.

Retire the Retire Pending Devices

Field	Description
Retire the Retire Pending Devices That have not checked-in more than (Days)	Days: 30 days is default, 365 days is the maximum number of days allowed.
Maximum Retire Pending Devices to Retire in Each Session	Select 100, 500, or 1000 (Default - 100)
Automatically Retire the Retire Pending Devices on a schedule	Select the check box to retire the retire pending devices based on a preset schedule.
Retire the Retire Pending Schedule Configuration	Select one of the following options to set the frequency of deletion: • **Daily -** Set to retire the pending devices everyday. • **Weekly -** Specify the day of the week to schedule the pending devices for retirement. • **Monthly -** Set to retire the pending devices the first day of every month.

When a device is retired and if the check-in happened long back then that last check-in time will only be considered for determining the device deletion. For example, if the device was last checked in 30 days back and if device is retired today (may be due to "Retire Devices That Have Been Not Checked-In More Than (Days)" option), and if the "Delete Devices That Have Been Retired More Than (Days)" is set as 30 days, then the device will be deleted immediately once the 'Delete Retired Device' job is executed.

12.1.3. GDPR Profiles

The Ivanti Neurons for MDM administrative portal now contains GDPR Profiles page that lets you assign GDPR profiles to user groups. You can assign the GDPR profile to only user groups and not to individual users.

Note the following points:

- You must first enable the GDPR Profiles to assign it to a specific user group.
- If you disable the GDPR profile, it will turn off all the profile restrictions that were already assigned to the user group.
- After you enable the GDPR profile the Edit functionality for some of the fields will be limited or disabled.

Fields that are hidden after GDPR profile assignment

If a user has a GDPR profile, then Ivanti Neurons for MDM hides the following fields by default when displaying information about the user:

- **User ID**
- **User's Name**
- **Email Address**
- **Serial Number**
- **ICCID**
- **IMSI**
- **MEID**
- **IP Address**
- **Phone Number**
- **IMEI**
- **eSIM Identifier**
- **Location**

> If Location is added to the GDPR profile then the Device Location fields Last located on, Latitude and Longitude are masked in the device details for the users assigned with the GDPR profile.

Enabling GDPR profile

You can enable GDPR profile and select specific fields that must be hidden from the Ivanti Neurons for MDM administrative portal and the devices.

ProcedureProcedure

	1.	**Log in to the Ivanti Neurons for MDM administrative portal.**
	2.	**Go to Admin > System > GDPR Profiles.**

	3.	Click **Enable**.

4.	Click the edit (pencil) icon.

	5. Select the fields that must be hidden.

6.	Click **Save**. The selected fields will be masked and do not display the values for the specific users.

Assign GDPR profile to User Groups

After you enable the GDPR profile you can assign it to specific user groups.

ProcedureProcedure

	1.	Log in to the Ivanti Neurons for MDM administrative portal.

	2. Go to Users > User Groups.

	3. Select a user group from the list.

	4.	Click the **Actions** drop-down list and select **Assign GDPR Profile**. The GDPR Profile is assigned to all the users of that specific group and all the selected values will be masked from view throughout the administrative portal and the user devices. Since the administrator is also in the All Users group, do not assign the GDPR Profiles to the All Users group.

12.1.4. Notification emails

Licence: Silver

You can configure the list of email addresses of the users who should receive email notifications based on the severity level of the notification.

The Notification Email feature is optional and you can turn on or turn off the feature as and when it is required. It is a prerequisite that you should be assigned System management role to use this feature.

1. Select **Admin > Notification Emails**. The **Notification Emails** page is displayed.
2. In the Notification Emails Settings section, click **ON** to enable the Notification Emails feature.
3. Click **Add recepient**. The **Add Recipient** pop-up is displayed.
4. In the **Add Recipient** pop-up, update the following fields:
    - Recipient Email ID - Enter the email ID of the recipient for whom the notification has to be sent.
    - Notification types to be sent - Select the notification type by selecting the checkbox. The following are the notification type options: **Critical Notification, Warning Notifications, Information Notifications**.
5. Click **OK**. The details of the settings are displayed in a table.
6. Click **Save** to apply the changes.

12.1.5. Roles Management

Roles are packaged groups of permissions that allows granting a set of permissions to an administrative user, while limiting their access to control specific areas of functionality. Ivanti Neurons for MDM provides a set of system roles that can be assigned (or edited) and a facility to create custom roles. Starting from you can search for specific permission based on the category and all the options that are associated with the specific role or permission in the UI are displayed. A tool tip is displayed for the permissions that are added as dependent permissions.

> The Roles Management page and the associated options are hidden for converged tenants who have access to both Ivanti Neurons for UEM and Ivanti Neurons for MDM.

There are two kinds of permissions available, and therefore two kinds of roles:

- **Space-specific roles** - The permissions are Space-specific, and therefore apply in a specific Space only. Examples are Device Management, App Management in a Space.
- **Cross-Space roles** - The permissions are, by nature, applicable to all roles. Examples are tenant-level settings such as MDM Certificates, App Catalogue Settings.

Creating a custom role

You can create a custom cross-Space or Space-specific roles. When you select a permission, the dependent permissions will be selected automatically. Accordingly, a user assigned with a custom role can only perform the specific actions (such as retire, wipe) that are available when the user visits the Devices page or the Device Details page.

When you apply the View User Registration PIN custom role, users can view the PIN of other users that have the same access level or with lesser privileges and the users cannot create PINs for other users.

> The newly created custom role cannot be assigned to anyone automatically. The tenant super admin needs to assign it to the required admin users who can later assign the same to other users as needed.

Procedure

1. Go to **Admin** > **Roles Management**.
2. Click **+Add Custom Role**.
3. In the **Create Role** page, enter the **Name** of the new role.
4. (Optional) add a description for the new role.
5. Under **Role Type**, select one of the following role types:
    - **Cross-Space Role**
    - **Space-Specific Role**
6. Under **Permissions**, select the required granular permissions.
7. See the following table for Admin and User permissions.
   Click **Save**.

The following table lists the permissions, roles, and attributes you can use to create a custom role:

Role Type	Permissions Category	Granular Permissions
Cross-Space Role		
Admin		
	Manage Custom Attributes	• Add Custom Attribute • Delete Custom Attribute • Edit Custom Attribute • View Custom Attribute
	Support Administrators	• Add Support Admins • Delete Support Admins • Disable Support Admins • View Support Admins and Show Login History
	Certificate Authority	• Add Certificate Authority • Delete Certificate Authority
	Connector	• Add Connector Logs • Delete Connector Logs • View Connector • Update Connector
	LDAP Management	• Add User/Group/OU • Add Server • Browse Server • Delete Server • Search Server • Sync Server • Remove User/Group/OU

Role Type	Permissions Category	Granular Permissions
		• View Serve All LDAP permissions in this section require View Connector permission. It will be automatically selected in the Connector section when you select any of these LDAP permissions.
	Licensing Management	View Licenses
	Manage App Distribution	**Distribution Update** The **Update App Distribution** permission is now available for custom roles under **Manage App Distribution**. Users with the System Management role automatically receive this permission by default. The app distribution page now includes **Allow Space Admin to Edit the Distribution** checkbox, which is enabled by default for new app versions. Users assigned a custom role with this new permission, as well as those with the App Management role (without System Management access), can modify this setting. For each application version, the availability of the Lock App Distribution setting is displayed on the distribution page, and all descoping attempts are now captured in the audit trail.
Users	User Management Actions	• View User • Update User • Send Message to User • Append/Assign Roles to User • Create User • Delete User • Invite User • View User Registration PIN
	Assign Custom User Attribute	• Delete Attribute • View Attribute • Add/Edit Attribute
	User Groups	• View User Group • Edit User Group

Role Type	Permissions Category	Granular Permissions
		• Append/Assign Roles to User Group • Create User Group • Delete User Group
	Report Management	• Create Report • Edit Report • Run Report • Delete Report Record • View Report • Delete Report • Download Report Record
Devices		
Space-Specific Role	Bulk Enrolment	• Create Bulk Enrollment • Update Bulk Enrollment • Assign User to Bulk Enrollment • View Bulk Enrollment • Delete Bulk Enrollment
Devices	Device Actions	• Assign Device to User • Clear Device Activation Lock • Delete Device • Disable Device Lost Mode • Enable Device Lost Mode • Device Force Checkin • Lock Device • Unlock Device

Role Type	Permissions Category	Granular Permissions
		• Device Force Logout • Reinstall Device System Apps • Restart Device • Schedule iOS Device Updates • Relinquishing Device Ownership • Retire Device • Cancel Retire Device • Shutdown Device • View Device • Wipe Device • Cancel Wipe Device • Update Device OS Version • Bulk Assign Via Upload • Start TeamViewer Session • Enter Kiosk Mode • Exit Kiosk Mode
	Assign Custom Device Attributes	• Add/Edit Device Custom Attribute • Delete Device Custom Attribute • View Device Custom Attribute All Assign Custom Device Attribute permissions in this section require Device Read permission. It will be automatically selected in the Device Actions section when you select any of these Assign Custom Device Attribute permissions.
	Device Configurations	• Exclude Profile • Push Profile • Push Excluded Profile • Retry Install on Error
	Device Groups	• Add Device Group • Delete Device Group • Edit Device Group • View Device Group

12.1.6. Spaces

This section contains the following topics:

- Spaces
- Managing Spaces
- Space Examples
- Delegating Devices
- Delegating Apps

12.1.6.1. Spaces

Licence: Silver

Spaces are used to separate a Unified endpoint management (UEM) system into independently managed entities for the purpose of delegated administration. Spaces can be created to reflect an organisational hierarchy. Ivanti Neurons for MDM supports single-level delegation with a central management entity referred to as a Default Space and a number of subordinate management entities referred to as Delegated Spaces. Every UEM system is created with a Default Space.

> The Spaces page and the associated options are hidden for converged tenants who have access to both Ivanti Neurons for UEM and Ivanti Neurons for MDM.

A Space allows for delegated administration of the following system components. Users and User Groups currently cannot be delegated.

- Devices
- Configurations
- Policies
- Device Groups
- Applications
- An App Catalogue
- An Apple Apps and Books Token

When an administrator logs in to the Ivanti Neurons for MDM Admin Portal on a tenant with at least a single Delegated Space, the administrator is presented with the Admin Portal login promo pop-up. The promo pop-up will not be displayed after delegated space creation and during user login if a delegated space is already created.

Roles for global and delegated Space administrators

An admin user with the appropriate roles to access the Default Space is referred to as a Global Admin. Access to the Default Space can be read-only or read-write access. A Global Admin with the appropriate Administrative Roles can create Delegated Spaces and assign Delegated Admins to manage them. A Delegated Admin can be assigned to manage one or more Delegated Spaces.

The Spaces that a given administrator can access are listed in the Spaces selector drop-down in the upper left-hand corner of the Devices and Apps tabs. To view and manage a Space, use the Spaces drop-down to switch to the desired Space.

A Global Admin has visibility and control over all Delegated Spaces, in addition to the Default Space. A Delegated Admin has visibility and control over only the Spaces which are assigned to them by a Global Admin. A Global Admin maintains central control over Delegated Spaces while a Delegated Admin has autonomy to manage the Spaces that have been delegated to them. This level of autonomy is determined by whether delegation is inherited or copied from the Default Space.

The following are the different user roles and the tasks that they can perform:

Inherited app in a delegated Space

- Existing Ratings or Reviews at time of delegation are inherited and visible to users in Del Space, including author username.
- Delegated Administrator cannot delete Ratings/Reviews for an inherited app.
- Delegated Administrator can export Ratings/Reviews for an inherited app.

- Users in Delegated Spaces can add Ratings/Reviews to inherited app.
- Users in Delegated Spaces can view Ratings/Reviews added by Users in Del Spaces, including author username.

App in a delegated Space (added, not inherited)

- Only Global Admin can enable or disable Reviews from **Apps > Catalogue Settings > Ratings & Reviews**.
- Users in Delegated Space can add Ratings/Reviews.
- Delegated Administrator can Delete reviews added by users in the same Delegated Space.
- Users in other Delegated Spaces, including Default, cannot view Ratings or Reviews added by Users in each Delegated Spaces.
- Delegated Administrator can export reviews added by all users, including usernames.

Delegated app in a default Space

- Global Admin can delete Ratings or Reviews added by a user in a Delegated Space.
- Global Admin can export all Ratings or Reviews including those added by users in Delegated Spaces.
- Users in Default Space can view Ratings or Reviews added by users in Delegated Spaces, including username.

Priority of a delegated Space

The Default Space in an UEM System always has the lowest priority. The priority of a Delegated Space relative to other Delegated Spaces is set by the Global Admin and can be changed at any time. Delegated Spaces are listed rank ordered, from highest priority to lowest on the Spaces page under the Admin tab in the Admin Portal.

Delegation through inheritance or copy

A key concept in delegated administration is whether a system component is inherited or copied from the default Space.

12.1.6.2. Managing Spaces

Spaces enable you to designate device groups for management by different administrators (delegated administration). The administrator for a space can define the configurations and policies applied to the devices in the space. After you create the spaces, you can assign each space to the relevant or appropriate administrator.

This space page includes:

- Search capabilities to quickly locate spaces.
- Pagination controls to navigate large numbers of spaces.
- Space prioritization controls for managing delegated space order.
- Options to select and delete multiple spaces.

> Default space cannot be deleted.

- Alphabetical sorting of spaces.
- A list of recently viewed spaces in the space selector.
- Persistent space selection across the Devices, Configurations, Policies and Content pages, reducing the need to reselect a space when navigating between pages.

> The user can view only the spaces assigned and not all the available spaces. As of now, this setting applies to the **Devices**, **Device Groups**, **Apps**, **App Inventory**, **Content**, **Configurations**, **Policies**, and **Certificate Management** modules only. Spaces selected from the Spaces list while viewing any of these modules are saved as administrator preferred default selection for that module. These preferences are not only saved for the current login session, but also for the future sessions.

The spaces you create inherit all configurations from the default space. Therefore, any configurations you create later in the default space are eligible to be applied to the other spaces. However, changes made to an existing configuration are not inherited.

The spaces you create receive copies of only those policies that exist in the default space at that time. Any policies you create later in the default space apply only to the default space.

Create the rules that define which devices are in the space. These rules can be filtered using the applicable operators, including the "begins with", "ends with", "contains", "does not contain", "does not begin with", "does not end with", "is less than", "is greater than", "is in range", "is equal to", and "is not equal to" operators. The rules can be nested together using the ANY (OR) or ALL (AND) options. The accuracy of the rules can be reviewed using the text that appears at the end of the rules.

The Ivanti Neurons for MDM Administrator portal displays the number of duplicate user groups and the corresponding number of GUIDs to identify duplicate groups, when the User Group Name attribute is selected in the rule builder. Also, a table under this rule displays the list of the duplicate user groups and their details such as User Group Name, GUID, Source and distinguished name (DN).

Rules can identify devices by:

- Entra ID Enrolled
- APNS Capable
- Alternative Serial Number (Android Only - applicable for Samsung devices in Device Admin or Device Owner mode)
- Android 5G Network Slicing Enabled
- Android Work Managed Device Non-GMS mode (AOSP) Enabled

- Android Dedicated Device
- Android Enterprise Capable
- Android Managed Device with Work Profile
- Android SafetyNet Attestation Type
- Android Work Enabled
- Android Security Patch Level (Android devices)
- Android Work Managed Devices (Device Owner) Enabled
- Android Work Profile Enabled
- Android Work Profile Enabled on Company Owned Devices Enabled
- Anti-phishing native status
- Anti-phishing status
- Anti-phishing VPN status
- Automated Device Enrollment Enrolled
- Automated Device Enrollment Enabled
- Autopilot Enrolled
- Azure Client Status Code
- Azure Device Compliance Report Time
- Azure Device Compliance Status
- Azure Device Identifier
- Sentry Blocked
- Access Blocked
- Bootstrap Token Available
- Bulk Provisioned Type (Apple Configurator or None)
- Carrier
- Client Last Check-in
- Client Registered
- Compliance
- Compliance Action Blocked
- Current Country Name (select the country name from the drop down list)
- Current MCC
- Current MNC
- Custom Device Attribute
- Custom LDAP Attribute
- Custom User Attribute
- Data Roaming
- Device Source
- Device Type

- Device Type (Apple)
- Display Name
- Encryption Enabled
- Home Country Name (select the home country from the drop down list)
- Home MCC
- Home MNC
- IMEI
- IMEI2 (only on Android devices with a dual SIM port and applicable for Android 8.0 or higher devices)
- Institutional Recovery Key Enabled
- IP Address
- Kiosk Mode
- Last Check-in
- Lost Mode Enabled
- MAM Only
- Manufacturer
- MTD activation status
- Multi-User Mode
- OS
- OS Version
- OS With Version
- Ownership
- Personal Recovery Key Enabled
- Phone No.
- Quarantined
- Recovery Lock Enabled
- Roaming
- Secure Apps Status
- Serial Number
- Status
- Supervised
- Supplemental Build Version
- Supplemental OS/Version Extra
- Unlock Token Available (iOS)
- User Enrollment Enrolled
- User Group
- Username
- Voice Roaming

- macOS Personal Recovery Key escrowed
- macOS Recovery Key Type

> These rules are available only for **Silver** license and above.

Creating a Space

Procedure

1. Go to **Admin** > **System** > **Spaces**.
2. Click **Create New Space**.
3. Enter a Space name.
4. Configure the appropriate rules and settings for the space.
5. Click **Save**.

Prioritising Spaces

Ivanti Neurons for MDM assesses spaces in order of appearance.

Procedure

1. Click **Prioritize Spaces**.
2. Select the up or down icon next to a space to adjust its priority.
3. Click **Save**.

Deleting Spaces

1. Go to **Admin** > **System** > **Spaces**.
2. Select one or more spaces using the check boxes.
3. Click **Delete**. Confirm the deletion when prompted

Assigning an Administrator to a Space

Procedure

1. Go to **Users**.
2. Search for the user who will be the administrator.
3. Click the link for the user to display detail.
4. Select Actions > Assign Roles.
5. Select **Device Management**.
6. Under **Device Management**, select the space for this administrator.
7. Click **Done**.

When this administrator logs in, only devices, configurations, and policies in the assigned space will be visible.

Cloning a Configuration or a Policy

You can clone a configuration or a policy if you need to duplicate them with a few differences. You can also associate the cloned configurations or policies to different device groups. All the policies can be cloned within a space. All configurations, except the user-provided Identity Certificate and Threat Defense, can be cloned within a space. The following configurations can also be cloned across spaces from the default space:

- iOS Restrictions
- Web Clip
- Certificate
- Passcode
- SCEP (iOS and Windows)
- Identity Certificate (dynamically generated)

- The name of a configuration or a policy type should be unique in a space. All other properties of a configuration or a policy can be cloned.
- The configurations will be cloned to all spaces which you, the administrator, have access to. You do not need to be a Global Administrator to clone a configuration.

Procedure

1. Go to **Configurations** or **Policies** depending on what you want to clone.
2. Click the link for the configuration or the policy to display the details.
3. Click the **Clone** icon.
4. In the pop-up window, enter a **Name** and optionally a **Description**.
5. Click **Next**.
6. Modify the configuration or the policy as per your requirements.
7. Click **Next**.
8. Configure the distribution.
9. Click **Done**.

For more information, see Space examples.

12.1.6.3. Space Examples

This topic provides examples related to how spaces can be used by administrators.

Administrator per location

ACME, Inc. has offices in North America and Europe. Due to language and time zone issues, ACME wants an administrator in the US to manage North American devices and an administrator in Germany to manage European devices.

To set up these Spaces, ACME made these changes:

1. Created a user group in Ivanti Neurons for MDM for users in Europe.
2. Created a user group in Ivanti Neurons for MDM for users in North America.
3. Created a Europe Space with the following rule:
4. User Group = Europe
   Created a North America Space with the following rule:
5. User Group = North America
   Assigned the Device Management role for each Space to the proper administrator.

ACME now has the following Spaces:

- Europe
- North America
- Default

Administrator per OS per location

ACME has decided that only Android experts should administer Android devices. One Android expert has been added to the North American organisation, and one has been added to the European organisation. So two new Spaces are needed.

To add the Spaces, ACME made these changes:

1. Created a Europe-Android Space with the following rules:
2. User Group = Europe
   OS = Android
   Created a North America-Android Space with the following rules:
3. User Group = North America
   OS = Android
   Assigned the Device Management role for each space to the proper administrator.

ACME now has the following Spaces:

- Europe-Android
- North America-Android
- Europe
- North America
- Default

Administrator for executives

ACME's executives have decided that they want special service from a special administrator. Only the most important executives are on this list.

To add this Space, ACME made these changes:

1. Created an Executives Space with the following rules:
2. Username = jdoe@acme.com
   Username = gkunz@acme.com
   Username = prizzo@acme.com
   Username = fvanhoff@acme.com
   Moved the Space to the top of the list in the **Space** page.
3. Otherwise, executives with Android devices would have the wrong administrator.
   Assigned the Device Management role for the Space to the special administrator.

ACME now has the following Spaces:

- Executives
- Europe-Android
- North America-Android
- Europe
- North America
- Default

Administrator for all other devices

When ACME opens a new office in Japan, the added devices will be assigned to the administrator of the default Space until someone creates a Japan Space.

12.1.6.4. Delegating Devices

Spaces are used to separate your devices into independently managed entities. Membership for Spaces is determined by rules you create. Device delegation allows a Global Admin to partition and independently manage devices in an UEM system. When devices are delegated, access to those devices can be assigned to a subset of delegated administrators, thus distributing admin responsibilities.

Delegated devices can be grouped into device groups and different custom configurations can be applied to them without affecting devices in the default Space or other Spaces.

Creating rules for delegating devices

The rules you define for a Space determine which devices belong to the Space. A device can belong to only one Space. Devices that do not match the rules for the Spaces you create automatically belong to the default Space.

1. Select **Any** if you want devices to be included in this definition if they meet any of the rules.
2. Select **All** if you want devices to be included in this definition only if they meet all of the rules.
3. Select one of the following rule types from the dropdown:
    - **Custom LDAP Attribute:** For rules based on LDAP attributes.
    - **OS**: For rules based on the device's operating system.
    - **User Group**: For rules based on the device's user group (as defined in the device management service).
    - **Username**: For rules based on the username associated with the device.
4. Define the criteria for the selected rule type:
    - **Custom LDAP Attribute:** Enter the name of the custom LDAP attribute that was configured in the LDAP settings.
    - **OS**: Select Android, iOS, macOS, or Windows.
    - **User Group**: Select one of the user groups displayed in the dropdown. These are the user groups defined under **Users > User Groups**.
    - **Username**: Type in a username.
5. To add another rule for this Space, click the + next to the previous rule.
6. Click **Preview** to see which devices will be assigned to the Space.
7. Click **Save** when you are satisfied with the devices in the Space.

Devices that no longer match the rules for a Space are automatically moved to the next matching Space. If the device does not match the rules of an existing Space, then the device moves to the Default Space. For example, removing a user from a user group can cause that user's devices to move to a different Space. Moves to a different Space can result in changes in policies and configurations.

12.1.6.5. Delegating Apps

App delegation allows a Global Admin to partition and independently manage apps in Ivanti Neurons for MDM. The Global Admin can centrally source and distribute public and in-house apps while maintaining the separation and control provided by delegated Spaces.

By centrally distributing an app, the Global Admin can predefine the management behavior of the app through app configurations as well as the apps' distribution rules. The app can then be delegated and made available in the App Catalogue of the delegated Space.

The delegated app is then distributed to users within a given delegated Space. When applications are delegated, access to those applications can be assigned to a subset of Delegated Administrators, thus distributing admin responsibilities.

App delegation requires one or more Delegated Spaces to be defined first. When an application is delegated it is assigned to all Spaces. App delegation Space is classified into:

- Default Space
- Delegated Spaces

Adding an app to a delegated Space

An application can be added to a Delegated Space by a Delegated or a Global Admin. The app appears only in the App Catalogue of the Delegated Space where it was added. If you add a previously delegated app from Default Space to a Delegated Space, it will result in an error. In this case, inheritance for the app must be first disabled in the Default Space so that it can be added to a Delegated Space. For more information, see **Adding a configuration** in Working with Configurations.

App distribution in a delegated Space

When an app is delegated from the Default Space, its Distribution rules are inherited. This app will be distributed to all the devices assigned to the Delegated Space which match the Distribution rules for the app.

The global administrators can delegate space administrators to edit the Dynamically Generated Identity Certificate for All Devices and for the Custom distribution option.

> The distribution changes are applicable only to the specific space. All other spaces continue to inherit the default space distribution settings.

> App approval settings for Android apps: App approval settings per space for Android apps is not supported. Apps approved in custom space take effect in all the spaces.

> Existing Android catalog apps: On tenants where public Android apps have already been added in default space, apps need to be undelegated before that public app can be added in another non-default space.

> Android Enterprise apps can be added only by the tenant-level admin, and **not** by the space-level admin. Managed Google Play is configured at the organization level, not per delegated space. As a result, new Android Enterprise apps can only be approved in the Default Space. Delegated admins can assign and manage already approved apps within their own spaces, but they cannot approve or add new Android Enterprise apps from within Delegated Spaces. All new apps must be approved in the Default Space first, and only then can they be assigned to the appropriate groups.

For more information, see **Adding a configuration** in **Working with Configurations**.

12.1.7. Support Administrators

Create a temporary support administrator to enable the service support team to log in with your **roles** and permissions. This user expires automatically in 7 days, or you can end access at any time. Creating a support administrator makes it easier for the support team to troubleshoot issues.

Creating a support administrator

Procedure

1. In the **Support Administrators** page, click **Add Support User**.
2. Click **Create User** to confirm.

This step sends an email to the device management service support team.

> The **Display Name** field shows "(disabled)" until a support team member activates the new account. The resulting display name will have the following format:

support-[random_ID]-[your_username]@[your_company].com

Once you create a support administrator, selecting **Admin > Support Administrators** takes you directly to the list of existing support administrators. Therefore, if you need to create additional support users, go directly to step 2 above.

> Newly created Support Administrator accounts are read-only by default. Custom roles aren't assigned automatically, reducing the risk of unintended configuration changes. An administrator can add roles and permissions later as needed.

Viewing user history

In the **Support Administrators** page, click **User History** to view the login history of the support administrators. The availability of the login history data in the Support Administrators page is restricted to the last 90 days of data.

Ending access for a support administrator

Procedure

1. In the **Support Administrators** page, click the **Delete** link to the right of the account you want to remove.
2. When prompted, click **Remove User** to confirm.

Suspending access for a support administrator

In the **Support Administrators** page, click the **Disable** link to the right of the account you want to suspend.

12.1.8. Admin > System Use Notification

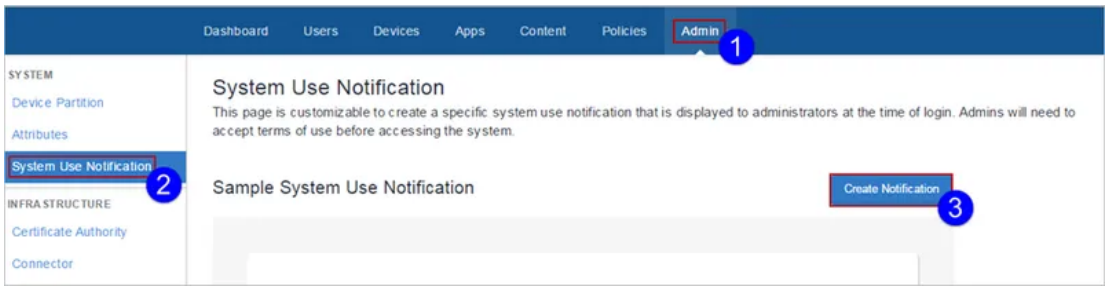
Licence: Silver

Use the System Use Notification feature to create a customised system use notification that appears to administrators at the time of login, and requires administrators to accept terms of use before accessing the system.

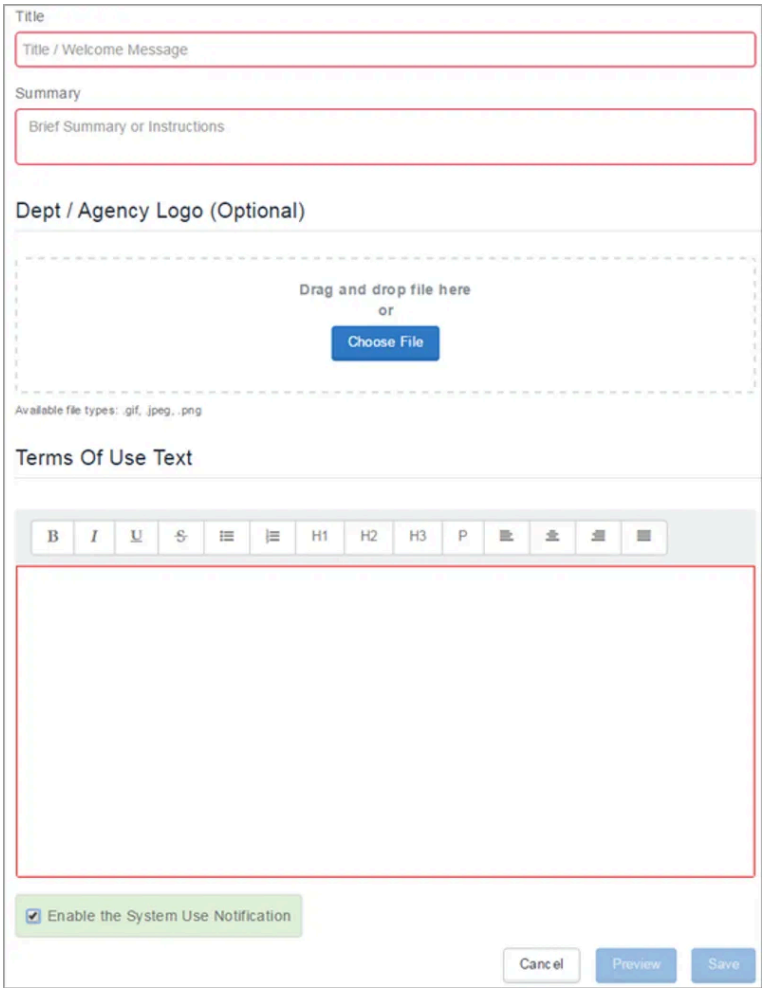
Creating a system use notification

Procedure

1. Select **Admin > System Use Notification**.
2. Click **Create Notification**.



The System Use Notification Details page appears.



Enter a title in the **Title** field.

4. Enter a summary or instructions in the **Summary** field.
5. Choose a logo if desired.
6. Enter terms of use text in the **Terms of Use Text** field. This is the text that the administrator will have to accept at login.
7. Place a check mark in the **Enable the System Use Notification** check box to turn on the notification.
8. Click **Preview** to invoke a preview of the system use notification.
9. Click **Save** when you are satisfied with the system use notification.

12.2. Infrastructure

This section contains the following topics:

- Access
- App Lists
- Exporting Audit Trails
- Certificate Management
- SCEP Configuration for External Certificate Authorities
- Derived Credential Providers
- Connector
- Using the httpproxy command for Connector
- Help@Work
- Infrastructure Identity
- Configuring LDAP server
- Sentry
- Enable Kerberos Authentication between Ivanti Neurons for MDM and SCEP server

12.2.1. Access

Applicable to: iOS and Android devices.

Access keeps business data secure while enabling a seamless and productive user experience on any device or app. Access establishes a data boundary that prevents users from accessing enterprise cloud services on unsecured devices, apps or cloud services.

Latest documentation

Visit **Product Documentation** and click Access for more information about Access and how to set up Access. Select the document appropriate to your version of Access.

12.2.2. App Lists

Licence: Silver

You can create lists of required, Allowlisted, and Blockedlisted apps for use with the **Allowed Apps policy**, where you can use these lists to help specify actions to take if a device's installed apps do not meet the requirements implied by the app lists. You cannot edit app lists once created because app lists can be referred to in **Allowed Apps policies**. Similarly, you cannot delete app lists referred to by any allowed apps policies.

Creating app lists

Procedure

1. Click **Admin > Infrastructure > App Lists**.
2. Click **Create New List**.
3. Under **App List Name** box, enter a name for the list.
4. Select the type of list, **Whitelist**, **Blacklist**, or **Required**.
5. Under **Add Apps** section, select the app type, **App Store**, **OS X store**, **Google Play**, or **App Catalog**.
6. Enter search criteria to narrow your choices.
7. Use the check boxes to select apps. You can use multiple searches and enable more than one check box.
8. Click the **View Apps** tab for a list of apps you have selected so far.
   Click **Save**.

Now you can use this list when you configure the **Allowed Apps** policy.

If you cannot see the **App Lists** page, it might be that you do not have the required permissions. You need one of the following **roles**:

- System Management
- System Read Only

12.2.3. Exporting Audit Trails

Audit Trails export is a feature which is used to export and upload all the audit trails information to a specific server location. The server should be accessible from the default port. Users can configure Audit Trail Export settings to get archives of Audit Trails automatically uploaded to a specific location on a daily basis.

> Audit Trails export is supported on Linux-based and Windows-based SFTP servers.

To configure the settings for exporting Audit Trails:

1. Select **Admin > Infrastructure > Audit Trails**. The **Audit Trails** page is displayed.
2. In the **Audit Trails** page, click **ON** to enable the export of audit trails.
3. In the **Export** section, update the following fields:

Feature	Description
Export format	Select any of the following format in which the Audit Trails data should be exported: • **JSON** • **CEF** (Common Event Format) The CEF log message contain the following default values: ◦ Version: CEF format version number. v25 is the current supported version. ◦ Device Vendor: Ivanti Inc ◦ Device Product: Ivanti Neurons for MDM ◦ Device Version: Latest Ivanti Neurons for MDM version at the time of event generation. ◦ Device Event Class ID: Entity ID unique per trail ◦ Name: Entity name and action per trail. Example: Promotion distribution configuration settings Create. ◦ Severity: Specifies the importance of the event. Example: Low. The CEF log message also includes extension fields which are a collection of the following key-value pairs: ◦ CS1 & CS1Label: Audit Trails meta data such as createdAt, entityType, entityName, and actionType. ◦ CS2 & CS2Label: Actor information. ◦ CS3 & CS3Label: Before action state. ◦ CS4 & CS4Label: After action state. In CEF export, if any of the fields(example: CS3 or CS4 keys) exceed the specified limitations, the actual value is replaced with the text "Value for this key exceeds mapped dictionary key allowed length".
Server	Enter the name of the server to exporting Audit Trails.
User	Enter the user name to login to the server.
Password	Enter the server login password.
Server path	Enter the path of the server and ensure that the given path exists on the server. Example: /Users/Test/Export.
Key Exchange Algorithm	Select the list of key exchange algorithms for exporting audit log for the outgoing SFTP configuration. The following key exchange algorithms are selected by default: • **diffie-hellman-group-exchange-sha1** • **diffie-hellman-group14-sha1** • **curve25519-sha256** • **diffie-hellman-group-exchange-sha256** (selected by default)
Ciphers	Select the list of encryption ciphers for exporting audit log for outgoing SFTP configuration. The following encryption ciphers are selected by default: • **aes128-ctr** • **aes192-ctr** • **aes256-ctr** (selected by default)

Feature	Description
HMAC	Select the list of HMAC algorithms for exporting audit log for the outgoing SFTP configuration. • **hmac-sha1 (selected by default)** • **hmac-sha2-256** • **hmac-sha2-512**

Note: The fields mentioned above will be in read-only mode if these fields are already configured. To edit the configured fields, you should click the **Edit** button. If the admin had already configured SFTP export, then after the upgrade all the Key Algorithms are selected.

Click **Test Connection and Save** to test the server connection and to save the Audit Trails export configuration.

The archived Audit Trails files are available in JSON format in a .zip file.

Verify the configuration settings in all the fields before saving the Audit Trails export settings. An error message is displayed if any of the entered field values are invalid.

Enable Audit Trails for Device Enrollment and Unenrollment in Spaces

When enabled, device movement between spaces is audit logged, including events triggered by device registration, device deletion, and space updates or deletion. Space admins can identify affected devices, filter logs by space and activity type, and export audit records to CSV.

12.2.4. Certificate Management

Licence: Silver

Using certificate authentication is an effective way to secure your mobile devices. Certificates are more secure than passwords, and they enable you to use a single credential to protect VPNs, wireless networks, email, etc. If your organisation has access to an external certificate authority, you can use a Connector to access it. If your organisation does not have access to a certificate authority, you can use Ivanti Neurons for MDM as a certificate authority. You can also use it as an intermediate certificate authority to other certificate authorities. The certificates generated by Ivanti Neurons for MDM are called self-signed certificates.

- SHA-1 certificates are deprecated while creating the identity certificates. You can choose other algorithms. While updating the certificates, if the older certificates use SHA-1, the same SHA-1 algorithm can be used. If the older certificates use an algorithm above SHA-1, then reverting to SHA-1 is not allowed.
- During the configuration of the local or external certificate authority, select the **Cache Identities on** Ivanti Neurons for MDM option to store certificates with the Ivanti Neurons for MDM service. Clear cache to generate certificates each time as needed.
- Certificates will be re-issued implicitly.
- For improving system efficiency, the certificates for the admin-created configurations are generated offline, using a First In First Out (FIFO) queue. During the period when the configurations are being generated offline, the configuration state will be **Pending Certificate Generation** under the **Status** column in the **Configurations** tab on the **Device Details** page. After the certificates are generated, the configurations are moved to the **Pending Install** state and are pushed, along with the certificates, to the devices via automatic force check-ins.
- All Certificate Authority certificates, including the certificates signed by DigiCert PKI Platform or GlobalSign external Certificate Authorities, are revoked when a device is retired, wiped, and when certificates are regenerated.

As an administrator, you can generate Ivanti Neurons for MDM certificate for smart card logon and custom object IDs (OIDs). You can generate certificates for the following authentication options:

- Client Authentication - enabled by default
- IPSEC – optional, admin can enable
- Smart Card Logon – optional, admin can enable
- Custom OIDs - optional, admin can enable

> This feature is only applicable for the following certificate authorities:
>
> - Local Certificate Authority
> - Intermediate Certificate Authority
> - External Certificate Authority - configure the application policies of CA template in NDES server to support IPSEC , Smart Card Logon and custom OIDs

> In the Device Admin, App Station, or other non-Android Enterprise modes, Certificate Management is not supported on Samsung devices using Samsung APIs. It is recommended to verify transition to Android Keystore based on Samsung recommendation.

For more information, see **Certificate configuration**.

Connecting to an on-premise SCEP certificate authority

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Install and configure a Connector (**Admin > Connector**). For more information, see **Connector**.
3. Go to **Admin** > **Infrastructure** > **Certificate Management**.
4. Click **Add** under the **Certificate Authority** section.
5. Select **Add an on-premise SCEP Certificate Authority** and click **Continue:**
6. Enter a name that identifies the configuration.
7. Select one of the following Certificate Authority Type:
   - Microsoft
   - EJBCA
   - Generic SCEP Server
     The Generic SCEP Server option can be used with most SCEP servers having a static challenge password.

Complete the displayed form.

9. Click **Done**.

Creating an external Certificate Authority

Choose this option if you want to use a third party Certificate Authority.

Procedure

1. In the **Certificate Management** page, click **Add** under **Certificate Authority** section.
2. In the Add Certificate Authority page, under Create an external Certificate Authority, click **Continue**.
3. Select GlobalSign or DigiCert PKI Platform as the external Certificate Authority.
4. Complete the remaining fields on the displayed form.
5. Click **Done**.

Viewing a certificate of the external certificate authority

You can view the details of a certificate and upload the intermediate/alternate root certificate for this certificate authority to replace the existing stored copy.

Procedure

1. Under the **Certificate Authority** in the **Certificate Management** page, click **Actions** next to the external certificate authority, and then click **View Certificate**. The **View certificate** window is displayed.
2. In the **View Certificate** window, click **Upload Certificate**. The **Upload Certificate: External CA** window is displayed.
3. Click **Choose File** to select the certificate to be uploaded.
4. Click **Done**.

Creating an intermediate certificate authority

- If you need a certificate, then generate a CSR and submit it to the signing authority. Once you receive the certificate from the signing authority, upload the certificate.

- If you already have the necessary certificate, upload it.

Generate a CSR (certificate signing request)

Procedure

1. Under the **Certificate Authority** section in the **Certificate Management** page, click **Add**
2. In the Add Certificate Authority section, under Create an Intermediate Certificate Authority, click **Generate CSR**.
3. Complete the displayed form.
4. Click **Generate**.
5. Copy the content between BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST to a text file.
6. Upload the text file to the certifying authority.
7. Click **Done**.

Uploading the signed certificate

Once you receive the signed certificate from the certifying authority you can upload the signed certificate.

Procedure

1. Under the **Certificate Authority** section in the **Certificate Management** page, find the entry for the CSR you generated.
2. Under section, select **Actions > Upload New Signed Certificate**.
3. Click **Choose File**.
4. Select the new signed certificate.
5. Click **Done**.

Uploading an existing certificate

This topic describes how to upload a signed certificate.

Procedure

1. Under the **Certificate Authority** section in the **Certificate Management** page, click **Add**.
2. In the Add Certificate Authority section, under Create an Intermediate Certificate Authority, click **Upload Existing Identity**.
3. In the **Name** field, enter a name for this certificate that distinguishes it from others.
4. Click **Upload**.
5. Select the certificate.
6. Enter the password for the certificate.
7. Click **Upload**.

Viewing a certificate of the intermediate certificate authority

You can view the details of a certificate and get the CRL(Certificate Revocation List) URL of the certificate authority.

Procedure

1. In the **Certificate Authority** section, click **Actions** next to the certificate authority and click **View Certificate**. The **View certificate** window is displayed.

2. In the **View Certificate** window, you can view the URL in the **CRL URL** field.
3. Click **Copy** to copy the URL to a clipboard and paste in another application. This URL can be used to configure Office 365 to accept certificates issued by the certificate authority.

Creating a Standalone Certificate Authority

Choose this option if you want to create a new, completely standalone (local and self-signed) Certificate Authority.

Procedure

1. Under the **Certificate Authority** section in the **Certificate Management** page, click **Add**.
2. In the Add Certificate Authority page, under Create a Standalone Certificate Authority, click **Continue**.
3. Complete the displayed form.
4. Click **Generate**.

Standalone Certificate Authority Expiry Notification

The Standalone (local) certificate authority expiry info is now visible as a tooltip under the **EXPIRATION DATE** column if the certificate expiry date is less than 30 days.

If the expiry date is less than 365 days, in addition to the notification sent, this info can be viewed under the **Dashboards** > **Notifications**. Select **Expiration** as filter.

Configuring the expiration period of the standalone certificate authority

You can configure the expiration period of the standalone (local) certificate authority.

Procedure

1. Under the **Certificate Authority** section in the **Certificate Management** page, click **Actions** next to the standalone certificate authority.
2. Click **Edit**.
   The **Edit Certificate Authority** window is displayed.
3. In the Client Certificate Template section, in the **Certificate Lifetime** field, enter the new expiration period in days.
4. Click **Save**.

You may receive notifications and emails (if optionally enabled) when the certificates issued by a local certificate authority are about to expire or are already expired.

- Notification on the days of the certificate expiry - Notifications are generated at pre-determined intervals during a certificate expiration window. The first notification occurs 365 days before expiration, followed by additional notifications that occurs 180 days, 60 days, 45 days and 7 days before expiration. You will receive this notification until you replace the certificate by navigating to **Admin > Certificate Management> Actions > Upload New Signed Certificate**.
- Notification on the expired certificate - you receive a notification when the certificate expires. You will have to replace the certificate to resume normal service.
- Notification when a new valid certificate is uploaded - The notification will be sent when the new signed certificate is uploaded.

Viewing a certificate of the standalone certificate authority

You can view the details of a certificate and get the CRL (Certificate Revocation List) URL of the local certificate authority.

Procedure

1. Under the **Certificate Authority** section in the **Certificate Management** page, click **Actions** next to the local certificate authority and click **View Certificate**. The **View certificate** window is displayed.
2. In the **View Certificate** window, you can view the URL in the **CRL URL** field.
3. Click **Copy** to copy the URL to a clipboard and paste in another application. This URL can be used to configure Office 365 to accept certificates issued by the local certificate authority.

Viewing a CRL lifetime of a Certificate Authority

You can view and edit the CRL lifetime of a local or intermediate certificate authority.

Procedure

1. Under the **Certificate Authority** section in the **Certificate Management** page, click **Actions** next to the local certificate authority and click **Edit**. The **Edit Certificate Authority** window is displayed.
2. In the **Edit certificate Authority** window, you can view the CRL Lifetime value. The minimum default value is 24 hours. The maximum value that can be entered is 10,950 hours.
3. Edit the CRL lifetime value and click **Save**.

Creating a Cloud Certificate Authority

Choose this option if you want to use a Cloud Certificate Authority.

Procedure

1. Go to **Admin** > **Infrastructure** > **Certificate Management**.
2. In the **Certificate Management** page, under the **Certificate Authority** section, click **Add**.
3. In the **Add Certificate Authority** page, under **Connect to a publicly-trusted Cloud Certificate Authority**, click **Continue**.
4. Enter a name in the **Name** box.
5. Select a Cloud Certificate Authority from the following options:
   - **Atos IDnomic CMS**
   - **DigiCert One PKI Platform**
   - **DigiCert PKI Platform**
   - **Entrust**
   - **GlobalSign**
6. Enter the base URL and upload the certificate data.
7. Click **Done**.

Using Advanced Search on certificates

You can use the Advanced Search option to search for issued certificates based on rules to identify and view the certificates with specific criteria. These rules can be filtered using the applicable operators, including the "begins with", "ends with", "contains", "does not contain", "does not begin with", "does not end with", "is less than", "is greater than", "is in range", "is equal to", and "is not equal to" operators. The rule options can be nested together using the ANY (OR) or ALL (AND) options. The issued certificates matching the

rules are displayed below the section. Starting from Ivanti Neurons for MDM release 76 the operators for all the certificate management templates have standard operators. The operators of the following templates are standardized in this release:

- Admin> Certificate Management> Issued Certificates> Advanced Search

Advanced Search on Issued Certificates

Procedure

1. Under the **Issued Certificates** section in the **Certificate Management** page, click the **Advanced Search** link.
2. Click **Any** if the users need to match at least one of the rules, or Click **All** if the certificate need to match all the rules.
3. Create a rule that defines the search criteria, for the following attributes:
    - **CA**
    - **Configuration Name**
    - **Expiry**
    - **Is Private Key**
    - **OS**
    - **Serial Number**
    - **Status**
    - **Usage Type**
    - **User**
4. (Optional) Click + to create additional rules, if needed.
5. (Optional) Click **Save** to save the query.
6. Click **Search**. The list of users matching the search criteria are displayed in the page.

Advanced Search on User Provided Certificates

Procedure

1. Under the **User Provided Certificates** section in the **Certificate Management** page, click the **Advanced Search** link.
2. Click **Any** if the users need to match at least one of the rules, or Click **All** if the certificate need to match all the rules.
3. Create a rule that defines the search criteria, for the following attributes:
    - **Certificate Name**
    - **Expiration Date**
    - **Issued By**
    - **Uploaded On**
4. (Optional) Click + to create additional rules, if needed.
5. (Optional) Click **Save** to save the query.
6. Click **Search**. The list of users matching the search criteria are displayed in the page.

Loading the Search queries for issued certificates

To view the list of saved Search queries.

Procedure

1. Under the **Issued Certificates** section in the **Certificate Management** page, click the **Advanced Search** link.
2. Click the 'Folder' icon. The **Advanced Search** window is displayed. The list of the created Search queries are displayed in the **Load Query** section. The following details are displayed in this section:
   - **Query Name** - The name of the loaded query.
   - **Query Content** - Displays the content on the rules defining the search query.
   - **Actions** - Select the action to be performed on the query.
3. Click **Load Query** in the **Actions** column to view the list of issued certificates matching the criteria defined in the loaded query. To delete a loaded query, click the Delete icon.

> Click **Export to CSV** to download the search result report contents in a CSV file for later reference or analysis.

Viewing the expiration period of the issued certificates

Under the **Issued certificates** section, in the **Expires (in days)** column you can view the days remaining for the certificate to expire if the expiry is within the next 30 days. If the certificate had already expired within the last 30 days, the **Expires (in days)** column for the certificate displays the number of days passed from the date of expiry.

For more information, see SCEP configuration for external certificate authorities.

Export to CSV

You can export the certificates to a CSV file for later reference or analysis.

Procedure

1. In the **Certificate Management** page, go to one of the following tabs.
   - **Certificate Authority**
   - **Issued Certificates**
   - **User Provided Certificates**
2. Click **Export to CSV**.
3. Click **Download**.
4. (Optional) Click **Delete** to delete the report.

12.2.5. SCEP Configuration for External Certificate Authorities

This feature enables support for Simple Certificate Enrollment Protocol (SCEP) configuration for external certificate authorities for Windows 10 devices.

> Delegation with custom distribution option is available for this configuration. For more information, see *Distributing the configuration* topic in **Working with Configurations**.

Setup an External Certificate Authority

You must first setup an External CA. You can skip to the next section if you already have an External CA.

1. Go to **Admin >Infrastructure > Certificate Management**.
2. Click **+Add**.
3. Enter a name for the Certificate Authority.
4. Use the pull-down menu to select Microsoft as the **Certificate Authority Type**.
5. Enter the **SCEP URL**.
6. Enter the **Username** and **Password**.
7. Enter the **Challenge URL**.
8. Click **Save**.

SCEP Configuration

Now you can proceed with the SCEP configuration.

1. Go to **Configuration > +Add**
2. Select the Windows icon.
3. Select **Identity Certificate** to go to the **Create Identity Certificate Configuration** page.
4. Enter a name for the configuration.
5. Select **Windows Config** from the list of SCEP configurations from the **Certificate Distribution** pull-down menu.
6. Select the External CA.
7. Enter the Certificate Distribution details.
    - Enter the subject. For example: CN=$
    - Select the number of Retries from the **Retry** pulldown menu.
    - Select the number of seconds to wait before each entry from the **Retry delay** pulldown menu.
    - Select a key size from the **Key Length** pulldown menu.
    - Select at least one certificate usage option.
    - Enter the length of time in the **Validity** field and pulldown menu.
    - Enter the CA Thumbprint.

- Go to the SCEP challenge URL copy the CA Thumbprint and paste it here or click **Create from Certificate**... to upload the certificate from which the CA Thumbprint can be created.
  Select at least one hashing algorithm from the **Hash Algorithm Family** options.

8. Click **Next**.

12.2.6. Derived Credential Providers

In the Derived Credential Providers page, you can view the list of derived credential providers used for certificate distribution. You can specify which derived credential providers should be set as default and also add other custom derived credential providers that you use.

To set a derived credential provider as default:

1. Go to **Admin > Derived Credential Providers**. The following derived credential providers are listed in the page.
    - **Entrust**
    - **Intercede**
    - **Purebred**
2. For the provider which you want to set as default, click **Set as Default** under the **Actions** column. When set, the check mark icon is displayed under the **Default provider** column for the provider indicating that it is the default credential provider.

To add a custom derived credential provider:

1. Go to **Admin > Derived Credential Providers**.
2. Click **+Add** .
3. Type the name of the derived credential provider in the text field under the **Name** column.
4. Click **Save**.
   When added, this custom derived credential provider is available as an option to be selected under **Brand** field while configuring the Derived Credential distribution under **Identity Certificate** configuration.

Click **Delete** under the **Actions** column to delete a derived credential provider.

> You will not be able to delete the derived credential provider if it is set as default.

12.2.7. Connector

Licence: Silver

Ivanti Neurons for MDM Connector provides access from your Ivanti Neurons for MDM service to corporate resources, such as an LDAP server or a Certificate Authority (CA). Set up one Connector per resource that you would like to access.

If you use Microsoft Active Directory or an LDAP server hosted in Amazon Web Services (AWS), you can host Ivanti Neurons for MDM Connector in AWS. No on-premise Connector is required.

The Connector automatically updates to the latest version of the software.

For the latest Ivanti Neurons for MDM Connector Installation Guide, visit **https://help.ivanti.com/#106** and search for "Connector".

Connector hosting options

You can host the Ivanti Neurons for MDM Connector on-premise in your datacentre or in Amazon Web Services (AWS):

- Host the Connector in AWS if you are using AWS-hosted Microsoft Active Directory or self-managed Microsoft Active Directory in AWS. You do not need a Connector on-premise in this case.
- To access on-premise resources, such as an LDAP Server or a CA, set up the Connector on-premise.

Hosting the connector on AWS

Customers can host Connector in AWS for use with the following AWS-hosted Microsoft Active Directory options:

- AWS Directory Service for Microsoft Active Directory
- Customer-managed Microsoft Active Directory in Amazon VPC

For more information on AWS Directory Service for Microsoft Active Directory, see **https://aws.amazon.com/directoryservice**. Refer to AWS documentation on hosting Microsoft Windows Server and Microsoft Active Directory in an Amazon VPC. Ivanti Neurons for MDM Connector supports Windows Server 2012, 2012 R2, 2015.

Setting up the Ivanti Neurons for MDM Connector AMI in AWS

To set up the Ivanti Neurons for MDM Connector AMI:

1. Log in to AWS with administrator credentials.
2. On the AWS services page, select **EC2** under **Compute**.
3. Expand **Images** and select **AMIs** in the left pane.
4. Select **Public Images** from the drop-down list in the right pane.
5. Search for the Ivanti Neurons for MDM Connector using keywords such as "mobileiron-kocab."
6. Select the latest version of the connector from the list and click **Launch**.
7. Follow the instructions for installing the Connector in the section, "Deploying Ivanti Neurons for MDM Connector in AWS" in the *Ivanti Neurons for MDM Connector Installation Guide* available at https://help.ivanti.com/mi/help/en_us/cld/*<version>*/inst/default.htm, where *version* is the version of the Ivanti Neurons for MDM Connector you are installing. For example, for the version 74 Ivanti Neurons for MDM Connector, find the guide at https://help.ivanti.com/mi/help/en_us/cld/**74**/inst/default.htm.

Hosting the connector on-premise

To host Ivanti Neurons for MDM Connector on-premise in your datacentre, click **Download Connector** to download and set up the Ivanti Neurons for MDM Connector. Extract the contents of the downloaded package and follow the setup instructions in the Ivanti Neurons for MDM Connector Installation Guide included in the package.

Accessing the Connector logs

You can access the Connector logs from the Connector service to help troubleshoot Connector related problems. You must have System Manager or System Read Only role.

1. Go to **Admin > Connector** to view the Connector page.
   The Connectors interface displays the Connector status (Enabled or Disabled), Connector Name, Connection (Connected or Not Connected), Version number, Logging Level, Actions (Disable or Remove the Connector).
2. Use the **Logging Level** pulldown menu to choose a level.
   The available logging levels are displayed in the pulldown menu in order from the lowest logging level to the highest logging level:
   - Error
   - Warn
   - Info
   - Debug
   - Trace

The Info level is the default logging level setting. If you choose another logging level a rotating Sync icon appears indicating that information is being collected at the level of logging that you selected. The logging level will reset to the Info level after an hour. The Trace level is the highest logging level setting. Use this level to collect all the messages at all the other levels. The sync icon is displayed for the duration of the request.

3. If needed, hover over the Sync icon to see the Cancel icon . Click the Cancel icon to cancel the logging level change.
4. Hover over the Request icon to display the Request information. Click the Request icon to request the files from the current log folder in a .zip file.
   The log files are added to a .zip file when a request is made. When a new request is made the .zip file from the previous request is deleted.
5. If needed, hover over the Request icon and it becomes the Cancel icon . Click the Cancel icon to stop the request.
   When a request is canceled before completion, the Download icon is not displayed because the previous log .zip file was deleted from the server. The original log files on the Connector are still available to request.
6. Click the Download icon when the request is completed to download the log .zip file containing log files collected during the latest request.
   The log file name is in the format: kocab.log. The name of the zip file that is downloaded consists of the server name, connection version, and a time stamp including day, month, year, and the time of the day in the format: <Connector_Hostname>_<Connector_Version>_<TimeStamp>.zip. The archived .zip file name is in the format: kocab.yyyy-mm-dd.0.log.gz.
7. Optionally, use the **Actions** pulldown menu to Disable or Remove the Connector.

If you cannot see the **Connector** page, it might be that you do not have the required permissions. You need one of the following **roles**:

- System Management
- System Read Only

For more information, see **Using the httproxy command for Connector**.

12.2.8. Using the httpproxy command for Connector

A new klish shell command has been created to help edit Connector configuration for your Ivanti Neurons for MDM installation. Use this command to change the login information and other parameters to configure the connector.

The httpproxy command is now available in this release with these requirements.

- klish shell

To configure your connector

1. Log in to klish shell.
2. Enter a ? for a list of available klish shell commands.
3. Enter **httpproxy** to show the current value of these parameters:
    1. enabled
    2. scheme
    3. server
    4. authtype
    5. username
    6. password
4. Enter **httpproxy ?** to see a list commands available for use with httpproxy.
    1. authtype - Set the authentication type of the http proxy to NONE, BASIC or NTLM
    2. disable - Disable the http proxy
    3. enable - Enable the http proxy
    4. host - Set the host of the http proxy - must be an FQDN or an IP either http or https
    5. password - Set the Authentication password of the http proxy
    6. port - Set the port of the http proxy
    7. scheme - Set the scheme of the http proxy - must be either http or https
    8. show - Show the current http proxy settings
    9. username - Set the authentication username of the http proxy
5. Use the commands listed above to setup your connector instance.

12.2.9. Help@Work

Licence: Platinum

Supported on: Android and iOS devices as supported by Ivanti Neurons for MDM

Use Help@Work for Android/iOS to provide remote assistance to users of Android and iOS devices. Help@Work for Android/iOS is based on the TeamViewer QuickSupport app. You will need a TeamViewer account to use Help@Work for Android/iOS. If you do not have an account, visit teamviewer.com for details.

Help@Work transforms the help desk experience for iOS 11.0+ and Android devices by allowing users to ask for help with a click of a button and to share their screen with a help desk agent. Users no longer waste valuable time trying to verbalize the issue, and IT staff is more efficient when troubleshooting device issues. This is not supported for MAM-only iOS devices.

> TeamViewer is supported on Android Device Owner devices in Kiosk mode.

> TeamViewer launch commands ceases to exist if the app exits or the device reboots.

> In Android devices, if the Teamviewer QuickSupport app is not installed, the user is prompted to download the app. In iOS devices, the app has to be pushed through App Catalog or if it is already installed on device, it must be converted as a managed app.

> The Teamviewer QuickSupport app should be in foreground for the session to be applied to the application. The TeamViewer host app is required for Unattended mode.

> The desktop application version that admin installs should be compatible with the Quicksupport version installed in the client device to support remote sessions.

Setting up Help@Work for Android or iOS

The following are one-time setup steps for branding and distributing Help@Work for Android or iOS:

1. Go to the **Admin** tab.
2. Under Infrastructure, click **Help@Work**.
3. **Help@Work** requires TeamViewer. In the Activate TeamViewer section, activate either **TeamViewer Attended** or **TeamViewer Unattended (Android only)** option by clicking the **Activate Now** button.
4. Review the TeamViewer license agreement and click **Agree** to continue. Your Enterprise Licence is now activated. This identifies Ivanti customers to TeamViewer so that access is granted.

> The **Remove Activation** option becomes available upon activating the TeamViewer. When you click **Remove Activation** present under the **Activate TeamViewer** section, the **Confirm Remove Activation** window appears on the screen. Click **Remove Activation** to remove the TeamViewer Activation, which in turn will remove the Help@Work functionality on all supported devices. However, you can activate TeamViewer using an existing account or a different account at a later stage.

> If you want to delete the **TeamViewer** account in Unattended mode, you must de-provision the associated devices for which the Unattended mode is enabled. To de-provision the associated devices, you must undistribute the **TeamViewer** app from the associated devices and do a force check-in. Ensure the TeamViewer app is deleted from all devices and then delete the binding of the account from the Admin console.

Distribute the TeamViewer app to users you wish to start remote sessions using the standard app distribution workflow. This is specific to **Attended** and **Unattended** modes. If the admin wants to control the device, the Universal add-on or OEM/model-specific add-on by TeamViewer needs to be distributed to the device as well. See App Configuration for instructions.

Starting a remote session using Help@Work for Android or iOS

A typical Help@Work for Androidor iOS session starts with an end-user needing help.

To start a Help@Work session with the user's device:

1. In Ivanti Neurons for MDM, go to **Devices**.
2. In the device list page, click on the device that needs support.
3. From the Actions menu, click **Start TeamViewer Remote Control** for Android devices or **Remote Display** for iOS devices. You will see two options:
    - Attended mode (default) - This option requires **TeamViewer Quick Support** app to be installed and Whitelisted in the target device.
    - Unattended mode (available on Android only) - This option requires **TeamViewer Host** app to be installed and Whitelisted in the target device.

> If you want to Whitelist the hostnames or override the content security policy, please contact the support team.

> The Unattended mode option works on Kiosk mode as well. It should be enabled from the TeamViewer integration page. The Unattended remote control requires TeamViewer host app on device, one time activation on a device, and a MI add-on license. For the one time activation, the permission prompt will be displayed when the TeamViewer host app installed and launched for the very first time. The administrator can use the "Auto-launch (settings in Managed App configuration)" TeamViewer app after installation if desired. The number of licenses is calculated based on TeamViewer host app distribution. If the TeamViewer host app is distributed to a device, one Unattended remote host session license is consumed. In addition to the TeamViewer host app, other add-on apps may be needed and should be allowed in kiosk or shared kiosk mode. Other add-ons might be needed depending on the device model and manufacturer.

> The Google Pixel devices do not persist this permission grant and require consent for permission for every session.

If the administrator has a valid TeamViewer token, the desktop client starts with a support session to the device. Otherwise, the administrator will be required to log in with TeamViewer and grant permissions.

To quickly initiate a remove session, administrators can login to the desktop application beforehand.

Installing TeamViewer

Install the TeamViewer app on the desktop to access and provide support for your users' remote devices. To install TeamViewer:

1. Download the installation package for the TeamViewer full version for Mac, Windows or Android from here: https://www.teamviewer.com/en/download/
2. Launch the TeamViewer installation program.
3. Select **Basic Installation**.
4. Select **Company / Commercial use**.
5. Click **Accept - finish**.

Requesting a TeamViewer account

You must have a TeamViewer account to provide support using TeamViewer. To obtain a TeamViewer account:

1. Go to https://login.teamviewer.com/.
2. Enter your email, name and password.
3. Click **Sign Up**.
4. Use the email account you entered in step 2 to receive an TeamViewer account activation email.
5. Complete the instructions in the email to activate your TeamViewer account.

Confirming TeamViewer session ID

TeamViewer generates a session ID when connection is established between the administrator's computer and the user's mobile device.

1. When the session ID is generated, Ivanti Neurons for MDM passes it to the TeamViewer QuickSupport app using the managed app configuration, which in turn uses this session ID to invoke the TeamViewer client on the device. For iOS, the session ID expires after 30 minutes.
2. The user is prompted to accept the TeamViewer EULA.

12.2.10. Infrastructure Identity

This section contains the following topics:

12.2.10.1. Configure Identity Provider

Licence: Silver

Configure an identity provider (IdP) to authenticate users who wish to register devices with Ivanti Neurons for MDM, access this Admin Portal, or access the Self-Service Portal. An on-prem LDAP compatible user directory is required. Ivanti Neurons for MDM works with any SAML 2.0 compatible IdP. Microsoft Entra ID Authentication (Entra ID), Microsoft ADFS (Active Directory Federation Services), Okta, OneLogin, PingOne, and Ping Identity's PingFederate have been verified to work with Ivanti Neurons for MDM.

Previously, if you setup SAML auth/IdP, SAML authentication is used for both device registration and portal authentication. Now, a toggle button is provisioned to choose different authentication methods for Admin Portal access and Device Registration. The bypass toggle is applicable only for device registration.

During device registration, the administrator can bypass the identity provider option and provide the user with the option to authenticate using a PIN instead of authentication using the identity provider page.

Overview

- If you are using Microsoft AD, or another on-premise LDAP directory, you will need to set up Connector to connect to and import users to Ivanti Neurons for MDM. Set up Connector or **LDAP** if you have not done so already.
- When an IdP is added, user authentication automatically switches from LDAP to IdP.
- Only one IdP provider is allowed.
- In case your IdP becomes inaccessible, use the Ivanti Neurons for MDM Tenant Admin (TA) account to access this Admin Portal and troubleshoot. The TA is a Local account and does not require external authentication. The TA account is created when your Ivanti Neurons for MDM is provisioned and information provided to the technical contact of your organisation, or equivalent. If you do not have your TA account information, contact your support representative.
- Ivanti Neurons for MDM supports Microsoft Entra ID (Entra ID) for authenticating users during registration of Windows 10 devices.

> Set the authentication type for your LDAP users using the tools provided by your IdP vendor. The authentication scheme of your IdP will take precedence over the Ivanti Neurons for MDM settings.Ivanti Neurons for MDM Authentication settings can be found here: **Users > User Settings > Device Registration Setting > Device Registration Authentication Type**.

- Apple Device Enrollment and Configurator device enrolments do not use IdP for user Authentication.
- To configure an identity provider to work for registering Apple Business Manager iOS and macOS devices, you must enable the **Enable Custom Enrollment** and the related **Ivanti Hosted webpage** settings found at **Admin > Apple > Device Enrollment >** *edit a device enrollment profile*. See **Device Enrollment** for more information:



IdP Set Up Types

The Ivanti Neurons for MDM Identity page guides you through the set up of the following types of IdP providers:

- **Ivanti Neurons for MDM IdP Setup**- Supported Ivanti Neurons for MDM IdP providers are Entra ID, OneLogin, Okta, and PingOne.
- **On-Prem IdP Setup**- Supported on-prem IdP providers are ADFS 3.0, PingFederate 8.2.1, and PingFederate 8.1.3.
- **Generic IdP Setup**- This is a generic set up path you can use if you are not using Microsoft ADFS, Okta, OneLogin, or PingFederate.

Configuring an identity provider (IdP)

Procedure

1. Go to **Admin** > **Identity** > **SAML Authentication**.
2. Click an identity provider set up type:
    - **Ivanti Neurons for MDM IDP Setup**
    - **On-Prem IDP Setup**
    - **Generic IDP Setup**
3. Select a corresponding IdP. If you selected **Generic IDP Setup** in step 3, then skip this step and continue from step 5.
4. Follow the instructions on the screen that appear for your chosen IdP.
5. Click **Done**.

> Administrators are allowed to single sign-on for up to 2 hours from their initial authentication with the IdP.

Setting up tasks you may need to complete

Depending on your chosen IdP, you will be guided through the following associated pages and steps:

IdP	Procedure
• Entra ID • Okta • OneLogin • Ping One	• Generating a key to upload to your IdP. • Logging into your IdP and uploading generated key. • Exporting a metadata file from your IdP and importing it into Ivanti Neurons for MDM.
• ADSF 3.0 • Ping Federate 8.2.1 • Ping Federate 8.1.3	• Download the metadata file from Ivanti Neurons for MDM. • Setting up a "Relying Party Trust" on ADFS or an “SP Connection” on PingFederate, and importing the Ivanti Neurons for MDM metadata file. • Exporting the metadata file from your IdP and importing it into Ivanti Neurons for MDM.
• Generic IdP	1. Download the metadata file from Ivanti Neurons for MDM. 2. Follow the instructions provided by your IdP vendor to configure your IdP server or service to communicate with Ivanti Neurons for MDM service as "Service Provider." This can include: 1. Uploading the metadata file from Step 1 above to your IdP. This configuration file contains the essential information that enables Ivanti Neurons for MDM, as a SAML 2.0 Service Provider, to communicate with your SAML 2.0 Identity Provider. The standard SAML 2.0 URLs, certificates and settings are included in the metadata file. Ivanti Neurons for MDM expects a SAML 2.0 compatible IdP to have the ability to import and process an XML metadata exported from a Service Provider. 2. Configuring your IdP to use RSA-SHA1 for signing SAML authentication requests. Information about the Signing Certificate used to verify the authentication requests is included in the metadata file downloaded in Step 1. 3. Configuring your IdP to include a username in the SAML responses sent to Ivanti Neurons for MDM. Specify the username in the [Name ID] element of the SAML Response from IdP. Export a metadata file from your IdP and importing it into Ivanti Neurons for MDM. 3. (Optional) - Include username in SAML Authentication Request: To include the username of authenticating user in the authentication request and to remove an additional user input when authenticating with an IdP. If you enable this option, authentication failures may happen. If you are sure about IdP validation, select the **I understand the impact of this change** option and toggle the **Include Username in SAML Authentication Request** setting to **ON**. Ivanti Access is a validated IdP for this setting.

Enabling local users to bypass IdP authentication

When an IdP or Ivanti Neurons for MDM connectivity goes down and needs troubleshooting from the Ivanti Neurons for MDM side, certain administrators need the ability to login to Ivanti Neurons for MDM without reliance on external systems, such as, LDAP or IdP, for authentication. Only local users with system admin roles can bypass IdP authentication.

Create a list of local users to bypass IdP authentication.

Procedure

1. Click **Admin > Identity**.
2. Under the Local Users to Bypass IdP Authentication section, click **+Add Users**.
3. From the list displaying only the local users with system admin roles, select a few users.
4. Click **Save**.

> To remove a user from the list of local users that bypass IdP authentication, click the remove icon next to the entry you want to delete.

If you cannot see the Identity page, it might be that you do not have the required permissions. You need one of the following **roles**:

- System Management
- System Read Only

12.2.10.2. User Provisioning with SCIM

This section contains the following topics:

- User Provisioning
- Generate a token from Ivanti Neurons for MDM
- Change the Token Status
- View the Token Status from Audit Trials
- Configure Attributes in SCIM Provisioning

User Provisioning

User Provisioning uses the SCIM protocol to synchronise an IdP with Ivanti Neurons for MDM and allows for partial user and group sync. User Provisioning uses the SCIM protocol to automatically create and update user and group objects sourced from an IdP to Ivanti Neurons for MDM. Just like the current integration with Entra ID and Okta, the users and groups provisioning process is automated; if changes are made to the user or group in IdP, the same changes are reflected in Ivanti Neurons for MDM.

> Username of a user provisioned via SCIM can be renamed in the Identity Provider (IdP) if the username is unique in Ivanti Neurons for MDM.

> SCIM users and groups can now be searched using their respective external Ids.

Generate a token from Ivanti Neurons for MDM

To start User Provisioning for an IdP, generate a token and the target URL from Ivanti Neurons for MDM.

> Ensure that you save the token and the target URL.

> A maximum of 2 tokens can be generated any time.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Go to **Admin** > **Identity** > **User Provisioning**.
3. Select Identity Provider (IdP) from the dropdown list.
4. To generate a new token, click **Generate**. A notification message appears, click **Generate**. A new page opens with details of the Token and the Target SCIM URL.
5. Click **Copy** to copy either the token or the SCIM URL.
6. Refresh the page. The **User Provisioning**page displays the Token Status table.

Change the Token Status

You can change the state of an existing token.

Procedure

1. Click the **Select** drop-down menu on the **User Provisioning Entra ID** page.
2. Click **Select** and make the following changes to the token:
    - **Set to Active**
    - **Set to Inactive**
    - **Renew**
    - **Remove**

View the Token Status from Audit Trials

You can view the logs of actions / events that took place on a SCIM token from the Audit Trials section. The SCIM token can have one of the following statuses:

- SCIM Token Created - A SCIM token has been created.
- SCIM Token Enabled - The SCIM token has been enabled.
- SCIM Token Disabled - The SCIM token has been disabled.
- SCIM Token Renewed - The SCIM token has been renewed.
- SCIM Token Deleted - The SCIM token has been deleted.

The DETAILS column also lists the SCIM vendor name (IDP) such as Azure, Okta, etc. which makes it easy to communicate with Ivanti Neurons for MDM.

Configure Attributes in SCIM Provisioning

This section describes how to create custom and enterprise attributes for an IdP during user provisioning.

Mapping attributes

After the connection is established, you can map the attributes between IdP and Ivanti Neurons for MDM. Ivanti Neurons for MDM supports the following user attributes:

Core attributes

- id
- userName
- displayname
- active
- givenName
- familyName
- emails

> For Entra ID IdP, external IdP is supported.

List of attributes for which update operation is allowed

- 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

Custom attribute

Schema - urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<CustomAttribute123Name>

Enterprise attribute

Currently only the Department attribute is supported.

Schema - urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department

12.2.10.2.1. User Provisioning for Entra ID IdP

This section contains the following topics:

- Establish a connection with Ivanti Neurons for MDM
- Provision assigned users and groups
- Provision all users and groups
- Verify assigned user provisioning
- User Provisioning for Entra ID IdP
- Edit Settings
- Configure Custom and Enterprise Attributes
- Migration considerations - Entra ID User Source to User Provisioning SCIM
- Migration considerations - LDAP to User Provisioning SCIM
- Important Notes - SCIM

Establish a connection with Ivanti Neurons for MDM

After you create the users and groups on your Entra ID Enterprise application, you can establish the connection between Entra ID and Ivanti Neurons for MDM.

Procedure

1. Log in to the Entra ID portal.
2. Go to **Enterprise Application** > Click **+ Create your own application**. The Create your own application window opens.
3. Specify the name of your app (**Default: Non-gallery**) and click **Create**. For example, Ivanti Neurons for MDM User Provisioning.
4. Go to **Provisioning** > **Edit provisioning** > **Admin Credentials**.
5. Copy and paste the Target SCIM URL from the Ivanti Neurons for MDM admin portal in the **Tenant URL** field in the Entra ID portal.
6. Copy and paste the Token from the Ivanti Neurons for MDM in the **Secret Token** field in the Entra ID portal.
7. Perform one of the following steps:
    - Select **Sync only assigned users and groups**. For more information, see Provision assigned users and groups
    - Select **Sync all users and groups**. For more information, see Provision all users and groups.

    > Select the Sync All Users and Groups option for migrating users.

Click **Test Connection**. A pop-up with a green check confirms the connection.

9. Click **Save**.
10. Expand **Mappings** from the **Provisioning** page on the Entra ID portal.
11. Click **Provision Entra ID Users**. The Attribute Mapping page opens.
12. Click **Delete** to delete the unsupported attributes.

Provision assigned users and groups

After the connection is established between Entra ID and Ivanti Neurons for MDM, you can provision users or groups.

> When provisioning groups, Entra ID does not add members of the nested groups to the selected group. Entra ID adds immediate members and group names to the group only and not the subgroup members during the sync process.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. In the application go to **Users and groups** > click **+ Add User/Group**. The Add Assignment page opens.
3. Search for the user or group from the **Search** field, click **Select**, and then **Assign**. The Users and Groups page opens.
4. Select the corresponding user or group checkbox.
5. Click **Provisioning** and then click **Start Provisioning**. The details of the successful configuration are displayed.

Provision all users and groups

After the connection is established between the Entra ID and Ivanti Neurons for MDM, you can provision users or groups.

Procedure

- Click **Provisioning** and then click **Start Provisioning**. The page opens with the details of the successful provision and the user will be provisioned to Ivanti Neurons for MDM.

Verify assigned user provisioning

After an assigned user is provisioned on the Entra ID portal, verify the provisioning on the Ivanti Neurons for MDM administrative portal.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Go to the **Users** tab under the main menu. The user that was provisioned will be present in the list of the users in this page.

> The provisioning process may take up to an hour.

Verify group provisioning

After a group is provisioned on the Entra ID portal, verify the provisioning on Ivanti Neurons for MDM.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Go to the **Users** tab > **User groups**. The group that was provisioned will be present in the list of the groups in this page.

> The provisioning process may take up to an hour.

Edit Settings

This topic helps you configure the Entra ID settings.

Procedure

1. Go to **Admin > Microsoft Azure > User Provisioning Entra ID**.
2. Click **Generate Token** and copy the token.
3. Refresh the page. The Entra ID Settings page opens.
4. Click **Edit Settings**.
5. Set **Automatically invite users imported from Entra ID** - Manage whether users imported from Entra ID to Ivanti Neurons for MDM are automatically invited to register via email.
6. Set **Managed Apple ID** - This option is disabled by default. Click the toggle button to enable it. Managed Apple ID can be set during provisioning via:
   - **User email address**
     - (Optional) select the Include "appleid" subdomain option to avoid conflict with existing Apple IDs.
   - Mapping to **Custom Attribute**

   > Custom attribute should evaluate to unique email address.
7. (Optional) Click **Add Custom Attribute** - Specify custom user attributes from your directory service that you want to apply to device management. Each attribute can then be referenced by $ in configuration fields that support variables. Use of this option requires consistent implementation of custom attributes across Entra ID servers. If an Entra ID server included in your implementation does not use this attribute, then features dependent on this attribute might not work as expected. The **Attribute Type** column displays **IDP** attribute in the **Custom Attributes** table in the **Edit Settings** section.
8. Click Save Changes after modifying the Entra ID settings.

Configure Custom and Enterprise Attributes

Procedure

1. Go to **Admin** > **Identity** > **User Provisioning**.
2. Under **Edit Settings**, click **+Add Custom Attribute**.
3. Enter a name in the **Attribute Name** field (for example, custAttr1) and click **Save Changes**. The attribute is listed and available on **Admin** > **System** > **Attribute** page. The attribute is denoted as IdP attribute and you can only perform Delete action.
4. Log in to the **Entra ID** portal.
5. Go to **Home** > **Enterprise Application** > Click on the SCIM application.
6. Click **Provision Entra ID Users** from the **Mappings** section.
7. Select the **Show advanced options** check box.
8. Click **Edit attribute list for customappsso**.
9. Enter a new entry for the custom attribute that you created in the Ivanti Neurons for MDM UI.
10. Add the schema for the Custom/ Enterprise (Department) attribute as follows:
    Custom attribute - **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<custAttr1> -** Refer to step 3.
    Enterprise attribute - **urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department**
11. Click **Save changes**.
12. Click **Add New Mapping** and select the Source and Target attributes from the drop-down menu.
13. Click **Ok** and **Save Mapping**.
14. Go to **Home** > **Enterprise Application** > Click on the SCIM application > **Users and groups**.

15. Click User name. The Profile Page opens.
16. Verify whether the value associated with the attribute appears on the Profile page.
17. (Optional) Click on the SCIM application > Provisioning > Provision on demand, search for the specific user, and click Provisioning. To validate the new attribute mappings performed in the previous steps.
18. Log in to the Ivanti Neurons for MDM administrative portal.
19. Go to **User** > **Users**> Select the user.
20. Click the **Attributes** tab, and verify the attribute value. The attribute is mapped for the specific user.

Migration considerations - Entra ID User Source to User Provisioning SCIM

- When migrating from Entra ID User Source to User Provisioning Entra ID (SCIM), select Sync All Users and Groups.
- After users and groups are updated with a SCIM Entra ID source, return to the Azure Provisioning page in Azure and set the specific users and groups to be managed by User Provisioning Entra ID using the Sync only assigned users and groups option.
- Ivanti Neurons for MDMWhen the sync is complete, you can remove the users and groups that are not defined in Azure from the Users and Groups lists.
- When the migration starts, the Entra ID User Source page is accessible in a read-only state.

Migration considerations - LDAP to User Provisioning SCIM

Prerequisites:

1. **Enable this LDAP Server** option is selected by default. This option must be deselected before migration.
2. Create an Enterprise App in Entra ID, add the Synced LDAP Users/Group (Same LDAP Users/Groups present in Ivanti) to SCIM App. Start Provisioning.

Key considerations for LDAP to SCIM Migration

- LDAP does not capture all information for synchronised users/groups, while SCIM logs user/group events in Audit Logs.
- LDAP user with custom attribute has the Type defined ldap, where as for SCIM, it is IdP. So, when the users with custom attribute are migrated from LDAP to SCIM, the corresponding IdP custom attribute should be created in SCIM App and the users will be migrated . When the user wants to update the ldap custom attribute later, the ldap.custom attribute value will not be updated in MDM after migration. The IdP attribute value will be updated.
- Migrate LDAP users who are associated with one or multiple custom attributes, specifically "ldap.custAttr1," indicating the registration of the LDAP device and the configuration (Identity Certificate Configuration) pushed to the device with the SAN Type corresponding to the value of the LDAP custom attribute.
- Migrate a LDAP User where Managed Apple ID associated with email Address - So, before Migration from LDAP to SCIM, if the user wants to persist the value of LDAP user's managed Apple ID, the Managed Apple Id in SCIM setting must be enabled and the settings must be saved.
- When LDAP User is removed in LDAP server , the user is still active but No sync flag is set to true for that particular synced LDAP User. In case of SCIM, When one provisioned user is deleted , the user status is disabled.
- Once SAML is configured for the Identity Provider (IdP) for SCIM users, all users from various sources like Local and LDAP will be authenticated through SAML. Only local users can be added to an exception list to bypass the IdP authentication flow. This configuration can be managed in the SAML page under **Admin** > **Identity** > **SAML**.
- Once SAML is configured for the migrated IDP (SCIM) users, device registration can be bypassed (not via IDP) for other users from different sources such as Local and LDAP. This can be managed under **Users** > **User Settings**.

- In LDAP, Users, Groups, and OU are supported, whereas In SCIM, Users and Groups are supported, but not OU.
- Nested group provisioning process is not supported in SCIM.

Important Notes - SCIM

- Email address is a mandatory field for provisioning and migrating users or members.
- SCIM provides one way provisioning from Microsoft Entra ID to Ivanti Neurons for MDM. Ivanti Neurons for MDM does not offer any sync options. If you delete a SCIM provisioned group or user from Ivanti Neurons for MDM, ensure that you also remove the user or group from Microsoft Entra ID.
- You can use one attribute (source or target) only once in the SCIM application mapping window in Microsoft Entra ID. The same source cannot be mapped twice to a specific target attribute.
- Inactive users cannot be provisioned or migrated to Ivanti Neurons for MDM using SCIM.
- Currently, Ivanti Neurons for MDM does not support SCIM event notification.
- Migration or provisioning duration depends on the number of users or groups involved.
- Microsoft Azure controls the provisioning interval and it is about approximately 40 minutes or more.
- During re-provisioning, Microsoft Entra ID will only retry the entries that failed. You can download the provision logs to verify the users that have succeeded or failed provisioning from Microsoft Entra ID.
- Duplicate groups from different sources are not allowed in SCIM.
- When a provisioned user is hard deleted from Microsoft Entra ID, the user is disabled in Ivanti Neurons for MDM.
- When a provisioned user group is deleted from Microsoft Entra ID, the group is deleted in Ivanti Neurons for MDM and the independent members that belong to the deleted group are disabled and are associated to All Users Group.
- When a provisioned member of a provisioned group is hard deleted in Microsoft Entra ID, the member is disabled in Ivanti Neurons for MDM however, the member is still associated to the group in Ivanti Neurons for MDM.
- When an attribute (Enterprise attribute or custom attribute) mapping is removed from an app, the removed attribute value is still reflected in Ivanti Neurons for MDM.
- When a user attribute of a provisioned user is updated with blank or empty value, the updated attribute value is not reflected in Ivanti Neurons for MDM.
- If the user attributes FName and LName (name.formatted) are blank during migration or update from Microsoft Entra ID to SCIM, the migration or update fails.
- If you delete a user in Entra ID, the corresponding SCIM API does not delete the user permanently but performs a soft delete and changes the user status from active to inactive. If you want to permanently delete the user, log in to Ivanti Neurons for MDM administrative portal and manually delete the inactive/ disabled user.
- When a local user already exists in Ivanti Neurons for MDM with a certain user ID, a similar user with the same user ID will be provisioned from Entra ID to MDM, the user source will be updated from Local to SCIM Entra ID.
- Entra ID with "Entra ID Premium P1" subscription has the privilege to provision the required group to be assigned and provisioned.

12.2.10.2.2. User Provisioning for Okta IdP

This section contains the following topics:

- Establish a connection with Ivanti Neurons for MDM
- Provision users and groups
- Verify assigned user provisioning
- Verify group provisioning
- Edit Settings
- Configure Custom/ Enterprise Attributes in SCIM User Provisioning

Establish a connection with Ivanti Neurons for MDM

Ivanti Neurons for MDMAfter you create the users and groups on your Okta application, you can establish the connection between Okta and .

Procedure

1. Log in to **Okta**.
2. Go to **Applications** > **Applications** > **Browse App Catalog**.
3. Search for **Add SCIM 2.0 Test App** (OAuth Bearer Token) and install the app.
4. Click on the app and go to **Provisioning** > **Integration**.
5. Click **Edit** and provide the base url and paste the generated token.
6. Click **Save**.
7. Go to **Provisioning** and click **Edit**.
8. Enable the necessary user actions and click **Save**.

Provision users and groups

After the connection is established between **Okta** and Ivanti Neurons for MDM, you can provision users or groups.

Procedure

1. Go to **Assignments** > **Assign** > **Assign to People** or **Assign to Group**.
2. 2. Select or search for an existing user or group and click **Assign**.
3. Repeat the process to add more **Users** or **Groups**.
4. Click **Done**.
5. Select the group and click **push Group by name** to save and sync the group.

Verify assigned user provisioning

After an assigned user is provisioned on the Okta portal, verify the user provisioning on Ivanti Neurons for MDM administrative portal.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.

2. Go to **Users**tab under the main menu. The provisioned user will be present in the list of users on this page.

Verify group provisioning

After a group is provisioned on the Okta portal, verify the provisioning on Ivanti Neurons for MDM.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Go to **Users** tab and click **User groups**. The provisioned group will be present in the list of the groups in this page.

Edit Settings

This topic helps you configure the Okta settings.

Procedure

1. Go to **Admin** > **Identity** > **User Provisioning Okta**.
2. Click **Edit Settings**.
3. Set **Automatically invite users imported from Okta** - Manage whether users imported from Okta to Ivanti Neurons for MDM are automatically invited to register via email.
4. (Optional) Click **Add Custom Attribute** - Specify custom user attributes from your directory service that you want to apply to device management. Each attribute can then be referenced by $ in the Configuration fields that support variables. Use of this option requires consistent implementation of custom attributes across Okta servers. If the Okta server that is included in your implementation does not use the custom attribute, the features that are dependent on the custom attribute might not work as expected. The **Attribute Type** column displays **IDP** attribute in the **Custom Attributes** table in the **Edit Settings** section.
5. Click **Save Changes** after modifying the Okta settings.

Configure Custom/ Enterprise Attributes in SCIM User Provisioning

Procedure

1. Go to **Admin** > **Identity** > **User Provisioning**.
2. Click **Edit Settings**.
3. Enter Custom Attribute (for example, custAttr1) and click **Save Changes**.
4. From the Okta Portal, click **Directory** > **Profile Editor**.
5. Click on **SCIM 2.0 Test App (OAuth Bearer Token) User** app.
6. Click **Add Attribute**.
7. Add the following custom attribute values, for example:
    - Display name (same custom attribute value that we provided in N-MDM, refer to step 3).
    - Variable Name : custAttr1
    - External Name: custAttr1
    - External namespace : **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User**
    - User Permission : (Read / Write)
8. Click **Save Attribute**.
9. Click **Profile Editor** > **Mappings**. You will see two sections for mappings (SCIM and Okta).

10. Map the custom attributes created in N-MDM to attributes defined in Okta, and save the mappings.
11. Go to **Users** and click on the required user.
12. Click **Profile** > **Edit** to edit the attributes.
13. Go to **Applications** > **SCIM 2.0 Test App (OAuth Bearer Token)** app.
14. Under the **Assignments** tab, click **Assign** and select **Assign to People**.
    The **Assign SCIM 2.0 Test App (OAuth Bearer Token) to People** window appears on the screen.
15. Select the required user and click **Assign**.
16. Click **Done**.

To verify the custom attribute and its mapping in Ivanti Neurons for MDM:

- Go to **Users** > **User** (any specific user) > **Attributes**. Make sure the mapped custom attribute for Okta is visible under the User attributes section.

12.2.11. Configuring LDAP server

Licence: Silver

Configuring an LDAP server and a Connector enables you to import users and groups from your corporate directory. After you have installed at least one Connector, you can add one or more LDAP servers.

Adding an LDAP server means configuring:

- the *connection* to the LDAP server
- the *search terms* necessary to view the target directory data
- the portion of the directory to *import*
- whether to automatically *invite users* in the selected portion of the directory

After you have added an LDAP server, you can return to this page to **edit the LDAP server information** or **change the LDAP users selected**.

> LDAP users must be imported after configuring an LDAP user. See **Importing LDAP users**.
> LDAP usernames, just like local usernames, must be globally unique. Please verify that users do not already have a local account with the same username, or, for organisations with more than one tenant, that the username has not already been associated with another tenant.

Adding an LDAP server

Procedure

1. Click **+Add Server**.
2. Provide the following information:
3. Click **Test Connection and Continue**.

Setting	What To Do
Name	Enter a name that identifies this server.
Description	Enter a description that clarifies the purpose of this server.
Directory URL	Enter the URL for the directory. Use one of the following formats: ldap://IP address or ldaps://IP address or Example: ldap://myserver1.mycompany.com:389
User ID	Enter the user ID for an account with the following characteristics: • managed by the LDAP server • can bind to the LDAP server and search the subtrees for user, group, and organisational unit This is generally an account with Directory Administrator Credentials (DN or Distinguished Name and password).
Password	Enter the password for the account.
Confirm Password	Re-enter the password for the account.
Directory Type	Select the type of directory from the list of supported directories. • Microsoft Active Directory • Open LDAP • Other (Open LDAP compatible)

4. This step validates the information you have provided so far.

- If the information proves valid, then the service retrieves the LDAP naming context, which it uses to fill in some of the fields on the next page.
- If the LDAP URL fails to connect, you can proceed with the next steps. However, this may result in limited functionality until the connection is resolved.

Complete the remaining settings:

5. Click **Next**.

Setting	What To Do
Directory Failover URL	Enter the URL for the secondary directory. Use the following format: ldap://IP address or Example: ldap://myserver2.mycompany.com:389
Sync Interval	Enter the period of time between each attempted synchronisation of LDAP data from the LDAP server. The default value is 15 minutes. Consider increasing the interval after you have successfully synchronised all target LDAP data and confirmed that your LDAP setup meets your needs.
Enable Sync Discard	Select to automatically discard the LDAP sync data if the reloaded data set declines significantly. This option ensures that abnormal behaviour on the part of the LDAP system will not result in unnecessary, disruptive updates on the service and removal of configurations from registered devices. Make sure this option is not selected if you plan to make major changes in your LDAP setup or on the LDAP server.
Enable this LDAP Server	Select to use this LDAP server with your service. Clear this setting if you want to retire this LDAP server or take it out of service. Though a configured failover to a second LDAP server would automatically replace this server, using this option enables you to plan ahead and avoid a brief lack of connectivity during failover.
Automatically invite users whenever they are imported	Select to automatically send invites to the users when they are imported from the LDAP server.
Upload CA Certificate	Click **Choose File** to upload the TLS certificate issued by the CA installed on this LDAP server. You can upload multiple CA certificates.
Chase Referrals	Applies only if you are using a multi-forested domain. This option indicates whether you want to use alternate domain controllers when the targeted domain controller does not have a copy of the requested object. • Select **Follow** if you want to use referrals. • Select **Ignore** if you do not want to use alternate domain controllers. • **Throw** currently has the same effect as **Ignore**. Selecting **Follow** delays LDAP authentication.
Search Results Timeout	Increase this timeout if you observe performance issues or incomplete results when browsing the data synchronised from the LDAP server.
Search Results Count	Set to the maximum number of records that should be returned from the LDAP server at one time. Scenarios that might require changing this setting to improve performance include: • The LDAP server is located far away or behind a high latency link. In this case, larger search results will take longer to retrieve than smaller ones, so defining a smaller set enables you to see subsets of updated data more quickly. • The LDAP is massive, and every search returns a huge results set. In this case, if performance is not an issue, defining a larger results set would make it possible to return all of the data with fewer searches.

For Sandbox environment, the LDAP sync interval cannot be scheduled less than 8 hours.

6. Use the following guidelines to configure the integration with the LDAP server:

7. Click **Browse** or **Search**.

Setting	What To Do
Group Member Format	Select **DN** or **UID** to indicate whether to use the distinguished name or the user ID in your search.
OU Search Attributes	Specify criteria for searching at the organisational unit level.
Base DN	Enter the distinguished name for the starting level at which you want your search to be rooted or begin. Your selection determines defaults for several other fields, which you can change, if necessary.
Object GUID	If necessary, change the default value to match your LDAP environment. This is the attribute that uniquely identifies an organisational unit across time and across OU name changes.
Attribute Name	If necessary, change the default value to match your LDAP environment.
Description	If necessary, change the default value to match your LDAP environment.
Attribute DN	If necessary, change the default value to match your LDAP environment.
Search Filter	If necessary, change the default value to match your LDAP environment.
Search Scope	Select the portion of the LDAP hierarchy to target: • **Base** (only the level of the search base entry) • **One Level** (the level beneath the search base) • **Subtree** (the subtree in the directory information tree beneath the search base DN)
User Search Attributes	Specify criteria for searching users in a given directory level.
Base DN	Enter the distinguished name for the starting level you want to search.
Attribute UID	If necessary, change the default value to match your LDAP environment.
Object GUID	If necessary, change the default value to match your LDAP environment. This is the attribute that uniquely identifies an user across time and across user name changes.
Attribute DN	If necessary, change the default value to match your LDAP environment.
Forename	If necessary, change the default value to match your LDAP environment.
Surname	If necessary, change the default value to match your LDAP environment.

Setting	What To Do
Display Name	If necessary, change the default value to match your LDAP environment.
Email Address	If necessary, change the default value to match your LDAP environment.
Principal Name	If necessary, change the default value to match your LDAP environment.
Locale	If necessary, change the default value to match your LDAP environment.
Member Of	If necessary, change the default value to match your LDAP environment.
Search Filter	If necessary, change the default value to match your LDAP environment.
Search Scope	Select the portion of the LDAP hierarchy to target: • **Base** (only the level of the search base entry) • **One Level** (the level beneath the search base) • **Subtree** (the subtree in the directory information tree beneath the search base DN)
Managed Apple ID	Choose to sync Managed Apple ID for the LDAP users. • **None** • **Pattern** - ◦ **User email address** ◦ **userUPN** Optionally, select the **Include "appleid" subdomain** option to avoid conflict with existing Apple IDs.
+Add Custom Attribute	(Optional) Specify up to 7 custom user attributes from your directory service that you want to apply to device management. Each attribute can then be referenced by $ in configuration fields that support variables. **Important:** Use of this option requires consistent implementation of custom attributes across LDAP servers. If an LDAP server included in your implementation does not use this attribute, then features dependent on this attribute might not work as expected.
Group Search Attributes	
Base DN	Enter the distinguished name for the starting level you want to search.
Object GUID	If necessary, change the default value to match your LDAP environment. This is the attribute that uniquely identifies a group across time and across group name changes.
Attribute DN	If necessary, change the default value to match your LDAP environment.

Setting	What To Do
Attribute Name	If necessary, change the default value to match your LDAP environment.
Description	If necessary, change the default value to match your LDAP environment.
Member	If necessary, change the default value to match your LDAP environment.
Search Filter	If necessary, change the default value to match your LDAP environment.
Search Scope	Select the portion of the LDAP hierarchy to target: • **Base** (only the level of the search base entry) • **One Level** (the level beneath the search base) • **Subtree** (the subtree in the directory information tree beneath the search base DN)

8. Confirm that your configuration returns the expected data.
9. You can do this by browsing or searching for a known item in the directory.

Click **Next**.

Deleting a custom LDAP attribute

You can delete a custom LDAP attribute and remove its values from the associated users or devices.

Procedure

1. Go to **Admin > Attributes**.
2. In the **Custom Attributes** section click on the **Delete** link next to the LDAP attribute that should be deleted. A confirmation window is displayed.
3. Click **Delete** to confirm deletion.

> that the **Delete** button is disabled by default. You should select the check box in the **I understand that deleting a Custom Attribute cannot be reversed** option to enable the **Delete** button.

Editing the LDAP server information

Procedure

1. Go to **Admin > LDAP**.
2. In the LDAP server entry, select the **Edit** icon from the **Actions** column to view the Connect LDAP Server page.
3. Make the necessary changes.
4. Click **Test Connection and Continue**.
   If the LDAP URL fails to connect, you may proceed with the next steps. However, this may result in limited functionality until the connection is resolved.
5. Click **Browse** or **Search**.

6. Confirm that your configuration returns the expected data.
   You can do this by browsing or searching for a known item in the directory.
7. Click **Done**.

Importing LDAP users

Procedure

1. Go to **Users**.
2. Click **+Add > Invite Users from LDAP**.
3. Click **Select Users** in the LDAP server entry.
4. In the Add LDAP Users page, enter the name of the user, group, or OU in the search field.
5. To add new users or groups, click **+Add** next to the entry you want to add.
6. Click **Next**.
7. Choose whether or not to send the invitation:
   - Invite None
     To send the invites later, go to **Users > Users** and select **Actions > Send Invite** to send the invitations.
   - Invite All

Click **Done**.

Updating the users, groups, or organisational units selected

Procedure

1. Go to **Admin > LDAP**.
2. In the LDAP server entry, select the **Manage Users** icon from the **Actions** column to view the Add LDAP Users page.
3. To add new users or groups, enter the name of the user or group in the search field.
4. Click **+Add** next to the entry you want to add.
5. To remove a user, group, or OU, click the remove icon next to the entry you want to delete.
6. Click **Done**.

Enabling LDAP Sync Discard Notification

Enabling LDAP sync discard notification helps prevent outages caused by unintended large scale changes to the LDAP environment.

Procedure

1. Go to **Admin > LDAP**.
2. In the LDAP server entry, select the **Edit** icon from the **Actions** column to view the Connect LDAP Server page.
3. Check the **Enable Sync Discard** check box.
4. Enter a value for the percentage of reloaded LDAP data to trigger sync discard.
5. Click **Test Connection and Continue**.
   If the LDAP URL fails to connect, you can proceed with the next steps. However, this might result in limited functionality until the connection is resolved.

6. Click **Done**.
7. Click the **Sync Now** icon in the LDAP server entry.
   When the change difference to be synced from LDAP to Ivanti Neurons for MDM falls above the set discard percentage, a WARNING notification is generated. When the changes are reverted to a value below the set percentage, the notification is CLEARED.

Trigger	Severity	Notification Type	Component Type	Component
LDAP Sync Discard	Warn	Data Sync	LDAP	LDAP server name
LDAP Sync Restored	Info	Data Sync	LDAP	LDAP server name

The Partial Sync Discard Notification is generated when one or more user records fail to sync from LDAP. In this case, a CSV file is included as an attachment with a list of users that failed to sync. If a user was discarded due to missing attributes, the list of missing attributes is also included in the exported CSV file.

Synchronising changes from the LDAP server

In the LDAP page, click the **Sync Now** icon in the LDAP server entry.

> If the display name is more than 128 characters, the LDAP sync will ignore such a user and proceeds with other users or user groups sync.

Troubleshooting Connectivity to the LDAPS Server

If you encounter issues connecting to the LDAPS (LDAP over SSL) server, you may be experiencing an issue with the certificate.

To resolve the issue:

- Verify that you are not using a self-signed certificate on the LDAPS server.
- Verify that the LDAPS certificate has not expired or been revoked. Also check for a hostname mismatch.

After verifying, wait for the automatic LDAP sync, or manually sync using the **Admin > LDAP > Sync Now** icon in the LDAP server entry.

If you cannot see the LDAP page, it might be that you do not have the required permissions. You need one of the following **roles**:

- System Management
- System Read Only

12.2.12. Sentry

Sentry is a component that acts as a gateway between mobile devices and your ActiveSync-enabled email system. Use Sentry to control which devices are allowed to access email. It is available to download as an ISO file that you can install on a virtual machine. Organisations should consider using a load balancer to maintain multiple (redundant) Sentrys.

Licence: Silver

Latest documentation

For the latest Sentry instructions, visit **Product Documentation** and click Sentry.

For the latest Sentry installation instructions, select the appropriate version of the *Standalone Sentry On-Premise Installation Guide*.

For Sentry upgrade instructions, select the appropriate version of the *Sentry Guide*. See the following sections in the Sentry Guide:

- For upgrade instructions using the Standalone Sentry System Manager UI, see "Standalone Sentry software updates."
- For upgrade instructions using the Standalone Sentry command line interface (CLI), see "Upgrading using CLI."

Before you upgrade, see the Standalone Sentry release notes for the version to which you are upgrading.

12.3. Apple Settings

This section contains the following topics:

- Apple Configurator
- Device Enrollment
- Configuring the Setup Assistant
- Install MDM Certificate
- Shared iPad devices for business
- School Manager
- Settings (Apple)

12.3.1. Apple Configurator

You can use this page to prepare Apple Configurator for setting up Ivanti Neurons for MDM device management on iOS devices. Apple Configurator makes it really easy to deploy iOS devices in large quantities. Additionally, Configurator lets administrators make iOS devices Supervised, which allows for greater levels of configuration and management capabilities. For more information about Apple Configurator, please see the Mac App Store.

The basic steps are:

1. Export the MDM profile from your Ivanti Neurons for MDM tenant.
2. Import the MDM profile into the Configurator.
3. Use the Configurator to apply the MDM profile to tethered devices.

Defining a default user for devices

Devices configured through the Apple Configurator are assigned to the nobody user in Ivanti Neurons for MDM unless you pick a different user:

1. Click in the **Assign configured devices** to field.
2. Start typing the username of the Ivanti Neurons for MDM user you want to select.
3. Select the username when it displays in the drop-down list.
4. Click **Save**.

Installing apps using Apple Configurator

Before using the Apple Configurator to install apps:

- Access to the Apple app store is restricted by the device configuration.
- Apps installation is permitted by the device configuration.
- Apple Configurator must be installed on the computer used to configure the devices.

To install apps using the Apple Configurator:

1. In Ivanti Neurons for MDM, go to **Admin > Apple Configurator**.
2. Switch the enrol devices toggle switch to On.
3. Click one of the following:
    - **Default User's plist**.
    - **Specific User's plist** - Enter the specific user's username or email ID.

In the Apple Configurator, go to **Prepare > Apps**.

5. Go to **Prepare > Setting and disable Supervision**.
6. Select the **Never update device** option in Update iOS.
7. Click **Prepare** (bottom of the Apple Configurator).
   The apps will be visible in the list of Installed apps on the device after a device check-in.

Installing apps using UEM server

To install apps using the UEM server:

1. Upload an app from the in-house store in the Apps tab.
2. Select the app.
3. Click the **App Configurations** tab.
4. Select **Install on Device**.
   Complete configuration settings.
5. Select **Actions > Force Check-in**.

What the end user needs to do

Apple requires the end-user has to launch the Go at least once, or the Ivanti Neurons for MDM Location feature will not function properly. This is to ensure that the end-user is aware that their location is being tracked.

Caution: If devices are deployed in single app mode using Configurator, then this approach will not be possible.

If you cannot see the **Install Apple Configurator** page, it might be that you do not have the required permissions. You need one of the following **roles**:

- System Management
- System Read Only

12.3.2. Account-driven Enrollment

This section is applicable for Account-driven User and Account-driven Device enrollments.

Supported devices

- Devices with iOS 15+ (for Account-Driven User Enrollment) and iOS17+ (for Account-Driven Device Enrollment)
- Devices with macOS 14+
- Devices with visionOS 1.1+

Prerequisites:

For Account-driven User Enrollment

- A user account in Ivanti Neurons for MDM with managed Apple ID (users in Apple Business Manager or Apple School Manager).
- Under the **Apple Enrollment** section, select **User Enrollment** from the **Select Apple Enrollment Type** dropdown list.
- Under the **Users** → **User Settings** →set the **Device Owner Settings** to **ON** > select **User Owned** option.

For Account-driven Device Enrollment

- A user account in Ivanti Neurons for MDM with managed Apple ID (users in Apple Business Manager or Apple School Manager).
- Under the **Apple Enrollment** section, select **Device Enrollment** from the **Select Apple Enrollment Type** dropdown list.
- Under the **Users** → **User Settings** →set the **Device Owner Settings** to **ON** > select **Company Owned** option.

Account-driven User Enrollment for iOS 15+, macOS 14+, and visionOS 1.1+ devices is an enrollment option designed for companies implementing BYOD (Bring Your Own Device). Account driven User Enrollment is a modified version of the MDM protocol and User Enrollment with Apple Business Manager with a much greater focus on user privacy, implemented with a level of security that enterprises need.

Account-driven Device Enrollment for iOS 17+, macOS 14+, and visionOS 1.1+ devices is an enrollment option designed for companies to enroll company-owned / corporate devices. Account-driven Device Enrollment leverages the MDM protocol and Device Enrollment with Apple Business Manager with a much greater focus on user privacy, implemented with a level of security that enterprises need. End users can enroll their devices using the Work Account feature in Settings.

Setup the discovery service

If your enterprise has an enterprise domain name, for example, acme.com, then the email ID for your device is devicename@acme.com.

1. The user enters username@acme.com to sign in to their work or school account, then the device makes a HTTP GET request call to the URL:
   https://acme.com/.well-known/com.apple.remotemanagement?user-identifier=user@acme.com
   For more information, see - https://developer.apple.com/documentation/devicemanagement/discover_authentication_servers
2. On the acme.com domain, configure redirection rule for the URI - /.well-known/com.apple.remotemanagement to redirect it to the following URL:
   https://<n-MDM cluster>/.well-known/com.apple.remotemanagement

Simplified service discovery for Account-driven Device Enrollment

> Applicable to iOS 18.2+, macOS 15.2+, and visionOS 2.2+ devices.

For account-driven enrollment, when a user enters their organisation email to sign into their work or school account, the device first searches for a well-known HTTP resource at the organisation's domain, which contains a link to the MDM enrollment URL.

Procedure

1. Sign-in to the Work or School account.
2. Verify domains in **Apple Business Manager** and **Apple School Manager** - Applies only to domains that have been verified within Apple Business Manager or Apple School Manager. If a domain is verified, the device can check with Apple Business Manager /Apple School Manager to get an alternate MDM enrollment URL.
3. Set a default Ivanti Neurons for MDM assignment for **Mac**, **Apple Vision Pro**, **iPhone**, and **iPad** platform types.
   For setting a default device assignment, follow the steps listed below:
   1. In **Apple Business Manager** / **Apple School Manager**, sign in with a user who has the role of Administrator or Device Enrollment Manager.
   2. Select your name at the bottom of the sidebar, select Preferences, then do one of the following:
      - Select Device Management Service Assignment below Your Device Management Services, then select Edit next to Default Device Management Service Assignment.
      - Select an existing service under Device Management Services, then select Change under Default Device Assignment.
   3. If you don't have any other configured device management services, change all automatic device assignments to the selected service, then select **Save**.
4. On the Ivanti Neurons for MDM console, navigate to **Admin** > **Apple** > **Device Enrollment**. In the **Device Enrollment** screen, **ADDE URL** and **ADDE URL SET TIME** columns are added.

> **First Preference**: The device checks the well-known HTTP resource at the organisation's domain.

Fallback Option: If the first method fails, the device contacts Apple ABM/ASM to fetch the alternative destination specified by Ivanti Neurons for MDM.

5. Under **Actions**, select **Configure ADDE URL**.
6. Refresh the page.

Device user instructions

This topic addresses the actions the device user needs to take for registering Account Driven User Enrollment or Account Driven Device Enrollment.

Procedure

1. On the device, go to one of the following:
   - For **iOS** device - **Settings** > **General** > **VPN** & **Device Management**.
   - For **macOS** device - **System Settings** > **Privacy & Security** > **Profiles**.
   - For **visionOS** device - **Settings** > **General** > **VPN** & **Device Management**.
2. Go to **Sign in to Work or School Account**.

3. Type the work or school account email address. Ensure that the email address is according to the following format: username@<enterprise domain name>, for example, username@acme.com.
4. The login page automatically takes the Managed Apple ID and takes the user through iReg flow. Ensure that you enter Ivanti Neurons for MDM credentials.
5. Type the work or school account credentials and click **Continue**.
6. After a 2-factor authentication, the device enrolment completes.

12.3.3. Device Enrollment

Device Enrollment is part of Apple Business Manager that enables customers to purchase devices in bulk and automatically enroll these devices in MDM during activation. If you choose to participate, you can use Ivanti Neurons for MDM as the MDM server for managing these devices. For more information, see https://business.apple.com/.

Connecting Ivanti Neurons for MDM to Device Enrollment

To use Ivanti Neurons for MDM as the MDM server for Device Enrollment, setup Apple Business Manager server token in Ivanti Neurons for MDM.

For each Apple Business Manager server, the following actions are available in Ivanti Neurons for MDM:

- Test Connection
- Add Device Enrollment Profile
- Download Public Key
- Device Enrollment Full Sync - Initiate full sync. It may take some time to be completed. After the sync is completed, you can view the information in the Last Sync column. You cannot initiate the full sync if it is already in progress.

> Ivanti Neurons for MDM notifies administrators when a DEP server sync fails, making it easier to identify issues. If you delete a DEP server, the system also deletes its related notifications.

- Upload New Token
- Delete

> The **Edit Authentication** and **Assign Device Enrollment Device Attribute** actions are now available for device enrollment profiles instead of device enrollment (MDM server).

Procedure

1. Go to **Admin** > **Apple** > **Device Enrollment**.
2. Click **Download Key**.
3. Save your Ivanti Neurons for MDM key.
4. Click **business.apple.com**.
5. Sign in using your Device Enrollment-eligible Apple credentials.
6. On the Apple Device Enrollment site:
7. In Ivanti Neurons for MDM, click **Upload**.
8. Click **Get Started**.
9. Select the trusted phone to use for authenticating to Apple service.
10. Enter the verification code sent to the selected phone.
11. Click **Add MDM Server**.
12. Enter a name to identify the virtual MDM server to be used with the service.
13. Click **Next**.

14. Upload the public key you downloaded earlier.
15. Click **Next**
16. Click **Your Server Token** to download the token.
17. Click **Done**.
18. Click **Next**.
19. Select an authentication option:

- **Prompt user for registration / login**

> Does not support devices operating with visionOS platform. Instead, use **Skip User Login** to enroll a device.

> Users will be prompted for a username and password. Users can enter either a password or a PIN for the password field. For macOS 15+ devices, additional options such as **Face ID**, **Touch ID**, or **security key** are also available for iDP users on passkey-supported identity providers. Password and PIN preferences can be configured in **Users** > User Settings related to authentication.

- **Skip user login**

> Devices assigned to the nobody user (anonymous) or a defined user can be reassigned to specific users at a later time from the **Devices** page.

Select one of the following options:

  - **Define one user to assign all devices to**
  - **Assign all devices to an anonymous user**

10. The selected option overrides the selections under User Settings.

Click **Upload** to install the key you received in Step 3.

11. Complete the displayed form to define the profile for your Device Enrollment devices:
12. Define which steps may be skipped by the user during device activation for the following setup options:.

Setting	What To Do
Name	Enter a name that identifies this Device Enrollment profile.
Description	Enter a description for the profile.
Department	Enter the department in your organisation that is associated with this profile.
Supervised Mode	Enables additional administrative control over configurations and restrictions. For iOS 13+ and macOS 10.15+ devices, this option is enabled by default.
iOS 17+	**OS Version for Enrollment** • **Require minimum OS version for enrollment**: Admin can set a minimum required OS version for devices enrollment. If device does not meet the minimum OS version criteria, the system prompts the user to upgrade to the required version. If the user denies to upgrade, the enrollment is blocked. **Latest Version**: Admin can set the latest OS version for devices enrollment. If device does not meet the minimum OS version criteria, the system prompts the user to upgrade to the required version. If the user denies to upgrade, the enrollment is blocked. **Specific Version**: Admin can set a minimum required OS version for devices enrollment. If device does not meet the minimum OS version criteria, the system prompts the user to upgrade to the required version. If the user denies to upgrade, the enrollment is blocked. • **Minimum iOS**: If the build version is not consistent with the OS version specified in the '**OSVersion**' key, the OS version will take precedence. • **Minimum Build version**: If the build version is not consistent with the OS version specified in the '**OSVersion**' key, the OS version will take precedence. This field is optional, if you enter incorrect build number • **Message**: A description of the error suitable for displaying to the user. If needed, ◦ the client will make a best-effort attempt to display the message, but may not ◦ be able to, due to local conditions. As a practice the message should be added. • **Add devices to beta program** **Beta Programs for iOS**: Enforces beta software versions on iOS during Automated Device Enrollment.
macOS 14+	**OS Version for Enrollment** • **Require minimum OS version for enrollment**: Admin can set a minimum required OS version for devices enrollment. If device does not meet the minimum OS version criteria, the system prompts the user to upgrade to the required version. If the user denies to upgrade, the enrollment is blocked. **Latest Version**: Admin can set the latest OS version for devices enrollment. If device does not meet the minimum OS version criteria, the system prompts the user to upgrade to the required version. If the user denies to upgrade, the enrollment is blocked. **Specific Version**: Admin can set a minimum required OS version for devices enrollment. If device does not meet the minimum OS version criteria, the system prompts the user to upgrade to the required version. If the user denies to upgrade, the enrollment is blocked. • **Minimum macOS**: If the build version is not consistent with the OS version specified in the '**OSVersion**' key, the OS version will take precedence.

Setting	What To Do
	• **Minimum Build version**: If the build version is not consistent with the OS version specified in the **'OSVersion**' key, the OS version will take precedence. This field is optional, if you enter incorrect build number • **Message**: A description of the error suitable for displaying to the user. If needed, ◦ the client will make a best-effort attempt to display the message, but may not ◦ be able to, due to local conditions. As a practice the message should be added. • **Add devices to beta program** **Beta Program for macOS** : Enforces beta software versions on macOS during Automated Device Enrollment.
Automatically download and install iOS updates	(iOS 9.0+ only) If the Automatic Downloads option is selected on the device under **Settings > iTunes & App Store**, the OS updates will be automatically downloaded, but not installed, even when the Device Enrollment Profile option is turned off. This setting will take preference when there is an iOS Software Updates configuration applicable to the Device Enrollment-enrolled supervised devices. Any change in this setting will be applicable to the Device Enrollment-enrolled supervised device even without reset of the device.
MDM Removable	Defines whether the user will be unable to unenrol from MDM after the device is registered. This setting is not applicable to **Shared iPads**.
MDM Mandatory	Defines whether the user will be unable to skip installing MDM during the activation process. For iOS 13+ and macOS 10.15+ devices, this option is enabled by default.
Do Not Use Profile From Backup	When enabled, the device does not use this profile when you restore the device from a backup. Applicable only for iOS 26+ and visionOS 26+ devices.
Allow Pairing	(Not applicable for iOS 13+ and macOS 10.15+) Allows host pairing functions, such as iTunes sync. Pairing is always allowed for hosts that have valid pairing certificates.
Return To Service	Set **Return to Service** to **True** to ensure that the application is preserved when the **Return to Service** action is executed. This allows the device to take a snapshot of the applications and provide a faster experience during the Return to Service process. If disabled device can still perform Return to Service, the application must be downloaded again during re-enrollment process. For leveraging **Apple Migration ABM** feature, this feature needs to be disabled. The device cannot be migrated if **Return to Service** is set to **True**. Applicable only for iOS 26+ and visionOS 26+ devices.
Certificate	Click **+ Add** to upload certificates.
Support Phone Number	Provide a phone number that device users can contact for help.

Setting	What To Do
Support Email Address	Provide an email address that device users can contact for help.
Custom Enrollment	(iOS 13.0+ and macOS 10.15+) Create custom enrollment web page(s). Specify your own custom web page (web view) to authenticate users during Device Enrollment. gov Use this page to display custom information such as authentication type, branding, consent text and privacy policy. See the "*Adding a custom Device Enrollment web page*" section following this procedure for more details. • Select **Enable Custom Enrollment** to enable this feature. • Enter the **URL**, such as https://mycustomweburl.com. This URL defines the value of the custom URL to present to the user in a web view.
Multi-User	(iOS 13.4+) Shared iPad for business Enables businesses to share devices between multiple employees, while still providing a personalised experience. Select **Multi-User Mode** to enable Shared iPad on a device. For more information, see **Shared iPad for business.** • This setting is not applicable to Apple Education. • Select the **Supervised Mode** setting to modify the Multi-User setting.
Quota Size	(iOS 13.4+) Shared iPad for Business. The value is in megabytes (MB) which denotes the storage allocated for a user in a device. If the value is too small, a default quota size is allocated by the device.
Resident Users	(iOS 13.4+) Shared iPad for Business The value denotes the number of users that can be persisted or residing on the device. If the value is greater than the value of maximum number of users that the device supports, MDM server uses that value (maximum number of users) as a default. Administrators can provide either Quota Size or Resident Users value. If both values are provided, MDM server uses Quota Size as default.
User session timeout	(iOS 14.5+) Shared iPad for Business Shows the timeout in seconds for a user session. The user session logs out automatically after the specified period of inactivity. The minimum value is 30 seconds. Setting this value to 0 removes the timeout and sets to device default timeout. Value from 1 to 29 is invalid. When set, the device is set to default timeout.
Temporary Session Timeout	(iOS 14.5+) Shared iPad for Business Shows the timeout in seconds for a guest or temporary session. The temporary session logs out automatically after the specified period of inactivity. The minimum value is 30 seconds,. Setting this value to 0 removes the timeout and sets to device default timeout. Value from 1 to 29 is invalid. When set, the device is set to default timeout.
Temporary Session Only	(iOS 14.5+) Shared iPad for Business If true, the user only sees the Guest Welcome pane and can only log in as a guest user.

Setting	What To Do
	If false, the user can sign in with a managed Apple ID (the existing behaviour). Default: false
Managed Apple ID Default Domains	(iOS 16.0+) Shared iPad for Business Specify a list of domains. Users can select their account domain from the list of domains in the QuickType keyboard.
Online Authentication Grace Period	(iOS 16.0+) Shared iPad for Business Specify the number of days the user can login without connecting to the network. Setting this value to zero enforces online authentication every time. **Default**: 0
Auto Lock Time	(iOS 17.0+) Specify the time (in seconds) after which the device goes to sleep mode. Minimum value is 120 sec.
Passcode Lock Grace Period	Specify the time (in seconds) after which the device user must enter the device passcode to unlock it. Min value is 0 sec and max value is 14400 sec.
Time Zone	Specify the timezone the device must belong to. **Example**: Pacific/Midway

Setup Options

- Skip Entering Passcode - Selecting this will auto enable Skip Apple Pay setup and Skip Touch ID.
- Skip Location Services
- Skip Restore From Backup
- Skip "Move to iOS" From Android
- Skip Terms Of Service
- Skip Signing In To Apple ID And iCloud - Selecting this will auto enable Skip Apple Pay setup.
- Skip Touch ID Setup (iPhone 5s, 6, 6+, iPad Air 2, iPad Mini 3 only) - Selecting this will auto enable Skip Apple Pay setup.
- Skip Apple Pay Setup (iPhone 6, 6+, iPad Air 2, iPad Mini 3 only)
- Skip Zoom Setup
- Skip Siri
- Skip intelligence (iOS 18+ and macOS 15+)
- Skip automatically sending diagnostic information
- Skip Cloud Storage (iOS 10.3+ & macOS 10.13.4+)
- Skip Display Tone Setup (iOS 9+ & macOS 10.14+)
- Skip Home Button Sensitivity
- Skip the keyboard selection screen
- Skip on-boarding informational screens - This information is for user education. For example: Cover Sheet, Multitasking & Control Centre.
- Skip the screen for Apple Watch migration
- Skip Choose Your Look screen (iOS 13.0+ & macOS 10.14+)
- Skip Screen Time (iOS 12.0+ & macOS 10.15+)
- Skip Privacy (macOS 10.13.4+ & tvOS 11.3+)
- Skip Enable Lockdown Mode (iOS 17.1+ and macOS 14.0+)
- Skip Software Update (iOS 12.0+ & macOS 15.4+)
- Skip Add Mobile Plan Pane (iPhone Xs, iPhone Xs Max, iPhone XR)
- Show custom text on the Login page - Select this option to enter a custom text message in the text box. This message will be displayed on the login page on the device during the Device Enrollment setup to provide any additional instructions to end-users to help them through the process.
- Auto advance setup - Select this option to setup assistant to automatically advance through the device setup screens. The default is set to false. Supported on tvOS and macOS 11 and later. Auto advance setup does not work on a WiFi connection, the device should be connected over an ethernet.
- Terms Of Address- Skips the Terms of Address pane. (iOS 16+)
- Skip Liquid Glass Pane (iOS 27.0+ & macOS 27.0+)

iOS

- Skip Get Started pane (13.0+)
- Skip iMessage & FaceTime (12.0+)

Setup Options

- Skip Spoken Language (13.0+)
- Skip Restore Completed (14.0+)
- Skip Update Completed (14.0+)
- Skip Safety (16.0+)
- Skip Action Button Setup Pane (17.0+)
- Skip Web Content Filtering Pane (18.2+)
- Skip Safety & Handling Pane (18.4+)
- Skip Multitasking Pane (26.0+)
- Skip OS Showcase Pane (26.0+)
- Skip Accessibility Appearance Pane (27.0+)

macOS

- Skip iCloud Analytics screen
- Skip True Tone Display screen (10.13.6+) - (Optional) Select this option to skip the True Tone Display window.
- Skip Accessibility (11.0+)
- Skip Unlock with Watch (12.0+)
- Skip Enable Lockdown Mode (14.0+)
- Skip Wallpaper Selection (14.1+)
- Skip Additional Settings Privacy Pane (26.0+)
- Skip Update Completed (14.0+)

tvOS

- Skip Apple TV home screen layout sync screen
- Skip the Apple TV provider sign in screen
- Skip Tap To Setup Option
- Skip The Aerial Screensaver Setup

macOS account setup assistant options

- Skip admin account creation
- Skip Primary Setup Account Creation
- Create primary accounts as regular users (as admin if not checked)

Await Device Configuration during Device Enrollment Setup

- Wait until configurations and high priority applications are pushed to devices - Select to push the configurations and high priority applications to the device before continuing with the remaining Device Enrollment setup screens. This setting will prevent the end-user from using the device before the required configurations and high priority applications are pushed to the device.

Setup Options
• Time Limit - Default time limit is 3 minutes. Maximum time is 10 minutes. To enable this feature, select the **Supervised Mode** option while editing the Device Enrollment profile.

Click **Save**.

The following table is populated in the **Admin** > **Apple** > **Device Enrollment** page:

Setting	What To Do
Name (Click on column heading to sort alpha-numerically.) Use the Search field to search for items from this column	MDM server name
Apple Account Name (Click on column heading to sort alpha-numerically.) Use the Search field to search for items from this column	Managed Apple ID
Number of Devices	Assigned devices count
Enrollment Profile(s)	Assigned device enrollment profiles count
Last Sync (Click on column heading to sort alpha-numerically.)	Last contacted time
Token Expires (Click on column heading to sort alpha-numerically.)	Token expiry date

- When new devices are added to Apple Device Enrollment, it might take up to 15 minutes for Ivanti Neurons for MDM to discover those new devices. The new devices are then assigned an enrolment profile. If you cannot add new devices to the Device Enrollment go to **Dashboard > Notifications** to check for notifications from Apple for Device Enrollment. If there are any updates to the EULA you will notified by email with steps to accept the new EULA.
- You can view all the custom device attributes that exist in your tenant and assign them to the devices during their enrolment via Apple Device Enrollment.
- In shared macOS devices, the ListUsers command shows a list all local users on the device and only the last check-in details of the user who registered the device.

Editing the Device Enrollment profile

Procedure

1. Go to **Admin** > **Apple** > **Device Enrollment**.
2. Find the name of the Apple Business Manager server (you created on the Apple site) in the Apple Account Name column.
3. Click the number link in the Enrollment Profile(s) column.
4. For a specific profile, select **Actions** > **Edit Device Enrollment Profile**.

5. Update and save the profile.

- If a Device Enrollment Profile is edited, the device count of the modified profile will be updated shortly.
- If you refresh the server token on Apple site, then the existing token will become invalid. However, the display in the Device Enrollment page, including the token expiration date, will remain until you upload the new token.
- If a Device Enrollment Profile is created or edited, the changes made to the profile can be viewed under the Audit Trials section. When you click the link under Details, you can view the Attributes, and the changes made to the attributes under the Before and After columns. You can notice the status of each Device Enrollment Profile as Created (for New profile), Updated (for editing any existing profile), or Deleted (for deleting any existing profile). For filtering the Device Enrollment Profiles under Audit Trails, you need to select Admin System as the Category, and Automated device enrollment type as the Type.

The Device Enrollment Profile contains the following details:

Setting	What To Do
Profile Name (Click on column heading to sort alpha-numerically.)	Enter a name that identifies this Device Enrollment profile.
Description (Click on column heading to sort alpha-numerically.)	Enter a description for the profile.
Department (Click on column heading to sort alpha-numerically.)	Enter the department in your organisation that is associated with this profile.
Support Phone Number (Click on column heading to sort alpha-numerically.)	Provide a phone number that device users can contact for help.
Number of Devices	Displays the number of devices for the profile
Actions	Manage profiles

Managing multiple Device Enrollment profiles

You can create multiple Device Enrollment profiles against each Apple Business Manager server. This way, different sets of devices can receive different configurations. Devices can also be moved from one Device Enrollment profile to another.

Procedure

1. Go to **Admin** > **Apple** > **Device Enrollment**.
2. Find the name of the Apple Business Manager server in the Apple Account Name column.
3. Click the number link in the Enrollment Profile(s) column.
4. To create a new Device Enrollment profile to be associated with the selected server, click **Create New Profile**. Create and save the profile.

5. To manage each profile, click **Actions** and select one of the following options:
    - **Set as Default Profile** - Set the profile as the default profile within same virtual server. New device registrations will receiving this default profile.
    - **Edit Profile** - Update existing profile.
    - **Edit Authentication** - Edits Device Enrollment authentication setting.
    - **Assign Device Enrollment Device Attribute** - Administrators use custom attributes for devices to associate additional properties with these objects. These properties can then be used to build groups or distribute configurations.
    - **Delete** - The default profile cannot be deleted. When a non-default profile is deleted, all the associated devices will be re-assigned to the default profile.
6. To move an enrolled device to from one profile to another within the same virtual server (and not between different Apple Business Manager servers), click the number link under the Number of Devices column. The reassignment of profiles are applicable to devices that are yet to be enrolled.
    1. To move a single device, click **Assign Enrollment Profile** for the specific device, select the profile from the drop-down list, and click **Assign**.
    2. To move multiple devices, select the devices and click **Actions** > **Assign Enrollment Profile**, select the profile from the drop-down list, and click **Assign**.

- If a Device Enrollment profile is edited, the device count of the modified profile will be updated shortly.
- If you refresh the server token on Apple site, then the existing token will become invalid. However, the display in the Device Enrollment page, including the token expiration date, will remain until you upload the new token.

Adding a custom Device Enrollment web page

Applicable to: iOS 13.0 and macOS 10.15 and supported newer versions

In the Custom Enrollment section, you can specify your own custom web page (web view) to authenticate users during Device Enrollment. Use this page to display custom information such as authentication type, branding, consent text and privacy policy.

Procedure

1. Go to **Admin** > **Apple** > **Device Enrollment**.
2. Find the name of the server you created on the Apple site.
3. Select **Actions** > **Edit Device Enrollment Profile**.
4. In the Custom Enrollment section, select **Enable Custom Enrollment**.
5. Select one of the following options:
    - **MobileIron Hosted webpage** - redirected to an Identity Provider (IDP) if the enrolment is using an identity provider such as Microsoft Active Directory Federation Services (ADFS) or Okta. This can also be redirected to the self-service portal for a Ivanti Neurons for MDM user with a non-IDP based authentication.
    - **Custom URL** - enter a URL such as https://mycustomweburl.com. This URL defines the value of the custom URL to present to the user in a web view loaded during the initial setup of a new Device Enrollment device or an erased device. Use this field to define your own authentication UI with authentication method. After the user is authenticated, the MDM enrollment profile is downloaded.

Workflow of the custom Device Enrollment web page

This section elaborates the behaviour of the custom Device Enrollment web page and the procedure to create the custom web page (web view).

When the custom web page specified in the **URL** field loads initially:

- The configuration web URL has an **https** scheme and is a **GET** request. The web page should use a publicly trusted certificate.
- A custom header **x-apple-aspen-deviceinfo** is appended to the GET request by the Apple device on which enrollment is initiated. It contains a base64 encoding of a CMS (Cryptographic Message Syntax) envelope that contains a plist with device attributes. This is the same information, in the same format, as provided in the initial POST request with token-based device enrollments.

When the custom web page loads subsequently:

- The device user interacts with the web page (web view) until the administrator's host server provides a **custom.mobileconfig** file to the client. The Ivanti Neurons for MDM server returns byte code of the MDM profile. In the administrator's host server, the custom.mobileconfig file should be set with a MIME type of **application/x-apple-aspen-config** so that the MDM profile for the device is downloaded and installed on the device.
- For authentication with Ivanti Neurons for MDM, the web page should contain the authentication user name and password credentials. It is recommended to create a separate user in Ivanti Neurons for MDM and assign Custom Enrollment role to the user fetching the MDM profile with the Ivanti Neurons for MDM server URL (for example, https://micloudDomain.com/c/i/dep/custom.mobileconfig).
- For device registration and to get the MDM profile from Ivanti Neurons for MDM, the administrator's host web server should make a POST call to the Ivanti Neurons for MDM server URL. It should also pass the header x-apple-aspen-deviceinfo with the value provided by the device when the device hits the GET URL to load the custom web page. If the registration user ID is not provided, the device is registered to the nobody user. Here are the additional details:
  - When a device hits the custom web URL configured in the Device Enrollment profile, administrator's host web server should capture the header "x-apple-aspen-deviceinfo" presented by the device.
  - To get the MDM profile for that device and its related user, administrator's host web server should make a POST call to the Ivanti Neurons for MDM server URL with the header x-apple-aspen-deviceinfo. It should contain basic authentication using a Ivanti Neurons for MDM user ID as a request parameter (for example, https://miCloudDomain.com/c/i/dep/custom.mobileconfig?user=name@company.com). The user should be assigned the Custom Enrollment role.
  - After the administrator's host web server receives the byte code, it should download the byte code to the device by setting response headers, Content-Disposition = attachment;filename="profile.mobileconfig" and Content-Type = application/x-apple-aspen-config.
- The web view closes and the OS attempts to install the profile, which must be an MDM enrollment profile.

> Ivanti Neurons for MDM does not authenticate the user ID for which the MDM profile is returned. Therefore, administrators should perform the necessary authentication for the user ID before requesting for the MDM profile.

For iOS, this workflow is supported during initial setup of an erased device. For macOS, this workflow is supported both within Setup Assistant and also via the Profiles preference pane, if Device Enrollment was skipped during Setup Assistant.

For developer information related to creating a custom web page, see the following Apple documentation references:

- **Web Views**
- **Authenticating Through Web Views**

- Sample code to implement a simple iPad web browser that can view either the desktop or mobile version of a website

Editing the Device Enrollment authentication setting

Procedure

1. Go to **Admin** > **Apple** > **Device Enrollment**.
2. Find the name of the server you created on the Apple site.
3. Select **Actions** > **Edit Authentication**.

Bootstrap token management for mobile accounts

Applicable to: macOS 10.15 devices and supported newer versions that are device enrolled in MDM using Apple School Manager or Apple Business Manager.

Ivanti Neurons for MDM supports bootstrap token management for mobile accounts. Bootstrap tokens enable mobile accounts to sign in to macOS devices that are using FileVault. Using this feature, all mobile accounts that log in get a SecureToken automatically. This feature is beneficial when multiple users log in to an encrypted machine.

When a managed admin account tries to login to a device:

- For the first login, the bootstrap token is requested from the MDM server.
- If the MDM server provides the bootstrap token, the device will create a SecureToken for the account automatically.
- The device enables FileVault for the user.

Bootstrap Token Available is a field available in the device details page and as a filter attribute while creating a new device group or a custom policy.

For troubleshooting and verification purposes, go to the device details page for a device. Use the Logs page to narrow the device logs using filters based on action names Set Bootstrap Token and Get Bootstrap Token.

Setting up managed macOS admin account using Device Enrollment

Ivanti Neurons for MDM supports Device Enrollment registration on devices that have been reset to factory default or are being activated for the first time. Using Device Enrollment, an admin account can be created on the macOS device. Ivanti Neurons for MDM supports only optional enrollment for macOS and, therefore, Ivanti Neurons for MDM ignores the **MDM Mandatory** field in the Device Enrollment profile because it only applies to iOS devices.

Procedure

1. Go to **Admin > Apple > Device Enrollment**.
2. Find the name of the server you created on the Apple site.
3. Select **Actions > Edit Device Enrollment Profile**.
4. Select one of the following options from the macOS account setup assistant options:
    - **Skip admin account creation** - Select this option to disallow creating an admin account, either visible or hidden. Deselect this option to allow an admin account to be created in the **Set up Managed macOS Admin Account** section (described below).
    - **Skip primary setup account creation** - Select this option to skip setting up the primary account on the macOS device. No user account is created besides an admin account. An additional section, **Set up Managed macOS Admin Account**, will be

displayed (described below) to create the managed macOS admin account. The account can also be hidden from Users & Groups.

- **Create primary accounts as regular users (as admin if not checked)** - Select this option to create a non-admin standard account as part of the enrollment. An admin account can still be created by the Admin and pushed to the device. An additional section, **Set up Managed macOS Admin Account**, will be displayed (described below) to create the managed macOS admin account. The account can also be hidden from Users & Groups.

After selecting one of the above options, enter the following details in the **Set up Managed macOS Admin Account** section if you want to create a managed macOS admin account:

- Full Name
- Account Name
- Password
- Confirm Password
- (Optional) Hide managed administrator account in Users & Groups

If you do not select **Skip Primary Setup Account Creation**, enter the following details in the **Set up Primary Account** section. This adds user channel support for managed admin account by setting managed local user short name to an administrator's short name.

- **Full Name**
- **Short Name**
- (Optional) **Prevent modification by end user** - This setting will be overridden if Full Name and/or Short Name have substitution variables and are evaluated empty. If you select this option, confirm you understand that this primary admin account setup is applicable only if one of the below options is set appropriately:
  1. Prompt User Registration/Login is selected in the Authentication setup view.
  2. MobileIron-hosted webpage is selected for Enrolment Customisation.

7. Select **Skip Primary Setup Account Creation** to enable user channel support for managed admin account. You can set managed local user short name to an administrator's short name.
8. Click **Save**.

Changing the local macOS admin account password

An administrator can change the local password of a local macOS admin account that was created by Setup Assistant during Device Enrollment enrolment.

Applicable to: macOS 10.11 or supported newer versions.

Procedure

1. Go to **Devices**.
2. Click the user name the device is associated with to view the device details page.
3. From the Actions menu, click **Set macOS Admin Password**.This action can be performed in Device List page as well by selecting one or more devices.
4. Enter the password.
5. Click **Save**.

Export to CSV

Ivanti Neurons for MDM lets you export the Device Enrolled devices to a CSV file.

Procedure

1. Go to **Admin** > **Apple** > **Device Enrollment**.
2. Click the specific device count link under the **Number of Devices** column.
3. Click the **Export to CSV** option to export the devices list and related details to a CSV file. Once the report is ready, you will be prompted with a message to either Download or Delete the report. You will also receive an email containing a link to download the report.
4. Click **Download**.
5. (Optional) Click **Delete** to delete the report.

12.3.4. Beta Enrollment

Ivanti Neurons for MDM can automatically enroll devices remotely at a later time if the device is supervised and runs iOS 18, iPadOS 18, macOS 15 or later. If necessary, a supervised device can be removed from beta programs and restrict a user from enrolling manually. This removes the need for manual steps performed by the user and allows for a streamlined process throughout the beta testing lifecycle.

Prerequisites

- Device Enrollment is mandatory for Beta Enrollment. For more information about Device Enrollment, see **Device Enrollment**.
- To offer AppleSeed for IT beta versions without the need for an Apple Account, an administrator in Apple Business Manager or Apple School Manager must sign in to the AppleSeed for IT portal, and accept the terms and conditions on behalf of their organisation for the current beta period.

Connecting Ivanti Neurons for MDM to Beta Enrollment

To use Ivanti Neurons for MDM as the MDM server for Beta Enrollment, setup Apple Business Manager or Apple School Manager server token in Ivanti Neurons for MDM.

Beta Enrollment section

Name	Description
Organisation Name	Name of the organisation.
Last Sync	Date and time at which the sync was performed.
Status	Status of the sync.
Beta Enrollment Token Sync	Click **Sync** to sync the newly available Beta enrollment tokens for beta updates.

12.3.5. Configuring the Setup Assistant

The Configuration Setup Assistant lets you select the setup screens that you want to skip or include during device setup for iOS and macOS devices.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative console.
2. Go to **Configurations**.
3. Select **Setup Assistant**.
4. Click the pencil (edit) icon.
5. Select the check boxes to skip the specific setup screens from the device.
6. Click **Done**.
7. Select **Device Channel**.
8. Select **All Devices**. The Setup Assistant configuration is pushed to the devices and the Configuration tab under in the Device Details page displays the Installed state.
9. Log in to the device. All the initial setup screens are skipped.

12.3.6. Install MDM Certificate

You must request and install an Apple MDM certificate to manage iOS devices. You also need to renew this certificate once a year. (The Apple account used for creating the certificate receives a notification from the Apple site when the expiration date approaches.) Use the MDM Certificate page to add or renew this certificate.

Acquiring and installing the MDM certificate

Procedure

1. Use the **MDM Certificate** page to download a certificate signing request (CSR) from your Ivanti Neurons for MDM tenant.
2. Upload the CSR to Apple to create a new certificate.
3. On the Apple site, add a note indicating what the certificate is for. This note will help you when it is time to renew the certificate. Save the resulting certificate.
4. Install the certificate for your Ivanti Neurons for MDM tenant.

Renewing the MDM certificate

Procedure

1. Click **Renew Certificate**.
2. Download a certificate signing request (CSR) from your Ivanti Neurons for MDM tenant.
3. Upload the CSR to Apple to renew the corresponding certificate.
4. On the Apple site, make sure you are renewing the correct certificate. Uploading a different certificate to Ivanti Neurons for MDM will automatically retire all registered iOS devices.
   Install the certificate for your Ivanti Neurons for MDM tenant.

You will receive a warning if you attempt to upload the wrong certificate.

If you cannot see the **Install MDM Certificate** page, it might be that you do not have the required permissions. You need one of the following **roles**:

- System Management
- System Read Only

12.3.7. Shared iPad devices for business

Shared iPad devices for business is available for the Managed Apple IDs that are created in Apple Business Manager with iOS 13.4 or supported newer versions.

- Shared iPad enables businesses to share devices between multiple employees, while still providing a personalised experience.
- Employees can sign in with a Managed Apple ID to begin loading their data, including their Mail accounts, files, iCloud Photo Library, app data and more.
- The data is stored in iCloud, so employees can sign in to any Shared iPad device that belongs to the organisation.

Shared iPad devices can be used in healthcare, retail, and industrial applications. For example, doctors and nurses can share one iPad device, as they can each securely access the user profile uniquely designed for them. In retail stores, front-line workers can be empowered with access to product information, resources, expertise to delight the customers and provide better shopping experiences.

How it works

- The iPad devices are added to Apple Business Manager, and are enrolled using an automated enrollment profile with the Shared mode on.
- Employees sign in to the Shared iPad device with a company-provided Managed Apple ID and password. Apple Business Manager administrator can manually create the accounts for the users or federate the account creation to an identity provider such as Entra ID.
- Each user can have their custom profile when they are logged into the Shared iPad device. Administrators can distribute apps based on the users role, responsibilities, and department.
- Users can log in as guest users on a Shared iPad device. The guest user log-in is enabled by default. A guest user need not sign in with a Managed Apple ID and password. The guest user login can be disabled by setting the **Allow Guest Session for Shared iPad** option to **False** in the **iOS Restrictions** configuration.
- Go to Ivanti Neurons for MDM **> Devices**, click on a Shared iPad device name, and click the **Users** tab to view the list of users on the device and their details (such as Managed Apple ID, Data Available in bytes, Data Used in bytes, Has Data to Sync to Ivanti Neurons for MDM).
- Go to the **Logs** tab, from the filters select the **Report User List** action to view additional user details.
- The guest user log-in in a Shared iPad device is different from the guest user management by Ivanti Neurons for MDM. By default, guest user account is disabled in Ivanti Neurons for MDM. To manage a guest user in a Shared iPad device, enable the guest user account.
- Screen recording is available from Control Centre on Shared iPad devices.
- Ivanti Neurons for MDM supports a substitution variable for Managed Apple ID, `${managedAppleID}`. This system variable is displayed in the system attributes section and in the device attributes section.
- Ivanti Neurons for MDM restricts an administrator from changing the Managed Apple ID of resident user(s) who were logged in to the Shared iPad device in the past along with the currently logged in users. If you try to change the Managed Apple ID, an error message indicates that the user's Managed Apple ID cannot be changed since the user is using a Shared iPad device.
- In the case of **Apple Apps and Books**, Apps and Books are installed on Shared iPad devices based on device-based licenses regardless of whether device-based licenses are selected or not.

Prerequisites

Ensure that the following prerequisites are met:

- A Shared iPad device requires Managed Apple ID. Administrators can manually create the accounts or federate to an identity provider such as Entra ID.
- The Shared iPad devices must contain iOS 13.4 or supported newer versions.
- The devices must be associated with Apple Business Manager accounts.
- The devices must contain storage of 32GB or more.

Note the following points:

- Ivanti Neurons for MDM restricts certain configurations, such as Passcode, for Shared iPad devices as Apple does not support them. Such configurations are not pushed to the devices (Devices > click a device name link > Configurations tab).
- The **Passcode** configuration does not apply to the Shared iPad devices as they require Managed Apple IDs, which are associated with passwords and not passcodes. The Unlock action from the Ivanti Neurons for MDM administrative portal will not clear passcode on a Shared iPad device.
- Select either the Device Channel or the User Channel during the distribution of the **iOS Restrictions configuration** to Shared iPad devices. You can distribute separate configurations and enforce restrictions that are applicable only to the device or the user channel.
- Ivanti Neurons for MDM verifies the expired accounts and retires the devices with expired accounts as owners. However, for a Shared iPad device, the device owner is the last logged-in user and may not be the legal owner. If an owners account expires, Ivanti Neurons for MDM excludes the Shared iPad devices from retiring .
- Go for iOS client is not supported for Shared iPad devices.
- Users cannot perform actions such as retire and wipe on Shared iPad devices. Only administrators can perform retire and wipe actions from the Ivanti Neurons for MDM administrative portal.
- Administrators cannot change the owner of Shared iPad device from the Ivanti Neurons for MDM administrative portal.
- Zero sign-on is not supported for Shared iPad devices.
- When the ListUsers command is enabled, all managed user IDs and their check-in time are displayed in the Device Enrollment (Part of Apple Business Manager) under the **Admin** tab.

Configuring a Shared iPad device

You can set up a Shared iPad device and configure the settings.

Procedure

1. Go to **Admin** > **Apple** > **Device Enrollment**.
2. Add the device to Apple Business Manager by enrolling the device using an automated device enrollment profile. For information about this procedure, see **Device Enrollment**.
3. In the Device Enrollment settings, enable:
   - **Supervised Mode**.
   - **Multi-User Mode** under **Shared iPad device for business**.
4. (Optional) Create a local user account. The device will be registered to this user. The authentication as this user happens only once during the registration.
5. Reset the Shared iPad.

> The registration process starts only after the reset. It takes a few minutes for the device to be registered and configured as a Shared iPad device.

6. The legal owner is assigned to the user account who registered the device. The administrator can change the legal owner from the **Devices** page.
7. On the device login screen, enter the Managed Apple ID credentials of the user.
    - Similar to macOS devices, you can push configurations on Shared iPad devices through both device and user channels.
    - The user substitution variables are not substituted for configurations (including the Managed App configuration) pushed in the device channel.
    - If the logged in user in a Shared iPad device is not a managed user- the Managed Apple ID does not belong to any user in the Ivanti Neurons for MDM administrative portal, the device is not assigned to anyone. The users will not be managed - the administrator cannot push user channel configurations from Ivanti Neurons for MDM.
    - By default, the default guest user created by Ivanti Neurons for MDM is disabled. When a guest user logs in, the device is not assigned to any user and the user is not managed. If the guest user has to be managed, the default guest user created by Ivanti Neurons for MDM must be enabled and the device is assigned to the default guest user after the guest user logs in. The user can then be managed.
    - The device owner information is displayed in the Ivanti Neurons for MDM > **Devices** page and in the device logs (device details page > **Logs**).

Managing legal owners for Shared iPads

You search and view the legal owners of the Shared iPad devices using their email IDs from the device listing page. You can change the legal owners of the Shared iPad devices by reassigning the existing legal owners to the new legal owners. If the legal owner of a non-Shared iPad device is reassigned, Ivanti Neurons for MDM ignores the assignment.

Procedure

1. Go to **Devices**.
2. Click the gear icon to select and add the **Legal Owner** column to the devices list page.
3. Select the Shared iPad devices.
4. Click **Actions > Assign to Legal owner**.

Sending an email to the legal owner of a Shared iPad device

You can send emails to the legal owner of a Shared iPad device.

Procedure

1. Go to **Devices**.
2. Click the name of the Shared iPad device.
3. Click the **email** icon.
4. Compose the email.
5. Click **Send**.

Using the Multi-User Mode attribute

You can use the Multi-User Mode attribute of the Shared iPad devices in Ivanti Neurons for MDM.

Procedure

1. In the **Devices** page, use the **Multi-User Mode** attribute.
2. Click **Advanced Search** and create a rule to find the devices using the **Multi-User Mode** attribute.
3. In the **Devices > Device Groups** page, create a dynamic device group for the Shared iPad devices using the **Multi-User Mode** attribute. For example, you can use this group as a distribution filter to distribute configurations.
4. In the **Policies** page, create a custom policy for the Shared iPad devices using the **Multi-User Mode** attribute.
5. In the **Apps > Distribution Filter**, use the **Multi-User Mode** attribute to limit the number of applications available for installation.

- Ivanti Neurons for MDM does not support multi-user mode for Apple School Manager devices. It is not recommended to enable the setting and push the Device Enrollment profile to Apple School Manager devices.
- The Multi-user Secure Sign-In for iOS configuration is not applicable to Shared iPad devices.

Deleting users from a Shared iPad device

You can delete a user or multiple user accounts from the Shared iPad devices. In the User list tab, the **Active** label is displayed for the currently logged in user. The Delete option is not applicable for the currently logged in user on the Shared iPad device. Users can be deleted from the **Devices** or the **Users** tab.

Deleting users from the Devices tab

Procedure

1. Go to the **Devices** tab > **Device Details**.
2. Go to the **Users** tab. The list of users are displayed.
3. Click **Delete All Users**.
4. Click the "**-**" minus sign to delete specific users.
    - (Optional) In the **Delete User** window, select **Force delete user even if the data sync to Ivanti Neurons for MDM is pending** option and click **Yes**.

      Selecting **Force Delete user even if the data sync to Ivanti Neurons for MDM is pending** will force delete the user even if the data is not already synced to the Ivanti Neurons for MDM administrative portal.

Deleting users from the Users tab

Procedure

1. Go to the **Users** tab.
2. Select a user or multiple users, go to the **Actions** drop-down menu, click **Delete**. A confirmation message appears. After you confirm the delete user command is issued to the devices.
3. Go to **Device logs** in the device details and verify that the Delete user command is sent to the selected users of the Shared iPad device.

Logging out users from a Shared iPad device

The administrator can log out users from a Shared iPad device.

Procedure

1. In the **Devices** page, select a Shared iPad device.
2. Select **Force Logout** from the **Actions** menu. A pop-up prompts for confirmation on logging out users from the Shared iPad device.
3. Click **OK** to approve the force logout.

12.3.8. School Manager

Licence: Gold

Applicable to: Supervised iOS 9.3+

Apple School Manager is an Apple cloud service dedicated to education institutions to provide services including purchasing apps in Apple Apps and Books, enrolling iPads through Apple Device Enrollment, and creating managed Apple IDs. With full integration with Apple School Manager, Ivanti Neurons for MDM UEM solution provides a seamless way to fully manage the iPads designated for teachers and students in order to leverage the School Manager ecosystem and apps such as Classroom.

> Apple Books are not supported.

Configuring School Manager

1. Go to **Admin > School Manager**.
2. Click the **Setup Education** option if it is turned off.
3. Select one of the following options:
   - **Sync with the Apple School Manager account to import school information**:
     1. Go to **Admin > Apple > Device Enrollment** to download your organisation's key files.
     2. Upload the key files to your Apple School Manager account to generate encryption keys.
     3. Download the encryption keys from Apple School Manager and upload the keys into Ivanti Neurons for MDM (**Admin > Apple > Device Enrollment**).

        > Existing Apple Device Enrollment accounts can be reused for Apple Education. Apple will give you the option to upgrade your Device Enrollment account to include Education capabilities when you access the Apple School Manager. For the upgrade instructions, visit https://support.apple.com/en-in/HT206960.

     When the encryption keys are accepted, the **Sync Now** button appears.

     4. Click **Sync Now** to start data sync with Apple School Manager.
   - **Import data from CSV files**:
     1. (Optional) Click **Download CSV templates ZIP file** to download a zip file that contains templates of all the data types.
     2. Click **Select files**...
     3. Add the following six CSV files:
        - Students data file (students.csv)
        - Roster data file (roster.csv)
        - Staff data file (staff.csv)
        - Classes data file (classes.csv)
        - Courses data file (courses.csv)
        - Locations data file (locations.csv)

        > Note: You must select all the six CSV files together, every time, before uploading them.

Click **Upload**.

4. (Optional) If the CSV files need to be modified, please retain all necessary data in all six files that had been previously uploaded. Make the required edits and upload them together once again.

Search for data from the **Classes** and **Individuals** tab.

> The individuals (students and staff) also appear in the **Users** page of Ivanti Neurons for MDM.

5. Create two device groups for devices that will be used for education by students and staff as follows:
    1. Go to **Admin > Custom Attributes**.
    2. Create custom attributes for students and staff that will be used to create dynamically managed device groups.
    3. Go to **Devices > Device Groups**.
    4. Click **Add+**.
    5. Create one each dynamically managed device group for students and staff using the custom attributes created previously as filters.
6. Assign registered devices to students and staff from the **Devices** page using the **Actions > Assign to user** option.
7. Create a Leader (staff) configuration and a Member (students) configuration by adding the **Configurations >** Education payloads.
8. Distribute the Leader (staff) and Member (students) configurations to the staff and student device groups.
   This distribution will push these configurations and install certificates on the respective devices.

> On the **Admin > School Manager** page, if there is no value present for the Class Name, the value is derived from the class system source identifier and the course identifier fields. These fields are optional in the Apple School Manager or the CSV file. However, it is recommended to enter a value at all times as their combination is used as the default identifier in the absence of a Class Name.

Pushing the Classroom app to the teachers

Using the Classroom app, the teachers (Leader) can manage the following scenarios:

- Classroom management ability to control iPads and apps remotely.
- Ability to create a class group.
- Ability for a teacher to view the student members of that group.
- Ability for a teacher to send content to the students in that group.
- Restrict what apps and content the students can view.

You can push the Classroom app from the Apple App Store.

Procedure

1. Go to the **Apps > App Catalog** page.
2. Click the **+Add** button.
3. Search for and select the Classroom app by Apple.
4. Click **Next**.
5. Enter the category and description.

6. Click **Next**.
7. Distribute the app to the teachers device group created previously.
8. Configure the app settings in the App Configurations page.
9. Click **Done**.

Disabling School Manager

Disabling School Manager will wipe all the current data. Please exercise caution while doing so.

1. Go to **Admin > School Manager**.
2. Click the **Setup Education** option if it is turned on.
3. Click **Yes**.

12.3.9. Settings (Apple)

Administrators can configure, enable, disable various settings for Apple devices.

Silent registration (for macOS only)

Silent registration for macOS devices is locked as Enabled. This applies to all new device registrations in the tenant and is supported by Mobile@Work 1.4 and or supported newer versions.

General settings

Disable Device Reconciliation - Administrators can now retain the device entries if they want to register the same device again. By default, this option is not selected. Select this option to retain the inactive device details.

> When Disable Device Reconciliation is not enabled, and If a device is re-registered with same user, new entry will be created. Otherwise, the device entry will be updated with new registration information.

Profile settings

Administrators can enable or disable sending emails to the end-users and notifications to the macOS and MobileIron Go for iOS clients if the MDM profile is not installed. The MDM profile notifications feature is enabled by default.

Procedure

1. Go to **Admin > Settings**.
2. Select or deselect the **Send email to user and notification to client if MDM profile is not installed** option.
3. Select the maximum number of emails/notifications between 1 to 4.
4. Click **Save**.

OS updates for automated device enrollment (iOS only)

Administrators can turn on iOS operating system updates for automated device enrollment. If this option is enabled, then the Device Enrollment devices will use the **Software Updates** configuration instead of the schedule OS update setting in the Device Enrollment Profile.

This option is disabled by default, in which case the schedule OS update setting in the Device Enrollment Profile is used. Turning on this setting is permanent and cannot be turned off. This setting will remove the schedule OS update setting in all the available Device Enrollment profiles.

> Supervised non-Device Enrollment devices use the Software Updates configuration.

Procedure

1. Go to **Admin > Settings**.
2. Select or deselect the **Use Software Update Configuration for Automated Device Enrollment** option.
3. Click **Yes** to confirm.
4. Click **Save**.

Multi-user Secure Sign-In

The administrators can clear the device password when the user logs out from the Multi-user Secure Sign web clip on iOS shared devices by selecting the "**Clear passcode after User logout**" option in the "**Multi User secure sign-in**" section under Admin > Apple > Settings

Priority Settings for Restrictions Configuration

The administrator can enable priority for multiple iOS and macOS restrictions configurations by selecting the **iOS Restrictions Configuration** or **macOS Restriction Configuration** options in the **Priority Settings for Restrictions Configuration** section under the **Admin >Apple > Settings**. This option is disabled by default. For more information on how priority works, see Prioritising Configurations

Procedure

1. Go to **Admin > Apple > Settings**.
2. In the **Priority Settings for Restrictions Configuration** section, select the **iOS Restrictions Configuration** or **macOS Restriction Configuration** option.
3. Click **Save** to enable priority. The "**Priority Settings for Restrictions Configuration (iOS or macOS) has been enabled**" banner is displayed. Before the priority is **Approved**:
    - **Edit distribution summary (if applicable)**: When priority setting is enabled, the distribution summary for the selected restrictions configuration is changed from "**Apply to devices in other spaces**" is changed to "**Apply to all devices in other device spaces as highest priority**" by default.
    - **Default priority is assigned in the order of creation**: For selected restriction type configuration, an existing default priority is assigned in the order it was created.
    - **Suspension of management of the configuration**: The management of the selected restrictions configuration (for example, iOS Restrictions Configuration) is suspended until you approve the priority.

> After priority is enabled, any changes in the restrictions are not processed until they are approved. Before approving, the admin can edit the distribution, distribution summary, or priority for restrictions configuration in the **Configurations** section.

4. Select the **Approve** option to put priority in effect.
5. Click **Save**.

> The **Approval** option is not available when deselecting an iOS or macOS Restrictions configuration option, the changes are applied instantly.

When priority setting is disabled, there is no priority associated with the configurations. All restriction configurations are pushed to the device if applicable (on next device sync).

- **Distribution summary (if applicable): When priority setting is disabled for restriction configuration, distribution summary is changed from Apply to all devices in other device spaces as highest priority or Apply to all devices in other device spaces as lowest priority to "Apply to devices in other spaces".**
- **No priority is assigned**: Assigned priority is removed for selected restrictions configuration

12.4. Work with Windows Devices

This section contains the following topics:

- Configuring Windows Autopilot Profiles
- Audit Trails on Windows Autopilot Profiles
- TenantLockdown CSP
- ADMX (GPO) Browser
- Configuring app inventory intervals
- Hardware Inventory

12.4.1. Configuring Windows Autopilot Profiles

Windows Autopilot is a Microsoft feature that helps administrators to setup and pre-configure new devices to make them business ready. The Autopilot feature helps with a quick, reliable, and seamless provisioning of Windows Desktop or HoloLens2 devices. In addition, the Autopilot feature helps perform the following tasks:

- Automatically join devices to Entra ID (Entra ID)
- Auto-enrol devices into MDM services
- Create and auto-assign devices to configuration groups based on the profile of the device
- Customise the enrolment experience
- Apply configurations and policies
- Install essential applications

Prerequisites

To operate the Windows Autopilot page, review the Ivanti Neurons for MDM partner steps and Azure licensing requirements. Make sure that the following prerequisites are met for the Autopilot feature to function as expected:

- **Azure Licensing for Autopilot requirements**: Check for “Windows Autopilot licensing requirements."
- **Azure Windows Autopilot Devices Registration**: Check for "Windows Autopilot registration overview."
- **Resellers adding devices to customer account**: Check for "Use Windows Autopilot profiles on new devices to customise a customer's out-of-box experience."

Additional Requirements

1. Integrate Entra ID tenants and Ivanti Neurons for MDM. For more information, see **Setup with Microsoft Azure**.
2. Make sure that you have an administrator account in Ivanti Neurons for MDM and Entra ID.
3. To leverage self-deploying profiles, create a fake user for enrollment of user-less self-deploying devices in Ivanti Neurons for MDM.
4. Create and sync a dummy user, fooUser@Entra IDPrimaryDomain.com from Entra ID Primary Domain.

> Microsoft licenses are not needed to create and sync a dummy user.

5. The "Custom domain names" page in Entra ID displays the primary domain of your Entra ID environment.
6. Make sure that the user can enroll devices and is not disabled. For example, if the primary domain is contoso.com, resulting user will be fooUser@contoso.com. If the primary domain is contoso.onmicrosoft.com, resulting user will be fooUser@contoso.onmicrosoft.com.
7. To provision the user with SCIM into Ivanti Neurons for MDM, edit the user details in Entra ID and add the email address. Generally, the email address will be the same as UPN.
8. Make sure that all the users, including the fooUser are present in Azure and Ivanti Neurons for MDM.
9. Administrators can create Autopilot Profiles using Microsoft Store for Business or Ivanti Neurons for MDM. To create profiles using Ivanti Neurons for MDM administrators require Global Entra IDmin and Intune administrator permissions.

> Administrators need Azure P1 or P2 and Ivanti Neurons for MDM Secure UEM or Secure UEM Premium licenses are needed. The Intune license is not needed for administrators.

> In Neurons for MDM, creating Autopilot Profiles feature leverages Microsoft Graph APIs for Autopilot, which are still in beta.

Autopilot Enrolment Modes

After you associate devices with a specific user profile group, based on the device usage, you can configure the Autopilot enrolment mode to allow users to quickly get started with their device. Ivanti Neurons for MDM provides the following Autopilot enrollment modes:

- Self-Deploying mode
- User-Driven (Pre-Provisioned mode)
- User-Driven

Self-deploying autopilot mode - The self-deployment Autopilot device enrollment mode makes sure that a seamless deployment of an enterprise device for a user by bypassing the initial device setup and by pushing all the necessary configuration files that are required for the device to securely get started. This mode secures the hardware, connects the device to the enterprise network, enrolls the device to the Entra ID (Entra ID), the MDM service, and to the Ivanti Neurons for MDM administrator portal using a dummy user ID and all the necessary configuration files are pushed to the device before the user logs in. After the mandatory configuration files are pushed to the device, the device restarts and displays the login screen for the enterprise user to get started. You can use the self-deploying mode for a device that can be used as a kiosk or digitally signed device.

User-driven pre-provisioning profile mode – Once the administrator creates a User-driven pre-provisioned profile, the administrator assigns the profile to a user group, and the device hardware ID is uploaded and assigned to the Entra ID group. The device will be associated to the user-driven pre-provisioned profile. This mode is used by the administrator to setup a device before it is handed over the enterprise user.

Procedure

Follow the steps for pre-provisioned deployment:

1. Connect the new hardware device to the LAN and press the Windows button five times.
2. The device displays a question prompt. Select the option Windows autopilot provisioning and click Continue. The Entra ID detects the User-driven pre-provisioning profile mode, and all the basic configuration settings are deployed in the device. The Windows Autopilot Configuration screen is displayed.
3. Click Proceed. The device progresses and secures the hardware, connects the device to the enterprise network, enrolls the device to the Entra ID (Entra ID), the MDM service, and to the Ivanti Neurons for MDM administrator portal using a dummy user ID and all the necessary configuration files are pushed to the device and a confirmation message appears.
4. You can now hand over the device to the user. When the user logs in to the device, the user ID is enrolled into the Ivanti Neurons for MDM administrator portal with the device details.

The following configurations are pushed automatically before the user logs in to the device:

Identity Certificate

Wi-Fi

Windows Hello For Business

The rest of the configurations are in Pending state and are pushed after the user logs in to the device using an email address.

During the Autopilot enrollment process in Self-deploying and User-driven (pre-provisioning) modes, the assigned .MSI, and .EXE apps will be installed on the device to complete the enrollment process. When installing the .MSI, and .EXE apps during Autopilot enrollment process, if the apps report or fail to report during the installation, the Autopilot process will be completed and the Reseal button will be enabled.

Creating Windows Autopilot User Profiles

After you configure the Entra ID (Entra ID) User Source and sync the users and Entra ID user groups with the Ivanti Neurons for MDM tenant, you can create the Autopilot profiles.

Procedure

1. Log in to the Ivanti Neurons for MDM administrator portal.
2. Go to **Admin > Microsoft Azure > Windows Device Management**.

If the Entra ID User Source is not configured, the **Add** button will be disabled. You need to configure the User Source using the **Windows Device Management** option present under the **Microsoft Azure** section.

3. Click **Add**.
   The **Add Windows Autopilot Profile** page appears on the screen.
4. Enter a profile name in the **Name** box.
5. Complete the **Profile Settings** using the table below this procedure.
6. Click **Next**.
   A new page with all the Entra ID Device Groups appears on the screen.
7. Select the one or more Entra ID Device Groups to which the Autopilot Profile must be assigned.
8. You can also create a Entra ID Device Group and assign the Autopilot Profile to this newly created group. See for more information.
   If you want to assign the Autopilot Profile to all the Entra ID Groups, select the **Assign to all Entra ID Groups** option.

You cannot assign more than one profile to “All Groups” due to a limitation from Microsoft.

9. Click **Done**.

Setting	Description
Device Type	Select one of the following two options depending on the device: • **Windows PC** • **HoloLens** - When this option is selected, the default deployment mode should be set to **Self-Deploying** mode. In rare cases, when enrolling HoloLens 2 devices using Autopilot, the enrolment might get stuck on the 'Setting up your device for work' screen. In such a rare case, the user must power off and on the device by pressing the Power button. The device then shows the Login screen where the user should enter the Entra ID credentials to complete the enrollment.
Deployment mode	• **Self-Deploying**: In this mode, the device deployment happens with little or no manual involvement. • **User-Driven**: Administrators can use this option to select the enrolment mode to configure a new device for the user before they hand over the device to the user.
User account type	• **Administrator**: Select this option if the user needs complete control once the device is deployed. • **Standard**: Select this option if the user needs authorisation to the basic options once the device is deployed.
Language	By default, the language will be Operating system specific. You can change to a different language from the list.
Convert all targeted devices to Autopilot	Select this option to convert all devices in the assigned group to Autopilot.
Allow Pre-provisioning	Select this option to register devices for Autopilot using the normal registration process. This option is not available when the **Self-Deploying** option is selected.
Automatically configure keyboard	Select **Yes** to skip the Keyboard selection in case the **Language** option is set to a different value other than the default value.
Device name template	Enter a template name to use during the device enrolment process.
Microsoft Software Licence Terms	You can Show or Hide this option only in User-Driven Deployment mode only.
Privacy settings	You can Show or Hide this option only in User-Driven Deployment mode only.
Change account options	You can Show or Hide this option only in User-Driven Deployment mode and when the User account type is Standard type.

Windows Device Management

The administrator can configure the Autopilot feature on a tenant using the new option Windows Device Management. This option makes it easier to integrate with Ivanti Neurons for MDM if the user has an Entra ID environment.

To access this option, **Admin** > **Microsoft Azure** > **Windows Device Management**.

This integration grants permissions to Ivanti Neurons for MDM to manage devices, Autopilot profiles, check Windows device compliance, and validate the Azure tenant.

Related Topics

- TenantLockdown CSP

Creating Entra ID Device Groups

The administrator can create Entra ID Device Groups, as and when needed, from the Entra ID Device Groups section. The Entra ID tenant validation must have been configured under the Device Compliance section to create Entra ID Device Groups.

Procedure

1. Go to **Admin** > **Microsoft Azure** > **Entra ID Device Groups**.
2. The **Entra ID Device Groups** page appears on the screen.
   Click **ADD**.
3. The **Group Settings** page appears on the screen.
   Provide the following details:
   - Group Name
   - Group Description
   - Membership Type
     - Static Device - The administrator will get the list of available static devices on the **Assign Members to Group** window. Select the required devices and click **Save**.
     - Dynamic Device - The administrator has to provide certain criteria from the **Dynamic Query** window.

The new Entra ID Device Group will be created and the administrator can add devices to the newly created group.

> After creating a dynamic group, the devices will be listed under the Devices tab of the specific device group after sometime.

Editing Autopilot Devices

Users can edit the Autopilot devices from the Ivanti Neurons for MDM administrative portal.

Prerequisites

Make sure that the following prerequisites are met:

- IT Admin user should have Azure Global Admin and Intune Admin permissions.
- A user-friendly name can be set only if the user is set.
- The device name cannot be unset once set.

Procedure

1. Log in to the Ivanti Neurons for MDM administrative portal.

2. Go to **Admin** > **Windows** > **Autopilot**. The Autopilot Devices are listed under the Autopilot Devices tab.
3. Click **Edit** (pencil icon). The edit page appears.
4. Edit the following details:
    - **User**
    - **User Friendly Name**
    - **Device Name**
    - **Group Tag**

Click **Save**. The device details are updated.

Deleting Autopilot Devices

Users can delete the Autopilot devices from the Ivanti Neurons for MDM administrative portal.

1. Log in to the Ivanti Neurons for MDM administrative portal.
2. Go to **Admin** > **Windows** > **Autopilot**. The Autopilot Devices are listed under the Autopilot Devices tab.
3. Click **Delete**. The device details are deleted.

12.4.2. Audit Trails on Windows Autopilot Profiles

Audit Trails keeps track of all the activities performed on all entities within Ivanti Neurons for MDM. These activities include adding, deleting, updating new devices, etc.

For more information, see **Audit Trails**.

The admin can perform the following activities using Audit Trails on all Windows devices enrolled in the Autopilot mode:

Autopilot Profiles

- Create
- Edit
- Delete
- Assign the profile to groups

Autopilot Devices

- Upload CSV
- Edit
- Delete

12.4.3. TenantLockdown CSP

The admin can lock all Windows devices to tenants using the TenantLockdown CSP feature. To use this feature, the devices must be enrolled using the Autopilot option. This configuration can be done at the device level.

In the Autopilot Self-deployed and User-driven modes, the admin can lock the devices directly to tenants. This is useful when the devices are lost or stolen. In such cases, even if the device is reset, the user will be forced to connect to the tenant and the local account creation is not supported in Self-deployed mode. But if the account creation has to be prevented in User-driven mode, the admin must enable the **Hide** option in **Change account options** setting during the Autopilot Profile configuration.

The admin can enable the TenantLockdown CSP by creating a Windows Restriction Configuration and selecting the **Require users to connect to the network during device set up (Autopilot profile is required)** option under **Other Restrictions**.

To remove a device from the TenantLockdown CSP, the admin must manually remove the device from the group or change the restrictions.

12.4.4. ADMX (GPO) Browser

Using ADMX (GPO) browser, you can view the GPO settings organised on the basis of the ADMX objects that exist in the tenant. You can search and view the default ADMX objects and also add (upload) custom ADMX files that provide an XML-based structure for defining the display of the GPO settings

To upload custom ADMX object:

1. Select **Admin > ADMX (GPO) Browser**. The **ADMX (GPO) Browser** page is displayed.
2. Click **Append**. The **Append Custom ADMX(GPO) Objects** window is displayed.
3. Click **Choose File** to select the ADMX file to be uploaded.

> Make sure that the ADMX file is a zip file.

4. Click **Append**. A confirmation message is displayed for a successful upload.

> Make sure that the root folder contains the *.admx* extension file after unzipping the zip file.

Searching GPO settings

In the ADMX (GPO) browser, you can search and select a GPO by clicking the relevant component from the GPO hierarchy tree in the left pane. The GPO hierarchy tree represents the path of the policy settings. You can alternatively, search for a specific GPO setting by typing the GPO name or the ADMX file name in the Search field. The details of the selected GPO setting is displayed in the right pane.

12.4.5. Configuring app inventory intervals

You can set Windows 10 application inventory collection intervals for multiple app source type inventories. The intervals are used when Privacy configuration is set to collect all apps from the device .

1. Navigate to **Admin > App Inventory Intervals**.
2. Select the interval (in hours) for collecting the app inventory from the drop down list for the following app source types.
    - **Non App Store Inventory Interval**
    - **App Store Inventory Interval**
    - **System Inventory Interval**
    - **Win32 Inventory Interval**
      The interval options to collect Windows app inventory are between **24** to **48** hours. The default value is **24** hours.

12.4.6. Hardware Inventory

You can enable the collection of hardware information from Windows 10 devices . Hardware Inventory details are retrieved using Bridge.

1. Navigate to **Admin>Hardware Inventory**.
2. Enable the option **Enable the collection of hardware inventory**.
3. In the **Inventory Interval**, select the frequency for collecting the hardware inventory. The following are the available options:
    - **Once a day**(default)
    - **Once a week**
    - **Every 30 days**

When the hardware inventory option is enabled, you can view the hardware details of the device under the **Hardware** tab in the device details page.

12.5. Setup with Microsoft Azure

This section contains the following topics:

- Using Microsoft Azure
- Entra ID Windows 10 Unified Endpoint Management Setup
- Assigning Entra ID UEM app
- Connect Ivanti Neurons for MDM with Entra ID User Source
- Azure Tenant
- Admin > Microsoft Azure > Office 365 App Protection

12.5.1. Using Microsoft Azure

Ivanti Neurons for MDM can be setup with Microsoft Azure for seamless enrollment for your users on their Windows desktop and Tablets devices running on Windows 10. Follow the steps below to configure and connect your instances.

This section contains the following topics:

Setting up Entra ID account

To set up Entra ID:

1. Go to https://azure.microsoft.com/en-in/pricing/purchase-options/ to purchase your Azure account.
2. Use your existing Hotmail or Outlook.com account, or create a new account and register as a new user.
3. Buy an Azure account by using one of the payment options and following the verification steps.
4. Ask Microsoft to Allowlist the Ivanti Neurons for MDM tenant.
5. Use the same Hotmail or Outlook.com account you used in step 2 to login to Entra ID at https://manage.windowsazure.com/https://manage.windowsazure.com/ as an admin.
6. Go to **Domain** tab.
   A default the domain, TestMiBGLRoutlook.onmicrosoft.com, is created for your account and any users created will belong to this domain. If needed you can recreate a custom domain.

Creating Users on Entra ID

To create users on Entra ID:

1. Go to active directory - > **Default Directory - >Users**.
2. Selecting the Add user option → Select New user in your organisation.
3. Enter the username. Click next **(→)**.
   The **User Profile** page is displayed.
4. Add the user information such as, first and last name and the display name.
5. Use the dropdown menu to assign the appropriate role to the user.
6. Generate the temporary password.
   The user will be required to change this password at the first login.

Connecting Entra ID to UEM for Windows 10 Devices

To connect Entra ID to UEM:

1. **Go to Admin > Microsoft Azure > Windows Enrollment And Compliance Using Entra ID.**
2. Complete the UEM setup steps described in the section, **Entra ID Windows 10 Unified Endpoint Management Setup**
3. Complete the **Assigning Entra ID UEM app** setup in the Azure portal.
4. In the Ivanti Neurons for MDM Admin Portal, type the domain name of your Entra ID account, and click Connect Azure portal, and then select the checkbox.
5. After signing in successfully, accept the consent that allows MobileIron AD Tenant Validation APP to verify that your Ivanti Neurons for MDM UEM APP is set up. A message appears indicating a successful connection.

Microsoft Passport for Work for Windows 10 Devices

Microsoft Passport for Work is replaced with Windows Hello for Business. For more Information, see **Windows Hello for Business Configuration**.

Windows device Entra ID enrollment

Prerequisites

Users must be registered in Ivanti Neurons for MDM.

Connect your domain to enroll user on their Windows 10+ devices.

1. Click **Join Entra ID**.
2. Enter username and password.
3. Click **Sign-in**.
4. Accept the EULA.
5. Click **Create PIN**.
    - If you have enabled Microsoft Passport for Work PIN complexity, you are prompted to set up a complex PIN as per the configured policy.
    - Entra ID authenticates the user and downloads a JWT (JSON Web Token) to the device.
    - The device is now enrolled.
    - User is contacted through the device for verification.
6. Enter and confirm a PIN.
7. Click **OK**.

Multi-User Support for Windows devices

Ivanti Neurons for MDM supports multi-user capabilities for the Windows 10 Entra ID enrolled devices. This capability includes pushing some profiles like VPN, WiFi, default email client profiles and Certificates to an individual user and not a device. It also supports distribution of in-house and public apps for the logged-in user. Each time a new Entra ID user logs onto a device,
Ivanti Neurons for MDM evaluates not just the device but also the user. If the user is new, Ivanti Neurons for MDM updates the device for that user. If the user is an existing user on the device then any changes to the device and user settings that need to be updated since their last login are evaluated.

The details of the Entra ID user who is logged into the device are reported in the Ivanti Neurons for MDM Admin portal. When the user logs out of the device and the second user logs into the device, the details of the second user is updated in the device details page.

Setting up Microsoft Store for Business with UEM

Microsoft Store for Business is a portal provided by Microsoft as a part of Azure. Administrators can login to this portal and shop the apps and distribute them to all the managed devices. Ivanti Neurons for MDM can be setup with Microsoft Store for Business to manage applications from within the Ivanti Neurons for MDM admin portal by setting up the following steps.

Step 1: Registering Entra ID application in the Microsoft Azure Portal

1. Open the first browser and log into the Microsoft Azure portal (**https://portal.azure.com/https://portal.azure.com/**).
2. Click **App registrations** on the left pane.

3. Click **+New application registration**.
4. Enter the following information to register MobileIron as an Azure app:
    - **Name**: Enter a name for the MobileIron app. (This field is required with a minimum of 4 characters.)
    - **Application Type**: Select Web app/API.
    - **Sign-on URL**: Enter the URL device users access to sign into MobileIron (required).
5. Click **Create** to add the app and return to the Azure home page.
6. Go to Settings and create a new key.

Step 2: Adding the application as a management tool

1. In Microsoft Store for Business Settings, click Manage.
2. Distribution Settings.
3. In the Add Management tool activate the created application.

Connecting the account in the Admin Portal

1. Go to **Admin > Microsoft Azure > Microsoft Store for Business**.
2. Under Step 1, **Register Entra ID application**, select the checkbox **Yes, I completed this step**.
3. Under Step 2, **Add Management Tool**, select the checkbox **Yes, I completed this step**.
4. Under Step 3, Connect Account, update the following fields:
    - Entra ID Domain
    - Application Identifier
    - Application key
    - Sync Interval (hours)
5. Click **Connect**. You will see a confirmation message that the MobileIron store for business is successfully setup.
6. Click **Sync App**. When successfully synced, the status displays as **Applications synced successfully**.

When the Microsoft Store for app is pushed to the device, the app details are available in the under **Installed apps** tab in the device details. Each Microsoft Store for business app reported from device, can be identified as **Microsoft Store for Business** in the **Source** column.

12.5.2. Entra ID Windows 10 Unified Endpoint Management Setup

To setup Windows 10 Unified Endpoint Management (UEM):

1. Login at https://portal.azure.com/ as admin user, and select Entra ID.
2. Select "Mobility (MDM and MAM)" in the left panel and then click **+ Add Application**.



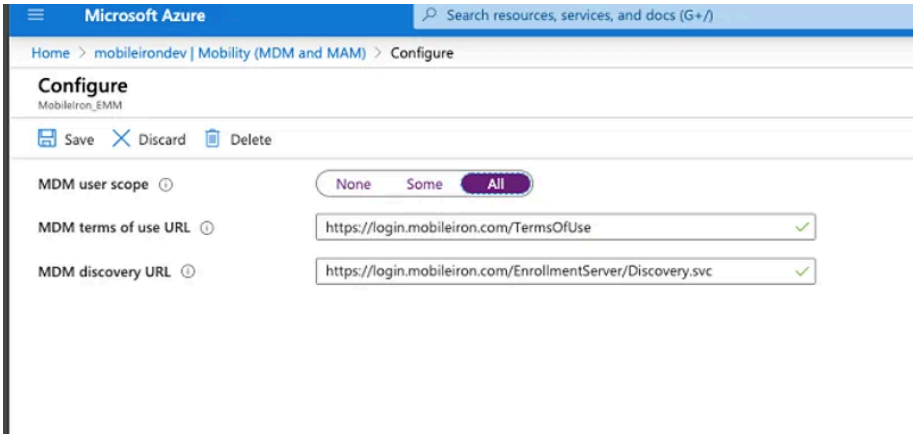
3. Select MobileIron_UEM application from App gallery and click **Add**.



12.5.3. Assigning Entra ID UEM app

To complete the assign user setup:

1. Click the MobileIron UEM app you created in Step 2 in **Entra ID Windows 10 Unified Endpoint Management Setup**
2. Under MDM user scope, assign it to your customised user groups or select **All**.



12.5.4. Connect Ivanti Neurons for MDM with Entra ID User Source

To work with Entra ID (Entra ID), you must configure Ivanti Neurons for MDM with details about your Microsoft Entra ID account. You require an existing and configured Microsoft Entra ID account. This solution requires no on-premise connector or LDAP.

This section contains the following topics:

- Use cases
- Using Entra ID
- Entra ID Settings

Use cases

You can connect Ivanti Neurons for MDM with Entra ID for one of the following use cases:

- Work with Microsoft Office 365
- Set up Microsoft Entra ID, Microsoft ADFS, or another SAML 2.0 Identity Provider (IdP) for user authentication
- Set up Microsoft Entra ID as your user source
- Sync users from Microsoft Entra ID and get started. All users and groups in your Entra ID domain will be synced to your Ivanti Neurons for MDM instance
  A notification is displayed in the **Notifications** page if there is an error in Entra ID sync due to the following reasons:
  - Entra ID service is unreachable
  - All user attributes are not synchronised with Entra ID
  - Some user attributes are not synchronised with Entra ID
- Environments with multiple IdPs are currently not supported.
- If you are not using Microsoft Entra ID as your user source, you can use Local Accounts or source users from LDAP. This requires setting up an Ivanti Neurons for MDM connector to access LDAP resources on-premise.
- Using Microsoft Entra ID only for user authentication and using an on-premise LDAP for user directory is currently not supported.

Using Entra ID

To use Entra ID, set up your Identity Provider for user authentication in one of the following methods:

- To use Microsoft Entra ID for both user source and user authentication, setup Entra ID as your IdP. Go to **Admin > Identity > Ivanti Neurons for MDM IdP Setup** and select **Entra ID** from the menu.
- To use Microsoft Entra ID for user source and to use ADFS for user authentication, setup ADFS as your IdP. Go to **Admin > Identity > On-Prem IdP Setup** and select ADFS from the menu.
- To use a SAML 2.0 IdP other than Entra ID and to use ADFS for user authentication, go to **Admin > Identity > Generic IdP Setup** and follow the instructions on the page.

For more information, see Configure Identity Provider.

Entra ID Settings

This topic helps you configure the Entra ID settings.

Procedure

1. Go to **Admin > Microsoft Azure > Entra ID User Source**.
2. Specify the following details:
    1. **Entra ID Name**.
    2. **Sync Interval** - Modify the frequency that Ivanti Neurons for MDM synchronises user data from your Entra ID.
    3. **Enable this Entra ID** - Use this option to enable or disable Entra ID instance.
    4. Select **Automatically invite users imported from Entra ID** - Manage whether users imported from Entra ID to Ivanti Neurons for MDM are automatically invited to register via email.
    5. Select **Managed Apple ID** - Choose to sync Managed Apple ID for the Entra ID users.
        - **None**
        - **Pattern** -
            - **User email address**
            - **userUPN**
            - (Optional) select the Include "appleid" subdomain option to avoid conflict with existing Apple IDs.
    6. (Optional) Click **Add Custom Attribute** - Specify custom user attributes from your directory service that you want to apply to device management. Each attribute can then be referenced by $ in configuration fields that support variables. Use of this option requires consistent implementation of custom attributes across Entra ID servers. If an Entra ID server included in your implementation does not use this attribute, then features dependent on this attribute might not work as expected.

Click **Save** after modifying the Entra ID settings.

12.5.5. Azure Tenant

This section contains the following topics:

- Requirements
- Apply the Intune licence to device users
- Adding MobileIron as a compliance partner
- Creating a conditional access policy in Microsoft Endpoint Manager
- Connecting Microsoft Azure to Ivanti Neurons for MDM
- Creating a partner device compliance policy
- Device status reporting from Ivanti Neurons for MDM to Azure
- De-provisioning of the Azure tenant

12.5.5.1. Azure Tenant Requirements

This section describes setting up Ivanti Neurons for MDM with Microsoft Azure Tenant.

Requirements

Microsoft

Ivanti Neurons for MDM customers must have a valid subscription to Microsoft Intune and assign a Microsoft Intune license to device users.

MobileIron

- Ivanti Neurons for MDM - Ivanti Neurons for MDM version 75 through the latest version as supported by MobileIron.
- Additional licensing - Azure Device Compliance is a Premium offering and is available to **Secure UEM Premium** and Platinum customers. A Platinum licence suffices for existing customers.
- Go for iOS (client) or Go for Android (client) version 75.0 through the latest version as supported by MobileIron.

Multiple Ivanti Neurons for MDMs support

If you have multiple Ivanti Neurons for MDMs connected to the same Azure tenant, disconnect from all Ivanti Neurons for MDMs or disable compliance policy for Entra ID compliance integration from a specific (single) Ivanti Neurons for MDM so that it does not upload device data to Azure

> Be sure to disable the compliance policy prior to disconnecting Ivanti Neurons for MDM.

Ivanti Neurons for MDM administrator's process

The process from the Ivanti Neurons for MDM administrator's perspective:

1. Administrator applies Intune licences to device users. See **Apply the Intune licence to device users**.
2. Administrator logs into Azure Portal.
3. Administrator adds MobileIron as an Azure compliance partner. See **Adding MobileIron as a compliance partner**.
4. Administrator creates the Conditional Access policy for the apps. See **Creating a conditional access policy in Microsoft Endpoint Manager**.
5. Administrator sets up the connection between MobileIron and Azure. See **Connecting Microsoft Azure to Ivanti Neurons for MDM**.
6. Administrator creates the device compliance policy in Ivanti Neurons for MDM. See **Creating a partner device compliance policy**.
7. The Conditional Access policy goes into effect. Depending upon whether the device is compliant or not, the access to the app(s) is granted or denied.

> Ivanti recommends the administrator run tests on each Microsoft app.

12.5.5.2. Apply the Intune licence to device users

- Do not use this feature if:
  - you are changing users or administering situations where users are likely to change
  - the device is owned by multiple users
- Ivanti recommends you do not perform Assign to User, and do not distribute the device compliance configuration to multi-user devices such as:
  - devices with Secure Sign-In WebClip
  - shared iPad devices
  - Android Kiosk mode devices

Ivanti Neurons for MDM license requirements

Device Compliance is a Premium offering and is available to Secure UEM Premium and Platinum customers. For existing customers, a Platinum licence suffices.

Assign bulk licences to device users

To bulk assign licences to existing device users:

Group based assignment

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

PowerShell based assignment

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. Adding MobileIron as a compliance partner

Prerequisites

- installed a Microsoft Intune licence. See **Apply the Intune licence to device users**.
- users created in Microsoft Azure
- groups created in Microsoft Azure

Procedure

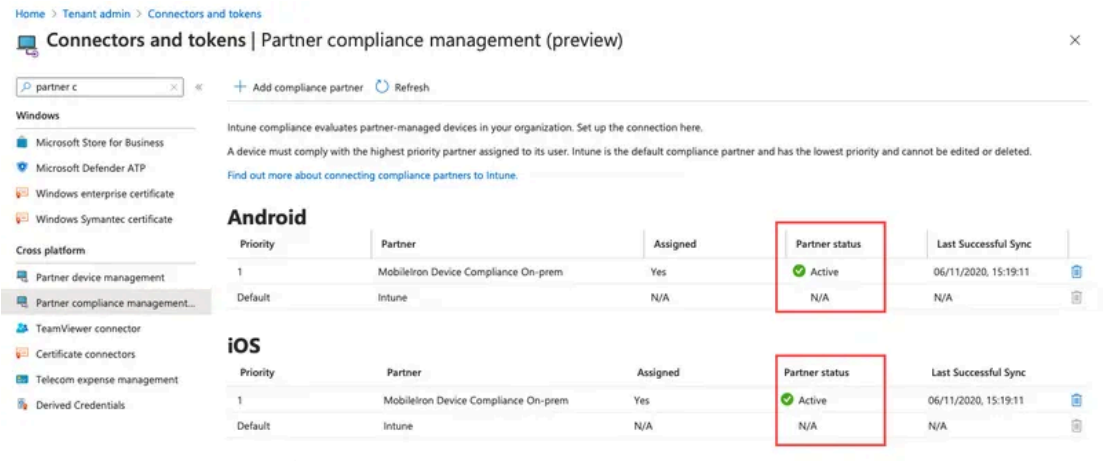
1. Login into: **https://endpoint.microsoft.com**.
2. In the left panel of the Microsoft Endpoint Manager admin centre page, click on Tenant Administrator. Click Connectors and Tokens > Partner Compliance Management.

3. To the right of the Search field, click + Add compliance partner.

4. In the Basics tab, select MobileIron Device Compliance Cloud from the drop-down of the Compliance partner field.

5. In the Platform field, select iOS or Android and then click Next.
6. Click the Assignments tab. In the Assign to drop-down, select the user/group of device users the compliance status is for. Select the user/group that has the licence.

7. Select Next.
8. Click Create. The new compliance partner appears on the Partner compliance management page.



12.5.5.4. Creating a conditional access policy in Microsoft Endpoint Manager

Procedure

1. Log in to Microsoft Endpoint Manager **https://endpoint.microsoft.com**.
2. In the Microsoft Endpoint Manager admin centre page, go to Home > Endpoint Security > Conditional Access.
3. Click Policies and then click + New Policy.



4. Enter the Name of the conditional access policy.



5. In Assignments, click to assign the policy to users and groups.



6. Click Cloud apps or actions and then click Select. Search for and select the apps required to be protected.



7. Click Conditions and then click Device Platform. Select the appropriate device platforms.



8. In the New conditional access policy page > Access controls, click Grant and make the access and block selections.

9. To enable the new policy, click On.



10. Click Create.

12.5.5.5. Connecting Microsoft Azure to Ivanti Neurons for MDM

Procedure

1. Log in to Ivanti Neurons for MDM and go to **Admin** > **Microsoft Azure**.
2. In the left navigational pane, click **Microsoft Azure** > **Device Compliance**.
3. Under the Connect Account section, provide the following details:
    - **Azure Tenant ID** - Find in your Microsoft Azure instance.
    - **Enrollment URL (Optional)** - If the device is not MDM enrolled, device users will be pointed to this URL for enrollment. When configuring, use HTTPS format. If you host a page in your organisation to redirect your device users for Remediation information, add that link here.
    - **Remediation URL (Optional)** - If the device is not in compliance, device users will be pointed to this URL for remediation. When configuring, use HTTPS format. If you host a page in your organisation to redirect your device users for Remediation information, add that link here.
4. Click **Connect Account**. The Azure Tenant Validation dialog box opens.

> Tenants currently connected to Azure and wishing to add device compliance for macOS devices need to disconnect the account and then re-establish the connection.

5. In the Azure Tenant Validation dialog, click the **link** present in Step 1.
6. **Log in**.
7. Review the permissions and then click **Accept**.

> If you log in and the page prompts you to log in again, close the browser tab/ window.

8. Return to Ivanti Neurons for MDM. In the Connect Azure Account dialogue box, select the **I have provided the consent** check box. Click **Confirm**.

- To edit the account, click **Edit Account**.
- To disconnect the account, click **Disconnect Account**. For additional instructions, see De-provisioning of the Azure tenant.
- All activity of adding, editing and deactivating an account are recorded in the Logs.

12.5.5.6. Creating a partner device compliance policy

Create a partner device compliance policy in Ivanti Neurons for MDM and apply the desired label. The partner compliance policy reports the device compliance status to Azure or BeyondCorp for conditional access.

Applicable to

- iOS
- Android
- Windows

Prerequisites

You must have an Azure Tenant ID or a Google BeyondCorp ID set up. For more information about Azure Partner Device Compliance, see **Connecting Microsoft Azure to Ivanti Neurons for MDM**.



Procedure

1. Log in to the Ivanti Neurons for MDM, go to **Configurations**.
2. Click **Add** and search for the **Partner Device Compliance** configuration.
3. Enter the following details on the **Create Partner Device Compliance Configuration** page:

Item	Description
Name	Enter a name.
+ Add Description	Enter an explanation.
Choose Partner	Select **Microsoft Azure Compliance**. or **Google BeyondCorp Compliance - Beta**.
Configuration Setup Report Compliance Status to Azure for iOS, macOS, and Android devices	Toggled ON by default. If you do not see this field, you need to set up your Azure Tenant ID. If the Report Compliance Status for iOS, macOS, and Android devices option is enabled, and the compliance policy is applied to the client, the client will display "Microsoft 365 Access" in the devices under Settings. The compliance status of the device is reported when: • device is out of compliance • the device is compliant • the device returns to compliance • 24 hours passes. If there is no change in the status, a report is sent once a week / every seven days.
Report Compliance Status to Google BeyondCorp for iOS, macOS and Android devices	Toggled ON by default. The compliance status of the device is reported when: • device is out of compliance • the device is compliant • the device returns to compliance • 24 hours passes. If there is no change in the status, a report is sent after every 24 hours.

4. Click **Next**.
5. **Enable this configuration** is selected by default.
6. Select a distribution level for the configuration. For more information about configuration distribution, see **Adding a configuration**.
7. Click **Done**.

12.5.5.7. Device status reporting from Ivanti Neurons for MDM to Azure

For the following cases, Ivanti Neurons for MDM reports device inventory and compliance status.

- On-device compliance state change
- On-device inventory change
- Once a week, Ivanti Neurons for MDM reports compliance and inventory status

Depending on the action chosen in the compliance policy, the following device status will be sent:

Action **(most restrictive one applies)**	**What Ivanti Neurons for MDM sends**
Block Email, AppConnect Apps, Quarantine	Device Non-compliant
Send Alert	Compliant to Azure
Retire device	Device data removed from Azure platform

Device Details page

To view the Azure information about the device, go to the Device Details page. The description of the fields and their possible values:

Field	Description
Azure Device Identifier	The device ID reported by Microsoft to the iOS or Android device. For example: 007c8232-9489-4074-9b35-345b16f0a72d. Ivanti Neurons for MDM receives this device ID as device users are required to register to Microsoft Authenticator application to use this feature. If unable to retrieve the Device ID, this field is left blank.
Azure Device Compliance Status	Lists the device's compliance status in Azure. Possible values: • In-progress • Successful • Failed
Azure Client Status Code	Indicates whether device is connected to Azure. Possible values: • Success - Able to retrieve device ID. • Internal_Error - An unrecoverable error occurred either within the client or on the server side. • Workplace_Join_Required - Registration of device required. Device user can mitigate this status. • Interaction_Required - An interactive log-in is required. Device user can mitigate this status. • Server_Declined_Scopes - Some scopes were not granted access to. • Server_Protection_Policies_Required - The requested resource is protected by an Intune Conditional Access policy. • User_Canceled -The device user cancelled the web Auth session by tapping the "Done" or "Cancel" button in the web browser. • Account_logged_out - Account logged out.
Azure Device Compliance Report Time	The time Ivanti Neurons for MDM reported the device compliance status to Microsoft Intune. A blank field indicates one of the following: • that feature is disabled • Ivanti Neurons for MDM received the data and has yet to call the Microsoft API • there is an error such as user_Cancelled or Internal Error

12.5.5.8. De-provisioning of the Azure tenant

If multiple Ivanti Neurons for MDMs are enabled to use the same Azure tenant, de-provision from all Ivanti Neurons for MDMs. If a single Ivanti Neurons for MDM needs to stop using Azure, you can disable the partner compliance policy for that Ivanti Neurons for MDM only.

If the administrator performs a disconnect on Ivanti Neurons for MDM, then Ivanti Neurons for MDM stops reporting the device inventory and compliance status to Azure.

Perquisites

- make sure all the devices as unmanaged
- make sure all the devices as non-compliant

Procedure

Microsoft

1. Log in to Microsoft Azure.
2. Go to Intune > Conditional Access. Make sure the conditional access policy is disabled.

Ivanti Neurons for MDM

1. Log in to Ivanti Neurons for MDM and go to Admin.
2. In the left navigational pane, click Microsoft Azure > Device Compliance for iOS & Android.
3. Click on Disconnect Account.



4. Click Yes.

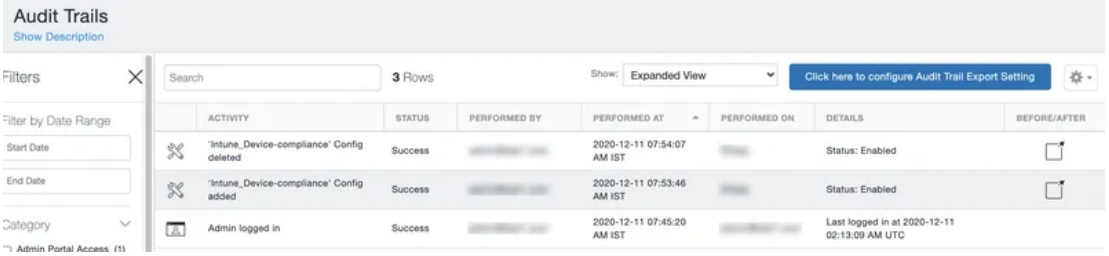
Retiring a device from Azure

Upon device retirement, Ivanti Neurons for MDM reports to Azure that the device is no longer under management and is non-compliant.

Azure deletes the retired device entry after 90 days.

Azure account activity recorded in the logs

All activity is recorded in the Logs.



12.5.6. Admin > Microsoft Azure > Office 365 App Protection

Licence: Gold

You can set up Office 365 App Protection policies to help protect your company's data. The policies enforce Data Loss Prevention (DLP) controls for Microsoft Office 365 apps using Microsoft Graph APIs. Some of these Graph APIs allow administrators to enforce app protection for native iOSand Androidapps that leverage the Graph SDK.

Use this feature to enforce policies such as:

- Prevent users printing from Office 365 apps.
- Preventing outbound data sharing from Office 365 apps.
- Enforce PIN for Office 365 apps.
- Disable Contacts sync from Office 365 apps.

Prerequisites for using Office 365 App Protection

Before you can use Office 365 App Protection, you must have:

- A valid MobileIron licence.
- Office 365 App Protection Feature enabled in Ivanti Neurons for MDM
- Intune subscription or an Microsoft EMS subscription that includes Intune.
    - Each use to which the policy is applied to requires a licence, however to enable and test the integration requires only a single licence.
- A valid Office Enterprise or Business subscription with access to Office 365 apps on a mobile device.
- One or more Office 365 apps.
- Synced your Active Directory users to your Entra ID.
- One Drive for Business installed on devices to protect data on Word, Excel, and PowerPoint. This is not mandatory.
- Access to Microsoft Azure portal (**https://portal.azure.com/**) to configure intune app protection policies.
- Intune Company Portal app installed on Android devices.
  Device users are not required to sign in, but this app must be installed on the device to protect data on device. Protection will be applicable when the user signs in to the app.

Registering MobileIron as an Azure app

This topic describes how to register and store your Azure tenant credentials with Ivanti Neurons for MDM software and to remotely manage app protection policies in the Microsoft Azure cloud for Android and iOS Office 365 apps. Though not necessary, you may open two browsers to perform the steps in the following procedures. Use the first browser to log into the Microsoft Azure portal. Use the second browser to log into the Ivanti Neurons for MDM Admin portal.

Procedure for Microsoft Azure Portal

> Microsoft may change the Azure portal user interface from time to time. These instructions assume that you are familiar with the Microsoft Azure Portal and can make necessary adjustments as you register MobileIron as an Azure app.

1. Open the first browser and log into the Microsoft Azure portal (**https://portal.azure.com/**).
2. Click **App registrations** on the left pane.
3. Click **+New application registration**.
4. Enter the following information to register MobileIron as an Azure app.
    - **Name:** Enter a name for the MobileIron app. (This field is required with a minimum of 4 characters.)
    - **Application Type:** Select Web app / API.
    - **Sign-on URL:** Enter the URL device users access to sign into MobileIron (required).

Click **Create** on the bottom of the pane to add the app and return to the Azure home page.

6. Click the newly created MobileIron app in the Azure home page.
7. Return to the Azure home page to assign permissions to the MobileIron Azure app.
8. To set required API permissions for the newly created MobileIron app, click the app name under App Registrations.
9. Click **API permissions** > **Add a permission**.
10. In the **Microsoft Graph > Delegated Permissions > Device Management Apps** section, select the **DeviceManagementApps.Read.All** permission and click **Save**. By default, the user. Read permission is enabled for the app.
11. To grant access, click **Grant admin consent for MobileIron**.
12. Perform the following procedure for Ivanti Neurons for MDM admin portal.

Procedure for Ivanti Neurons for MDM Admin Portal

1. Open the second browser and log into the Ivanti Neurons for MDM admin portal.
2. Go to **Admin > Microsoft Azure > Office 365 App Protection**.
3. Paste **Application ID** in the Ivanti Neurons for MDM admin portal.
4. **Procedure**
    1. Go to the Azure portal.
    2. Select the MobileIron app > **Properties**.
    3. Copy the **Application ID**.
    4. Return to **Admin > Microsoft Azure > Office 365 App Protection** on the Admin Portal.
    5. Paste it into the **Application ID** field.

Paste the **Application Secret** (Client Secret) in the Ivanti Neurons for MDM admin portal.

5. **Procedure**
    1. Go to the Azure portal.
    2. Select the MobileIron app.
    3. Click **Keys** and enter a name in **Key description** and select an expiration time-period in **Duration**.
    4. Click **Save** and copy the **Key** value.
    5. Return to **Admin > Microsoft Azure > Office 365 App Protection** on the Admin Portal.

6. Paste it into the **Application Secret** (Client Secret) field.

Paste the **Tenant ID** in the Ivanti Neurons for MDM admin portal.

6. **Procedure**
    1. Go to the Azure portal.
    2. Click Entra ID in the left pane then click Properties.
    3. Copy the Directory ID.
    4. Return to **Admin > Microsoft Azure > Office 365 App Protection** on the Admin Portal.
    5. Paste it into the **Tenant ID** field.

Enter your Intune admin **Username** and **Password**.

- The Azure account should have either global admin rights or limited admin + Intune service administration rights.
- Ivanti recommends creating a local Azure account with just the Intune service administration rights. User accounts that are federated to an identity provider are not supported by Microsoft for authentication with the Graph API's.

Click **Authenticate and Save**.
If the date submitted is incorrect, an error message is displayed.

Policies for Office 365 App Protection

After configuring Microsoft Graph credentials, go to **Apps > Office 365 App Protection** to add new Office 365 App Protection policies for iOS or Android devices for different user groups.

The policies are listed on the **Apps > Office 365 App Protection** page, under the **App Policies** tab. This list of policies provides tabular details such as the updated time stamp, platform, apps assigned, and user groups deployed.

Adding an Office 365 App Protection policy for iOS devices

Procedure

1. Go to **Apps > Office 365 App Protection**.
2. Click **App Policies > + Add**.
3. Enter a **Name** and an optional **Description** for the policy.
4. Under Choose OS, click **iOS**.
5. Under **Data Relocation**, select from the following settings and options:
    - Prevent iTunes and iCloud backups
    - Allow app to transfer data to other apps - All apps (default), Policy managed apps, None
    - Allow app to receive data from other apps - All apps (default), Policy managed apps, None
    - Prevent "Save As"
    - Restrict cut, copy and paste with other apps - Any app (default), Blocked, Policy managed apps, Policy managed with paste in
    - Restrict web content to display in the Managed Browser
    - Encrypt app data - When device is locked (default), When device is locked and there are open files, After device restart, Use device settings

- Disable contact sync
- Disable printing

6. Under **Access**, select from the following settings and options:
   - Require PIN for access
   - Number of attempts before PIN resets (default 5)
   - Allow simple PIN
   - PIN length (default 4)
   - Allow Fingerprint instead of PIN (iOS 8+)
   - Disable app PIN when device PIN is managed
   - Require corporate credentials for access
   - Block managed apps from running on jailbroken or rooted devices
   - Recheck access requirements after (Minutes)
     - Timeout - Must be a value between 1 and 65535 (default 30)
     - Offline - grace period Must be a value between 1 and 65535 (default 720)
     - Offline interval (days) before app data is wiped - Must be a value between 1 and 65535 (default 90)

   Require minimum iOS operating system

   - Require minimum iOS operating system (Warning only)
   - Require minimum app version
   - Require minimum app version (Warning only)
   - Require minimum Intune app protection policy SDK version

Click **Next**.

8. Select and assign apps that this policy will apply to.
9. Click **Next**.
10. Select user groups that this policy will apply to.
11. Click **Done**.

Adding an Office 365 App Protection policy for Android devices

Procedure

1. Go to **Apps > Office 365 App Protection**.
2. Click **App Policies > + Add**.
3. Enter a **Name** and an optional **Description** for the policy.
4. Under Choose OS, click **Android**.
5. Under **Data Relocation**, select from the following settings and options:
   - Prevent Android backups
   - Allow app to transfer data to other apps - All apps (default), Policy managed apps, None
   - Allow app to receive data from other apps - All apps (default), Policy managed apps, None

- Prevent "Save As"
- Restrict cut, copy and paste with other apps - Any app (default), Blocked, Policy managed apps, Policy managed with paste in
- Restrict web content to display in the Managed Browser
- Encrypt app data
- Disable app encryption when device encryption is enabled
- Disable contact sync
- Disable printing

6. Under **Access**, select from the following settings and options:
   - Require PIN for access
   - Number of attempts before PIN resets (default 5)
   - Allow simple PIN
   - PIN length (default 4)
   - Allow Fingerprint instead of PIN (Android 6+)
   - Disable app PIN when device PIN is managed
   - Require corporate credentials for access
   - Block managed apps from running on jailbroken or rooted devices
   - Recheck access requirements after (Minutes)
     - Timeout - Must be a value between 1 and 65535 (default 30)
     - Offline - grace period Must be a value between 1 and 65535 (default 720)
     - Offline interval (days) before app data is wiped - Must be a value between 1 and 65535 (default 90)
   - Block screen capture and Android assistant
   - Require minimum Android operating system
   - Require minimum Android operating system (Warning only)
   - Require minimum app version
   - Require minimum app version (Warning only)
   - Require minimum Intune app protection policy SDK version
7. Click **Next**.
8. Select the apps that this policy will apply to.
9. Click **Next**.
10. Select the user groups that this policy will apply to.
11. Click **Done**.

Modifying an Office 365 App Protection policy

Procedure

1. Go to **Apps > Office 365 App Protection**.
2. Click **App Policies**.

3. Click the name of the policy you want to modify.
4. On the policy details page, click **Edit**.
5. Modify the policy configuration settings.
6. Click **Next**.
7. Modify the list of apps that this policy will apply to.
8. Click **Next**.
9. Modify the user groups that this policy will apply to.
10. Click **Done**.

Deleting an Office 365 App Protection policy

Procedure

1. Go to **Apps > Office 365 App Protection**.
2. Click **App Policies**.
3. Under the **Actions** column, click the remove icon against the policy name you want to delete.
4. Click **Yes** to confirm.

Office 365 App Configurations

Go to the **Apps > Office 365 App Protection** page, under the **App Configuration** tab to add, modify, or delete Office 365 App Configurations for different user groups. In these app configurations, administrators can add a list of key-value pairs. and assign the configurations to one or more Office 365 apps. The App Configuration tab lists configurations with tabular details such as the updated time stamp, apps assigned, and deployment status.

Adding an Office 365 App Configuration

Procedure

1. Go to **Apps > Office 365 App Protection**.
2. Click **App Configuration > + Add**.
3. Enter a **Name** and an optional **Description** for the configuration.
4. Enter the key-value pairs.
5. Click **Next**.
6. Select the apps that this configuration will apply to.
7. Click **Next**.
8. Select the user groups that this configuration will apply to.
9. Click **Done**.

Modifying an Office 365 App Configuration

Procedure

1. Go to **Apps > Office 365 App Protection**.
2. Click **App Configuration**.

3. Click the name of the configuration you want to modify.
4. On the configuration details page, click **Edit.**
5. Alternatively, click either **App Distribution** or **User Group Distribution** tabs. Click **Edit** to modify only those settings and click **Save**.
6. Modify the configuration settings.
7. Click **Next**.
8. Modify the list of apps that this configuration will apply to.
9. Click **Next**.
10. Modify the user groups that this configuration will apply to.
11. Click **Done**.

Deleting an Office 365 App Configuration

Procedure

1. Go to **Apps > Office 365 App Protection**.
2. Click **App Configuration**.
3. Under the **Actions** column, click the remove icon against the configuration name you want to delete.
4. Click **Yes** to confirm.

Out of compliance users with Office 365 apps

Administrators can review the list of users and their devices due to non-compliance. Use this page to wipe any Office 365 apps on such flagged devices.

Wiping Office 365 apps

Procedure

1. Go to **Apps > Office 365 App Protection**.
2. Click **Out of Compliance Users**.
3. Perform one of the following actions:
   - Select the users from the list and click **Wipe Office 365 Apps**.
   - Click the name of the user to display the list of devices that have out of compliance apps. Under the **Action** column, click **Wipe Office 365 Apps** icon against a specific device.
   - Click the name of the user to display the list of devices that have out of compliance apps. Click the name of a specific device to view the apps listed with bundle IDs/package names and the flagged reasons. Click **Wipe Office 365 Apps**.
4. Click **Yes** to confirm the action.

Alternatively, perform the following steps:

1. Go to **Users**.
2. Click the name of the user to display the user details page.
3. Click **Action > Wipe Office 365 Apps**.
4. Select the devices from which the Office 365 apps need to be wiped.

5. Click **OK** to confirm the action.

Cancelling wipe requests of Office 365 apps

Procedure

1. Go to **Users**.
2. Click the name of the user to display the user details page.
3. Click the **Office 365 Protection** tab.
4. From the **Select Report Type** drop-down box, select the **Wipe Requests** report to display the corresponding information.
5. Select the devices from which the wipe requests need to be cancelled. Only devices with the Wipe Pending status can be selected.
6. Click **Cancel Wipe**.
7. Click **OK** to confirm the action.

App reports for users with Office 365 App Protection

Administrators can select one of the following reports to review the list of users with Office 365 App Protection and related information:

- App Policy Report
- App Configuration Report
- Wipe Requests

Information in the App Reports includes Bundle ID/Package Name, Device Name, Device Type, Policies or Configurations (deployed to the device), Status (Synced, Synced but out of date, or Not Synced), and the time of Last Check-in. Information from the App Reports can be exported to a CSV file for later reference or analysis.

Information in the Wipe Requests report includes Display Name, User Name, Device Name, Device Type, and Wipe Status (Wipe Pending or Wipe Complete).

Perform the following steps to view one of the reports:

1. Go to **Users**.
2. Click the name of the user to display the user details page.
3. Click the **Office 365 Protection** tab.
4. From the **Select Report Type** drop-down box, select one of the reports to display the corresponding information.
5. (Optional) From the Wipe Requests report page, select the devices from which the wipe requests need to be cancelled and click **Cancel Wipe**. Only devices with the Wipe Pending status can be selected.
6. (Optional) Click **Export to CSV** to download the report contents in a CSV file for later reference or analysis.

12.6. Connect with Google Apps

This section contains the following topics:

- Managed Google Play Accounts (Android Enterprise Accounts)
- Android device registration
- Android Management API
- Google Apps API
- Admin - Android Enterprise

12.6.1. Managed Google Play Accounts (Android Enterprise Accounts)

Licence: Silver

Managed Google Play Accounts are required to enable use and configuration of Android Enterprise devices. You no longer have to use Google Apps Directory Sync (GADS) or use Google accounts to register devices.

Important: If you have already set up Android Enterprise, you must first retire those devices to be able to use this feature.

Configuring Android Enterprise using managed Google Play Account

Procedure

1. Log in to the Ivanti Neurons for MDM portal.
2. Go to **Admin > Google > Android Enterprise**.
3. Under Managed Google Play Account, click Authorise Google to display the Google Play for Work page.
4. Enter your **Google Play Account Email ID**.
5. Click **Get Started**.
6. Accept the Android Enterprise agreement.
7. Click **Confirm**.
8. Click **Complete Registration**.
   The **Android Enterprise Configured** section displays the following information:
   - **Status**
   - **Admin Email**
   - **Enterprise Type**
   - **Google Enterprise ID**

When Android Enterprise is set up using managed Google Play Accounts, there is a limitation on the number of devices enrolled per user. To overcome this limitation, while creating a new user, select the **Android Enterprise device Account** option to enable Android Enterprise work managed device enrolments attached to this account to be automatically assigned a Google Device Account.

Device Accounts are intended for COSU (single-use) deployments (e.g., with Kiosk mode). Users with device accounts may have limited access to Google Play.

Occasionally, a managed Google Play account or its token expires for a variety of reasons like authentication token expiry or the account or enterprise being deleted. In such scenarios, Google Play services will notify the client with a broadcast action that will trigger the client to reprovision the device by removing the existing account and adding an account with a new token obtained from the UEM server.

In case, account re-provisioning fails either because the old account could not be removed or due to many attempts at re-provisioning, user will be notified to start over again by retiring the client or factory resetting the device as the case may be depending on whether device is in work profile mode or in managed device mode, respectively.

Migrate existing Managed Google Play Account to Managed Google Domain Account (BTE)

This feature enables migration of Android Enterprise accounts and devices from **Managed Google Play Account** to **Managed Google Domain Account**.

The migration consists of:

- Account Upgrade
- Device Migration

Prerequisites

- Devices must be enrolled in either Work Managed Device or Work Profile mode; devices enrolled in Work Profile on Company-Owned Device (WPCOD) mode must be running Android 12 or later.
- Devices are assigned valid corporate or business email IDs.

> If the device is assigned to non-corporate email ID, administrator must reassign a valid corporate email ID for the device to be eligible for migration.

Upgrade Android Enterprise Account

Upgrade the Android Enterprise account from Managed Google Play Account to Managed Google Domain Account.

Procedure

1. Go to Admin > Google > Android Enterprise.
2. Click **Upgrade Account**.
3. Sign in using a valid corporate or business email ID.
4. Complete the upgrade process.
5. Refresh the page.

Apply Device Migration Configuration

Procedure

1. Navigate to Configurations >> +Add.
2. Select the **Android Enterprise: Device Migration from Managed Google Play to Managed Google Account** configuration > **Edit** > **Next** > **All Devices or Custom** > **Slow Rollout Distribution** – By default, the **Manual Rollout** option is selected > Choose from drop down **Custom % of devices in selection summary (slow rollout)** or **All devices in selection summary**.
3. Click **Done**.

Complete Device Migration

Procedure

1. On the device, tap **Continue** when prompted for "Add your work account".
2. Verify the **corporate email ID**.
3. Enter the password.

4. Complete **two-factor authentication (2FA)**, if available.
5. Complete Account Setup process.

Verify Migration

On the Device

1. Open **Google Play Store**.
2. Confirm the account type has changed from Work account to Corporate domain account.

In the Admin Console

- To view the **Android Enterprise: Device Migration from Managed Google Play to Managed Google Account** configuration status, navigate to **Devices** > **Devices** > **Device Details** > **Configuration** > **Android Enterprise: Device Migration from Managed Google Play to Managed Google Account)**. Ensure the configuration status is in Installed state.

Monitoring Migration Status

Administrators can track migration (**Migrated to Managed Google Account**) progress using:

- **Device Details** – view migration status per device
- **Advanced Search** – filter migrated and non-migrated devices
- **Device Groups** – grouping migrated and non-migrated devices

These options help identify devices that require further action.

New Enrollment with Managed Google Domain Account (BTE)

Android Enterprise can be configured using **Managed Google Domain Account** with or without Google Authentication.

Procedure

1. Log in to the portal.
2. Go to Admin > Google > Android Enterprise.
3. Under **Managed Google Play Account**, click **Authorise**.
4. Enter your **Corporate** or **Business Email ID** and click **Next**.
5. Select **Create a new binding with..** in the **Select a binding option** page.
6. Click **Confirm**. The **Skip** and **Enable** options will be displayed.

- **Skip**- To continue without authentication
- **Enable** – To continue with authentication

The Android Enterprise section displays the following information:

- **Status**: Displays the connection status.
- **Admin Email**: Displays the Corporate or Business email ID.
- **Enterprise Type**: Displays the enterprise type.
- **Google Authentication Settings**: Displays No/Yes based on authentication requirement.
- **Google Enterprise ID**: Displays a unique Google enterprise ID.

- **Enterprise Name**: Displays the enterprise name.

12.6.2. Android device registration

During an Android device registration, if you require phone permissions from users which is required to report IMEI, phone number and other phone identifiers to complete registration, you can configure this option. When configured, the device users will be prompted to grant permission to allow Go client to access device identifiers.

> This configuration is applicable only for new registrations of all Android devices with Android version above 6.0.

1. Select **Admin > Google > Registration**.
2. Select **Require Android device identifiers during registration (Work Profile & Device Admin)**.
3. Click **Save**.

For more information about Lost Mode, see **Managing Android devices in Lost Mode**

12.6.3. Android Management API

Android Management API (AMAPI) is the Cloud Platform API from Google that integrates Google Android UEM functions to Ivanti Neurons for MDM. In the Android Enterprise setup, you can enable the Android Management API framework to manage Android Enterprise devices without the need to have a client app to be installed on the devices for device management. Currently, Go app is not supported to be pushed to the device for other features such as MTD, etc.

When you have an Android Enterprise account configured in your setup, you will be able to enable and use the Android Management API framework. After enabling, you can:

- Add an enrollment profile to use the QR code for device enrollment.
- Create a dedicated devices configuration (corporate-owned single-use, or COSU) for the enrolled device to serve a specific purpose.

Android Management API is currently supported only on devices running on Android version 9 or above that has Google Play installed and provisioned in Dedicated mode. The Corporate Dedicated mode is also referred to as Corporate Owned Single Use (COSU) mode and is a flavour of the device owner mode. This feature also supports the following device actions:

- Lock
- Reboot
- Sync to server
- Wipe

Device check ins are scheduled at regular intervals (hourly). But for immediate action, use the device action 'Sync to server' in the device details page. AMAPI devices do not send mandatory check-ins to Ivanti Neurons for MDM. Inventory updates are performed as and when there is an activity on the device.

Enabling Android Management API

To enable the Android Management API, go to **Admin > Android Enterprise > Authorise Google (needs a valid Google address) > Android Enterprise Enabled**.

The status of the enabled Android Management API feature (**Yes** for enabled and **No** for disabled) is also shown in the Device details page.

> GSuite accounts are currently not supported with COSU.

Adding an Enrollment Profile

An Enrollment profile is required to be created for enrolling Android device using the QR code scan or the alphanumeric string of the token. Enrollment Profiles can only be created when the Android Management API is enabled. You can also create custom device attributes to be associated with the enrollment profile.

1. Select **Admin > Android Enterprise> Enrollment Profiles**.
2. Configure the following settings in the **Enrollment Profile - Corporate Owned Dedicated Device** window.
3. Click **Save**. The **Profile Summary** window shows the following token details:

Setting	Description
Name	Enter a name that identifies this enrollment profile.
Description	Enter a description that clarifies the purpose of this enrollment profile.
Username	Enter the first few letters of a valid user name and select one from the matching results that are displayed. A valid user name could be from a local user or an LDAP user. Enrollment profiles tag the devices enrolled using the QR code in the profile to be displayed as a device belonging to the user for whom the enrollment profile was created.
Token Validity	Enter the number of days for the validity of the authentication token QR code scan. The number entered should be between 1 - 30. Device resets if you use the token or enrollment profile post the expiry period.
Custom Device Attributes	In the Actions column click **+Add New** to add custom device attributes to be associated with the enrollment profile. 1. Select the custom device attribute from the drop-down list in the **Attribute name** column. 2. In the **Value** column, enter the value of the custom attribute. 3. Click **Save**. The added custom device attribute is displayed in the table. To delete, click **Delete** options in the Actions column. The custom attributes can only be added to an enrollment profile during profile creation. The attributes fields cannot be edited after the profile creation.

- Name
- Description
- Username
- Token creation date
- Token expiry date
- Token value
- QR Code
- Custom Device Attributes.

> Devices are reset if proper configuration for the device fails to be acquired within the time interval of 10 minutes post registration. In such cases, you should re-register using the enrollment token/QR code

When an enrollment profile is created, it is listed in the **Enrollment Profiles** page. You can perform any of the following actions on the **Actions** column.

- Click on the View icon to view the details of the enrolment profile in the Profile Summary window. The QR code is also displayed in this window.
- Click on the Edit icon to edit the details of the enrolment profile.

> You can edit only the token validity. Other attributes cannot be edited.

Click the Delete icon to delete the enrollment profile.

Creating the COSU configuration

Administrators can configure dedicated devices that can be used for a specific purpose using Android Enterprise using the Dedicated devices (corporate-owned single-use, or COSU) configuration. The COSU configuration is distributed to Work Managed Devices (Device Owner mode) to provide only one app available to users in Kiosk mode. Devices that are in Work Profile on Company Owned Device are not supported.

Using this configuration, the admin can configure the devices to have the app pinned to the screen so that the Kiosk mode user cannot unpin this app and navigate away from the app to other screens of the device or use any other app on the device.

> Other apps can also be force-installed on the AMA device by selecting the "Install on device" option under Advanced Options & App Configuration, but you will not be able to interact with them while the Kiosk app is pinned to the screen via the configuration. For multi-app Kiosk, it is recommended to use the Kiosk functionality of Work Managed Device (device owner mode). This gives more control on apps and device settings and can also be extended to a multi-user mode.

Admins can make configuration changes such as allowing system navigation and the ability to use other apps pushed to the device for the end-user via the Google DPC by reviewing the various options based on the needs.

COSU configurations are determined by the priority assigned to them. The highest priority configuration is used in pushing the policy configuration to Google. COSU configurations are applied to devices within the defined space. It can be delegated to other spaces, if defined in default space.

To configure:

1. Go to **Configuration > +Add**.
2. In the **Lockdown & Kiosk: Android Enterprise Configuration**, click **Dedicated devices (corporate-owned single-use, or COSU)**.
3. Enter a name for the configuration.
4. Enter a description.
5. You can configure the following settings by clicking the relevant tabs:

- **App settings**
- **General lockdowns**
- **Kiosk customisation**
- **System Settings**

The following table provides the details of the configurable fields:

Setting	Description
App Setting	
App Name **General Lockdowns**	Select the app to be pinned on the device by typing the name of the app and by typing the initial letter of the app name until you see the desired app in the drop-down. If you do not see the desired app in the drop-down, ensure that the app you wish to deploy is a Public/Private app available in the Play Store and is added to the app catalog. This field is mandatory. You will not be allowed to create the configuration if you do not select an app to be added in this field. You can add only public and private apps. In-house apps and Web Apps (Private) cannot be added.
Keep Display On	Configure the battery plugged in modes for which the device stays on. Select any of the following options: • **AC** - Power source is an AC charger • **Wireless** • **USB** - Power source is a USB port • **Any** - Power source is from either AC charger or USB port or a wireless charger.
Kiosk Customisation **Customise Status Bar**	Select any of the following options for customising the status bar on the target devices: • **Notification and system info enabled** - To show system info and notifications on the status bar. • **Only System info enabled**- To show only system info on the status bar.
Customise System Navigation	Select any of the following options to specify the access to navigation features (Home, and Overview buttons) in kiosk mode.: • **Enabled** - Enables Home and Overview buttons navigation. Users can navigate out of the specified app if this option is selected. • **Disabled** - Disables Home and Overview buttons navigation. • **Home button only** - Enables only the home button navigation. Back button is available with all these options.
Enable Global Actions	Select to enable global actions in kiosk mode. Restart and shut down functionality associated with the power buttons is controlled via this option.
Enable System Error Dialogues	Select to enable error dialogues for crashed or unresponsive apps in kiosk mode.
System Settings	

Setting	Description

System Updates Settings	Configure the following settings to manage system updates:
	• **System Update** - Select the type of system update required.
	  ◦ **Automatic** - Install automatically as soon as an update is available.
	  ◦ **Postpone** - Postpone automatic install up to a maximum of 30 days.
	  ◦ **Windowed** - Install automatically within a daily maintenance window. Set the start and the end hours for the maintenance window period.
	  The updates installed on devices might vary based on the supported feature set, Android version, and the Google DPC version installed on the device.
	• **Freeze Period** - When a device is set within the freeze period, all the incoming system updates are blocked and not installed. Click **Add Freeze Period** to set the **Start Date** and the **End Date** of the freeze period.
	When a device is outside the freeze period, normal update behaviour is applied. If the end date is before the start date, then the freeze period extends between the current and the successive year.
	The freeze period can be set to a maximum of 90 days. Two consecutive freeze periods must be separated by a minimum of 60 days.

6. Click **Next**.
7. Select one of the following distribution options:

- **All Devices**
- **No Devices** (default)
- **Custom**

8. Click **Done**.

Managing apps on AMAPI devices

When the COSU configuration is distributed to devices, the apps are pushed and pinned to the screen on the AMA device. Irrespective of the COSU configuration being pushed to the device, apps that are installed on the AMA device can still be managed. The following are the details on the app management on these devices:

- Only public, private apps are supported; in-house apps and web-clips are not supported.
- Apps are pushed only if the installation settings have the "Install on Device" or "Silent Install" options are enabled. Apps that are assigned to the user/device without any of these options enabled will not be seen on the device or on the device's Play Store for any user action.
- The supported app configurations are Managed Google Play, and Work Managed Device (Android for Work) Settings. Managed configurations for apps are supported, including support for managed configuration for OEMConfig apps.

> The time for the completion of the installation and un-installation of configurations might vary based on the notifications from Google (messaging service) on whether the desired action is performed.

- The Go app will now be installed by default as part of the AMA device registration. During the registration process, the app will be pinned to the screen and once the setup is complete, will run in the background.

Policies except for the device registration requirement, enforcement based on manufacturer, OS version and security patch level are not supported. Device Allowlisting that allows only the Allowlisted devices to register with Ivanti Neurons for MDM is supported.

Managing apps feedback support on AMAPI devices

The app feedback support can be managed on AMAPI (COSU) devices. When a device is registered in AMAPI (COSU) mode, the managed app configuration will be pushed to Ivanti Neurons for MDM directly from Google without any intervention from the Go app. The Managed App Feedback information can be viewed at the device level from **Device details > Installed apps > View feedback**, or can be viewed at the individual app level by navigating to the specific Android app in App catalog under the "App Config Feedback" tab for the overall report across all devices. For information on app feedback mechanism, see **Synchronising and fetching app feedback**.

AMAPI Limitations

Currently, AMAPI has the following limitation:

- Only dedicated devices (COSU mode) are supported.

Supported Configurations

The following configurations are supported for AMAPI:

- App Distribution (single or multiple apps)
- Managed App Config for apps pushed to the device
- Wi-Fi configuration
- Android Enterprise Lockdown-Dedicated (COSU) configuration
- Always-on VPN Configuration

12.6.4. Google Apps API

Google customers who use Single Sign On (SSO) to authenticate user access to Google Apps services may not be able to use Exchange to connect users to email, contacts, and calendar due to limitations in the protocol that prevent devices from supporting SSO-triggered redirects to external authentication services. This service addresses this condition by creating and managing account passwords for ActiveSync connectivity.

Prerequisites

Before attempting to configure the Google Apps API feature, you need:

- Admin access to an account on https://console.developers.google.com/.
- Admin access to an account on https://admin.google.com.

Enabling the Google Apps API feature

Procedure

1. Select **Admin > Google > Google Apps API**.
2. Click **Step 1: Google Dev**at the bottom of the rectangle on the left labelled 1.
3. The Step 1: Google Dev page appears.
   Follow the instructions that appear on the Step 1: Google Dev page, and then click **Done**.
4. Click **Step 2: Google Admin**at the bottom of the middle rectangle labelled 2.
5. The Step 2: Google Admin page appears.
   Follow the instructions that appear on the Step 2: Google Admin page, and then click **Done**.
6. Enter the Google Admin user name in the **Enter the Google Admin user name** field in the rectangle on the right labeled 3.
7. In the same rectangle, click **Choose File** to upload the JSON file you downloaded in Step 1.
8. Click **Save**.
9. If you cannot see the Google Apps API page, it might be that you do not have the required permissions. You need one of the following **roles**:
   - System Management
   - System Read Only

12.6.5. Admin - Android Enterprise

Licence: Silver

- Android Enterprise-enabled Ivanti, Inc productivity apps like Email+, Docs@Work, and Web@Work require Gold license.
- Tunnel for Android Enterprise requires Platinum license.

Android Enterprise enables use and configuration of Android Enterprise apps. Android Enterprise users can view and install apps from the app catalog as well as via Google Play.

If you are a new customer, the app distribution is set to per device by default. You cannot change this setting. For upgrading customers, you have a choice between apps distribution per user or per device. Also for upgrading customers, app distribution per user is selected by default. Many users have multiple devices. If a user has multiple devices, when app distribution is set per device then you can make a different set of apps available on each device.

This section contains the following topics:

- Configure Android Enterprise
- Configuring the Android Enterprise Work Profile

Configure Android Enterprise

1. In the Ivanti Neurons for MDM portal, click **Admin > Google > Android Enterprise**.
2. Select one of the following options:
    - **Managed Google Play Account:** For enterprises that are not G Suite subscribers, this method allows users to be enrolled with Android Enterprise without sending any personal information (email addresses to Google). Ivanti Neurons for MDM will provision and manage users automatically with Google. You will be asked to authorise Android Enterprise with an admin Google account.
    - **Managed Google Account:** For enterprises who are G Suite subscribers, this method allows your users to enroll in Android Enterprise with their Google accounts. Each user is required to have a Google account to enroll with Android Enterprise.

Follow the directions on the screen for completing the configuration process:

4. For the automatic method, this includes:
    - Enabling your UEM API and creating your Enterprise Credentials.
    - Enrolling in Google by authorizing the owner of the integration. This should be an IT account rather than a personal account.
    - Setting your credential by dragging and dropping your Service Account JSON Client ID.

For the alternate method, this includes:

- Refer to the CLIENT ID in the below section, and add it to the Google Admin.
- Look up your MDM token in the Google Admin and service account in the Google Cloud Console.
- In Ivanti Neurons for MDM, enter your MDM token, enterprise Google domain, and Enterprise Admin email address to connect to the Google service.
- In Ivanti Neurons for MDM, drag and drop your Service Account JSON Client ID.
- In Ivanti Neurons for MDM, authorise Ivanti Neurons for MDM to view and /or manage your Google Users by clicking **Authorise**.

The Ivanti Neurons for MDM user interface guides you through these steps.

CLIENT ID to bind Ivanti Neurons for MDM with Managed Google Account

Add the client id as **140561810807-tiiglke17laibbrt5darupmvo4ae7cbj.apps.googleusercontent.com** in the Admin Console to bind the Ivanti Neurons for MDM tenant with Managed Google Account.

Configuring the Android Enterprise Work Profile

1. In the Ivanti Neurons for MDM portal, go to **Configurations**.
2. Click **+Add**.
3. Select **Lockdown & Kiosk: Android Enterprise** configuration.
4. Enter a configuration name and description.
5. Click the **Work Profile** lockdown type.
   Select the **lockdown settings** you want to apply to the target devices.
   Important: When the user adds a Google Account using Add account in Settings, the Google authentication server checks if the domain of the account is registered as an UEM-managed domain. Verify that **Enforce UEM policies on Android devices** is checked. If so, the Go client is automatically installed or updated (if it is not already installed on the device) and launched. Once the user goes through the registration process, the user is prompted to create a Work Profile and the Google Account is automatically migrated to the work profile.

12.7. Work with ChromeOS Devices

This section contains the following topics:

- ChromeOS and Ivanti Neurons for MDM
- Distribute Android apps to ChromeOS devices
- ChromeOS Blueprint Configuration
- Device Actions
- FAQs
- Recommended Steps for evaluation

12.7.1. ChromeOS and Ivanti Neurons for MDM

ChromeOS is a Linux-based operating system created and distributed by Google. Ivanti Neurons for MDM supports devices working on Android, Windows, iOS, and macOS. This support has now been extended to ChromeOS devices as well. Ivanti Neurons for MDM provides a unified and simple mobility management solution for configuring and managing your ChromeOS devices. Ivanti provides a unified, simple, and feature-rich solution for ChromeOS devices similar to the admin workflows that are available for iOS, Android, Windows, and Mac on Ivanti Neurons for MDM. The administrator can simply connect Ivanti Neurons for MDM with their Google Cloud (also referred to as Google Admin console) using a simple integration from **Admin > Google > ChromeOS Management**.

Prerequisites

1. Must have a managed Google Admin account.
2. The LDAP users and OUs must be imported on Google Admin Console. Ivanti Neurons for MDM supports only OUs imported from an LDAP source. Local OUs are not supported.
3. The administrator must have synchronised the organisation units (user groups) into the Ivanti Neurons for MDM. This can be done by configuring the LDAP server and adding the organisation units.

Authorizing Google

The ChromeOS devices available on the Google Admin console cannot be registered directly on the Ivanti Neurons for MDM. Instead, these devices are registered with Google and information about these devices is synced between Google and Ivanti Neurons for MDM. The administrator must authorise Google to import the devices and perform other actions like assigning apps, configurations, etc.

Procedure

1. Go to **Admin → Google > ChromeOS Management**.
2. Click **Authorise Google**.
3. Select the Google Admin account that you want to authorise.
4. Click **Continue** to accept the permissions to provide the required services.
   The **ChromeOS successfully setup** confirmation appears on the screen. You can also find the domain information below the confirmation.

Syncing ChromeOS devices from Google

The administrator must sync the ChromeOS devices from the Google Admin console. When using the Google Admin console to access the ChromeOS devices for the first time, the administrator must manually sync the devices using the Sync Now option from the ChromeOS Management page.

> After syncing the devices manually for the first time, the subsequent syncs will happen automatically on an hourly basis.

Deleting the Google Admin Console integration with Ivanti Neurons for MDM

Delete integration revokes the OAuth token we received from Google to access Google resources. It deletes the ChromeOS devices, inventory associated with Blueprint config and app config, and the enrollment metadata. The Blueprint configuration and uploaded apps will not be deleted.

In case the tenant enrollment is not deleted, you can raise a ticket to check the issue.

Procedure

1. Go to **Admin → Google > ChromeOS Management**.
2. Under the ChromeOS Ivanti Neurons for MDM Registration section, Click **Delete**.
   A pop up appears on the screen indicating whether you want to proceed with the Delete operation, and all the devices associated with this integration will be deleted. Select **Ok**.

12.7.2. Distribute Android apps to ChromeOS devices

The administrator can distribute Android apps from the App Catalog to ChromeOS devices.

Prerequisites

1. Android Enterprise must be configured. For information on setting up Android Enterprise, see **Setting up Android Enterprise**.
2. Android apps must be present in the App Catalog.
3. Ensure that the ChromeOS device (Chromebook) user is part of a User Group (also referred to as Organisational Unit) before distributing Android apps and ChromeOS Blueprint Configuration.

Once the Android app is identified, you need to distribute the app following the similar process that you follow to distribute any other app. When you are distributing the Android app, make sure to select the User Groups to which you want to distribute the app and perform a Silent Install on the device.

> If your existing Android app deployment is set to be distributed to devices / device groups or users, you will have to change the distribution to be based on User Groups. This can impact exising deployments if the app is already in use. It is recommended to do this on a completely new app first.

> Install Settings allows administrators to control the final silent installation and it is required to push the app to ChromeOS devices. User Groups must be selected here.

12.7.3. Add and distribute ChromeOS extension apps

The administrator can add ChromeOS extension apps to the App Catalog and distribute these apps to ChromeOS devices.

Procedure

1. Go to **Apps** > **App Catalog**.
2. Click **+ Add**.
3. Select **ChromeOS** from the list. The **Add ChromeOS App Details** page appears on the screen.
4. Provide the following details: **App Name** - Name of the ChromeOS extension app, **Extension ID** - You can get this info from the Chrome web store.
5. Click **Next**. The **App Configurations** page appears on the screen. You will be able to select an immediate update that will occur at the next device check-in, or you can choose to have the app update automatically when new versions become available.
6. Select one of the app distribution options and provide the required details.

> The ChromeOS app distribution is supported only for LDAP user groups.

Once the ChromeOS extension app is identified, you need to distribute the app following the similar process that you follow to distribute any other app. When you are distributing the ChromeOS extension app, make sure to select the User Groups to which you want to distribute the app and perform a Silent Install on the device.

> Install Settings allows administrators to control the final silent installation and it is required to push the app to ChromeOS devices. User Groups must be selected here.

You can edit the information about a ChromeOS extension app or delete a ChromesOS extension app from the App Catalog. You must follow the similar process that you follow to edit or delete any other app from the App Catalog.

Edit a ChromeOS extension app

1. Go to **Apps > App Catalog > Details**.
2. Click **Edit**. Make the required changes and click **Save**.

For information about Deleting an app, see **Deleting Apps from the App Catalog**.

12.7.4. ChromeOS Blueprint Configuration

The ChromeOS Blueprint Configuration has the following settings:

- Device settings
- User and browser settings
- Managed guest session settings

You can apply ChromeOS configuration on specific User Groups (also referred to as Organisational Units). When you try to distribute the ChromeOS Blueprint Configuration, only the User Groups section will be available, and all the LDAP User Groups that are also associated with the authorised Google Admin Console will be listed under the section. You can select one or more from the listed groups and apply the configuration.

Procedure

1. Go to **Configurations > Add**.
2. Select **Google ChromeOS** under the OS section. The **ChromeOS Blueprint configuration** tab appears on the screen.
3. Click **ChromeOS Blueprint**. The **Create ChromeOS Blueprint Configuration** page appears on the screen.
4. Enter a name for the configuration in the **Name** box.
5. Under the Configuration Setup, you can modify the Device Settings, User and browser settings, and Managed guest session settings, as needed and toggle the "Push to device" button to apply the modified settings.
6. Click **Next**.
7. Select **Custom** for the distribution options.

> Only the LDAP User Groups will be available to distribute the configuration.

> In the case of distributing the configuration to everyone, it can be done only for the LDAP User Groups available in Ivanti Neurons for MDM and Google Admin Console.

Select one or more groups and click **Done**.

> When the distributed settings are undistributed, the applied settings will not be reverted.

> You can upload files in ChromeOS Blueprint Configuration.

12.7.5. Device Actions

The following actions are supported on ChromeOS devices:

- **Wipe** - The Wipe action deletes all the data from a device and the device will be reset to factory settings. For more information, see **Wiping a Device**.
- **Lock** - The Lock action restricts you to perform any further action on the device. For more information, see **Locking a Device**.
- **Unlock** - The Unlock action releases the device for further use. For more information, see **Unlocking a Device**.

12.7.6. FAQs

This section lists some of the common FAQs you might have when using the ChromeOS devices on Ivanti Neurons for MDM.

- How does Chromebook management differ from other OS?
- Google allows only LDAP User Group-based distribution of configurations as of now and the administrator should ensure when working with configurations or apps, distribution is based on LDAP user groups. Local user groups and Device Groups are not supported for ChromeOS device management.
  What licensing do I need with Ivanti for managing ChromeOS devices?
- ChromeOS devices should have licenses such as Chrome Enterprise Upgrade or Chrome Education Upgrade. These can be purchased from resellers as part of hardware or as standalone licenses. Refer to Google documentation for more information. To get started with Chrome device management, Secure UEM (Unified Endpoint Management) licensing is required with Ivanti.
  Will Mobile Threat Defense (MTD) or a similar solution be available? Do I need a separate license for MTD?
- This is not available currently in the product, please refer to current limitations. We will provide more information on changes with feature capability via FAQ and release announcements.
  Why do the configs and apps tab not have details as is the case for other devices?
- Since configurations are distributed to User Groups and not applied based on the user logged in, at present the configurations are not shown in device details. Apps follow the same logic of distribution and have the same limitation. We will provide more information on changes with these limitations via FAQ and release announcements.
  How many configurations are currently supported for ChromeOS?
- With ChromeOS, we have reduced the number of configuration tiles available and have reduced the admin tasks associated with the configuration. We refer to this configuration as “ChromeOS Blueprint”. ChromeOS Blueprint supports close to 700 configurations on these devices. Refer to Google’s documentation for configuration options.
  How is it easy to manage one configuration for all devices?
- The administrators can simply clone an existing configuration and modify it (if required) for their respective user groups. You don’t have to start from scratch.
  How do I add VPN configuration to Chrome devices?
- This can be done using the Android apps, and not using native VPN.
  Do device actions such as Retire and Wipe work on these devices?
- Chromebooks in Enterprise are always managed by an organisation and data on such a device is considered completely organisational. With this in mind:
  - Retire is blocked
  - Wipe is allowed
  - Lock is allowed
  - Unlock is allowed
  - Other actions – are not supported

Which Chromebooks, in terms of hardware are supported by Ivanti?

- Devices supported by Google Cloud device management solutions are inherently expected to be supported by Ivanti. Ivanti does not currently publish a list of specific hardware supported by Ivanti’s solution.
  Which version of Chrome OS is supported?
- Google Cloud supports only the latest stable version of ChromeOS and Ivanti’s support follows the model supported by Google due to the nature of backend integrations.

Can you list the current limitations since this is the very first launch of this capability?

With new Chrome OS support, we are working hard towards providing capabilities that our customers are eagerly waiting for. Below are some limitations that admins should take notice of:

- Chrome OS extensions (browser apps) are not currently supported (as “apps”) for distribution.
- Managed app config for Android apps is not currently supported.
- Wi-Fi configuration API was recently released and is not currently supported.
- Certificate distribution is currently not supported.
- Distributing Ivanti Go (previously known as MobileIron Go) Android app is currently not supported.
- Ivanti Tunnel (VPN) app is currently not supported.
- Spaces and space delegation is currently not supported.
- Mobile Threat Defense solution is currently not supported.
- Ivanti’s Zero Sign-on solution is supported on these devices, categorised as unmanaged devices.
- Policy actions are not fully supported.

12.7.7. Recommended Steps for evaluation

The following steps are recommended to validate a solution:

1. Create a separate OU (User Group) which has a test user in your directory source (example, Active Directory). This will avoid any impact to active Organisational Units.
2. Sync users between Ivanti, Google, and directory source (LDAP). Verify that the “test OU” is available in User Groups.
3. Integrate Ivanti Neurons for MDM with Google as highlighted in steps above.
4. Create ChromeOS Blueprint Configuration and distribute this only to the “test OU” User Group.
5. Boot up a Chromebook (out of box or previously registered). Ensure it is available in the Devices list.
6. Verify that the ChromeOS Blueprint settings are available on the device.
7. Follow similar steps for Android app distribution.

12.8. Firmware Management

This section contains the following topics:

- Enrolling to Zebra OTA service
- Samsung E-FOTA License Management (Decommissioned)

12.8.1. Enrolling to Zebra OTA service

When enrolled to the Zebra OTA(Over The Air) service you can enable the Zebra OTA configuration to receive and update the firmware details of Zebra devices registered with Ivanti Neurons for MDM.

Procedure

1. Go to **Admin > Infrastructure > Zebra OTA**. The **Zebra OTA Service** page is displayed.
2. Under the **Link to Zebra's OTA service**, click **Begin**.
3. Enter your Zebra OTA credentials to login and follow the steps to request an approval to avail the Zebra services.
4. Click **Complete Verification** to get the confirmation on the connection to the Zebra service. When the connection is confirmed, the status of the successful enrolment is displayed in the Zebra OTA Service page.

To revoke the enrollment, click **Revoke** under the **Actions** column. The **Revoke** action removes all Zebra OTA configurations from the existing configurations. To re-enrol with Zebra OTA, click **Refresh**. Refresh action has no impact on the existing configurations.

After enrolment, you can enable the Zebra firmware configuration which Go client receives and applies to Zebra devices (running on Android version 8.0 or supported newer versions) in Device Owner mode. When the configuration is applied, the firmware is downloaded and installed on the device as scheduled in the configuration. For more information on enabling the Zebra firmware configuration, see System Update Configuration.

On completion of firmware update, you can view the firmware update status on the Zebra device under the **System Update** column in the Devices page. The following are the possible status:

- **Unknown** - Not supported by client or OS
- **Current** - Device has the most current update available
- **Pending** - System update configuration is applied but the update has not been downloaded or applied
- **Downloading** - System update is being downloaded to the client
- **Available** - System update is currently available for the device
- **Error** - Error in download or installation.

The **Zebra Patch Version** column in the Devices page displays the Zebra patch information of the device.

> The **Zebra Patch Version** is not supported for devices on Android 11 and later; only the **Zebra Full Upgrade** is supported.

12.8.2. Samsung E-FOTA License Management (Decommissioned)

Samsung E-FOTA service will be decommissioned in July 2022. For more information, see Samsung announcement.

> You cannot configure Samsung E-FOTA service from now. However, if you have an existing E-FOTA configuration, you can deactivate the configuration by navigating to **Admin** > **Firmware Management** > **Samsung E-FOTA** and clicking on **Deactivate** option.

12.9. Manage Scripts and Files

Administrators can manage scripts and files which can be used in Configurations and pushed to devices.

This section contains the following topics:

All Scripts

Files

12.9.1. All Scripts

Applicable to: macOS and Windows devices

In the **Admin > Scripts and Files > All Scripts** page, Ivanti Neurons for MDM allows users with System Management role to create or upload, and manage scripts that can be used in configurations and distributed to devices. You can associate custom attributes with the scripts and assign the resultant values to the configured devices. Use Audit Trails to view logs of the script changes and Device Details page to view the execution results.

You can write a script that configures any settings on devices. For example, you can run scripts that:

- force device users to change their passwords monthly,
- lock the screen after 5 minutes of idle time, or
- configure a secured Wi-Fi network.

This section contains the following topics:

- Adding a script
- Modifying a script
- Using script variables (applicable to Windows and macOS)
- Testing a script
- Verifying the script execution results

Adding a script

You can create or upload a repository of bash scripts (for macOS) and ps1 scripts (for Windows). This repository can be used in a configuration, such as Mobile@Work for macOS Script, to select a script and distribute it to execute on the devices as per the specified schedule in the configuration.

For example, you can create a shell script for execution on devices. You can use wrappers if necessary. The execution of binary files from within a shell script is not supported.

> Ivanti highly recommends you test your shell scripts before running them on the devices to ensure their robustness and quality. Run your script locally, and correct any errors that result.

Procedure

1. Go to **Admin > Scripts > All Scripts**.
2. Click **+ Add**.
3. Enter a Name and Description for the script.
4. Under the Platform type, select macOS or Windows.
5. Select one of the following **Script Type**:
    - **bash**
    - **zsh**
    - **python**
    - **swift**

- **ps1**

6. Select the **Run as root** check box to run the script as root on devices. By default, this option is cleared.
7. In the **Script Editor**, you can type, drag and drop, or copy and paste a script in the text box.
8. Alternatively, click **Import code from a Script** to drag and drop an existing script file or click Choose File to browse and select the script file to be uploaded to Ivanti Neurons for MDM. This will replace any existing script in the script editor. This action cannot be undone. Click **Import**. The code from the uploaded script will be displayed in the script editor.
9. (Optional) In the **Custom attributes available** section, select one or more displayed device custom attributes to associate them with the script. They can be used to assign the resultant script execution values to the device custom attributes of the configured devices. Click **Sample Code for Custom Attributes** to view a sample code using custom attributes in a script.
10. Click **Save**.

The custom attribute names in the script should be in lower case. If the custom attributes are referred to in any scripts, then the attributes cannot be removed. When you modify a custom attribute (for example, its name) and if it is associated with a script, then you should make the corresponding changes in the associated scripts.

Modifying a script

To edit or remove a script:

1. Go to **Admin > Scripts > All Scripts**.
2. Under the **Actions** column for the script, click the corresponding icon for edit or delete action.
3. Follow the instructions on the screen to complete the action.

When a script (content, name, description) is changed, all the configurations that are associated with the script are redistributed to the devices.

Using script variables (applicable to Windows and macOS)

Define and store script inputs such as environment and substitution variables in the script repository. In the Mobile@Work for macOS script configuration or Ivanti Bridge for Windows Scripts and Actions Configuration, depending on which script is linked, the related script variables will be available for use as required. This feature requires **Mobile@Work for macOS** 1.71.0 through the most recently released version as supported by Ivanti Neurons for MDM. For Windows, this feature requires **Ivanti Bridge**.

Use the variables to run a script with different values every time it runs. For example, an administrator can create a script to use the $ environment variable as the script variable and associate it with a Mobile@Work for macOS script configuration. When the configuration is distributed and installed on each user device, Ivanti Neurons for MDM sends a different registered user email address for each device to take certain actions. The Ivanti Neurons for MDM administrative portal supports custom variables.

To add a script variable:

1. Go to **Admin > Scripts > All Scripts**.
2. In the Script Input section, click **+ Add**.
3. In the Add Script Input - Environment Variable pop-up page, enter the following details:
   - Label to Show - This text will be shown as a label in the Mobile@Work for macOS script configuration page. For example, Enter OS Folder, Enter Apache Number, and so on.
   - Environment Variable Name - For example, JAVA_HOME, OS_VERSION, and so on. Ivanti Neurons for MDM substitutes values for the script variables while sending the configuration details to a target device as the values are persisted in the database.

- Environment Variable Default Value - For example, 1024, bin/java, $, and so on. The input variables would be used in the script uploaded or edited by an administrator. See also the following notes.

In the Preview region, review how the environment variable's value will be shown as script input in the configuration page.

5. Click **Save**.

This way, only the label and the default value are available to the configuration and not the environment variable name, which provides a layer of abstraction.

- Alphanumeric value (for example, 1024, bin/java, root@localhost) or system attributes (for example, $) are acceptable as environment variable's value.
- The environment variable's value can be modified or deleted during deployment in the configuration page.
- If the environment variable's value is not provided, ensure a value is provided during script deployment. Otherwise, empty value will be passed to the script.
- After a script configuration is distributed and installed on the device, editing environment variables in the **Admin > Scripts and Files > All Scripts** page will not impact the existing configurations associated with the script. See also **Mobile@Work for macOS script configuration**. For Windows, see **Ivanti Bridge for Windows Scripts and Actions Configuration**.

Editing a script variable

To modify a script variable, click the edit (pencil) icon against the variable and save the changes.

If a script configuration refers to a script having script variables, editing the label of an existing script variable will also reflect in the script configuration. However:

- A change in the default value of the script variable will not reflect in existing configurations.
- A change in the default value of the script variable will reflect in any new configurations created with the preceding script.

Deleting a script variable

To delete a script variable, click the delete (minus) icon against the variable and confirm.

A newly created script variable, or deletion of an existing script variable will reflect even in an already existing configuration.

Testing a script

Test run a script in the debug tool quickly before testing it on a device and without necessarily having to save the scripts.

Prerequisites

- This feature requires **Mobile@Work for macOS** 1.71.0 through the most recently released version as supported by Ivanti Neurons for MDM.
- For Windows, this feature requires **Ivanti Bridge for Windows Scripts and Actions Configuration**.

Procedure

1. Go to **Admin > Scripts > All Scripts**.
2. In the Script Editor, add or import a script.
3. If the tenant has multiple spaces, then select a space.
4. In the Test Script section, select macOS as the platform.

5. In the **Find devices** text field, find and select the device on which the script can be tested. The device can be searched by serial number,user name,device name, andOS version.
6. Click **Test Now**. This way, an environment variable can be added, edited, and deleted, and the script can be tested with that state (without even saving the changes made). For **Windows** Script, a pop up appears on the screen that the Script execution will start and you can view the status from Device Details Logs tab after sometime.
7. Click **Save**.
8. Wait for the script to be pushed and executed on the device.
9. Review the published test results in the Script Input (containing environment variable details), Script Output, and Custom Attributes sections. The default values of the environment variables are also displayed.

Verifying the script execution results

To view the logs of the script execution results:

1. Go to **Devices**.
2. Click the name of the device.
3. Click the **Logs** tab.
4. In a row that displays the Script Execution action, you can verify the following information:
    - Script name in the Details column.
    - Script execution status in the Status column.
    - Script execution date and time in the Date column.
    - Script execution logs (device log plist) by clicking the eye icon under the Actions column.

Use filters to display the **Script Execution** rows. Logs from these rows include the output (plist) of standard output and standard error for the scripts.

6. Use filters to display the **Script Execution Result Processing** rows. Logs from these rows include details (plist) of how the results were processed.
    - If a script did not have any custom attributes associated with it, there will not be any results to process. Such scripts will not be displayed in the list of the filtered rows.
    - If a script had custom attributes associated with it and if they were in the expected format, then the custom attributes from the results are mapped and the status is displayed as Success. You can verify the mapped custom attributes and their values in the **Attributes** tab.
    - If a script had custom attributes associated with it and if they were not in the expected format, then the custom attributes from the results are not mapped and the status is displayed as Error.
    - If the result format is correct but not all the associated custom attributes are sent in the result, the status is displayed as Error.
    - If a script variable is sent with the script, Script Execution Result Processing logs will include details (plist) for the script variable.

Related topics:

- **Mobile@Work for macOS Script configuration**
- **How to create a configuration**
- **Ivanti Bridge for Windows Scripts and Actions Configuration**

12.9.2. Files

Applicable to: macOS devices

The Ivanti Neurons for MDM allows users with System Management role to create or upload, and manage files used for configuring and distributing to devices.

Procedure

1. Go to **Admin** > **Scripts and Files** > **Files**.
2. In the **Files** page, click **+ Add**.
3. In the **Create File** window, enter the following details:
    1. In the **Name** field, enter a name to identify the file.
    2. In the **Description** field, enter a description that clarifies the purpose of this file.
    3. In the **Upload File** pane, click **Choose a file** to upload the .zip file. Alternatively, you can drag and drop a file from your device.
4. Click **Save**.
   The newly added file appears on the **Files** page.

Editing a file

1. Go to **Admin** > **Scripts and Files** > **Files**.
2. Select the file that you want to edit and click **Edit**.
   The **Edit File** window appears.
3. (optional) You can edit the **Name** and **Description** fields.
4. In the **Upload File** pane, click **Choose a different file** to upload the .zip file. Alternatively, you can drag and drop a file from your device.
5. Click **Update**.

Deleting a file

To delete the existing **Files**, navigate to **Admin** > **Scripts and Files** > **Files**, select all the files that you want to delete and click **+ Delete**.

If the **File(s)** is associated with a configuration, Ivanti Neurons for MDM will display a **Warning** message, **"File cannot be deleted as it is being used by other policies."**

12.10. Branding

This section contains the following topics:

- Admin > Apple App Catalogue (Branding)
- Branding the Android App Catalog
- Admin > Android Kiosk Branding
- Branding Email Templates
- Self-Service Portal
- Self-Service Portal (Branding)
- Multi User Sign-In (Webclip) Branding
- Organisation

12.10.1. Admin > Apple App Catalogue (Branding)

Licence: Gold

You can brand the Apple {{app catalog}} to make its appearance more familiar to your end users for iPhone, iPad, and Mac devices. You can customise the following items in the Apple app catalogue:

- App Icon (PNG, 360px square)
- App Name
- App Banner Image (PNG, 360x64)
- Text colour

> There are two modes to access Apple App Catalog: Standalone App Catalog and Integrated App Catalog. Standalone App Catalog is available on iPhone, iPad and Mac devices. Integrated App Catalog is available for iOS and Mac devices.

Branding the Apple app catalogue

The changes made in this page affects the Home Screen, Splash Screen and App Home Screen. The procedure is similar for both Standalone App Catalog and Integrated App Catalog.

Procedure

1. In the **Apple App Catalog Branding** page, click **Customise** (upper right).
2. In the **App Icon** section, drag the logo file to the dotted box, or click **Choose File** to select it from your file system. The app icon is displayed on the iOS home screen
3. In the **App Name** section, edit the **App Catalog Name** text to change the label shown on the splash screen.
4. The name and icon are applied on the home screen banner. To change a custom banner image, deselect the **Apply the name and icon on the home screen banner** option. This will display the **App Banner Image** section.
5. To change the app banner image, drag and drop the new banner image file to the dotted box, or click **Choose File** to select it from your file system. The app banner image appears on the top bar in the app home screen.
6. In the **Text Colour** section, click the hex colour code box to pick a colour or enter the hex colour code to assign to the text and icons. This will apply to the text on the splash screen, app name, the banner and action button.
7. Click **Save Changes**.

The app catalog name you enter applies to Android, iOS and macOS.

12.10.2. Branding the Android App Catalog

Licence: Gold

You can brand the Android {{app catalog}} to make its appearance more familiar to your end users. You can customise the following items in the Android app catalogue:

- Catalogue logo (PNG, 360x64)
- Catalogue name
- Action bar colour
- Shortcut icon
- Shortcut name

Branding the Android app catalogue

Procedure

1. In the **Android App Catalog Branding** screen, click **Customise** (upper right).
2. To change the App Catalog Logo, drag the logo file to the dotted box, or click **Choose File** to select it from your file system.
3. Click the **Action Bar Colour** field to display a colour palette to select from or enter the hex number for the colour you prefer.
4. Edit the **App Catalog Name** text to change the label for the catalog.
5. The app catalog name you enter applies to Android, iOS and macOS.
   To change the Shortcut Icon, drag the icon file to the dotted box, or click **Choose File** to select it from your file system.
6. Edit the **Shortcut Name** text to change the label for the app shortcut.
7. Click **Save Changes**.

12.10.3. Admin > Android Kiosk Branding

Licence: Silver

You can brand the Android kiosk page to make its appearance more familiar to your end users. You can customise the following items:

- banner logo (PNG, 840x114) or text
- banner border colour
- banner background colour
- screen background colour
- screen background image (1280x800)
- screen background format

Branding the Android kiosk screen

Procedure

1. Navigate to **Admin>Android Kiosk**.
2. In the **Kiosk Mode Branding** page, click **Create Branding**.
3. In the **Name** field, type the name of the kiosk mode branding.
4. If you want to turn off the banner, uncheck **Enable Top Banner**.
5. Click the **Banner Background Colour** field to display a colour palette to select from or enter the hex number for the colour you prefer.
6. Click the **Banner Border Colour** field to display a colour palette to select from or enter the hex number for the colour you prefer.
7. Select **Image/Logo** or **Text** to set the banner content.
8. If you selected **Image/Logo**, drag and drop the image file or click **Choose File** to select one.
9. If you selected **Text**, type the text you want to display in the banner.
10. Click the **Background** tab.
11. Click the **Background Colour** field to display a colour palette to select from or enter the hex number for the colour you prefer.
12. To change the background image:
13. a. Delete the default image.
    b. Drag and drop the preferred image or click **Choose File** to select one.
    c. Select the preferred layout.
    Click **Save Changes**.
    The created kiosk mode branding is displayed in the **Kiosk Mode Branding** page. To further edit the customised branding, click on the Edit icon in the **Actions** column. To delete the customised branding, click the Delete icon. On deleting the custom kiosk branding, the configuration using the branding will revert to the default branding.

12.10.4. Branding Email Templates

You can brand the end user email invitation to make its appearance more familiar to your end users. Click **Revert to Default Settings** to clear the customisations.

You can customise the following email templates in all of your supported languages:

- **End User Invitation** - Invite a user to connect their devices to get access to apps and configurations.
- **Password Reset Notification** - The system sends reminder emails 7-days and a 24-hours prior to the password expiration for local accounts. This does not apply to LDAP accounts.
- **Registration Confirmation**- Email sent after a user completes registration. You can use this to thank users for registering and to point them to more learning resources.
- **Policy Compliance Notification**- Email sent when devices go out of compliance.

This section contains the following topics:

- Previewing and testing an email template
- Customising the message headers
- Customising an email template
- Supported email variables

Previewing and testing an email template

You can preview and test the email templates. The test allows you to send an email based on the template to an email address you specify.

To preview and test an email template:

1. Click **Admin**.
2. Under Email Templates, click **End User Invitation**, **Password Reset Notification**, **Registration Confirmation**, or **Policy Compliance Notification**.
3. Click the **Preview and Test** link associated with the email template you wish to preview and test.
4. View the rendered template in the rendered template pane.
5. Specify a test email address to which to send the test email.
   If the email address you specify belongs to a current user, the test email substitutes values for most of the email template variables, affording a very accurate idea of the user experience of the email. However, the test email does not substitute values for variables Ivanti Neurons for MDM generates at the time it generates an actual email invitation.
6. Click **Send Test Email**.

Customising the message headers

1. Click **Admin**.
2. Click **Email Templates**.
3. Click the **Edit** icon link (under Actions column) associated with the email template you wish to edit.
4. Provide new settings as desired for **Email Display Name**, **From Email Address**, **Reply-to Email Address**, and **Set up SMTP Email Configuration**.

5. If you customise the From and Reply-To email addresses, it is recommended that you Allowlist the Email Relay Service to ensure that your emails aren't blocked by email SPAM filtering services. See **this document** for more information.
   Click **Save**.
6. Review the preview of the email template and click **Save**.

Using SMTP configuration

The **Set up SMTP Email Configuration** is added to enable the admin to configure their own email server integration for outbound notifications.

1. Go to **Admin > Branding > Email Settings**, enable the **Set up SMTP Email Configuration** option.
2. Update the following feilds:
   - SMTP server
   - SMTP server port
   - Protocol
   - User Name
   - Password
3. Click **Test** to send a test mail, a **Test Email** pop-up screen is displayed.
4. Enter the **Recipient** name and **Body** of the message, click **Save**.

> If the credentials are not correct, and error message is displayed.

5. Click **Save**

The following table summarises fields and descriptions in the SMTP Configuration window:

Fields	Description
SMTP Server	Specify the IP address or fully-qualified host name for the SMTP server the Ivanti Neurons for MDM Server will use.
SMTP Server Port	Specify the port configured for the SMTP server.
Protocol	If the SMTP server you are configuring is a secured server, that is, it uses the SMTPS protocol, then select the SMTPS button. Otherwise, leave SMTP selected.
User Name	Enter the user name required for SMTP authentication.
Password	Enter the password required for SMTP authentication.

Customising an email template

1. Select **Admin > Branding > Email Templates**.
2. Select the template to edit, **End User Invitation**, **Password Reset Notification**, **Registration Confirmation**, or **Policy Compliance Notification**.

3. Click the edit pen icon adjacent to the email template you wish to customise.

4. Edit the subject line if desired.
5. Edit the email template containing HTML elements in the body pane to customise the message content.

You can use the variables displayed on the right in the body of the email. See **Supported email variables**.

6. Click **Preview** to preview the email template as you create iterations to your satisfaction.
7. When you are ready to save the template, click **Preview**. This renders the preview and provides a save function.

8. Click **Save** if you are satisfied with the preview.

Allowlisted and Blockedlisted content in customised user invitation

While customising the user invitation email template in **End user invitation**, there are a set of Allowlisted HTML tags and attributes that are allowed. There are also a list of Blockedlisted strings that are not allowed in the user invitation to prevent Cross Site Scripting (XSS) vulnerability.

You are allowed to use only the Allowlisted tags and attributes in the invitation email. The following table lists the Allowlisted tags and the corresponding attributes that are allowed.

> Some Allowlisted tags(Example: <big>) should not have any Allowlisted attribute and therefore are displayed blank.

Allowlisted Tags	Allowlisted Attributes
<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"]

Allowlisted Tags	Allowlisted Attributes
	[]
	[]
<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"]

The following are the list of Blockedlisted strings that are not allowed in the customised user invitation.

- Script, @import, ¼script¾, script>, <script, <script>, </script>, javascript, alert(, moz-binding, expression(, +ADw-SCRIPT+AD4-,+ADw-/SCRIPT+AD4-, xml:base
- Special characters and search for javascript or script
- The meta content attribute containing "url=" case insensitive
- The img src not containing .svg.
- Attribute value containing "\00"

If any of the above Blockedlisted strings are used in the HTML content of the end user invitation, an error message is displayed when you click **Preview**. This error message lists the HTML content that is not allowed in the end user invitation. Edit and remove the HTML content that is not allowed and then click **Preview** to proceed further.

> You will not be allowed to save the edited templates containing Blockedlisted HTML content.

Supported email variables

Ivanti Neurons for MDM offers several variables you can use to customise your email templates.

End user invitation variables

Variable	Description
$	The user activation URL - this is thehyperlink around the$ text.
$	The cluster registration URL - it is NOTfound in the default template, but isreferenced indirectly (via the$ variable).
$	The product brand name - this is defined as the <title> tag in the header of the default template.
$	The company Logo URL - this is the one image in the default template - it points to an image in the MobileIron CDN. Updating the **User Branding** settings changes the value referred by **$**.
${message:$	The register the user device title.
${message:$}	Email invitation title.
${message:$}	Verification that the user in on their device.
${message:$}	The email invitation Get Started text.
${message:$}	Login and registration instructions.
${message:$}	Email and apps pushed to the device information.
${message:$}	Registration information if the user is not on their device, which includes the cluster registration URL.
${message:$}	The email invitation footer that includes the company website label.
$	The company website label - it is NOTfound in the default template, but isreferenced indirectly (via the$ variable).

Password expiration notification variables

Variable	Description
$	The password reset URL.
$	The product brand name - this is defined as the <title> tag in the header of the default template.
$	The company Logo URL - this is the one image in the default template - it points to an image in the MobileIron CDN. Updating the **User Branding** settings changes the value referred by **$**.
${message:$}	The password expiration notification title.
${message:$}	The password expiration notification introductory paragraph.
${message:$}	The password reset URL name.
${message:$}	The email invitation footer that includes the company website label.
$	The company website label - it is NOTfound in the default template, but isreferenced indirectly (via the$ variable).

Registration confirmation variables

Variable	Description
$	The product brand name - this is defined as the <title> tag in the header of the default template.
$	The company Logo URL - this is the one image in the default template - it points to an image in the MobileIron CDN. Updating the **User Branding** settings changes the value referred by **$**.
${message:$}	The registration confirmation title.
${message:$}	The registration confirmation introductory paragraph.

Policy compliance variables

Variable	Description
$	This variable will be replaced by the content that is entered into the subject line in the send email compliance action within the policy.
$	This variable will be replaced by the content that is entered into the message portion in the send email compliance action within the policy.
$	The product brand name - this is defined as the <title> tag in the header of the default template.
$	The company Logo URL - this is the one image in the default template - it points to an image in the MobileIron CDN. Updating the **User Branding** settings changes the value referred by **$**.
${message:$}	The email invitation footer that includes the company website label.
$	The company website label - it is NOTfound in the default template, but isreferenced indirectly (via the$ variable).

Custom user attribute variables

An admin can use **custom user attributes** as email variables in the customised email template under the following conditions:

- The custom user attributes exist on the **Admin > Attributes** page.
- An admin has **assigned the custom user attributes to users**, with values given for the custom user attributes for each user.

12.10.5. Self-Service Portal

The invitation to register includes a link to the Self-Service Portal. End users can use this portal to do the following tasks:

- Lock
- Unlock
- View Location (if enabled in the **Privacy configuration**)
- Wipe
- Retire
- Change account info (name, password, email address)
- Force Check-in
- Add encryption and signing certificates

To register additional devices, end users click the registration portal link displayed in the Self-Service Portal.

If end users misplace the URL for the Self-Service Portal, send them to **https://mydevices.mobileiron.com/user/login.html**. For iOS users, consider creating a **Web Clip configuration** for the Self-Service Portal.

Uploading signing and encryption certificates

You can allow your end users to upload their email signing and encryption certificates in the Self-Service Portal within the User Provided Certificates configuration. This setting can be configured using the User Provided Certificates configuration. When configured, the end users can upload their email signing and encryption certificates.

1. In the **My Certificates** tab, click **Add Certificate**. The **Add certificate** window is displayed.
2. Update the following fields:

Field name	Description
Certificate Type	Select the type of certificate to be uploaded. The options are: • **Encryption certificate** • **Signing Certificate** These options are created from the Ivanti Neurons for MDM Admin Portal. See **Identity Certificate Configuration** for more information.
Certificate to Upload	Click **Choose File** to select the certificate file to be uploaded. Ensure that the file is in PKCS12 format.
Password	Type the password used for the file.

3. Click **Upload**.

After uploading, you can view the list of certificates in a table displaying the following details.

Field name	Description
Certificate Name	Specifies the type of certificates either **Encryption** or **Signing**.
Issued By	the details of the certificate issued.
Uploaded On	The date when the certificate was uploaded.
Expiration Date Actions	The expiry date of the certificate. You can perform the following actions: • **Edit Certificate** - edit certificate details. • **Clear Private Key** - deletes the private key from the certificate package(PKCS#12). • **Delete Certificate** - deletes the certificate from the Ivanti Neurons for MDM server.

When the user uploads a certificate configuration, the server re-pushes the configuration that is using the certificate.

> Delete and Clear private key by a user will not re-push the configurations.

For more information, see **Self-Service Portal Branding**.

12.10.6. Self-Service Portal (Branding)

Licence: Silver

You can customise the **Self-Service Portal** with your organisation's logo. If you do not add your logo, the Self-Service Portal displays the default service logo.

Branding the Self-Service Portal

Procedure

1. In the Self-Service Portal Branding screen, click **Customise** (upper right).
2. Drag the logo file (PNG, 182x34) to the dotted box, or click **Choose File** to select it from your file system.
3. Click **Save Changes**.

12.10.7. Multi User Sign-In (Webclip) Branding

Customise your multi-user secure sign-in for iOS by adding a new title and webclip icon.

Procedure

1. Go to **Admin > Multi User Sign-In (Webclip)**.
2. In the Multi User Sign-In (Webclip) screen, click **Customise**.
3. Drag the logo file to the dotted box, or click **Choose File** to select it from your file system.
4. To change the Label, edit the **Secure Sign-in** text.
5. To change the webclip icon, drag and drop the webclip file to the dotted box, or click **Choose File** to select it from your file system.
6. Preview the updates and click **Save Changes**.

For iPhone and iPod touch devices, create icons that measure 120 x 120 pixels or 60 x 60 pixels (standard resolution).

For iPad devices, create icons that measure 152 x 152 pixels or 76 x 76 pixels (standard resolution).

For more information, see **Multi-user Secure Sign-In for iOS**.

12.10.8. Organisation

You can provide branding name to the organisation or personalise system alert email subject lines by incorporating tenant-specific identifiers (e.g., customer name) into each subject. If you do not update the Organisation name, the Organisation screen will display the default value.

Branding the Organisation

Procedure

1. In the Organisation screen, enter the desired name in the **Name** field.
2. To add a prefix, click **Edit** and enable the option **Prefix the Organisation name in all system generated emails e.g., License expiry**.
3. Click **Save** to apply your changes.

12.11. Adding management of non-iOS devices

Licence: Gold

You are currently using a version of Ivanti Neurons for MDM that is optimised for iOS devices. This section describes how to switch to allow management of non-iOS devices. After switching you will also be able to manage the following devices:

- Android 5.0 or supported newer versions
- Windows 10+

Switching to include management of non-iOS devices cannot be reversed.

To switch to include non-iOS devices:

1. Click **Admin > Allowed Platforms**.
2. Click the **Allow All Platforms** button.
3. Check **I understand that this cannot be undone** to confirm that you know and understand that this operation cannot be undone.
4. Click the **Allow All Platforms** button.

13. Packages

This section contains the following topics:

- Upgrading
- Secure UEM and Secure UEM Premium packages
- Legacy Bronze, Silver, and Gold packages
  - Silver
  - Gold
  - Platinum
- Sandbox for preview or testing

Secure UEM and Secure UEM Premium packages

The Secure UEM and Secure UEM Premium packages offer the following features:

	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)		✓

These packages are subject to change. You should contact **Ivanti Sales** to confirm the current scheme.

Legacy Bronze, Silver, and Gold packages

This section describes the legacy Bronze, Silver, and Gold packages. The packaging has evolved to the **Secure UEM and Secure UEM Premium** scheme.

Bronze

Ivanti Neurons for MDM basic features are provided in the Bronze package. You can expand the Bronze package by:

- adding more devices
- adding Silver
- adding Gold

- adding Platinum

These additions expand your mobile solution beyond basic device configuration.

Administrators can contact **Support** if they are interested in enabling one or more of the **On-demand features** on their tenant(s) that are disabled by default.

Silver

Upgrading to Silver adds the following features:

- **LDAP and Connector:** Support for adding corporate directories and certificate authorities to Ivanti Neurons for MDM.
- **Sentry:** Support for email access control.
- **Spaces:** Support for designating devices for management by different administrators (delegated administration).
- **Supervised mode:** Device-level support for fine-grained configuration, including single-app mode.
- **Self-Service Portal branding:** Use your logo in the Self-Service Portal.
- **Certificate Authorities:** Use Ivanti Neurons for MDM as a certificate authority.
- **Silent app install/uninstall:** Automatically deploy and remove apps from a mobile device.
- **App Allowlist/Blockedlist/required apps:** Monitor and control which apps are installed on devices.
- **Web content filter:** Apply website Allowlist/Blockedlist policies to all web browsers.
- **Apple-specific functionality:** Enable/restrict AirPlay, AirDrop, iOS wallpaper distribution, and Apple TV.
- **Open-in management:** Control which mobile apps can open what enterprise content.
- **Apple Apps and Books:** Distribute mobile app licences to devices, and reclaim and reassign those licences when a device is retired.
- **Android Enterprise (Android for Work) support**
- **Device Enrollment:** Enables customers to purchase devices in bulk and automatically enroll Apple devices in MDM during activation.
- **Per-App Configuration:** Deploy configured mobile apps at scale, with little to no required action by the end user.
- **3rd-party Per-App VPN:** VPN security is now immediate, invisible, and specific to the mobile app.
- **Policy Tiered Actions**
- App Distribution Filters
- **Audit Trails**
- **Android Kiosk mode:** Support for configuring Android devices to operate in kiosk mode.
- **Android Kiosk branding:** Change the background and banner of the kiosk screen displayed when device operate in kiosk mode.
- **Office 365 Data Loss Prevention (DLP) Using Microsoft Graph APIs**: Enforces DLP controls for Office 365 apps via Graph APIs.

Gold

Upgrading to Gold adds the features provided by Silver as well as the following features:

- **Single sign on:** Users authenticate once and are automatically logged in to other enterprise mobile apps.
- **iOS and Android App Catalog custom branding:** Display your company logo in the app catalog.
- **Increased content limit:** 50 files, 25 MB each

- **AppConnect for iOS:** Secure and configure AppConnect-enabled apps.
- **AppTunnel for iOS:** Secure app access to enterprise resources.
- **Docs@Work for iOS:** Enable users to view, store, and share documents.
- **iOS 8 certificate-based single sign on**
- **iOS 8 iBook/ePub management**
- **macOS support**
- **User branding**
- **Mobile Application Management (MAM) with AppConnect**
- **Derived Credentials**
- **Windows 10 (includes Bridge) support**

Platinum

Upgrading to Platinum adds the features provided by Gold as well as the following features:

- **Tunnel:** Configure app-specific access to enterprise data.
- **Help@Work**
- **Monitor**
- **ServiceConnect (ServiceNow, Splunk)**

Sandbox for preview or testing

Ivanti Neurons for MDM customers can get a sandbox tenant to preview and test new releases before they hit production when **Premium Plus** support is purchased.

13.1. Upgrading

This section contains the following topics:

- Upgrading a licence
- Requesting an upgrade
- Upgrading from a previous release

Upgrading a licence

The basic features are provided in the Bronze package. You can expand the Bronze package by:

- adding more devices
- adding Silver
- adding Gold
- adding Platinum

These additions expand your mobile solution beyond basic device configuration.

Requesting an upgrade

Procedure

1. Select **Upgrade Options** from the admin drop-down menu.
2. Click **Request Upgrade / Add Devices** (upper right).
3. Select the items you want to add and enter your phone number.

A representative will contact you in about 24 hours with details.

Upgrading from a previous release

When upgrading from a previous release, the settings on the **Edit Device Enrollment Profile** page are not preserved. Note your option settings before upgrading.

- If **Skip signing in to AppleID and iCloud** is enabled before upgrading, then **Skip Apple Pay setup** will be enabled after upgrading.
- If **Skip entering passcode** is enabled before the upgrade, then **Skip Touch ID** and **Skip Apple Pay setup** will be enabled after the upgrade.

Procedure

1. After the upgrade is complete, return to the **Edit Device Enrollment Profile** page to edit the Device Enrollment profile to restore the desired settings.
2. Click **Save**.

After upgrading several configuration settings are affected.

- Promotion options are set to **Off**.
  Installation settings are set to **No**.
  Don't Show in App Catalog option is no longer selected.
  Silent Install on Android Samsung Knox is set to False.

iOS Management Flags are set to:

- Backup to iCloud.
- Remove on enrolment.

Note: These iOS Management flag settings can be selected for each app individually.

App settings:

- App settings are now called Configurations.
- All other app settings remain as they were prior to the upgrade.

For more information, see **Packages**.

14. Device Licences

Ivanti Neurons for MDM device-based licenses define the number of devices you can register, the amount of content you can configure for distribution to devices, and which features are available. If you reach your limit for devices, a red triangle displays in the Admin page. If you reach your limit for content, the service will prevent you from adding more and display a message to indicate that you have reached your limit.

14.1. Tenant Suspension

Access to a tenant used with an evaluation license or a production license might be suspended by Ivanti Neurons for MDM. An Evaluation Licence might be suspended when the evaluation period expires or when the usage allowance has been exceeded. A Production License might be suspended when the subscription period expires or when the usage allowance has been exceeded. Ivanti Neurons for MDM will restore a suspended tenant when the license has been renewed or when additional licenses have been purchased, in case of an overage.

When a tenant licence is suspended:

- Existing registered devices continue to function normally.
- Administrators cannot log in to the Admin portal.
- New devices cannot be registered.
- API access to the tenant is blocked.
- End users can continue to access the Self-Service portal.

Tenant Suspension Action and Error Messages

Suspension Action	Error	Error message displayed	Location
End Customer-integration API access is blocked.	API Call fails.	Access denied. Your Evaluation Licence has expired. Please renew your licence to re-enable API access. Contact your System Administrator for details.	API error 401.
New devices are blocked from registering.	An error message is displayed on the enrolment screen.	Unable to register your device. The licence for your system has expired. Please contact your system administrator for details. Previously enrolled devices will continue to operate normally.	Following password verification.
Administrator is blocked from logging in to the Admin portal.	An error message is displayed on the login screen.	Unable to login. Your Licence has expired. Please renew your licence to regain access to the Admin Portal and to enrol new devices. Devices that have been previously enrolled devices will continue to operate normally. Contact your sales representative to renew your licences. Note that the Admin password expires after one year (365 days).	Following password verification.

15. Opening a Support Ticket

Visit the **Ivanti Support Portal** to open a support ticket.

16. Third-Party Attributes

Ivanti Neurons for MDM includes components developed by third parties. You can view the list **here**.

17. Apps@Work

Starting from Ivanti Neurons for MDM release 83, you can transition to Apps@Work native experience from Go application. For newly created tenants the Apps@work Webclip configuration is not distributed by default for iOS devices that are installed through iReg or client. The administrator has to manually distribute the webclip config to the devices that are registered through iReg or client. Note the following points:

Ivanti Neurons for MDM **administrative portal**:

- By default, only new tenants get the App Catalog for Native Client configuration distributed to iOS devices.
- For existing tenants, by default, the Apps@Work Native application is not distributed.
- The administrator must push the App Catalog for Native Client configuration to the devices to make Apps@Work available in a Native Appstore experience.

Client:

- Go application now displays a tab for Apps@Work.
- The App Catalog for Native Client configuration has the App Catalog Identity for Native Client certificate and App Station identity certificate. Ivanti Neurons for MDM pushes the certificates with the App for Native Client configuration.

Apps@Work Features

The Apps@Work tab has the following features:

- Access Apps@Work tab from the Go application
- Search
- Installing an app - Button States
- Featured Applications and Banner
- Application Update Notification
- Application Update Notification

Access Apps@Work tab from the Go application

- A new tab is added in Go app for Apps@Work.
- Two default tabs are available in Apps@Work-All Apps and Categories.
- All Apps tab lists all the apps in an alphabetical order.
- Categories tab displays only the categories that have any applications in it.
- Each category displays the number of applications present in it.
- MyApps under Categories is a list item that contains all the installed applications. MyApps will always be the first category and the rest of the categories are listed alphabetically.
- When no applications are installed the MyApps list displays None.
- When you click on a category, all the applications that are specific to the category are listed with the Install option. The wizard lets you install each application individually or you can click Install All to install all the applications in the category. You will be prompted to permit the installation for each application.

Search

- Tap the search (lens) icon to search for the following:
  - New Releases-a list of newly released apps appears when no text is typed in the search bar
  - Type any text and the search field will dynamically predict and display the matching applications.
  - The search result count is displayed as a sub-heading
  - You can tap the Install button to install an applicaiton without navigating to the details page.

Installing an app - Button States

- Since the app installation requires the server to process the request and push the app down to the device, the install button will not display the progress in real-time
- The install button changes states from Install > Requested > Installed.
- An alert message appears, for the first time, indicating that an installation is requested.
- The alert also appears when you tap the "Requested" button.
- The Installed status is not a button.

Featured Applications and Banner

- The Featured tab is visible based on administrator configuration.
- The Featured tab is the default landing page when no updates are available.
- The Featured App Banner displays one application in the banner.
- The Featured App contains a list of all the featured applications.

Application Update Notification

- Go sends a notification when any application updates are available. The notification does not display the name of the application.
- If you tap the application update notification, you will be redirected to the All Apps page in Apps@Work.
- In the Go application, the Apps@Work tab icon displays a badge count of number of applications that have pending updates.
- In the Apps@Work tab, the Updates Available sub-section appears under the All Apps tab and displays the count of the applications that are available for update.
- A red dot icon is displayed for every application that requires an update.

Settings-My Devices

- The My Devices tab is now moved under Settings.
- If you tap the application update notification, you will be redirected to the All Apps page in Apps@Work.
- In the Go application, the Apps@Work tab icon displays a badge count of number of applications that have pending updates.
- In the Apps@Work tab, the Updates Available sub-section appears under the All Apps tab and displays the count of the applications that are available for update.
- A red dot icon is displayed for every applicaiton that requires an update.

18. Enable Kerberos Authentication between Ivanti Neurons for MDM and SCEP server

You can use Kerberos authentication to communicate between Ivanti Neurons for MDM and SCEP. The following sections discuss how to enable Kerberos authentication on SCEP servers and Ivanti Neurons for MDM.

> This feature will be functional when Ivanti Neurons for MDM Connector 93 version is available.

Pre-configuration steps

1. Check which service account is in use for the SCEP service on the SCEP server.
2. On the SCEP server, check that the service account is a member of the local IIS_USRS group.
3. On the CA server certificate template that is being provisioned, check that the service account has enroll permission.

Configuring Windows servers

1. Run the following command on a domain controller:
   setspn -s http/<SCEP-SERVER-FQDN> <domain>\<service account>
2. In **Active Directory Users and Computers**, click the **Delegation** tab of the service account:
   1. Under **Trust this user for delegation to specified services only**, select **Use Kerberos only**.
   2. Click **Add** and add the SCEP server name.
   3. Select the HTTP service.
   4. Click **OK**.
3. Do the following on the IIS server to make sure that Application Pool credentials are used to decrypt Kerberos tickets:
   1. Check that the SCEP Application Pool is running under the service account that you verified earlier.
   2. To enable useAppPoolCredentials, on the Microsoft SCEP Admin (mscep_admin) or Microsoft SCEP (mscep) webpage, select **Configuration Editor > System.webServer > Security > Authentication > Windows Authentication** and set the value to useAppPoolCredentials=True.
4. Disable **Anonymous Authentication** on the Microsoft SCEP Admin webpage (mscep_admin) by selecting **Authentication > Anonymous Authentication** and click **Disable**.
5. Disable Kernel mode authentication in the Windows authentication advanced settings.

> Make sure to use **Negotiate** as the first option in the authentication service.

6. Disable Kernel mode authentication in the Windows authentication advanced settings webpage.
7. Restart the IIS service.

Configuring Kerberos

This section discusses how to configure Kerberos on Ivanti Neurons for MDM server.

Configuring Kerberos settings in Ivanti Neurons for MDM

Navigate to **Admin > Infrastructure > Kerberos**, enter the following setting as given in the table:

UI Section	Choice
Active Directory's Kerberos Realm	IVANTI.COM
Corresponding Key Distribution Centre (KDC) server	kdc.ivanti.com
Service user credentials	user@realm For example: serviceuser@IVANTI.COM
Domains for outbound communication with Microsoft AD Certificate Services (hostnames are not case sensitive and must end with .ivanti.com or .IVANTI.COM) SCEP or NDES server: You can also use hostnames, such as: ndes.ivanti.com or scep.ivanti.com	

Enabling Kerberos authentication on the Microsoft SCEP Certificate Enrollment configuration on an existing certificate authority

Perform the following steps to enable Kerberos authentication on an existing certificate authority:

1. In Ivanti Neurons for MDM, select **Admin > Infrastructure > Certificate Management**.
2. Select the certificate authority type with the **External** option.

> These external certificate authority types should denote as Microsoft.

3. From the **Actions** drop-down, select **Edit**.
4. In the **Edit External CA** window, select the checkbox **Prefer Kerberos authentication** to enable Kerberos authentication.

Enabling Kerberos authentication on the Microsoft SCEP Certificate Enrollment configuration on for a new certificate authority

Perform the following steps to enable Kerberos authentication for a new certificate authority:

1. In Ivanti Neurons for MDM, select **Admin > Infrastructure > Certificate Management**.
2. Select the **+Add** option.
3. In the **Add Certificate Authority** window, select **Connect to an on-premises SCEP Certificate Authority** option.
4. Click Continue.
5. In the **Add an External Certificate Authority** window, perform the following steps:
    1. Select the **Microsoft** option from the **Certificate Authority Type** drop-down.
    2. Select the checkbox **Prefer Kerberos authentication** to enable Kerberos authentication.
    3. Fill in all the required fields.
    4. Click **Done**.

19. Ivanti Neurons for MDM Administrator Guide

September 2026

A modern approach to mobile security, Ivanti Neurons for MDM provides unified endpoint management (UEM) solutions in a highly scalable, secure, and easy to update infrastructure that supports millions of devices around the world.

{{If your language is unavailable}}

New features summary

View as PDF

Videos

20. Welcome

21. Welcome CSH

22. Windows Update Management

As an administrator, you can view and approve the updates reported by Windows devices that you want to be updated using Windows Update Management. By using this feature you can prevent unnecessary or untested updates from being installed in devices.

Update Management feature requires devices to be configured with **Software Updates** configuration with **Require update approval** option enabled. Only by applying this configuration to the devices, the devices report updates for installation and wait for approval.

Managing updates

1. Go to the **Admin>Windows Updates**. The following details of the updates are displayed in the page.
   Creation Date: The date when the update was created.**Title**: Describes the type of update along with the Knowledge Base article number.

> When clicked on the update, the description is displayed.

Classification: Classifies the type of update into one of the following categories:

- Critical Updates
- Definition Updates
- Driver Updates
- Security Updates
- Updates
- Upgrade
- Update Rollups

Distribution: The distribution performed for the update. For example, it display **All** when the update is distributed to all the devices.

> If the update is distributed to a certain specific number of groups, it displays the count of the distribution. For example, it displays 3 if the distribution is performed only to 3 groups.

2. In addition, you can view if an update has been distributed to the required devices or not. The following columns have numbers that indicate the number of devices present under different category of the updates:
   - Eligible devices
   - Installed devices
   - Failed devices
   - Reboot pending devices

When you click on any of these numbers, you will be directed to the filtered view on the Devices page to know the status of updates and perform the required actions.
Review the updates and select the update that you would like to distribute to the devices by clicking the check-box for the update.

3. Under **Actions**, click **Set Distribution**.
4. In the **Distribute Windows Update** window, select any of the following distribution options:
   All Devices: Distributes the updates to all the devices.
   No Devices: Withholds the updates to be distributed to devices**Custom**: Distributes the updates for the specified device groups.

5. Click **Save**.

Searching and filtering updates

You can search and filter updates based on the following criteria:

- Knowledge base article ID
- Configured distribution

Filtering based on Knowledge base article ID:

1. In the **Windows Update Management** page, type the Knowledge base ID in the quick search field(only the number in the Search field.
   Example: For KB4056892, type 4056892. The update that matches with the search criteria is displayed on the page.

> You can further look for additional information on the update by clicking **Support** and **More Information** link. The **Support** links to the Microsoft web page that provides product support information for the update and the **More Information** links to the Microsoft web page that displays more information on the update, such as the Knowledge Base article.

Filtering based on configured distribution:

In the **Windows Update Management** page, select any of the following filtering options based on the configured distribution:

- **All**: Displays all the updates.
- **Configured**: Displays the list of updates that are distributed to devices.
- **Unconfigured**: Displays the list of updates for which the distribution is not specified.

> Configured and Unconfigured filters are based on the distribution performed and the distribution can also be **None**.

Viewing updates for a device

To view the detailed update information specific to a device:

1. Go to **Devices > Devices**.
2. Click a device name to view the details page.
3. Go to **Updates** tab. The updates for the device that are pending (update approved by the admin but not reported as installed on the device), failed, and installed are displayed.

> You can also see notifications about new Windows updates available in the Notifications page under Dashboard. The notification includes creation date of the notification, number of notifications available and the purpose of the notification. The Windows update notification is also visible in the top right corner of the Admin Portal.