ivanti

NMDM Admin Guide DE

ivanti

CONTENTS

1. **Wissenswertes über Ivanti Neurons for MDM** **9**
2. **Zusammenfassung der neuen Funktionen** **10**
3. **Videos** **14**
4. **Erste Schritte** **17**
   - 4.1. macOS-Geräte konfigurieren 24
   - 4.2. Registrierungsbestätigungs-E-Mails konfigurieren und verwenden 27
   - 4.3. Benachrichtigungs-E-Mails zur Einhaltung von Richtlinien konfigurieren und verwenden 28
   - 4.4. Bei Bedarf abrufbare Funktionen. 29
   - 4.5. Vorbereiten der Android Enterprise-Geräteunterstützung 32
5. **Dashboard** **33**
   - 5.1. Arbeiten mit Widgets 34
   - 5.2. App-Einblicke 40
   - 5.3. Verwendung geplanter Berichte 45
   - 5.4. Anpassbare Berichte verwenden 52
6. **Benutzer** **60**
   - 6.1. Benutzer hinzufügen 61
   - 6.2. Benutzergruppen 65
   - 6.3. Benutzereinstellungen 70
   - 6.4. Benutzer-Branding 81
   - 6.5. Benutzerregistrierung mit Apple Business Manager 82
   - 6.6. Benutzerlizenzen 91
   - 6.7. Benutzer verwalten 92
     - 6.7.1. Hinzufügen eines App-API-Benutzers für Cisco ISE Operations 93
     - 6.7.2. Zuweisen von Rollen an Benutzer 94
     - 6.7.3. Benutzerrollen 96
     - 6.7.4. Benutzer suchen und filtern 99
     - 6.7.5. Benutzer zu Benutzergruppen zuordnen 102
     - 6.7.6. Benutzer einladen 103
     - 6.7.7. Aktivieren und Deaktivieren von Benutzern 104
     - 6.7.8. Mehrere Administrator-Anmeldungen verwalten 106
     - 6.7.9. Passwort ändern 107
     - 6.7.10. Nachricht senden 109
     - 6.7.11. Benutzer aus Benutzergruppen entfernen 111
     - 6.7.12. Benutzer löschen 112
     - 6.7.13. Exportieren der Benutzer 113
     - 6.7.14. Angepasste Attribute Benutzern zuweisen 114
     - 6.7.15. Anpassbare Attribute für Benutzer entfernen 115
     - 6.7.16. Benutzer-Regionaleinstellung ändern 116
     - 6.7.17. Bearbeiten eines Benutzernamens 117
     - 6.7.18. Opting-Out von der Sammlung von Standortdaten 118
     - 6.7.19. Informationen zum Timeout 119
     - 6.7.20. Systemnutzungsanalyse deaktivieren 120
     - 6.7.21. Geräteregistrierung durch PIN-Generierung 121
7. **Geräte** **122**
   - 7.1. Erste Schritte mit der Geräten 123
   - 7.2. Gerätegruppen 138
   - 7.3. Nicht verwaltete Geräte 144
   - 7.4. App-Inventar 145
   - 7.5. Verwalten von Geräten 148
     - 7.5.1. Bereitstellen von Apple-Geräten 150
     - 7.5.2. Bereitstellen von Windows-Diensten 159
     - 7.5.3. Apple Remote Desktop auf macOS-Geräten aktivieren 163
     - 7.5.4. Geräteregistrierung (iOS, macOS und Android) 164
     - 7.5.5. Geräteregistrierung (Windows 10+-PC und Microsoft HoloLens 2) 168
     - 7.5.6. Local Admin Password Solution (LAPS) 171
     - 7.5.7. Bereitstellungspaketregistrierung mit PIN 173
     - 7.5.8. Verwenden der Massenregistrierung für Windows-Geräte 177
       - 7.5.8.1. Ivanti Massenregistrierung 179
     - 7.5.9. Passworteinstellungen ändern 181

7.5.10. Den Gerätenamen ändern ... 182
7.5.11. Suchen nach und Filtern von Geräten ... 183
7.5.12. Geräteeigentümer verwenden ... 186
7.5.13. Verwaltetes Gerät mit Arbeitsprofil ... 193
7.5.14. Verwendung der Massenregistrierung für Android ... 194
7.5.15. Massenregistrierung mit CSV-Dateiupload ... 197
7.5.16. Device_to_User_BulkEnrollment ... 200
7.5.17. Verwendung der mobilen Registrierung von Samsung Knox ... 201
7.5.18. Registrieren von Oculus-Geräten ... 205
7.5.19. Bluetooth auf einem Gerät aktivieren ... 208
7.5.20. iOS-Update planen ... 209
7.5.21. Installieren Sie die iOS System-Apps neu. ... 210
7.5.22. Zuweisen eines neuen Benutzers für ein Gerät ... 211
7.5.23. Neuzuweisen eines Android-Geräts ... 212
7.5.24. Erzwingen einer Geräteanmeldung ... 213
7.5.25. Lokalisierung eines Geräts ... 214
7.5.26. Gerät sperren ... 215
7.5.27. Verwalten von Apple-Geräten im Verloren-Modus ... 216
7.5.28. Verwalten von Android-Geräten im Verloren-Modus ... 218
7.5.29. Debug-Protokolle anfordern ... 220
7.5.30. Apple_Enhanced_Logging ... 221
7.5.31. Gerät außer Dienst stellen ... 222
7.5.32. Verzichten auf Gerätebesitz ... 223
7.5.33. Gerät „wipen“ ... 224
7.5.34. Löschen von Geräten ... 226
7.5.35. Gerät entsperren ... 227
7.5.36. Geräte neu starten und herunterfahren ... 229
7.5.37. Passwort-Einschränkungen löschen (nur iOS) ... 231
7.5.38. Sentry-Zuordnung für ein Gerät löschen ... 232
7.5.39. Anpassbare Attribute für Geräte zuweisen ... 233
7.5.40. Anpassbare Attribute von Geräten entfernen ... 234
7.5.41. App-Feedback synchronisieren und abrufen ... 235
7.5.42. Definition des Firmware-Passworts ... 237
7.5.43. Neuen persönlichen Wiederherstellungsschlüssel ausstellen ... 238
7.5.44. Wiederherstellungssperre einstellen oder ändern ... 240
7.5.45. Apple-Zugriffsverwaltung ... 241
7.5.46. Registrierung über Gruppenrichtlinie ... 242
8. Apps ... 243
8.1. App-Katalog ... 244
8.2. App-Verwaltung mit DDM (deklarativer Geräteverwaltung) ... 264
8.2.1. Einstellungen für DDM-App-Verwaltung ... 266
8.3. Apps@Work (iOS, Android, Windows und macOS) ... 269
8.4. iOS Apps@Work AppStore-Funktionen ... 272
8.5. iOS Go – Erweiterte Funktionen ... 275
8.6. Anzeige der App-Details ... 282
8.7. App-Konfiguration ... 285
8.8. Zuweisen benutzerdefinierter Attribute zu Apps ... 302
8.9. Verwaltete Konfigurationen für Android ... 304
8.10. Verwaltung von Google Play-Apps ... 310
8.11. Löschen von Apps aus dem App-Katalog ... 312
8.12. Upgrading von hauseigenen Apps ... 313
8.13. Suche des Paketnamens für eine Android App ... 314
8.14. Kategorien ... 315
8.15. Verteilungsfilter ... 316
8.16. Ausschließen oder Verteilen von Apps ... 319
8.17. Rezensionen ... 320
8.18. Apple Apps and Books ... 322
8.19. Katalogeinstellungen ... 332
8.20. App-Abhängigkeiten bereitstellen ... 335
8.21. Bereitstellen von Divide Productivity mit Android Enterprise ... 338
8.22. Konfiguration der Provisioner-App ... 341
8.23. Verwalten von Windows-Anwendungen ... 343

8.24. Ivanti Bridge ... 346
9. Inhalt ... 351
9.1. Inhalte verwalten ... 352
9.2. Kategorien ... 354
10. Konfigurationen ... 355
10.1. Arbeiten mit Konfigurationen ... 356
10.2. Konfiguration für das Benutzer-Selbstbedienungsportal erstellen ... 369
10.3. Anpassbare Konfiguration ... 371
10.4. Übertragen von SyncML via Push auf Geräte mit benutzerdefinierten Konfigurationen ... 373
10.5. Konfiguration des Startbildschirm-Layouts ... 374
10.6. Konfiguration der App-Kontrolle: Kontrolle der Apps, die auf dem Gerät installiert sind ... 376
10.7. App-Benachrichtigungen - Konfiguration ... 378
10.8. Export von Konfigurationen ... 380
10.9. Prioritätenvergabe für Konfigurationen ... 381
10.10. Konfigurationen verwalten ... 382
10.10.1. Konfigurationstypen ... 383
10.10.2. Variablen ... 399
10.10.3. AppConnect-Konfigurationen ... 404
10.10.3.1. Übersicht über AppConnect ... 405
10.10.3.2. AppConnect-Passcode ... 406
10.10.4. Sicherheitskonfiguration ... 408
10.10.4.1. Android Enterprise ... 410
10.10.4.2. Apple PassKeys-Bescheinigung ... 413
10.10.4.3. Standardeinstellungen für App-Datenschutz ... 414
10.10.4.4. Bearbeiten der Android Enterprise-Standardkonfiguration ... 417
10.10.4.5. Einrichten von Android Enterprise ... 419
10.10.4.6. Android Enterprise: Work Managed-Gerät, nicht GMS-Modus (AOSP) ... 426
10.10.4.7. Android Work Challenge ... 427
10.10.4.8. Zertifikatskonfiguration ... 432
10.10.4.9. Zertifikatstransparenz ... 434
10.10.4.10. Konfiguration der Zertifikatswiderrufsprüfung ... 435
10.10.4.11. Erstellen einer Konfiguration für den autonomen Einzel-App-Modus ... 436
10.10.4.12. Erstellen der DNS-Proxykonfiguration ... 437
10.10.4.13. Konfigurieren der Geräteprotokollierung ... 438
10.10.4.14. Konfiguration "Datenträgerverwaltung" ... 440
10.10.4.15. Android-Verschlüsselung ... 441
10.10.4.16. Verschlüsselter DNS ... 442
10.10.4.17. Externe Intelligence-Einstellungen ... 445
10.10.4.18. Bedrohungsabwehr ... 446
10.10.4.19. FileVault 2 ... 447
10.10.4.20. FileVault-Wiederherstellungsschlüssel ... 448
10.10.4.21. Konfiguration der FileVault-Optionen ... 449
10.10.4.22. Identitätszertifikat ... 450
10.10.4.23. Konfiguration der iOS-Aktivierungssperre ... 457
10.10.4.24. Individuelle iOS-Konfiguration ... 461
10.10.4.25. Intelligence-Einstellungen ... 462
10.10.4.26. iOS-Einschränkungen ... 465
10.10.4.27. Konferenzraum-Anzeige ... 486
10.10.4.28. Tastatureinstellungen ... 487
10.10.4.29. Sperre & Kiosk: Android-Geräte Administratormodus ... 489
10.10.4.30. Konfiguration des Kiosk-Modus für Android ... 492
10.10.4.31. Kiosk für unter Android freigegebenes Gerät konfigurieren ... 494
10.10.4.32. Sperre & Kiosk: Android Enterprise ... 495
10.10.4.33. Sperre & Kiosk-Modus: Samsung Knox Standard ... 523
10.10.4.34. Konfiguration "Local Administrator Password Solution" ... 527
10.10.4.35. macOS-Firewall ... 528
10.10.4.36. Einschränkungen für macOS ... 530
10.10.4.37. macOS AppStore-Einschränkungen ... 537
10.10.4.38. Beschränkungen beim Brennen von CDs/DVDs in macOS ... 538
10.10.4.39. Kontrolle zulässiger Medien (zurückgestuft) ... 539
10.10.4.40. Einstellungen für macOS Finder ... 543
10.10.4.41. Erweiterungsrichtlinie für den macOS Kernel ... 544

10.10.4.42. Mobile@Work für macOS ... 545
10.10.4.43. Konfiguration der Update-Regeln für macOS Software ... 551
10.10.4.44. Zertifikatspräferenz ... 552
10.10.4.45. Active Directory (macOS) ... 553
10.10.4.46. Identitätspräferenz ... 556
10.10.4.47. Automatische Kontoerstellung für Office 365 (macOS) ... 557
10.10.4.48. Authentifizieren ... 559
10.10.4.49. Apple App-Katalog ... 561
10.10.4.50. Verwaltete Domänen ... 562
10.10.4.51. Passwortkonfiguration ... 563
10.10.4.52. Datenschutzpräferenz (macOS) ... 567
10.10.4.53. Datenschutzeinstellungen ... 569
10.10.4.54. Informationen zur Datenschutzerklärung für Kunden ... 572
10.10.4.55. Einstellungen für Ivanti Go-Client ... 573
10.10.4.56. Siri-Einstellungen ... 575
10.10.4.57. Konfiguration "Dienstkonfigurationsdateien" ... 577
10.10.4.58. [Software Updates] ... 579
10.10.4.59. Konfiguration "Einstellungen für Softwareupdate" ... 586
10.10.4.60. Konfiguration der Sicherheitspräferenzen ... 590
10.10.4.61. Zeitserver ... 591
10.10.4.62. Web-Content-Filter ... 592
10.10.4.63. Windows-Firewall ... 595
10.10.4.64. Schutz von Windows-Informationen ... 598
10.10.4.65. Windows-Einschränkungen ... 603
10.10.4.66. Einschränkungen für Windows Desktop ... 609
10.10.4.67. Desktop-Einstellungen für Windows 10 ... 612
10.10.4.68. Konfiguration von Windows Hello for Business ... 614
10.10.4.69. Konfiguration "Windows KI-Verwaltung" ... 615
10.10.4.70. Play Integrity (ehemals SafetyNet-Bestätigung) ... 617
10.10.4.71. Erweiterter Android-Passcode und Sperrbildschirm ... 618
10.10.4.72. Microsoft Defender for Endpoint ... 619
10.10.4.73. Zertifikat-basierte Authentifizierung ... 620
10.10.5. Konfigurationen für Benutzerressourcen ... 622
10.10.5.1. CalDAV-Konfiguration ... 623
10.10.5.2. CardDAV-Konfiguration ... 624
10.10.5.3. Google-Konfiguration ... 625
10.10.5.4. E-Mail-Konfiguration ... 627
10.10.5.5. Konfiguration von Exchange ... 631
10.10.5.6. Schriftkonfiguration ... 635
10.10.5.7. Konfiguration für abonnierte Kalender ... 636
10.10.5.8. Erstellen einer Web-Clip-Konfiguration ... 637
10.10.5.9. Installation von Office 365 ... 639
10.10.5.10. Windows GPO-Einstellungen ... 641
10.10.5.11. Konfiguration der BitLocker-Verschlüsselung ... 643
10.10.6. Konfiguration des Unternehmensnetzwerkzugangs ... 648
10.10.6.1. AirPlay-Konfiguration ... 649
10.10.6.2. AirPrint-Konfiguration ... 650
10.10.6.3. Always-on VPN – Konfiguration ... 651
10.10.6.4. Standard-App-Runtime-Berechtigungen ... 655
10.10.6.5. Bildung ... 657
10.10.6.6. Globale Proxy-Konfiguration ... 658
10.10.6.7. Globale Proxykonfiguration (Android) ... 659
10.10.6.8. LDAP-Konfiguration ... 660
10.10.6.9. Konfiguration des macOS Servers ... 661
10.10.6.10. Tunnel ... 662
10.10.6.11. AppTunnel konfigurieren ... 663
10.10.6.12. Per-App VPN-Konfiguration ... 669
10.10.6.13. Single Sign-On-Konfiguration ... 680
10.10.6.14. Netzwerkrelais-Konfiguration ... 692
10.10.6.15. Sichere Anmeldung für mehrere Benutzer in iOS ... 694
10.10.6.16. Konfiguration der Android-APN-Einstellungen ... 697
10.10.6.17. VPN-Konfiguration ... 701

10.10.6.18. VPN-on-Demand ... 713
10.10.6.19. WLAN-Konfiguration ... 722
10.10.7. Konfiguration des Mobilfunknetzes ... 731
10.10.7.1. APN-Konfiguration ... 732
10.10.7.2. Mobilfunk ... 733
10.10.7.3. Konfiguration "Privates Mobilfunknetz" ... 736
10.10.7.4. Konfiguration für iOS Telecom-Voreinstellungen ... 737
10.10.7.5. Erweiterte 5G-Network-Slicing-Konfiguration ... 738
10.10.7.6. eSIM-Konfiguration ... 740
10.10.8. Andere Konfiguration ... 743
10.10.8.1. Konfiguration verknüpfter Domänen ... 745
10.10.8.2. Konfiguration der Android-Dateiübertragung ... 746
10.10.8.3. Apple TV-Konfiguration ... 750
10.10.8.4. AirPlay Spiegelung ... 751
10.10.8.5. Browser-Einstellungen ... 753
10.10.8.6. Konfiguration des Single-App-Modus für iOS ... 756
10.10.8.7. iOS-MDM-Profil definieren ... 759
10.10.8.8. Konfigurieren eines iOS-MDM-Profils ... 761
10.10.8.9. Content-Caching ... 762
10.10.8.10. Erstellen einer Android-Tastenkombination ... 766
10.10.8.11. Erstellen von Konfigurationen für Einstellungen für Barrierefreiheit ... 767
10.10.8.12. Erstellen der Konfiguration für den Bildschirmschoner ... 770
10.10.8.13. Bildschirmschoner des Benutzers konfigurieren ... 771
10.10.8.14. Einstellungen für den Gerätenamen ... 772
10.10.8.15. Gerätehintergrundkonfiguration ... 773
10.10.8.16. EMA Server-Integrationskonfiguration ... 776
10.10.8.17. Energiesparkonfiguration ... 777
10.10.8.18. Ethernet-Konfiguration (macOS) ... 783
10.10.8.19. Google BeyondCorp-Konfiguration ... 787
10.10.8.20. Sperrbildschirm-Nachricht - Konfiguration ... 791
10.10.8.21. Konfiguration des Anmeldefensters – macOS ... 793
10.10.8.22. macOS Systemerweiterungskonfiguration ... 794
10.10.8.23. MAM-Only ... 795
10.10.8.24. Verwaltete Google Play-Konfiguration ... 797
10.10.8.25. Einstellungen für den Migrationsassistenten ... 798
10.10.8.26. Konfiguration "Benachrichtigungen" ... 800
10.10.8.27. Druckereinstellungen ... 801
10.10.8.28. Bloatware-Konfiguration entfernen ... 803
10.10.8.29. Konfiguration "Safari-Erweiterung und -Einstellungen" ... 804
10.10.8.30. Konfiguration der Samsung Mobiltelefon-Einschränkungen ... 808
10.10.8.31. Konfiguration "Standardbrowser" – iOS und visionOS ... 809
10.10.8.32. Konfiguration "Hosteinstellungen für Bildschirmfreigabe" ... 810
10.10.8.33. Single App Mode-Konfiguration ... 812
10.10.8.34. Konfiguration der Empfehlungskadenz für Softwareupdates ... 815
10.10.8.35. Startmenü und Taskleiste ... 816
10.10.8.36. Konfiguration der Systemaktualisierung ... 819
10.10.8.37. Updateverwaltung unter Windows 10 ... 824
10.10.8.38. Zeitplanung von Windows Apps ... 827
10.10.8.39. Windows BIOS-Konfiguration ... 828
10.10.8.40. Windows BitLocker ... 836
10.10.8.41. Windows Kiosk-Konfiguration ... 837
10.10.8.42. Konfiguration der Windows-Lizenz ... 842
11. Richtlinien ... 843
11.1. Arbeiten mit Richtlinien ... 844
11.2. Anpassbare Richtlinie ... 850
11.3. Zulässige Apps überwachen und kontrollieren ... 874
11.4. Prioritäten für Richtlinien ... 882
11.5. Windows-Hardwarerichtlinie ... 883
12. Administrator ... 884
12.1. [System] ... 885
12.1.1. Attribute ... 886
12.1.2. Einstellungen für die Gerätebereinigung ... 893

12.1.3. DSGVO-Profile 899
12.1.4. Benachrichtigungs-E-Mails 901
12.1.5. Rollenverwaltung 902
12.1.6. Räume 910
12.1.6.1. Räume 911
12.1.6.2. Spaces verwalten 913
12.1.6.3. Beispiele für Spaces 918
12.1.6.4. Geräte delegieren 920
12.1.6.5. Apps delegieren 921
12.1.7. Support-Administratoren 923
12.1.8. Administrator > Benachrichtigung zur Systemnutzung 924
12.2. Infrastruktur 926
12.2.1. Zugriff 927
12.2.2. App-Listen 928
12.2.3. Audit-Protokolle exportieren 929
12.2.4. Zertifikatsverwaltung 932
12.2.5. SCEP-Konfiguration für externe Zertifizierungsstellen 940
12.2.6. Anbieter abgeleiteter Anmeldeinformationen 942
12.2.7. Connector 943
12.2.8. Der Befehl httpproxy für den Connector 946
12.2.9. Help@Work 947
12.2.10. Infrastruktur-Identität 950
12.2.10.1. Identity Provider konfigurieren 951
12.2.10.2. Benutzerbereitstellung mit SCIM 955
12.2.10.2.1. Benutzerbereitstellung für Entra ID IdP 958
12.2.10.2.2. Benutzerbereitstellung für Okta IdP 964
12.2.11. Konfigurieren eines LDAP-Servers 967
12.2.12. [Sentry] 977
12.3. Apple-Einstellungen 978
12.3.1. Apple Configurator 979
12.3.2. Kontogesteuerte Registrierung 981
12.3.3. Geräteregistrierung 984
12.3.4. Beta-Registrierung 1000
12.3.5. Konfigurieren von Setup Assistant 1001
12.3.6. MDM-Zertifikat installieren 1002
12.3.7. Gemeinsam genutzte iPad-Geräte für Unternehmen 1003
12.3.8. School Manager 1008
12.3.9. Einstellungen (Apple) 1011
12.4. Arbeiten mit Windows-Geräten 1014
12.4.1. Windows Autopilot-Profile konfigurieren 1015
12.4.2. Audit-Protokolle auf Windows Autopilot-Profilen 1021
12.4.3. TenantLockdown CSP 1022
12.4.4. ADMX (GPO) Browser 1023
12.4.5. App-Bestandsaufnahmeintervalle konfigurieren 1024
12.4.6. Hardware-Bestand 1025
12.5. Einrichtung mit Microsoft Azure 1026
12.5.1. Verwendung von Microsoft Azure 1027
12.5.2. Entra ID Windows 10 Unified Endpoint Management-Setup 1030
12.5.3. Zuweisen der Entra ID UEM-App 1031
12.5.4. Verbinden von Ivanti Neurons for MDM mit der Entra ID-Benutzerquelle 1032
12.5.5. Azure-Mandant 1034
12.5.5.1. Azure Tenant Requirements 1035
12.5.5.2. Intune-Lizenz für Gerätebenutzer übernehmen. 1037
12.5.5.3. MobileIron als Compliance-Partner hinzufügen 1038
12.5.5.4. Richtlinie für bedingten Zugriff im Microsoft Endpoint Manager erstellen 1039
12.5.5.5. Verbinden von Microsoft Azure mit Ivanti Neurons for MDM 1040
12.5.5.6. Konformitätsrichtlinie für Partnergeräte erstellen 1041
12.5.5.7. Melden des Gerätestatus von Ivanti Neurons for MDM an Azure 1043
12.5.5.8. Bereitstellung des Azure-Mandanten aufheben 1045
12.5.6. Administration > Microsoft Azure > Office 365 App-Schutz 1047
12.6. Mit Google Apps verbinden 1056
12.6.1. Verwaltete Google Play-Konten (Android Enterprise-Konten) 1057

12.6.2. Android-Geräteregistrierung ... 1061
12.6.3. Android-Verwaltungs-API ... 1062
12.6.4. API für Google Apps ... 1068
12.6.5. Administration > Android Enterprise ... 1069
12.7. Arbeiten mit ChromeOS-Geräten ... 1071
12.7.1. ChromeOS und Ivanti Neurons for MDM ... 1072
12.7.2. Verteilen von Android-Apps an ChromeOS-Geräte ... 1074
12.7.3. Hinzufügen und Verteilen von Apps mit ChromeOS-Erweiterung ... 1075
12.7.4. ChromeOS Blueprint-Konfiguration ... 1076
12.7.5. Geräteaktionen ... 1077
12.7.6. Häufig gestellte Fragen ... 1078
12.7.7. Empfohlene Schritte für die Evaluierung ... 1080
12.8. Firmware-Verwaltung ... 1081
12.8.1. Für Zebra OTA-Service registrieren ... 1082
12.8.2. Samsung E-FOTA-Lizenzverwaltung (außer Betrieb) ... 1083
12.9. Verwalten von Skripten und Dateien ... 1084
12.9.1. Alle Skripte ... 1085
12.9.2. Dateien ... 1090
12.10. Branding ... 1091
12.10.1. Administration > App-Katalog für Apple (Branding) ... 1092
12.10.2. Branding des Android App-Katalogs ... 1093
12.10.3. Admin > Android Kiosk-Branding ... 1094
12.10.4. Branding von E-Mail-Vorlagen ... 1095
12.10.5. Selbstbedienungsportal ... 1104
12.10.6. Branding für das Selbstbedienungsportal) ... 1106
12.10.7. Anmeldung mit Branding für mehrere Benutzer (Web-Clip) ... 1107
12.10.8. Organisation ... 1108
12.11. Hinzufügen der Verwaltung von Nicht-iOS-Geräten ... 1109
13. Pakete ... 1110
13.1. Upgrades durchführen ... 1114
14. Gerätelizenzen ... 1116
14.1. Zeitweilige Sperre eines Mandanten ... 1117
15. Öffnen eines Support-Tickets ... 1118
16. Attribute von Drittanbietern ... 1119
17. Apps@Work ... 1120
18. Aktivieren der Kerberos-Authentifizierung zwischen Ivanti Neurons for MDM und SCEP-Server ... 1123
19. Ivanti Neurons for MDM 127 – Administratorhandbuch ... 1126
20. Welcome ... 1127
21. Welcome CSH ... 1128
22. Windows-Updatemanagement ... 1129

1. Wissenswertes über Ivanti Neurons for MDM

Als moderner Ansatz für mobile Sicherheit bietet die Cloud Unified Endpoint Management (UEM)-Lösungen in einer hoch skalierbaren, sicheren und einfach zu aktualisierenden Infrastruktur, die Millionen von Geräten auf der ganzen Welt unterstützt.

- Sofortige Updates: Erhalten Sie automatische Software- und Sicherheitsupdates und Zugang zu neuen Funktionen, sobald diese verfügbar sind.
- Skalierbarkeit nach Bedarf: Skalieren Sie die Bereitstellung entsprechend Ihren neuen Unternehmensanforderungen, ohne dass Sie sich um die Kapazitätsplanung kümmern müssen.
- Minimierung der Hardware-Kosten: Durch den Wegfall der Notwendigkeit, Hardware vor Ort zu warten, entfallen bei Cloud-Diensten die Verwaltungskosten.
- Hohe Betriebszeit und hohe Verfügbarkeit.
- Vorhandene Investitionen maximieren: Umverteilung der IT-Ressourcen von der Hardware-Wartung auf strategischere Aufgaben, die einen Mehrwert für das Unternehmen schaffen.

Zeigen Sie eine Zusammenfassung der in diesem Release verfügbaren **Zusammenfassung der neuen Funktionen** an.

2. Zusammenfassung der neuen Funktionen

Dieser Abschnitt enthält Zusammenfassungen der neuen Funktionen und Verbesserungen, die in dieser Version verfügbar sind. Sofern verfügbar, wird auch auf die Dokumentation verwiesen, in der diese Funktionen und Erweiterungen beschrieben werden.

Allgemeine Funktionen und Erweiterungen

Android-Funktionen

Funktionen von iOS, macOS, watchOS, visionOS und tvOS

Windows-Funktionen

Allgemeine Funktionen und Erweiterungen

- **Verbesserte Verarbeitung der macOS-Paket-ID**: Die interne macOS-PKG-App-Bereitstellung wurde verbessert. Die korrekte Paket-ID wird jetzt automatisch während des Hochladens der App erkannt und vorbefüllt, und es wird sichergestellt, dass dieselbe Paket-ID an die Geräte gesendet wird. Dies verbessert die Genauigkeit der App-Identifikation, beseitigt Diskrepanzen beim Installationsstatus von Server und Gerät und verbessert die Meldung des Installationsstatus. Bundle-IDs können jetzt beim Hochladen überprüft und bearbeitet werden, bevor sie nach der Bereitstellung gesperrt werden.
- **Sichtbarkeit der Bundle-ID für installierte Apps**: Der Abschnitt "Installierte Apps" auf der Seite "Gerätedetails" enthält jetzt die Spalte "Bundle-ID", die in den Seiteneinstellungen angezeigt oder ausgeblendet werden kann.
- **Automatische Wiederholung fehlgeschlagener Android-App-Installationen**: Fehlerhafte Android-App-Installationen, die nach einem Fehlversuch in einen Fehlerstatus wechseln, werden jetzt automatisch eine Stunde nach der Geräteregistrierung wiederholt. Installationsbefehle werden alle 30 Minuten für bis zu fünf Versuche erneut gesendet, um die Erfolgsquote der Anwendungsbereitstellung zu verbessern.
- **Protokollierung von Geräteverschiebungen für Bereiche**: Es wurde eine Einstellung zum Aktivieren von Audit-Protokollen für die Vornahme und Aufhebung der Geräteregistrierung in Bereichen hinzugefügt, die es ermöglicht, das Verschieben von Geräten zwischen verschiedenen Bereichen zu verfolgen. Weitere Informationen finden Sie unter Audit-Protokolle exportieren.
- **Betriebssystem-Plattformfilter für die Gerätebereinigung**: Administratoren können jetzt Aktionen im Rahmen der Gerätebereinigung nach Plattform filtern, wenn sie Geräte entfernen, die stillgelegt wurden oder deren Stilllegung aussteht. Standardmäßig bleiben alle unterstützten Plattformen ausgewählt, sodass das bestehende Verhalten erhalten bleibt. Administratoren können die Auswahl ändern und die Bereinigungsvorgänge je nach Bedarf auf bestimmte Plattformen beschränken. Weitere Informationen finden Sie unter Einstellungen für die Gerätebereinigung.
- **Richtliniensynchronisierung für Schutz der Office 365-App**: Bislang konnten Administratoren Apps direkt innerhalb von Ivanti Neurons for MDM auswählen, während sie Richtlinien für den App-Schutz erstellten oder änderten. Microsoft hat die API, die zum Abrufen der Liste verfügbarer Apps verwendet wurde, eingestellt, sodass die Listen der geschützten Apps in Ivanti Neurons for MDM leer angezeigt werden. Die Richtlinienverwaltung für den Schutz der Microsoft Office 365-App wird an Änderungen in Microsoft Intune angepasst. Anwendungen, die in Intune konfiguriert sind, werden jetzt automatisch mit Ivanti Neurons for MDMsynchronisiert, um eine kontinuierliche Transparenz der geschützten Anwendungen zu gewährleisten. Während die App-Entfernung weiterhin von Ivanti Neurons for MDM unterstützt wird, müssen neue App-Zuweisungen in Microsoft Intune konfiguriert werden. Sie werden dann automatisch abgebildet.
- **Protokollierung von Geräteverschiebungen für Spaces**: Administratoren können jetzt mithilfe von Audit-Protokolle Geräteverschiebungen zwischen Spaces verfolgen. Wenn diese Option aktiviert ist, zeichnet die neue Prüfeinstellung ein Ereignis auf, wenn ein Gerät aus einem Space entfernt und einem anderen hinzugefügt wird. Dadurch verbessert sich die Transparenz automatisierter und regelbasierter Space-Zuweisungen. Weitere Informationen finden Sie unter Audit-Protokolle exportieren.

- **Automatische Zuweisung benutzerdefinierter Attribute unter Verwendung von Gerätegruppen**: Administratoren können jetzt benutzerdefinierte Attribute auf Ebene der Gerätegruppe zuweisen. Geräte, die Mitglieder einer Gerätegruppe sind, übernehmen automatisch die konfigurierten Attributwerte, wodurch die manuelle Konfiguration reduziert und eine konsistente Gerätekategorisierung ermöglicht wird. Weitere Informationen finden Sie unter **Gerätegruppen**.
- **Einschränkung der Geräteregistrierung auf Betriebssystemebene**: Beschränken Sie die Geräteregistrierung nach Plattform, sodass nur genehmigte **Apple**-, **Android**- und **Windows**-Geräte registriert werden können. Weitere Informationen finden Sie unter **Benutzereinstellungen**.

Android-Funktionen

- **Updates für Apps verhindern, die gerade verwendet werden**: Administratoren können jetzt festlegen, dass eine verwaltete Android-App, die gerade in Verwendung ist, nicht aktualisiert wird. Wenn **Während der Verwendung der App nicht aktualisieren** aktiviert ist, werden App-Updates verschoben, bis der Benutzer die App schließt oder in den Hintergrund verschiebt, wodurch Unterbrechungen während der aktiven Sitzungen minimiert werden. Weitere Informationen finden Sie unter **App-Konfiguration**.
- **Kiosk-Modus nach Änderung der Sperrrichtlinie beibehalten** – Die Beibehaltung des Kiosk-Modus nachdem die Sperrrichtlinie geändert wurde, wird jetzt unterstützt. Die Geräte kehren nach der Aktualisierung der Sperrrichtlinien automatisch in den Kiosk-Modus zurück, wodurch manuelle Eingriffe reduziert und Unterbrechungen bei Geräten mit Zweckbindung minimiert werden. Weitere Informationen finden Sie unter **Sperre & Kiosk: Android Enterprise**.
- **Unzensierte Benachrichtigungen aktivieren**: Die Sichtbarkeit von Benachrichtigungen auf dem Sperrbildschirm von Geräten des Gerätebesitzers kann jetzt konfiguriert werden. Administratoren können Benachrichtigungsinhalte auf dem Sperrbildschirm anzeigen, ausblenden oder bearbeiten, um vertrauliche Informationen zu schützen und gleichzeitig die Benachrichtigungsfunktion zu erhalten. Weitere Informationen finden Sie unter **Erweiterter Android-Passcode und Sperrbildschirm**.
- **Gerät-zu-Benutzer-Zuordnung während der Massenregistrierung von Profilen**: Die Gerät-zu-Benutzer-Zuordnung bei der Massenregistrierung von Profilen wird jetzt unterstützt. Administratoren können jedem Gerät über die Massenregistrierungs-CSV-Datei oder während des manuellen Hinzufügens eines Geräts einen bestimmten Benutzer zuweisen. Dadurch wird eine automatische Benutzerzuweisung während der Registrierung ermöglicht, während administrative Aufgaben nach der Registrierung reduziert werden. Administratoren können Benutzerzuweisungen auch vor der Geräteregistrierung aktualisieren. Weitere Informationen finden Sie unter **Gerät-zu-Benutzer-Zuordnung in Massenregistrierungsprofilen**.

Funktionen von iOS, macOS, watchOS, visionOS und tvOS

- **Neue Skip Keys für Geräteregistrierungsprofile**: Administratoren können jetzt die folgenden Skip Keys beim Erstellen von Profilen für die Geräteregistrierung verwenden:
  - **Liquid Glass-Bereich überspringen** (iOS 27.0+ und macOS 27.0+)
  - **Bereich für Barrierefreiheit-Erscheinungsbild überspringen** (27.0+)
    Diese Skip Keys vereinfachen die Registrierung insofern, als Administratoren bestimmte Einrichtungsfenster während der Geräteregistrierung ausblenden können. Weitere Informationen finden Sie unter **Geräteregistrierung**.
- **Unterstützung für DDM-Systemzustand von Gerätekomponenten**: Ivanti Neurons for MDM unterstützt jetzt den DDM-Systemzustand von Gerätekomponenten auf der Seite **Gerätedetails**. Administratoren können diesen Status im Abschnitt **Systemzustand von Gerätekomponenten** anzeigen und damit den Systemzustand im Blick behalten, der von den überwachten Geräten gemeldet wird. Weitere Informationen finden Sie unter **Erste Schritte mit der Geräten**.
- **Neue Felder für Gerätedetails für Apple-Geräte**: Die neu hinzugefügten Felder für die **Gerätedetails** bieten einen besseren Einblick in den Zustand der Apple-Geräteverwaltung. Administratoren können jetzt folgende Details anzeigen:

  - **Mehrbenutzer-Modus** für Geräte, die mit iOS 27.0+ betrieben werden. Dieses Feld gibt an, ob ein iPad als gemeinsam genutztes Gerät konfiguriert ist.
  - **MDM-Registrierungstyp** für Geräte mit iOS 27.0+, macOS 27.0+, tvOS 27.0+, visionOS 27.0+ und watchOS 27.0+
  - **MDM-Wiederinbetriebnahme** unter App-Beibehaltung für Geräte, die mit iOS 27.0+ und visionOS 27.0+ betrieben werden Diese Felder ermöglichen es Administratoren, Informationen zu Gerätekonfiguration und -registrierung direkt über die Seite "Gerätedetails" zu überprüfen. Weitere Informationen finden Sie unter **Erste Schritte mit der Geräten**.

- **Unterstützung für die Konfiguration "App-Datenschutz-Standardeinstellungen"**: Administratoren können jetzt **App-Datenschutz-Standardeinstellungen** für eine oder mehrere Apps mithilfe von Apple Device Declarative Management (DDM) konfigurieren. Wenn eine App zum ersten Mal gestartet wird, erhalten Benutzer eine einzige Eingabeaufforderung zur Erteilung ihrer Zustimmung, sodass sie empfohlene Berechtigungen für unterstützte Datenschutzkomponenten wie Kamera, Mikrofon, Standort, Bluetooth und lokalen Netzwerkzugriff gewähren oder verschieben können. Weitere Informationen finden Sie unter **Standardeinstellungen für App-Datenschutz**.

> Die Konfiguration der App-Datenschutz-Standardeinstellungen wird jetzt auf überwachten Geräten mit macOS 27.0+ unterstützt.

- **Neues DDM-App-Verwaltungsattribut hinzugefügt**: Das Feld **Apple DDM-App aktiviert** für das DDM-App-Verwaltungsattribut wurde zu den Seiten für die erweiterte Suche und die Geräteliste hinzugefügt. Es zeigt an, auf welchen Geräten Apps über DDM verteilt werden. Administratoren können dies über die Benutzereinstellungen aktivieren. Weitere Informationen finden Sie unter **Erste Schritte mit der Geräten**.
- **Verbesserte macOS-Konfiguration für erweitertes SSO**: Die macOS-Konfiguration für erweitertes SSO wurde aktualisiert, sodass Token-Attribute wie **preferred_username** und **name** korrekt zugeordnet werden. Dies behebt Konfigurationsfehler, die durch ungültige Token-zu-Benutzer-Zuordnungen verursacht werden, und ermöglicht die erfolgreiche Bereitstellung von SSO-Profilen auf Geräten.
- **Erweiterte Protokollierung von Apple**: Administratoren können die erweiterte Protokollierung von Apple jetzt mithilfe eines von AppleCare bereitgestellten Tokens auf unterstützten Apple-Geräten initiieren. Die Gerätedetails zeigen den Sitzungsstatus, das Token und Zeitstempelinformationen an. Aktive Sitzungen können bei Bedarf abgebrochen werden. Weitere Informationen finden Sie unter **Erweiterte Protokollierung von Apple**.
- **Sperrmodusstatus** (iOS 27+, macOS 27+): Das Anzeigen und Filtern von Geräten nach Sperrmodus unter Verwendung des neuen Feldes **Sicherheitssperrmodus** wird jetzt auf der Seite **Gerätedetails**, in der **erweiterten Suche** und bei den Gerätegruppenregeln unterstützt. Dieses Feld gibt an, ob der Sperrmodus auf einem Gerät aktiviert (**wahr**) oder deaktiviert (**falsch**) ist. Weitere Informationen finden Sie unter **Erste Schritte mit der Geräten**, **Gerätegruppen** und **Anpassbare Richtlinie**.
- **Ende der Unterstützung von macOS-Softwareupdate-Einstellungen**: Die Konfiguration **macOS-Softwareupdate-Einstellungen** wird auf macOS 27 und späteren Geräten nicht mehr unterstützt. Diese Konfiguration gilt jetzt nur für unterstützte Versionen bis macOS 26.x. Weitere Informationen finden Sie unter **Konfiguration der Update-Regeln für macOS Software**.
- **Änderung bei der Unterstützung von Einschränkungen** (iOS 27+, macOS 27+): Die Einschränkungen **Installieren von Sicherheitsverbesserungen im Hintergrund zulassen** und **Entfernen von Sicherheitsverbesserungen im Hintergrund zulassen** wurden aktualisiert und werden auf Geräten ab iOS 27 und ab macOS 27 nicht mehr unterstützt. Weitere Informationen finden Sie unter **iOS-Einschränkungen** und **Einschränkungen für macOS**.
- **Updates zur Konfiguration der Siri-Einstellungen** (iOS 27.0+, macOS 27.0+, tvOS 27.0+ und visionOS 27.0+): Es werden jetzt neue Einschränkungseinstellungen in der Konfiguration für Siri-Einstellungen unterstützt. Weitere Informationen finden Sie unter **Siri-Einstellungen**.
- **Updates zur Konfiguration der Intelligence-Einstellungen** (iOS 27.0+, macOS 27.0+ und visionOS 27.0+): Es werden jetzt neue Einschränkungseinstellungen in der Konfiguration für Intelligence-Einstellungen unterstützt. Weitere Informationen finden Sie unter **Intelligence-Einstellungen**.

- **Safari-Datenschutzeinstellungen** (iOS 27.0+, macOS 27.0+): Es werden jetzt Safari-Datenschutzeinstellungen in der Konfiguration "Safari-Erweiterung und -Einstellungen" unterstützt, die es Administratoren ermöglichen, Standardberechtigungen für Kamera und Mikrofon für bestimmte Websites mithilfe der deklarativen Geräteverwaltung von Apple (Declarative Device Management, DDM) zu konfigurieren. Weitere Informationen finden Sie unter **Konfiguration "Safari-Erweiterung und -Einstellungen"**.

Windows-Funktionen

- **Konfiguration für Windows AI Management**: Windows AI Management unterstützt jetzt zusätzliche Windows AI CSP-Richtlinien für die Verwaltung der Funktionen Microsoft Copilot, Windows Recall und Microsoft Paint AI. Administratoren können den Copilot-Hardwareschlüssel deaktivieren, die Microsoft Copilot-App entfernen, die KI-Datenanalyse für Recall deaktivieren, die Speicherlimits für Recall-Snapshots konfigurieren und Image Creator, Cocreator und Generatives Füllen in Paint deaktivieren. Die Unterstützung für Richtlinien für einen bestimmten Benutzerbereich und Gerätebereich wurde ebenfalls hinzugefügt, was eine granularere Steuerung der KI-Funktionen auf Windows-Geräten ermöglicht. Weitere Informationen finden Sie unter **Konfiguration "Windows KI-Verwaltung"**.

Funktionen von Mobile Threat Defense

Mobile Threat Defense (MTD) schützt verwaltete Geräte vor mobilen Bedrohungen und Sicherheitslücken, die die Sicherheit des Geräts, des Netzwerks und der Apps beeinträchtigen. Informationen zu den MTD-Funktionen für die aktuelle Version finden Sie in der Anleitung für Mobile Threat Defense für Ihre Plattform, die im Abschnitt MOBILE THREAT DEFENSE auf der Seite Ivanti **Produktdokumentation** verfügbar ist.

> Jede Version der MTD-Anleitung enthält alle Funktionen von Mobile Threat Defense, die derzeit vollständig getestet und für den Einsatz in Server- und Client-Umgebungen verfügbar sind. Aufgrund der Lücke zwischen Server- und Client-Releases werden neue Versionen der MTD-Anleitung mit dem letzten Release der Serie zur Verfügung gestellt, sobald die Funktionen voll funktionsfähig sind.

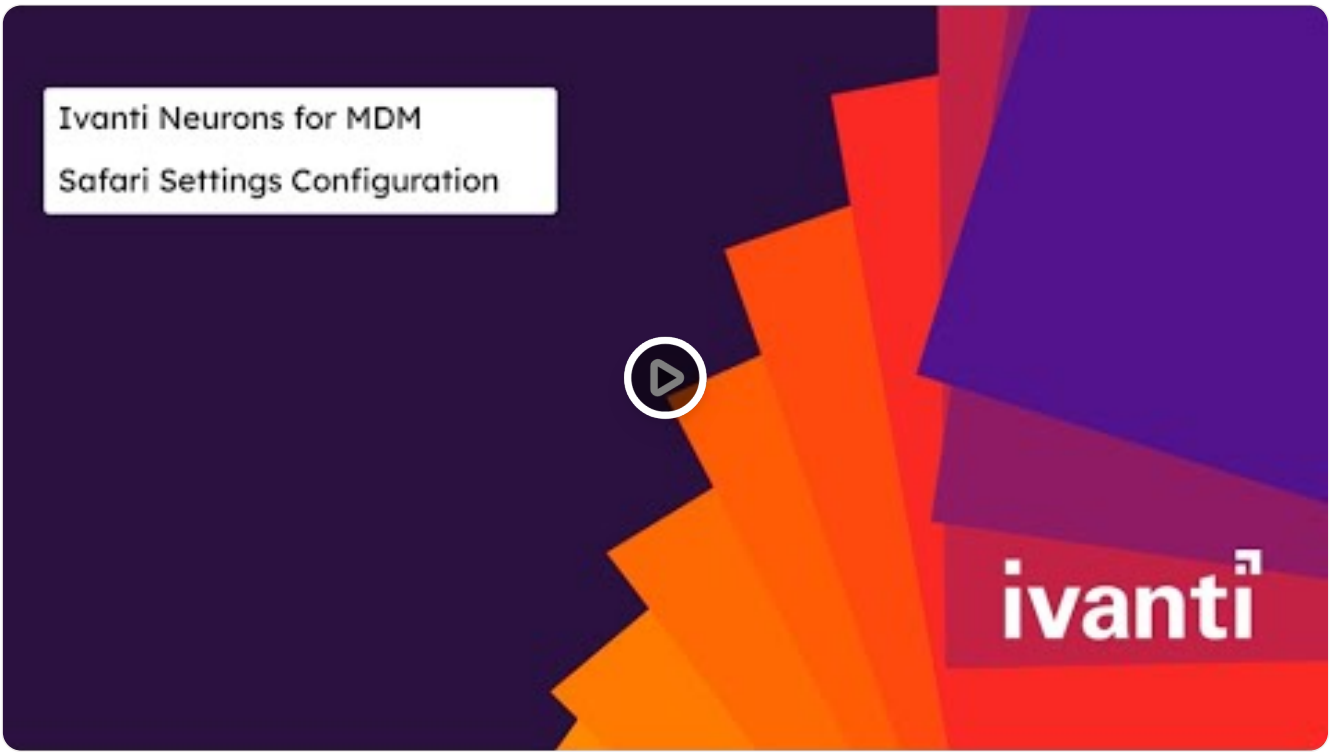
3. Videos

Verfügbare 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.



Suchen Sie ein Video zu einer bestimmten Funktion oder Funktionalität in Ivanti Neurons for MDM? Teilen Sie uns Ihr Feedback im Abschnitt "**War dieser Artikel nützlich?**?" auf jeder Seite dieses Dokuments mit.

4. Erste Schritte

Dieser Abschnitt enthält Übersichten über die Einrichtung und Nutzung von Funktionen, die eine Interaktion innerhalb des Neurons for MDM-Portals erfordern. Dieser Abschnitt enthält die folgenden Themen:

- Lösungsübersicht
  - Hauptmerkmale
  - Abbildung der Architektur
  - Ivanti Neurons for MDM Anwendungen
  - Rollen
  - Erste Schritte
- Bevorzugte Sprache im Browser einstellen
- Einheitliche Navigationsoberfläche für Ivanti Neurons for MDM und Access
- Geräteadministratormodus (DA) zur Verwaltung von Android-Geräten - veraltet

Lösungsübersicht

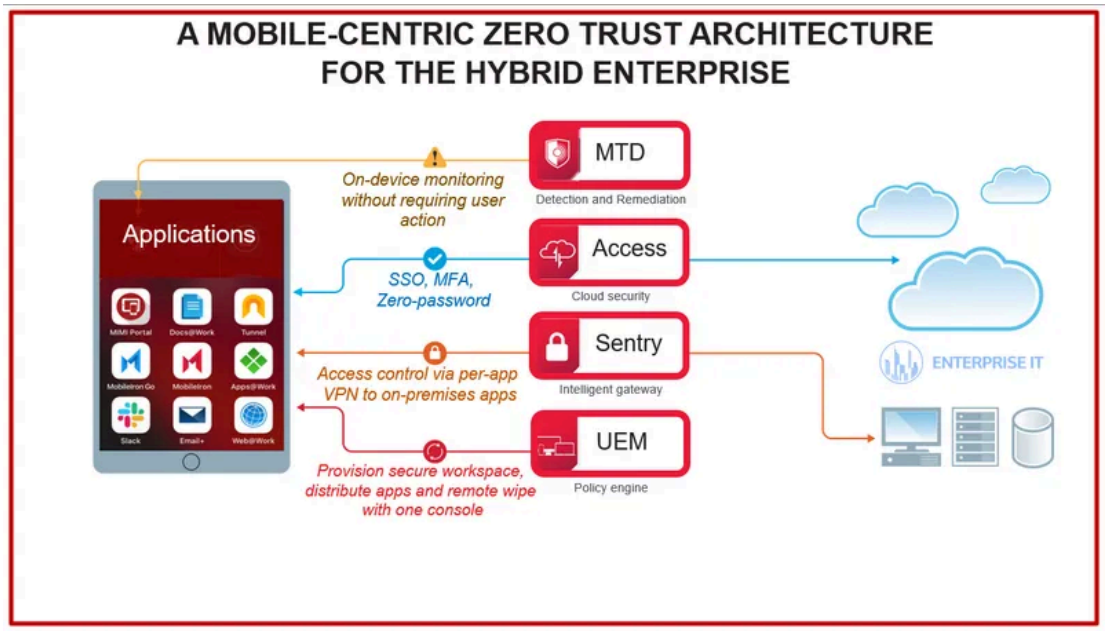
Der fortlaufende Zugriff auf Unternehmensdaten auf mobilen Geräten und anderen Endpunkten außerhalb des Unternehmensnetzwerks verlangt nach einem klaren Schwerpunkt auf der Sicherheit. Zur Einhaltung der aktuellen Sicherheitsanforderungen müssen Unternehmen einige Verfahren überdenken:

- Endgeräte wie Mobiltelefone und Laptops bereitstellen
- Zugriff anhand einer Reihe von zwingend erforderlichen Daten gewähren
- Gespeicherte und übertragene Daten schützen
- Maßnahmen je nach Bedarf erzwingen

Die -Lösung für dieses moderne Problem bewältigt alle Herausforderungen. Sie können Endpunkte überwachen und adaptive Richtlinien auslösen, mit denen Sie Bedrohungen beheben, Geräte unter Quarantäne stellen und die Compliance wahren. Die Kombination aus den folgenden Komponenten hilft Ihrem Unternehmen, das Mobilgeräte-zentrierte Zero-Trust-UEM-Framework zu realisieren:

- Ivanti Neurons for MDM Cloud – Einen sicheren Workspace auf jedem Gerät erstellen, dessen Apps, Konfigurationen und Richtlinien je nach Rolle des Benutzers zusammengestellt werden. Die Benutzer erhalten einfachen, sicheren Zugriff auf die Ressourcen, die sie zum produktiven Arbeiten benötigen
- **Sentry** – Ein intelligentes In-Line-Gateway, das für den sicheren Zugriff auf die lokalen Ressourcen sorgt
- **Access** – Benutzer, Geräte, Apps, Netzwerkstyp und Vorhandensein von Bedrohungen überprüfen. Die adaptive Zugriffskontrolle ist die Basis des Zero-Trust-Modells. Access bietet Single Sign-On und Sicherheit in der Cloud
- Ivanti Neurons for MDMMobile Threat Defense – Die Kombination aus Cloud und Mobile Threat Defense (MTD) schützt Daten auf Geräten und im Netzwerk mit modernster Verschlüsselung und Bedrohungsüberwachung, damit Angriffe auf Geräte-, Netzwerk- und App-Ebene erkannt werden

Die folgende Abbildung zeigt die Lösungsübersicht:



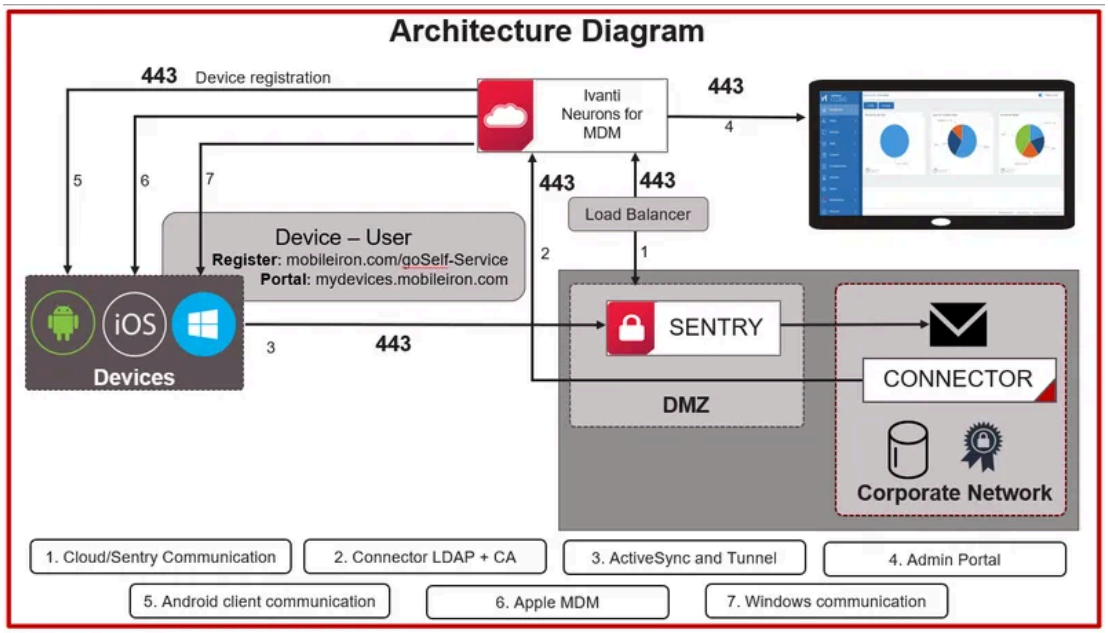
Hauptmerkmale

Ivanti Neurons for MDMDie Cloud-Plattform bietet fundamentale Transparenz und die Kontrollen zur Absicherung, Verwaltung und Überwachung unternehmenseigener bzw. mitarbeitereigener Mobilgeräte oder Desktops, die auf unternehmenskritische Daten zugreifen. Ivanti Neurons for MDM Unternehmen können mit der Cloud-Plattform eine Vielzahl von Mitarbeitergeräten im Unternehmen absichern und zugleich den gesamten Lebenszyklus des Geräts verwalten. Dies betrifft:

- Konfiguration und Durchsetzung von Richtlinien
- App-Verteilung und App-Verwaltung
- Skript-Management und -Verteilung für Desktop-Geräte
- Geräteaktionen
- Zugriffskontrolle und Multifaktor-Authentifizierung
- Erkennung und Eindämmung von Bedrohungen

Abbildung der Architektur

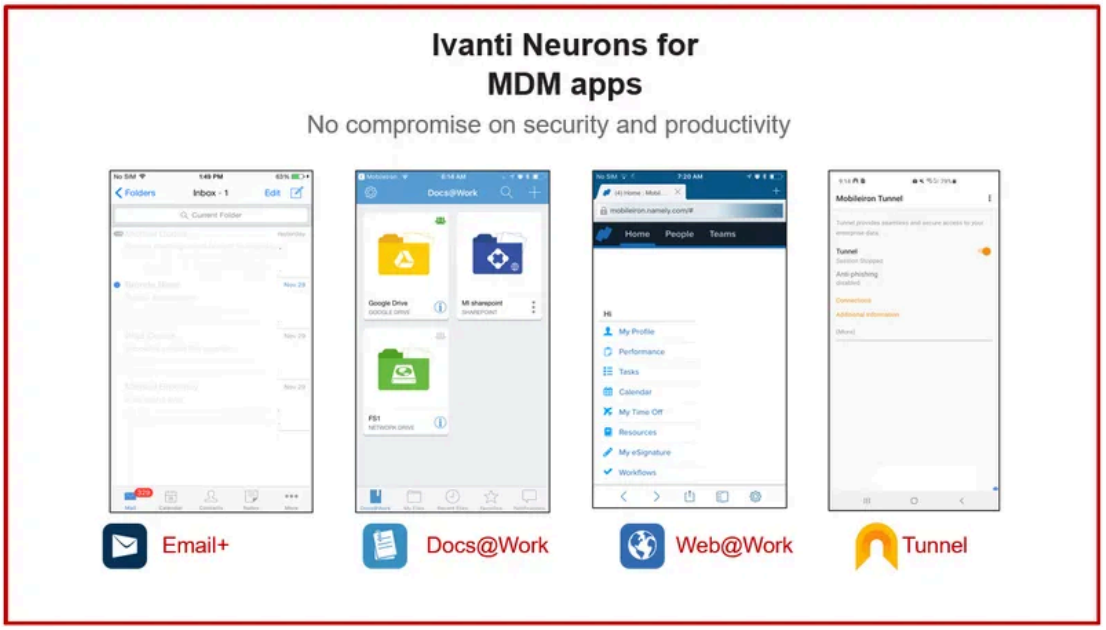
Ivanti Neurons for MDMDie folgende Abbildung zeigt die Architekturübersicht der Cloud-UEM-Plattform:



Ivanti Neurons for MDM Anwendungen

- **App-Katalog** – Der App-Katalog ist eine anpassbare App-Storefront für Unternehmens-Apps. IT-Administratoren können private oder unternehmenseigene Apps direkt auf den Geräten ihrer Endbenutzer veröffentlichen. Der App-Katalog lässt sich mit dem Apple Volume Purchase Program kombinieren und erleichtert damit die sichere Verteilung mobiler Apps aus iOS-Geräten. Ivanti macht sich zudem Funktionen in verwalteten iOS-Apps und Android Enterprise zunutze. Ivanti Neurons for MDMAuf der Cloud-UEM-Plattform vereinfacht dies die Konfiguration der Einstellungen und Sicherheitsrichtlinien auf App-Ebene für die beiden erweiterten App-Sicherheitsfunktionen.
- **Email+** – Plattformübergreifende sichere PIM-Anwendung für iOS und Android. Email+ bietet sichere E-Mails, Kalender, Kontakte und Aufgaben auf unternehmenseigenen und persönlichen Geräten über die Kommunikation mit einem ActiveSync-Server in Ihrem Unternehmen.
- **Docs@Work** – Die Benutzer können sicher auf Inhalte aus Repositories wie Microsoft SharePoint und Cloud-Diensten wie Box und Dropbox zugreifen, sie erstellen, bearbeiten, markieren und gemeinsam nutzen. Dies ist wichtig, damit die Benutzer auch unterwegs so produktiv wie möglich arbeiten.
- **Web@Work** – Sicherer Browser, der den Unternehmensbenutzern einen einfachen und sicheren Zugang auf Web-Inhalte im Firmenintranet ermöglicht. Mit Web@Work können Sie den Zugriff auf die Unternehmensdaten auf autorisierte Benutzer beschränken. Die Kombination aus Web@Work und App Tunnel schützt Unternehmensdaten während der Übertragung. Mit Web@Work greifen die Benutzer schnell und einfach auf interne Web-Ressourcen zu.

Ivanti Neurons for MDMDie folgende Abbildung zeigt die Cloud-Anwendungen:



Rollen

Administrator – Als Unternehmensadministrator sind Sie für folgende Aufgaben verantwortlich:

- Sie bieten nahtlosen, sicheren Zugriff der Unternehmensbenutzer auf Workspace-E-Mails, Anwendungen, Konfigurationen und Verbindungen wie WLAN und VPN.
- Sie trennen persönliche Daten auf den Mitarbeitergeräten von den Unternehmensdaten, sodass keine Unternehmensdaten in die persönlichen Apps gelangen und die IT-Abteilung nicht unbeabsichtigt auf persönliche Daten zugreift.

Benutzer – Als Unternehmensbenutzer greifen Sie nahtlos über sichere, moderne Mobilgeräte, Desktops und Cloud-Dienste auf Unternehmensanwendungen und persönliche Daten zu. Weitere Informationen zu den verschiedenen Aufgaben, die Sie als Benutzer durchführen können, finden Sie unter **Benutzer**. und **Rollenverwaltung**.

Erste Schritte

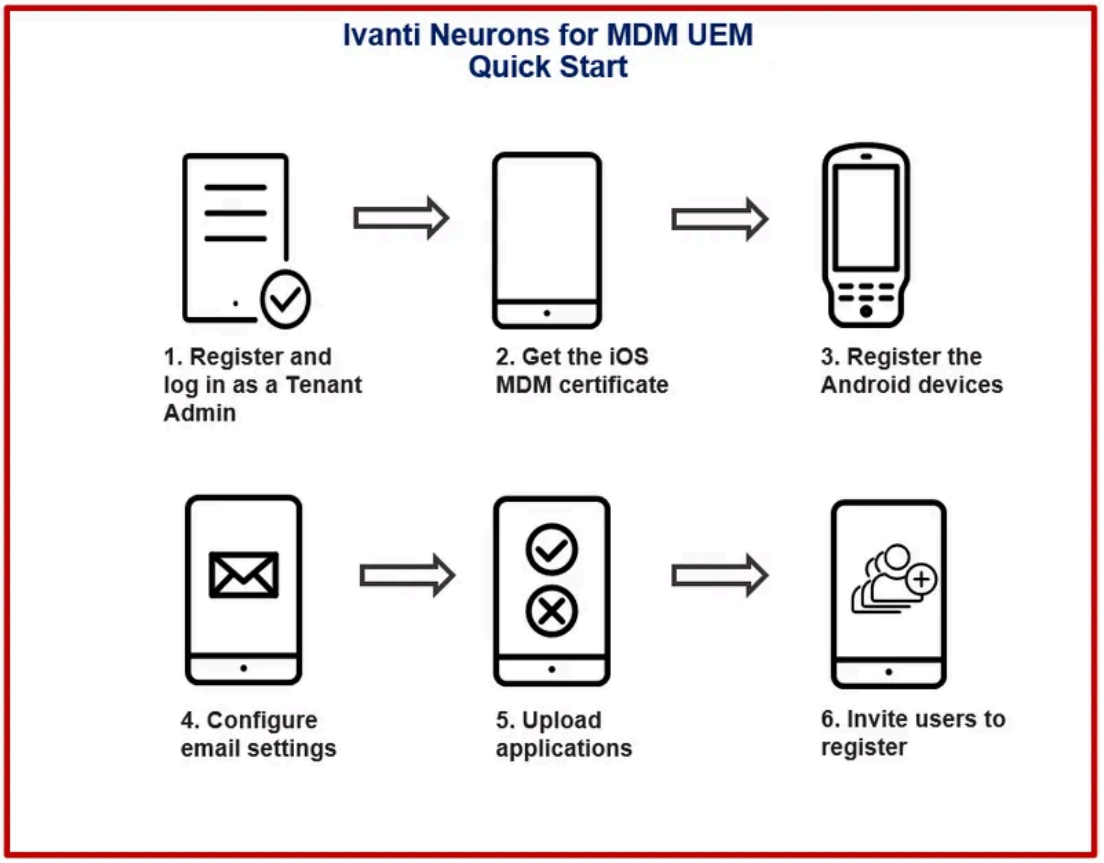
Ivanti Neurons for MDMRegistrierte neue Benutzer finden in diesem Abschnitt die nötigen Schritte, mit denen sie das Onboarding in die Cloud-Dienste schnell und einfach erledigen.

Ivanti Neurons for MDMIvanti Neurons for MDMWenn Sie die Cloud-Plattform abonniert haben, erstellt Ivanti einen Cloud-Mandanten für Sie. Sie erhalten eine E-Mail an die registrierte E-Mail-Adresse. Diese E-Mail enthält eine PDF mit folgenden Informationen zum Mandanten, der für Ihr Unternehmen erstellt wurde:

- Informationen zum erworbenen Software-Bundle
- URL und Super-Administrator-Anmeldedaten des Mandanten
- Support-Community und FAQs zur Cloud Ivanti Neurons for MDM
- Technische Dokumentation und Software-Downloads

> Ivanti, Inc stellt keine Softwareschlüssel bereit. Ivanti Neurons for MDMIvanti Neurons for MDMWenn Sie sich beim Cloud-Mandanten mit den Super-Administrator-Anmeldedaten anmelden und die Nutzungsbedingungen akzeptieren, aktivieren Sie damit das Cloud-Produkt.

Ivanti Neurons for MDMDie folgende Abbildung zeigt die Schritte für den Einstieg in die Cloud:



Verfahren

1. Klicken Sie auf die URL in der Mandantenregistrierungs-E-Mail. Die Eingabeaufforderung zum Zurücksetzen des Passworts wird angezeigt.
2. Ändern Sie Ihr Passwort.
3. Melden Sie sich mit der ID und dem Passwort beim Mandantenkonto an. Der Begrüßungs-Assistent wird geöffnet.
4. Füllen Sie das **Begrüßungsformular** aus, akzeptieren Sie die Nutzungsbedingungen und klicken Sie auf **Weiter**.
5. Anweisungen zur Installation des iOS-MDM-Zertifikats finden Sie unter **MDM-Zertifikat installieren**.

Wenn Sie Ihre iOS-Geräte erst später verwalten möchten, können Sie die Installation des iOS-MDM-Zertifikats überspringen. Der Assistent fordert Sie dann auf, die Android-Geräte Ihres Unternehmens zu registrieren. Wird die Installation des iOS MDM-Zertifikats übersprungen, können sich iOS-Geräte nicht registrieren. Den Benutzern wird eine Meldung angezeigt, dass die Registrierung von iOS-Geräten nicht aktiviert wurde.

6. Anweisungen zum Registrieren der Android-Geräte im Android Enterprise-(AE)-Modus finden Sie unter **Verwaltete Google Play-Konten (Android Enterprise-Konten)**. Der Assistent fordert Sie dann auf, E-Mail-Konten einzurichten.

Wenn Sie Ihre Android-Geräte erst später verwalten möchten, können Sie die Registrierung der verwalteten Android-/Google Play-Konten überspringen. Wenn Sie die Registrierung für ein verwaltetes Google-Play-Konto überspringen, können Sie keine Geräte mit Android Enterprise registrieren. Android-Geräte können auch über den Geräteadministrator registriert werden, es fehlen dann jedoch wichtige Funktionen, wie verwaltetes Google-Play und die App-Konfiguration.

7. Anweisungen zum Konfigurieren der E-Mail-Einstellungen und ActiveSync finden Sie unter **Konfiguration von Exchange** und **E-Mail-Konfiguration**.
8. Klicken Sie auf **Weiter**. Die Eingabeaufforderung zur Erstellung des Passcodes wird angezeigt.
9. Wählen Sie einen Passcodetyp aus und klicken Sie auf **Weiter**.
10. Wählen Sie die hochzuladenden Anwendungen und klicken Sie auf **Weiter**.
11. Geben Sie die E-Mail-Adressen der Benutzer an und klicken Sie auf Weiter.Die Benutzer erhalten eine E-Mail, in der sie gebeten werden, ihre Mobilgeräte zu registrieren. Eine Übersicht der Konfiguration wird angezeigt.
12. Klicken Sie auf **Fertigstellen**. Die Dashboard-Seite wird angezeigt.
13. Nähere Einblicke erhalten Sie wie folgt:
    - Gehen Sie zu Benutzer. Alle eingeladenen Benutzer werden aufgelistet.
    - Gehen Sie zu **Apps**. Alle hochgeladenen Anwendungen werden aufgelistet.
    - Gehen Sie zu **Konfigurationen**. Alle Konfigurationen, die Sie während der Registrierung übertragen haben, werden aufgelistet.

Weitere Informationen zu den verschiedenen Aufgaben als Benutzer finden Sie im Abschnitt **Administrator**.

Bevorzugte Sprache im Browser einstellen

Wenn ein Benutzer als seine Browsersprache eine nicht unterstützte Sprache eingestellt hat, kann der Benutzer en_US (Englisch, Vereinigte Staaten) als Standardsprache für das Portal festlegen.

Die bevorzugte Sprache für den Safari-Browser auf Geräten mit macOS 10.15+ können Benutzer wie folgt einstellen:

1. Gehen Sie auf dem macOS-Gerät zu **Systemeinstellung**.
2. Gehen Sie zu Sprache und Region > Allgemeines.
3. Legen Sie en_US (oder eine andere Sprachoption) als Bevorzugte Sprache fest.

Einheitliche Navigationsoberfläche für Ivanti Neurons for MDM und Access

Ivanti Neurons for MDM Für Neukunden in einigen Clustern ist Access als einheitliche Navigationsoberfläche mit Cloud verfügbar. Ivanti Neurons for MDMMelden Sie sich mit Ihren Cloud-Administrator-Anmeldedaten an. Die Zugriffsoptionen sind im linken Navigationsbereich als separate Registerkarte verfügbar. Besuchen Sie die **Produktdokumentation** und klicken Sie auf Access, um weitere Informationen über Access und die Einrichtung von Access zu erhalten.

Die einheitliche Navigationsoberfläche umfasst die folgenden Funktionen:

- Ivanti Neurons for MDMEinheitliche Anmeldung für Cloud und Access.
- Ivanti Neurons for MDMDer Produktpicker im linken Navigationsbereich erlaubt ein Umschalten zwischen Cloud- und Access-Produkten.
- Ivanti Neurons for MDMProduktauswahlspeicher: Bei der ersten Anmeldung erscheint das Cloud-Admin-Portal.
  Ivanti Neurons for MDMBei späteren Anmeldungen wird „Cloud“ oder „Access“ angezeigt, je nachdem, welches Produkt bei der ersten Anmeldung ausgewählt wurde.
- Ivanti Neurons for MDMLinker Navigationsbereich sowohl für Cloud als auch für Access.
- Bereich mit einheitlichen Kontoeinstellungen und Links zu Optionen wie Upgrade-Optionen, Dokumentation, Support-Portal, Passwortänderung und Abmeldung.

Geräteadministratormodus (DA) zur Verwaltung von Android-Geräten - veraltet

Ivanti Neurons for MDMDer Geräteadministratormodus (DA) zur Verwaltung von Android-Geräten wird ab Cloud 78 schrittweise eingestellt.

Ivanti Neurons for MDMAlle neuen Benutzer mit einem neuen Mandanten, der in Cloud 78 erstellt wurde, können (ab Android 6) keine Geräte mehr im DA-Modus registrieren. Alle neuen Mandanten, die die DA-Registrierung für Android 6 bis Android 9 aktivieren müssen, müssen den Ivanti-Support kontaktieren.

- Geräte mit Android 10 und höher werden weiterhin für die Registrierung im DA-Modus gesperrt.
- Für bestehende Anwender (mit oder ohne bestehende DA-Implementierungen) gibt es keine Änderungen bei der Verwaltung der bestehenden DA-Geräte (Android 6 bis Android 11). Bei einem Upgrade auf Ivanti Neurons for MDM 78 können jedoch alle neu registrierten Geräte mit Android 10+ von vorhandenen Mandanten ebenfalls nicht mehr im DA-Modus betrieben werden. Solche Mandanten könnten nur Geräte der Versionen Android 6 bis Android 9 im DA-Modus anmelden.
- Wenn Benutzer DA-Geräte von einer Core-Instanz zu Ivanti Neurons for MDM R78 migrieren möchten, muss Android Enterprise aktiviert sein und mindestens eine Systemkonfiguration an das Zielset verteilt sein (PO, DO oder COPE), bevor Sie die Migration auslösen. Dieser Schritt ist wichtig, um zu verhindern, dass Geräte nach der Migration stillgelegt werden.

DA-Registrierungstyp	Vorhandener Mandant (mit Upgrade auf Cloud R78)	Neuer Mandant
Neue DA-Anmeldung eines Gerätes mit OS >=10	Nicht zulässig	Nicht erlaubt
Neue DA-Registrierung von Geräten mit OS < 10	Zulässig	Nicht erlaubt
Vorhandene DA-Geräte mit OS >= 10	Bleiben aktiv	Entfällt
Vorhandene DA-Geräte mit OS < 10	Bleiben aktiv	Entfällt
Migrierte DA-Geräte mit OS >= 10	Werden außer Dienst gestellt	Werden außer Dienst gestellt
Migrierte DA-Geräte mit OS < 10	Bleiben aktiv	Werden außer Dienst gestellt

4.1. macOS-Geräte konfigurieren

Dies ist ein Übersichtsthema mit einer Liste gängiger Prozeduren und weiteren Inhalten zur Konfiguration von macOS-Geräten unter Ivanti Neurons for MDM. Sie können über das Ivanti Neurons for MDM-*Administratorhandbuch* auf alle macOS-Themen zugreifen.

INHALT

- Geräte registrieren
- Vorlage für Benutzereinladung konfigurieren
- Zero Sign-On-Funktionen einrichten
- Mobile@Work für macOS-Client einrichten
- macOS-Shell-Skripte einrichten
- macOS-Konfigurationen einrichten
- macOS-Richtlinien einrichten

Geräte registrieren

Die meisten Benutzer beginnen mit der Geräteregistrierung. Sie können jeden der folgenden Ansätze nutzen, um die Registrierung zu starten:

- Eine Einladung an einen oder mehrere Endbenutzer senden (iReg-Registrierung). Weitere Informationen finden Sie im Abschnitt Geräteregistrierung unter *macOS-Geräteregistrierung*.
- Geräteregistrierung und Benutzerregistrierung mit Apple Business Manager

Device_Registration.htm**Weitere Informationen finden Sie unter Geräteregistrierung.**

Vorlage für Benutzereinladung konfigurieren

Sie können die E-Mail-Einladung für den Endbenutzer mit Ihrem eigenen Design versehen, damit sie von Ihren Endbenutzern leichter wiedererkannt wird. Weitere Informationen finden Sie unter Branding von E-Mail-Vorlagen.

Sie können Sie den Geräteregistrierungsprozess mit Namen und Logos kundenspezifisch anpassen, die Ihre Benutzer bereits kennen. Weitere Informationen finden Sie unter Benutzer-Branding.

Weitere Informationen finden Sie unterRegistrierungsbestätigungs-E-Mails konfigurieren und verwenden.

Zero Sign-On-Funktionen einrichten

Die Dokumentation zu Zero Sign-on finden Sie unter „Zero Sign-on mit Access“ in der *Access-Anleitung*.

User_Settings.htm**Informationen über die automatische Zero-Touch-Registrierung finden Sie unter Benutzereinstellungen, Abschnitt „Einstellungen für neue Geräteregistrierungen konfigurieren“, Schritt 13.**

Mobile@Work für macOS-Client einrichten

Mobile@Work für macOS-App bietet:

- Skripting-Funktionen auf macOS-Geräten
- App Catalog für Endanwender

- Push-Nachrichten
- Benutzer-Onboarding-Bildschirm (Begrüßungs-/Statusbildschirm) für automatische Geräteregistrierungen

Stellen Sie vor der Push-Übertragung von Mobile@Work an die Endbenutzer sicher, dass die **Mobile@Work for macOS Configuration.htmMobile@Work für macOS** erstellt und und für die Verteilung an die macOS-Zielgeräte festgelegt wurde.

Sie können das Benutzer-Onboarding für macOS-Geräte während des automatisierten **Device Enrollment**-Prozesses aktivieren. Sobald die Geräteregistrierung abgeschlossen ist, wird Mobile@Work für macOS zusammen mit den Profilen, Konfigurationen und Apps auf das Gerät übertragen.

macOS-Shell-Skripte einrichten

Ivanti Neurons for MDMIvanti Neurons for MDM ermöglicht Ihnen, eigene macOS-Shell-Skripte zu erstellen, die Sie dann in hochladen und auf verwalteten macOS-Geräten starten können. Sie können die Skripte mit der Mobile@Work for macOS-Skriptkonfiguration konfigurieren. Mobile@Work liefert die Ergebnisse der Script-Ausführung an Ivanti Neurons for MDM zurück, diese werden dann in den Geräteprotokollen angezeigt. Sie können die Geräteprotokolle auf der Seite mit den Gerätedetails des macOS-Geräts auf der Registerkarte **Protokolle** überprüfen. Weitere Informationen zum Erstellen, Hochladen und Verwalten des Skript-Repositorys finden Sie unter **Alle Skripte**.

Bevor Sie Shell-Skripte auf macOS-Geräten ausführen können, müssen Sie sicherstellen, dass die Benutzer die App Mobile@Work for macOS auf ihren Geräten ausführen und eine Konfiguration für Mobile@Work for macOS auf ihre Geräte übertragen haben. Skripte können einmalig oder in regelmäßigen Abständen ausgeführt werden. Ivanti Neurons for MDMDurch Skripting können Administratoren auch Informationen von einem Gerät sammeln und dann in der Cloud als benutzerdefiniertes Attribut speichern. Wenn Sie z. B. die Java-Version auf einem macOS-Gerät kennen müssen, können Sie diese Informationen sammeln und als benutzerdefiniertes Geräteattribut für jedes Gerät speichern. **Mobile@Work for macOS Configuration.htm**Weitere Informationen finden Sie unter Mobile@Work for macOS-Skriptkonfiguration erstellen inMobile@Work for macOS.

macOS-Konfigurationen einrichten

Configurations.htm Konfigurationen sind Sammlungen von Einstellungen, die Sie an Geräte senden. Sie können Konfigurationen zum Beispiel zum automatischen Einrichten von VPN-Einstellungen und Passwortanforderungen auf diesen Geräten verwenden. Nutzen Sie die Seite **Konfigurationen** zum Auswählen, Einrichten und Verteilen von Richtlinien. **Configuration_types.htm**Es stehen viele Konfigurationstypen zur Verfügung. Auf der **Seite** können Sie eine Liste der verfügbaren macOS-Konfigurationen einsehen, darunter die folgenden Konfigurationen:

- **WLAN**
- **Passwort**
- **VPN**
- **Verschlüsselter DNS**
- **FileVault 2**
- **FileVault-Wiederherstellungsschlüssel**
- **macOS-Firewall**
- **Einschränkungen für macOS**
- **macOS AppStore-Einschränkungen**
- **Einstellungen für macOS Finder**
- **Erweiterungsrichtlinie für den macOS Kernel**

- Active Directory (macOS)
- Automatische Kontoerstellung für Office 365 (macOS)

Sie können Benutzerdefinierte Konfigurationen verwenden, um eine vordefinierte Konfigurationsdatei zu importieren und zu verteilen.

macOS-Richtlinien einrichten

Richtlinien bestimmen die Anforderungen für Geräte und die Aktionen, wie ausgelöst werden, wenn ein Gerät diese Anforderungen nicht erfüllt. Jede Richtlinie besteht aus einer Regel und einer Compliance-Aktion (die durchgeführt wird, wenn die Regel verletzt wird). Nutzen Sie die Seite Richtlinien zum Auswählen, Einrichten und Verteilen von Richtlinien. Datenschutz/Verschlüsselung deaktiviert und Zulässige Apps sind macOS-Richtlinien. Sie können Benutzerdefinierte Richtlinien verwenden, um eine benutzerdefinierte Richtlinie anhand der von Ihnen angegebenen Geräte- und Benutzerattribute, Abschnittskriterien, Werte und Compliance-Aktionen zu erstellen.

macOS-Apps verteilen

Ivanti Neurons for MDMApp_Catalog.htmMobileIron unterstützt die Verteilung von macOS-Apps über das MDM-Protokoll von Apple und die Mobile@Work-App.Administratoren können sich für eines oder beide der folgenden Konzepte entscheiden:

- MDM-Protokoll von Apple - Administratoren können nur bestimmte PKG-Formate (Verteilungsformate) als interne Apps hochladen und auch Apps aus dem Mac App Store verteilen (mit Unterstützung der Lizenzierung für „Apps and Books“ von Apple). Dieses Konzept erlaubt es Administratoren jedoch nicht, DMG- und andere PKG-Formate zu verteilen.
- App Mobile@Work for macOS – Um Apps an Benutzer zu verteilen, können Administratoren mit MobileIron Packager (MIP) beliebige PKG-, DMG- oder .app-Dateien in eine MIP-Datei konvertieren. Laden Sie die MIP-Datei als interne App zu Ivanti Neurons for MDM hoch.

> Ivanti Neurons for MDMSie können Mac Packager Utility von MobileIron unter „MobileIron Software Downloads“ herunterladen.

Administratoren können mit Mobile@Work hauseigene Apps verteilen, die im DMG-, PKG- oder .app-Format vorliegen. Für Apps, die nur im Mac App Store erhältlich sind, können Administratoren weiterhin die nativen MDM-Funktionen von Apple nutzen, u.a. auch die Funktionen für die „Apps and Books“-Lizensierung von Apple.

4.2. Registrierungsbestätigungs-E-Mails konfigurieren und verwenden

Administratoren können E-Mails an Benutzer konfigurieren und auslösen, nachdem sie die Registrierung abgeschlossen haben. Diese E-Mail kann z. B. zusätzliche Anweisungen für Benutzer nach der erfolgreichen Registrierung enthalten. Administratoren können den Versand dieser E-Mail während der Benutzereinladung aktivieren.

Vorgehensweise:

- **Funktion konfigurieren:**
  - Konfigurieren Sie die E-Mail-Vorlage. Die englische E-Mail-Vorlage sieht standardmäßig so aus wie hier, Sie können sie aber überarbeiten und an Ihre Zwecke anpassen, indem Sie den Anweisungen unter **E-Mail-Vorlage anpassen** unter **Branding von E-Mail-Vorlagen** folgen:



  - Aktivieren Sie die E-Mail zur Bestätigung der Registrierung. Siehe dazu **Bestätigungs-E-Mails zur Benutzerregistrierung konfigurieren**in den **Benutzereinstellungen**.
- **Funktion verwenden:**
  - Senden Sie dem Benutzer die Einladung zur Registrierung, wie unter **Benutzer einladen** beschrieben. Wenn sich der Benutzer erfolgreich registriert hat, sendet die Cloud diesem Benutzer eine E-Mail zur Bestätigung der Registrierung.

4.3. Benachrichtigungs-E-Mails zur Einhaltung von Richtlinien konfigurieren und verwenden

Administratoren können die E-Mails, die von den Richtlinien „Benutzerdefiniert“ und „Erlaubte Apps“ gesendet werden, in eine E-Mail-Vorlage zur Benachrichtigung über die Richtlinien-Compliance einbinden, um E-Mail-Aktionen an Benutzer zu senden, deren Geräte nicht mehr konform sind. Der folgende Prozess beschreibt die Konfiguration:

- **Funktion konfigurieren:**
  - **Konfigurieren Sie die E-Mail-Vorlage**.
    Die englische E-Mail-Vorlage sieht standardmäßig so aus wie hier, Sie können sie aber überarbeiten und an Ihre Zwecke anpassen, indem Sie den Anweisungen unter **E-Mail-Vorlage anpassen** unter **Branding von E-Mail-Vorlagen** folgen:
    
  - **Aktivieren Sie die Benachrichtigungsvorlage zur Richtlinien-Compliance**. Diese Vorlage funktioniert in Verbindung mit der Nachricht, die Sie mit den E-Mail-Aktionen der Richtlinien für angepasste und erlaubte Anwendungen erstellen. Cloud fügt die Informationen, die Sie in diesen E-Mail-Aktionen angeben, in die Vorlage zur Benachrichtigung über die Einhaltung von Richtlinien ein. Sie können die E-Mail-Vorlage für die Richtlinien-Compliance aktivieren, wenn Sie eine Richtlinie für angepasste oder erlaubte Apps erstellen oder bearbeiten. Weitere Informationen zur Aktivierung der Vorlage zur Benachrichtigung über die Richtlinien-Compliance einer benutzerdefinierten Richtlinie oder einer Richtlinie für erlaubte Apps finden Sie unter **Kundenspezifische Richtlinie hinzufügen** und **Richtlinie für zulässige Apps erstellen**
- **Funktion verwenden:**
  - Wenn ein Gerät bei aktivierter Richtlinienbenachrichtigungsvorlage nicht mehr mit einer Richtlinie des Typs „Benutzerdefiniert“ oder „Erlaubte Apps“ konform ist, sendet die Cloud dem Geräteeigentümer eine E-Mail, wobei die E-Mail zunächst in die Richtlinienbenachrichtigungsvorlage verpackt wird. Ihre Interaktion mit der Funktion besteht darin, diese wie oben zusammengefasst zu konfigurieren, während die Cloud selbst die Funktion nutzt.

4.4. Bei Bedarf abrufbare Funktionen.

Ivanti Neurons for MDM Die Cloud enthält bestimmte, nach Bedarf abrufbare Funktionen, die standardmäßig deaktiviert sind. Einige dieser Funktionen verschlechtern die Leistung und sind möglicherweise für die Bereitstellung in einer Produktionsumgebung noch nicht geeignet.

Administratoren können sich an den **Support** wenden, wenn sie eine oder mehrere bei Bedarf verfügbare Funktionen für ihre Mandanten aktivieren möchten, die standardmäßig deaktiviert sind.

Die folgende Tabelle enthält die Liste der dokumentierten On-Demand-Funktionen:

Funktion	Beschreibung	Plattformen	Lizenz
Funktionen für Windows 10	Funktionen, die nur für Geräte mit Windows 10 verfügbar sind.	Windows 10	• Bisher: Gold • Aktuell: Sicheres EUM Unter **Pakete** finden Sie weitere Informationen über ältere und aktuelle Angebote.
Kopieren der URL des App-Katalogs in die Zwischenablage	Administratoren können mit dieser Funktion die URL des App-Katalogs für Apps in die Zwischenablage kopieren. Diese URL kann an die Benutzer per E-Mail verteilt werden. Wenn der Benutzer auf einem registrierten Gerät auf den Link klickt, wird der App-Katalog mit der App im Browser geöffnet und der Benutzer kann die App installieren. Die Administratoren müssen die Verbreitung dieser URL auf die vorgesehenen Benutzer beschränken.	• iOS- • macOS	Entfällt - (mandantenspezifisch)
Konfigurieren Sie einen Webclip als App.	Konfigurieren Sie einen **Web-Clip** als App im App-Katalog, um die Web-Anwendung für die Benutzer im App-Katalog zur Verfügung zu stellen. Der Webclip kann als Konfiguration definiert werden, eine Konfiguration muss jedoch per Push durch den Administrator übertragen werden. Benutzer können die Web-Anwendung auf ihren Geräten installieren oder die Installation ablehnen. Eine Webclip-Konfiguration dagegen können die Benutzer nicht ablehnen.	iOS-	Entfällt - (mandantenspezifisch)
Registrierung von Whitelist-Geräten aktivieren	**User_Settings.htm**Erlauben Sie die Geräteregistrierung mit Whitelist-Seriennummern unter Benutzer > Benutzereinstellungen > Standardeinstellung für die Geräteregistrierung.	• iOS- • macOS	Entfällt - (mandantenspezifisch)
Authentifizierung mit Zertifikaten	**Die Funktion zur Authentifizierung mit Zertifikaten** ermöglicht es Administratoren, sich mit digitalen Zertifikaten und einem vom Mandanten angegebenen Hostnamen oder einem Vanity-Hostnamen anzumelden. Diese Authentifizierungseinstellung kann über die Vanity Host-Konfiguration auf der Registerkarte **Admin** konfiguriert werden.	Diese Funktion ist nicht plattformspezifisch.	Entfällt - (mandantenspezifisch) Diese Funktion ist nur in NA3-Cluster-Umgebungen verfügbar, und nur, wenn sie vom Support aktiviert wurde.

Funktion	Beschreibung	Plattformen	Lizenz
Eine dedizierte Gerätekonfiguration (für unternehmenseigene Einzweckgeräte oder COSU) erstellen	Android_Management_API.htmAdministratoren können mit Android Enterprise für einen bestimmten Zweck dedizierte Geräte konfigurieren, indem sie die dedizierten Geräte (unternehmenseigene Einzel- oder COSU-Konfiguration) verwenden. Die COSU-Konfiguration wird an die vom Unternehmen verwalteten Geräte verteilt (Geräteeigentümermodus) und stellt den Benutzern im Kioskmodus nur eine Anwendung zur Verfügung.	Android Enterprise	hinzufügen
Zeitraum für Dashboard-Inaktivität	Standardmäßig ist der Zeitraum für die Dashboard-Inaktivität auf 15 Tage festgelegt. Diese Einstellung lässt sich je nach Bedarf des Mandanten anpassen und darf maximal 30 Tage betragen. Falls Sie eine längere Inaktivitätsperiode benötigen, wenden Sie sich an das Support-Team.	Diese Funktion ist nicht plattformspezifisch.	

4.5. Vorbereiten der Android Enterprise-Geräteunterstützung

In diesem Abschnitt werden die Mindestanforderungen an das Netzwerk für Android Enterprise-Geräte beschrieben. Bei Android-Geräten müssen Sie normalerweise keine eingehenden Ports in der Firewall öffnen, damit diese ordnungsgemäß funktionieren. Es gibt jedoch eine Reihe von ausgehenden Verbindungen, die Administratoren beim Einrichten ihrer Netzwerkumgebungen für Geräte mit Android Enterprise beachten müssen.

Die Liste der Netzwerkänderungen in der folgenden Tabelle ist nicht vollständig und kann sich ändern. Sie enthält bekannte Endpunkte für aktuelle und frühere Versionen von Enterprise Management API- und GMS-Apps.

> Ivanti Neurons for MDM Zusätzlich zu den in der folgenden Tabelle aufgeführten Ports ist für Android Enterprise-Geräte Zugang zur Cloud erforderlich.

Informationen zu den Anforderungen für Android Enterprise-Geräte finden Sie im Abschnitt zu den **Android Enterprise-Netzwerkanforderungen** in der Android Enterprise-Hilfe.

Google gibt keine spezifischen IPs an, sodass Sie Ihre Firewall so einrichten sollten, dass Ihre Firewall abgehende Verbindungen zu allen IP-Adressen in den IP-Blöcken akzeptiert, die in Google ASN 15169 aufgelistet sind, siehe dazu **http://bgp.he.net/AS15169#_prefixes**.

> Die IPs von Google-Peers und Edge-Nodes sind in den AS15169-Blöcken nicht aufgeführt. Weitere Informationen zum Edge-Netzwerk von Google finden Sie unter **https://peering.google.com/**.

5. Dashboard

Das Dashboard zeigt wichtige Statistiken über registrierte Geräte und Benutzer an. Jeder Bereich auf dem Dashboard wird als Widget bezeichnet. Für jedes Widget bestimmt man:

- die Kategorie der angezeigten Daten (z. B. Geräte oder Benutzer)
- die Kriterien, nach denen die Daten angeordnet werden (z. B. nach Version oder Modell des Betriebssystems)
- die Kriterien, nach denen die Daten gefiltert werden (z. B. dass nur iOS-Geräte angezeigt werden)
- die Art, wie die Daten angezeigt werden (z. B. als Kreis- oder Balkendiagramm)

Berichte und andere Informationen überprüfen

Das **Dashboard** zeigt wichtige Statistiken über registrierte Geräte und Benutzer an. Jeder Bereich auf dem Dashboard wird als Widget bezeichnet.

Sie können zusätzliche Informationen wie folgt verifizieren:

- **Benachrichtigungen überprüfen**: Wechseln Sie zur Seite **Dashboard > Benachrichtigungen** oder klicken Sie auf das Glockensymbol (oben rechts), um die Benachrichtigungen zu überprüfen und ggf. Maßnahmen zu ergreifen.
- **Berichte**: Rufen Sie die Seite **Dashboard > Berichte** auf, um auf die Daten in Ihrem Unified Endpoint Management (UEM)-System zuzugreifen.
- **Audit-Protokolle**: Rufen Sie die Seite **Dashboard > Audit-Protokolle** auf, um auf die chronologischen Aufzeichnungen zu den Aktivitäten innerhalb von Ivanti Neurons for MDM zuzugreifen. Um diese Funktion zu aktivieren, gehen Sie auf die Seite **Admin > Audit-Protokolle** und klicken auf **Audit-Protokolle aktivieren**.
- App-Einblicke: Rufen Sie die Seite **Dashboard > App-Einblicke** auf, um die App-Verteilung und andere App-Details anzuzeigen und zu analysieren.

In diesem Abschnitt werden folgende Themen behandelt:

- Arbeiten mit Widgets
- App-Einblicke
- Verwendung geplanter Berichte
- Anpassbare Berichte verwenden

5.1. Arbeiten mit Widgets

Dieser Abschnitt enthält die folgenden Themen:

- Widget ergänzen
- Anordnen der Widgets
- Widget bearbeiten
- Benachrichtigungen überprüfen
- Berichte
- Audit-Protokolle

Das Dashboard zeigt wichtige Statistiken über registrierte Geräte und Benutzer an. Jeder Bereich auf dem Dashboard wird als Widget bezeichnet. Für jedes Widget bestimmt man:

- die Kategorie der angezeigten Daten (z. B. Geräte oder Benutzer)
- die Kriterien, nach denen die Daten angeordnet werden (z. B. nach Version oder Modell des Betriebssystems)
- die Kriterien, nach denen die Daten gefiltert werden (z. B. dass nur iOS-Geräte angezeigt werden)
- die Art, wie die Daten angezeigt werden (z. B. als Kreis- oder Balkendiagramm)

Widget ergänzen

1. Klicken Sie (oben rechts) auf **Hinzufügen**.
2. Ordnen Sie dem Widget einen Namen zu.
3. Wählen Sie eine Datenkategorie.
4. Bestimmen Sie die Filteroptionen, wenn sie angezeigt werden.
5. Wählen Sie den Standardanzeigetyp (Kreisdiagramm, Balkendiagramm, Liniendiagramm).
6. Klicken Sie auf **Fertig**.

Anordnen der Widgets

Es werden immer drei Widgets in einer Reihe angezeigt. Sie können jedoch die Reihenfolge ändern, in der die Widgets angezeigt werden:

1. Klicken Sie auf Anordnen (oben rechts).
2. Ziehen Sie die Kästchen in die gewünschte Reihenfolge, in der die Widgets angezeigt werden sollen.
3. Klicken Sie auf **OK**.

Widget bearbeiten

1. Klicken Sie auf das Einstellungssymbol des entsprechenden Widgets (oben rechts).
2. Wählen Sie **Bearbeiten**.
3. Nehmen Sie Ihre Änderungen vor.
4. Klicken Sie auf **Fertig**.

Benachrichtigungen überprüfen

Klicken Sie auf das Glockensymbol (oben rechts) oder gehen Sie auf die Seite **Dashboard > Benachrichtigungen**, um die Benachrichtigungen zu prüfen und gegebenenfalls Maßnahmen unter Berücksichtigung folgender Kriterien zu ergreifen:

- Komponentenart
  - APP
  - LDAP,
  - Entra ID
  - Geräte-Whitelist
  - Apps and Books
  - iOS-
  - Android-
  - macOS
  - visionOS
  - watchOS
  - tvOS
  - Mandant
  - CA
  - Connector
  - [Sentry]
  - Device Enrollment Server-Token

Benachrichtigungsart

  - Ablauf
  - Datensynchronisation
  - Nutzungslimit
  - Aktion des Administrators
  - Server-Authentifizierungsfehler
  - Validierungsfehler
  - Statuswechsel

[Severity]

  - Bereinigt
  - Informationen
  - Kritisch
  - Warnung

Administratoren können mit der APP-Komponente schnell alle App-spezifischen Benachrichtigungen auf der Benachrichtigungsseite sowie im Benachrichtigungsabschnitt mit dem Glockensymbol überprüfen. Wenn für Google Play-Apps neue Berechtigungen akzeptiert werden müssen, können die Administratoren diese durch einen Klick auf die Benachrichtigungen akzeptieren. Sie müssen nicht jede einzelne App-Seite aufrufen, um Berechtigungen zu überprüfen und zu akzeptieren.

> Ivanti Neurons for MDM Kunden/Mandanten erhalten die Genehmigungsbenachrichtigungen der Android Go-App auch dann, wenn die Android Go-App nicht in den App-Katalog importiert wurde.

Benutzerpasswortablauf und ID-Änderungsbenachrichtigungen überprüfen

Administratoren können auf der Seite **Benachrichtigungen** überprüfen, welche Passwörter in Kürze ablaufen. Sie werden außerdem über die Passwörter informiert, die am nächsten Tag bzw. innerhalb der kommenden zwei Wochen ablaufen und erhalten Links zu den CSV-Berichtdateien mit einer Liste der entsprechenden Benutzer. Nach Ablauf des Passworts werden keine Benachrichtigungen mehr generiert.

Die Administratoren können auch eine Benachrichtigung aufrufen, die die Benutzer auflistet, deren IDs (UIDs) während der letzten LDAP-Synchronisation geändert wurden.

Benachrichtigung löschen

Sie können diese Benachrichtigungen unabhängig vom Schweregrad nach Belieben per Hand aus der Seite **Benachrichtigungen löschen** entfernen.

1. Klicken Sie auf der Seite **Benachrichtigungen** zum Löschen einer Benachrichtigung auf das betreffende Symbol in der Spalte **Aktionen**. Das Fenster **Löschen der Benachrichtigung bestätigen** wird angezeigt.
2. Klicken Sie auf Benachrichtigung löschen. Nach dem Löschen ändert sich der Status der Benachrichtigung in der Spalte **Status** auf **gelöscht**.

> Die Gesamtzahl der gelöschten Benachrichtigungen wird auf der Seite Benachrichtigungen angezeigt.

Berichte

Auf der Seite **Dashboard > Berichte** können Sie auf die Daten in Ihrem Enterprise Mobility Management-System (UEM-System) zugreifen. So können Administratoren z.B. bei der Erstellung von Berichten über Geräte und blockierte Geräte Informationen wie den Namen des Geräte-Space und angepasste Geräteattribute mit der entsprechenden Filteroption zu Berichten hinzufügen. Dementsprechend haben diese Berichte Spalten für den Geräte-Space-Namen bzw. für angepasste Geräteattribute. Angepasste Geräteattribute sind bei der Erstellung eines Berichts unter den Filteroptionen verfügbar. Administratoren können aus der Liste der benutzerdefinierten Geräteattributschlüssel für die Geräte die verfügbaren Operatoren auswählen.

Ab Ivanti Neurons for MDM 76 gibt es für die Operatoren aller Berichtsvorlagen Standardoperatoren. Die Operatoren der folgenden Vorlagen sind in diesem Release standardisiert:

- Dashboard > Berichte > Bericht erstellen

Einen Bericht erstellen Sie wie folgt:

1. Auswahl – wählen Sie eine vordefinierte Berichtvorlage aus.
2. Bereich definieren – legen Sie den Zeitraum für die Berichtdaten fest.
3. Details definieren – geben Sie Ihrem Bericht einen Namen und passen Sie ihn nach Wunsch an.
4. Starten oder zeitlich planen – erzeugen Sie den Bericht sofort oder erstellen Sie einen Zeitplan.
5. Teilen - Definieren Sie, wer Ihren Bericht empfangen soll.

Verwandte Themen:

- Dashboard > Berichte (geplante)

- Dashboard > Berichte (anpassbare)

Schnellsuche: Navigieren Sie zur Registerkarte „Berichte“. Mit dem Feld für die Schnellsuche können Sie in den folgenden Spalten suchen und dabei auch Leer- oder Sonderzeichen einschließen:

- NAME
- BESCHREIBUNG
- NAME DER VORLAGE

Audit-Protokolle

Audit-Protokolle zeichnen chronologisch die in Ivanti Neurons for MDM durchgeführten Aktivitäten auf. Diese Datensätze umfassen Aktionen, die von Administratoren, Endbenutzern und Systemkomponenten durchgeführt werden.

Administratoren verwenden **Audit-Protokolle´**, um Änderungen zu überprüfen, Aktionen zu verifizieren, Probleme zu beheben und Compliance-Prüfungen zu unterstützen. **Audit-Protokolle** verfolgen Aktionen wie das Hinzufügen, Aktualisieren und Löschen verwalteter Entitäten, einschließlich Geräten. Weitere Informationen finden Sie unter Geräteregistrierung (iOS, macOS und Android).

Audit-Protokoll aktivieren

Aktivieren Sie die Option **Audit-Protokolle**, um die Aktivitäten zu erfassen, die innerhalb von Ivanti Neurons for MDM durchgeführt werden.

Verfahren

1. Wechseln Sie zu **Admin** > **Infrastruktur** > **Audit-Protokolle**.
   Der Bereich **Audit-Protokolle** wird angezeigt.
2. Setzen Sie den Umschalter für **Audit-Protokolle exportieren** auf EIN.

> Nach dem Aktivieren von Audit-Protokolle können Sie die Option nicht mehr deaktivieren. Wenden Sie sich zur Deaktivierung an den Support von Ivanti.

Audit-Protokolle anzeigen

Gehen Sie wie folgt vor, um weitere Details zu **Audit-Protokolle** anzuzeigen:

Verfahren

1. Wechseln Sie zu **Dashboard** > **Audit-Protokolle**.

Der Bereich **Audit-Protokolle** wird angezeigt.

2. In den folgenden Tabellen sind die Details aufgeführt, die im Bereich **Audit-Protokolle** angezeigt werden:

Einstellung	Beschreibung
Symbol	Zeigt das Aktivitätssymbol für das Prüfereignis an.
Aktivität	Zeigt die durchgeführte Aktion an, z. B. Geräte-Check-in oder Admin-Anmeldung.
[Status]	Zeigt an, ob die Aktivität erfolgreich war oder fehlgeschlagen ist. Wenn ein Bericht fehlschlägt, können Sie den Berichtsauftrag im **Berichtsverlauf** wiederholen. Verwenden Sie diese Option, um den fehlgeschlagenen Auftrag erneut auszuführen, ohne einen neuen Berichtszeitplan zu erstellen.
Durchgeführt durch	Zeigt den Administrator oder Benutzer an, der die Aktivität durchgeführt hat.
Durchgeführt am	Zeigt das Datum und die Uhrzeit an, zu der die Aktivität stattgefunden hat.
Durchgeführt am	Zeigt das Gerät, Konto oder Objekt an, das von der Aktivität betroffen ist.
Details	Zeigt zusätzliche Informationen über die Aktivität an.
Typ	Zeigt den Aktivitätstyp an, z. B. Geräteaktion oder Konto.
Kategorie	Zeigt den Funktionsbereich für die Aktivität an, z. B. Geräteverwaltung oder Zugriff auf Admin-Portal.

3. Klicken Sie auf die Schaltfläche **Aktionen**, um die folgenden Optionen auszuführen:

- **Einstellung für Audit-Protokolle konfigurieren**: Wählen Sie diese Option, um die Konfiguration **Audit-Protokolle** unter **Admin** > **Infrastruktur** > **Audit-Protokolle** anzuzeigen.
- **Als CSV-Datei exportieren**: Wählen Sie diese Option, um die **Audit-Protokolle** zu exportieren und herunterzuladen.

4. (Optional) Zeigen Sie über die **Filter** nur bestimmte **Audit-Protokolle** an.

Aktivitätsdetails anzeigen

Das Symbol für **Änderungen – vorher & nachher** wird unter **Dashboard** > **Audit-Protokolle** > **Details** (Spalte) angezeigt. Administratoren können somit Attributwerte vor und nach einer geprüften Aktion einfacher vergleichen. Dieser Vergleich erleichtert das Identifizieren durchgeführter Änderungen, das Überprüfen der Benutzer- oder Systemaktivität sowie die Fehlerbehebung bei Konfigurationsupdates.

Klicken Sie auf das Symbol, um die Details zum Audit-Protokoll-Vergleich im Bereich **Audit Protokolle: Änderungen – vorher & nachher** anzuzeigen. Folgendes werden aufgeführt:

Einstellung	Beschreibung
Attribut	Zeigt den Namen des modifizierten Attributs an. Beispiel: `createdAt`.
Vorher	Zeigt den Attributwert an, bevor die Aktion durchgeführt wurde. Wird rot hervorgehoben.
Nach	Zeigt den Attributwert an, nachdem die Aktion durchgeführt wurde. Wird grün hervorgehoben.

Erweiterte Suche für Audit-Protokolle

Verwenden Sie die Option "Erweiterte Suche", um Audit-Protokolle basierend auf Regeln zu durchsuchen. Definieren Sie spezifische Kriterien, um Aktivitäten zu identifizieren und anzuzeigen. Sie können die folgenden Attribute heranziehen, um eine erweiterte Suche durchzuführen:

- **Aktivität**
- **Kategorie**
- **Erstellt um**
- **Durchgeführt durch**
- **Durchgeführt am**
- **Space-Name**
- **[Status]**
- **Typ**

Berichte für Audit-Protokolle erstellen

Sie können **Audit-Protokolle**-Berichte so planen, dass sie alle 12 oder 24 Stunden ausgeführt werden, oder aber benutzerdefinierte Berichte erstellen. Zusätzlich lassen sich **Audit-Protokolle**-Berichte nach Bedarf ausführen. On-Demand-Berichte sind nicht geplant und enthalten die **Audit-Protokolle**-Daten der letzten 24 Stunden.

Sie können einen Audit-Protokolle-Bericht in folgenden Formaten erstellen:

- CSV
- JSON
- CEF

Zusätzlich können Sie beim Erstellen eines Berichts für **Audit-Protokolle** > **Berichtverteilung die Option SFTP-Export auswählen**, um alle Audit-Protokolle-Informationen zu exportieren und zu einem bestimmten Server hochzuladen. Für den Export von Audit-Protokollen wird SFTP verwendet (Secure Shell File Transfer Protocol). Der Server muss über den Standardport zugänglich sein. Sie können die Einstellungen für den **Audit-Protokolle-Export** so konfigurieren, dass die Audit-Protokolle-Archive täglich automatisch an einen bestimmten Speicherort hochgeladen werden. Weitere Informationen finden Sie unter **Audit-Protokolle exportieren**.

Weitere Informationen zum Erstellen eines Berichts finden Sie unter **Verwendung geplanter Berichte** und **Anpassbare Berichte verwenden**.

5.2. App-Einblicke

Dieser Abschnitt enthält die folgenden Themen:

- App-Verteilung anzeigen
- App-Details anzeigen
- Diagramme zur Verteilung einzelner Apps hinzufügen
- Diagramm für nicht verwaltete iOS-Apps hinzufügen
- Die 10 meistinstallierten verwalteten Apps hinzufügen
- Die 5 am besten bewerteten internen Apps hinzufügen

App Insights ist eine Funktion im Dashboard, mit der Sie die folgende App-Verteilung anzeigen und analysieren können:

- Verteilung einer hauseigenen App mit Installation
- Verteilung einer öffentlichen App mit Installation
- Nicht verwaltete iOS-Apps
- Die wichtigsten 10 installierten verwalteten Apps
- Die 5 wichtigsten internen Apps

Analyse der 5 wichtigsten Apps, die installiert werden müssen: Dies sind eigene oder öffentliche Apps, die an viele Benutzer verteilt, aber relativ selten installiert wurden. Die Tabelle mit den nicht verwalteten iOS-Apps zeigt an, welche Apps auf den Geräten nicht verwaltet werden. Sie können die Liste der nicht verwalteten Apps sowie die Geräte anzeigen, auf denen sie installiert sind, und die App in eine verwaltete App umwandeln. Dies sind die App-Verteilungen, bei denen ein Administrator eingreifen muss, um die Verteilung zu verbessern. Diese Übersichten zeigen grafisch die Geräte, auf denen die App bereits installiert ist. Das Tortendiagramm stellt eine allgemeine Übersicht über die Verteilung der öffentlichen und eigenen Apps dar; dies hilft nicht nur bei der Analyse der Zahl der Geräte, auf denen die App noch installiert werden muss, sondern ermöglicht auch eine Detailsuche, um weitere App-spezifische Informationen zu erhalten. Klicken Sie dazu auf den spezifischen Bereich des Diagramms. Sie können außerdem auch ein einzelnes Verteilungsprogramm hinzufügen, das die versionsspezifische Verteilung einer bestimmten einzelnen App darstellt.

> Das Dashboard zeigt nur Informationen zu Geräten an, die sich in den letzten 15 Tagen angemeldet haben.

App-Verteilung anzeigen

Gehen Sie auf die Seite **Apps** unter **Dashboard**, um folgende Diagramme anzuzeigen:

- Verteilungen hauseigener Apps mit Installation
- Verteilungen öffentlicher Apps mit Installation
- Nicht verwaltete iOS-Apps

Standardmäßig werden die Tabellen für 5 eigene sowie 5 öffentliche Apps und für nicht verwaltete iOS-Apps angezeigt. Die Grafiken sind von links nach rechts beginnend mit der App mit der höchsten Nichtinstallationsrate sortiert.

Das Tortendiagramm zeigt in zwei Farben den Installationsstatus an. Blau steht für die Geräte, auf denen die App installiert ist. Rot zeigt die Anzahl der Geräte, auf denen die Installation noch ausgeführt werden muss. Die Zahl der Geräte wird angezeigt, wenn Sie den Mauszeiger über die jeweilige Farbregion bringen.

Sie können ein Diagramm löschen, indem Sie auf die Löschoption in der Ecke oben rechts im Diagramm klicken.

App-Details anzeigen

Die Mitte des Tortendiagramms zeigt außerdem die Anzahl der Geräte an, bei denen die Installation noch ausgeführt werden muss. Beispiel: 750/1000 bedeutet, dass bei 750 von 1000 Geräten noch eine Installation erforderlich ist.

Das Tortendiagramm zeigt in 3 Farben die Verteilung der App an.

- Blau bezieht sich auf die Anzahl der Geräte, auf denen die App installiert ist. Wenn Sie in den blauen Bereich des Diagramms klicken, wechseln Sie zur Seite **Geräte**. Auf der Seite **Geräte** zeigt die Spalte **App-Version** die installierte App-Version und das Datum der App-Installation an.

> Sie können für die Geräte auch die installierten App-Versionen anzeigen, wenn Sie die entsprechenden Versionen im Abschnitt Versionen im linken Fenster auswählen.

- Der rote Bereich zeigt die Anzahl der Geräte, auf denen die App noch installiert werden muss. Klicken Sie in den roten Bereich des Diagramms, um zur Seite **Geräte** zu wechseln. Auf der Seite **Geräte** können Sie die Geräte anzeigen, auf denen die App noch installiert werden muss.

In der Mitte des Diagramms wird ein App-Symbol angezeigt. Wenn Sie auf das Symbol klicken, wechseln Sie zur Seite mit den App-Details unter **Apps> App-Katalog**.

Klicken Sie auf die Registerkarte **Geräte mit installierter App**, um die Liste der Geräte anzuzeigen, bei denen die ausgewählte App installiert ist.

Klicken Sie auf die Registerkarte **Geräte ohne installierte App**, um eine Liste der Geräte anzuzeigen, bei denen die ausgewählte App nicht installiert ist.

Diagramme zur Verteilung einzelner Apps hinzufügen

Sie können Tortendiagramme mit der Einzelverteilung einer bestimmten Version einer App auf der Seite „Apps“ hinzufügen. Der rote Bereich enthält die Liste der qualifizierten Geräte, auf denen die App installiert sein müsste. Diese Diagramme stellen grafisch die folgenden Details zur App-Verteilung dar:

- Geräte, auf denen eine bestimmte Version der App installiert ist.
- Geräte, auf denen andere Versionen der App installiert sind.
- Geräte, auf denen die App nicht installiert ist.

Verfahren

1. Klicken Sie auf der Seite **Apps** auf **+Hinzufügen**. Das Fenster **App-Diagramm hinzufügen** wird angezeigt.
2. Wählen Sie in der Dropdown-Liste **Diagrammart** die Option **Verteilung einer einzelnen App** aus.
3. Klicken Sie in das Kontrollkästchen der App-Liste, für die Sie die Verteilung einer einzelnen App als Diagramm anzeigen wollen.

> Sie können alternativ nach einer bestimmten App suchen, indem Sie den App-Namen in dem Feld „Suche nach Apps“ eingeben.

4. Klicken Sie auf **Tabelle hinzufügen**. Die Verteilungsdiagramme für die einzelne App werden auf der Seite „Apps“ angezeigt.

> Sie können aus der Liste maximal 9 Apps auswählen.

In der Mitte des Diagramms steht die Anzahl der Geräte, auf denen die angegebene App-Version installiert ist.

Beispiel: 5/10 bedeutet, dass auf 5 von 10 Geräten die angegebene App-Version installiert ist.

Das Tortendiagramm zeigt in 3 Farben die Verteilung der App an.

- Der grüne Bereich steht für die Geräte, auf denen eine bestimmte Version der App installiert ist. Klicken Sie in den grünen Bereich des Diagramms, um zur Seite **Geräte** zu wechseln. Diese Seite zeigt eine Liste der Geräte, auf denen die angegebene Version der App installiert ist. Sie können auch Geräte anzeigen, bei denen andere Versionen der App installiert sind, indem Sie die Optionen zur **App-Version** im linken Fenster ändern.
- Der hellgrüne Bereich steht für die Geräte, auf denen andere Versionen der App installiert sind. Klicken Sie in den hellblauen Bereich des Diagramms, um zur Seite **Geräte** zu wechseln. Diese Seite zeigt in einer Liste die Geräte an, auf denen andere Versionen der App installiert sind. Sie können auch die Geräte anzeigen, bei denen andere App-Versionen installiert sind, indem Sie die Versionsoptionen im Abschnitt **App-Version** im linken Fenster ändern.
- Rot steht für die Geräte, auf denen die App nicht installiert ist. Die Zahl der Geräte wird angezeigt, wenn Sie den Mauszeiger über die jeweilige Farbregion bringen. Klicken Sie in den roten Bereich des Diagramms, um zur Seite **Geräte** zu wechseln und die Geräte anzuzeigen, auf denen die App nicht installiert ist. Das linke Fenster zeigt außerdem an, seit wann die App im App-Katalog verfügbar ist.

In der Mitte des Diagramms wird ein App-Symbol angezeigt. Wenn Sie auf das Symbol klicken, wechseln Sie zur Seite mit den App-Details unter **Apps> App-Katalog**. Klicken Sie auf die Registerkarte **Geräte mit installierter App**, um die Liste der Geräte anzuzeigen, bei denen die ausgewählte App installiert ist. Klicken Sie auf die Registerkarte **Geräte ohne installierte App**, um eine Liste der Geräte anzuzeigen, bei denen die ausgewählte App nicht installiert ist.

Sie können ein Diagramm löschen, indem Sie auf die Löschoption in der Ecke oben rechts im Diagramm klicken.

Diagramm für nicht verwaltete iOS-Apps hinzufügen

Sie können eine Liste der nicht verwalteten Apps in der Tabelle für nicht verwaltete iOS-Apps auf der Seite „Apps“ identifizieren und anzeigen. Diese Tabelle wird automatisch angezeigt, wenn ein Administrator dem Katalog eine nicht verwaltete iOS-App hinzufügt. Der Administrator kann diese Tabelle nach Bedarf löschen oder ergänzen.

Verfahren

1. Klicken Sie auf der Seite **Apps** auf **+Hinzufügen**. Das Fenster **App-Diagramm hinzufügen** wird angezeigt.
2. Klicken Sie in der Dropdown-Liste **Tabellenart** auf **Nicht verwaltete Apps**.
3. Klicken Sie auf **Tabelle hinzufügen**. Die Tabelle mit den nicht verwalteten iOS-Apps wird auf der Seite **Apps** angezeigt.

Sie sehen in der Tabelle, wie viele Apps im App-Katalog nicht verwaltet werden. Am unteren Rand der Tabelle finden Sie 3 Spalten mit folgenden Details:

- **Geräte mit nicht verwalteten iOS-Apps**: Gibt die Anzahl der nicht verwalteten iOS-Apps an. Klicken Sie auf den Link, um die Liste der Geräte mit nicht verwalteten Apps in dem Fenster „Geräte mit nicht verwalteten iOS-Apps“ anzuzeigen.
- **Gesamtzahl der Apps im App-Katalog**: Zeigt die Gesamtzahl der Apps im App-Katalog an.
- **Nicht verwaltete iOS-Apps in %**: Gibt die Anzahl der nicht verwalteten iOS-Apps in Prozent an.

Wenn eine App bereits direkt über den iTune App Store installiert ist, können Sie die App und die Daten der App in eine verwaltete App übernehmen. So konvertieren Sie diese App in eine verwaltete App:

1. Klicken Sie auf den Zahlenlink in der Spalte **Geräte mit nicht verwalteten iOS-Apps**. Das Fenster **Nicht verwaltete iOS-Apps** wird angezeigt.

2. Wählen Sie mindestens eine nicht verwaltete App aus der Liste und klicken Sie auf den Zahlenlink unter „Nicht verwaltete iOS-Apps“. Die ausgewählten Apps werden in verwaltete Apps konvertiert; der Status wird bei der nächsten Geräteanmeldung aktualisiert.

> Sie können die Daten von nicht verwalteten Apps im CSV-Format exportieren, wenn Sie auf den Link Als CSV-Datei exportieren klicken.

Die 10 meistinstallierten verwalteten Apps hinzufügen

Sie können die zehn wichtigsten installierten verwalteten Apps identifizieren und in der Tabelle der 10 wichtigsten installierten verwalteten Apps auf der App-Seite anzeigen. Der Administrator kann diese Tabelle nach Bedarf löschen oder ergänzen.

Standardmäßig ist auf der Seite Apps die Tabelle mit den wichtigsten zehn installierten verwalteten **Apps** verfügbar. Wenn die Tabelle gelöscht wurde, kann der Administrator sie über die Seite **Apps** ergänzen.

Verfahren

1. Klicken Sie auf der Seite **Apps** auf **+Hinzufügen**. Das Fenster **App-Diagramm hinzufügen** wird angezeigt.
2. Wählen Sie in der Dropdown-Liste **Tabellenart** die Tabelle **Die 10 wichtigsten installierten verwalteten Apps** aus.
3. Klicken Sie auf **Tabelle hinzufügen**. Die Tabelle der wichtigsten 10 installierten verwalteten Apps wird auf der Seite **Apps** angezeigt.

Sie können die wichtigsten 10 installierten verwalteten Apps nach Kategorie sortiert in der Dropdown-Liste **Zeigen** auswählen. Die verfügbaren Kategorien sind:

- **Alle Apps** (standardmäßig ausgewählt)
- **Interne Apps**
- **Öffentliche Apps**

Jeder Balken in der Tabelle steht für eine bestimmte App, der Name der App wird ebenfalls angezeigt. Bewegen Sie den Mauscursor über den jeweiligen Balken, um die Plattform (Android, iOS oder Windows) und die Anzahl der Geräte anzuzeigen, auf denen die App installiert ist.

Wenn Sie auf den Balken einer bestimmten App klicken, wird die Seite **Geräte** mit den Details der Geräte angezeigt, auf denen die App installiert ist. Die linke Hälfte der Geräteseite zeigt die Anzahl der Geräte an, auf denen die App installiert ist. Klicken Sie auf das Symbol X in der linken Hälfte, um wieder die Seite **Apps** im Dashboard anzuzeigen.

Sie können eine Tabelle löschen, indem Sie auf die Löschoption in der Ecke oben rechts in der Tabelle klicken.

Die 5 am besten bewerteten internen Apps hinzufügen

Sie können die 5 am besten bewerteten internen Apps in der Tabelle der 5 am besten bewerteten internen Apps auf der App-Seite identifizieren und anzeigen. Der Administrator kann diese Tabelle nach Bedarf löschen oder ergänzen.

Standardmäßig ist die Übersicht mit den 5 am besten bewerteten internen Apps auf der Seite **Apps** verfügbar. Wenn die Tabelle gelöscht wurde, kann der Administrator sie über die Seite **Apps** ergänzen.

Verfahren

1. Klicken Sie auf der Seite **Apps** auf **+Hinzufügen**. Das Fenster **App-Diagramm hinzufügen** wird angezeigt.
2. Wählen Sie in der Dropdown-Liste **Tabellenart** die Tabelle **Die 5 wichtigsten installierten verwalteten Apps** aus.

3. Klicken Sie auf **Tabelle hinzufügen**. Die Tabelle der wichtigsten 5 installierten verwalteten Apps wird auf der Seite **Apps** angezeigt.

Diese Tabelle zeigt die Daten durch ein Logo der App und die Bewertung der App mit Sternchen an. Die Sternchenbewertung wird durch Sternchensymbole sowie durch Integerzahlen ersetzt (maximale Bewertung = 5). Die Anzahl der Benutzer, die die App bewertet haben, wird ebenfalls angezeigt.

> Die Anzahl der Bewertungen für eine App ist nicht nur auf diesen Administrator und Raum beschränkt, sondern basiert auf den Bewertungen aller Benutzer der App. Die Bewertung ist der Mittelwert aller Bewertungen für die App durch verschiedene Benutzer, die die App über Apps@Work auf ihren registrierten Geräten angezeigt haben.

Bei einem Klick auf die entsprechende App erscheint die Seite **App-Details** mit spezifischen Details der App.

Sie können eine Tabelle löschen, indem Sie auf die Löschoption in der Ecke oben rechts in der Tabelle klicken.

5.3. Verwendung geplanter Berichte

Lizenz: Silver

Mit der Funktion für geplante Berichte können Sie mit sofort verwendbaren vordefinierten Vorlagen Berichte zu verschiedenen Kennzahlen planen und erstellen. Sie müssen die Rolle als Systemadministrator oder eine schreibgeschützte Rolle für das System haben, wenn Sie diese Funktion aufrufen wollen. Sie können derzeit maximal 40 Berichte erstellen.

> Der Bericht über Richtlinienverstöße enthält möglicherweise mehrere Datensätze für dasselbe Gerät, wenn für das Gerät mehrere Tunnelinstanzen erstellt wurden. Dies gilt sowohl für Standardberichte als auch für benutzerdefinierte Berichte.

Erstellen eines Berichts

Sie können einen Bericht planen und generieren.

Verfahren

1. Wechseln Sie zu **Dashboard** > **Berichte**.
2. Klicken Sie auf die Option Bericht erstellen, um die Seite „Berichtvorlage auswählen“ anzuzeigen.
3. Wählen Sie eine Vorlage für Ihren Bericht aus den Optionen aus, die Sie konfiguriert haben.
   - **Gesperrte Geräte**: Bericht über Geräte, deren Zugriff durch Sentry derzeit gesperrt ist.
   - **Geräte**: Bericht über die Geräte aller Partitionen Ihres Systems.
   - **Richtlinienverletzungen**: Bericht über Richtlinienverletzungen in Ihrem System.
   - **Benutzer**: Bericht über die Benutzer in Ihrem System.
   - **Ablaufstatus des Benutzerkennworts**: Bericht zum Ablaufstatus der Benutzerkennwörter in Ihrem System.
   - **Am häufigsten installierte Apps**: Bericht über alle Anwendungen in Ihrem System, sortiert nach der Anzahl der Installationen je Anwendung.
   - **Nicht verwaltete Apps**: Bericht über die nicht verwalteten Anwendungen in Ihrem System.
   - **Alle Anwendungen**: Bericht über alle Anwendungen auf von Ihnen verwalteten Geräten.
   - **Audit-Protokolle**: Bericht über sämtliche Aktivitäten, die auf allen Entitäten innerhalb von Ivanti Neurons for MDM durchgeführt wurden.
4. Klicken Sie auf **Weiter**.
   Die Seite **Berichtdetails** wird angezeigt.
   - Geben Sie einen **Bericht-Namen** ein.
   - (Optional) Geben Sie für den Bericht eine **Beschreibung** ein.

Wählen Sie für den **Ereignisbereich** aus folgenden Optionen:
Für vorhandene Berichte:

- **Alle Ereignisse**
- **Vorheriger Tag**
- **Vorherige Woche**
- **Vorheriger Monat**

- **Vorheriger Bereich** – Zeigt den Bericht an, der mithilfe des Schiebereglers für den Bereich über das vorherige Release des Ivanti Neurons for MDM-Administrationsportals erstellt wurde. Wenn der Administrator eine der obigen Optionen für einen Bericht auswählt und speichert, wird die Option "Vorheriger Bereich" nicht angezeigt. Der Bereichswert ist nur auf der Seite "Berichtsübersicht" verfügbar.

Für neue Berichte:

- **Alle Ereignisse**
- **Vorheriger Tag**
- **Vorherige Woche**
- **Vorheriger Monat**

Klicken Sie auf **Weiter**. Die Seite "Berichtsdaten" wird angezeigt.

6. Klicken Sie auf **Spalten anpassen**, um im Abschnitt **Berichtspalten** Spalten hinzuzufügen, zu entfernen oder neu anzuordnen. Klicken Sie alternativ auf den Spaltennamen, um die hinzugefügte Spalte zu entfernen.
7. (Optional) Aktivieren Sie das Kontrollkästchen **Alle Spalten auswählen**, um alle in der Liste angezeigten Salten gleichzeitig auszuwählen.
8. Klicken Sie auf die Option Standardeinstellungen wiederherstellen, um wieder die zuvor erstellten Spalten anzuzeigen. Um die Spalten wieder anzuzeigen, ohne Anpassungen vorzunehmen, können Sie eine der Vorlagen auf der Seite **Berichtvorlage auswählen** wählen.
9. Erstellen Sie Filter mit den spezifischen Regeln des Abschnitts **Erweiterte Filter**.

> Es sind nicht alle Filteroptionen für alle Berichte verfügbar. Weitere Informationen zur Liste der verfügbaren Filter finden Sie beim Thema **Filter** unter diesem Verfahren.

> Die folgenden neuen Hardwareattribute sind für Windows-Geräte beim Erstellen von Berichten verfügbar: BitLocker-Verschlüsselung, Betriebssystemedition, Systemversion, Platinenhersteller, Platinenprodukt, Platinenstatus, BIOS-Hersteller, BIOS-Version, Festplattenpartitionen, Optischer Laufwerktstyp, CPU-Name und CPU-Status.

10. (Optional) Klicken Sie auf das Symbol **+**, um eine andere Regel hinzuzufügen, oder auf das Symbol **Gruppe hinzufügen**, um eine andere Gruppe mit Regeln hinzuzufügen.
11. Klicken Sie auf **Weiter**. Die Seite "Berichtszeitplan" wird angezeigt.
12. Wählen Sie *eines* der folgenden Formate zum Herunterladen des Berichts aus:
    - CSV
    - PDF
    - **CSV und PDF**
      Bei PDF-Berichtdateien sind bis zu 10 Spalten zulässig. Im Abschnitt "Berichtsdiagramme" werden zwei Diagrammtypen angezeigt, die in den PDF-Berichten zulässig sind.
      Der Bericht **Alle Anwendungen** unterstützt nur das CSV-Format.

Klicken Sie auf **Automatisch planen**, um einen automatisch auszuführenden Bericht einzurichten, indem Sie die Häufigkeit festlegen. Klicken Sie alternativ auf **Manuell**, um den Bericht einmal auszuführen und per E-Mail zu erhalten.

- Wählen Sie *eine* der Optionen für **wiederkehrende Berichte** aus:
  - **Täglich**

        - **Wöchentlich**
        - **Monatlich**
        - **Vorheriger Zeitplan** – für vorhandene Berichte
    - Wählen Sie das **Startdatum** und (optional) das **Enddatum** aus.
14. Klicken Sie auf **Weiter**. Die Seite "Berichtverteilung" wird angezeigt. Wählen Sie die Empfänger für den Bericht aus.
15. (Optional) Fügen Sie externe E-Mail-IDs hinzu, indem Sie auf den Link **Externe E-Mail hinzufügen** klicken.
16. Klicken Sie auf **Fertig**. Die **Berichtverteilung** – **Übersicht** wird angezeigt.
17. (Optional) Klicken Sie auf **Bearbeiten**, um den Bericht anzupassen.
18. Klicken Sie auf **Speichern**.
19. Klicken Sie auf das Symbol zum Herunterladen, um das Format des Berichts auszuwählen. Eine E-Mail mit der Schaltfläche **Bericht herunterladen** zum Herunterladen des Berichts wird an die Empfänger des Berichts gesendet.

Filter

Regeloptionen	Beschreibung
Aktivierungssperre aktiviert	Die rollenabhängige Aktivierungssperre wird mit **JA** oder **NEIN** aktiviert. Beispiel für eine Regel: „Aktivierungssperre aktiviert hat Status JA“.
App-Tunnel-Status	Regel für den Apptunnel-Status **SPERREN** oder **ZULASSEN**. Beispiel für eine Regel: Apptunnel-Status ist „Sperre“.
Akkustand	Akkuzustand des Gerätes Beispiel einer Regel:'Batteriezustand ist gleich 1080' Der eingegebene Wert für den Batterieladezustand sollte in Sekunden angegeben werden.
Letzte Client-Anmeldung	Regel basierend auf der letzten Anmeldung des Clients innerhalb des Datumsbereichs. Beispiel für die Regel: „Letzte Client-Anmeldung zwischen dem 02.04.2019, 06:00:00 Uhr und dem 05.04.2019, 17:00:00 Uhr.“
Compliance-Status	Regel für den Compliance-Status, d. h. **JA** oder **NEIN**. Beispiel für eine Regel: "Compliance-Status gleich Ja".
Aktueller Ländername	Geben Sie den aktuellen Ländernamen ein. Beispiel für eine Regel: „Compliance-Status gleich Frankreich“.
Aktueller MCC	Die Regel basiert auf dem aktuellen Mobilfunk-Ländercode. Regelbeispiel: 'Aktueller MCC ist gleich 410'.
Aktueller MNC	Die Regel basiert auf dem aktuellen Mobilfunknetzcode. Regelbeispiel: 'Aktueller MNC ist gleich 06'.
Geräteregistrierung aktiviert	Regelabhängige Geräteregistrierung, mit **JA** bzw. **NEIN** aktiviert. Regelbeispiel: „Aktivierte Geräteregistrierung entspricht JA.“
Nativer Anti-Phishing-Status	Wählen Sie eine der folgenden Optionen für den Nativen Anti-Phishing-Status aus: • Ist gleich • ist nicht gleich Mögliche Werte: • Nicht aktiviert • Nicht zutreffend • Aktiviert • Unbekannt
Anti-Phishing-VPN-Status	Wählen Sie eine der folgenden Optionen für den Anti-Phishing-VPN-Status aus: • Ist gleich • ist nicht gleich Mögliche Werte: • Nicht aktiviert • Nicht zutreffend • Aktiviert

Regeloptionen	Beschreibung
	• Unbekannt
In der Geräteregistrierung registriert	Regel basierend auf der Registrierung in der Geräteregistrierung mit **Ja** oder **Nein**. Regelbeispiel: 'In der Geräteregistrierung registriert ist gleich Ja'
Datenschutz	Zeigt an, ob der Datenschutz auf dem Gerät aktiviert ist. Mögliche Werte sind **Ja** und **Nein**. Beispiel einer Regel: „Datenschutz ist gleich JA'.
Daten-Roaming aktiviert	Regel zum Daten-Roaming, aktiviert mit **JA** oder **NEIN**. Beispiel für eine Regel: „Daten-Roaming aktiviert, falls Status JA ist.“
Geräte-Sperrstatus	Die Regel basiert auf dem Geräte-Sperrstatus. Regelbeispiel: 'Geräte-Sperrstatus ist Sperre'
Geräte-ID	Regel für eine bestimmte Geräte-ID oder einen Bereich von Geräte-IDs. Beispiel für die Regel: "Geräte-ID größer 45". X
Inlands-MCC	Die Regel basiert auf dem Ländercode für das Inlands-Mobilfunknetz. Regelbeispiel: „Inlands-MCC ist gleich 310'.
Eigener MNC	Die Regel basiert auf dem Inlands-Mobilfunknetzcode. Regelbeispiel: 'Inlands-MNC ist gleich 510'.
IMEI	Regel für einen spezifischen IMEI-Wert. Beispiel für die Regel: "IMEI beginnt mit 9900"
Einladestatus	Wählen Sie eine der folgenden Einladungsstatusoptionen aus: • Kein/e • Ausstehend • Abgelaufen • **Abgeschlossen** Beispiel für die Regel: "Einladungsstatus gleich Ausstehend".
Standortdatendienst aktiviert	Regel für den Standortdienst aktiviert mit **JA** oder **NEIN**. Beispiel für die Regel: „Standortdienst aktiviert hat Status JA.“
MTD-Aktivierungsstatus	Wählen Sie eine der folgenden Optionen für den MTD-Aktivierungsstatus aus: • Ist gleich • ist nicht gleich Mögliche Werte sind: • Nicht zutreffend • Fehler • Ausstehend • Geschützt
Quarantänestatus	Regel für den Standortdienst aktiviert mit **JA** oder **NEIN**. Beispiel für eine Regel: „Roaming ist gleich JA"

Regeloptionen	Beschreibung
Registriert bei	Die Regel zur Auswahl des Datums- und Zeitbereichs, in dem das Gerät registriert wurde. Beispiel für die Regel: „Registriert zwischen dem 03.10.2017, 09:00:00 Uhr und dem 20.10.2017, 17:00:00 Uhr.“
Roaming	Regel je nach Roaming, d. h. **JA** oder **NEIN**. Beispiel für eine Regel: "Roaming gleich Ja'
[Status]	Wählen Sie eine der folgenden Einladungsstatusoptionen aus: • Aktiv • Außerdienststellung ausstehend • Außerdienststellung gesendet • Außer Dienst gestellt • Außerdienststellung abgebrochen • Wipe ausstehend • Wipe gesendet • Wipe abgeschlossen • Wipe abgebrochen Regelbeispiel: "Status ist gleich Abschaltung ausstehend".
Voice-Roaming aktiviert	Regelabhängiges Voice-Roaming, mit **JA** bzw. **NEIN** aktiviert. Regelbeispiel: aktiviertes "Voice-Roaming entspricht "Ja","
WLAN-MAC-Adresse	Geben Sie eine bestimmte MAC-Adresse ein. Beispiel für die Regel: "WLAN-Mac-Adresse entspricht nicht 00-14-22-01-23-45".
iCloud-Datensicherung aktiviert	Regel für die Datensicherung in der iCloud aktiviert mit **JA** oder **NEIN**. Beispiel einer Regel: „Cloud-Datensicherung aktiviert ist gleich JA.“
Aktivierungsstatus des iTunes Store-Kontos	Regel für Aktivierungsstatus des iTunes Store-Kontos **JA** oder **NEIN**. Beispiel für die Regel: Aktivierungsstatus für das iTunes Store-Konto ist nicht „NEIN“.
Plattformtyp	Gilt für den Bericht "Alle Anwendungen".
Quelle	Gilt für den Bericht "Alle Anwendungen".
Benutzerdefinierte Attribute	Gilt für den Bericht "Alle Anwendungen".
Verwaltet	Gilt für die Berichte "Alle Anwendungen" und "Am häufigsten verwendete Anwendungen".
App-Identifikator	Standardeinstellung für den Bericht "Alle Anwendungen".
MEID	Gilt für den Bericht "Nicht verwaltete Apps".

Ausführen von Aktionen für einen Bericht über die Seite "Geplante Berichte"

Sie können diverse Aktionen auf der Seite "Geplante Berichte" ausführen.

Verfahren

1. Wechseln Sie zu **Dashboard** > **Berichte**.
2. Klicken Sie auf der Seite **Meine geplanten Berichte** auf das Dropdownmenü **Aktionen**, und wählen Sie eine der folgenden Optionen aus:

Aktionsoptionen	Durchgeführte Aktion
Anzeigen	Ermöglicht Ihnen, den Bericht anzuzeigen.
Bearbeiten	Ermöglicht Ihnen, den Bericht zu bearbeiten. Der Bericht zeigt außerdem den Bereich an, der im letzten Release ausgewählt wurde (Vorheriger Bereich).
Jetzt ausführen	Führt den Bericht aus.
CSV herunterladen	Lädt den Bericht im CSV-Format herunter.
PDF herunterladen	Lädt den Bericht im PDF-Format herunter.
Löschen	Löscht den Bericht.

Anzeigen von Berichtsdetails

Sie können die Berichtsdetails anzeigen und einige Aktionen für den erstellten Bericht ausführen.

Verfahren

1. Wechseln Sie zu **Dashboard** > **Berichte**.
2. Klicken Sie zum Anzeigen der Berichtsdetails auf der Seite **Meine geplanten Berichte** auf den Berichtsnamen. Die Berichtsseite wird geöffnet.
3. Auf dieser Seite werden die Berichtsübersicht und der Berichtsverlauf angezeigt.

Verwandte Themen:

- Weitere Informationen zum Zuweisen einer kundenspezifischen Rolle für einen Benutzer finden Sie unter **Rollen zuweisen**.
- Unter **Benutzerrollen** finden Sie eine Liste der Standardrollen.
- **Rollenverwaltung**
- **Anpassbare Berichte verwenden**

5.4. Anpassbare Berichte verwenden

Lizenz: Gold

Mit der anpassbaren Berichtsfunktion können Sie Berichte mit verschiedenen Metriken aus fertigen Vorlagen erstellen und anpassen. Sie müssen die Rolle als Systemadministrator oder eine schreibgeschützte Rolle für das System haben, wenn Sie diese Funktion aufrufen wollen. Sie können derzeit maximal 40 Berichte erstellen.

Dieser Abschnitt enthält die folgenden Themen:

Bericht erstellen

Ausführen von Aktionen für einen Bericht

Anzeigen von Berichtsdetails

Bericht erstellen

Sie können Berichte über das Ivanti Neurons for MDM-Administrationsportal planen und generieren.

Verfahren

1. Wechseln Sie zu **Dashboard** > **Berichte**.
2. Klicken Sie auf die Option Bericht erstellen, um die Seite „Berichtvorlage auswählen“ anzuzeigen.
3. Wählen Sie eine Vorlage für Ihren Bericht aus den Optionen aus, die Sie konfiguriert haben.
   - **Gesperrte Geräte**: Bericht über Geräte, deren Zugriff durch Sentry derzeit gesperrt ist.
   - **Geräte**: Bericht über die Geräte aller Partitionen Ihres Systems.
   - **Richtlinienverletzungen**: Bericht über Richtlinienverletzungen in Ihrem System.
   - **Benutzer**: Bericht über die Benutzer in Ihrem System.
   - **Ablaufstatus des Benutzerkennworts**: Bericht zum Ablaufstatus der Benutzerkennwörter in Ihrem System.
   - **Am häufigsten installierte Apps**: Bericht über alle Anwendungen in Ihrem System, sortiert nach der Anzahl der Installationen je Anwendung.
   - **Nicht verwaltete Apps**: Bericht über die nicht verwalteten Anwendungen in Ihrem System.
   - **Alle Anwendungen**: Bericht über alle Anwendungen auf von Ihnen verwalteten Geräten.
   - **Audit-Protokolle**: Bericht über sämtliche Aktivitäten, die auf allen Entitäten innerhalb von Ivanti Neurons for MDM durchgeführt wurden.
4. Klicken Sie auf **Weiter**. Die Seite "Berichtdetails" wird angezeigt.
5. Geben Sie einen **Bericht-Namen** ein.
6. (Optional) Geben Sie für den Bericht eine **Beschreibung** ein.
7. Wählen Sie für den **Ereignisbereich** aus folgenden Optionen:
   Für vorhandene Berichte:
   - **Alle Ereignisse**
   - **Vorheriger Tag**
   - **Vorherige Woche**
   - **Vorheriger Monat**

- **Vorheriger Bereich** – Zeigt den Bericht an, der mithilfe des Schiebereglers für den Bereich über das vorherige Release des Ivanti Neurons for MDM-Administrationsportals erstellt wurde. Wenn der Administrator eine der obigen Optionen für einen Bericht auswählt und speichert, wird die Option "Vorheriger Bereich" nicht angezeigt. Der Bereichswert ist nur auf der Seite "Berichtsübersicht" verfügbar.

Für neue Berichte:

- **Alle Ereignisse**
- **Vorheriger Tag**
- **Vorherige Woche**
- **Vorheriger Monat**

Klicken Sie auf **Weiter**. Die Seite "Berichtsdaten" wird angezeigt.

9. Klicken Sie auf **Anpassen**, um einen kundenspezifischen Bericht zu erstellen.

> Auf der Seite **Dashboard > Berichte** erscheint in der Spalte mit dem Vorlagennamen das Wort "Benutzerdefiniert" als Hinweis, dass der Bericht angepasst wurde.

10. Klicken Sie auf **Spalten anpassen**, um im Abschnitt **Berichtspalten** Spalten hinzuzufügen, zu entfernen oder neu anzuordnen. Klicken Sie alternativ auf den Spaltennamen, um die hinzugefügte Spalte zu entfernen.
11. (Optional) Aktivieren Sie das Kontrollkästchen **Alle Spalten auswählen**, um alle in der Liste angezeigten Salten gleichzeitig auszuwählen.
12. Klicken Sie auf die Option Standardeinstellungen wiederherstellen, um wieder die zuvor erstellten Spalten anzuzeigen. Um die Spalten wieder anzuzeigen, ohne Anpassungen vorzunehmen, können Sie eine der Vorlagen auf der Seite **Berichtvorlage auswählen** wählen. Die Standardspalten sind durch ein Vorhängeschlosssymbol gekennzeichnet.
13. Erstellen Sie Filter mit den spezifischen Regeln des Abschnitts **Erweiterte Filter**.

> Es sind nicht alle Filteroptionen für alle Berichte verfügbar. Weitere Informationen zur Liste der verfügbaren Filter finden Sie beim Thema **Filter** unter diesem Verfahren.

> Die folgenden neuen Hardwareattribute sind für Windows-Geräte beim Erstellen von Berichten verfügbar: BitLocker-Verschlüsselung, Betriebssystemedition, Systemversion, Platinenhersteller, Platinenprodukt, Platinenstatus, BIOS-Hersteller, BIOS-Version, Festplattenpartitionen, Optischer Laufwerktstyp, CPU-Name und CPU-Status.

14. (Optional) Klicken Sie auf das Symbol **+**, um eine andere Regel hinzuzufügen, oder auf das Symbol **Gruppe hinzufügen**, um eine andere Gruppe mit Regeln hinzuzufügen.
15. Klicken Sie auf **Weiter**. Die Seite "Berichtszeitplan" wird angezeigt.
16. Wählen Sie *eines* der folgenden Formate zum Herunterladen des Berichts aus:
    - **CSV**
    - **PDF**
    - **CSV und PDF**
      Bei PDF-Berichtdateien sind bis zu 10 Spalten zulässig. In dem Abschnitt „Berichtdiagramme“ werden die beiden Diagrammarten angezeigt, die in den PDF-Berichten zulässig sind.
      Der Bericht **Alle Anwendungen** unterstützt nur das CSV-Format.

Klicken Sie auf **Automatisch planen**, um einen automatisch auszuführenden Bericht einzurichten, indem Sie die Häufigkeit festlegen. Klicken Sie alternativ auf **Manuell**, um den Bericht einmal auszuführen und per E-Mail zu erhalten.

- Wählen Sie *eine* der Optionen für **wiederkehrende Berichte** aus:
  - **Täglich**
  - **Wöchentlich**
  - **Monatlich**
  - **Vorheriger Zeitplan** – für vorhandene Berichte
- Wählen Sie das **Startdatum** und (optional) das **Enddatum** aus.

> Die Option „Jetzt starten“ erzeugt einen einmaligen Bericht. Sie können die gleiche Vorlage zur Erstellung geplanter Berichte verwenden. Auf der Seite **Dashboard > Berichte** wird in den Spalten „Häufigkeit“ und „Nächster geplanter“ angezeigt, dass für diese Berichte kein Zeitplan existiert.

18. Klicken Sie auf **Weiter**. Die Seite "Berichtverteilung" wird angezeigt. Wählen Sie die Empfänger für den Bericht aus.
19. (Optional) Fügen Sie externe E-Mail-IDs hinzu, indem Sie auf den Link **Externe E-Mail hinzufügen** klicken.
20. Klicken Sie auf **Fertig**. Die **Berichtverteilung** – **Übersicht** wird angezeigt.
21. (Optional) Klicken Sie auf **Bearbeiten**, um den Bericht anzupassen.
22. Klicken Sie auf **Speichern**.
23. Klicken Sie auf das Symbol zum Herunterladen, um das Format des Berichts auszuwählen. Eine E-Mail mit der Schaltfläche **Bericht herunterladen** zum Herunterladen des Berichts wird an die Empfänger des Berichts gesendet.

Filter

Regeloptionen	Beschreibung
Aktivierungssperre aktiviert	Die rollenabhängige Aktivierungssperre wird mit **JA** oder **NEIN** aktiviert. Beispiel für eine Regel: „Aktivierungssperre aktiviert hat Status JA“.
App-Tunnel-Status	Regel für den Apptunnel-Status **SPERREN** oder **ZULASSEN**. Beispiel für eine Regel: Apptunnel-Status ist „Sperre“.
Akkustand	Akkuzustand des Gerätes Beispiel einer Regel:'Batteriezustand ist gleich 1080' Der eingegebene Wert für den Batterieladezustand sollte in Sekunden angegeben werden.
Letzte Client-Anmeldung	Regel basierend auf der letzten Anmeldung des Clients innerhalb des Datumsbereichs. Beispiel für die Regel: „Letzte Client-Anmeldung zwischen dem 02.04.2019, 06:00:00 Uhr und dem 05.04.2019, 17:00:00 Uhr.“
Compliance-Status	Regel für den Compliance-Status, d. h. **JA** oder **NEIN**. Beispiel für eine Regel: "Compliance-Status gleich Ja".
Aktueller Ländername	Geben Sie den aktuellen Ländernamen ein. Beispiel für eine Regel: „Compliance-Status gleich Frankreich“.
Aktueller MCC	Die Regel basiert auf dem aktuellen Mobilfunk-Ländercode. Regelbeispiel: 'Aktueller MCC ist gleich 410'.
Aktueller MNC	Die Regel basiert auf dem aktuellen Mobilfunknetzcode. Regelbeispiel: 'Aktueller MNC ist gleich 06'.
Geräteregistrierung aktiviert	Regelabhängige Geräteregistrierung, mit **JA** bzw. **NEIN** aktiviert. Regelbeispiel: „Aktivierte Geräteregistrierung entspricht JA.“
Nativer Anti-Phishing-Status	Wählen Sie eine der folgenden Optionen für den Nativen Anti-Phishing-Status aus: • Ist gleich • ist nicht gleich Mögliche Werte: • Nicht aktiviert • Nicht zutreffend • Aktiviert • Unbekannt
Anti-Phishing-VPN-Status	Wählen Sie eine der folgenden Optionen für den Anti-Phishing-VPN-Status aus: • Ist gleich • ist nicht gleich Mögliche Werte: • Nicht aktiviert • Nicht zutreffend • Aktiviert

Regeloptionen	Beschreibung
	• Unbekannt
In der Geräteregistrierung registriert	Regel basierend auf der Registrierung in der Geräteregistrierung mit **Ja** oder **Nein**. Regelbeispiel: 'In der Geräteregistrierung registriert ist gleich Ja'
Datenschutz	Zeigt an, ob der Datenschutz auf dem Gerät aktiviert ist. Mögliche Werte sind **Ja** und **Nein**. Beispiel einer Regel: „Datenschutz ist gleich JA'.
Daten-Roaming aktiviert	Regel zum Daten-Roaming, aktiviert mit **JA** oder **NEIN**. Beispiel für eine Regel: „Daten-Roaming aktiviert, falls Status JA ist.“
Geräte-Sperrstatus	Die Regel basiert auf dem Geräte-Sperrstatus. Regelbeispiel: 'Geräte-Sperrstatus ist Sperre'
Geräte-ID	Regel für eine bestimmte Geräte-ID oder einen Bereich von Geräte-IDs. Beispiel für die Regel: "Geräte-ID größer 45". X
Inlands-MCC	Die Regel basiert auf dem Ländercode für das Inlands-Mobilfunknetz. Beispiel für eine Regel: 'Eigener MCC-Code ist gleich 310'.
Eigener MNC	Die Regel basiert auf dem Inlands-Mobilfunknetzcode. Regelbeispiel: 'Inlands-MNC ist gleich 510'.
IMEI	Regel für einen spezifischen IMEI-Wert. Beispiel für die Regel: "IMEI beginnt mit 9900"
Einladestatus	Wählen Sie eine der folgenden Einladungsstatusoptionen aus: • Kein/e • Ausstehend • Abgelaufen • **Abgeschlossen** Beispiel für die Regel: "Einladungsstatus gleich Ausstehend".
Standortdatendienst aktiviert	Regel für den Standortdienst aktiviert mit **JA** oder **NEIN**. Beispiel für die Regel: „Standortdienst aktiviert hat Status JA.“
MTD-Aktivierungsstatus	Wählen Sie eine der folgenden Optionen für den MTD-Aktivierungsstatus aus: • Ist gleich • ist nicht gleich Mögliche Werte sind: • Nicht zutreffend • Fehler • Ausstehend • Geschützt
Quarantänestatus	Regel für den Standortdienst aktiviert mit **JA** oder **NEIN**. Beispiel für eine Regel: „Roaming ist gleich JA"

Regeloptionen	Beschreibung
Registriert bei	Die Regel zur Auswahl des Datums- und Zeitbereichs, in dem das Gerät registriert wurde. Beispiel für die Regel: „Registriert zwischen dem 03.10.2017, 09:00:00 Uhr und dem 20.10.2017, 17:00:00 Uhr.“
Roaming	Regel je nach Roaming, d. h. **JA** oder **NEIN**. Beispiel für eine Regel: "Roaming gleich Ja'
[Status]	Wählen Sie eine der folgenden Einladungsstatusoptionen aus: • Aktiv • Außerdienststellung ausstehend • Außerdienststellung gesendet • Außer Dienst gestellt • Außerdienststellung abgebrochen • Wipe ausstehend • Wipe gesendet • Wipe abgeschlossen • Wipe abgebrochen Regelbeispiel: "Status ist gleich Abschaltung ausstehend".
Voice-Roaming aktiviert	Regelabhängiges Voice-Roaming, mit **JA** bzw. **NEIN** aktiviert. Regelbeispiel: aktiviertes "Voice-Roaming entspricht "Ja","
WLAN-MAC-Adresse	Geben Sie eine bestimmte MAC-Adresse ein. Beispiel für die Regel: "WLAN-Mac-Adresse entspricht nicht 00-14-22-01-23-45".
iCloud-Datensicherung aktiviert	Regel für die Datensicherung in der iCloud aktiviert mit **JA** oder **NEIN**. Beispiel einer Regel: „Cloud-Datensicherung aktiviert ist gleich JA.“
Aktivierungsstatus des iTunes Store-Kontos	Regel für Aktivierungsstatus des iTunes Store-Kontos **JA** oder **NEIN**. Beispiel für die Regel: Aktivierungsstatus für das iTunes Store-Konto ist nicht „NEIN“.
Plattformtyp	Gilt für den Bericht "Alle Anwendungen".
Quelle	Gilt für den Bericht "Alle Anwendungen".
Benutzerdefinierte Attribute	Gilt für den Bericht "Alle Anwendungen".
Verwaltet	Gilt für die Berichte "Alle Anwendungen" und "Am häufigsten verwendete Anwendungen".
App-Identifikator	Standardeinstellung für den Bericht "Alle Anwendungen".
MEID	Gilt für den Bericht "Nicht verwaltete Apps".

Ausführen von Aktionen für einen Bericht

Sie können diverse Aktionen auf der Seite "Geplante Berichte" ausführen.

Verfahren

1. Wechseln Sie zu **Dashboard** > **Berichte**.
2. Klicken Sie auf der Seite **Meine geplanten Berichte** auf das Dropdownmenü **Aktionen**, und wählen Sie eine der folgenden Optionen aus:

Aktionsoptionen	Durchgeführte Aktion
Anzeigen	Ermöglicht Ihnen, den Bericht anzuzeigen.
Bearbeiten	Ermöglicht Ihnen, den Bericht zu bearbeiten.
Jetzt ausführen	Führt den Bericht aus.
CSV herunterladen	Lädt den Bericht im CSV-Format herunter.
PDF herunterladen	Lädt den Bericht im PDF-Format herunter.
Löschen	Löscht den Bericht.

Anzeigen von Berichtsdetails

Sie können die Berichtsdetails anzeigen und einige Aktionen für den erstellten Bericht ausführen.

Verfahren

1. Wechseln Sie zu **Dashboard** > **Berichte**.
2. Klicken Sie zum Anzeigen der Berichtsdetails auf der Seite **Meine geplanten Berichte** auf den Berichtsnamen. Die Berichtsseite wird geöffnet.
3. Wählen Sie eine der folgenden Optionen aus:

Aktionsoptionen	Durchgeführte Aktion
Umschalten	Ermöglicht Ihnen, den Bericht zu aktivieren oder zu deaktivieren.
Jetzt ausführen	Führt den Bericht aus.
Anzeigen	Ermöglicht Ihnen, die Berichtsdetails anzuzeigen. Verwenden Sie das Dropdownmenü "Aktionen", um eine der folgenden Aufgaben auszuführen: • **Deaktivieren** • **Neueste CSV/PDF herunterladen** (je nach ausgewähltem Berichtstyp, z. B. CSV, PDF oder CSV & PDF wird die Option zum Herunterladen angezeigt) • **Historie** • **Löschen**
Löschen	Löscht den Bericht.

Verwandte Themen:

- Weitere Informationen zum Zuweisen einer kundenspezifischen Rolle für einen Benutzer finden Sie unter **Rollen zuweisen**.
- Unter **Benutzerrollen** finden Sie eine Liste der Standardrollen.
- **Rollenverwaltung**
- **Verwendung geplanter Berichte**

6. Benutzer

Bevor Sie jemanden zur Anmeldung von Mobilgeräten einladen, müssen Sie für diese Person einen Benutzereintrag erstellen. Sie müssen außerdem einen Benutzer für jede Person erstellen, die die Cloud verwendet, um Geräte zu verwalten oder Content zu veröffentlichen (Administratoren).

Dieser Abschnitt enthält die folgenden Themen:

- **Benutzergruppen**
- **Benutzereinstellungen**
- **Benutzer-Branding**
- **Benutzerregistrierung mit Apple Business Manager**
- **Kontogesteuerte Benutzerregistrierung**
- **Benutzerlizenzen**
- **Benutzer verwalten**

6.1. Benutzer hinzufügen

Dieser Abschnitt enthält die folgenden Themen:

- Benutzer hinzufügen
- Mehrere Benutzer hinzufügen
- Benutzer durch Hochladen einer Datei hinzufügen
- Einen Administrator hinzufügen
- Der Benutzer „Nobody“
- PIN-Informationen für die Geräteregistrierung anzeigen

Sie können einen einzelnen Benutzer oder mehrere gleichzeitig hinzufügen. Wenn Sie viele Benutzer hinzugefügt haben, sollten Sie die Anzeige **filtern**, um nur die für Sie relevanten Einträge anzuzeigen.

Auf dieser Seite können Sie außerdem

- einer Benutzergruppe zuordnen /aus einer Benutzergruppe entfernen
- Nachrichten an Benutzer senden
- Benutzer zur Anmeldung einladen
- Benutzern Rollen zuweisen
- Benutzerpasswörter ändern
- Benutzer löschen
- PIN generieren

Alle Geräte-Eigentümerprofile sind einem Gerätekonto zugeordnet. Bei Gerätekonten gibt es keine Einschränkungen der Zahl der zugeordneten Geräte. Arbeitsprofile (Mitarbeiter-eigene Arbeitsprofile) werden Benutzerkonten zugeordnet.

Benutzer hinzufügen

Verfahren

1. Gehen Sie zu **Benutzer**.
2. Klicken Sie (oben rechts) auf **+Hinzufügen**.
3. Wählen Sie **Einzelner Benutzer**.
4. Füllen Sie das Formular mit den Angaben des Benutzers aus:
    - E-Mail-Adresse (erforderlich)
    - Vorname
    - Nachname

> Im Feld „Benutzername“ wird die von Ihnen eingegebene E-Mail-Adresse angezeigt. In den meisten Fällen sollten Sie die Standardeinstellungen nicht bearbeiten. Weitere Informationen finden Sie unter **Wann ein Benutzername zu bearbeiten ist**

    - Anzeigename

> Wenn Sie den Anzeigenamen dieses Benutzers ändern möchten, bearbeiten Sie den Text im Feld **Anzeigename** .

5. Wenn Sie ein Passwort zuweisen möchten, geben Sie dieses in den Feldern Passwort und Passwort bestätigen ein.
    - Wenn Sie ein Passwort zuweisen, müssen Sie dieses dem Benutzer für die Registrierung seiner Geräte mitteilen.
    - Wenn Sie kein Passwort zuweisen, muss der Benutzer bei der Registrierung seiner Geräte ein Passwort erstellen.
6. Wählen Sie die Option **Regionaleinstellungen** aus der Dropdown-Liste.
7. Geben Sie die **verwaltete Apple-ID** ein. Sie können „appleid“ als Unterdomäne für die verwaltete Apple-ID aufnehmen, um Konflikte mit bestehenden Apple-IDs zu vermeiden. Zum Beispiel user@appleid.yourdomain.com. Die Subdomain muss eine gültige verifizierte Subdomain im Apple Business Manager sein.

> Das Konto kann nicht mit einer anderen verwalteten Apple-ID aktualisiert werden, wenn es ein aktives benutzerregistriertes Gerät mit der verwalteten Apple-ID des aktuellen Kontos gibt.

(Optional) Weisen Sie eine oder mehrere Benutzergruppen zu. Die verwaltete Apple-ID kann nicht aktualisiert werden, wenn es ein Gerät mit dem Status „Aktiv“ und „Außerdienststellung ausstehend“ gibt.

10. Wenn Sie vor der Einladung dieses Benutzers erst andere Eigenschaften bestimmen möchten, deaktivieren Sie die Option **Einladung jetzt senden.** Ansonsten wird die E-Mail-Einladung gesendet, wenn Sie auf **Fertig** klicken.
11. Klicken Sie auf **Fertig**, um den Benutzer hinzuzufügen.

Bei Android-Geräten sind Gerätekonten für verwaltete Einzweck-Geräte vorgesehen, wobei ein einziges lokales Dienstkonto zur Registrierung einer großen Anzahl von Geräten verwendet werden kann. Beim Anlegen eines neuen Benutzers muss das unter **Admin > Google > Android Enterprise** verfügbare Android Enterprise-Gerätekonto aktiviert sein. Gerätekonten sind (statt der Benutzerkonten) für vom Geräteeigentümer verwaltete Google Play-Kontoregistrierungen standardmäßig aktiviert.

Markieren Sie das Kontrollkästchen **Gerätekonto für Android Enterprise**, damit mit diesem Konto verbundene, verwaltete Geräteregistrierungen durch Android Enterprise automatisch einem Google-Gerätekonto zugeordnet werden.

Wenn Sie einen lokalen oder LDAP-Benutzer für Android-Geräte bearbeiten, werden den dem Benutzer zugeordneten, durch den Geräte-Eigentümer verwalteten Geräten mit Google Play-Konten beim nächsten Geräte-Check-in Gerätekonten zugeordnet, sofern folgende Bedingungen erfüllt sind:

- Die Funktion wird aktiviert, indem Sie in das Kontrollkästchen **Gerätekonto für Android Enterprise** klicken.
- Die App GO auf dem Android-Gerät hat die Version 47 oder höher.

Mehrere Benutzer hinzufügen

Schritte :

1. Gehen Sie zu Benutzer.
2. Klicken Sie (oben rechts) auf **+Hinzufügen**.
3. Wählen Sie **Mehrere Benutzer**.
4. Standardmäßig können Sie E-Mail-Adressen manuelleingeben. Tippen oder fügen Sie die E-Mail-Adressen der Benutzer, getrennt durch Kommas, ein.
5. Beispiel: jdoe@mycompany.com, jsmith@mycompany.com, tjones@mycompany.com
   Wenn Sie vor der Einladung dieses Benutzers erst andere Eigenschaften bestimmen möchten, deaktivieren Sie die Option **Einladung jetzt senden**.

6. Ansonsten wird die E-Mail-Einladung gesendet, wenn Sie auf **Fertig** klicken.
   Klicken Sie auf **Fertig**, um den Benutzer hinzuzufügen.

Benutzer durch Hochladen einer Datei hinzufügen

Schritte:

1. Gehen Sie zu **Benutzer**.
2. Klicken Sie (oben rechts) auf **+Hinzufügen**.
3. Wählen Sie **Mehrere Benutzer**.
4. Wählen Sie **CSV-Datei hochladen**.
5. Klicken Sie auf **CSV-Vorlage herunterladen**.
6. Bearbeiten Sie die Vorlage mit folgenden Informationen für jeden Benutzer:
   - Benutzer-ID (erforderlich)
   - E-Mail-Adresse (erforderlich)
   - Passwort
   - Vorname
   - Nachname
   - Name anzeigen
   - Benutzergruppen
   - Kundenspezifische Attribute
7. Dies ist die gleiche Information, die Sie eingeben, wenn Sie einen einzelnen Benutzer hinzufügen. Eine Datei kann max. 10.000 Einträge enthalten.
   Speichern Sie die Datei.
8. Ziehen Sie sie in den Hochladebereich oder wählen Sie die Option **CSV-Datei hochladen**, um die Datei auszuwählen.
9. Sobald die hochgeladenen Benutzerinformationen angezeigt werden, können Sie die erforderliche Bearbeitung vornehmen.
10. Klicken Sie auf **Weiter** (unten rechts).
11. Wenn Sie nicht sofort Einladungen versenden wollen, klicken Sie auf Keine Einladungen versenden.
12. Klicken Sie auf **Fertig**.

Einen Administrator hinzufügen

Schritte :

1. Klicken Sie (oben rechts) auf **Hinzufügen**.
2. Wählen Sie Einzelner Benutzer.
3. Füllen Sie das Formular mit den Angaben des Benutzers aus:
   - E-Mail-Adresse
   - Vorname
   - Nachname
4. Im Feld **Benutzername** wird die von Ihnen eingegebene E-Mail-Adresse angezeigt.
   Wenn Sie den Anzeigenamen dieses Benutzers ändern möchten, bearbeiten Sie den Text im Feld **Anzeigename** .

5. Geben Sie im Feld **Passwort** ein Passwort zur Zuweisung ein.
6. Geben Sie das Passwort erneut im Feld **Passwort bestätigen** ein.
7. Klicken Sie auf **Fertig**, um den Benutzer hinzuzufügen.
8. Teilen Sie das Passwort der Person mit, die sich um die Verwaltung der Geräte kümmert.

Der Benutzer „Nobody“

Der Nobody-Benutzer ist ein Standardbenutzer, der nicht gelöscht werden kann. Der Dienst verwendet diesen Benutzer für Geräte, denen noch keine Benutzer zugeordnet sind, beispielsweise ausgesonderte Geräte.

PIN-Informationen für die Geräteregistrierung anzeigen

Wenn Administratoren neue Benutzer hinzufügen, wird den Administratoren die erzeugte Registrierungs-PIN angezeigt, wenn als Authentifizierungsart der Geräteregistrierung "Nur PIN" eingestellt ist. Diese Information kann nützlich sein, um die Benutzer bei der Geräteregistrierung zu unterstützen.

- Bei einzelnen Benutzern wird die PIN über die Seite **Benutzer > Benutzer zur Registrierung einladen** angezeigt, außerdem erscheinen die Informationen im Abschnitt für die PIN-Informationen auf der Seite mit den Benutzerdetails.
- Bei mehreren Benutzern werden die PINs in einer Spalte der Benutzerliste neben dem PIN-Status (gültig oder abgelaufen) der Spalte „PIN ausgestellt“ und der Spalte „PIN läuft ab“ angezeigt.

Wenn Sie keine Aufgaben auf der Seite **Benutzer** ausführen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie brauchen eine der folgenden **Rollen** :

- Systemverwaltung
- Benutzermanagement

6.2. Benutzergruppen

Dieser Abschnitt enthält die folgenden Themen:

- Dynamisch verwaltete Benutzergruppe erstellen
- Manuell verwaltete Benutzergruppe erstellen
- Benutzergruppe aus einer der doppelten Benutzergruppen erstellen
- Erstellen einer Benutzergruppe durch Hochladen einer CVS-Datei

User_Roles.htmErstellen Sie eine Benutzergruppe, um mehreren Benutzern Apps und Rollen zuzuordnen. Sie können beispielsweise eine Managergruppe erstellen, wenn Sie allen Abteilungsmanagern Administratorrechte für Apps und Content geben wollen.

Sie können eine Benutzergruppe erstellen und mit einer der folgenden Methoden verwalten:

- **Dynamisch verwaltet (häufigste Option):** Lokale und LDAP-Benutzer werden nach bestimmten Regeln bzw. Attributen dynamisch in einer Gruppe ergänzt/entfernt.
- **Manuell verwaltet (begrenzte Anwendung):** Benutzer in einer Gruppe manuell ergänzen/entfernen. Manuell verwaltete Gruppen werden nur für Testzwecke empfohlen, die nur wenige Berechtigungen erfordern.

Sie können Text im Feld **Suche** eingeben, um eine Liste aller Benutzergruppen anzuzeigen, deren Namen mit dem eingegebenen Text beginnen.

- Die Suchergebnisse werden während der Texteingabe in Echtzeit als Liste möglicher Treffer angezeigt.
- Wählen Sie den gewünschten Benutzergruppennamen aus der Liste der möglichen Treffer für die nachfolgende Aktion aus.
- Bei der Suche wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Dynamisch verwaltete Benutzergruppe erstellen

> Das folgende Verfahren ist für dynamische Benutzergruppen nicht relevant.

Verfahren

1. Klicken Sie auf **+Hinzufügen**.
2. Geben Sie den Namen einer Benutzergruppe in das Feld **Name** ein.
3. (Optional) Klicken Sie auf diese Option **Beschreibung hinzufügen**, um eine Beschreibung für die Benutzergruppe zu ergänzen.
4. Klicken Sie auf die Option **Dynamisch verwaltet (häufigste Option)**.
5. Definieren Sie Regeln bzw. Attribute entsprechend Ihren Anforderungen. Folgende Regeloptionen sind verfügbar:
    - Benutzerdefiniertes LDAP-Attribut
        - msExchPoliciesIncluded
        - msExchMailboxGrid
        - mailNickname

    Standard-LDAP-Attribut

        - samAccountName
        - userPrincipalName

Standard-Benutzerattribut

- email_address
- distinguished_name
- last_name
- display_name
- first_name
- Benutzergruppe
- Kundenspezifisches Benutzerattribut

Benutzergruppe DN

- Benutzergruppen-GUID
- Name der Benutzergruppe

6. Wählen Sie für jede Regel lokale bzw. LDAP-Benutzer aus. Sie können mit den Filterkriterien für die **Benutzergruppe** eine Untergruppe einschließen oder ausschließen.
7. Ergänzen Sie weitere Regeln, indem Sie auf das Plus-Symbol klicken.
   Sie können mit den OperatorenANY (jede) oder ALL (alle) bedingten Filter für die ergänzten Regeln definieren.
8. Erstellen Sie eine Regelgruppe, indem Sie auf das Hierarchiesymbol neben dem Plus-Symbol klicken.
9. Überprüfen Sie die Regeln und Attribute der Benutzergruppe in der Textabfrage, die unter den Auswahloptionen für die Regeln angezeigt wird.
10. Überprüfen Sie in dem Abschnitt **Ergebnisse** die Benutzerdetails, die den konfigurierten Kriterien entsprechen. Wenn Sie eine Regel oder ein Attribut ergänzen oder modifizieren, werden Ihnen die Benutzer angezeigt, die die Kriterien erfüllen.
11. Klicken Sie auf **Speichern**, um die konfigurierte Benutzergruppe zu speichern.

Manuell verwaltete Benutzergruppe erstellen

1. Klicken Sie auf **+Hinzufügen**.
2. Geben Sie einen Gruppennamen ein.
3. (Optional) Klicken Sie auf **Beschreibung hinzufügen**, um eine Beschreibung zu ergänzen.
4. Klicken Sie auf die Option **Manuell verwaltet (eingeschränkte Verwendung)** .
5. Geben Sie im Feld Benutzer suchen die E-Mail-Adresse jedes Benutzers ein, der in die Gruppe aufgenommen werden soll.
   Mit jeder Tasteneingabe werden passende Benutzer gesucht und angezeigt, sofern vorhanden.
6. Wählen Sie die Benutzer aus, die Sie in der Gruppe hinzufügen wollen. Sie können weitere Benutzer nach Bedarf suchen und ergänzen.
7. Klicken Sie auf **Speichern**.

> Sie können eine manuell verwaltete Benutzergruppe erstellen und diese Benutzergruppe dann zu einer dynamisch verwalteten Benutzergruppe hinzufügen. In einem solchen Szenario hat das Bearbeiten der manuell verwalteten Benutzergruppe keinen Einfluss auf die Regel für die dynamisch verwaltete Benutzergruppe. Sie können eine manuell verwaltete Benutzergruppe nicht löschen, wenn sie zu einer dynamisch verwalteten Benutzergruppe hinzugefügt wurde.

Benutzergruppe aus einer der doppelten Benutzergruppen erstellen

Neurons for MDM 127Ab zeigt das Administrator-Portal die Anzahl doppelter Benutzergruppen und die zugehörige Anzahl der GUIDs an, damit doppelte Gruppen identifiziert werden können, wenn das Attribut „Name der Benutzergruppe“ im Regeleditor ausgewählt wird.Eine Tabelle unter dieser Regel zeigt außerdem die Liste der doppelten Benutzergruppen zusammen mit Details wie Name der Benutzergruppe, GUID, Quelle und Distinguished Name (DN).

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administratorportal an.
2. Gehen Sie zu **Benutzer** , **Benutzergruppen**.
3. Klicken Sie auf **+Hinzufügen**. Der Assistent „Benutzergruppe erstellen“ wird geöffnet.
    1. Geben Sie einen Namen in das Feld **Name** ein.
    2. Wählen Sie **Name der Benutzergruppe** im Regeleditor, wählen Sie **ist gleich** und wählen Sie *einen* der doppelten Benutzergruppennamen aus.
    3. Klicken Sie auf das Plus-Symbol (**+**), um weitere Regeln hinzuzufügen.
    4. Wählen Sie **Benutzergruppen-GUID**, **ist gleich**.
    5. Kopieren Sie die GUID aus der Tabelle, in der die Liste der doppelten Benutzergruppennamen und GUIDs angezeigt wird, und fügen Sie sie ein. In den Ergebnissen werden die zugeordneten Benutzer angezeigt, die in die neue Gruppe aufgenommen werden.
    6. Klicken Sie auf **Speichern**. Die aufgelisteten Benutzer befinden sich nun in der neuen erstellten Benutzergruppe.

Wenn Sie keine Aufgaben auf der Seite **Benutzergruppen** ausführen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie brauchen eine der folgenden **Rollen**:

- Systemverwaltung
- Benutzermanagement

Erstellen einer Benutzergruppe durch Hochladen einer CVS-Datei

Diese neu hinzugefügte Funktion ermöglicht es Administratoren, unter Verwendung einer CSV-Datei Benutzergruppen zu erstellen und diesen Benutzer hinzuzufügen.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administratorportal an.
2. Gehen Sie zu **Benutzer** , **Benutzergruppen**.
3. Klicken Sie auf **+Hinzufügen**.
4. Wählen Sie **Benutzergruppen aus CSV-Datei importieren** aus. Der Assistent "Benutzergruppe importieren" wird geöffnet.
    1. Klicken Sie im Abschnitt "CSV herunterladen" auf **CSV-Vorlage herunterladen**, um die CSV-Vorlage herunterzuladen. Mithilfe der Vorlage können Sie die Datei bearbeiten und Benutzergruppen erstellen. Den neuen oder auch bestehenden Benutzergruppen können Sie dann Benutzer hinzufügen.
    2. Klicken Sie nach dem Bearbeiten und Speichern der CSV-Datei auf **Datei auswählen** um die CSV-Datei hochzuladen.
    3. Klicken Sie auf **Hochladen**. Bei erfolgreichem Hochladen wird eine Bestätigungsmeldung angezeigt.

Eigenschaft	Beschreibung
Begrenzung der Größe der CSV-Datei	Die maximale Größe der CSV-Datei für den Import ist auf 2 MB begrenzt.
Anforderungen an das Format der CSV-Datei	CSV-Dateien müssen exakt 2 Spalten enthalten: accountUid und groupName. • Die Werte für accountUid und groupName müssen zwingend angegeben werden. • Datensätze, die diese Kriterien nicht erfüllen, werden beim Import verworfen. Administratoren können zu Referenzzwecken eine Muster-CSV-Datei aus dem Importabschnitt herunterladen.
Fehler beim Importieren	Wenn während des CSV-Imports Fehler auftreten, wird eine Fehlerdatei generiert. • Administratoren können diese Fehlerdatei herunterladen und prüfen, welche CSV-Zeilen fehlerhaft verarbeitet wurden, um die Fehlerursachen nachzuvollziehen. • Die Fehlerdatei enthält die fehlerhafte CSV-Zeile und eine Erläuterung des Fehlers.
Bedingungen für erfolgreichen Import	Das Importieren von Benutzern und Benutzergruppen gelingt nur dann, wenn die Benutzergruppe lokal ist und manuell verwaltet wird. • Der Benutzer muss im System vorhanden sein, damit der Importvorgang erfolgreich ist.

Bedingungen für das Erstellen einer Benutzergruppe und Hinzufügen eines Benutzers mit einer Muster-CSV-Datei

Details zur Muster-CSV-Datei

accountUid: test_user_1@org.com

groupName: test_group_1

Bedingungen	Beschreibung
Vorhandene Gruppe	Wenn die Gruppe test_group_1 bereits existiert, wird ihr der Benutzer test_user_1@org.com zugeordnet.
Nicht vorhandene Gruppe	Wenn die Gruppe test_group_1 nicht existiert, wird eine neue Gruppe mit dem Namen test_group_1 erstellt und der Benutzer test_user_1@org.com wird ihr zugeordnet.
Nicht lokale Gruppen	Wenn die Gruppe test_group_1 existiert, aber nicht lokal ist, wird der Datensatz mit der Begründung 'Gruppe ist nicht lokal' in die CSV-Fehlerdatei aufgenommen.
Gruppe nicht manuell verwaltet	Wenn die Gruppe test_group_1 existiert, aber nicht manuell verwaltet wird, wird der Datensatz mit der Begründung 'Gruppe wird nicht manuell verwaltet' in die CSV-Fehlerdatei aufgenommen.
Nicht vorhandener Benutzer	Wenn der Benutzer test_user_1@org.com nicht existiert, wird der Datensatz mit der Begründung 'Benutzer nicht gefunden' in die CSV-Fehlerdatei aufgenommen.
Benutzer und Gruppe existieren nicht	Wenn sowohl der Benutzer test_user_1@org.com als auch die Gruppe test_group_1 nicht existieren, wird eine neue Gruppe mit dem Namen test_group_1 erstellt und der Datensatz wird mit der Begründung 'Benutzer nicht gefunden' in die CSV-Fehlerdatei aufgenommen.

6.3. Benutzereinstellungen

Dieser Abschnitt enthält die folgenden Themen:

- Standardeinstellung bearbeiten
- Benutzerdefinierte Einstellung hinzufügen
- Benutzerdefinierte Einstellung löschen
- Die Einstellungen für neue Geräteregistrierungen konfigurieren
- Gerätelimit pro Benutzer konfigurieren
- Löschlimit für das Gerät konfigurieren
- Benutzereinstellungen
- Self Service Portal-Authentifizierung konfigurieren
- Passwortkomplexität einstellen
- Nutzungsbedingungen definieren
- Erinnerungs-E-Mails für die Einladung des Benutzers konfigurieren
- Bestätigungs-E-Mails zur Benutzerregistrierung konfigurieren
- Benutzerarbeitsplan konfigurieren
- Administrationsportal-Authentifizierungseinstellung konfigurieren

Benutzereinstellungen bestimmen die Registrierungsoptionen für das Gerät. Es gibt verschiedene Typen:

- **Einstellung für Geräteregistrierung**: Legt die Authentifizierung mit Kennwort und/oder PIN fest, den Apple-Registrierungstyp und den Gerätebesitzer.
    - Wenn Sie zuvor SAML auth/IdP eingerichtet haben, wird die SAML-Authentifizierung sowohl für die Geräteregistrierung als auch für die Portalauthentifizierung verwendet.
    - **Einstellungen für die plattformspezifische Geräteregistrierung** – Administratoren können jetzt die Geräteregistrierung auf Betriebssystemebene steuern, indem sie die Registrierung beim System durch bestimmte Apple-, Android- und Windows-Plattformen unterbinden. Diese neue Einstellung für die Einschränkung auf Betriebssystemebene wird als übergeordnete Registrierungssteuerung angewendet. Wenn sie für eine Plattform aktiviert ist, werden die zugehörigen Registrierungsbeschränkungen für diese Plattform automatisch deaktiviert. Dadurch können Unternehmen Registrierungsrichtlinien durchsetzen und gleichzeitig verhindern, dass nicht unterstützte Geräteplattformen registriert werden.

Einstellung des Gerätelimits: bestimmt die Anzahl der Geräte, die ein Benutzer registrieren kann.

- **Limit für Komplettlöschung**: Legt die maximale Anzahl der Geräte fest, die in einem Vorgang vollständig gelöscht werden können.
- **Selbstbedienungsportal-Authentifizierungseinstellung:** Legen Sie den Passwort-Authentifizierungstyp für das Selbstbedienungsportal fest.
- **Passwortkomplexität einstellen**: Definiert die Passwortkomplexität sowie Richtlinienparameter für lokale Konten zur Geräteregistrierung und den Zugang zum Selbstbedienungsportal und zum Administratorportal.
- Nutzungsbedingungen – Einstellungen: Bestimmt die Nutzungsbedingungen, die dem Benutzer für jede Geräteregistrierung angezeigt werden.

- **Einstellung für die Erinnerung an die Einladung des Benutzers:** Definiert, zu welchen Tagen und in welcher Häufigkeit wegen der Einladung Erinnerungs-E-Mails an den Benutzer versendet werden.
- **Einstellung zur Bestätigung der Benutzerregistrierung:** Steuert die Möglichkeit, die E-Mail zur Bestätigung der Benutzerregistrierung zu versenden. Unter **Registrierungsbestätigungs-E-Mails konfigurieren und verwenden** finden Sie eine Übersicht über die Lösung und unter **Bestätigungs-E-Mails zur Benutzerregistrierung konfigurieren** für spezifische Anweisungen zu den Benutzereinstellungen.
- **Einstellung für Benutzerarbeitszeitplan:** Steuert die Möglichkeit, einen Benutzerarbeitszeitplan zu konfigurieren, der die gesamte Kommunikation von Sentry zu verwalteten Geräten während der vorgeschriebenen arbeitsfreien Zeiten blockiert. Nützlich für Standorte mit dem „Recht auf Nichterreichbarkeit".
- **Auth-Einstellungen des Administratorportals:** Steuert, ob die Cloud den Administrator nur nach dem Passwort oder nach Passwort und PIN fragt.

Sie können die Standardeinstellungen für die Gruppe **Alle Benutzer** bearbeiten oder benutzerdefinierte Einstellungen hinzufügen und diese anderen Gruppen zuweisen.

Standardeinstellung bearbeiten

Klicken Sie auf den Link **Bearbeiten** für die Einstellung mit dem Schlosssymbol. Sie können Standardeinstellungen nicht löschen.

Benutzerdefinierte Einstellung hinzufügen

Klicken Sie auf den Link **Einstellungen für spezifische Benutzergruppen hinzufügen**.

Benutzerdefinierte Einstellung löschen

Klicken Sie auf das X-Symbol.

Die Einstellungen für neue Geräteregistrierungen konfigurieren

Sie können die Mindestversion des Betriebssystems, die Authentifizierungsart und den Geräteeigentümer bei Neugeräteregistrierungen konfigurieren. Die durch ältere Versionen der Cloud erzeugte URL für die Geräteregistrierung funktioniert mit der aktuellen Version nicht mehr. Der Administrator muss die URL für die Geräteregistrierung neu erstellen.

Registrierung von Whitelist-Geräten

Die Option zur Registrierung von Whitelist-Geräten ist nur in den Standard-Benutzereinstellungen und nicht in den benutzerdefinierten Benutzereinstellungen verfügbar. Sie können eine CSV-Datei mit der Vorlage hochladen, die Seriennummern und benutzerdefinierte Geräteattribute der Geräte enthält, die in die Whitelist eingetragen werden. Sie können ein oder mehrere vorhandene benutzerdefinierte Geräteattribute zum Erstellen der Whitelist hinzufügen. Auf diese Weise können Sie Gerätegruppen oder Spaces nach der Registrierung Attribute zuweisen.

Um benutzerdefinierte Attribute zu erstellen, gehen Sie zu **Admin > Attribute**. iOS- und macOS-Geräte können nicht über iReg registriert werden, wenn die Whitelist-Funktion aktiviert und die Seriennummer des Geräts nicht in der CSV-Datei angegeben ist. Wenn die CSV-Datei eine doppelte Seriennummer enthält, wird der letzte Eintrag in der CSV-Datei verwendet, und bei der Registrierung werden zur Gerätezuweisung die diesem Eintrag zugeordneten benutzerdefinierten Geräteattributeverwendet.

Wenn die Option **Geräte-Whitelist** aktiviert ist, können sich nur die in der Whitelist enthaltenen Geräte bei Ivanti Neurons for MDM registrieren. Diese Funktion gilt nur für Geräte, die sich über den webbasierten Registrierungsprozess registrieren. Dies hat keine Auswirkungen auf die bereits bei Ivanti Neurons for MDM registrierten Geräte. Wenn die Seriennummer des Geräts nach der

Registrierung aus der CSV-Datei entfernt wird, wird das Gerät nicht abgeschaltet. Der in der CSV-Datei angegebene Benutzer ist optional und wird nur zugewiesen, wenn der Benutzer in der CSV-Datei angegeben und ein gültiger Benutzer ist.

Wenn Sie eine neue CSV-Datei hochladen möchten, können Sie die vorhandene CSV-Datei löschen und die neue Datei hochladen. Whitelisting wird nur mit iReg unterstützt; wenn der Go-Client benötigt wird, entscheiden Sie sich stattdessen für die Zero-Touch-Registrierung. Damit Funktionen wie AppConnect und Threat Defense funktionieren, muss der Go-Client auf dem System installiert sein. Da wir die In-App-Registrierung nicht unterstützen, kann der Benutzer das Gerät zunächst über iReg registrieren; später kann die Go-App aus dem App Catalog auf die Geräte übertragen werden. Indem der Benutzer die Installation der App akzeptiert, wird das Gerät zu einem verwalteten Gerät, und alle Funktionen funktionieren nach der Registrierung weiterhin. Die Zero-Touch-Konfiguration kann nicht auf Geräten verwendet werden, bei denen der AppConnect-Status aktiv oder inaktiv ist. Sie kann nur verwendet werden, wenn der AppConnect-Status „Kein“ ist. Der AppConnect-Status bleibt als „Kein“ erhalten, bis der Go-Client nach der Registrierung über iReg auf dem Gerät gestartet wird.

Verfahren

1. Melden Sie sich bei Ivanti Neurons for MDM an.
2. **Gehen Sie zu Benutzer** > **Benutzereinstellungen**.
3. Klicken Sie unter **Einstellungen für die Geräteregistrierung** auf **+ Einstellung für bestimmte Benutzergruppen hinzufügen**.
4. Bearbeiten Sie die Standardeinstellungen für den **Geräteregistrierungs-Authentifizierungstyp** oder fügen Sie einen neuen hinzu.
5. Geben Sie einen Namen in das Feld **Name** ein.
6. (Optional) Geben Sie eine Beschreibung der Einstellung ein.
7. Definieren Sie im Abschnitt **Betriebssystemeinstellungen** die minimale Betriebssystemversion für iOS, macOS oder Windows:
8. Wählen Sie den Umschalter **Mindestversion aktivieren** und dann eine Betriebssystemversion aus der Dropdownliste aus.

> Die Einstellung "Mindestversion aktivieren" gilt nicht für DEP-Geräteregistrierungen.

Für **Android**:

- Aktivieren Sie die Option **Minimaler Sicherheitspatch** (nur Android) und geben Sie den Zeitraum an, indem Sie die Dauer aus den folgenden Dropdown-Listenoptionen auswählen:
  - **Tage**
  - **Monate**
  - **Jahre**

  Aktivieren Sie die Option **Hersteller-Whitelist/Blacklist** und wählen Sie eine der folgenden Optionen:

  - **Whitelist erstellen** – erlaubt nur die Registrierung von Geräten dieser Hersteller.
  - **Blacklist erstellen** – verhindert, dass Geräte von diesen Herstellern registriert werden.
    Hersteller hinzufügen:
    1. Klicken Sie auf **Hersteller hinzufügen**.
    2. Geben Sie den Namen des Herstellers in dem Feld **Herstellername** ein.
    3. Klicken Sie auf **Speichern**. Der hinzugefügte Herstellername wird in der Tabelle angezeigt.

> Beim Namen des Herstellers ist die Groß- und Kleinschreibung zu beachten. Klicken Sie für den Hersteller auf **Bearbeiten** oder **Löschen**, um einen hinzugefügten Herstellernamen zu bearbeiten oder zu löschen.

Wählen Sie im Abschnitt Apple-Anmeldung den Apple-Anmeldungstyp aus:

- **Geräteregistrierung**
- **Benutzerregistrierung** - Standardmäßig ist die Benutzerregistrierung für iOS- und iPadOS-Geräte verfügbar.
- (Optional) **macOS-Gerät einbeziehen (macOS 10.15+)** - Wählen Sie diese Option, um die Benutzerregistrierung auch für macOS-Geräte zu verwenden.

Aktivieren Sie im Abschnitt **Einladungsmethode zur Registrierung (nur iOS und Android)** die Option **Nur MAM-Registrierung**.

> Diese Option muss für die Registrierung von MAM-Only-Geräten aktiviert werden. Nach der Aktivierung werden die Benutzer zum Public App Store umgeleitet und können dort den AppStation-Client herunterladen.

11. Wählen Sie im Abschnitt **Authentifizierungstyp der Geräteregistrierung** eine der folgenden Optionen aus dem Dropdownmenü **Registrierungstyp auswählen** aus. Wenn Sie die Geräteregistrierung verwenden, achten Sie darauf, dass Ihre Konfiguration für die Geräteregistrierung mit Ihrer Auswahl übereinstimmt.
    - **Nur Passwort**
    - **Nur PIN** Bei Auswahl dieser Option wird die Schaltfläche zum Umschalten von "IdP-Geräteregistrierungsauthentifizierung umgehen" gesperrt.
    - **Passwort und PIN**

      > HINWEIS: Benutzer können weiterhin eine PIN erhalten, um die Kontoaktivierung abzuschließen.

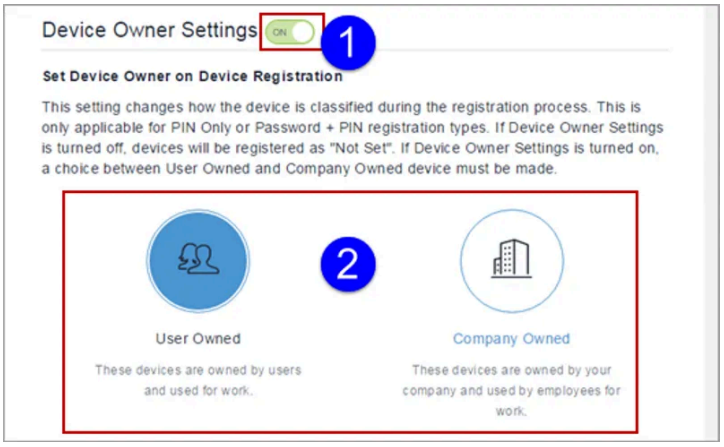
> Diese Einstellung wirkt sich sowohl auf die normale Registrierung als auch auf die Registrierung für die Geräteanmeldung aus.

Geben Sie Folgendes für PINs an. Während der Geräteregistrierung kann ein Benutzer bei Bedarf auf **PIN erneut senden** klicken.

- **PIN-Nutzungsdauer**: die Gültigkeitsdauer der PIN (1–30 Tage).
- **PIN-Länge**: die Anzahl der Zeichen (4–12).
- **Benutzer darf neue PIN anfordern**: (wenn sie sie vergessen haben oder wenn sie abgelaufen ist).

Sie können auch die Geräteeigentümer-Einstellungen aktivieren und dann auf Eigentum des Benutzers bzw. Eigentum des Unternehmens klicken. Diese Einstellung ändert die Klassifizierung des Geräts während des Registrierungsprozesses.

- Wenn die Option **Geräteeigentümereinstellungen** aktiviert ist und der Administrator dieses Gerät als Eigentum des Benutzers markiert hat, wird dem Benutzer die Option angezeigt, das Gerät als Eigentum des Benutzers oder Eigentum des Unternehmens zu kennzeichnen, wenn sich das Gerät registriert; diese Einstellung ist auch über das Selbstbedienungsportal möglich. Bei Geräten, die mit User Enrollment registriert sind, lauten die Standardeinstellungen für den Gerätebesitzer „User Owned“, unabhängig von der Auswahl des Administrators.
- Bei überwachten Geräten ist die Einstellung für Geräteeigentümer immer "Eigentum des Unternehmens".



Klicken Sie auf **+Add**, um mindestens eine Benutzergruppe auszuwählen, der Sie die Einstellung zuteilen möchten.

15. (Diese **bei Bedarf aktivierbare Funktion** ist nur für iOS- und macOS-Geräte verfügbar.) Aktivieren Sie optional die Option **Geräte-Whitelist**, damit die Geräteregistrierung mit Whitelist-Seriennummern erfolgt.
16. Klicken Sie auf **Weiter**. Die Seite "Verteilung der Benutzereinstellung" wird aufgerufen.
17. Wählen Sie die Benutzergruppenverteilung aus.
18. Klicken Sie auf **Fertig**.
19. Senden Sie den Benutzern eine Einladung. Weitere Informationen finden Sie unter **Benutzer einladen**.

Beachten Sie Folgendes:

> Wird ein Benutzergerät nur mit der PIN-Option registriert, erhält der Benutzer via E-Mail eine Registrierungsbestätigung mit einer PIN zur Authentifizierung.

- Wird eine PIN an die E-Mail-ID des Benutzers gesendet.
- Der Benutzer gibt die PIN auf der Registrierungsseite des Geräts ein.
- Wenn die PIN richtig ist, wird der Benutzer durch den Registrierungsprozess geführt.

Configure Identity Provider.htm#To_configure_an_identity_provider Ivanti Neurons for MDMFür Benutzer, die mit einem SAML-Identitätsanbieter (IdP) konfiguriert sind, unterstützt die Authentifizierung mit PIN bei der Registrierung des Geräts. Der Authentifizierungstyp für die Geräteregistrierung sollte "PIN" oder "PIN und Kennwort" sein. Die Funktionalität "PIN und Kennwort" sorgt als Zwei-Faktor-Authentifizierung für zusätzliche Sicherheit. Wenn in diesem Fall ein solcher Benutzer versucht, ein Gerät zu registrieren:

- Wird eine PIN an die E-Mail-ID des Benutzers gesendet.
- Der Benutzer gibt die PIN auf der Registrierungsseite des Geräts ein.
- Wenn die PIN korrekt ist, wird der Benutzer auf die Anmeldeseite des IdP weitergeleitet, wo er den IdP-Benutzernamen und das Passwort eingibt.
- Wenn die IdP-Anmeldeinformationen korrekt sind, wird der Benutzer auf das Gerät umgeleitet, um den Registrierungsprozess abzuschließen.

Gerätelimit pro Benutzer konfigurieren

Verfahren

1. Bearbeiten Sie die Standardeinstellungen für das **Gerätelimit** oder fügen Sie eine neue hinzu.
2. (Optional) Klicken Sie auf **+ Einstellungen für spezifische Benutzergruppen hinzufügen**, um ein Gerätelimit für bestimmte Benutzergruppen zu konfigurieren.
3. Bearbeiten oder weisen Sie einen Namen zur Identifizierung der Einstellung zu.
4. Geben Sie eine optionale Beschreibung der Einstellung ein.
5. Wählen Sie im Dropdownmenü **Maximale Anzahl aktiver Geräte** das aktive Limit für Apple-Geräte aus.
6. Wählen Sie im Dropdownmenü **Maximale Anzahl der mit einem iPhone koppelbaren Apple watchOS-Geräte** das aktive Gerätelimit für die Kopplung aus.
7. (Optional) Wenn **+ Einstellungen für spezifische Benutzergruppen hinzufügen** markiert ist, klicken Sie auf **Weiter** und wählen Sie mindestens eine Benutzergruppe für die Verteilung dieser Einstellung aus.
8. Klicken Sie auf **Fertig**.

Löschlimit für das Gerät konfigurieren

Verfahren

1. Bearbeiten Sie die Standardeinstellung für das **Geräte-Löschlimit**.
2. Aktivieren Sie die Option **Löschlimit für alle Benutzer aktivieren (einschließlich Standardrollen)**.
3. Geben Sie in das Feld **Maximale Anzahl der Geräte, die ein Benutzer gleichzeitig löschen kann** die maximale Anzahl der Geräte ein, die gleichzeitig gelöscht werden können. Der Standardwert ist 1. Sie können als Löschlimit für das Gerät einen Maximalwert von 200 festlegen.
4. Klicken Sie auf **Fertig**.

Self Service Portal-Authentifizierung konfigurieren

Verfahren

1. Bearbeiten Sie die Standardeinstellung **Self-Service-Portal-Authentifizierung** oder klicken Sie auf **Einstellung für spezifische Benutzergruppen hinzufügen**, um eine neue Einstellung hinzuzufügen.
2. Bearbeiten oder weisen Sie einen Namen zur Identifizierung der Einstellung zu.
3. Geben Sie eine optionale Beschreibung der Einstellung ein.
4. Wählen Sie eine **Authentifizierungsart für das Self-Service-Portal** aus dem Dropdown-Menü. Es kann eine der folgenden Optionen sein:
   - Passwort
   - Zertifikat
5. Klicken Sie auf **Weiter**.
6. Wählen Sie eine oder mehrere Benutzergruppen aus, an die diese Konfiguration verteilt werden soll.
7. Klicken Sie auf **Fertig**.

Passwortkomplexität einstellen

Definieren Sie Passwortkomplexität sowie Richtlinienparameter für lokale Konten zur Geräteregistrierung und greifen Sie dann auf das Selbstbedienungsportal und das Administratorportal zu.

> Beachten Sie, dass die Sicherheit eines Passwortes von der Passwortlänge, den Eigenschaften des Passworts und den Richtlinien abhängt, die Sie hier einstellen.

Damit definieren Sie auch den Schwierigkeitsgrad für die Auswahl eines gültigen Passworts durch einen Benutzer. Wenn Sie für Ihre Endbenutzer lokale Konten verwenden und sichere Passwörter für den Zugang zum Administratorportal haben möchten, sollten Sie eine PIN für die Geräteregistrierung verwenden, damit die Passwortkomplexität nicht die Geräteregistrierung behindert. Verwenden Sie die Einstellung „Geräteregistrierungs-Authentifizierung“, um den Authentifizierungsmodus für die Geräteregistrierung unter **Benutzereinstellungen > Geräteregistrierungseinstellung** auszuwählen.

Verfahren

1. Bearbeiten Sie die Standardvorgabe für die **Passwortkomplexität**.
2. Definieren Sie die folgenden Einstellungen zur Passwortkomplexität:

Einstellung	Aktion
Mindestlänge des Passworts	Stellen Sie mit dem Schieberegler die Mindestlänge eines Passwortes ein, damit die Benutzer keine zu kurzen und unsicheren Passwörter verwenden. Nummernkreise zwischen 8 und 32.
Obligatorische Eigenschaften	Definieren Sie die Anzahl der Passwortzeichen, die ein Passwort haben muss. Es sollten mindestens 3 Merkmale übereinstimmen (bei Behördenkunden 4 Merkmale).
Obligatorische Sonderzeichen (Symbole)	Legen Sie die Anzahl der nicht-alphanumerischen Zeichen fest, die ein Passwort enthalten muss.
Großbuchstaben erforderlich	Legen Sie die Anzahl der Großbuchstaben fest, die ein Passwort enthalten muss.
Obligatorische Kleinbuchstaben	Legen Sie die Anzahl der Kleinbuchstaben fest, die ein Passwort enthalten muss.
Obligatorische Ziffern	Legen Sie die Anzahl der Ziffern fest, die ein Passwort enthalten muss.
Passwortvalidierungen	
Ziffernsequenz zulässig	Legen Sie die Anzahl der sich wiederholenden Ziffern in einer Sequenz fest. Beispiel: 123.
Zeichenwiederholung zulässig	Legen Sie die Anzahl der sich wiederholenden Buchstaben in einer Sequenz fest. Beispiel: bbc.

3. Passen Sie mit der folgenden Passwortrichtlinieneinstellung das Verhalten an.

Einstellung	Aktion
Bisher verwendete Passwörter	Verstellen Sie den Schieberegler, um die Anzahl der neuen Passwörter für ein Benutzerkonto zu ändern, die verwendet werden müssen, bevor wieder ein altes Passwort verwendet werden darf. Nummernkreise zwischen 3 und 36.
Passwortverfallsdauer	Bewegen Sie den Schieberegler, um die Gültigkeitsdauer des Passworts in Tagen festzulegen. Nummernkreise zwischen 30 und 365 Tagen.
Inaktivitäts-Zeitüberlauf	Bewegen Sie den Schieberegler, um die Zeit anzugeben, die ein Benutzer vor einer Admin-Portal- oder einer Self-Service-Portal-Sitzungszeit inaktiv sein darf. Zahl variiert zwischen 5 und 60 (Minuten).
Schwellenwert für fehlgeschlagene Anmeldungen	Stellen Sie mit einem Schieberegler die Anzahl der fehlgeschlagenen Anmeldeversuche ein, bevor das Konto 5 Minuten lang gesperrt wird. Nummernkreise zwischen 2 und 5. Wenn die Zahl der fehlgeschlagenen Versuche innerhalb des Schwellenwerts liegt, wird dem Benutzer bei der Sperre eine Meldung angezeigt, dass er die Anmeldung erneut versuchen kann. Wenn die Zahl der fehlgeschlagenen Versuche den Schwellenwert überschreitet, wird dem Benutzer bei der Sperre eine Meldung angezeigt, dass er die Anmeldung nach einer bestimmten Zeit (in Minuten) erneut versuchen kann.

4. Klicken Sie auf **Fertig**. Auch wenn Sie die Standardeinstellung für die Passwortkomplexität ändern, bleibt ein älteres Passwort des vorhandenen lokalen Kontos unverändert. Nach Ablauf der Gültigkeit wird der Benutzer aufgefordert, ein neues Passwort einzugeben. Administratoren, die versuchen, sich im Administratorportal anzumelden, können sich an das Helpdesk wenden, um Unterstützung beim Reset des Passworts zu erhalten.

> Bei einer Geräteregistrierung sollte nur eine Registrierung per PIN verwendet werden.

Nutzungsbedingungen definieren

Verfahren

1. Erstellen Sie eine neue Einstellung für die **Nutzungsbedingungen**.
2. Weisen Sie einen Namen zur Identifizierung der Einstellung zu.
3. Geben Sie eine optionale Beschreibung der Einstellung ein.
4. Wählen Sie **Benutzer auffordern ...** aus. aus.
5. Geben Sie einen anzuzeigenden Titel und Text ein.
6. Klicken Sie auf **+Add**, um mindestens eine Benutzergruppe auszuwählen, der Sie die Einstellung zuteilen möchten.
7. Klicken Sie auf **Speichern**.

> Sobald die Nutzungsbedingungen akzeptiert wurden, können sie nicht gelöscht werden. Sie können die Aufforderungen zur Neuregistrierung ausschalten, indem Sie die Option Den Benutzer auffordern ... aus.

Erinnerungs-E-Mails für die Einladung des Benutzers konfigurieren

Administratoren können mit dieser Einstellung zum Versand von Erinnerungs-E-Mails den Benutzer an Geräteregistrierungen erinnern.

Verfahren

1. Vorhandene **Einstellung zur Einladung des Benutzers** bearbeiten oder neue hinzufügen.
2. Bearbeiten oder weisen Sie einen Namen zur Identifizierung der Einstellung zu.
3. Geben Sie eine optionale Beschreibung der Einstellung ein.
4. Achten Sie darauf, dass die Option „Erinnerungs-Einladungen an **Benutzer**“ aktiviert ist.
5. Wählen Sie in dem Abschnitt „Anfangs- und Enddatum definieren“ aus, wann der Versand von E-Mail-Erinnerungen beginnen und enden soll.

> Es können maximal 30 E-Mails versendet werden. Um dieses Limit zurückzusetzen, muss der Administrator die Einladungen neu versenden.

6. Wählen Sie in dem Bereich „Häufigkeit definieren“ aus, wie oft Sie E-Mail-Erinnerungen versenden wollen.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie eine Verteilungsebene für diese Konfiguration aus.
9. Klicken Sie auf **Fertig**.

Bestätigungs-E-Mails zur Benutzerregistrierung konfigurieren

Administratoren können E-Mails an neue Benutzer senden, die die Registrierung abgeschlossen haben.

Verfahren

1. Bearbeiten Sie eine vorhandene **Einstellung zur Einladung des Benutzers** oder fügen Sie eine neue hinzu.
2. Bearbeiten oder weisen Sie einen Namen zur Identifizierung der Einstellung zu.
3. Geben Sie eine optionale Beschreibung der Einstellung ein.
4. Stellen Sie sicher, dass die Option **Bestätigungs-E-Mail bei erfolgreicher Benutzerregistrierung senden** aktiviert ist.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie eine Verteilungsebene für diese Konfiguration aus.
7. Klicken Sie auf **Fertig**.

Benutzerarbeitsplan konfigurieren

Administratoren können für Benutzer einen Arbeitsplan konfigurieren, der die gesamte Kommunikation zwischen Sentry und den verwalteten Geräten während der vorgeschriebenen arbeitsfreien Zeiten blockiert. Dies ist nützlich für Benutzer in Regionen mit dem mit dem „Recht auf Nichterreichbarkeit“.

Verfahren

1. Klicken Sie auf **Benutzer**.
2. Wählen Sie **Benutzereinstellungen**.
3. Wählen Sie im Abschnitt **Benutzer-Arbeitszeitplaneinstellung** die Option **+Einstellungen für spezifische Benutzergruppen hinzufügen**.
4. Geben Sie einen Namen für die Einstellung ein.

5. Schalten Sie die Einstellung ein.
6. Wählen Sie die Zeitzone aus.
7. Legen Sie fest, wie viele Stunden die Cloud das Exchange ActiveSync-Protokoll, AppConnect-fähige Apps und verwaltete Apps blockieren soll.
8. Klicken Sie auf **Weiter**.
9. Konfigurieren Sie die Verteilung und klicken Sie dann auf **Fertig**.

> Es kann bis zu 1 Stunde und 15 Minuten dauern, bis die Änderungen auf dem Gerät wirksam werden.

Administrationsportal-Authentifizierungseinstellung konfigurieren

Administratoren können den Authentifizierungstyp zur Authentifizierung der Benutzeranmeldung festlegen. Diese Einstellung legt fest, ob die Benutzer nur ihr Passwort oder Passwort und PIN eingeben müssen.

Verfahren

1. Bearbeiten Sie eine vorhandene **Admin Portal Auth-Einstellung** oder fügen Sie eine neue hinzu.
2. Bearbeiten oder weisen Sie einen Namen zur Identifizierung der Einstellung zu.
3. Geben Sie eine optionale Beschreibung der Einstellung ein.
4. Wählen Sie im **Administrationsportal-Authentifizierungstyp** eine der folgenden Optionen aus:

Option	Beschreibung
Passwort	Wählen Sie diese Option aus, um zur Authentifizierung nur die Anmeldung per Passwort zu verwenden. HINWEIS: Benutzer können weiterhin eine PIN erhalten, um die Kontoaktivierung abzuschließen.
Passwort und PIN	Wählen Sie diese Option aus, um zur Authentifizierung der Anmeldung Passwort und PIN zu verwenden. Wenn Sie diese Option auswählen, werden die folgenden zusätzlichen Felder angezeigt: • **PIN-Verwendungsdauer**: Klicken Sie auf die Verwendungsdauer in Minuten in der PIN-Dropdown-Liste. Die Einstellung für Minuten sollte zwischen 1 und 15 liegen. • **PIN-Länge**: Wählen Sie in der Dropdown-Liste aus, wie viele Zeichen für die PIN verwendet werden müssen. Die PIN-Länge sollte zwischen 4 und 12 liegen. Diese Option gilt nur für lokale Konten und nicht für LDAP-Administrationskonten.
Benutzer darf eine neue PIN anfordern	Wählen Sie diese Option aus, damit Benutzer eine neue PIN anfordern können.

5. Klicken Sie auf **Weiter**.
6. Wählen Sie eine Verteilungsebene für diese Konfiguration aus.
7. Klicken Sie auf **Fertig**.

Für Benutzer, die mit einem SAML Identity Provider (IdP) konfiguriert sind, unterstützt Ivanti Neurons for MDM die PIN-Authentifizierung am Administrationsportal. Der Authentifizierungstyp des Admin-Portals sollte „PIN und Passwort“ sein. Diese

Funktion ermöglicht als Zwei-Faktor-Authentifizierung zusätzliche Sicherheit. Wenn in diesem Fall ein solcher Benutzer versucht, sich am Portal anzumelden:

- Wird eine PIN an die E-Mail-ID des Benutzers gesendet.
- Der Benutzer gibt die PIN auf der Anmeldeseite des Administrationsportals ein.
- Wenn die PIN korrekt ist, wird der Benutzer auf die Anmeldeseite des IdP weitergeleitet, wo er den IdP-Benutzernamen und das Passwort eingibt.
- Wenn die IdP-Anmeldeinformationen korrekt sind, wird der Benutzer an das Administratorportal weitergeleitet.

Bei der Anmeldung am Administratorportal kann ein Benutzer auf **Passwort vergessen** klicken, um sein Passwort zurückzusetzen. Auf dem nächsten Bildschirm kann der Benutzer ein neues Passwort und die PIN (die aufgrund der Einstellungen des vorhergehenden Authentifizierungsmodus abgefragt wird) eingeben, die an die E-Mail-Adresse des Benutzers gesendet wurde. Klicken Sie bei Bedarf auf **PIN erneut senden**. Der Benutzer muss 15 Minuten warten, bis er eine neue Anfrage vom Typ "Kennwort vergessen" senden kann.

> Wenn diese Konfiguration an Geräte verteilt wird, führt der nächste erfolglose Anmeldeversuch (Standardwert: 5 Versuche) mit Passwort oder PIN zur Kontosperrung des Benutzers, und ihm wird eine Meldung über die Sperrung angezeigt.

6.4. Benutzer-Branding

Mit Benutzer-Branding können Sie den Geräteregistrierungsprozess mit Namen und Logos kundenspezifisch anpassen, die Ihre Benutzer kennen. Sie können das Benutzer-Branding wie folgt anpassen:

- Definieren Sie einen kundenspezifischen Host-Namen für die Registrierungs-URL.
- Zeigen Sie Ihr Logo in der Registrier-E-Mail und im Registrierbildschirm an.
- Zeigen Sie ein benutzerdefiniertes Favicon bei der Registrierung an.

> Durch Aktualisieren der obigen Einstellungen ändert sich der Wert, auf den **$** verweist.

Lizenz: Gold

Voraussetzung:

- Legen Sie den Host-Namen fest, den Sie für die benutzerdefinierte URL verwenden wollen. Er muss folgende Anforderungen erfüllen:
  - Keine Leerzeichen
  - Keine Sonderzeichen

Benutzen Sie eine Logo-Datei mit folgenden Eigenschaften:

  - PNG-Format
  - 580 x 80 Pixel

Verwenden Sie eine Favicon-Datei mit folgenden Eigenschaften:

  - PNG-Format
  - 64 x 64 Pixel

Schritte:

1. Gehen Sie zu **Benutzer > Benutzer-Branding**.
2. Klicken Sie auf Anpassen (oben rechts).
3. Geben Sie in dem Feld **Host-Name** ein Kürzel ein, das Sie als Host-Namen in Ihrer URL verwenden wollen.
4. Klicken Sie auf **Verfügbarkeit prüfen**, um zu bestätigen, dass der eingegebene Host-Name nicht bereits verwendet wird.
5. Wenn der Host-Name nicht verfügbar ist, geben Sie einen anderen Namen ein.
6. Notieren Sie die entsprechende Registrierungs-URL unter URL Vorschau.
7. Klicken Sie auf **Weiter**.
8. Klicken Sie unter Logo auf Datei auswählen, um das Logo für die Registrierungs-E-Mail und den Registrierungsbildschirm hochzuladen.
9. Klicken Sie auf **Weiter**.
10. Klicken Sie unter **Favicon** auf **Datei wählen**, um das Favicon hochzuladen, das bei der Registrierung statt des Cloud-Favicons erscheinen soll.
11. Klicken Sie auf **Fertig**.

6.5. Benutzerregistrierung mit Apple Business Manager

Dieser Abschnitt enthält die folgenden Themen:

Gilt für:

- Nicht überwachte Geräte mit iOS 13.0 bis zur neuesten Version, die von Ivanti Neurons for MDM unterstützt wird.
- Geräte mit macOS 10.15 oder unterstützten neueren Versionen Ivanti Neurons for MDM.

Der Apple Business Manager ist für IT-Teams eine Möglichkeit, die Bereitstellung von Geräten zu automatisieren, Inhalte zu kaufen und zu verteilen und die Rollen in ihren Unternehmen zu verwalten. Apple Business Manager implementiert die Benutzerregistrierung - eine Registrierungsoption für Unternehmen, die ein BYOD-Programm (Jeder bringt sein eigenes Gerät mit) implementieren. Die Benutzerregistrierung ist eine modifizierte Version des MDM-Protokolls mit einem deutlich stärkeren Datenschutz der Benutzer; implementiert wird ein Sicherheitsniveau, wie es Unternehmen benötigen.

Über die Benutzerregistrierung kann der Administrator folgende Aktionen durchführen:

- Verwaltete Apps installieren und entfernen
- Netzwerkkonfigurationen installieren und entfernen
- Ein partielles VPN für verwaltete Anwendungen und Konten installieren
- Die Verwendung eines Passworts verlangen.

Voraussetzungen für die Aktivierung der Benutzerregistrierung

Im Folgenden sind die Voraussetzungen für die Aktivierung der Benutzerregistrierung aufgeführt. Wenn eine der Anforderungen nicht erfüllt ist, erfolgt die Registrierung als Geräteregistrierung.

- Ein nicht überwachtes Gerät mit iOS 13.0 bis zur neuesten Version, die von Ivanti Neurons for MDM unterstützt wird, oder ein Gerät mit macOS 10.15 oder bis zur neuesten Version, die von Ivanti Neurons for MDM unterstützt wird.
- Die Benutzereinstellung für das Feld „Apple Enrollment Type“ sollte auf „User Enrollment“ gesetzt werden.
- Ein Apple Business Manager-Konto.
    - Das Apple App-Lizenzkonto muss zu demselben Apple Business Manager Konto gehören.
    - Wenn im Apple Business Manager unter „Standorte“ ein Konto aufgeführt ist, muss Apps and Books dem gleichen Standort zugeordnet sein. Möglicherweise müssen Sie einen neuen Standort hinzufügen (z. B. US-Westküste).

Verwaltete Apple-ID – Die verwaltete Apple-ID, die jedem registrierten Gerät zugeordnet werden muss.

- Diese verwaltete Apple-ID ermöglicht die Authentifizierung für die MDM-Verwaltung und die App-Lizenzierung.
- Wenn MDM Anwendungen und Medien per Push verteilt, werden die erforderlichen Apple-Lizenzen der mit dem Gerät verbundenen verwalteten Apple-ID zugewiesen.
- Als Teil der DSGVO-Compliance werden verwaltete Apple-IDs in der Benutzerliste und den Benutzerdetailseiten maskiert, da die Apple ID als Teil der Benutzerdaten betrachtet wird.
- Verwaltete Apple-IDs wurden zuerst vom Apple School Manager verwendet und werden nun vom Apple Business Manager für das User Enrollment genutzt.

> Die verwaltete Apple-ID des Geräts und das Apps and Books Location-Token sollten aus der Organisation des gleichen Apple Business Manager-Kontos stammen.

Bei Unterschieden wird im Ivanti Neurons for MDM Admin-Portal eine Benachrichtigung angezeigt, wenn die Lizenzzuweisung für eine App fehlschlägt.

Microsoft Entra ID ist konfiguriert für die föderierte Authentifizierung oder eine manuell im Apple Business Manager erstellte Apple-ID mit einer validierten Domäne.

- Anweisungen zur Verwendung der föderierten Authentifizierung finden Sie im **Apple Business Manager User Guide** auf der Apple-Website. Eine Anmeldung ist erforderlich.

Gerätebenutzer, die mit LDAP synchronisiert werden, sind einer Geräteverwaltungsrolle zuzuordnen und mit einer verwalteten Apple-ID zu verknüpfen.

Auf der Seite **Benutzerliste** und der Seite **Geräteliste** können Sie die Spalte „Verwaltete Apple-ID“ hinzufügen, die für alle Benutzer angezeigt werden soll. Auf der Listenseite **Geräte** können Sie die Spalte „Angemeldete Benutzerregistrierung“ hinzufügen, um den Status der Benutzeranmeldegeräte anzuzeigen. Darüber hinaus enthalten die Benutzer- und Geräteexporte diese Spalten in CSV-Dateien.

Priorität der Registrierungen

- Die Benutzerregistrierung wird über den Go for iOS-Client und iReg unterstützt. Apple bietet keine Unterstützung mehr für die Benutzerregistrierung über Ivanti Go for iOS und iReg. Die **kontogesteuerte Benutzerregistrierung** ist nur im Work- oder School-Konto des Geräts verfügbar.
- Automatisierte Geräteregistrierungen und Apple Configurator-Registrierungen sind immer Geräteregistrierungen.
- Wenn die MAM-Konfiguration für ein Gerät übernommen wird, hat die MAM-Registrierung Vorrang vor der Benutzerregistrierung.
- Wenn sowohl die Anforderungen für Nur-Authentifizierung als auch für die Benutzerregistrierung erfüllt sind, hat die Benutzerregistrierung Vorrang.
- Wenn Sie ein Gerät vom Go for iOS-Client aus neu registrieren, ist der Registrierungstyp derselbe wie bei der Geräteregistrierung, unabhängig von der Änderung des Registrierungstyps in Ivanti Neurons for MDM. Wenn beispielsweise für ein Gerät eine Benutzerregistrierung vorgenommen wurde, die Registrierungsart in Ivanti Neurons for MDM in „Geräteregistrierung“ geändert und das Gerät vom Go-Client erneut registriert wird, behält das Gerät weiterhin die Benutzerregistrierung und erhält nicht die Gerätregistrierung.

Unterschied zwischen Standard-MDM-Registrierung und Benutzerregistrierung

Dieser Abschnitt erläutert den Unterschied zwischen der Standard-MDM-Registrierung und der Benutzerregistrierung mit dem Apple Business Manager.

Standard-MDM-Registrierung

Die folgende Liste gibt an, welche Rechte ein Ivanti Neurons for MDM-Server in einer Standard-MDM-Registrierung hat, nicht aber im Benutzerregistrierungsmodus.

Der MDM-Server:

- Kann das Gerät nicht löschen.
- Sieht nicht die privaten Anwendungen, die der Gerätebenutzer auf dem Gerät installiert hat.

- Kann vom Benutzer installierte Anwendungen nicht in MDM-Anwendungen konvertieren.
- Gerätepasscode kann nicht gelöscht werden (d. h. das Gerät entsperren).
- Kann keine lange, komplexe Geräte-Passcode-Anforderung festlegen.
- Kann kein geräteweites VPN und kein WLAN-Proxy konfigurieren, und auch keine Mobilfunkfunktionen verwalten.
- Kann Gerätekennungen wie die UDID, Seriennummer oder IMEI nicht anzeigen.
- Kann nicht viele geräteweite Einschränkungen anwenden (z. B. die Bewertung von App-Inhalten einschränken), die iCloud blockieren und die überwachten Einschränkungen übernehmen.

Benutzerregistrierung mit dem Apple Business Manager

Bei der Benutzerregistrierung kann der MDM-Server nach wie vor alle Aufgaben ausführen, die zur Verwaltung von Unternehmensanwendungen, Konten und Daten erforderlich sind.

Die Benutzerregistrierung kann:

- Hausinterne Apps oder Apps mit Benutzer-Lizenzen für Apps and Books (Apple) installieren.
  - Die Lizenzen werden in der Reihenfolge ihrer Anforderung vergeben und von den verwalteten Apple-IDs verbraucht.
  - Die Lizenz, die von einer auf dem Gerät des registrierten Benutzers installierten App verbraucht wird, ist nicht identisch mit der Lizenz, die von der gleichen App bei der Installation auf dem Gerät des registrierten Benutzers verbraucht wird.
  - Überprüfen Sie den Lizenztyp für Apple Apps and Books-Anwendungen auf einer Benutzerdetailseite über die Registerkarte „Lizenznutzung“ - der Registrierungstyp wird als „User Enrollment“ oder „Device Enrollment“ angezeigt.

Passcode-Payload-Einstellungen erzwingen – Beispiel:

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

Daten für vom Unternehmen verwaltete Anwendungen, Zertifikate und Profile abfragen.

- Ein VPN pro App für Apps, E-Mails, Kontakte und Kalender konfigurieren, die durch MDM installiert wurden.
- Einige Einschränkungen durchsetzen, z. B. verwaltete Öffnungsrechte, verwaltete Kontakte, verwaltete Daten auf dem Sperrbildschirm und einige andere.

Unternehmensdaten werden in einem separaten Apple File System (APFS)-Volume gespeichert, das bei der Registrierung erstellt und getrennt von den Daten der Gerätebenutzer verschlüsselt wird. Dieses Volume enthält Daten, die von verwalteten Anwendungen, Enterprise Notes, Enterprise iCloud Drive-Dokumenten, Enterprise Keychain-Einträgen, verwalteten E-Mail-Anhängen und -Texten sowie Kalenderanhängen gespeichert werden. Wenn Sie die Registrierung von MDM aufheben, werden das Volume und die Schlüssel zerstört.

Drittanbieter-Apps können nur eine persönliche App oder eine über die Cloud verwaltete App sein. Der MDM-Dienst kann keine Apps verwalten, die der Gerätebenutzer bereits installiert hat. In diesem Fall muss der Administrator den Gerätebenutzer auffordern, die private App zu löschen, bevor die App über MDM installiert wird. Der MDM-Dienst kann keine Apps verwalten, die der Benutzer bereits installiert hat. Einige Systemanwendungen wie Notes and Files unterstützen jedoch sowohl Arbeits- als auch private Konten.

User Enrollment für macOS-Geräte

Die Benutzerregistrierung wird für Geräte mit macOS 10.15 oder unterstützten neueren Versionen unterstützt Ivanti Neurons for MDM.

- Mobile@Work für macOS wird für Geräte mit macOS-Benutzerregistrierung nicht unterstützt.
    - Selbst wenn die App auf das Gerät mit macOS-Benutzerregistrierung verteilt wird, wird die App nicht per Push von MDM auf das Gerät übertragen.
    - Daher werden Mobile@Work-Funktionen wie die Skriptverwaltung und die App-Verwaltung für die Packager-Apps (MIP) nicht für mit macOS User Enrollment registrierte Geräte unterstützt.

App-Abhängigkeit und Verhaltensänderungen in mit macOS User Enrollment registrierten Geräten.

    - Bei mit macOS User Enrollment registrierten Geräten funktioniert die App-Abhängigkeit teilweise, da MDM den Installationsstatus der erforderlichen Apps nicht kennt (nicht bestätigen kann), bevor die Haupt-App verteilt wird.
    - Apps und Konfigurationen können an Benutzer und Benutzergruppen verteilt werden, die zu den mit macOS User Enrollment registrierten Geräten gehören. Die Apps zeigen jedoch immer die Schaltfläche **Installieren** statt der Schaltfläche „Installiert“ an, da MDM den Installationsstatus von Apps in mit macOS User Enrollment registrierten Geräten nicht anzeigen kann.
    - Installierte Apps werden als angeforderte Apps auf der Seite **Geräte > App-Bestand** angezeigt, da die mit macOS User Enrollment registrierten Geräte dem Ivanti Neurons for MDM-Server im Bestandsbericht nicht mitteilen, ob die Apps installiert sind.

Im Verteilungsfilter für Apps können die Attribute „Mit User Enrollment registriert“ und „Automatische mit Device Enrollment registriert“ je nach Bedarf für die benutzerdefinierte Verteilung verwendet werden.

- Benutzerbasierte Lizenzen mit verwalteten Apple IDs werden zur Installation von Apple Apps and Books-Apps unterstützt. Geräte-Lizenzen sind nicht zulässig. Der App-Katalog zeigt nur Apple Apps and Books-Apps an.
- Nicht alle Konfigurationen, Richtlinien und Aktionen sind zulässig. Siehe dazu die vollständige Liste der Konfigurationen und Richtlinien nach der Beschreibung dieses Verfahrens.
    - Wenn nicht unterstützte Konfigurationen an ein unter macOS User Enrollment registriertes Gerät verteilt werden, erfolgt keine Verteilung oder Übernahme auf dem Gerät. Ggf. wird eine Meldung wie „Einschränkungen – kein gültiger Anforderungstyp“ angezeigt.
    - In ähnlicher Weise werden nicht unterstützte Verwaltungsgeräteaktionen in der Ivanti Neurons for MDMBenutzeroberfläche angezeigt.
    - Nicht unterstützte Berichte werden nicht über Ivanti Neurons for MDM gesendet.

Nachfolgend sind die nicht unterstützten Konfigurationen und Richtlinien aufgeführt, die an mit macOS User Enrollment registrierte Geräte verteilt werden sollen:

- Passwort
- Tunnel
- Tunnel (bei Bedarf)
- VPN-Konfigurationen
- Office 365 Auto-Kontoerstellung
- Erweiterungsrichtlinie für den macOS Kernel
- Datenschutzpräferenz
- Einschränkungen für macOS
- [Software Updates]
- AirPrint
- MI Client Datenschutz

- FileVault 2
- FileVault-Wiederherstellungsschlüssel
- Firewall
- Systemrichtlinienregel
- Zertifikatspräferenz
- Systemrichtlinienkontrolle
- Durch Systemrichtlinie verwaltet
- macOS AppStore-Einschränkungen
- Beschränkungen beim Brennen von CDs/DVDs in macOS
- Einstellungen für macOS Finder
- Mobile@Work für macOS
- Mobile@Work für macOS-Script
- Kontrolle zulässiger Medien
- Zeitserver
- Erlaubte Apps-Richtlinie

Unterschied zwischen Benutzerregistrierung und Geräteregistrierung

Dieser Abschnitt erläutert den Unterschied zwischen der Benutzerregistrierung und der Geräteregistrierung.

User Enrollment gilt für Geräte mit iOS 13.0 und macOS 10.15 bis zur letzten unterstützten Version. Geräte bis zur Version iOS 13.0 und macOS 10.15 werden als Geräte mit „Geräteregistrierung“ erkannt, unabhängig davon, ob der Gerätebenutzer für die Benutzerregistrierung aktiviert wurde.

> Beim User Enrollment für den Apple Business Manager ist eine Löschung oder Entsperrung nicht möglich. Das Benutzerportal wird diese Optionen jedoch weiterhin anzeigen, auch wenn sie nicht funktionieren.

Benutzerregistrierung vs. Geräteregistrierung			
Funktionalität	Benutzer-Registrierung	Mobile Application Management (MAM)	Geräteregistrierung
Gerät löschen und die privaten Anwendungen des Benutzers anzeigen.	✗	✗	✓
Verwaltete in nicht verwaltete konvertieren und umgekehrt.	✗	✗	✓
Geräte-Passcode löschen, ein geräteweites VPN oder den WLAN-Proxy konfigurieren oder Mobilfunkfunktionen verwalten	✗	✗	✓
Siehe dazu Gerätekennungen wie Seriennummer, IMEI	✗	✗	✓
Beaufsichtigte Einschränkungen übernehmen	✗	✗	✓ (Nur überwachte Geräte)
Kann Anwendungen und Konten installieren und konfigurieren	✓	✓	✓
Kann ein App-spezifisches VPN für Apps, E-Mails, Kontakte und Kalender konfigurieren, die mit MDM installiert wurden.	✓	✗	✓
Kann einige Einschränkungen erzwingen, z. B. verwaltete Öffnungsrechte, verwaltete Kontakte, verwaltete Daten auf dem Sperrbildschirm und einige andere.	✓	✗	✓
Kann Daten zu den vom Unternehmen verwalteten Anwendungen, Zertifikaten und Profilen abfragen.	✓	✗	✓

Verbinden von Ivanti Neurons for MDM mit Apple Business Manager

Dieser Abschnitt erläutert, wie die Benutzerregistrierung mit dem Apple Business Manager erfolgt.

Voraussetzungen

- Sie müssen über ein Apple Business Manager Konto verfügen. Siehe **https://business.apple.com/**.
- Sie müssen ein Apple-**MDM-Zertifikat** zur Verwaltung von iOS-Geräten anfordern und installieren.

Erstellen lokaler Benutzer zum Aktivieren der Benutzerregistrierung

Dieser Abschnitt erläutert, wie lokale und LDAP-Benutzer angelegt und die Benutzerregistrierung für nicht überwachte Apple-Geräte eingestellt wird. Die Benutzerregistrierung funktioniert nicht auf überwachten Geräten oder Geräten, die mit dem Device Enrollment von Apple registriert sind.

Manuell verwaltete (statische) Benutzergruppe erstellen

Dies ist ein einmaliges Verfahren. Wenn Sie diese Gruppe bereits erstellt haben, fahren Sie mit dem Abschnitt „Benutzer für die Benutzerregistrierung erstellen“ fort.

Verfahren

1. Gehen Sie zu **Benutzer >** Benutzergruppen.
2. Erstellen Sie eine manuell verwaltete (statische) Benutzergruppe, z. B. die Benutzerregistrierungsgruppe, um Benutzer mit dieser Geräteregistrierungsart als Benutzerregistrierung hinzuzufügen.
3. Klicken Sie auf **Speichern**.

Einstellung für die Geräteregistrierungsart definieren

Dies ist ein einmaliges Verfahren. Wenn Sie diese Gruppe bereits erstellt haben, fahren Sie mit dem Abschnitt „Benutzer für die Benutzerregistrierung erstellen“ fort. Bei mit User Enrollment registrierten Geräten lautet die Standardeinstellung für den Gerätebesitzer \“User Owned.“

Verfahren

1. Gehen Sie zu **Benutzer >** Benutzereinstellungen.
2. Klicken Sie im Abschnitt „Einstellung für die Geräteregistrierung“ auf **+ Einstellung für bestimmte Benutzergruppen hinzufügen**.
3. Definieren Sie eine neue Einstellung, z. B. UE-Registrierung, für Benutzer mit dieser Geräteregistrierungsart als Benutzerregistrierung.
4. Wählen Sie im Abschnitt „Apple-Anmeldung“ **als Apple-Anmeldungsart** User Enrollment.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite „Verteilung der Benutzereinstellungen“ die neu erstellte Benutzergruppe, z. B. die Benutzerregistrierungsgruppe.
7. Klicken Sie auf **Fertig**.

Lokalen Benutzer für die Benutzerregistrierung anlegen

Als Voraussetzung müssen Sie eine manuell verwaltete Benutzergruppe und eine Geräte-Registrierungseinstellung für die Benutzerregistrierung erstellen.

Verfahren

1. Gehen Sie zu BenutzerUsers.htm.
2. Klicken Sie auf **+ Hinzufügen** > **Einzelbenutzer**.
   Geben Sie die neuen Benutzerinformationen ein und fügen Sie sie der neu geschaffenen Benutzergruppe hinzu, z. B. der Gruppe „Benutzerregistrierung“. Weitere Informationen finden Sie unter *Hinzufügen eines Benutzers* im Thema **Benutzer**.

LDAP-Benutzer zur Aktivierung der Benutzerregistrierung importieren

Voraussetzungen

- Als Voraussetzung müssen Sie einen Ivanti Neurons for MDM Connector für den Zugriff auf **LDAP-Ressourcen** einrichten.
- Wählen Sie bei der Einstellung **Verwaltete Apple-ID** die Option **Muster** (E-Mail-Adresse des Benutzers) aus. Stellen Sie sicher, dass das Muster für die verwaltete Apple-ID eindeutig ist. Andernfalls wird das Konto nicht mit der verwalteten Apple-ID

aktualisiert, wenn die gleiche verwalteten Apple-ID in einem anderen Konto vorhanden ist.

- Fügen Sie optional die Unterdomäne "appleid" ein, um Konflikte mit bestehenden Apple-IDs zu vermeiden.
- Sie können Benutzer aus LDAP importieren und zur Benutzerregistrierung einladen. Für die importierten LDAP-Benutzer werden die verwalteten Apple-IDs mit der Ivanti Neurons for MDM synchronisiert, was Voraussetzung für die Benutzerregistrierung ist.

Verfahren

1. Gehen Sie zu **Benutzer**.
2. Klicken Sie auf **+Hinzufügen > Benutzer aus LDAP einladen**.
3. Klicken Sie in dem LDAP-Server-Eintrag auf **Benutzer auswählen.**
4. Geben Sie auf der Seite „LDAP-Benutzer hinzufügen“ den Namen des Benutzers, der Gruppe oder der Organisationseinheit in dem Suchfeld ein.
5. Klicken Sie zum Hinzufügen neuer Benutzer oder Gruppen neben dem Eintrag, den Sie ergänzen wollen, auf **+ Hinzufügen**.
6. Klicken Sie auf **Fertig**.

Importieren von Entra ID-Benutzern zum Aktivieren der Benutzerregistrierung

Eine Voraussetzung ist, dass Sie Ivanti Neurons for MDM mit Microsoft Entra ID verbinden.

Sie können Entra ID-Benutzer zur Benutzerregistrierung einladen. Für die importierten Entra ID-Benutzer werden die verwalteten Apple-IDs mit Ivanti Neurons for MDM synchronisiert, was Voraussetzung für die Benutzerregistrierung ist.

Verfahren

1. Wechseln Sie zu **Admin >** Entra ID-Benutzerquelle.
2. Bearbeiten Sie die Einstellungen.
3. Wählen Sie die Option **Dieses Entra ID aktivieren**.
4. Wählen Sie bei der Einstellung für die verwaltete Apple-ID eine oder mehrere der folgenden Optionen aus:
    - **Muster**
        - **E-Mail-Adresse des Benutzers** – Stellen Sie sicher, dass das Muster für die verwaltete Apple-ID eindeutig ist. Andernfalls wird das Konto nicht mit der verwalteten Apple-ID aktualisiert, wenn die gleiche verwalteten Apple-ID in einem anderen Konto vorhanden ist.
        - Wählen Sie alternativ **userUPN** aus.
5. Fügen Sie optional die Unterdomäne "appleid" ein, um Konflikte mit bestehenden Apple-IDs zu vermeiden.
6. Wählen Sie die Option **Aus Entra ID importierte Benutzer automatisch einladen**. Benutzer, die aus Entra ID in Ivanti Neurons for MDM importiert wurden, erhalten automatisch eine Einladung zur Registrierung per E-Mail.
7. Klicken Sie auf **Speichern**.

Anweisungen für Gerätebenutzer zum Registrieren über die Benutzerregistrierung

Dieser Abschnitt befasst sich mit den Aktionen, die der Gerätebenutzer zur Registrierung mit Apple User Enrollment durchführen muss.

Verfahren

1. Öffnen Sie auf dem iOS-Gerät, das Sie registrieren möchten, die Einladungs-E-Mail; diese enthält einen Link und einen Text, der den Endbenutzer zu einem Registrierungslink wie mobileiron.com/go führt.

2. Öffnen Sie den Registrierungslink in Safari.
3. Die Anmeldeseite wird angezeigt. Der Gerätebenutzer muss sich mit seinen lokalen Benutzer- oder LDAP-Anmeldedaten anmelden.
   Die Registrierungsseite wird mit der Meldung angezeigt, dass das Profil heruntergeladen wurde.
   Tippen Sie auf Einstellungen. Die Seite mit den Einstellungen wird angezeigt.
4. Tippen Sie auf Anmelden in [Ihr Firmenname].
5. Die Seite „User Enrollment“ wird angezeigt.
6. Tippen Sie auf Mein [Ihr Gerät] registrieren. Tippen Sie beispielsweise auf „Mein iPhone registrieren“.
   Wenn Sie auf „Abbrechen und Profil löschen“ tippen, müssen Sie den Registrierungsprozess von vorn beginnen.
   Sie erhalten eine Anmeldung entweder für Apple oder für Ihren Federated Account. Geben Sie das Passwort für Ihre verwaltete Apple-ID ein. (Die verwalteten Apple-ID wird am oberen Ihrer Anmeldeseite aufgelistet.)
   Möglicherweise wird Ihnen die Option angeboten, angemeldet zu bleiben; treffen Sie eine Auswahl.
   Eine Seite zeigt die Meldung „Die Registrierung ist erfolgreich“ an.

Verwenden von Geräteprotokollen zur Fehlerbehebung

Um Fehler oder Probleme für ein benutzerregistriertes Gerät zu beheben, beginnen Sie mit der Prüfung der Geräteprotokolle.

Verfahren

1. Gehen Sie zu Geräte.
2. Klicken Sie auf den Gerätenamen, um die Seite mit den Gerätedetails anzuzeigen. Sie können die Felder „Angemeldete Benutzerregistrierung“ und „Registrierte Verwaltete Apple-ID“ überprüfen.
3. Klicken Sie auf die Registerkarte Protokolle.
4. Schränken Sie im Bereich „Filter“ die Geräteprotokolle ein, indem Sie nach den Aktionsnamen (z. B. Abmeldung, Gerätename, Bootstrap-Token festlegen, Bootstrap-Token abrufen usw.), Status, Start- und Enddatum filtern.
5. Klicken Sie in der Spalte „Aktionen“ auf das Augensymbol, um die Geräteprotokolldetails, z. B. die Registrierungs-ID, anzuzeigen.
6. Klicken Sie auf **OK**.

6.6. Benutzerlizenzen

Ivanti Neurons for MDM -Lizenzen auf Benutzerbasis definieren die Anzahl der registrierbaren Benutzer, die Anzahl der der pro Lizenz zulässigen Geräte, die Größe des Inhalts, der zur Verteilung an Geräte konfiguriert werden kann, und welche Funktionen verfügbar sind. Wenn Sie die maximale Anzahl an Benutzern erreicht haben, wird auf der Administrationsseite ein rotes Dreieck angezeigt. Wenn Sie die maximale Menge an Inhalten erreicht haben, hindert Sie der Dienst daran, mehr Inhalt hinzuzufügen und zeigt eine Nachricht an, die angibt, dass Sie die Grenze erreicht haben.

Um zu ermitteln, wie viele Benutzerlizenzen Sie brauchen, sollten Sie folgende Punkte berücksichtigen:

- Jede Benutzerlizenz, die unter dem Secure UEM- oder Secure UEM Premium-Paket erworben wird, erlaubt die Registrierung von bis zu fünf Geräten.
- Wenn ein Benutzer mehr als fünf Geräte registriert, wird eine weitere Benutzerlizenz angefordert.
- Es gibt kein Limit für die Anzahl der Benutzerlizenzen, die ein Benutzer anfordern kann.
- Lizenzen werden freigegeben, wenn Geräte außer Dienst gestellt oder gelöscht werden.

Wenn beispielsweise Benutzerin 1 am ersten Arbeitstag ihr Diensttelefon registriert, fordert sie eine Benutzerlizenz an. In der Folgewoche registriert sie mit der gleichen Benutzerlizenz zwei Privattelefone und ein Tablet. Wenn sie ein weiteres Tablet registriert, verfügt sie über vier Geräte und fordert damit eine zweite Benutzerlizenz an. Wenn ihr Privattelefon gestohlen wird, löscht sie das Gerät, damit wird die zweite Benutzerlizenz frei.

Anzeigen der Anzahl von Geräten/Lizenzen für einen Benutzer

Schritte:

1. Gehen Sie zu **Benutzer**.
2. Klicken Sie auf den Link für den Benutzer.

In dem linken Fenster werden die Benutzerdetails aufgelistet, darunter auch die Lizenznutzung.

6.7. Benutzer verwalten

Dieser Abschnitt enthält die folgenden Themen:

- Hinzufügen eines App-API-Benutzers für Cisco ISE Operations
- Zuweisen von Rollen an Benutzer
- Benutzerrollen
- Benutzer suchen und filtern
- Benutzer zu Benutzergruppen zuordnen
- Benutzer einladen
- Aktivieren und Deaktivieren von Benutzern
- Mehrere Administrator-Anmeldungen verwalten
- Passwort ändern
- Nachricht senden
- Benutzer aus Benutzergruppen entfernen
- Benutzer löschen
- Exportieren der Benutzer
- Angepasste Attribute Benutzern zuweisen
- Anpassbare Attribute für Benutzer entfernen
- Benutzer-Regionaleinstellung ändern
- Bearbeiten eines Benutzernamens
- Opting-Out von der Sammlung von Standortdaten
- Informationen zum Timeout
- Systemnutzungsanalyse deaktivieren
- Geräteregistrierung durch PIN-Generierung

6.7.1. Hinzufügen eines App-API-Benutzers für Cisco ISE Operations

Sie können einen API-Benutzer mit der Rolle "Cisco ISE Operations" hinzufügen. Dadurch kann Cisco ISE mit den Cisco ISE-APIs in Ivanti Neurons for MDM interagieren. Nachdem Sie diesen Benutzer angelegt haben, können Sie API-Aufrufe mithilfe seiner Anmeldedaten aus Cisco ISE gegenüber Ivanti Neurons for MDM authentifizieren. Mit diesen APIs kann Cisco ISE Geräteinformationen abrufen, Aktionen auf Geräten ausführen, beispielsweise eine Komplettlöschung oder eine Löschung der Unternehmensdaten, eine PIN-Sperre auslösen und Mitteilungen an Geräte versenden.

> Der API-Benutzer kann sich nicht am Admin-Portal anmelden. Dieser Benutzer ist nur für die Aktivierung der API-Nutzung vorgesehen.

> Nur dem Super-Administrator eines Mandanten ist standardmäßig die Rolle Cisco ISE Operations zugeordnet. Der Super-Administrator muss die übrigen Benutzer im System explizit auswählen, die diese Rolle besitzen sollen, und ihnen diese Rolle zuweisen. Benutzer mit der Rolle Cisco ISE Operations können die Rolle wiederum anderen geeigneten Benutzern im System zuweisen.

Verfahren

1. Wechseln Sie zu **Benutzer** > **Benutzer**.
2. Klicken Sie auf **[Add]**.
3. Wählen Sie die Option **API-Benutzer**.
4. Füllen Sie das Formular mit den Angaben des Benutzers aus:
    - E-Mail-Adresse
    - Vorname
    - Nachname

> Im Feld „Benutzername“ wird die von Ihnen eingegebene E-Mail-Adresse angezeigt. In den meisten Fällen sollten Sie die Standardeinstellungen nicht bearbeiten. Siehe **Zeitpunkt zur Bearbeitung eines Benutzernamens**.

Wenn Sie den Anzeigenamen dieses Benutzers ändern möchten, bearbeiten Sie den Text im Feld **Anzeigename** .

6. Vergeben Sie ein Passwort, indem Sie es in dem Feld **Passwort** und **Passwort bestätigen** eingeben.
7. Lassen Sie die Rolle **API Management Cisco ISE Operations** im Abschnitt **Rollen zuweisen** ausgewählt.
8. Klicken Sie auf **Fertig**, um den Benutzer hinzuzufügen.

Wenn Sie keine Aufgaben auf der Seite **Benutzer** ausführen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie brauchen eine der folgenden **Rollen**:

- Systemverwaltung
- Benutzermanagement

6.7.2. Zuweisen von Rollen an Benutzer

Sie können Benutzern Zugriff auf Ivanti Neurons for MDM-Daten und -Funktionen gewähren, indem Sie ihnen **Rollen** zuweisen. Rollen können Sie Benutzern oder Benutzergruppen direkt zuweisen. Wird eine Rolle einer Benutzergruppe zugeordnet, erhalten alle Benutzer dieser Gruppe diese Rolle.

> Die Rolle "Benutzer schreibgeschützt" ist den Benutzern nicht standardmäßig zugewiesen.
> Die Seite "Rollen" und die zugehörigen Optionen sind für Mandanten ausgeblendet, die sowohl Zugriff auf Ivanti Neurons for UEM als auch Ivanti Neurons for MDM haben.

Benutzer können keine Berechtigungen zuweisen, die sie nicht bereits besitzen. Die Berechtigungen und Rollen, die den Benutzern nicht zugewiesen sind, werden nicht zur Auswahl angezeigt. In diesem Fall wird eine Fehlermeldung angezeigt. Wenn ein Ivanti Neurons for MDM-Administrator oder ein Partner-Administrator versucht, einem Partner-Administrator eine Rolle zuzuweisen, gibt Ivanti Neurons for MDM eine Meldung aus, die darauf hinweist, dass ein Partner-Administrator diesen Vorgang über das Dienstanbieterportal durchführen muss.

Weitere Informationen über Rollen finden Sie unter **Roles_Management.htm**.

Verfahren:

1. Gehen Sie zu:
   - **Benutzer > Benutzer** *oder*
   - Benutzer > Benutzergruppen.

Wählen Sie mindestens einen Benutzer oder eine Benutzergruppe aus.

3. Klicken Sie auf **Aktionen**.
4. Klicken Sie auf der Seite mit den Benutzerdetails oder der Seite mit den Benutzergruppendetails auf **Rollen zuweisen** *oder* Wählen Sie auf der Seite mit der Benutzerliste bzw. Benutzergruppenliste die Option **Rollen anfügen**.
5. Wählen Sie aus den Rollen, die Sie zuweisen wollen, mindestens eine der folgenden Rollen aus:
   - Systemverwaltung | Space-übergreifend
   - Systemdateien schreibgeschützt | Space-übergreifend
   - Benutzerverwaltung | Space-übergreifend
   - Nur schreibgeschützter Benutzer | Space-übergreifend
   - LDAP-Benutzer-Import und -Einladung | Space-übergreifend
   - Geräteverwaltung | Space-spezifisch
   - Gerät schreibgeschützt | Space-spezifisch
   - Apps- und Content-Verwaltung | Space-spezifisch
   - App und Content schreibgeschützt | Space-spezifisch
   - Geräteaktionen | Space-spezifisch
   - Cisco ISE-Operations | Space-spezifisch
   - Verwaltung geplanter Aufgaben | Space-übergreifend
   - Gemeinsame Plattformdienste (CPS) | Space-übergreifend
   - Migrationsmanagement mit minimaler Benutzerbeeinträchtigung | Space-übergreifend

- Anpassbare Geräteregistrierung | Space-übergreifend
- Microsoft Graph bearbeiten | Cross-Space
- Komplettlöschung senden/abbrechen | Space-übergreifend
- Microsoft Graph anzeigen | Space-übergreifend
- Zugriffsintegration verwalten | Space-übergreifend

Klicken Sie auf **Weiter**.

7. Wenn die ausgewählten Rollen an einen Space gebunden sind, wählen Sie für alle Space-gebundenen Rollen Spaces aus.

> Wenn nur ein Space (der Standard-Space) vorhanden ist, wird bei der Zuweisung einer Space-abhängigen Rolle der Schritt zur Space-Definition übersprungen.

Die Übersichtsseite zeigt den Namen des Spaces für die Space-gebundene Rolle als Standard-Space an.
Überprüfen Sie die Übersicht der zuzuweisenden Rollen und klicken Sie auf **Fertig**.

Helpdesk-Mitarbeitern die Berechtigung für grundlegende Geräteaktionen erteilen

Die Helpdesk-Rollen erlauben den Mitarbeitern allgemein die Anzeige von Daten. Manche Unternehmen erlauben jedoch auch einfache Geräteaktionen:

- Check-in erzwingen
- Sperren
- Entsperren
- Nachricht senden
- Gerät löschen
- Wipe durchführen

Verfahren

Sie können Berechtigungen für die Aktionen bereitstellen.

1. Gehen Sie zu **Benutzer > Benutzer*** oder ***Benutzer > Benutzergruppen**.
2. Wählen Sie mindestens einen Benutzer oder eine Benutzergruppe aus.
3. Klicken Sie auf **Aktionen**.
4. Wählen Sie auf der Seite mit den Benutzerdetails bzw. Benutzergruppendetails die Option **Rollen zuweisen** *oder*
   Wählen Sie auf der Seite mit der Benutzerliste bzw. Benutzergruppenliste die Option Rollen anfügen.
5. Wählen Sie **Gerät schreibgeschützt**.
6. Wählen Sie **Geräteaktionen**.
7. Klicken Sie auf **Fertig**.

> Stellen Sie sicher, dass Sie "Schreibgeschütztes Gerät" auswählen, bevor Sie "Geräteaktionen" für die Benutzer auswählen, um die erwarteten Berechtigungen zu erhalten.

6.7.3. Benutzerrollen

Benutzerrollen bestimmen, welche Seiten Benutzern in Cloud angezeigt werden und welche Aktionen sie durchführen können. Die folgende Tabelle zeigt die Rollen, die Sie zuordnen können sowie deren Bedeutung.

Rolle	Beschreibung	Space-spezifisch
Systemverwaltung	Erlaubt einem Administrator die Verwaltung von Einstellungen der Mandanten-Ebene, beispielsweise der MDM-Zertifikate, App Catalog-Einstellungen und weitere.	Nein
System schreibgeschützt	Erlaubt einem Administrator die Anzeige von Einstellungen der Mandanten-Ebene, beispielsweise der MDM-Zertifikate, App Catalog-Einstellungen und weitere.	Nein
Benutzermanagement	Erlaubt das Hinzufügen und Entfernen von Benutzern, die Zuordnung von Rollen und die Ergänzung von Benutzern in Benutzergruppen.	Nein
Benutzer schreibgeschützt	Erlaubt einem Administrator die Anzeige der Benutzer und Benutzergruppen sowie der Apps und Content-Kataloge.	Nein
Geräteverwaltung	Erlaubt einem Administrator die Verwaltung von Gerätegruppen, Konfigurationen und Richtlinien sowie die Durchführung aller Geräteaktionen.	„Ja“,
Geräts schreibgeschützt	Erlaubt einem Administrator die Anzeige der Gerätegruppen, Konfigurationen und Richtlinien.	„Ja“,
Verwaltung von Apps und Inhalten	Erlaubt es einem Administrator, Apps und Content hinzufügen, zu verteilen und zu entfernen.	„Ja“,
App und Inhalt schreibgeschützt	Daten in "Benutzer", "Anwendungen", "Content" einschließlich AppConnect-Aufgaben anzeigen	„Ja“,
Geräteaktionen	Erlaubt es einem Administrator, Geräteaktionen auszulösen, beispielsweise: • Check-in erzwingen • Sperren • Entsperren • Nachricht senden • Gerät löschen • Wipe durchführen Sie müssen vor der Auswahl der Geräteaktionen die Option „Gerät schreibgeschützt“ auswählen. Anderenfalls verfügen die Benutzer nicht über die erwarteten Berechtigungen.	„Ja“,
LDAP-Benutzerimport und Einladung	Erlaubt einem Administrator die Registrierung von LDAP-Benutzern und den Versand von Einladungen zur Geräteregistrierung.	Nein
Cisco ISE Operations	Erlaubt einem Administrator den Aufruf der für die Cisco ISE-Integration benötigten APIs.	Nein
Verwaltung geplanter Aufgaben	Damit kann ein Administrator Aufgaben für verschiedene Verwaltungsoperationen erstellen und zeitlich planen.	Nein
Gemeinsame	Erlaubt es einem Administrator, gemeinsame Plattformdienste zu verwenden.	Nein

Rolle	Beschreibung	Space-spezifisch
Plattformdienste (CPS)		
Migrationsverwaltung mit geringen Benutzerstörung	Erlaubt es einem Administrator, die Einstellungen für die Migration mit geringen Störungen des Benutzers zu verwalten.	Nein
Benutzerdefinierte Geräteregistrierung	Erlaubt es einem Administrator, ein Gerät mit der benutzerdefinierten Geräteregistrierung zu registrieren.	Nein
Microsoft Graph bearbeiten	Erlaubt einem Administrator die Bearbeitung von Microsoft Graph API-Einstellungen zum Schutz von Office 365 Apps.	Nein
Rolle für Microsoft Graph anzeigen	Erlaubt es einem Administrator, die für den Schutz von Office 365 Apps verwendeten Microsoft Graph API-Einstellungen anzuzeigen.	Nein
Befehl zur Komplettlöschung senden/abbrechen	Erlaubt es einem Administrator, einen Befehl zur Komplettlöschung an ein Gerät zu senden oder einen erteilten Befehl zur Komplettlöschung abzubrechen, bevor er ausgeführt wird.	Nein
Zugriffsintegration verwalten	Ermöglicht es einem Administrator, die Zugriffsintegration zu verwalten.	Nein

Weitere Informationen finden Sie unter **Rollen zuweisen**

6.7.4. Benutzer suchen und filtern

Dieser Abschnitt enthält die folgenden Themen:

Suchen nach einem Benutzer

Wenn Sie viele Benutzer hinzugefügt haben, kann es hilfreich sein, Filter oder Suchvorgänge zu nutzen, um einen Benutzereintrag schnell zu lokalisieren.

Verfahren

1. Gehen Sie zu **Benutzer**.
2. Geben Sie Zeichen in das Suchfeld ein.

Verwenden der erweiterten Suche für Benutzer

Mit der Option „Erweiterte Suche“ können Sie anhand von Regeln nach Benutzern suchen, um die Benutzer nach bestimmten Kriterien zu identifizieren und anzuzeigen. Die Regeln können miteinander mit den Optionen ANY (OR) oder ALL (AND) verschachtelt werden. Die mit den Regeln übereinstimmenden Benutzer werden unterhalb des Abschnitts angezeigt. Die Regeln können unter Verwendung folgender Operatoren konstruiert werden:

- beginnt mit
- endet mit
- enthält
- enthält nicht
- beginnt nicht mit
- endet nicht mit
- ist kleiner als
- ist größer als
- liegt innerhalb des Bereichs
- Ist gleich
- ist nicht gleich

Ab Neurons for MDM 127 zeigt das Ivanti Neurons for MDM-Administrationsportal die Anzahl doppelter Benutzergruppen und die zugehörige Anzahl der GUIDs an. Damit lassen sich doppelte Gruppen identifizieren, wenn das Attribut "Name der Benutzergruppe" im Regeleditor ausgewählt wird. Eine Tabelle unter dieser Regel zeigt außerdem die Liste der doppelten Benutzergruppen zusammen mit Details wie Name der Benutzergruppe, GUID, Quelle und Distinguished Name (DN).

Verfahren

1. Klicken Sie auf der Seite „Benutzer“ auf den Link **Erweiterte Suche**.
2. Klicken Sie auf **Beliebig**, wenn die Benutzer mindestens eine der Regeln erfüllen müssen, oder auf **Alle**, wenn die Benutzer alle Regeln erfüllen müssen.
3. Erstellen Sie eine Regel für die Suchkriterien, z. B. Benutzergruppe, benutzerdefiniertes Benutzerattribut und benutzerdefiniertes LDAP-Attribut.
4. (Optional): Klicken Sie auf +, um weitere Richtlinien zu erstellen.

5. (Optional) Klicken Sie auf **Speichern**, um die Abfrage zu speichern.
6. Klicken Sie auf **Suchen**. Die Liste der Benutzer, die die Suchkriterien erfüllen, wird auf der Seite angezeigt.

Laden der Suchabfragen für Benutzer

Verfahren

1. Klicken Sie auf der Seite „Benutzer“ auf den Link **Erweiterte Suche**.
2. Klicken Sie auf das Symbol „Ordner“. Das Fenster **Erweiterte Suche** wird angezeigt. Die Liste der erstellten Suchanfragen wird im Abschnitt **Abfrage laden** angezeigt. Folgende Details werden in diesem Abschnitt angezeigt:
   - **Abfragename** - Der Name der geladenen Abfrage.
   - **Abfrageinhalt** - Zeigt den Inhalt der Regeln an, die die Suchabfrage definieren.
   - **Aktionen** - Wählen Sie die Aktion aus, die mit der Abfrage ausgeführt werden soll.
3. Klicken Sie in der Spalte **Aktionen** auf **Abfrage laden**, um die Liste der Benutzer anzuzeigen, die die in der geladenen Abfrage definierten Kriterien erfüllen.
   Um eine geladene Abfrage zu löschen, klicken Sie auf das Löschsymbol.

Filtern von Benutzern

In der seitlichen Navigationsleiste "Filter" sind verschiedene Abschnitte aufgelistet, die Ihnen die Suche nach einem bestimmten Benutzer erleichtern. Der Assistent "Filter verwalten" enthält eine Liste aller Abschnitte, die Sie in der Filter-Navigationsleiste anzeigen können.

Verfahren

1. Gehen Sie zu **Benutzer**.
2. Markieren Sie die entsprechenden Kontrollkästchen in den Abschnitten, die im Assistenten "Filter verwalten" aufgeführt sind. Sie können über folgende Abschnitte suchen:
   - Support-Administratoren
   - Google Status
   - Einladungsstatus
     - Abgeschlossen (Der Benutzer hat die Einladung erhalten und beantwortet.)
     - Abgelaufen (Der Benutzer hat nicht rechtzeitig geantwortet.)
     - Nicht eingeladen (Sie haben diesen Benutzer nicht eingeladen.)
     - Ausstehend (ausstehende Benutzerantwort.)

   Passwortablauf

     - Läuft ab (Benutzer mit Passwortablaufoption sind auf Enddatum festgelegt.)
     - Niemals (Benutzer, bei denen das Passwort auf „Läuft nie ab“ eingestellt ist.)
   - Benutzergruppe (Wählen Sie die für Sie relevante Benutzergruppe aus.)
   - Benutzerquelle
     - LDAP,
     - Entra ID
     - Dienstplan

        - Salesforce
        - Lokal
    - Synchronisieren
        - Direkte Synchronisierung – Führt die Benutzer auf, die direkt über den LDAP-Server synchronisiert wurden.
        - Keine Synchronisierung – Führt die Benutzer auf, die vom LDAP-Server entfernt wurden.
        - Indirekte Synchronisierung – Führt die Benutzer auf, die indirekt über den LDAP-Server synchronisiert wurden.
        - Nicht zutreffend
3. (Optional) Klicken Sie auf **Standardeinstellungen wiederherstellen**, um die Auswahl auf die Standardfilter zurückzusetzen. In der Filter-Navigationsleiste werden die ausgewählten Abschnitte angezeigt. Wenn Sie alle Kontrollkästchen im Assistenten "Filter verwalten" deaktivieren, werden in der seitlichen Filter-Navigationsleiste alle Abschnitte angezeigt.
4. Klicken Sie in einen Bereich außerhalb des Assistenten "Filter verwalten", um den Assistenten zu beenden.
5. Klicken Sie auf das X-Symbol, um die seitliche Filter-Navigationsleiste zu schließen. Durch Klicken auf **Filter** können Sie die seitliche Navigationsleiste erneut aufrufen.

6.7.5. Benutzer zu Benutzergruppen zuordnen

Dieser Abschnitt enthält die folgenden Themen:

- Benutzer über die Seite Benutzer zuweisen
- Benutzer über die Seite Benutzergruppen zuweisen

Die Zuordnung von Benutzern zu Benutzergruppen ist eine ideale Möglichkeit, den Zeitaufwand für Aufgaben zu reduzieren, die sich immer wiederholen, beispielsweise:

- Verteilen von Apps
- Zuweisen von Rollen

Benutzer über die Seite Benutzer zuweisen

1. Gehen Sie zu **Benutzer**.
2. Wählen Sie die Benutzer aus, die Sie bearbeiten möchten.
3. Klicken Sie auf **Aktionen**.
4. Wählen Sie **Der Gruppe zuweisen**.
5. Wählen Sie die Gruppen aus oder klicken Sie auf Neue erstellen, um eine neue Gruppe zu erstellen.
6. Klicken Sie auf **Speichern**.

Benutzer über die Seite Benutzergruppen zuweisen

1. Gehen Sie zu **Benutzer > Benutzergruppen**.
2. Wählen Sie die Benutzergruppen aus, die Sie bearbeiten möchten.
3. Klicken Sie (oben rechts) auf **Aktionen**.
4. Wählen Sie Benutzer zuordnen.
5. Geben Sie die E-Mail-Adresse jedes Benutzers ein.
6. Klicken Sie auf **Benutzer zuordnen**.

6.7.6. Benutzer einladen

Wenn Sie einen Benutzer hinzufügen, haben Sie die Möglichkeit, diesen Benutzer dazu einzuladen, Geräte anzumelden. Diese Option ist sogar standardmäßig ausgewählt. Die eingeladenen Benutzer erhalten eine E-Mail-Benachrichtigung mit den für die Anmeldung erforderlichen Daten. Sie können einen Benutzer auch über die Seite Benutzer > Benutzer einladen (bzw. erneut einladen).

Verfahren

1. Gehen Sie zu **Benutzer**.
2. Wählen Sie die Benutzer aus, die Sie einladen möchten.
3. Wählen Sie **Aktionen > Einladung senden** aus. Die Einladungsvorschau wird zusammen mit einer Option zur Definition des Eigentumsstatus des Geräts als **Eigentum des Benutzers oder Eigentum des Unternehmens** angezeigt.

4. Sie können auch die **Geräteeigentümer-Einstellungen** aktivieren.
5. Klicken Sie auf **Eigentum des Benutzers** oder **Eigentum des Unternehmens**. Diese Einstellung ändert die Klassifizierung des Geräts während des Registrierungsprozesses. Dies gilt nur für die Registrierungsarten "Nur PIN" oder "Passwort + PIN". Wenn die **Einstellungen für den Geräteeigentümer** deaktiviert sind, werden die Geräte als "nicht festgelegt" registriert. Bei überwachten Geräten lautet die Einstellung für den Geräteeigentümer "Firmeneigentum".
6. Klicken Sie auf **Senden**. Wenn eine PIN-basierte Registrierung durchgeführt wurde, erhält der Benutzer eine PIN an seine registrierte E-Mail-Adresse. Wurde eine QR-Code-basierte Registerierung festgelegt, erhält der Benutzer einen QR-Code.
7. Klicken Sie auf **OK**.

> Wenn die Funktion zur Registrierungsbestätigung per E-Mail aktiviert ist, wie unter **Registrierungsbestätigungs-E-Mails konfigurieren und verwenden** beschrieben, sehen Sie außerdem eine Erinnerung, dass der Benutzer nach erfolgreicher Registrierung eine Registrierungsbestätigungs-E-Mail erhält. Um die E-Mail zu erhalten, muss der Benutzer in der Verteilerliste stehen, die Sie in den **Bestätigungs-E-Mails zur Benutzerregistrierung konfigurieren** unter **Benutzereinstellungen** für die Benutzerregistrierung angeben.

Weitere Informationen finden Sie unter **LDAP-Benutzer importieren**.

6.7.7. Aktivieren und Deaktivieren von Benutzern

Dieser Abschnitt enthält die folgenden Themen:

- Lokale Benutzer aktivieren und deaktivieren
- LDAP-Benutzer aktivieren und deaktivieren

Die lokalen und LDAP-Benutzer können aktiviert oder deaktiviert sein. Je nach Status können Sie benutzerspezifische Richtlinien mit der Bedingung „Benutzer aktiviert“ erstellen und eine Aktion für die Bedingung im Regeleditor festlegen. Es kann beispielsweise eine kundenspezifische Richtlinien-Regel geben, die Geräte außer Dienst zu stellen, die deaktivierten lokalen bzw. LDAP-Benutzern gehören.

Lokale Benutzer aktivieren und deaktivieren

Standardmäßig ist ein lokaler Benutzer aktiviert, wenn er erstellt wird.

Verfahren

1. Gehen Sie zu **Benutzer**.
2. Klicken Sie auf den Anzeigenamen des Benutzers.
3. Klicken Sie auf **Bearbeiten**. Das Fenster **Authentifizierung erforderlich** wird angezeigt.
4. Geben Sie Ihr Administrator-Passwort ein und klicken Sie auf **Authentifizieren**.

> Bei mehrfacher Falscheingabe des Passworts und beim Überschreiten des in den 'Einstellungen für die Passwortkomplexität' festgelegten Schwellenwerts für fehlgeschlagene Anmeldungen wird das Konto gesperrt und Sie werden von der aktuellen Sitzung abgemeldet.

5. Aktivieren oder deaktivieren Sie die Option **Aktiviert**, um den lokalen Benutzer zu aktivieren bzw. zu deaktivieren.
6. Klicken Sie auf **Speichern**.

LDAP-Benutzer aktivieren und deaktivieren

Sie können LDAP-Benutzer nur für Microsoft Active Directory aktivieren oder deaktivieren. Wenn Sie in Microsoft Active Directory die Eigenschaften für ein Benutzerkonto öffnen, auf die Registerkarte **Konto** klicken und die Kontrollkästchen des Dialogsfelds **Konto**-Optionen aktivieren oder deaktivieren, werden dem Attribut **UserAccountControl** Zahlenwerte zugeordnet. An dem dem Attribut zugeordneten Wert erkennt Windows, welche Optionen aktiviert wurden. Wenn Sie dem Attribut UserAccountControl einen Wert zugeordnet haben, wird der Benutzerstatus nach der LDAP-Synchronisation mit der Cloud geändert.

Folgende Werte können Sie zuordnen:

- 512 - Aktiviert.
- 514 - Deaktiviert.
- 66048 - Aktiviert, Passwort läuft nie ab.
- 66050 - Deaktiviert, Passwort läuft nie ab.

Anzeigen von Benutzerkonten

Verfahren

1.	Klicken Sie auf **Start**.

2.	Wechslen Sie zu **Programme**.

3. Wechseln Sie zu **Verwaltung**.

4.	Klicken Sie auf **Active Directory-Benutzer und -Computer**.

Weitere Informationen finden Sie unter **https://support.microsoft.com/en-in/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-pro**.

Sie können die Attribute anzeigen und bearbeiten, indem Sie entweder das Tool "Ldp.exe" oder das Snap-in "Adsiedit.msc" verwenden. Mit diesen Tools sollten nur erfahrene Administratoren Active Directory bearbeiten. Beide Tools sind verfügbar, wenn Sie die Support-Tools des Original-Windows-Installationsdatenträgers installiert haben.

6.7.8. Mehrere Administrator-Anmeldungen verwalten

Da mehrere Sitzungen des Ivanti Neurons for MDM-Administratorportals unterstützt werden, kann der Administrator mehrere Seiten des Portals gleichzeitig anzeigen. Wenn Sie Administrator sind, können Sie Ihre letzten Anmeldedaten anzeigen, damit Sie bei mehreren Anmeldungen nicht die Übersicht verlieren.

Letzte Administratoranmeldung anzeigen

Verfahren

1. Klicken Sie auf das **Konto**.
2. Rufen Sie den Eintrag **Letzte Anmeldung:** auf.

6.7.9. Passwort ändern

Dieser Abschnitt enthält die folgenden Themen:

- Passwort auf der Registerkarte Benutzer ändern
- Einstellung anwenden, dass das Passwort nie abläuft
- Einstellung entfernen, dass das Passwort nie abläuft

> Wenn ein Benutzer eine Systemverwaltungsrolle hat, wird die Option **Passwort ändern** nur für einen Superuser oder den derzeit angemeldeten Benutzer angezeigt.

Sie können Ihr Ivanti Neurons for MDM-Kennwort ändern. Wenn Sie die entsprechende Berechtigung haben, können Sie auch das Passwort eines anderen Benutzers ändern.

Verfahren

1. Klicken Sie auf das Symbol für Ihr Konto (oben rechts).
2. 
   Wählen Sie in dem Pull-down-Menü die Option **Passwort ändern**.
3. Geben Sie Ihr aktuelles Passwort ein.
4. Geben Sie Ihr neues Passwort ein.
5. Geben Sie Ihr neues Passwort noch einmal ein.
6. Damit das Passwort nicht abläuft, wählen Sie die Option **Nie ablaufendes Passwort einstellen**.

> Wenn Sie das Passwort so einstellen, dass es nie abläuft, überschreibt diese Einstellung die unter „Benutzer > Benutzereinstellungen > Einstellung der Passwortkomplexität“ definierte **Passwort-Ablaufdauer**.

7. Klicken Sie auf **Fertig**.

> Deaktivieren Sie die Option **Passwort läuft nie ab**, um das Ablaufdatum des Passworts für das lokale Konto zurückzusetzen. Nachdem Abwahl dieser Option zeigt ein Pop-up-Fenster das vorherige Ablaufdatum des Passworts, das für den Benutzer verwendet wurde.

Passwort auf der Registerkarte Benutzer ändern

Verfahren

1. Gehen Sie zu **Benutzer**.
2. Klicken Sie auf den Anzeigenamen des Benutzers.
3. Klicken Sie auf **[Edit]** (oben links). Das Fenster **Authentifizierung erforderlich** wird geöffnet. Administratoren (die entweder lokale Benutzer oder LDAP-Benutzer sind) müssen sich vor der Bearbeitung des Benutzers durch Eingabe des Administrator-Passworts authentifizieren.
4. Geben Sie Ihr Administrator-Passwort ein und klicken Sie auf **Authentifizieren**.

> Bei mehrfacher Falscheingabe des Passworts und beim Überschreiten des in den 'Einstellungen für die Passwortkomplexität' festgelegten Schwellenwerts für fehlgeschlagene Anmeldungen wird das Konto gesperrt und Sie werden von der aktuellen Sitzung abgemeldet.

5. Geben Sie das neue Passwort in das Feld **Aktuelles Passwort** ein.

> Dieses Feld wird nicht angezeigt, wenn Sie das Passwort für einen anderen Benutzer ändern.

6. Geben Sie das neue Passwort in das Feld Passwort ändern ein.
7. Bestätigen Sie das neue Passwort.
8. Klicken Sie auf **Speichern** (oben links).

Einstellung anwenden, dass das Passwort nie abläuft

1. Gehen Sie zu **Benutzer**.
2. Wählen Sie mindestens einen Benutzer aus.
3. Klicken Sie auf **Aktionen**.
4. Wählen Sie **Ewiges Passwort zuweisen**. Das Fenster **Nie ablaufendes Passwort für das lokale Konto einstellen** wird angezeigt.
5. Klicken Sie auf [**Submit**].

Einstellung entfernen, dass das Passwort nie abläuft

1. Gehen Sie zu **Benutzer**.
2. Wählen Sie mindestens einen Benutzer aus.
3. Klicken Sie auf **Aktionen**.
4. Wählen Sie **Ewiges Passwort entfernen**. Das Fenster **Ewiges Passwort für das lokale Konto entfernen** wird angezeigt.
5. Klicken Sie auf [**Submit**]. Sobald diese Einstellung entfernt ist, wird das Ablaufdatum des letzten Passworts für den Benutzer verwendet.

6.7.10. Nachricht senden

Dieser Abschnitt enthält die folgenden Themen:

- Nachricht an Benutzer senden
- Nachricht an Geräte senden

Sie können eine Nachricht an einen beliebigen bekannten Benutzer senden. Die Nachrichten können per E-Mail oder als Push-Benachrichtigunegn übermittelt werden. Nur Benutzer mit angemeldeten Geräten können Push-Nachrichten erhalten.

Voraussetzungen

- Stellen Sie bei iOS-Geräten sicher, dass der Go-Client installiert ist.
- Stellen Sie bei macOS-Geräten sicher, dass der Mobile@Work-Client installiert ist.

Nachricht an Benutzer senden

1. Gehen Sie zu **Benutzer > Benutzer**.
2. Wählen Sie die Benutzer aus, an die Sie eine Nachricht senden möchten.
3. Klicken Sie (oben rechts) auf **Aktionen**.
4. Klicken Sie auf **Nachricht senden**.
5. Wenn Sie keine E-Mail versenden möchten, deaktivieren Sie das Kontrollkästchen Eine E-Mail senden.
6. Wenn Sie eine E-Mail senden möchten, geben Sie einen Betreff und einen Nachrichtentext ein.
7. Wenn Sie eine Push-Benachrichtigung senden möchten, aktivieren Sie das Kontrollkästchen Eine Push-Nachricht senden und geben Sie einen Nachrichtentext ein.
8. Klicken Sie auf **Senden**.

Nachricht an Geräte senden

1. Gehen Sie zu **Geräte > Geräte**.
2. Wählen Sie die Geräte aus, an die Sie eine Nachricht senden möchten.
3. Klicken Sie (oben rechts) auf **Aktionen**.
4. Klicken Sie auf **Nachricht senden**.
5. Sie können auch auf den Link mit dem Gerätenamen klicken, um die Seite mit den Gerätedetails anzuzeigen und anschließend auf das Symbol **Nachricht senden** .
6. Wenn Sie keine E-Mail versenden möchten, deaktivieren Sie das Kontrollkästchen Eine E-Mail senden.
7. Wenn Sie eine E-Mail senden möchten, geben Sie einen Betreff und einen Nachrichtentext ein.
8. Wenn Sie eine Push-Benachrichtigung senden möchten, aktivieren Sie das Kontrollkästchen Eine Push-Nachricht senden und geben Sie einen Nachrichtentext ein.

> Eine Push-Benachrichtigung kann auch URLs enthalten, auf die Benutzer zugreifen können.

9. Klicken Sie auf **Senden**.
   Wenn eine Push-Benachrichtigung an einen Benutzer gesendet wird, sieht der Benutzer ein Glöckchensymbol in der Toolbar des

Gerätebildschirms. Wenn er auf das Glöckchensymbol tippt, kann der Benutzer die bisher empfangenen Benachrichtigungen anzeigen, eine Aktion ausführen oder die Benachrichtigung löschen.

Verfügbar sowohl auf den Seiten **Geräte** als auch **Benutzer** können Administratoren bestimmte Geräte- oder Benutzerattribute in Nachrichten einfügen, die anschließend zur Zustellung an Endbenutzer in die Warteschlange gestellt werden.

6.7.11. Benutzer aus Benutzergruppen entfernen

Dieser Abschnitt enthält die folgenden Themen:

- Benutzer über die Seite Benutzer entfernen
- Benutzer über die Seite Benutzergruppen entfernen

Die Entfernung eines Benutzers aus einer Benutzergruppe bedeutet:

- User_Roles.htmSämtliche, dieser Gruppe zugewiesenen Rollen werden dem Benutzer entzogen.
- Apps, die der Gruppe zugeordnet wurden, sind im App-Katalog des Benutzers nicht mehr verfügbar.
- Apps, die als entfernbar konfiguriert wurden, werden von den Geräten des Benutzers entfernt.

Benutzer über die Seite Benutzer entfernen

1. Wählen Sie den Benutzer aus, den Sie bearbeiten möchten.
2. Klicken Sie (oben rechts) auf **Aktionen**.
3. Wählen Sie **Aus Gruppe entfernen**.
4. Wählen Sie die Gruppen aus.
5. Klicken Sie auf **Entfernen**.

Benutzer über die Seite Benutzergruppen entfernen

1. Klicken Sie auf die Benutzergruppe, um deren Details anzuzeigen.
2. Klicken Sie (oben rechts) auf **Bearbeiten**.
3. Klicken Sie auf den Link Entfernen neben dem Benutzer, den Sie entfernen möchten.
4. Klicken Sie (oben rechts) auf **Speichern**.

6.7.12. Benutzer löschen

Dieser Abschnitt enthält die folgenden Themen:

- Was passiert, wenn Sie einen lokalen Benutzer löschen
- Was ist mit LDAP-Benutzern?

Verfahren

1. Gehen Sie zu Benutzer > Benutzer.
2. Wählen Sie den entsprechenden Eintrag des Benutzers aus.
3. Klicken Sie (oben rechts) auf **Aktionen**.
4. Wählen Sie Löschen.

Wenn ein Ivanti Neurons for MDM-Administrator oder ein Partner-Administrator versucht, einen Partner-Administrator zu löschen, gibt Ivanti Neurons for MDM eine Meldung aus, die darauf hinweist, dass ein Partner-Administrator diesen Vorgang über das Dienstanbieterportal durchführen muss.

> Wenn bei einem Benutzer Geräte mit dem Konto verknüpft sind, müssen Sie zuerst die Geräte stilllegen und löschen und dann den Benutzer löschen. Wenn der Benutzer keine Geräte besitzt, können die Benutzerinformationen beim Löschen des Benutzers gelöscht werden.

Was passiert, wenn Sie einen lokalen Benutzer löschen

- Alle Informationen zu einem gelöschten Benutzer werden aus dem System gelöscht.
- Dem Benutzer zugeordnete Geräte werden ausgesondert.
- Von dem Benutzer hochgeladener Content bleibt erhalten.
- Für das Benutzerkonto sind keine weiteren Geräteregistrierungen möglich.

Was ist mit LDAP-Benutzern?

- Wenn der LDAP-Server deaktiviert wurde, kann ein LDAP-Benutzer nicht permanent gelöscht werden. Bei der nächsten Synchronisation der LDAP-Daten wird ein gelöschter LDAP-Benutzer wiederhergestellt.
- Wenn der LDAP-Server bzw. die Gruppe gelöscht wurde, wird aus dem LDAP-Benutzer ein lokaler Benutzer, der gelöscht werden kann.
- Wird ein Benutzer aus LDAP gelöscht, wird er dadurch nicht aus der Cloud gelöscht. Der Synchronisierungsstatus wechselt zwar in "NO_SYNC", aber der Benutzer wird nicht entfernt.

6.7.13. Exportieren der Benutzer

Als Administrator können Sie eine Liste mit Benutzern aus Ivanti Neurons for MDM exportieren.

> Wenn die Geräteregistrierungs-PIN des Benutzers in eine CSV-Datei exportiert wird, wird diese aus Sicherheitsgründen mit '' maskiert.

Verfahren

1. Gehen Sie zu **Benutzer > Benutzer**.
2. Wählen Sie einen oder mehrere Benutzer aus der Liste aus.
3. Klicken Sie auf **Als CSV-Datei exportieren**.

Sie erhalten eine Meldung, die darauf hinweist, dass der Export etwas Zeit in Anspruch nimmt. Nach dem Einreichen des Requests müssen Sie warten, bis dieser abgeschlossen ist, bevor sie einen weiteren Request senden können. Sobald der Bericht bereitsteht, werden Sie aufgefordert, den Bericht herunterzuladen oder zu löschen. Der Administrator erhält außerdem eine E-Mail mit einem Link zum Herunterladen des Berichts.

> Die Details der Attribute **Benutzerdefinierter Benutzer** und **LDAP** können ebenfalls zusammen mit weiteren Details in eine CSV-Datei exportiert werden.

> Wird ein Benutzer mit einem Feldwert hinzugefügt, der das Zeichen +, -, = oder @ enthält, wird den Benutzerdaten in der exportierten CSV-Datei automatisch ein einfaches Anführungszeichen als Präfix (') vorangestellt und dem Längsstrich (|) wird ein Backslash (\) angehängt. Dadurch soll die Anfälligkeit für Injektionen in Excel verhindert werden.

6.7.14. Angepasste Attribute Benutzern zuweisen

Sie können angepasste Attribute, beispielsweise das Attribut „Abteilung“, einem oder mehreren Kunden zuweisen. Jedes Attribut hat einen entsprechenden Wert, den Sie für Aufgaben wie die Erstellung von Konfigurationen und Benutzergruppen verwenden können. Sie können benutzerdefinierte Attribute einem oder mehreren Benutzern zuweisen.

Verfahren

1. Wechseln Sie zu **Admin > System >Attribute** und erstellen Sie ggf. neue benutzerdefinierte Attribute.
2. Gehen Sie zu **Benutzer**.
3. Wählen Sie mindestens einen Benutzer aus.
4. Klicken Sie auf **Aktionen**.
5. Wählen Sie die Option **Benutzerdefinierte Attribute zuweisen**.
6. Wählen Sie eine der folgenden Optionen aus:
    - Zuweisung (Überschreiben) aller Attribute erzwingen, selbst wenn Werte vorhanden sind.
    - Nur überschreiben, wenn der Wert leer ist, Attribute mit vorhandenen Werten überspringen.

Wählen Sie die Attribute aus, die Sie zuweisen wollen, und geben Sie deren Werte ein (leere Werte sind nicht zulässig).

8. Klicken Sie auf **Zuweisen**.

Verwandte Themen:

- Attribute
- Variablen

6.7.15. Anpassbare Attribute für Benutzer entfernen

Sie können benutzerdefinierte Attribute von einem oder mehreren Benutzern entfernen.

> Handeln Sie mit Bedacht, da diese Aktion nicht rückgängig gemacht werden kann.

Verfahren

1. Gehen Sie zu **Benutzer**.
2. Wählen Sie mindestens einen Benutzer aus.
3. Klicken Sie auf **Aktionen**.
4. Wählen Sie die Option **Angepasste Attribute entfernen**.
5. Wählen Sie die Attribute aus, die Sie entfernen möchten.
6. Klicken Sie auf **Entfernen**.

Verwandte Themen:

- Attribute
- Variablen

6.7.16. Benutzer-Regionaleinstellung ändern

Standardmäßig entspricht das Gebietsschema des Benutzers dem des Mandanten. Bei Bedarf können Sie das Gebietsschema eines einzelnen Benutzers ändern.

Verfahren

1. Gehen Sie zu **Benutzer**.
2. Klicken Sie auf den Anzeigenamen des Benutzers.
3. Klicken Sie auf **Bearbeiten**. Das Fenster **Authentifizierung erforderlich** wird angezeigt.
4. Geben Sie Ihr Administrator-Passwort ein und klicken Sie auf **Authentifizieren**.

> Bei mehrfacher Falscheingabe des Passworts und beim Überschreiten des in den 'Einstellungen für die Passwortkomplexität' festgelegten Schwellenwerts für fehlgeschlagene Anmeldungen wird das Konto gesperrt und Sie werden von der aktuellen Sitzung abgemeldet.

5. Klicken Sie in dem Feld „Region“ auf **Wechseln**.
6. Wählen Sie im Fenster **Benutzergebietsschema ändern** das gewünschte Gebietsschema aus der Dropdownliste **Benutzergebietsschema ändern in:** aus.
7. Klicken Sie auf **Fertig**.
8. Klicken Sie auf **Speichern**.

6.7.17. Bearbeiten eines Benutzernamens

Wenn Sie einen Benutzer hinzufügen, wird der Text, den Sie für die E-Mail-Adresse eingeben, auch automatisch für den Benutzernamen aufgeführt. In den meisten Fällen sollten Sie den Standard-Benutzernamen nicht verändern, da:

- ein Benutzername im Format einer E-Mail-Adresse benötigt wird.
- Es ist zweckmäßig, die Benutzernamen-**Variable** in Konfigurationen zu verwenden, obwohl auch die E-Mail-Adresse verwendet werden kann.

Einen Benutzernamen müssen Sie nur dann in dem seltenen Fall bearbeiten, dass ein Konflikt mit einem bestehenden Benutzernamen existiert, da Benutzernamen im gesamten Gerätemanagementsystem eindeutig sein müssen. Ein Konflikt kann zum Beispiel auftreten, wenn sich zwei Abteilungen innerhalb einer Organisation für das Gerätemanagementsystem anmelden.

Auftreten eines Konflikts mit einem Benutzernamen

Wenn Sie aufgrund eines Konflikts mit einem Benutzernamen keinen Benutzer hinzufügen können, geben Sie einen neuen Benutzernamen im Format einer E-Mail-Adresse ein. Die E-Mail-Adresse muss nicht zu einem bestehenden E-Mail-Konto gehören. Sie können beispielsweise folgende E-Mail-Adresse ändern:

kschmidt@meinefirma.com

für

ksmith21@mycompany.com ändern

Wenn Sie einen Benutzernamen bearbeiten, werden alle Einstellungen, die den Benutzernamen als Variable umfassen, nicht für diesen Benutzer funktionieren. Erstellen Sie stattdessen Einstellungen, in denen die E-Mail-Adresse verwendet wird.

6.7.18. Opting-Out von der Sammlung von Standortdaten

Dieser Abschnitt enthält die folgenden Themen:

- Für iOS-Geräte
- Für Android-Geräte

Falls eine Datenschutzkonfiguration angewendet wird, die das Erfassen von Standortdaten erlaubt, kann der Gerätebenutzer diese Konfiguration überschreiben.

Für iOS-Geräte

iOS-Gerätebenutzer können Standortdienste deaktivieren, um das Senden von Standortdaten an das Gerätemanagementsystem zu verhindern. Dies erfolgt über folgende Einstellung:

Einstellungen > Datenschutz > Lokalisierungsdienste

Für Android-Geräte

Benutzer von Android-Geräten können den Standort ausschalten, um die Erfassung von Standortdaten zu verhindern. Wo sich diese Einstellung befindet, variiert je nach Hersteller. Benutzer von Android- Geräten werden auch dazu aufgefordert, die Anfrage für die Standortdaten zu akzeptieren.

6.7.19. Informationen zum Timeout

Das Inaktivitäts-Timeout des Administrationsportals liegt zwischen 5 und 60 Minuten, das Timeout erfolgt nach 24 Stunden.

Verfahren

1. Gehen Sie zu **Benutzer > Benutzereinstellungen**.
2. Bearbeiten Sie die Standardvorgabe für die **Passwortkomplexität**.
3. Stellen Sie im Abschnitt mit den Passwortrichtlinien mit dem Schieberegler **Inaktivitätszeitüberschreitung** die Zeit ein, die ein Benutzer vor einer Admin-Portal- oder einer Self-Service-Portalsitzung inaktiv sein darf. Der Wert variiert zwischen 5 und 60 (Minuten).
4. Klicken Sie auf **Fertig**.

6.7.20. Systemnutzungsanalyse deaktivieren

Es werden anonyme Produktdiagnose- und Nutzungsdaten gesammelt, um bei der Produktverbesserung zu helfen.

Wenn Sie Ihre Nutzungsdaten vertraulich handhaben möchten, können Sie das Versenden von Analysen zur Systemnutzung abwählen.

Verfahren

1. Klicken Sie auf den Link **Nutzungsdaten**, der sich im unteren Bereich der Seite im Ivanti Neurons for MDM-Administrationsportal befindet. Das Fenster **Nutzungsdaten** wird angezeigt.
2. Deaktivieren Sie das Kontrollkästchen **Diagnose- und Nutzungsdaten versenden**.
3. Klicken Sie auf **Speichern**.

6.7.21. Geräteregistrierung durch PIN-Generierung

Dieser Abschnitt enthält die folgenden Themen:

- Für einen oder mehrere Benutzer über die Benutzer-Landingpage
- Für einen einzelnen Benutzer über die Benutzerdetails

Sie können PINs für die Geräteregistrierung für Benutzer generieren, ohne eine Einladungs-E-Mail zu senden. Dadurch wird die Geräteregistrierung erheblich vereinfacht.

Für einen oder mehrere Benutzer über die Benutzer-Landingpage

1. Gehen Sie zu **Benutzer** > **Benutzer**.
2. Wählen Sie den oder die Benutzer aus, für den/die Sie eine Registrierungs-PIN generieren möchten. Sie können einen oder mehrere Benutzer auswählen.
3. Klicken Sie auf die Schaltfläche **Aktionen**.
4. Wählen Sie aus dem Dropdownmenü die Option **PIN generieren** aus.
5. Die generierten PINs werden in der Spalte **REGISTRIERUNGS-PIN** angezeigt.
6. Klicken Sie zum Anzeigen der PINs auf **PIN anzeigen**.

Für einen einzelnen Benutzer über die Benutzerdetails

1. Gehen Sie zu **Benutzer** > **Benutzer**.
2. Klicken Sie auf den Benutzernamen, für den Sie eine Registrierungs-PIN generieren möchten, um die Benutzerdetails aufzurufen.
3. Klicken Sie im Abschnitt "Benutzerinformationen" auf **PIN generieren**.
4. Klicken Sie auf **PIN anzeigen**, um die generierte PIN anzuzeigen.

> Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen zum Generieren von PINs für Benutzer verfügen. Die Option "PIN generieren" ist nur für Benutzer aktiviert, deren Geräteregistrierungsstatus "Kennwort & PIN" lautet.

7. Geräte

Dieser Abschnitt enthält die folgenden Themen:

- Erste Schritte mit der Geräten
- Gerätegruppen
- App-Inventar
- Verwalten von Geräten

7.1. Erste Schritte mit der Geräten

Dieser Abschnitt enthält die folgenden Themen:

- Geräte verwalten
- Durchführen von Aktionen auf einem Gerät
- Zeitzone für ein Gerät einstellen
- Geräte nach Kriterien auflisten
- Detaillierte Geräteinformationen anzeigen
- Geräten Benutzer und benutzerdefinierte Attribute im Massenverfahren zuweisen oder Benutzer und Attribute ändern
- Exportieren von Geräten in eine CSV-Datei
- Nach Geräteprotokollen suchen

Ivanti Neurons for MDMJeder Eintrag auf der Seite entspricht einem auf der Seite Geräte registrierten Mobilgerät und enthält wichtige Informationen über das Gerät. Die Seite „Geräteliste“ zeigt Geräte mit folgenden Informationen an:

- [Name]
- E-Mail-Adresse
- Telefonnr.
- Betriebssystem
- Gerätetyp
- [Status]
- Letzte Anmeldung
- Verstoßzähler
- Raum
- Rechtmäßiger Eigentümer (für gemeinsam genutzte iPads)

Die WLAN-IP-Adresse wird dem Ivanti Neurons for MDMServer gemeldet. Eine Änderung der IP-Adresse wird bei jeder Anmeldung gemeldet. Eine DSGVO-konforme IP-Adresse ist als Option auf der Gerätelistenseite und auf der Gerätedetailseite verfügbar. Für diese Funktion müssen die Geräte über Go 5.5 für iOS oder spätere Versionen und Go 72 oder spätere Versionen für Android registriert werden, soweit sie von der Cloud unterstützt werden.

> Da neue DSGVO-Felder (wie IP-Adresse und eSIM-ID) im Laufe der Ivanti Neurons for MDM Releases hinzugefügt werden, müssen Admins, welche die DSGVO bereits konfiguriert haben, das DSGVO-Profil bearbeiten, wenn sie die neuen Felder ausblenden wollen.

Die Gerätekennung (EID) wird als iOS-Attribut angezeigt, wenn eine Geräteliste im Tabellenkalkulationsformat (CSV) exportiert wird. Der EID und der mobilen EID (MEID) (wenn vorhanden) wird eine EID-Zeichenkette bzw. eine MEID-Zeichenkette vorangestellt.

> Der Ivanti Neurons for MDM Server kann dasselbe Gerät nicht mit unterschiedlichen Client-IDs und Registrierungen für verschiedene Mandanten verarbeiten. Der Server kann die Instanz nur verarbeiten, wenn das gleiche Gerät zwar unterschiedliche Client-Identifikatoren verwendet, diese aber für den gleichen Mandanten registriert sind.

Geräte verwalten

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Gehen Sie zu **Geräte**.
3. Wählen Sie mindestens ein Gerät aus.
4. Wählen Sie eine Aktion aus der Dropdownliste **Aktionen** aus.

In der folgenden Tabelle sind die auf der Seite „Geräte“ verfügbaren Aktionen aufgeführt:

Kategorie	Aktion
Allgemein	• Zu Gruppe hinzufügen • AppConnect entsperren > • Anpassbare Attribute zuweisen • **Benutzer zuweisen** • Compliance-Status des Geräts synchronisieren • Remotedesktop deaktivieren • Remotedesktop aktivieren • Bluetooth aktivieren/deaktivieren • **Check-in erzwingen** • **Sperren** • Anpassbare Attribute entfernen • Neustart/Herunterfahren • Compliance-Status des Geräts synchronisieren • **Gerät außer Dienst stellen** • **Mitteilung senden** • Eigentumsstatus definieren • **Entsperren** • **Wipe durchführen**
iOS-	• **Dem rechtmäßigen Eigentümer zuweisen** (nur gemeinsam genutzte iPads) • iOS System-Apps neu installieren • Zeitzone einstellen
macOS	• Automatisches Admin-Passwort für macOS einstellen • Firmware-Passwort einstellen/ändern • Wiederherstellungssperre einstellen/ändern
Android-	• Kiosk-Modus aufrufen • Kiosk-Modus beenden
Windows	Skripte und Aktionen über Ivanti Bridge

Durchführen von Aktionen auf einem Gerät

Über das Aktionsmenü (Schaltfläche mit den Auslassungszeichen) können Sie verschiedene Aktionen auf einem bestimmten Gerät durchführen.

Verfahren

1. Klicken Sie auf den Namen eines Geräts. Die Seite mit den Gerätedetails wird geöffnet.
2. Klicken Sie auf dieser Seite auf das Menü Aktionen (Ellipse), um eine der folgenden Geräteaktionen durchzuführen:

- Gerätename wechseln
- Gerät löschen
- Gruppenmitgliedschaft bearbeiten
- Bluetooth aktivieren/deaktivieren
- Skripte und Aktionen über Ivanti Bridge
- Ivanti Bridge-Protokoll abrufen
- **Auf Zuständigkeit verzichten**
- Debug-Protokolle anfordern
- Gerät neu starten/herunterfahren
- Gerät löschen
- Eigentumsstatus definieren
- Wiederherstellungssperre einstellen/ändern
- Wipe durchführen
- Compliance-Status des Geräts synchronisieren

Zeitzone für ein Gerät einstellen

Betrifft: Geräte mit iOS 14.0+ und tvOS 14.0+

Für diese Aktion sind keine Ortungsdienste erforderlich. Die Zeitzonen-Geräteaktion wird auch auf der Gerätedetailseite eines Geräts angezeigt. Änderungen der Zeitzone im Gerät werden ebenfalls auf dem Server Ivanti Neurons for MDM berücksichtigt.

> **iOS Restrictions.htm**Diese Geräteaktion löst einen Fehler aus, wenn die Einschränkung Datum & Uhrzeit automatisch erzwingen in der Konfiguration iOS-Einschränkungen aktiviert ist.

Verfahren

1. Wählen Sie mindestens ein Gerät aus.
2. Klicken Sie für die ausgewählten Geräte auf Aktionen > Zeitzone einstellen.
3. Geben Sie den String für die Zeitzone im Olson-Zeitzonen-ID-Format ein, z.B. Pacific/Midway. Zum Beispiel Pacific/Midway.
4. Klicken Sie auf Zeitzone einstellen.

Geräte nach Kriterien auflisten

Mithilfe der seitlichen Navigationsleiste "Filter" können Sie nur bestimmte Geräte aus der gesamten Geräteliste anzeigen. Verwenden Sie die Dropdownliste "Space", um alle oder nur bestimmte Spaces auszuwählen, für die Geräte und die zugehörigen Informationen angezeigt werden sollen. Sie können entweder über die Anzeigeversion oder die Bundle-Version suchen. Ab Cloud 76 werden auf der Seite „Geräte“ sowohl die Bundle-Version als auch die Anzeigeversion der Geräte angezeigt.

> Wenn Sie von der Seite „Gerätegruppen“ (durch Klicken auf den Hyperlink Anzahl der Geräte in der Spalte) oder von der Seite „App-Bestandsaufnahme“ (durch Klicken auf den Hyperlink Anzahl installierter Geräte in der Spalte) zur die Gerätelistenseite navigieren, wird eine Meldung mit dem Namen des Spaces angezeigt, für den die Geräte auf der Seite aufgelistet sind.

Detaillierte Geräteinformationen anzeigen

Klicken Sie in der Spalte „Name“ auf den Link eines Eintrags, um die Seite mit den Gerätedetails anzuzeigen. Die Seite mit den Gerätedetails enthält mehrere Registerkarten mit folgenden Informationen:

- **Übersicht** – Die folgende Tabelle führt die Details auf, die auf der Registerkarte "Übersicht" angezeigt werden:
- **Arbeiten mit Konfigurationen**Konfigurationen– Details der verwendetenKonfigurationenWeitere Informationen finden Sie unterArbeiten mit Konfigurationen.

Abschnittsname	Beschreibung
Allgemein	• Standort des Gerät • Hersteller • WLAN-MAC-Adresse • WLAN-IP-Adresse (Android-Geräte) • Netzwerkanbindung - (iOS-Geräte) • Enthält Akku – (nur für macOS 13.3+) • IP-Adresse • Öffentliche IP-Adresse – Zeigt die IP-Adresse des Geräts für Android oder ChromeOS an. Falls das Gerät eine Verbindung zu einem VPN- oder einen Proxyserver herstellt, wird die Proxy-WAN-IP-Adresse angezeigt. • Modellnummer – (macOS 13.3+ und iOS 16.4+) • Seriennummer • Alternative Seriennummer (Android-Geräte) – Herstellerspezifische Seriennummer für Samsung-Geräte im Geräteverwaltungs- oder Gerätebesitzermodus. • PIN sperren – Administratoren können ein verwaltetes Gerät per Remotezugriff sperren und eine eindeutige PIN generieren, um es manuell zu entsperren. Wählen Sie **Anzeigen** aus, damit die PIN für Benutzer mit Administratorrechten auf der Seite **Gerätedetails** angezeigt wird. Gilt nur für macOS-Geräte. • Speichernutzung – (außer bei Windows) verwendeter und verfügbarer interner Speicher auf Geräten • Verfügbare Batterieladung (Android) • Batteriestatus (Android) – Ladevorgang läuft, Entladevorgang läuft, Vollständig geladen und Ladevorgang inaktiv • Voraussichtliche Akkurestladung (Windows) • Geschätzte Akkulaufzeit (Windows) • Update verfügbar (macOS) • Verfügbarer Update-Name (macOS) • Betriebssystemversion • Betriebssystem Build-Version • Zusätzliche Buildversion • Zusätzliches BS/Version Extra • Apple Silicon Gerät • Firmwareversion • Gerätequelle • Rechtmäßiger Eigentümer • Mehrfach-Benutzer-Modus • Zeitzone

Abschnittsname	Beschreibung
	• Letzter bekannter Passcode zum Entsperren des Geräts • Sicherheitssperrmodus • System-Update (Android-Geräte) • Zebra Patch-Version (Android-Geräte) • Letzte Hotfix-ID - (bei Windows-Geräten) • Letzter Hotfix installiert am – (bei Windows-Geräten) • MDM-Registrierungstyp • MDM-Wiederinbetriebnahme (iOS 27.0+ und visionOS 27.0+)
Einstellungen	• Gerätename • Geräte-Identifikator • Gerät-GUID • Gerät für Device Enrollment (Apple-Geräte) • Device Enrollment registriert (Apple-Geräte) • Automatische Geräteregistrierung aktiviert • Automatische Geräteregistrierung eingereicht • Angemeldete Benutzerregistrierung (Apple-Geräte) • Registrierte verwaltete Apple-ID (Apple-Geräte) • Gerätegruppen • Sprache • MDM-Gerätekennungen • Geräte-Client-ID • App-Version des Clients • Client App-BundleID • Kunde registriert • EAS Gerät-IDs • Aktivierungssperre aktiviert • Deklarative Verwaltung durch Apple aktiviert • Apple DDM-App aktiviert • Aktivierungssperre sperren – Bypasscode • Nutzungsbedingungen • Verantwortung • iTunes-Konto aktiv • Geräte-Locator-Dienst aktiviert • Isoliert • Von Sentry blockiert

Abschnittsname	Beschreibung

	• Von Access blockiert
	• Von Compliance-Aktion blockiert
	• APNS-fähig
	• Überwachter Modus (iOS- und macOS-Geräte) - Identifiziert ein überwachtes Gerät. Gerät bleibt in direkter Kontrolle des IT-Teams. Der überwachte Modus ermöglicht zusätzliche Gerätefunktionen (z. B. Außendienst-Einsätze, Geräte für die Ladenkasse im Einzelhandel), „Leihgeräte“ im Gastgewerbe und im Dienstleistungssektor und Geräte, die im Klassenzimmerlabor von Schülern gemeinsam genutzt werden.
	• PIN löschen - Klicken Sie auf **Anzeigen**, um die PIN anzuzeigen.
	• Verwalteter macOS-Admin-Benutzer (macOS-Geräte)
	• Lokales macOS-Passwort des Administrators (macOS-Geräte) – Wählen Sie **Anzeigen** aus, um das **Passwort des Administrators**, **Letzte Kennwortrotation**, **Nächste Rotation** und **Grund** zu registrierten und verwalteten Geräten anzuzeigen, die die automatisierte Geräteregistrierung verwenden.
	Nachdem das Kennwort vom Administrator angezeigt wurde, kann es bis zu einer Stunde dauern (nächster Check-in), bis das Kennwort im Vergleich zum angezeigten Zeitpunkt der **nächsten Rotation** rotiert.
	• Geräteverschlüsselungsstatus – (macOS-Geräte)
	  ◦ FileVault-Verschlüsselung aktiviert
	  ◦ Persönlicher Wiederherstellungsschlüssel verwendet
	  ◦ Wiederherstellungsschlüssel für Institutionen verwendet
	• Bootstrap-Token verfügbar
	• Systemintegritätsschutz aktiviert
	• Firmware-Passwort
	  ◦ Passwort
	  ◦ Änderung ausstehend
	  ◦ Befehlsstatus
	  ◦ Options-ROMs zulassen
	• Wiederherstellungssperre
	  ◦ Passwort
	  ◦ Wiederherstellungssperre aktiviert
	• Skripte über Mobile@Work for macOS
	• Firewall-Einstellungen – (macOS-Geräte)
	  ◦ Firewall aktiviert
	  ◦ Alle eingehenden Verbindungen sperren
	  ◦ Stealth-Modus
	• Status der Anwendungs-Firewall – (macOS-Geräte)
	• Firewall-Status (Windows-Geräte)

Abschnittsname	Beschreibung
	• Letzte Datensicherung in der iCloud - (iOS-Geräte) • Nachfrist für die Passcodesperre – (iOS-Geräte) • Android-ID • Android Sicherheits-Patchlevel (für Android-Geräte) • Kiosk-Modus (Android-Geräte) • Android-SafetyNet-Attestierungstyp (Android-Geräte) • Geräte, die Android Enterprise unterstützen (Android-Geräte) • Geräte mit aktiviertem Android Enterprise (Android-Geräte) • Samsung-Geräte mit SAFE-Unterstützung (Android-Geräte) • In Android Enterprise verwaltete Geräte aktiviert (Geräteeigentümer) • Android-Arbeitsprofil auf unternehmenseigenen Geräten aktiviert • Nativer Anti-Phishing-Status • Anti-Phishing-Status • Anti-Phishing-VPN-Status • Verwaltetes Android-Gerät mit Arbeitsprofil • Sperre des Android-Arbeitsprofils auf unternehmenseigenen Geräten aktiviert • Help@Work verfügbar • Zebra-fähig • Secure Apps Status • Verschlüsselungsstatus für Secure Apps • Sichere Apps Verschlüsselungsmodus • FCM aktiviert • MTD-Aktivierungsstatus
Informationsschutz für Windows (Windows-Geräte)	• WIP • App-Sperre konfiguriert • Obligatorische EDP-Einstellungen
Telefonie	**Gerätedienst-Abonnements** • Telefonnummer • Mobilfunktechnologie • IMSI • ICCID • IMEI • IMEI 2 - (Nur auf Android-Geräten mit 2 SIM-Slots. Für Android 8.0 oder höher) • MEID • Standort des Gerät

Abschnittsname	Beschreibung
	• Mobilfunkanbieter • Eigener MCC-Code • Eigener MNC-Code • Aktueller Ländername • Heimatlandname • Mobilfunktechnologie • Roaming • Aktueller Betreiber • Aktueller MCC-Code • Aktueller MNC-Code • Daten-Roaming • Sprach-Roaming • EID – (gilt für unterstützte Android-Geräte) **SIM-Dienst-Abonnements** – (gilt für unterstützte iOS-Geräte) Bei unterstützten iOS-Geräten werden diese Eigenschaften für mehrere aktive eSIM-Dienstabonnements angezeigt. • Version der Mobilfunkanbieter-Einstellungen • Netzwerk der Mobilfunkanbieter-Einstellung • Aktueller MCC-Code • Aktueller MNC-Code • EID • ICCID • IMEI • Datenübertragung bevorzugt • Sprachübertragung bevorzugt • Bezeichnung • Label-ID • Telefonnummer • SIM-Slot • Roaming aktiv • Betreibernetzwerk des Abonnenten **SIM-Dienst-Abonnements** – (gilt für unterstützte Android-Geräte) Bei unterstützten Android-Geräten werden diese Eigenschaften für mehrere aktive Dienstabonnements angezeigt. • Version der Mobilfunkanbieter-Einstellungen • Aktueller MCC-Code • Aktueller MNC-Code

Abschnittsname	Beschreibung
	• ICCID • Datenübertragung bevorzugt • Sprachübertragung bevorzugt • Abonnement-ID • Telefonnummer • SIM-Slot • Ist eingebettet • Wird verwaltet
Compliance des Azure-Geräts	• ID des Azure-Geräts • Compliance-Status des Azure-Geräts • Azure Client-Status-Code • Zeit des Compliance-Berichts für das Azure-Gerät • Azure Intune-Gerätebenutzer UPN
Google BeyondCorp-Geräte-Compliance **Batterieinformationen**	• Geräte-Identifikator • Compliance-Status • Uhrzeit des Compliance-Berichts • Benutzer • Akkustand – Zeigt den aktuellen, vom Android-Betriebssystem gemeldeten Ladezustand der Batterie an. • Akkuzustand – Gemäß Meldung des Android-/Mac-/iOS- oder iPad-Geräts. • Batterieladezustand – gemäß Meldung vom Android-Betriebssystem • Prozentualer Batteriezustand (OEM-spezifisch) – Prozentualer Batteriezustand für unterstützte Gerätehersteller wie Zebra-Geräte • Batterieherstellungsdatum (OEM) – Herstellungsdatum der Batterie für unterstützte Gerätehersteller wie Zebra-Geräte • Batterieladezyklen (OEM) – Anzahl der insgesamt durchgeführten Zyklen für unterstützte Gerätehersteller wie Zebra-Geräte
Systemzustand von Gerätekomponenten (gilt für überwachte Geräte mit iOS 27.0+ und macOS 27.0+)	• **Basisband**: Gibt den Systemzustand des Basisbands des Geräts an. • **Kamera**: Gibt den Systemzustand der Kamera des Geräts an. • **Display**: Zeigt den Systemzustand des Gerätedisplays an. • **Face-ID**: Gibt den Systemzustand der Face-ID des Geräts an. • **Nahfeld**: Gibt den Systemzusatnd der Nahfeldkommunikation (NFC) des Geräts an. • **Touch-ID**: Gibt den Systemzustand der Touch-ID des Geräts an. • **Ultrabreitband**: Gibt den Systemzustand des Ultrabreitbands des Geräts an.

- **Installierte Apps** - Zeigt die Details zu den auf dem Gerät installierten Anwendungen an. Das Installationsdatum der aktuellen Version der installierten App wird in der Spalte **App-Datum** angezeigt. Durchsuchen Sie die installierten Apps wie folgt nach dem Gerät:
- App-Name
- Bundle-ID oder Paket-ID

> Das Installationsdatum der Apps aus der Quarantäne ist das Datum, an dem das Gerät aus der Quarantäne entfernt wird.

> Bei Android Enterprise-Geräten können Sie die Nutzungsdetails zu installierten Apps ebenfalls nach Tag, Woche, Monat oder Jahr sortiert anzeigen. Zum Anzeigen der Details muss die Option **Erfassung von App-Nutzungsdaten aktivieren** im Abschnitt **Konfigurations-Setup** aktiviert sein. Anschließend können Sie **App-Nutzung – Tag**, **App-Nutzung – Woche**, **App-Nutzung – Monat** oder **App-Nutzung – Jahr** auswählen, um die Details zur App-Nutzung anzuzeigen.

- **Verfügbare Apps** – Zeigt die Details zu den für das Gerät verfügbaren Anwendungen an. Durchsuchen Sie die verfügbaren Apps wie folgt nach dem Gerät:
- App-Name
- Bundle-ID oder Paket-ID

Wenn Sie in der Spalte **App-Konfigurationen** die Option **Name der Konfiguration** auswählen, werden Sie zur Registerkarte **App-Konfiguration** des App-Katalogs weitergeleitet, wo Sie die Optionen für die App-Konfiguration überprüfen können. Bei Bedarf können Sie die App-Konfigurationen für das Gerät auf der Seite **Übersicht über App-Konfigurationen** modifizieren. Weitere Informationen zum Konfigurieren einer App finden Sie unter **App-Konfiguration**.

Wenn Sie in der Spalte **App-Konfigurationen** die Option **Name der Konfiguration** auswählen, werden Sie zur Registerkarte **App-Konfiguration** des App-Katalogs weitergeleitet, wo Sie die Optionen für die App-Konfiguration überprüfen können. Bei Bedarf können Sie die App-Konfigurationen für das Gerät auf der Seite **Übersicht über App-Konfigurationen** modifizieren. Weitere Informationen zum Konfigurieren einer App finden Sie unter **App-Konfiguration**.

> Merken Sie sich Name und Typ der betreffenden App-Konfiguration für das zugewiesene Gerät auf der Seite **App-App-Konfigurationen**.

> Die Spalte **Status** gibt Aufschluss über den Installationsstatus der Anwendung auf dem Gerät. Der Installationsstatus wird nur für verwaltete Anwendungen erfasst. Der Installationsstatus für nicht verwaltete Anwendungen wird mit "Nicht installiert" angezeigt. Sie müssen die Anwendung in eine verwaltete Anwendung konvertieren, damit der korrekte Installationsstatus angezeigt wird.

- **AppConnect-Apps** – Details zu den installierten AppConnect-Apps.
- **Richtlinien** - Details zu den angewendeten Richtlinien. Prüfen Sie bei gefährdeten Geräten in der Spalte „Verstoß“ den Grund für den Verstoß. Wenn das Gerät durch Rooting gefährdet ist, zeigt das System den Grund in der Spalte **Verstoß** an:

Priorität (1 = höchste)	Verstoß
1	Gefährdetes Plugin
2	Client manipuliert
3	Unbekannter Gerätehersteller: unbekannt
4	Verdächtiger Ordner erkannt: [Pfad]
5	Verdächtige Binärdatei gefunden: [Pfad]
6	Ordner /data ist durchsuchbar ODER Ordner /data/data ist durchsuchbar
7	Gefunden /system/app/Superuser.apk
8	Paketmanager gefährdet
9	Verdächtige App gefunden: [Paket]

- **Zertifikate** - Details zu den installierten Zertifikaten.
  Zur Verwendung des Zertifikats prüfen Sie die Spalte „Nutzungsart“. Wenn das Zertifikat gerätespezifisch ist, wird als Nutzungsart „Gerät“ angezeigt. Wenn das Zertifikat benutzerspezifisch ist, wird als Nutzungsart „Benutzer“ angezeigt.
- Sentry - Informationen zu Sentry (ActiveSync-Zuordnungen)
- Attribute - Benutzerdefinierte Attribute und Geräteattribute
- **Benutzer** - Zeigt die Liste der aktiven Benutzer für das überwachte MacOS-Gerät an.

> Die verbesserte Registerkarte Benutzerzeigt die verwaltete Apple-ID als Hyperlink, der auf die Benutzerkontodetailseite auf dem gemeinsam genutzten iPad weiterleitet.

- **Protokolle** – Gerätefilter anzeigen und anpassen. Sie können folgende Aktionen über Filter durchführen:
  - Wählen Sie den Namen der Aktion aus, um Geräte basierend auf Anwendungsaktionen zu filtern.
  - Wählen Sie den Status aus.
  - Geben Sie Start- und Enddatum an.
- **Hardware** - Hardwarebestandsdetails (System, Motherboard, BIOS, Festplatte, CD-ROM, Prozessor und physischer Speicher)

Geräten Benutzer und benutzerdefinierte Attribute im Massenverfahren zuweisen oder Benutzer und Attribute ändern

Sie können mit dieser Funktion eine CSV-Datei hochladen und damit Benutzer bzw. kundenspezifische Attribute für viele Geräte gleichzeitig zuweisen und ändern.

Verfahren

1. Klicken Sie auf der Geräteseite auf das Symbol **Massenzuweisung durch Upload** (neben der Schaltfläche „Aktionen“).
2. (Optional) Klicken Sie auf **Vorlage herunterladen**, um eine CSV-Vorlagendatei zu speichern, die Sie dann bearbeiten und hochladen.

3. Sobald Sie die CSV-Datei erstellt haben, klicken Sie auf **Datei auswählen**, um den Speicherort der CSV-Datei zu suchen. Sie können auch die CSV-Datei per Drag&Drop in den Datenabschnitt „Datei“ ziehen.
4. Wählen Sie eine der folgenden Optionen aus:
    - **Zuweisung (Überschreiben) aller Attribute erzwingen, selbst wenn Werte vorhanden sind.**
    - **Nur überschreiben, wenn der Wert leer ist, Attribute mit vorhandenen Werten überspringen.**

Klicken Sie auf **Hochladen**.

Exportieren von Geräten in eine CSV-Datei

Sie können die Gerätedetails für ein bestimmtes Gerät über die Option **Als CSV-Datei exportieren** auf der Seite **Geräte** exportieren.

Verfahren

1. Gehen Sie zu **Geräte**.
2. Wählen Sie alle oder mehrere Spaces aus, um die Informationen in Bezug auf bestimmte Bereiche anzuzeigen.
3. Klicken Sie auf den Link zum Zählen der Geräte. Es wird die Seite "Geräteliste" angezeigt, die mit dem ausgewählten Space verknüpft ist.
4. Klicken Sie auf die Option **Als CSV-Datei exportieren**, um die Geräteliste und die verknüpften Details in eine CSV-Datei zu exportieren. Es wird eine Popup-Meldung angezeigt, aus der hervorgeht, dass die Verarbeitung des Exportberichts einige Zeit dauert wird. Warten Sie, bis die Anforderung abgeschlossen ist, bevor Sie eine andere Anforderung übermitteln. Sobald der Bericht bereitsteht, werden Sie mit einer Meldung aufgefordert, den Bericht herunterzuladen oder zu löschen.
5. Klicken Sie auf **Herunterladen**. Der Administrator erhält außerdem eine E-Mail mit einem Link zum Herunterladen des Berichts.
6. (Optional) Klicken Sie zum Löschen des Berichts auf **Löschen**.

Nach Geräteprotokollen suchen

Verfahren

1. Gehen Sie zu **Geräte** > **Geräte**, und klicken Sie auf den Spaltenlink **Name** für einen Eintrag.
2. Klicken Sie auf die Registerkarte **[Logs]**.
3. Benutzen Sie die Filter Aktion, Status, Startdatum und Enddatum, um die angezeigten Geräte einzugrenzen. Sie können folgende Aktionen über Filter durchführen:
    1. Wählen Sie den Namen der Aktion aus, um Geräte basierend auf Anwendungsaktionen zu filtern.
    2. Wählen Sie den Status aus.
    3. Geben Sie Start- und Enddatum an.
4. In der Spalte "Gerätedetails" wird der Status der Anwendung wie folgt angezeigt:
   Für alle Geräte zeigt der Status folgende Details an:
    - App-Name, App-Version, Bundle-ID oder Paket-ID
    - Status der Installation
    - Etwaige Fehler und Fehlerursachen
      Beispiel: - appOrConfigName=Name:<app name>;Identifier=<bundleid>;iTunesStoreId:<itunesid>;Status:<status or error reason from Apple>version: <app version>

Für Windows-Geräte zeigt der Status folgende Details an:

- Bundle-ID oder Paket-ID, Status und Fehler einschließen
  Beispiel:
- Für den Typ – Anwendungsinventar und Status – bestätigen – wird appType angezeigt.
- Für den Typ – Anwendungsinventar und Status – senden – wird nichts angezeigt.
- Für den Typ – installieren/deinstallieren und Status – erfolgreich/fehlgeschlagen/senden – wird "Bundle- ID oder Paket-ID, Status, Name, Version und Fehler einschließen" angezeigt.

Wenn Sie die Seite **Geräte** nicht sehen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie brauchen eine der folgenden **Rollen**:

- Geräteverwaltung
- Geräts schreibgeschützt

7.2. Gerätegruppen

Dieser Abschnitt enthält die folgenden Themen:

- Gerätegruppe hinzufügen
- Gerätegruppe entfernen
- Exportieren von Geräten in eine CSV-Datei
- Benutzerdefinierte Attribute zu Gerätegruppen zuweisen

Auf der Seite **Gerätegruppen** können Sie Listen der Geräte erstellen, die in gleicher Weise behandelt werden sollen. Sie können Richtlinien und Konfigurationen für die Gerätegruppen definieren und diesen zuweisen. Im Folgenden werden die von Ivanti Neurons for MDM erstellten Standardgerätegruppen dargestellt:

- Alle Geräte
- Android-Geräte
- Android-Enterprise-Geräte
- iOS-Geräte
- Gerätetyp (Apple)
- tvOS-Geräte
- macOS-Geräte
- visionOS-Geräte
- watchOS-Geräte
- Windows-Geräte

Die Details der Apps, die einer bestimmten Gerätegruppe zugeordnet sind, werden in der Registerkarte **Apps** für die spezifische Gerätegruppe angezeigt.

Gerätegruppe hinzufügen

> Das Hinzufügen einer Gerätegruppe ist für dynamische Benutzergruppen nicht relevant.

Je nachdem, welche Art von Lizenz Sie besitzen, können Sie eine neue Gerätegruppe basierend auf Regeln hinzufügen, sodass nur Geräte mit bestimmten Kriterien berücksichtigt werden. Die mit den Regeln übereinstimmenden Geräte werden unterhalb des Regeleditor-Abschnitts angezeigt. Die Regeln können miteinander mit den Optionen ANY (OR) oder ALL (AND) verschachtelt werden. Die Regeln können unter Verwendung folgender Operatoren konstruiert werden:

- beginnt mit
- endet mit
- enthält
- enthält nicht
- beginnt nicht mit
- endet nicht mit
- ist kleiner als

- ist größer als
- liegt innerhalb des Bereichs
- Ist gleich
- ist nicht gleich
- ist nicht leer
- ist leer

Der Ivanti Neurons for MDM-Administrator zeigt eine Anzahl doppelter Benutzergruppen und die zugehörige Anzahl der GUIDs an, damit doppelte Gruppen identifiziert werden können, wenn das Attribut "Name der Benutzergruppe" im Regeleditor ausgewählt wird. Eine Tabelle unter dieser Regel zeigt außerdem die Liste der doppelten Benutzergruppen zusammen mit Details wie Name der Benutzergruppe, GUID, Quelle und Distinguished Name (DN).

Bronze-Lizenz:

Regeln können Geräte anhand der folgenden Kriterien identifizieren:

- Gerätetyp
- Nach Betriebssystem (wird automatisch eingetragen)
- Betriebssystemversion
- Betriebssystem mit Version
- Benutzergruppe

Silver-Lizenz:

Regeln können Geräte anhand der folgenden Kriterien identifizieren:

- Bei Entra ID registriert
- Alternative Seriennummer (nur für Android - für Samsung-Geräte im Geräteverwaltungs- oder Gerätebesitzermodus)
- Dediziertes Android-Gerät
- Für Android Enterprise geeignet
- Verwaltetes Android-Gerät mit Arbeitsprofil
- Android-SafetyNet-Attestierungstyp
- Android Enterprise aktiviert
- Android Sicherheits-Patchlevel (für Android-Geräte)
- In Android Enterprise verwaltete Geräte aktiviert (Geräteeigentümer)
- Android Enterprise aktiviert
- Android-Arbeitsprofil auf unternehmenseigenen Geräten aktiviert
- Nativer Anti-Phishing-Status
- Anti-Phishing-Status
- Anti-Phishing-VPN-Status
- APNS-fähig
- Apple Silicon Gerät
- Automatische Geräteregistrierung aktiviert

- Automatische Geräteregistrierung eingereicht
- ID des Azure-Geräts
- Compliance-Status des Azure-Geräts
- Azure Client-Status-Code
- Zeit des Compliance-Berichts für das Azure-Gerät
- Baseband-Systemzustand
- BitLocker-Verschlüsselung
- Von Sentry blockiert
- Von Access blockiert
- Bootstrap-Token verfügbar
- Massenbereitstellungstyp (Apple Configurator oder Keine)
- Mobilfunkanbieter
- Kamera-Systemzustand
- Letzter Check-in durch Client
- Client registriert
- Compliance
- Von Compliance-Aktion blockiert
- Aktueller Ländername (wählen Sie den aktuellen Ländernamen aus der Auswahlliste)
- Aktueller MCC-Code
- Aktueller MNC-Code
- Kundenspezifisches Geräteattribut
- Benutzerdefiniertes LDAP-Attribut
- Kundenspezifisches Benutzerattribut
- Daten-Roaming
- Gerätename
- Gerät registriert
- Gerätequelle
- Gerätetyp
- Anzeigename
- Display-Systemzustand
- Verschlüsselung aktiviert
- Face-ID-Systemzustand
- Festplattenpartitionen
- Name des Heimatlandes (wählen Sie den Namen des Heimatlandes aus der Auswahlliste)
- Eigener MCC-Code
- Eigener MNC-Code
- IMEI

- IMEI2 (nur auf Android-Geräten mit dualem SIM-Port und ab Version 8.0)
- Institutioneller Wiederherstellungsschlüssel aktiviert
- IP-Adresse
- Kiosk-Modus
- Letzte Anmeldung
- Nur MAM
- Hersteller
- MDM-Registrierungstyp
- MDM-Wiederinbetriebnahme (iOS 27.0+ und visionOS 27.0+)
- Mehrbenutzer-Modus (iOS 27.0+)
- MTD-Aktivierungsstatus
- NFC-Systemzustand
- Betriebssystem
- Betriebssystem-Build-Version
- Betriebssystemedition
- Betriebssystemversion
- Betriebssystem mit Version
- Verantwortung
- Telefonnr.
- Öffentliche IP-Adresse (Android- oder ChromeOS-Geräte)
- Persönlicher Wiederherstellungsschlüssel aktiviert
- Isoliert
- Wiederherstellungssperre aktiviert
- Roaming
- Secure Apps Status
- Sicherheitssperrmodus
- Seriennummer
- [Status]
- Überwacht
- Systemversion
- Gesamte Gerätekapazität
- Gesamtspeicher in MB
- TPM-Version
- Touch-ID-Systemzustand
- Freischalt-Token verfügbar (iOS)
- Benutzerregistrierung aktiviert
- Benutzergruppe

- Ultrabreitband-Systemzustand
- Sprach-Roaming
- Persönlicher Wiederherstellungsschlüssel für macOS hinterlegt
- macOS Wiederherstellungsschlüsseltyp

Verfahren

1. Klicken Sie auf **[Add]**.
2. Geben Sie einen Namen für die Gruppe ein.
3. Geben Sie eine optionale Beschreibung für die Gruppe ein.
4. Wählen Sie die Art der Gerätegruppe, die Sie erstellen möchten:
    - **Dynamisch verwaltet**: Definieren Sie mit Regeln, welche Geräte in der Gruppe vorhanden sind.
        - **Aus erweiterter Suche laden**: Wählen Sie diese Option aus, um eine Bibliothek Ihrer gespeicherten Suchen zu öffnen. Durch Wählen einer Abfrage werden automatisch der Name und die Regelkriterien der Gerätegruppe basierend auf der ausgewählten Suche eingetragen.

        > Sie können diese Abfragen erstellen und speichern, indem Sie zu **Geräte** > **Geräte** > **Erweiterte Suche** navigieren. Jede dort gespeicherte Abfrage kann hier automatisch geladen werden.

    Manuell verwaltet: Geben Sie jeden Benutzer ein, dessen Geräte in der Gruppe enthalten sein sollen.
5. Für dynamisch verwaltete Gruppen:
    1. Erstellen Sie eine Richtlinie, die diese Gruppe definiert.
    2. **Beispiel**: Betriebssystem ist iOS
       Klicken Sie gegebenenfalls auf +, um weitere Richtlinien zu erstellen.
    3. **Beispiel**: Gerät ist iPhone 5S
       Klicken Sie auf Beliebig, wenn die Geräte mindestens eine der Richtlinien erfüllen sollen.
    4. Klicken Sie auf Alle, wenn die Geräte alle Richtlinien erfüllen sollen.
6. Für manuell verwaltete Gruppen:
    1. Geben Sie den Namen eines Benutzers ein, dessen Gerät Sie hinzufügen wollen.
    2. Wählen Sie das gewünschte Gerät aus der angezeigten Liste.
    3. Wiederholen Sie die Schritte a und b, bis alle Geräte in der Liste angezeigt sind.

Klicken Sie auf **Speichern**.

Gerätegruppe entfernen

Verfahren

1. Gehen Sie zu **Geräte** > **Gerätegruppen**.
2. Klicken Sie in das Kontrollkästchen für die Gerätegruppe, die Sie entfernen wollen.
3. Klicken Sie auf **Gerätegruppe löschen**.

Exportieren von Geräten in eine CSV-Datei

Sie können die Gerätedetails für eine bestimmte Gerätegruppe über die Option **Als CSV-Datei exportieren** auf der Seite **Gerätegruppen** exportieren.

Verfahren

1. Gehen Sie zu **Geräte** > **Gerätegruppen**.
2. Wählen Sie alle oder mehrere Spaces aus, um die Informationen in Bezug auf bestimmte Bereiche anzuzeigen.
3. Klicken Sie auf den Link zum Zählen der Gerätegruppe. Es wird die Seite "Geräteliste" angezeigt, die mit dem ausgewählten Space verknüpft ist.
4. Klicken Sie auf die Option **Als CSV-Datei exportieren**, um die Geräteliste und die verknüpften Details in eine CSV-Datei zu exportieren. Es wird eine Popup-Meldung angezeigt, aus der hervorgeht, dass die Verarbeitung des Exportberichts einige Zeit dauert wird. Warten Sie, bis die Anforderung abgeschlossen ist, bevor Sie eine andere Anforderung übermitteln.
5. Klicken Sie auf **Herunterladen**. Sie erhalten eine E-Mail mit einem Link zum Herunterladen des Berichts.
6. (Optional) Klicken Sie zum Löschen des Berichts auf **Löschen**.

Wenn Sie die Seite **Gerätegruppen** nicht sehen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie brauchen eine der folgenden **Rollen**

- Geräteverwaltung
- Geräts schreibgeschützt

Benutzerdefinierte Attribute zu Gerätegruppen zuweisen

Administratoren können jetzt benutzerdefinierte Attribute direkt Gerätegruppen zuweisen. Jedes Gerät, das Mitglied einer Gerätegruppe wird, erbt automatisch die konfigurierten benutzerdefinierten Attributwerte, sodass nach der Registrierung keine Attribute manuell den einzelnen Geräten zugewiesen werden müssen. Verwenden Sie Gerätegruppen, um benutzerdefinierte Attributwerte automatisch Geräten zuzuweisen, die dann Mitglieder der Gruppe werden.

Verfahren

1. Gehen Sie zu **Geräte** > **Gerätegruppen**.
2. Wählen Sie eine vorhandene Gruppe aus oder erstellen Sie eine.
3. Klicken Sie auf der Seite "Gerätedetails" auf **Attribute**.
4. Klicken Sie auf **Neu hinzufügen**.
5. Wählen Sie das benutzerdefinierte Attribut aus und geben Sie den erforderlichen Wert an.

7.3. Nicht verwaltete Geräte

Dieser Abschnitt enthält die folgenden Themen:

- Gerät sperren
- Gerät freischalten
- Gerät aus der Geräteliste löschen

Lizenz: Silver

Wenn Sie eine Sentry-E-Mail-Zugriffskontrolle eingerichtet haben, werden alle nicht registrierten Geräte, die auf Ihr E-Mail-System zugreifen, als nicht verwaltete Geräte bezeichnet. Sie legen fest, ob nicht verwaltete Geräte standardmäßig E-Mail-Zugriff haben wollen, wenn Sie Sentry konfigurieren. Sie können den E-Mail-Zugriff für diese Geräte manuell sperren oder erlauben.

> Die Seite für unverwaltete Geräte wird alle 5 Minuten aktualisiert. Änderungen in der Verwaltung werden daher nicht sofort angezeigt.

Gerät sperren

Verfahren

1. Wählen Sie das entsprechende Gerät aus.
2. Klicken Sie auf **Aktionen > Blockieren**.

Das Gerät bleibt gesperrt, bis Sie auf **Aktionen erlauben > oder Aktionen > löschen** klicken.

Gerät freischalten

Verfahren

1. Wählen Sie das entsprechende Gerät aus.
2. Klicken Sie auf **Aktionen > Zulassen**.

Das Gerät hat weiter Zugriff auf E-Mails, bis Sie auf **Aktionen > sperren** oder **Aktionen > löschen** klicken.

Gerät aus der Geräteliste löschen

Verfahren

1. Wählen Sie das entsprechende Gerät aus.
2. Wählen Sie **Aktionen > Löschen**.

Wenn das Gerät das nächste Mal versucht, auf Ihr E-Mail-System zuzugreifen, erscheint es wieder in dieser Liste, und Sie müssen die zuvor für das Gerät definierte Aktion (Sperren oder Zulassen) wiederholen.

7.4. App-Inventar

Dieser Abschnitt enthält die folgenden Themen:

- App-Anzeige filtern
- Installierte Geräte für eine App anzeigen
- Apps-Liste anzeigen
- Anzeigen der auf einem Gerät installierten Win32- oder Win32-Store-Apps
- Benutzerdefinierte Ansichtsberechtigung erstellen
- Exportieren eines App-Inventars

Der App-Bestand ist die Liste der auf registrierten Geräten ermittelten Apps. Auf dieser Seite erhalten Administratoren Informationen zu den Apps, die von registrierten Geräten verwendet werden. Sie können beispielsweise folgende Fragen beantworten:

- Welche Apps sind die beliebtesten?
- Beziehen iOS-Geräte ihre Apps direkt aus dem App-Store?
- Wie viele Android-Benutzer haben optional eine hauseigene App heruntergeladen?
- Wie viele Geräte nutzen eine veraltete Version einer App?

App-Anzeige filtern

Wenn Sie die Seite **Geräte > App-Bestand** aufrufen, werden alle Apps angezeigt. Wenn Sie diese Liste einschränken möchten, damit nur bestimmte Apps angezeigt werden, nutzen Sie die Filter (im linken Bereich). Um die Liste beispielsweise so einzugrenzen, dass nur die privaten Apps von Google Play angezeigt werden, wählen Sie **Private** im Abschnitt **Source**.

Sie können den App-Bestand auf den Geräten aller oder mehrerer Spaces anzeigen, indem Sie mehrere Spaces aus der Dropdown-Liste auswählen. Wenn Sie mit der Maus über die angezeigten Apps fahren, wird die Zahl der Geräte angezeigt. Sie können auf das Zählersymbol für eine App klicken, um alle Geräte anzuzeigen, auf denen diese App installiert ist. Jeder Datensatz für einen App-Bestand wird nach Space gruppiert.

Sie können die Suche nach App-Name oder nach Bundle-/Paket-ID durchführen.

Wenn Sie mehrere Spaces ausgewählt haben und dann den Mauszeiger über dem Wert **Gesamt** in der Spalte **Anz. Install.** platzieren, wird die Anzahl der Installationen pro Geräte-Space angezeigt.

Installierte Geräte für eine App anzeigen

Klicken Sie auf die Zahl bei **Verwaltet**, **Nicht verwaltet**, oder **Gesamt**, die in der Spalte **Installierte Anzahl** aufgeführt ist.

Apps-Liste anzeigen

Klicken Sie auf das Pull-down-Menü **#Angefordert** für die App im App-Bestand, um die Geräte anzuzeigen, die die App angefordert haben. Dies gilt nur für MAM-Only-Geräte.

Anzeigen der auf einem Gerät installierten Win32- oder Win32-Store-Apps

Das App-Inventar zeigt die Win32- oder Win32-Store-Apps eines Gerätes an, wenn die Datenschutzkonfiguration des betreffenden Geräts die Erfassung von Informationen über alle Apps auf dem Gerät erlaubt. Die Datenschutzrichtlinie für das Gerät ist

konfigurierbar.

Verfahren

1. Ermitteln Sie, welche Datenschutzeinstellungen für das gewünschte Gerät gelten, indem Sie die Anweisungen unter **Geräte** ausführen.
2. Gehen Sie zu **Konfigurationen**.
3. Für die Datenschutzeinstellungen haben Sie in Schritt 1 Folgendes notiert:
    1. Wählen Sie die Konfiguration aus.
    2. Klicken Sie auf [Edit].
    3. Wählen Sie unter **App-Bestand erfassen** die Option **Für alle Apps auf dem Gerät**.
    4. Klicken Sie auf **Fertig**.

> Der Win32AppInventory-CSP zeigt die Liste aller auf dem Gerät installierten Win32- und Win32 Store-Apps an und zwar alle 24 Stunden, nachdem die Inventarscans auf dem Gerät ausgeführt wurden.

Benutzerdefinierte Ansichtsberechtigung erstellen

Sie können für die Benutzer benutzerdefinierte Anzeigeberechtigungen festlegen.

Verfahren

1. Gehen Sie zu **Admin**.
2. Gehen Sie zu **Rollenverwaltung**.
3. Klicken Sie auf **Benutzerdefinierte Rolle hinzufügen**.
4. Wählen Sie die Option **Space-spezifische Rolle**.
5. Geben Sie den Namen des Benutzers in das Feld **Name** ein.
6. Klicken Sie im Menü **Geräte** auf **App-Bestand**.
7. Aktivieren Sie das Kontrollkästchen **Ansicht**.
8. Klicken Sie im Menü **Geräte** auf **Geräte-Aktionen**.
9. Klicken Sie auf **Speichern**.
10. Gehen Sie im Hauptmenü zu **Benutzer**.
11. Klicken Sie auf den neuen Benutzer, den Sie erstellt haben.
12. Klicken Sie auf **Rollen zuweisen**.
13. Aktivieren Sie das Kontrollkästchen **app | Space-spezifisch** und klicken Sie auf **Weiter**.
14. Auf der Seite **Zusammenfassung** werden die Berechtigungen für die von Ihnen erstellte Rolle angezeigt.
15. Klicken Sie auf **Fertig**.
16. Melden Sie sich als neuer Benutzer an.
17. Klicken Sie im Hauptmenü auf **Geräte**.
18. Klicken Sie auf **App-Bestand**.
19. Die Seite **App-Bestand** zeigt jetzt nur noch die für den Benutzer erlaubten Anwendungen an.

Exportieren eines App-Inventars

Als Administrator können Sie mithilfe der Option **Als CSV-Datei exportieren** App-Inventar-Berichte anfordern.

Verfahren

1. Wechseln Sie zu **Geräte > App-Inventar**.
2. Wählen Sie Inventar aus der Liste aus.
3. Klicken Sie auf **Als CSV-Datei exportieren**.
4. Wählen Sie eine der folgenden Optionen aus:

- Mit **Apps als CSV exportieren** exportieren Sie alle Anwendungen im App-Inventar.
- Mit **Geräte als CSV exportieren** exportieren Sie eine bestimmte Anwendung gemäß der nachstehenden Tabelle:

Option	Beschreibung
Bundle-ID	Geben Sie die Bundle-/Paket-ID der Anwendung ein.
Möchten Sie den Exportvorgang durchführen?	Wählen Sie eine der folgenden Optionen aus: • Insgesamt installiert • Verwaltet • Nicht verwaltet • Angefordert (für Nur-MAM-Geräte)

5. Klicken Sie auf **Exportieren**.

Der Administrator erhält eine Meldung, in der er informiert wird, dass der Export etwas Zeit in Anspruch nimmt. Nach dem Einreichen des Requests muss der Administrator warten, bis dieser abgeschlossen ist, bevor er einen weiteren Request senden kann. Wenn der Bericht bereitsteht, erhält der Administrator eine Meldung, in der er angeben muss, ob er den generierten Bericht herunterladen oder löschen möchte. Der Administrator erhält außerdem eine E-Mail mit einem Link zum Herunterladen des Berichts.

Wenn Sie die Seite **App-Bestand** nicht sehen können, kann es sein, dass Sie nicht über die erforderlichen Berechtigungen verfügen. Sie brauchen eine der folgenden **Rollen**:

- Geräteverwaltung
- Gerät schreibgeschützt

7.5. Verwalten von Geräten

Dieser Abschnitt enthält die folgenden Themen:

- Bereitstellen von Windows-Diensten
- Apple Remote Desktop auf macOS-Geräten aktivieren
- Geräteregistrierung (iOS, macOS und Android)
- Geräteregistrierung (Windows 10+-PC und Microsoft HoloLens 2)
- Bereitstellungspaketregistrierung mit PIN
- Verwenden der Massenregistrierung für Windows-Geräte
- Passworteinstellungen ändern
- Den Gerätenamen ändern
- Suchen nach und Filtern von Geräten
- Geräteeigentümer verwenden
- Verwaltetes Gerät mit Arbeitsprofil
- Verwendung der Massenregistrierung für Android
- Massenregistrierung mit CSV-Dateiupload
- Verwendung der mobilen Registrierung von Samsung Knox
- Registrieren von Oculus-Geräten
- Bluetooth auf einem Gerät aktivieren
- iOS-Update planen
- Installieren Sie die iOS System-Apps neu.
- Zuweisen eines neuen Benutzers für ein Gerät
- Neuzuweisen eines Android-Geräts
- Erzwingen einer Geräteanmeldung
- Lokalisierung eines Geräts
- Gerät sperren
- Verwalten von Apple-Geräten im Verloren-Modus
- Debug-Protokolle anfordern
- Gerät außer Dienst stellen
- Verzichten auf Gerätebesitz
- Gerät „wipen“
- Löschen von Geräten
- Gerät entsperren
- Geräte neu starten und herunterfahren
- Passwort-Einschränkungen löschen (nur iOS)
- Sentry-Zuordnung für ein Gerät löschen
- Anpassbare Attribute für Geräte zuweisen

- Anpassbare Attribute von Geräten entfernen
- App-Feedback synchronisieren und abrufen
- Definition des Firmware-Passworts
- Neuen persönlichen Wiederherstellungsschlüssel ausstellen
- Wiederherstellungssperre einstellen oder ändern
- Apple-Zugriffsverwaltung
- Registrierung über Gruppenrichtlinie

7.5.1. Bereitstellen von Apple-Geräten

Ivanti Neurons for MDM unterstützt die Verwaltung all Ihrer Apple-Geräte. Mithilfe dieser umfassenden Lösung können Sie Ihre Geräteflotte bereitstellen, verwalten, aktualisieren und sichern und Ihren Endbenutzern eine herausragende Benutzererfahrung bieten.

Dieser Abschnitt enthält die folgenden Themen:

- Installieren des Apple-MDM-Zertifikats
- Registrieren von Apple-Geräten
- Ivanti Go for iOS Client
- Verwalten von Anwendungen für Apple-Geräte
- Konfigurationen verwalten
- Verwalten von Softwareupdates
- Einrichten von iOS/iPadOS-Geräten
- Einrichten von watchOS-Geräten
- Unterstützte Geräteaktionen für watchOS-Geräte
- Einrichten von visionOS-Geräten
- Unterstützte Geräteaktionen für visionOS-Geräte
- Einrichten von macOS-Geräten
- Einrichten von tvOS-Geräten
- Unterstützung für deklarative Geräteverwaltung (DDM)

Installieren des Apple-MDM-Zertifikats

Zum Verwalten von Apple-Geräten müssen Sie zunächst ein Apple-MDM-Zertifikat zum Verwalten von iOS-Geräten anfordern und installieren. Verlängern Sie das Apple-MDM-Zertifikat einmal jährlich. (Das für die Erstellung des Zertifikats verwendete Apple-Konto erhält eine Benachrichtigung von Apple, wenn das Ablaufdatum ansteht.) Verwenden Sie die Seite "MDM-Zertifikat", um dieses Zertifikat hinzuzufügen oder zu verlängern.

Folgen Sie den Schritten unter MDM-Zertifikat installieren

Registrieren von Apple-Geräten

Wählen Sie eine der folgenden Methoden, um Geräte zu registrieren:

- Automatische Geräteregistrierung
- Apple School Manager
- Apple Configurator

Ivanti Go for iOS Client

Im nächsten Schritt wählen Sie den Registrierungstyp aus, den Ihr Unternehmen für Ihre Geräte zugelassen hat. Ivanti Neuros for MDM unterstützt derzeit Folgendes:

- Geräteregistrierung (iOS, macOS und Android)

- Benutzerregistrierung mit Apple Business Manager
- Kontogesteuerte Benutzerregistrierung
- Einstellungen (Apple)

Verwalten von Anwendungen für Apple-Geräte

Die Seite "App-Katalog" in Ivanti Neurons for MDM dient Administratoren als Schnittstelle, über die sie ihren App-Katalog effizient verwalten können. Diese Funktionalität umfasst die Orchestrierung mobiler Anwendungen, die Endbenutzern zur Verfügung stehen, und beinhaltet sowohl öffentliche App Stores als auch Anwendungen, die für die Verteilung über Ivanti Neurons for MDM vorgemerkt sind.

Unterstützte Apps:

Der App-Katalog aggregiert verschiedene App-Typen, darunter Apps aus öffentlichen App Stores, benutzerdefinierte Apps, intern entwickelte Apps, über AppConnect aktivierte Apps, GoClient for iOS und M@W for macOS und optimiert dadurch den Importvorgang für die daran anschließende Konfiguration und Verteilung.

Auf Geräten, die mit reinen Mobile Application Management (MAM)-Konfigurationen betrieben werden, müssen iOS-Benutzer beim Aufrufen des App-Katalogs ein Authentifizierungszertifikat auswählen. Dieser Authentifizierungsschritt ist wichtig, um den Zugriff auf die aufgeführten Apps zu sichern und robusten Sicherheitspraktiken zu entsprechen.

> M1-Chipsatz-MacBooks von Apple bieten besondere Unterstützung für iPhone- und iPad-VPP-Apps innerhalb von [Ihr Softwareprodukt]. Insbesondere sind nur Administratoren befugt, unterstützte iPhone- und iPad-VPP-Apps via Push zu übertragen, sodass Benutzer diese nicht direkt über die App installieren können.

Ausführlichere Implementierungsanweisungen und Informationen zu den Konfigurationsoptionen finden Sie in der umfassenden Dokumentation im Administratorhandbuch und in den nachstehenden Ressourcen:

- Verwalten von Apps
- App-Katalogeinstellungen
- Einrichten von Apple Apps and Books
- Unternehmens-App Store Apps@Work
- macOS AppStore-Einschränkungen

Konfigurationen verwalten

Konfigurationen sind Sammlungen von Einstellungen, die Sie als Administrator an Geräte senden. Sie können zum Beispiel Konfigurationen verwenden, um automatisch VPN-Einstellungen und Passcodeanforderungen auf den Geräten einzurichten. Die vorhandenen Konfigurationen für Ihr System sind auf der Konfigurationsseite aufgelistet. Sie können mehrere Konfigurationen auf der Seite "Konfigurationen" auswählen und via Push gleichzeitig auf mehrere Geräte übertragen. Diese Konfigurationen können via Push an Geräte in ausgewählten Spaces übertragen werden, ohne die in anderen Spaces zu beeinträchtigen. Konfigurationen können auf einem einzelnen Space, auf mehreren oder auf allen Spaces gleichzeitig bereitgestellt werden.

Die meisten Konfigurationen in Ivanti Neurons for MDM sind für alle Plattformen gleich. Weitere Einzelheiten zum Arbeiten mit Konfigurationen finden Sie unter "Arbeiten mit Konfigurationen".

Einige Konfigurationen werden nur auf bestimmten Plattformen unterstützt. Sie können die Liste nach der für die Konfigurationstypen unterstützte Plattform überprüfen.

Verwalten von Softwareupdates

Beginnen Sie, indem Sie die Softwareupdatekonfiguration für Ihre iOS- und macOS-Geräte einrichten.

> Beim Einrichten eines geplanten Fensters für Softwareupdates wird der Befehl zum Aktualisieren des Betriebssystems jede Stunden via Push an das Gerät gesendet, um sicherzustellen, dass das Fenster nicht versäumt wird. Das Apple-Verhalten sieht vor, dass jedes Mal, wenn der Befehl zum Aktualisieren des Betriebssystems vom Gerät empfangen wird, ein Popupfenster eingeblendet wird, in dem der Benutzer aufgefordert wird, ein Upgrade durchzuführen. Der Benutzer kann den Zeitpunkt dreimal verschieben. Nach dem dritten Mal erzwingt das Gerät gemäß Apple-Verhalten das Upgrade.

Für macOS-Geräte lassen sich einige spezifische Regeln anwenden. Siehe "Konfigurieren der Regeln für macOS-Softwareupdates".

Befehl zum Aktualisieren des Betriebssystems für iOS

Sie können über die Geräteliste oder die Geräteseite auch einen einmaligen Updatebefehl an ein oder mehrere Geräte senden. Siehe "Befehl zum Planen von Betriebssystemupdates".

Einrichten von iOS/iPadOS-Geräten

Die folgenden Konfigurationen werden für iOS/iPadOS unterstützt:

- **iOS/iPadOS-Einschränkungen**
- **eSIM-Konfiguration**
  - **Datenerhaltungsplan**
- **Konfigurationen für mobile Netzwerke**
- **Verloren-Modus aktivieren**
- **iOS-MDM-Profil definieren**
- **Single-App-Modus**
  - **Autonomer Single-App-Modus**
- **Gemeinsam genutztes iPad für Unternehmen**
- **Education-Konfiguration**
- **Individuelle iOS-Konfiguration**
- **Nachricht auf Sperrbildschirm**

Einrichten von watchOS-Geräten

Sie können jetzt Apple watchOS-Geräte bei Ivanti N-MDM registrieren, während Sie die Kopplung mit den iOS-Geräten durchführen.

Diese Funktion unterstützt derzeit watchOS 10+.

ProcedureVerfahren

1. Sie müssen das überwachte Gerät mit iOS 17+ registrieren.
2. Weisen Sie dem iOS-Gerät die Apple Watch-Registrierungskonfiguration zu.
3. Sie können Ihre Apple Watch jetzt mit dem iPhone koppeln.

> Sie können die Apple Watch koppeln, nachdem Sie die Watch-Konfiguration via Push an das iPhone übertragen haben. Die Remoteverwaltung für eine Apple Watch lässt sich nicht aktivieren, wenn Sie Watch-Konfiguration an das iPhone pushen, nachdem Sie die Apple Watch damit gekoppelt haben.

Die folgenden Konfigurationen werden für watchOS-Geräte unterstützt:

- **Mobilfunk-Konfiguration**
- **Zertifikatskonfiguration**
- **Zertifikatstransparenz**
- **Identitätszertifikat-Konfiguration**
- **iOS-Einschränkungen**
- **Kennworteinstellungen**
- **Per-App VPN-Konfiguration**
- **WLAN-Konfiguration**

Unterstützte Geräteaktionen für watchOS-Geräte

Die folgenden Geräteaktionen werden für watchOS-Geräte unterstützt:

- Passcode löschen
- Apple Watch sperren
- Apple Watch komplett löschen
- Registrierung von Apple Watch aufheben Ivanti Neurons for MDM

> Durch das Aufheben der Registrierung eines gekoppelten iOS-Geräts werden die Watch zurückgesetzt und die Kopplung mit dem iOS-Gerät aufgehoben.

Einrichten von macOS-Geräten

Die folgenden Konfigurationen werden für macOS unterstützt:

- **Einschränkungen für macOS**
- **Konfigurieren von macOS-Geräten**
- **Arbeiten mit Skripten und dem Mobile@Work-Client**
- **Konfigurieren eines iOS-MDM-Profils**
- **Einrichten des Firmwarekennworts**
- **Aktivieren von FileVault**
  - **FileVault-Wiederherstellungsschlüssel**
  - **Konfiguration der FileVault-Optionen**
- **Plattform und erweitertes SSO**
- **Active Directory macOS**
- **Firewall**

- Ethernet
- Office 365-Kontoerstellung
- macOS-Systemerweiterungen
- Einschränkungen für das Brennen von Medien
- Datenschutzeinstellungen

Einrichten von tvOS-Geräten

Die folgenden Konfigurationen werden für tvOS unterstützt:

- Apple TV-Konfiguration
- Apple TV-Einschränkungen
- Konferenzraum-Anzeige
- AirPlay Spiegelung

Einrichten von visionOS-Geräten

Sie können jetzt Apple visionOS-Geräte bei Ivanti Neurons for MDM registrieren.

Diese Funktion unterstützt derzeit visionOS 1.1+.

Wählen Sie eine der folgenden Methoden, um visionOS-Geräte zu registrieren:

- Kontogesteuerte Geräteregistrierung
- Kontogesteuerte Benutzerregistrierung
- Geräteregistrierung

Die folgenden Konfigurationen werden für visionOS-Geräte unterstützt:

- CalDAV-Konfiguration
- CardDAV-Konfiguration
- Zertifikatskonfiguration
- Konfiguration der Zertifikatswiderrufsprüfung
- Zertifikatstransparenz
- Erstellen der DNS-Proxykonfiguration
- Verschlüsselter DNS
- E-Mail-Konfiguration
- Konfiguration von Exchange
- Google-Konfiguration
- Identitätszertifikat
- iOS-Einschränkungen
- LDAP-Konfiguration
- Verwaltete Domänen
- Netzwerkrelais-Konfiguration

- Per-App VPN-Konfiguration
- Single Sign-On-Konfiguration
- Konfiguration für abonnierte Kalender
- VPN-Konfiguration
- Web-Content-Filter
- WLAN-Konfiguration

Unterstützte Geräteaktionen für visionOS-Geräte

Die folgenden Geräteaktionen werden für visionOS-Geräte unterstützt:

- Komplettlöschung von Apple Vision Pro
- Stilllegung von Apple Vision Pro
- Entsperrung von Apple Vision Pro

Unterstützung für deklarative Geräteverwaltung (DDM)

Bei der deklarativen Geräteverwaltung von Apple handelt es sich um ein modernes Verwaltungsprotokoll, das es verwalteten Geräten ermöglicht, proaktiv und autonom eigene Verwaltungseinstellungen mit weniger Kommunikation anzuwenden. Die deklarative Geräteverwaltung wird beim Registrieren neuer Geräte oder beim Check-in von bereits registrierten Geräten aktiviert.

Die deklarative Geräteverwaltung wird auf folgenden qualifizierten Geräten automatisch aktiviert:

- Computer mit macOS 13 oder später
- Geräte mit iOS 16 oder iPadOS 16 oder später
- Geräte, die über die Benutzerregistrierung registriert wurden, unterstützen die deklarative Geräteverwaltung auf iOS oder iPadOS 15 oder später.
- Apple TV-Geräte mit tvOS 16 oder später
- Apple Watch-Geräte mit watchOS 10 oder später
- Apple Vision Pro-Geräte mit visionOS 1.1 oder später

Derzeit werden folgende Funktionen der deklarativen Verwaltung unterstützt:

- **Statuskanäle**:
  - Änderungen an der Betriebssystemversion
  - Passcode-Compliance
  - Passcode vorhanden
- **Konfiguration**:
  - Konfiguration "Deklarative Verwaltung"

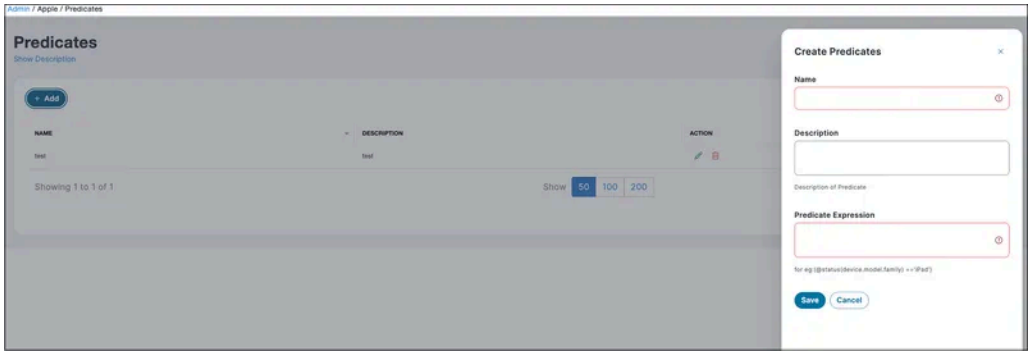
Prädikate in DDM-Konfigurationen

Prädikate sind Ausdrücke in Cocoa-Sprache, mit denen sich Flexibilität und Granularität bei der Aktivierung einer Konfiguration auf einem Gerät erzielen lassen. Der Ausdruck befindet sich auf dem Gerät und wird angewendet, wenn die Bedingungen des Prädikats erfüllt sind. Wir haben eine neue Funktion hinzugefügt, mit der Sie Prädikate erstellen, speichern und auf beliebige DDM-Konfigurationen anwenden können.

Die DDM-Konfiguration verfügt über eine neue Option auf der Seite "Verteilung", über die sich ein Prädikat anwenden lässt. Die bereits erstellten Prädikate finden Sie in der Dropdownliste in diesem Abschnitt.

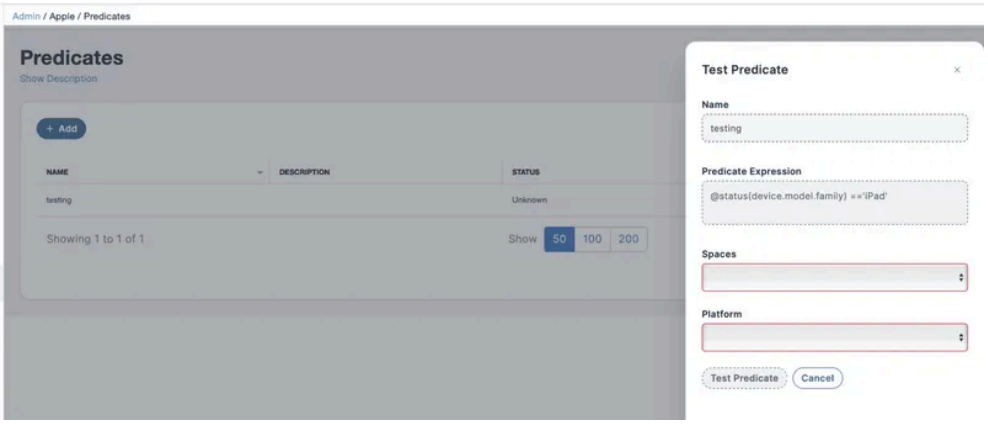
Erstellen von Prädikaten

1. Wechseln Sie zu **Admin** > **Apple** > **Prädikate**.
2. Klicken Sie auf **Hinzufügen**. Das Fenster **Prädikate erstellen** wird angezeigt.
3. Geben Sie folgende Informationen ein:
   - **Name** – Der Name des Prädikats.
   - **Beschreibung** – Fügen Sie eine passende Beschreibung hinzu.
   - **Prädikatausdruck** – Der Prädikatausdruck. Zum Beispiel: @status(device.model.family) =='iPad'



4. Klicken Sie auf **Speichern**. Es wird ein Dialogfeld angezeigt, in dem die Erstellung des Prädikats bestätigt wird.
5. Überprüfen Sie die Gültigkeit der Prädikatsyntax, indem Sie die Seite aktualisieren und die Werte im Status-Feld überprüfen (Werte **Unbekannt**, **In Bearbeitung**, **Gültig**, **Ungültig**).
   1. Klicken Sie auf **Testen**. Das Fenster **Prädikat testen** wird angezeigt. 
   2. Geben Sie folgende Informationen ein:
      - **Name** – Standard
      - **Prädikatausdruck** – Standard
      - **Spaces** – Standard-Space
      - **Plattform** – iOS/macOS
      - **Gerätename** – Bezieht sich auf den Prädikatausdruck.

      > Das Feld **Gerätename** wird nur dann unter dem Feld **Plattform** angezeigt, wenn zuvor Details für die Felder **Spaces** und **Plattform** aus den Dropdownlisten ausgewählt wurden.



3. Klicken Sie auf **Prädikat testen**.
4. Es wird ein Dialogfeld angezeigt, in dem das Initiieren des Prädikattests bestätigt wird.
5. Aktualisieren Sie die Seite, um den Status der Prädikatsyntax anzuzeigen.
    - Bei einem korrekten Prädikatausdruck wechselt der Status von **Unbekannt** zu **In Bearbeitung** zu **Gültig**.
    - Bei einem falschen Prädikatausdruck wechselt der Status von **Unbekannt** zu **In Bearbeitung** zu **Ungültig**.
6. Wiederholen Sie das Verfahren, wenn Sie mehrere Prädikate mit unterschiedlichen Prädikatausdrücken erstellen möchten.

Verteilen von Prädikaten für eine DDM-Konfiguration

1. Erstellen Sie eine von DDM unterstützte Konfiguration.
2. Setzen Sie den Umschalter Aktivierung mit Prädikaten auf EIN und fügen Sie die Prädikate nach Bedarf über die Schaltfläche + hinzu.



Wechseln Sie zum Bearbeiten oder Löschen eines Prädikats zu **Admin** > **Apple** > **Prädikate**. Die Liste der verfügbaren Prädikate ist auf dieser Seite verfügbar. Klicken Sie auf **Bearbeiten**, um Änderungen an dem vorhandenen Prädikat vorzunehmen und zu speichern. Zum Löschen eines vorhandenen Prädikats wählen Sie es aus und klicken Sie auf **Löschen**.

> Sie können ein Prädikat nicht löschen, wenn es mit einer Konfiguration verknüpft ist.

Verwaltungseigenschaften für eine DDM-Konfiguration

Administratoren können über Folgendes Prädikate erstellen:

- Benutzer- und Gerätevariablen
- Benutzerattribute
- Geräteattribute

Beispiel für die Verwendung von Verwaltungseigenschaften in Prädikaten (benutzerdefinierten Attributen):

Prädikat zur Überprüfung, ob der Vorname des Benutzers "test" lautet: @property(userFirstName)=='test'

Weitere Beispiele

- Hardwarefamilie eines Geräts (Mac, iPhone, iPad usw.):
  @status(device.model.family) =='iPad'
  Falls "wahr", ist ein Passcode auf dem Gerät vorhanden. Falls "falsch", ist kein Passcode auf dem Gerät vorhanden.
  @status(passcode.is-present)==true
- Die auf dem Gerät verwendete Betriebssystemfamilie, z. B. macOS oder iOS:
  @status(device.operating-system.family)=='iPadOS'
- Die auf dem Gerät verwendete Betriebssystemversion, z. B. 15.0:
  @status(device.operating-system.version)=='18.2'
  @status(device.operating-system.version)<'18.3'
  @status(device.operating-system.version)>='18.2'
- Boolescher Wert, der angibt, ob File Vault auf dem Gerät aktiviert ist:
  @status(diskmanagement.filevault.enabled)==true
- Beispiel für Verwaltungseigenschaften (benutzerdefinierte Attribute):
  Prädikat zur Überprüfung, ob der Vorname des Benutzers "test" lautet
  @property(userFirstName)=='test'

7.5.2. Bereitstellen von Windows-Diensten

Dieser Abschnitt enthält die folgenden Themen:

- Übersicht
- Geräteverwaltung
- Windows-Geräteregistrierung
- Windows-Updatemanagement
- App-Verwaltung und App-Verteilung
- App-Kontrolle
- Windows-Geräteverwaltungskonfigurationen
- Windows-Gerätecompliance
- Windows-Apps und Hardwareinventar

Übersicht

MI Cloud unterstützt Sie bei der Verwaltung all Ihrer Windows-Laptops und -Desktops, einschließlich HoloLens 2 End-to-End-Lebenszyklusmanagement für Geräte. Die Lösung hilft Ihnen bei Konfiguration, Registrierung, Bereitstellung, Sicherung, Anwendungsverwaltung, Überwachung, Software- und Betriebssystemaktualisierungen bis hin zur Stilllegung.

Geräteverwaltung

Unterstützte Windows-Geräte:

- Windows PC 10+
- Microsoft HoleLens 2

Weitere Informationen zur Geräteverwaltung und zur Berichtsfunktion finden unter **Geräte**.

Windows-Geräteregistrierung

Ivanti Neurons for MDM unterstützt alle Standardmethoden der Geräteregistrierung für Windows-Geräte:

- Manuelle Registrierung
- Massenregistrierung
- via SCCM und Ivanti EPM
- Windows Autopilot
- Entra ID-Registrierung

Weitere Informationen zu den Registrierungsmethoden finden Sie unter **Verwendung von Microsoft Azure**.

Informationen zur Unterstützung mehrerer Benutzer finden Sie unter **Using_Microsoft_Azure.htm#Multi**.

Windows-Updatemanagement

- Konfigurieren und Planen von Windows-Updates – Erstellen Sie zum Konfigurieren und Planen von Windows-Updates eine Konfiguration über Konfiguration – **[Software Updates]**.

- Windows-Updateverwaltung – Sie können die von Windows-Geräten gemeldeten Updates mithilfe der Windows-Updateverwaltung anzeigen und genehmigen. Mit dieser Funktion können Sie verhindern, dass nicht benötigte oder nicht getestete Updates auf den Geräten installiert werden. Weitere Informationen finden Sie unter **Windows-Updatemanagement**.

App-Verwaltung und App-Verteilung

Benutzer haben die Möglichkeit, den kompletten Apple-Lebenszyklus (Import, Konfiguration, Planung, Verteilung, Aktualisierung und Entfernung) für Windows-Anwendungen durchzuführen.

Unterstützte App-Typen:

- Intern
- MSB
- Öffentlicher Store

Unterstützte App-Erweiterungen:

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

Weitere Details zum Verwalten von Windows-Apps finden Sie unter **App-Konfiguration**. Informationen zum Automatisieren von App-Updates finden Sie unter **Zeitplanung von Windows Apps** und **Arbeiten mit Konfigurationen**.

App-Kontrolle

Mit der Konfiguration der App-Kontrolle können Sie Apps auf Geräteebene als Whitelist oder Blacklist kategorisieren. Bereits installierte Apps werden ausgeblendet und können nicht gestartet werden. Apps sind im App Store weiter sichtbar, können jedoch nicht gestartet oder heruntergeladen werden. Jedes Gerät, an das die App Control-Konfiguration verteilt wird, nutzt diese Konfiguration und ignoriert eventuelle Einstellungen der Richtlinie für zulässige Apps. Die App-Konfiguration überschreibt alle App-relevanten Richtlinien, die sich auf die gleiche App auf den Zielgeräten beziehen.

Weitere Informationen finden Sie unter **Konfiguration der App-Kontrolle: Kontrolle der Apps, die auf dem Gerät installiert sind**.

Windows-Geräteverwaltungskonfigurationen

Die Unterstützung für Windows 10+-PC und Microsoft HoloLens 2 umfasst Folgendes:

- **Geräteregistrierung (Windows 10+-PC und Microsoft HoloLens 2)**
- **Passwortkonfiguration**
- **Konfiguration von Exchange**
- **Konfigurationen**
- **Geräte**
- **Apps**
- **Zeitplanung von Windows Apps**
- **Konfiguration der App-Kontrolle: Kontrolle der Apps, die auf dem Gerät installiert sind**

- Windows-Updatemanagement
- Melden des Gerätestatus von Ivanti Neurons for MDM an Azure
- Windows Autopilot-Profile konfigurieren
- Übertragen von SyncML via Push auf Geräte mit benutzerdefinierten Konfigurationen
- Richtlinien
- Windows-Einschränkungen
- Identitätszertifikate
- Windows Hello for Business
- WLAN- und VPN-Profile

> An HoloLens-Geräte verteilte Konfigurationen, die von diesem Gerätetyp nicht unterstützt werden, werden auf der Registerkarte "Konfigurationen" bei den Gerätedetails nicht als verteilte Konfigurationen gemeldet.

Windows-Funktionen (werden nur für Windows PC unterstützt):

- Ivanti Bridge
- Windows BIOS-Konfiguration
- Windows BitLocker
- Windows Kiosk-Konfiguration
- Konfiguration der Windows-Lizenz
- EMA Server-Integrationskonfiguration
- Druckereinstellungen
- Bloatware-Konfiguration entfernen
- ADMX (GPO) Browser

Windows-Gerätecompliance

Cloud kann mit Microsoft Azure eingerichtet werden, um Benutzer nahtlos auf ihren Windows-Desktops und Tablets ab Windows 10 zu registrieren. Informationen zum Konfigurieren der Azure-Mandantenintegration zur Aktivierung der Windows-Gerätecompliance finden Sie unter Verwendung von Microsoft Azure.

Windows-Apps und Hardwareinventar

Windows-App-Inventar

Das App-Inventar ist die Liste der auf registrierten Geräten ermittelten Apps. Auf dieser Seite erhalten Sie Informationen zu den Apps, die von angemeldeten Geräten verwendet werden. Weitere Informationen finden Sie unter App-Inventar.

> Das App-Inventar zeigt die Win32-Apps oder Win32-Store-Apps eines Gerätes an, wenn die Datenschutzkonfiguration des betreffenden Geräts die Erfassung von Informationen über alle Apps des Geräts erlaubt.

Konfigurieren von Intervallen für die App-Inventarisierung

Sie können die Intervalle für die Inventarisierung von Windows 10-Apps für das Inventar mehrerer App-Quelltypen festlegen. Die Intervalle werden verwendet, wenn die Datenschutzkonfiguration so eingestellt ist, dass sie alle Apps des Geräts erfasst.

Weitere Informationen finden Sie unter **App-Bestandsaufnahmeintervalle konfigurieren**.

Windows-Hardwareinventar

Sie können die Erfassung von Hardwareinformationen von Windows 10-Geräten aktivieren. Die Details werden mithilfe von Bridge abgerufen. Weitere Informationen finden Sie unter **Hardware-Bestand**.

7.5.3. Apple Remote Desktop auf macOS-Geräten aktivieren

Dieser Abschnitt enthält die folgenden Themen:

- Apple Remote Desktop auf macOS-Geräten aktivieren
- Apple Remote Desktop auf macOS-Geräten aktivieren

Apple Remote Desktop auf macOS-Geräten aktivieren

Die Apple Remote Desktop-Funktion aktiviert die Bildschirmfreigabe und Sie können die Geräte per Fernzugriff verwalten. Diese Funktion ist für überwachte MacOS 10.14.4+-Geräte verfügbar.

Verfahren

1. Wählen Sie unter **Geräte** ein oder mehrere überwachte MacOS-Geräte aus.
2. Klicken Sie für die Geräte auf **Aktionen** > **Remote-Desktop-Aktion aktivieren**.
3. Klicken Sie zur Bestätigung auf **Remote Desktop aktivieren**.

Apple Remote Desktop auf macOS-Geräten aktivieren

Verfahren

1. Wählen Sie unter **Geräte** ein oder mehrere überwachte MacOS-Geräte aus.
2. Klicken Sie für die Geräte auf **Aktionen** > **Remote-Desktop-Aktion aktivieren**. Die Bildschirmfreigabe ist deaktiviert und Sie können die Geräte nicht per Fernzugriff verwalten.

7.5.4. Geräteregistrierung (iOS, macOS und Android)

Dieser Abschnitt enthält die folgenden Themen:

- **Verwaltungsprofil manuell installieren**
- **Einladung versenden (iOS, macOS und Android)**
- **Endnutzer anweisen, die App herunterzuladen (iOS und Android)**

Die meisten Benutzer beginnen mit der Geräteregistrierung. Sie können jeden der folgenden Ansätze nutzen, um die Registrierung zu starten:

- Eine Einladung an einen oder mehrere Endbenutzer senden (iReg-Registrierung)
- Endbenutzer anweisen, die Go herunterzuladen (In-App-Registrierung)

> Wenn die iOS- und macOS-Geräte-MDM-Registrierung mit dem Fehler *Profilinstallation fehlgeschlagen; SCEP-Server hat ungültige Antwort zurückgegeben* fehlschlägt, muss der Gerätebenutzer den Geräteregistrierungsprozess noch einmal von vorne beginnen. Dies ist meistens dann der Fall, wenn der Gerätebenutzer länger als erwartet benötigt, um den MDM-Registrierungsprozess für iOS- und macOS-Geräte durchzuführen, nachdem das Profil auf das Gerät heruntergeladen wurde. Weitere Erläuterungen erhalten Sie beim Ivanti Support.

Ivanti Neurons for MDM unterstützt die Benutzerverwaltung eines einzelnen Benutzers (lokaler Benutzer oder registrierter Active Directory (AD)-Benutzer) auf MacOS-Geräten. Administratoren können Geräte für die Benutzer verwalten, Geräteprofile und Benutzerprofile übernehmen und somit App Store, App-Verteilung, Konfigurationen und Richtlinien (auch für Apps@Work, Einschränkungen und Sicherheit) nutzen.

Um MacOS-Geräte mit einem AD-Benutzer zu verwalten, muss der AD-Benutzer der Benutzer sein, der während der Registrierung angemeldet ist. Ein anderer, nicht registrierter Benutzer kann die registrierten benutzerbezogenen Profile (z. B. Identitätszertifizierungen, VPN) nicht einsehen. Konfigurationen auf Geräteebene können jedoch von jedem angemeldeten Benutzer eingesehen und verwendet werden.

> **Users.htm**Ivanti Neurons for MDM Der Endbenutzer muss bereits ein Konto in der Cloud besitzen, erst dann können Sie mit dem Geräteregistrierungsprozess beginnen. Für LDAP-Benutzer bedeutet dies, dass ein **Connector** und ein **LDAP-Server** eingerichtet werden müssen und der Benutzer vom LDAP-Server importiert werden muss. Für lokale Benutzer bedeutet dies, dass ein **Benutzer hinzugefügt** werden muss.

> Ivanti Neurons for MDMDie durch ältere Versionen der Cloud erzeugte URL für die Geräteregistrierung funktioniert mit der aktuellen Version nicht mehr. Der Administrator muss die URL für die Geräteregistrierung neu erstellen.

Verwaltungsprofil manuell installieren

Gilt für:

- Ivanti Neurons for MDMmacOS 12.2 bis zur letzten freigegebenen Version, die von unterstützt wird.
- Ivanti Neurons for MDMmacOS 11.0 bis zur letzten freigegebenen Version, die von unterstützt wird.

iOS-Geräteregistrierung

App-interne Registrierung auf iOS-Geräten:

- Während der Geräteregistrierung mit Go app wird eine Seite mit Anweisungen zum Installieren des Profils angezeigt.
- Klicken Sie auf die Option **Heruntergeladenes Profil installieren** und dann auf **Verstanden**.
- Das heruntergeladene Profil ist einige Minuten lang gültig, danach ist eine erneute Registrierung erforderlich.

macOS-Geräteregistrierung

Zur Registrierung von macOS-Geräten im Selbstbedienungsportal muss ein Benutzer folgende Schritte durchführen:

Verfahren

1. Melden Sie sich mit ihren Anmeldeinformationen an.
2. Über die Seite „Installationsverwaltungsprofil“ wird das Profil auf das lokale System des Benutzers heruntergeladen.
3. Doppelklicken Sie auf das heruntergeladene Profil, um es in den Systemeinstellungen des Benutzers sichtbar zu machen.

> Den Benutzern steht nur eine begrenzte Zeit zur Verfügung, um das Profil zu installieren, danach wird es ungültig.

4. Öffnen Sie **Profile** in den Systemeinstellungen. Wenn das Profil auf das Gerät heruntergeladen wird, können Benutzer mit dem Link „Profile“ eine Webseite anzeigen. Klicken Sie auf **Profile**, um die Einstellungen-App zu öffnen.
5. Klicken Sie auf **Installieren**, um das Verwaltungsprofil zu installieren.
6. Fahren Sie fort und beenden Sie den Installationsvorgang. Geben Sie das Passwort ein, wenn Sie dazu aufgefordert werden.

Einladung versenden (iOS, macOS und Android)

Beginnen Sie den Registrierungsprozess mit dem Senden einer Einladung. Ivanti Neurons for MDM bietet folgende Möglichkeiten, um den Endbenutzern eine Einladung zur Registrierung eines Geräts zu senden:

- über den **Start-Assistenten**
- wenn Sie **einen oder mehrere Benutzer hinzufügen**
- über die Benutzerseite (**Aktionen > Einladung senden**)

> Falls der Endbenutzer die Einladung nicht mehr vorliegen hat, können Sie die URL weiterleiten, die in der Einladung enthalten war. Stellen Sie sicher, dass Sie **/go** an das Ende der URL hinzufügen.

Endbenutzer mit einem Ivanti Neurons for MDM-Konto und einem Kennwort benötigen keine Einladung, um den Registrierungsprozess zu starten. Sie können ihnen die URL senden, die in der Einladung enthalten ist.

Endnutzer anweisen, die App herunterzuladen (iOS und Android)

Die Go-Anwendung steht für Android- und iOS-Geräte zur Verfügung. Sie können Endbenutzern Anleitungen bereitstellen, wie die App von einem öffentlichen App-Store heruntergeladen werden kann und wie die Registrierung der App gestartet wird. Die E-Mail-Einladung enthält die folgenden Angaben:

- Link zur Registrierungsseite
- PIN für die einmalige Verwendung (falls vom Administrator festgelegt)
- Grundlegende Anweisungen für die nächsten Schritte

Falls Sie für das Konto bereits ein Kennwort festgelegt haben, können Sie dieses an die Unternehmens-E-Mail-Adresse des Endbenutzers senden. Wenn Sie zur Authentifizierung LDAP verwenden, ziehen Sie in Betracht, den Endbenutzer zu informieren, dass Anmeldeinformationen für das Netzwerk benötigt werden.

Wenn der Benutzer die Installation des MDM-Profils während der Registrierung nicht abschließt, sendet Ivanti Neurons for MDM dem Benutzer regelmäßig Push-Benachrichtigungen an das Gerät mit der Aufforderung, den Registrierungsprozess abzuschließen.

Der Benutzer kann entweder Benutzername und Kennwort verwenden oder den QR-Code scannen, um mit der Geräteregistrierung über Go app zu beginnen. Folgende Details werden benötigt:

- **Benutzername**: E-Mail-Adresse
- **Kennwort**: Falls in den **Benutzereinstellungen** angegeben und ein temporäres Kennwort vom Administrator definiert wurde.
- **QR-Code**: Generieren Sie den QR-Code über das Ivanti Neurons for MDM-Self-Service-Portal. Wenn Sie versuchen, über die Option **QR-Code scannen** einen QR-Code zu scannen, wird eine Aufforderung angezeigt, in der der Benutzer aufgefordert wird, Zugriff auf die Kamera des Geräts zuzulassen. Nachdem Sie die Berechtigung dazu erteilt haben, scannt die Kamera den QR-Code und das Gerät wird registriert. Diese Option wird ab Android 9 bzw. ab iOS 14 unterstützt.

Wenn Sie als Endbenutzer eine Registrierungs-E-Mail auf Ihrem Mobilgerät erhalten, tippen Sie auf den Link, um den Registrierungsprozess zu starten. Falls Sie die E-Mail auf einem Laptop oder Desktop erhalten, geben Sie die URL in einen Browser auf Ihrem Mobilgerät ein, um den Registrierungsprozess zu starten.

Die einmalig verwendbare PIN ist enthalten, wenn für das Endbenutzerkonto noch kein Kennwort für das Ivanti Neurons for MDM-Benutzerkonto definiert wurde oder Ihre **Benutzereinstellungen** eine Registrierungs-PIN verlangen. Nach Eingabe der PIN wird der Endbenutzer aufgefordert, ein Passwort für das Konto zu erstellen, sofern das Passwort noch nicht existiert.

> Wenn bei Geräten mit Android Enterprise die Registrierung abgeschlossen ist, werden eventuell manuell installierte Zertifizierungsstellen-Zertifikate für ein Arbeitsprofil oder ein vom Unternehmen verwaltetes Gerät deinstalliert.

Erneutes Registrieren von iOS-Geräten

Gehen Sie folgendermaßen vor, um Ihr Gerät erneut zu registrieren:

1. Starten Sie den Go Client auf dem Gerät.
2. Wechseln Sie zu **Einstellungen** > **Fehlerbehebung** > **Gerät erneut registrieren**. Die erneute Registrierung wird eingeleitet. Dabei werden einige Bestätigungsfenster angezeigt.
3. Tippen Sie bei den Eingabeaufforderungen auf **Ja**.

> Wenn Sie während der Profilinstallation auf **Abbrechen** tippen, stoppt der Registrierungsprozess und der Ivanti Neurons for MDM-Server deaktiviert die Geräte-MDM.

Um den Prozess der erneuten Registrierung noch einmal zu starten, müssen Sie das bereits heruntergeladene Profil neu installieren. Das heruntergeladene Profil ist einige Minuten lang gültig. danach müssen Sie die erneute Registrierung über den Go Client durchführen.

Erneutes Registrieren von Geräten

Der Administrator kann ein Gerät erneut registrieren, indem er die Vorgänge zum Stilllegen, Zurücksetzen oder Löschen verwendet, ohne den aktiven Eintrag manuell zu löschen. Diese Methode bietet sich insbesondere für erneute Registrierungen an, bei denen der

neue und der bestehende Eintrag zum selben Mandanten gehören. Die Geräteseite zeigt den Status des Geräts im Ivanti Neurons for MDM-Administrationsportal wie folgt an:

- **Aktiv** – Die Geräteregistrierung war erfolgreich.
- **Stillgelegt** – Das Gerät wird zurückgesetzt und der Status wird mit "Stillgelegt" angezeigt.
- **Komplettlöschung abgeschlossen** – Das Gerät wird zurückgesetzt und der Status wird mit "Komplettlöschung abgeschlossen" angezeigt.
- **Zurücksetzen** – Das Gerät wird zurückgesetzt und bis zur nächsten Registrierung auf dem Server als aktiv angezeigt.

Auf der Seite "Audit-Protokolle" werden Geräteregistrierung, erneute Registrierung und Stilllegung für Android-Geräte aufgeführt. **Arbeiten mit Widgets**Weitere Informationen finden Sie unter Arbeiten mit Widgets.

> Bei Versionen bis Android 9.x wird nach der erneuten Registrierung nur ein einziger Eintrag angezeigt. Ab Version Android 10.x werden mehrere Einträge angezeigt. Es ist jedoch nur der letzte Eintrag aktiv und die älteren Einträge werden als stillgelegt angezeigt.

7.5.5. Geräteregistrierung (Windows 10+-PC und Microsoft HoloLens 2)

Dieser Abschnitt enthält die folgenden Themen:

Für die Geräteregistrierung sind zwei Verfahren möglich:

- Manuelle Registrierung
  - Einladung
  - Endbenutzer-Registrierung
- Windows Autopilot
- Mit SCCM und Ivanti EPM über eine Bereitstellungspaketregistrierung mit PIN. **Provisioning Package Enrollment with PIN.htm**Bereitstellungspaketregistrierung mit PIN
- **Massenregistrierung**

Manuelle Registrierung

Die meisten Benutzer beginnen mit der Geräteregistrierung. Sie können jeden der folgenden Ansätze nutzen, um die Registrierung zu starten:

- E-Mail-Einladung
- Schicken Sie Benutzer zur Implementierung an die URL
- Der Endbenutzer **muss bereits ein Konto** in der Cloud besitzen, erst dann können Sie mit dem Geräteregistrierungsprozess beginnen. Für LDAP-Benutzer bedeutet dies, dass ein **Connector** und ein **LDAP-Server** eingerichtet werden müssen und der Benutzer vom LDAP-Server importiert werden muss. Für lokale Benutzer bedeutet dies, dass ein **Benutzer hinzugefügt** werden muss.
- Die durch ältere Versionen der Cloud erzeugte URL für die Geräteregistrierung funktioniert mit der aktuellen Version nicht mehr. Der Administrator muss die URL für die Geräteregistrierung neu erstellen.

Versenden einer Einladung

In den meisten Fällen beginnen Sie die Registrierung mit dem Senden einer Einladung. bietet folgende Möglichkeiten, um den Endbenutzern eine Einladung zur Registrierung eines Geräts zu senden:

- im **Start-Assistenten**
- wenn Sie **einen oder mehrere Benutzer hinzufügen**
- auf der Benutzerseite (**Aktionen > Einladung senden**)

Wenn Endbenutzer ihre Einladung verlegen, sie auf einem Desktop-Computer oder Laptop erhalten, oder sie aus irgendeinem Grund nicht erhalten haben, können Sie ihnen die URL schicken, die in der Einladung stand. Ergänzen Sie am Ende Ihrer Service-URL einfach **\go**.

Endbenutzer mit einem Konto in der Cloud und definiertem Kontopasswort benötigen keine Einladung, um den Registrierungsprozess zu beginnen. Sie können sie an die URL weiterleiten, die in der Einladung gestanden hätte.

Durchführen des Registrierungsprozesses für Endbenutzer

Fordern Sie Ihre Gerätebenutzer auf, den Registrierprozess abzuschließen. Sie können die folgenden Anweisungen als Vorlage verwenden und die erforderlichen Änderungen vornehmen:

Verfahren

1. Öffnen Sie einen Browser auf dem Windows 10+-PC.
2. Navigieren Sie zu mobileiron.com/go.
   Sie werden auf eine neue Seite mit einer Registrierungs-URL umgeleitet.
3. Kopieren Sie die Registrierungs-URL in die Zwischenablage.
4. Tippen Sie auf **Konto hinzufügen** am unteren Rand der Seite **Einstellungen**.
5. Geben Sie die E-Mail-Adresse ein, über die Sie die Einladung erhalten haben.

> Wenn der Cloud-Benutzername nicht mit der in der Cloud eingegebenen E-Mail-Adresse des Benutzers übereinstimmt, fordern Sie den Benutzer auf, seinen Benutzernamen einzugeben, wenn er nach der E-Mail-Adresse gefragt wird.

Fügen Sie die kopierte URL des Workplace-Servers in das nächste Textfeld ein.

7. Tippen Sie auf **sign in**.
8. Geben Sie Ihr Passwort in dem nächsten Textfeld ein.
9. Lassen Sie die anderen Felder leer.
10. Tippen Sie auf **sign in**.
11. Klicken Sie in dem Bildschirm **Konto hinzugefügt** auf **Fertig**.
    Der Startbildschirm für den Workplace zeigt, dass ein Konto hinzugefügt wurde.

Windows Autopilot

Windows Autopilot ist eine Microsoft-Funktion, mit denen Administratoren neue Geräte einrichten und unternehmensfertig vorkonfigurieren können. Die Autopilot-Funktion ermöglicht die schnelle, zuverlässige und nahtlose Bereitstellung von Windows Desktop- oder HoloLens2-Geräten. Darüber hinaus erleichtert die Autopilot-Funktion die Ausführung der folgenden Aufgaben:

- Geräte automatisch in Entra ID einbinden
- Geräte automatisch bei MDM-Diensten registrieren
- Geräte erstellen und automatisch zu Konfigurationsgruppen nach dem Profil des Geräts zuweisen
- Registrierungsabläufe anpassen
- AppConnect-Konfigurationen und Richtlinien anwenden
- Wichtige Anwendungen installieren

Ivanti unterstützt alle Modi von Autopilot-Profilen:

- Benutzergesteuert
- Benutzergesteuert/vorab bereitgestellt (bislang White Glove)
- Self-Deployment-Modus

Weitere Informationen finden Sie unter **Windows Autopilot-Profile konfigurieren**.

Zur Sicherheit und zum Schutz gegen unbefugte Nutzung können alle Autopilot-Windows-Geräte mit der Funktion „TenantLockdown CSP“ an einen Mandanten gebunden werden. Damit diese Funktion verwendet werden kann, müssen die Geräte mit der Autopilot-Option registriert werden. Diese Konfiguration wird auf Geräteebene angewendet. Siehe dazu **TenantLockdown CSP**.

Entra ID-Standardregistrierung

Nachdem Benutzer zum Entra ID-Mandanten hinzugefügt wurden, können sie ihre Geräte direkt über das Arbeitskonto registrieren.

Verfahren

1. Wechseln Sie auf einem Windows-Gerät zu **Einstellungen > Konten > Auf Arbeits- oder Schulkonto zugreifen**.
2. Wählen Sie "Geschäfts-, Schul- oder Unikonto hinzufügen" aus und klicken Sie anschließend auf **Verbinden**.
3. Geben Sie die E-Mail-Adresse Ihres Arbeitskontos an.

Das Gerät wird automatisch bei Ivanti Neurons for MDM registriert.

7.5.6. Local Admin Password Solution (LAPS)

Mit **Local Administrator Password Solution (LAPS)** wird die sichere Verwaltung von Kennwörtern für Windows-Geräte automatisiert. LAPS erzwingt zufällige, regelmäßige Kennwortänderungen und speichert diese Kennwörter sicher in einem Verzeichnis, um das Risiko lateraler Bewegungen bei einer Kompromittierung zu reduzieren.

Modernes LAPS lässt sich in Azure und die neuesten Windows-Plattformen für Geräteverwaltung integrieren und ermöglicht dadurch das sichere Speichern und Abrufen von Kennwörtern sowie die Richtlinienkonfiguration mit Ivanti Neurons for MDM und dem AzurePortal. Dadurch ist gewährleistet, dass die Administrator-Anmeldeinformationen sowohl auf Legacy- als auch auf über die Cloud verwalteten Windows-Endpunkten geschützt und prüfbar sind.

> Zur Verwendung von LAPS mit Ivanti Neurons for MDM sollten Azure-Administratoren sicherstellen, dass die N-MDM-App zu ihrem Azure-Mandanten hinzugefügt wurde und über die erforderliche LAPS-Berechtigung (**DeviceLocalCredential.Read.All**) verfügt.

> Über die Richtlinieneinstellung **Administrator-Kontoname** kann die LAPS-Konfiguration angeben, für welche lokalen Admin-Konten sie gilt. Wenn der in der Konfiguration angegebene Kontoname nicht auf dem Gerät vorhanden ist, kann der Kontoname nicht verwaltet werden. Ist das Feld **Administrator-Kontoname** hingegen leer, verwendet die Richtlinie standardmäßig das integrierte lokale Admin-Konto, das anhand seiner bekannten relativen Kennung (RID) identifiziert wird.

> Bei Anwendung der LAPS-Konfiguration wird das Kennwort des lokalen Administratorkontos des Geräts durch den Administrator verwaltet, und das Kennwort wird in Azure Active Directory generiert.

Weitere LAPS-Funktionen

- Kennwortspeicherung in Azure – Lokale Administratorkennwörter können jetzt sicher im Azure-Geräteobjekt gespeichert werden.
- Kennwortabruf – Administratoren können die Gerätekennwörter direkt über das Azure-Portal abrufen.
- Konfigurierbare Einstellungen – Die konfigurierbaren LAPS-Einstellungen können im Ivanti Neurons for MDM-Portal verwaltet werden.
- Bedarfsorientierte Kennwortrotation – Administratoren können Gerätekennwörter manuell über das Ivanti Neurons for MDM-Portal rotieren.
- Automatische Kennwortzurücksetzung bei Verwendung – Kennwörter können automatisch zurückgesetzt werden, sobald auf sie zugegriffen wird.

LAPS-Konfiguration erstellen

Voraussetzungen

- Die LAPS-Lösung muss für Ihre Geräte aktiviert sein. Diese Lösung ist NICHT standardmäßig für alle verfügbar. Wenden Sie sich an das Team vom technischen Support, um Unterstützung anzufordern.
- Die Geräte müssen bei Azure Device Operations (ADO) registriert sein.

Verfahren

1. Initiieren Sie auf Ihrer Plattform für Konfigrationsverwaltung die Erstellung der LAPS-Konfiguration.
2. **Legen Sie die erforderlichen Parameter fest**:

- **Verzeichnis sichern** – Wählen Sie "Kennwort nur in Microsoft Entra ID sichern" aus.
- **Name des lokalen Administrators** – Geben Sie den Administrator-Kontonamen Ihres Systems an (z. B. Admin).

3. **Zusätzliche Einstellungen konfigurieren** – Legen Sie diese gemäß der Sicherheitsrichtlinie Ihres Unternehmens fest. Falls nicht anders angegeben, werden die Standardwerte herangezogen.
   - **PasswordAgeDays** – Anzahl der Tage bis das Kennwort für das lokale Administratorkonto automatisch rotiert.
   - **PasswordComplexity** – Geben Sie die Anforderungen an die Kennwortkomplexität an (z. B. alphanumerische Zeichen, Sonderzeichen).
   - **PasswordLength** – Legen Sie die gewünschte Länge für das Kennwort des lokalen Administratorkontos fest.
   - **PostAuthenticationActions** – Definieren Sie Aktionen, die nach der Authentifizierung durchgeführt werden sollen.
   - **PostAuthenticationResetDelay** – Legen Sie die Verzögerung (in Stunden/Minuten) fest, nach der das Kennwort nach der Authentifizierung zurückgesetzt werden soll.
4. **LAPS-Konfiguration verteilen**
   - Weisen Sie das LAPS-Konfigurationsprofil einem ADO-registrierten Benutzer/Gerät zu.
   - Nach Anwendung der Konfiguration wird ein zufälliges Kennwort für das lokale Administratorkonto erstellt und unter folgendem Pfad sicher in Microsoft Entra ID gespeichert:
     Geräte → Geräte verwalten → Wiederherstellung des lokalen Administratorkennworts.
5. **Kennwortrotation**
   - Das Kennwort wird automatisch gemäß dem in **PasswordAgeDays** festgelegten Wert rotiert.
   - Sie können den Status der Kennwortrotation in den Geräteprotokollen überprüfen.

Kennwortrotation

Gehen Sie folgendermaßen vor, um eine sofortige Rotation des Kennworts für das lokale Administratorkonto zu erzwingen:

1. **Zum Gerät navigieren** – Rufen Sie die Seite mit den Gerätedetails in Ihrer Verwaltungskonsole auf.
2. **Kennwortrotation initiieren**
   - Klicken Sie auf das Menü mit den drei Punkten (...).
   - Wählen Sie **Lokales Administratorkennwort rotieren** aus.
   - Bestätigen Sie bei Aufforderung die Aktion. Daraufhin wird eine Anfrage für eine Kennwortrotation übermittelt.
3. **Check-In und Bestätigung**
   - Das Gerät verarbeitet die Kennwortänderung beim nächsten erzwungenen Check-In.
   - Aktualisieren Sie die Seite in Microsoft Entra ID, um das aktualisierte Kennwort im Abschnitt zur Kennwortwiederherstellung anzuzeigen.

7.5.7. Bereitstellungspaketregistrierung mit PIN

Ivanti Neurons for MDM Der Administrator kann die von SCCM oder Ivanti Endpoint Manager verwalteten Geräte bei der Cloud registrieren. Ivanti Neurons for MDMDas Tool "Bereitstellungspaket" ermöglicht Unternehmen die Optimierung des Umstiegs von Windows-Geräten in die moderne Cloud-Verwaltung ohne Ausfallzeit oder Unterbrechungen für die Benutzer. Ivanti Neurons for MDM Einen nahtlosen Übergang erzielen Sie, indem Sie ein eindeutiges Bereitstellungspaket von der Cloud Console herunterladen und dieses dann über das vorhandene Verwaltungstool oder die Verwaltungsdomäne bereitstellen. Ivanti Neurons for MDMBeim Ausführen des Pakets wird der Endpunkt im Hintergrund in der Cloud registriert; danach steht der Endpunkt zur fortlaufenden Verwaltung zur Verfügung. So können Administratoren die Geräte zunächst auf einfache Weise migrieren und dann später flexibel im Over-the-Air-Verfahren konfigurieren. Ivanti Neurons for MDMWenn die Cloud-Registrierung eines Geräts im Hintergrund abgeschlossen ist, wird das Gerät mit MDM verbunden und von den beiden Verwaltungsstellen gemeinsam verwaltet.
Ivanti Neurons for MDMIvanti Neurons for MDMSobald ein Administrator die gewünschten Windows-Abläufe in Cloud konfiguriert hat, kann die Legacy-Verwaltungsplattform abgeschaltet werden, sodass Cloud als einzige Verwaltungsstelle des Geräts verbleibt.

> Eine Ausnahme für diese Regel gilt, wenn ein Gerät von Microsoft Endpoint Manager (MEM), ehemals SCCM, übertragen wird. Der vorhandene MEM-Client arbeitet so lange im Koexistenzmodus (nicht im Mitverwaltungsmodus), bis die MEM-Plattform abgeschaltet wird. Ivanti Neurons for MDMWenn der Koexistenzmodus aktiviert ist, deaktiviert der MEM-Client automatisch bestimmte Funktionen zugunsten der Cloud, die diese Workloads bereitstellt. Weitere Informationen finden Sie in der **Microsoft-Dokumentation zu Koexistenz**.

Ivanti Neurons for MDMUm präzisere Verhaltensweisen zu erzielen, wenn MEM und andere Verwaltungsplattformen von Drittanbietern verwendet werden, empfiehlt Ivanti, das Cloud-Bereitstellungspaket-Tool in Ihrer Umgebung zunächst zu testen.

Voraussetzungen

- Benutzerkonten müssen über LDAP, Entra ID, lokales Hochladen durch den Benutzer oder andere Identitätsintegrationen in Ivanti Neurons for MDMimportiert werden.
- Auf allen Geräten ist **Windows Configuration Designer** installiert.
- PIN-basierte Registrierung aktivieren auf Ivanti Neurons for MDM
- Benutzernamen sollten keine Leerzeichen enthalten. Dies könnte dazu führen, dass der Übergang eines Benutzergeräts fehlschlägt.
- Dieses Tool kann in Umgebungen bereitgestellt werden, die nicht mit Entra ID arbeiten.
- Für die Hauptelemente der Ivanti Neurons for MDM Modern Windows Management Suite ist Entra ID nicht erforderlich. Für Co-Verwaltung oder Co-Existenz müssen bestimmte Workloads/Konfigurationen möglicherweise bei einer unbeaufsichtigten Registrierung bereitgestellt werden, um Beeinträchtigungen beim Umstieg zu vermeiden.
- Das Bereitstellungspaket wird derzeit nur für SCCM und Ivanti Endpoint Manager unterstützt.

Verfahren

1. Wechseln Sie zu **Admin > Windows > Bereitstellungspaket**.
2. Wählen Sie Benutzer oder Benutzergruppen, um PINs zu erzeugen, und klicken Sie auf Bereitstellungspaket herunterladen (ZIP-Datei).
3. Das Bereitstellungspaket wird den SCCM-/Ivanti Endpoint Manager-Administratoren zur Verfügung gestellt, damit sie die Dateien dekomprimieren und an die jeweiligen von ihnen verwalteten Geräte übergeben können. Informationen zum Durchführen dieses Schritts finden Sie unter **Pakete und Programme in Configuration Manager**.

4. Nach dem Transfer lösen Administratoren das setup.ps1-Skript via Remotezugriff auf den Geräten aus. Informationen zum Auslösen des Skripts finden Sie unter **Erstellen und Bereitstellen von Skripten mit dem Konfigurationsmanager**.
5. Ivanti Neurons for MDM Die Geräte werden in der Cloud registriert.

Die für die Benutzer erzeugte PIN ist nur 24 Stunden gültig. Nach Ablauf der PIN muss eine neue PIN erzeugt werden.

Die Datei mit den PINs wird vom Gerät gelöscht, sobald die Registrierung abgeschlossen ist.

Registrieren von SCCM-Geräten bei Cloud Ivanti Neurons for MDM

Verfahren

1. Ivanti Neurons for MDMLaden Sie alle Bereitstellungsdateien von der Cloud für ausgewählte Benutzer herunter.
2. Wählen Sie die zu registrierenden Konten oder Gruppen aus.
3. Stellen Sie die Paketdateien unter Verwendung von SCCM auf den Clientgeräten bereit:
    1. Überprüfen Sie, ob die erforderlichen Clients in SCCM vorhanden sind. Ist der Windows-Konfigurationsdesigner nicht auf dem Client vorhanden, sollte der Administrator den Designer via Push übertragen und auf dem Client bereitstellen.
    2. Erstellen Sie auf dem SCCM-Server einen Ordner, kopieren Sie die komprimierte Bereitstellungsdatei in den Ordner und extrahieren Sie sie.
    3. Erstellen Sie eine .bat-Datei, um den Inhalt des Ordners zu kopieren, in dem die Dateien auf dem Clientgerät extrahiert werden.
    4. Wechseln Sie in SCCM zu **Softwarebibliothek > Anwendungsverwaltung > Pakete** und erstellen Sie ein Paket, um den Inhalt des Ordners auf den Client zu kopieren. Geben Sie den Zielordner ein, in den Sie den Inhalt kopieren möchten.
    5. Stellen Sie das Paket auf dem Gerät oder am Gerätestandort bereit.
    6. Im Abschnitt "Überwachung" können Sie den Bereitstellungsstatus überwachen und prüfen, ob die Dateien in den Zielordner des Clients kopiert wurden.
4. Führen Sie das Skript aus, um ein Gerät zu registrieren:
    1. Wechseln Sie zu **Softwarebibliothek > Skripte** und erstellen Sie ein Skript.
    2. Geben Sie einen Namen für das Skript ein und importieren Sie das PowerShell-Skript **setup.ps1** aus dem extrahierten Ordner.
    3. Genehmigen Sie das Skript und führen Sie das Skript auf dem Zielgerät aus.
    4. Wählen Sie **Jetzt starten** aus und klicken Sie auf **Speichern**. Die geplante Aufgabe beginnt mit der Ausführung des Skripts. Bei erfolgreicher Ausführung wird der Status grün angezeigt.
5. Wechseln Sie zum Überprüfen der Geräteregistrierung zu **Einstellungen** > **Bereitstellungspaket hinzufügen oder entfernen** > **Details**.

Registrieren von Ivanti Endpoint Manager-Geräten bei Cloud Ivanti Neurons for MDM

Verfahren

1. Ivanti Neurons for MDMLaden Sie alle Bereitstellungsdateien von der Cloud für ausgewählte Benutzer herunter.
2. Wählen Sie die zu registrierenden Konten oder Gruppen aus.

3. **Fall 1**: Für die Registrierung des Geräts mit demselben Benutzernamen wird ein Gerätename berücksichtigt – In dem Fall ist die E-Mail-Adresse keine gültige Benutzer-E-Mail-Adresse. Eine E-Mail-Adresse mit dem Gerätenamen plus der AD-Domäne gilt als Registrierungs-E-Mail-Adresse. Zum Initiieren der PowerShell-Ausführung muss der Administrator das Konto als LocalSystemAccount festlegen und als primäre Datei "setup.ps1" verwenden.
   Fall 2: Für die Registrierung des Geräts wird eine gültige Benutzer-E-Mail-Adresse berücksichtigt und es gelten keine Einschränkungen hinsichtlich der Modifizierung von Dateien am Gerätestandort – Verwenden Sie zur Registrierung die E-Mail-Adresse des angemeldeten Benutzers. Um diese Registrierung zu aktivieren, der Administrator das Konto als CurrentUserAccount festlegen und "setup.ps1" als primäre Datei für die Initiierung der PowerShell-Ausführung verwenden.
   Fall 3: Für die Registrierung des Geräts wird eine gültige E-Mail-Adresse berücksichtigt, und es gelten Einschränkungen hinsichtlich der Modifizierung von Dateien am Gerätestandort. Verwenden Sie für die Registrierung die E-Mail-Adresse des angemeldeten Benutzers. Dieser Fall enthält zwei untergeordnete Fälle:
   - Verwenden von zwei Skripten für die Registrierung – Erstellen Sie ein Verteilungspaket mit **setupEPMCopyContentsToTempFolderStep1.ps1** und führen Sie es über das Konto des aktuellen Benutzers aus. Die Dateien werden in einen temporären Speicherort kopiert. Erstellen Sie ein weiteres Verteilungspaket mit **setupEPMCopyContentsToTempFolderStep2.ps1** und führen Sie es über das Local System-Konto aus.

     > Gehen Sie wie folgt vor, falls der Gerätebenutzer Einschränkungen in Bezug auf das Modifizieren des Ordners mit den Paketdateien unterliegt: Kopieren Sie die Dateien in einen temporären Ordner, erstellen Sie die Benutzer-ID, und erstellen Sie ein PowerShell-Paket. Das PowerShell-Paket wird über das Skript **setupEPMCopyContentsToTempFolderStep2.ps1** ausgeführt. Nach der Installation wird der temporäre Ordner gelöscht.

   Benutzerkontensteuerung (UAC) aktivieren/deaktivieren

   1. Aktualisieren Sie den Registrierungseintrag, um die UAC-Steuerung zu deaktivieren und einen Neustart des Computers durchzuführen.
   2. Führen Sie das PowerShell-Paket über das Konto des aktuellen Benutzers und unter Verwendung von setup.ps1 aus.
   3. Aktualisieren Sie den Registrierungseintrag, um die UAC-Steuerung zu aktivieren und einen Neustart des Computers durchzuführen.

Erstellen Sie das PowerShell-Paket:

1. Überprüfen Sie, ob die erforderlichen Clients in Endpoint Manager vorhanden sind.
2. Kopieren Sie die Dateien in das Verzeichnis C:\Programme\LANDesk\ManagementSuite\LANDesk\files\. Erstellen Sie einen Unterordner in dem Ordner und extrahieren Sie die Dateien.
3. Erstellen Sie das Paket: **Verteilung > Verteilungspakete > Neu > Windows > PowerShell**.

   > Der Administrator kann die Pakete basierend auf der auf den Geräten festgelegten Restriktionsstufe an unterschiedliche Geräte verteilen.

4. Geben Sie im Abschnitt für die erste Datei den Paketnamen ein und laden Sie setup.ps1 aus dem Ornder hoch, der die kopierten Dateien enthält.
5. Kopieren Sie im Abschnitt für die zusätzlichen Dateien mithilfe von **Hinzufügen** die übrigen Dateien (außer dem Skript setup.ps1).
6. Wählen Sie im Bereich "Konten" das Konto des aktuellen Benutzers aus.
7. Klicken Sie auf **Speichern**.

4. Erstellen Sie die geplante Aufgabe:
    1. Wählen Sie das erstellte Paket aus, klicken Sie mit der rechten Maustaste und wählen Sie **Geplante Aufgabe(n) erstellen** aus. Es wird eine geplante Aufgabe erstellt.
    2. Ziehen Sie das Gerät in den Abschnitt für geplante Pakete.
    3. Klicken Sie mit der rechten Maustaste auf das geplante Paket und wählen Sie **Eigenschaften** aus.
    4. Überprüfen Sie das Paket.
    5. Wählen Sie als Tasktyp **Push** aus.
    6. Wählen Sie **Jetzt starten** aus und klicken Sie auf **Speichern**. Die geplante Aufgabe beginnt mit der Ausführung des Skripts. Bei erfolgreicher Ausführung wird der Status grün angezeigt.
5. Wechseln Sie zum Überprüfen der Geräteregistrierung zu **Einstellungen** > **Bereitstellungspaket hinzufügen oder entfernen** > **Details**. Alternativ hat der Administrator die Möglichkeit, eine Geräteregistrierung über die Diagnoseprotokolle des Geräts zu verifizieren.

7.5.8. Verwenden der Massenregistrierung für Windows-Geräte

Ivanti Neurons for MDMMit der Funktion zur Massenregistrierung können Sie schnell viele Android-Geräte in der Cloud registrieren.

Voraussetzungen:

- Benutzerkonten müssen in Ivanti Neurons for MDM unter Verwendung des Entra ID Premium Account importiert werden.
- Auf allen Geräten ist **Windows Configuration Designer** installiert.

Verfahren:

1. Verknüpfen Sie die Ivanti Neurons for MDM- und die Entra ID-Mandanten. Siehe **Verbinden von Entra ID mit UEM für Windows 10-Geräte**.
2. Öffnen Sie die App **Windows Configuration Designer** und wählen Sie **Desktopgeräte bereitstellen** aus. Ein Fenster für ein neues Projekt wird angezeigt.
3. Geben Sie folgende Details ein:
    - Name – Ein eindeutiger Name für Ihr Projekt.
    - Projektordner – Der Speicherort auf dem Gerät, an dem das Projekt gespeichert werden soll.
    - Beschreibung – Optionale Beschreibung des Projekts.

Klicken Sie auf **Fertig stellen**, um das Fenster für das neue Projekt zu schließen und eine Reihe von Schritten durchzuführen.

5. **Gerät einrichten**
   Geben Sie einen eindeutigen Namen für Ihre Geräte ein. Der Name kann die Seriennummer (%SERIAL%) oder willkürlich gewählte Zeichen enthalten.
6. Optional können Sie einen Produktschlüssel eingeben, wenn Sie Fenster aktualisieren, das Gerät für die gemeinsame Nutzung konfigurieren oder vorinstallierte Software entfernen möchten.
7. **Netzwerk einrichten**
   Optional können Sie die WLAN-Geräte konfigurieren, zu denen Sie beim ersten Starten eine Verbindung herstellen möchten. Falls keine Netzwerkgeräte konfiguriert werden, ist eine kabelgebundene Netzwerkverbindung beim ersten Starten des Geräts erforderlich.
8. **Kontoverwaltung**
   Wählen Sie **In Entra ID registrieren** aus, geben Sie ein Datum für den **Ablauf des Massentokens** ein und klicken Sie anschließend auf **Massentoken abrufen**.
9. Geben Sie Ihre Entra ID-Anmeldeinformationen ein, um einen Massentoken abzurufen.
10. Klicken Sie auf der Seite **Bei allen Apps angemeldet bleiben** auf **Nein, nur bei dieser App anmelden**.
    - Klicken Sie auf "Weiter", nachdem der Massentoken abgerufen wurde, und erstellen Sie das Paket.
    - Ein Benutzer mit Bereitstellungspaket wird im Azure-Portal erstellt – Benutzerprinzipalname (z. B. package_0ea893a5-1e93-4d21-a6b1-dc788946fd1d@miwinqe.onmicrosoft.com). Kopieren Sie die Datei (runtime ppkg tool) auf ein Speichergerät.

> Für den Entra ID-Benutzer der den Massentoken erstellt, und den Paketbenutzer sollte MFA nicht aktiviert sein. Zum Überprüfen müssen Sie OOBE + Entra ID für diesen Benutzer zusammenführen.

Erstellen Sie den (in Azure erstellten) Paketbenutzer neu oder synchronisieren Sie ihn mit Ivanti Neurons for MDM.

Führen Sie eine Massenregistrierung für ein Gerät durch, indem Sie das indem Bereitstellungspaket enthaltene Flash-Laufwerk verwenden. Sie können auch auf das vorhandene Gerät doppelklicken, um eine Post-OOBE-Erfahrung durchzuführen. Falls das Paket beim ersten Versuch nicht installiert werden konnte, wird auch der zweite Versuch fehlschlagen. Prüfen Sie, ob das neue Gerät in Ivanti Neurons for MDM erstellt wurde und ob Entra ID zum Paketbenutzer gehört.

7.5.8.1. Ivanti Massenregistrierung

Administratoren können (über ppkg) mehrere Windows-Geräte mit einem generischen Benutzer registrieren, der mit dem Präfix **windows-bulkenroll** beginnt, und die Benutzerzuweisung später vornehmen.

Voraussetzungen:

- Erstellen Sie auf Ivanti Neurons for MDM ein Benutzerkonto mit dem Präfix **windows-bulkenroll**, z. B. **windows-bulkenroll**-user1@abc.com, **windows-bulkenroll**-user2@abc.com.

Erstellen eines PPKG-Pakets mit Windows Configuration Designer

1. Laden Sie **Windows Configuration Designer** herunter und installieren Sie das Produkt.
2. Erstellen Sie ein neues Projekt.
3. Klicken Sie auf **Desktop bereitstellen**.
4. Geben Sie den Namen des Projekts ein und wählen Sie einen Pfad aus.
5. Geben Sie im Abschnitt **Gerät einrichten** den Gerätenamen ein.
6. Geben Sie im Abschnitt **Netzwerk einrichten** den Netzwerknamen ein (um das Netzwerk ggf. einzurichten; kann auch deaktiviert werden).
7. Wählen Sie im Abschnitt **Kontoverwaltung** die Option **Bei lokalem Admin registrieren** aus. Geben Sie **Benutzername** und **Kennwort** ein und klicken Sie auf **Weiter**.
8. Klicken Sie im Abschnitt **Anwendungen hinzufügen** auf **Weiter**.
9. Wählen Sie im Abschnitt **Zertifikate hinzufügen** die Option **Zu erweitertem Editor wechseln** aus und klicken Sie auf **Fortfahren** > **Ja**.
10. Wechseln Sie zu **Laufzeiteinstellungen** > **Arbeitsplatzregistrierungen**. Geben Sie den **UPN** ein (den Benutzer, den Sie in Ivanti Neurons for MDM im Abschnitt mit den erforderlichen Komponenten erstellt haben). Wählen Sie aus den folgenden Optionen:
    - AuthPolicy: OnPremise
    - DiscoveryServiceFullUrl: https://login.mobileiron.com
    - Secret: Geben Sie das Kennwort ein.

Klicken Sie auf **Datei** > **Speichern**.

12. Klicken Sie auf **Exportieren** > **Bereitstellungspaket**.
13. Klicken Sie in den nachfolgenden Bildschirmen auf **Weiter** und dann auf **Erstellen**.
    Die .ppkg-Datei wird am angegebenen Speicherort gespeichert.

Bereitstellen des Geräts im OOBE-Modus mit ppkg

Stellen Sie die Geräte mit der neu erstellten .ppkg-Paketdatei aus dem obigen Abschnitt bereit. Nachdem das Gerät registriert wurde und der Check-in erfolgreich war, ist der Geräteeintrag auf dem MDM-Server mit dem Benutzer und dem Präfix **windows-bulkenroll** sichtbar.

Gerät einem Benutzer zuweisen

1. Klicken Sie auf der Seite "Geräte" auf den Benutzer mit dem Präfix **windows-bulkenroll**.
2. Klicken Sie auf **Einem Benutzer zuweisen**. Das Fenster "Einem Benutzer zuweisen" wird angezeigt.

3. Wählen Sie das Gerät in der Liste aus oder suchen Sie nach dem Gerät.
4. Wählen Sie das gewünschte Gerät aus.
5. Klicken Sie auf **Einem Benutzer zuweisen**. Das ausgewählte Gerät wird dem Benutzer zugewiesen.

Wenn sich der Benutzer zum ersten Mal am Gerät anmeldet, muss das Kennwort geändert werden.

> Die Option "Einem Benutzer zuweisen" ist nur für Geräte verfügbar, die über die Ivanti Massenregistrierung registriert wurden.

> Für die in dieser Kategorie registrierten Geräte funktionieren nur Konfigurationen und Anwendungen auf Geräteebene. Konfigurationen und Anwendungen auf Benutzerebene werden nicht unterstützt.

7.5.9. Passworteinstellungen ändern

Dieser Abschnitt enthält die folgenden Themen:

- Konfiguration des zugewiesenen Passcodes ändern
- Eine andere Passcode-Konfiguration zuweisen

Passcode_Settings.htmVerwenden Sie die einem Gerät zugewiesene Passwortkonfiguration, um die Passworteinstellungen zu ändern. Sie haben folgende Möglichkeiten:

- Ändern der Einstellungen für die zugewiesene Konfiguration

ODER

- Zuweisen einer anderen Passwortkonfiguration

Änderungen, die Sie an der Konfiguration vornehmen, wirken sich auf alle Geräte aus, denen die Konfiguration zugewiesen ist.

Konfiguration des zugewiesenen Passcodes ändern

Verfahren

1. Gehen Sie zu **Geräte**.
2. Suchen Sie den Eintrag des Geräts in der Liste.
3. Klicken Sie in der Spalte **Name** auf den Link.

> Wenn eine Passwortkonfiguration zugewiesen wurde, wird diese in der Registerkarte „Konfigurationen“ angezeigt.

Klicken Sie in der Registerkarte „Konfigurationen“ auf den Link Passwortkonfiguration.

5. Klicken Sie (oben rechts) auf **Bearbeiten**.
6. Nehmen Sie die entsprechenden Änderungen vor.

Eine andere Passcode-Konfiguration zuweisen

Verfahren

1. Vergewissern Sie sich, dass jemand die von Ihnen benötigte Konfiguration erstellt hat.
2. Gehen Sie zu **Geräte**.
3. Suchen Sie den Eintrag des Geräts in der Liste.
4. Klicken Sie in der Spalte **Name** auf den Link.

7.5.10. Den Gerätenamen ändern

Administratoren können den Namen eines Geräts manuell ändern (wenn sie nicht die Konfiguration zur Bearbeitung des Gerätenamens verwenden).

Gilt für:

- überwachte iOS-Geräte
- überwachte tvOS-Geräte
- Geräte mit macOS 10.10+

Verfahren

1. Gehen Sie zu **Geräte**.
2. Suchen Sie den Eintrag des Geräts in der Liste.
3. Führen Sie eine der folgenden Schritte aus:
    - Fügen Sie die Spalte **Gerätename** hinzu, falls noch nicht vorhanden, indem Sie rechts auf das Zahnradsymbol für die Einstellungen klicken und **Gerätename**auswählen.
    - Klicken Sie auf den Link in der Spalte **Name**, um die Seite mit den Gerätedetails aufzurufen.
4. Klicken Sie neben dem Gerätenamen auf das Stiftsymbol Bearbeiten.
5. Geben Sie einen neuen Gerätenamen ein und klicken Sie auf das Häkchensymbol.
6. Überprüfen Sie im Anzeigefeld „Gerätename überschreiben“ die Hinweise und klicken Sie auf **OK**.

Der neue Name wird per Push an das Gerät übertragen, sobald es sich das nächste Mal anmeldet. Diese Aktion kann nicht rückgängig gemacht werden.

> Wenn zuvor eine Konfiguration für den Standard-Gerätenamen definiert wurde, überschreibt diese Aktion den in der Konfiguration festgelegten Namen.

7.5.11. Suchen nach und Filtern von Geräten

Dieser Abschnitt enthält die folgenden Themen:

- Gerät suchen
- Nach Geräten filtern
- Erweiterte Suche verwenden
- Suchanfragen laden

Gerät suchen

Das Ivanti Neurons for MDM-Administrationsportal zeigt die Anzahl doppelter Benutzergruppen und die zugehörige Anzahl der GUIDs an, damit doppelte Gruppen identifiziert werden können, wenn das Attribut "Name der Benutzergruppe" im Regeleditor ausgewählt wird. Eine Tabelle unter dieser Regel zeigt außerdem die Liste der doppelten Benutzergruppen zusammen mit Details wie Name der Benutzergruppe, GUID, Quelle und Distinguished Name (DN).

Verfahren

1. Gehen Sie zu **Geräte**.
2. Geben Sie den Gerätenamen in das Feld **Suchen** ein. Alle Geräte, die die eingegebenen Zeichen enthalten, werden angezeigt.

Nach Geräten filtern

In der seitlichen Navigationsleiste "Filter" sind verschiedene Abschnitte aufgelistet, die Ihnen die Suche nach einem bestimmten Gerät erleichtern. Der Assistent "Filter verwalten" enthält eine Liste aller Abschnitte, die Sie in der Filter-Navigationsleiste anzeigen können.

Verfahren

1. Gehen Sie zu **Geräte**.
2. Markieren Sie die entsprechenden Kontrollkästchen in den Abschnitten, die in der seitlichen Filter-Navigationsleiste aufgeführt sind.
   Beispiel:
   - Wählen Sie in dem Abschnitt „Benutzer aktiviert“ Ja aus, um nur die Geräte anzuzeigen, deren Benutzer aktiviert sind.
   - Wenn Sie Geräten angepasste Attribute zugewiesen haben, können Sie die Geräte nach diesen Attributen filtern, indem Sie auf das Symbol für die Einstellungen (oben rechts) klicken.
   - Wählen Sie in dem Statusabschnitt Außer Dienst gestellt und iOS aus, um nur außer Dienst gestellte iOS-Geräte anzuzeigen.

(Optional) Klicken Sie auf **Standardeinstellungen wiederherstellen**, um die Auswahl auf die Standardfilter zurückzusetzen. In der Filter-Navigationsleiste werden die ausgewählten Abschnitte angezeigt. Wenn Sie alle Kontrollkästchen im Assistenten "Filter verwalten" deaktivieren, werden in der seitlichen Filter-Navigationsleiste alle Abschnitte angezeigt.

4. Klicken Sie in einen Bereich außerhalb des Assistenten "Filter verwalten", um den Assistenten zu beenden.
5. (Optional) Klicken Sie auf das X-Symbol, um die seitliche Filter-Navigationsleiste zu schließen. Durch Klicken auf **Filter** können Sie die seitliche Navigationsleiste erneut aufrufen.
   - Falls Sie eines der Stoppwörter verwenden, die in der Datei "stopwords.txt" der Apache SOLR-Serverkonfiguration aufgeführt sind, werden die Wörter nicht indiziert. Deshalb werden die Entitäten, die die Stoppwörter enthalten, nicht bei den Suchergebnissen angezeigt.

- Beispiele für Entitäten sind Geräte, Benutzer, Gruppen, Attribute, Anwendungen, Zertifikate, Auditprotokolle, Content und Benachrichtigungsmodule.
- Beispiele für Stoppworte sind ein, einer, wenn, sein, in usw.

Erweiterte Suche verwenden

Mit der Option "Erweiterte Suche" können Sie anhand von Regeln nach einem Gerät suchen, um Geräte mit bestimmten Kriterien zu identifizieren und anzuzeigen. Diese Regeln können unter Verwendung der anwendbaren Operatoren erstellt werden, beispielsweise mit den Operatoren „beginnt mit“, „endet mit“, „enthält“, „enthält nicht“, „beginnt nicht mit“, „endet nicht mit“, „ist kleiner als „‚“ ist größer als „‚“ liegt im Bereich „‚„‚ „ist gleich“ und „ist nicht gleich“. Die Regeln können miteinander mit den Optionen ANY (OR) oder ALL (AND) verschachtelt werden. Mit den Regeln übereinstimmende Geräte werden unterhalb des Abschnitts angezeigt.

Ivanti Neurons for MDMDer Cloud-Administrator zeigt die Anzahl doppelter Benutzergruppen und die zugehörige Anzahl der GUIDs an, damit doppelte Gruppen identifiziert werden können, wenn das Attribut "Name der Benutzergruppe" im Regeleditor ausgewählt wird. Eine Tabelle unter dieser Regel zeigt außerdem die Liste der doppelten Benutzergruppen zusammen mit Details wie Name der Benutzergruppe, GUID, Quelle und Distinguished Name (DN).

Verfahren

1. Klicken Sie auf der Seite "Geräte" auf den Link **Erweiterte Suche**. Der Assistent für die erweiterte Suche wird aufgerufen.
2. Klicken Sie auf eine der folgenden Optionen:
   - Klicken Sie auf Beliebig, wenn die Geräte mindestens eine der Richtlinien erfüllen sollen.
   - **Alle** – Klicken Sie hier, wenn die Geräte alle Regeln erfüllen sollen.

Erstellen Sie eine Regel, die diese Suchkriterien definiert. Beispiel: 'APNS-Fähigkeit ist gleich Ja'.

4. (Optional): Klicken Sie auf +, um weitere Richtlinien zu erstellen.
5. Klicken Sie auf **Suchen**. Die Liste der Geräte, die den Suchkriterien entsprechen, wird auf der Seite angezeigt.
   - Für Geräte mit iOS 14.0+ ist die eSIM-ID (EID) eines Geräts auf der Gerätedetailseite verfügbar. Über die eSIM-ID (EID) können Provider die SIM-Karte einem bestimmten Gerät zuordnen. Das Feld eSIM ID (EID) ist DSGVO-konform.
   - Ivanti Neurons for MDMDa neue DSGVO-Felder (wie IP-Adresse und eSIM-ID) im Laufe der Releases hinzugefügt werden, müssen Admins, die DSGVO bereits konfiguriert haben, das DSGVO-Profil bearbeiten, wenn sie die neuen Felder ausblenden wollen.
   - Die erweiterte Suche zeigt den Status der Wiederherstellungssperre eines Geräts.

Suchanfragen laden

Liste der gespeicherten Suchanfragen anzeigen.

Verfahren

1. Klicken Sie auf "Erweiterte Suche" und dann auf das Ordnersymbol. Die Liste der erstellten Suchanfragen wird im Abschnitt **Abfrage laden** angezeigt.
   - **Abfragename** - Der Name der geladenen Abfrage.
   - **Abfrageinhalt** - Zeigt den Inhalt der Regeln an, die die Suchabfrage definieren.
   - **Aktionen** - Wählen Sie die Aktion aus, die mit der Abfrage ausgeführt werden soll.
2. Klicken Sie in der Spalte **Aktionen** auf **Abfrage laden**, um die Liste der Geräte anzuzeigen, die die in der geladenen Abfrage definierten Kriterien erfüllen.

3. Klicken Sie auf **Löschen**, um eine geladene Abfrage zu löschen.

7.5.12. Geräteeigentümer verwenden

Dieser Abschnitt enthält die folgenden Themen:

- Bereitstellen von Android Enterprise-Geräten unter Verwendung eines QR-Codes oder NFC-Bumps
- Bereitstellen von Android Enterprise-Geräten unter Verwendung eines Client-Tokens

Lizenz: Gold

Sie können Geräte als "Unternehmenseigentum" oder "Mitarbeitereigentum" kennzeichnen, sobald diese Geräte registriert sind. Diese Kennzeichnung hilft Ihnen bei der Verwaltung von Richtlinien, die davon abhängen, ob der Benutzer ein eigenes oder ein unternehmenseigenes Gerät verwendet. Mit der richtigen Lizenz können Sie dann den Eigentümerstatus in Regeln verwenden, mit denen Sie Gerätegruppen erstellen.

Bei einem neuen oder auf die Werkseinstellungen zurückgesetzten Gerät stellen Sie den Geräteeigentümermodus mit der APP Provisioner und einer der folgenden Optionen bereit:

- NFC-Bump (Nahfeldkommunikation)
- QR-Code

Bei einem sogenannten NFC-Bump drücken Sie das Mastergerät oder ein als Vorlage verwendetes Gerät gegen ein neues oder auf die Werkseinstellungen zurückgesetztes Gerät, um das neue Gerät zu konfigurieren.

Zum Einscannen eines QR-Codes müssen Sie gegebenenfalls auf den Bildschirm eines neuen oder auf die Werkeinstellungen zurückgesetzten Geräts tippen, ein WLAN konfigurieren und den Code einscannen, wenn das Gerät für die Bereitstellung vorbereitet ist.

Während der Bereitstellung im Geräteeigentümer-Modus mit NFC- oder QR-Code akzeptiert die Bereitsteller-App ein Registrierungstoken. Bei der Registrierung wird das Registrierungstoken an den Server gesendet. Wenn es auf dem Server vorhanden ist und das Gerät einem Benutzer zugewiesen wird, ist das Gerät erfolgreich registriert.

Der GO-Client kontrolliert das Gerät, sobald es im Geräteeigentümermodus arbeitet, und sperrt sich für den Bildschirm, bis das Gerät in der Cloud registriert ist, damit die Benutzer den Bereitstellungsprozess nicht verlassen können. Der Geräteeigentümermodus unterstützt auch den Kiosk-Modus. Informationen zur Konfiguration finden Sie unter: Sperre und Kioskkonfiguration .

Wichtig

- Wenn Sie ein Gerät im Geräteeigentümermodus abschalten, wird das Gerät auf die Werkeinstellungen zurückgesetzt.
- Für alle Geräte im Geräteeigentümermodus können optional alle System-Apps aktiviert werden.
- Ein Gerät kann immer nur einen aktiven Geräteeigentümer haben.
- Nur Geräte, die für Android Enterprise geeignet sind, können Geräte im Geräteeigentümermodus starten.
- Bei Samsung-Geräten mit Knox-Standard im Geräteeigentümermodus werden die Benutzer aufgefordert, die Samsung-ELM-Lizenz zu aktivieren. Diese Aufforderung erscheint auch auf Samsung-Geräten im Geräteeigentümermodus, wenn Sie ein Upgrade des GO-Clients einer älteren Version auf die aktuelle Version durchführen, die von der Cloud unterstützt wird. Nach der Aktivierung wird die Seriennummer auf der Seite mit den Gerätedetails angezeigt. Sie stimmt mit der Anzeige in dem Feld Gerät > Einstellungen > Seriennummer überein.

Bereitstellen von Android Enterprise-Geräten unter Verwendung eines QR-Codes oder NFC-Bumps

Zum Bereitstellen von Android Enterprise-Geräten unter Verwendung eines QR-Codes oder NFC-Bumps müssen Sie die Provisioner-App von Google Play auf das Mastergerät herunterladen und installieren.

Kompatible Komponenten

Provisioner-Version: 1.3.0.

Der MobileIron Provisioner ist kompatibel bzw. funktioniert mit folgenden Versionen:

Objekt	[Version]
Android OS (auf dem bereitzustellenden Gerät)	• 5.0 - oder unterstützte neuere Versionen ist bei Verwendung von NFC erforderlich. • 7.0 - oder unterstützte neuere Versionen ist bei Verwendung des QR-Codes erforderlich. Das Gerät muss für Android Enterprise geeignet sein.
Android-Betriebssystem (auf dem Mastergerät)	5.1 - bis zur letzten freigegebenen Version. Für NFC-Bump muss das Gerät NFC-fähig sein. Bei Verwendung des QR-Codes ist dies nicht erforderlich.
UEM-Serverprodukt, aktiviert für Android Enterprise	Geben Sie eine der folgenden Optionen ein: Ivanti Neurons for MDM oder als zulässig beschriftetes Ivanti Neurons for MDM.
Android Client App	Die aktuelle Version der Client-App wird durch den Provisioner automatisch auf dem bereitgestellten Gerät installiert.

Voraussetzungen

Um ein Android Enterprise-Gerät als vom Unternehmen verwaltetes Gerät bereitzustellen, müssen Sie:

- sicherstellen, dass die benötigte Konfiguration für Android Enterprise definiert ist und für das registrierte Gerät verwendet wird.

> Die Standardkonfiguration "Android Enterprise: Gerät mit firmenseitiger Verwaltung" muss für das Gerät aktiviert sein.

Android Enterprise auf dem Server aktivieren

- Ein NFC-fähiges Android-Gerät (nur bei Verwendung von NFC) als Master-Gerät bereithalten, auf dem die App MobileIron Provisioner installiert ist.
- über für Android Enterprise geeignete Geräte verfügen, die bereitgestellt werden sollen

Um Android Beam für NFC Bump zu aktivieren:

Verfahren

1. Gehen Sie auf dem Gerät zu **Einstellungen**.
2. Gehen Sie zu **Netzwerke > Drahtlose Netzwerke**.
3. Wählen Sie in dem Abschnitt **Konnektivität** die Option **Teilen & Verbinden** aus.
4. Schieben Sie den **NFC-**Schalter auf **ON**.
5. Schieben Sie den Schalter für **Android Beam** auf **ON**.

Die Schritte zur Aktivierung von Android Beam und NFC können je nach Gerät abweichen.

Bereitstellen von Android Enterprise-Geräten, um sie firmenseitig zu verwalten

Verfahren

1. Laden Sie die Provisioner-App aus Google Play auf das Android Master-Gerät herunter und installieren Sie die App.
2. Starten Sie den Provisioner auf dem Mastergerät.
3. Wählen Sie als Bereitstellungsmethode „NFC“ oder „QR-Code“ aus.
4. Tippen Sie auf die **bereitzustellende App** und wählen Sie die Client-App, die Sie auf dem bereitgestellten Gerät installieren wollen:

Wählen Sie diese Client App:	**Zur Registrierung mit folgendem UEM-Server:**
Los	Ivanti Neurons for MDM
At Work UEM	(als zulässig beschriftetes) Ivanti Neurons for MDM

5. Füllen Sie die übrigen Felder in der Provisioner-App aus. Manche Felder werden automatisch ausgefüllt, wenn ein unterstütztes WLAN erkannt wird. Die WLAN-Felder werden nicht angezeigt, wenn Sie als Option "QR-Code" ausgewählt haben. Beachten Sie die folgenden Richtlinien:

Feld	**Wert**
Wählen Sie die App für die Bereitstellung aus.	Go- oder At Work-App
Zeitzone	Geben Sie die Zeitzone ein, die für das Gerät konfiguriert werden soll.
Region	Geben Sie die Regions- und Spracheinstellungen ein, die für das Gerät konfiguriert werden sollen.
Alle System-Apps aktivieren.	Klicken Sie in das Kontrollkästchen, um alle System-Apps zu aktivieren.
WLAN SSID	Geben Sie SSID des WLANs ein, die das Mastergerät verwenden soll.
WLAN-Sicherheitsprotokoll	Geben Sie das WLAN-Sicherheitsprotokoll ein.
WLAN-Passwort	Geben Sie das Passwort für das WLAN ein.
Massenregistrierung	Die Funktion zur Massenregistrierung ist optional. Wenn Sie die Massenregistrierung verwenden wollen, müssen Sie einen Hostnamen eingeben. Sie können auch einen Benutzernamen eingeben und dann die Schnellstartoption auswählen. Um die Funktion zur Massenregistrierung zu überspringen, sollten Sie diese Felder leer lassen.

6. Tippen Sie auf **Weiter**.
7. Wenn Sie als Option **NFC** ausgewählt haben, tippen Sie auf **Weiter**. Der Bildschirm **NFC-Bump** wird auf dem Mastergerät angezeigt. Verfahren Sie wie im Abschnitt **NFC Bump** beschrieben.
8. Wenn Sie **QR-Code** ausgewählt haben, wird auf dem Mastergerät der Bildschirm **Diesen QR-Code scannen** angezeigt. Setzen Sie wie im Abschnitt **QR-Code** beschrieben fort.

Führen Sie die Schritte unten für den NFC-Bump aus.

Überprüfen Sie, ob das Zielgerät den Android Begrüßungsbildschirm anzeigt.

9. Halten Sie das Master-Gerät mit dem Rücken gegen das Zielgerät, um eine NFC-Übertragung zu beginnen. Wenn die NFC-Übertragung erfolgreich war, gibt das Zielgerät einen Piepton aus und lädt anschließend die ausgewählte Client-App herunter. Wenn keine WLAN-Verbindung aufgebaut wird oder das Gerät die Client-App nicht herunterladen kann, wird das Gerät automatisch auf die Werkeinstellungen zurückgesetzt.
10. Wenn Sie einen Piepton hören oder eine andere Anzeige außer dem Begrüßungsbildschirm sehen, können Sie die Geräte entkoppeln. Dies dauert in der Regel einige Sekunden. Wenn das Gerät nicht verschlüsselt ist, verschlüsselt es sich zunächst, bevor es mit dem nächsten Vorgang fortsetzt.
11. Sie können weitere Geräte durch „NFC-Bump“ der Geräte mit dem Master-Gerät bereitstellen. Das Zielgerät muss den Begrüßungsbildschirm anzeigen, und auf dem Mastergerät muss der Bildschirm "NFC-Bump" angezeigt werden.

Führen Sie zur Bereitstellung mit QR-Code die Schritte unten aus.

Überprüfen Sie, ob das Zielgerät den Android Begrüßungsbildschirm anzeigt.

12. Tippen Sie auf dem Begrüßungsbildschirm in Android auf dem Zielgerät sechsmal auf die gleiche Stelle des Bildschirms.
13. Sie werden aufgefordert, ein WLAN zu konfigurieren, damit der Setup-Assistent einen QR-Code-Scanner auf das Zielgerät herunterladen kann.
14. Sobald der QR-Code-Scanner heruntergeladen ist, wird die Kamera gestartet.
15. Halten Sie das Zielgerät in einigen Zentimetern Abstand zum Master-Gerät, bis der QR-Code erfolgreich gescannt wurde. Der Setup-Assistent lädt dann die Client-App herunter. Wenn der Assistent die Client-App nicht herunterladen kann, wird automatisch ein Reset auf die Werkeinstellungen durchgeführt.
16. Sie können zusätzliche Geräte bereitstellen, indem Sie den QR-Code auf dem Master-Gerät einscannen. Das Zielgerät muss über eine scanbereite Kamera verfügen und auf dem Mastergerät muss "Diesen QR-Code scannen!" angezeigt werden.
17. Sie können den QR-Code auch exportieren, indem Sie auf das Teilen-Symbol tippen. Die Optionen für den Export sind je nach Gerät unterschiedlich.

Bereitstellen von Android Enterprise-Geräten unter Verwendung eines Client-Tokens

Sie können ein Android Enterprise-Gerät im Geräteeigentümermodus bereitstellen, wenn Sie anstelle des NFC-Bumps oder des QR-Codes ein Client-Token verwenden. Bei diesen Verfahren können Sie sich auf einem Gerät mit einem Token anmelden; das erleichtert die automatische Installation der GO- oder At Work-App als Client und die Bereitstellung im Geräteeigentümermodus:

> Branded Client-Token werden auf Geräten unterstützt, die mit verwalteten Google Play-Konten bereitgestellt werden und Android 6 oder unterstützte neuere Versionen verwenden. Weitere Details finden Sie in der Entwickleranleitung für Android UEM. https://developers.google.com/android/work/prov-devices#Key_provisioning_differences_across_android_releases.

Voraussetzungen für dieses Verfahren:

- Sie müssen mit einem Android Enterprise-Konto registriert sein.
- Das Gerät muss für Android Enterprise geeignet sein.
- Auf dem Gerät muss mindestens Android 6 mit der aktuell freigegebenen Version laufen.
- Sie müssen ein neues oder auf die Werkeinstellungen zurückgesetztes Gerät haben.

Konfiguration (für Geräte mit Android 5.0+)

Verfahren

1. Gehen Sie im Ivanti Neurons for MDM-Portal zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Wählen Sie **Sperre und Kiosk: Android Enterprise** aus.
4. Die Seite **Sperre und Kiosk: Konfiguration für Android Enterprise erstellen** wird angezeigt.

Geben Sie einen Konfigurationsnamen und die Beschreibung ein.

5. Wählen Sie eine Sperrart aus.

Klicken Sie auf **Verwaltete Geräte (Geräteeigentümer)**.

6. Die Einstellungsoptionen für die Sperre des Android-Geräteeigentümers werden angezeigt.

Optional können Sie auch folgende Einstellungen auswählen:

- WLAN oder WLAN-Einstellungen deaktivieren
- Kamera deaktivieren
- Bluetooth deaktivieren
- Bluetooth-Einstellungen nicht zulassen
- Screenshots deaktivieren
- Hauptlautstärke stummschalten
- Apps-Kontrolle verweigern
- Anmeldeinformationen nicht zulassen
- Notfallrundsendungen nicht zulassen
- Mobile Netzwerke nicht zulassen
- Internetweiterleitung nicht zulassen
- VPN nicht zulassen
- Reset auf Werkeinstellung nicht zulassen
- Zurücksetzen auf die Werkseinstellungen aktivieren

> Sie können auch eine Liste autorisierter Google-Konto-IDs (als Ganzzahl) angeben, mit denen das Gerät nach einem Reset auf die Werkseinstellungen bereitgestellt werden kann, oder den Mauszeiger über dem Hilfesymbol bewegen, wenn Sie nicht wissen, wie Sie autorisierte Konto-IDs laden.

Kontoänderungen verweigern

- NFC deaktivieren (abgehender Beam)

- Abgehende Gespräche nicht zulassen
- Sicherer Start nicht zulassen
- Standortfreigabe verweigern
- Debugging-Funktionen nicht zulassen
- Apps-Verifizierung sicherstellen
- SMS nicht zulassen
- Einschalten des Mikrofons nicht zulassen
- Automatische Zeit nicht zulassen
- Automatische Zeitzone nicht zulassen
- Daten-Roaming deaktivieren
- Automatische WLAN-Deaktivierung nicht zulassen
- Eingabemethoden beschränken
- Zugangsdienste beschränken
- USB-Dateitransfer deaktivieren
- Externe Medien deaktivieren
- Keyguard deaktivieren (ohne Wirkung, wenn PIN/Passcode eingestellt ist)
- Bildschirm bei Verbindung mit Ladegerät eingeschaltet lassen
- Erstellung von Fenstern nicht zulassen
- Hinweise für neue Anwender überspringen

Im Abschnitt **System-Apps aktivieren/deaktivieren** können Sie optional auswählen, welche der folgenden System-Apps Sie aktivieren oder deaktivieren wollen:

7. Optional können Sie den **Kiosk-Modus** aktivieren.

Objekt	[Version]
Voreingestellte System-Apps	
Integrierte Kamera	Klicken Sie auf die Umschaltfläche, um die integrierte Kamera-App **EINZUSCHALTEN** oder **AUSZUSCHALTEN**.
Integriertes Telefon	Klicken Sie auf die Umschaltfläche, um die integrierte Telefon-App **EINZUSCHALTEN** oder **AUSZUSCHALTEN**.
Paket-ID der System-App	Um andere als die voreingestellten System-Apps zu aktivieren oder zu deaktivieren, klicken Sie auf das + (Plus)-Symbol und ergänzen die Paket-ID der System-App. Klicken Sie zum Entfernen der System-App auf das –(minus)-Symbol.

Folgende Einstellungen werden angezeigt:

- Aufgaben-Sperr-Modus aktivieren
- Kiosk-Modus automatisch aufrufen (nur bei der Erstkonfiguration)

- Schnelleinstellungen deaktivieren
- Benutzerzugang für WLAN-Einstellungen zulassen
- Benutzerzugang für Bluetooth-Einstellungen zulassen
- Benutzerzugang für Standort-Einstellungen zulassen
- Verzögerung der Anwendungs-Updates durch Benutzer zulassen
- Benutzer darf auf Zugriffsdatums- und -zeiteinstellungen zugreifen.
- Benutzer darf auf mobile Netzwerkeinstellungen zugreifen.
- Sprachauswahl dem Benutzer überlassen
- Freigegebenes Gerät aktivieren (eine der folgenden Optionen auswählen)
  - Anmelden erlauben
  - Abmeldung aktivieren (Zeitüberschreitung in Stunden eingeben)

Sie können auch die Standard- oder kundenspezifischen Branding-Optionen aus der Dropdown-Liste auswählen.

8. Sie können optional auch einen Kiosk-Exit-PIN erstellen, um den Kioskmodus zu verlassen.
9. Sie können auch eine Whitelist der Apps erstellen, die den Benutzern im Kiosk-Modus angeboten werden.

Gerät bereitstellen

Verfahren

1. Schalten Sie das Gerät ein und geben Sie Ihr WLAN-Passwort ein. Ihr Gerät verlangt von Ihnen ggf. die Eingabe eines anderen Passworts.
2. Geben Sie im Bildschirm **Konto verifizieren** das Token für Android Enterprise ein. Klicken Sie auf **Weiter**.
3. Klicken Sie in dem Bildschirm **Google-Dienste** auf **Installieren**.
4. Akzeptieren Sie die Nutzungsbedingungen.
5. Klicken Sie in dem Setup-Bildschirm für das vom Unternehmen verwaltete Gerät auf **Weiter**. Der GO- oder At Work-Client wird heruntergeladen und auf dem Gerät installiert. Das Gerät schaltet dann um in den Geräteeigentümermodus.

Verwandte Themen

- Verwendung der Massenregistrierung für Android
- Gerätegruppen

7.5.13. Verwaltetes Gerät mit Arbeitsprofil

Verwaltetes Gerät mit Arbeitsprofil auf unternehmenseigenem Gerät ist ein Modus in Android Enterprise, bei dem das Gerät ein unternehmenseigenes Gerät ist, bei dem die privaten Daten vom Rest getrennt sind. Dieser Modus unterstützt zwei Profile: Sie können betriebliche Apps in dem verwalteten Profil bereitstellen und dem Benutzer erlauben, private Apps und Daten zu speichern. Der Modus „Verwaltetes Gerät mit Arbeitsprofil auf unternehmenseigenem Gerät" wird erstellt, indem eine Konfiguration „Verwaltetes Gerät mit Arbeitsprofil" an ein Gerät verteilt wird, das im Modus „Gerätebesitzer" bereitgestellt ist.

Weitere Informationen über verwaltete Geräte mit Arbeitsprofil-Sperreinstellungen finden Sie unter **Sperre & Kiosk: Android Enterprise**.

> Dieser Modus erfordert mindestens Android 8.0 bzw. die letzte freigegebene Version.

Auf dem verwalteten Gerät mit Arbeitsprofil können App-Konfigurationen, Apps, die Widgets profilübergreifend verwenden, Client-Zertifikat Aliasnamen und ID-Zertifikate verwendet werden.

Die folgenden Konfigurationen gelten für verwaltete Geräte mit Arbeitsprofil:

- Erweiterter Passcode
- Always On VPN
- Zertifikat
- Identitätszertifikat
- Google-Konto
- Passwort
- Telefoneinschränkungen bei Samsung-Mobiltelefonen
- Bedrohungsabwehr
- WLAN
- Standard-App-Runtime-Berechtigungen
- SafetyNet-Attestierung
- Passwort
- Lokale Aktionen von Threat Defense

7.5.14. Verwendung der Massenregistrierung für Android

Mit der Funktion zur Massenregistrierung können Sie schnell viele Android-Geräte in der Cloud registrieren.

Lizenz: Silver

Führen Sie die folgenden Aufgaben aus, bevor Sie die Massenregistrierung verwenden:

1. Installieren Sie Android SDK mit der Android Debug Bridge (adb) auf dem Computer, mit dem Sie die Geräte registrieren. http://developer.android.com/tools/help/adb.htmlWeitere Informationen zur Android Debug Bridge finden Sie unter: http://developer.android.com/tools/help/adb.html.
2. USB-Debugging aktivieren.
   Die Schritte zur Aktivierung des USB-Debugging auf Android-Geräten sind je nach Android-Release unterschiedlich.
   Informationen zur Aktivierung des USB-Debugging siehe: http://developer.android.com/tools/device.html.
3. Installieren Sie den GO-Client auf jedem Gerät.
4. Verbinden Sie die Geräte über USB-Kabel mit dem Computer, mit dem Sie die Geräte registrieren.

Go kann gestartet und mit der Shell Android Debug Bridge (adb) bei einem Server registriert werden. Die Android Debug Bridge ist ein Tool, das Sie über die Befehlszeile in Windows oder über das Terminal in iOS aufrufen können. Sie können damit mit einem verbundenen Android-Gerät kommunizieren. Für die adb-Shell gilt folgendes Befehlsformat:

> 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

> Mit dem Registrierungsprotokoll (mirp) werden relevante Daten für die Registrierung kodiert.

Gültige Schlüssel und gültige Werte sind:

Schlüssel	Wert
Benutzer	Die E-Mail-Adresse des Benutzers, die bei Verwendung von iReg in das Feld für den Benutzernamen eingetippt werden müsste. Erforderlich.
Passwort	Benutzerpasswort
pin	Registrierungs-PIN für den Benutzer
quickStart	**Bei der Einstellung auf TRUE: wird der Begrüßungsbildschirm nur kurz angezeigt.** Die Willkommensseite ändert sich, sobald nach der Animation die Schaltfläche "Weiter" angezeigt wird, ohne dass der Benutzer auf "Weiter" tippen muss. Diese rationelle Bereitstellung gilt zudem für alle Geräte: • Die Aufforderungen zu Datenschutz und Tastenkombinationen für den Benutzer werden übersprungen. • On zebra devices, the client shall grant admin privileges to itself without a user prompt. Als Version ist mindestens Version Zebra MX 4.3 erforderlich **Bei Einstellung auf FALSE: wird der Begrüßungsbildschirm wie üblich angezeigt, der Benutzer muss auf der Willkommensseite auf die Option ''Weiter'' tippen.** Optional, die Standardeinstellung ist FALSE.

> Für die Massenregistrierung muss ein Passwort, eine PIN oder ein Token verwendet werden.

Dieser Beispielbefehl definiert einen Server, Benutzer, ein Passwort, die PIN und 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

Beispielskript für die Massenregistrierung

Sie können dieses Skript als Beispiel verwenden und daraus Ihr eigenes Skript für die Massenregistrierung entwickeln. Dieses Beispielskript registriert alle mit dem Bereitstellungscomputer verbundenen Geräte mit dem gleichen Benutzer und dem gleichen Passwort.

```
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
```

Potenzielle Fehlermeldungen

Hier einige mögliche Fehlermeldungen, die bei der Massenregistrierung auftreten können.

Fehler	Lösung
mirp scheme not found	Beispiel für einen Befehl mit Mirp-Schema: am start -a android.intent.action.MAIN -d“xxxmirp://?
URL ungültig	Diese Meldung wird angezeigt, wenn kein Datenstring versendet wird. Überprüfen Sie, ob die URL korrekt ist.
Keine Serverinformationen gefunden	Die Serverinformationen fehlen oder wurden falsch eingegeben.
Keine Benutzerinformationen gefunden	Überprüfen Sie, ob der Benutzerschlüssel eingegeben wurde.
Kein Passwort/keine PIN gefunden	Überprüfen Sie, ob eine PIN oder ein Passwort eingegeben wurde.

Wenn mehrere Profile für die Massenregistrierung erstellt wurden:

- Ein nativ registriertes, vollständig verwaltetes Android Enterprise-Gerät erhält das benutzerdefinierte Attribut, das für das erste Profil erstellt wurde.
- Wenn ein Gerät beim Migrieren von Geräten in einem Massenregistrierungsprofil enthalten ist, werden die für das betreffende Gerät definierten, benutzerdefinierten Attribute bei der Migration auf das Gerät angewendet. Dieses Verhalten ist identisch für das migrierte, vollständig verwaltete Android Enterprise-Gerät, da dieses das benutzerdefinierte Attribut des ersten Profils erhält.

Alle für das betreffende Gerät erstellten Profile gelten außerdem als aktiv.

7.5.15. Massenregistrierung mit CSV-Dateiupload

Mit der Massenregistrierung können Sie mehrere Android-Geräte durch Verwendung der Gerätekennungen registrieren. Sie können die CSV-Datei hochladen, um Geräte in großer Zahl hinzuzufügen.

Verfahren

1. Klicken Sie auf der Seite **Geräte** auf die Registerkarte **Massenregistrierung**. Die Seite **Massenregistrierung** wird angezeigt.
2. Klicken Sie auf **[Add]**.
3. Geben Sie in das Textfeld **Profilname** den Namen des Profils ein. Optional klicken Sie auf **Beschreibung hinzufügen** um für die CSV-Datei eine Beschreibung hinzuzufügen.
4. Klicken Sie in dem Abschnitt **CSV hochladen** auf **CSV-Vorlage herunterladen**, um die CSV-Vorlage herunterzuladen. Mit dem vorhandenen Format können Sie die Datei bearbeiten, um Geräte hinzuzufügen.

> Ermöglicht die Massenregistrierung per CSV-Datei mit bis zu 200.000 Zeilen auf einmal.

5. Klicken Sie nach dem Bearbeiten und Speichern der CSV-Datei auf **CSV hochladen** um die CSV-Datei hochzuladen. Bei erfolgreichem Hochladen wird eine Bestätigungsmeldung angezeigt.

> Zeilen mit unzureichenden Informationen führen zu CSV-Importfehlern. Jeder Datensatz muss mindestens die Seriennummer und Herstellerinformationen oder den IMEI-Wert enthalten.

> Um die hinzugefügte CSV-Datei zu entfernen, klicken Sie auf das „Minus“-Symbol. Um eine andere CSV-Datei zum Hochladen auszuwählen, klicken Sie auf den Link **Andere Datei wählen**.

6. Optional: Wählen Sie **Massen-Upload und Zuweisung benutzerdefinierter Attribute ohne Token**, um Geräte jeder Art ohne Generierung eines Tokens zu registrieren. Diese Option ist standardmäßig ausgewählt.

Die Massenregistrierung ohne Token kann auch angewendet werden, wenn die IMEI oder die Kombination aus Seriennummer und Hersteller (mit oder ohne benutzerdefinierte Attribute) in der hochgeladenen CSV-Datei enthalten ist. Die Registrierung des Geräts hängt jedoch von der Richtigkeit der in der CSV-Datei hochgeladenen Attributwerte ab. In der folgenden Tabelle werden die Ergebnisszenarien je nach der für die Massenregistrierung eingegebenen Attributwertkombination erläutert:

Szenario	**Eingegebene Attributwerte**			**Geräteregistrierungsstatus**
	IMEI	**Seriennummer**	**Hersteller**	
1	Richtig	Falsch	Falsch	Gerät ist registriert
2	Falsch	Richtig	Richtig	Gerät ist registriert
3	Falsch	Falsch	Richtig	Das Gerät ist nicht registriert.
4	Falsch	Richtig	Falsch	Das Gerät ist nicht registriert.

> Beim Namen des Herstellers ist die Groß- und Kleinschreibung zu beachten.

7. Wählen Sie im Feld **Benutzer auswählen** einen Benutzer aus.
   Das Registrierungstoken wird in der Spalte „Registrierungstoken“ angezeigt. Klicken Sie zum Aktualisieren des Registrierungstokens auf **Aktualisieren**.
   Das Ablaufdatum des Tokens wird im Abschnitt **Tokenablauf** angezeigt. Klicken Sie auf **Erweitern**, um den Ablaufzeitraum für das Token zu verlängern. Geben Sie in dem Feld **Verlängern bis** die Anzahl der Tage ein, die das Token verlängert werden soll.

Die angegebene Anzahl der Tage sollte zwischen 7 und 999 liegen. Das Token läuft standardmäßig nach 7 Tagen ab.
Diese Seite wird nicht angezeigt, wenn Sie die Option **Massen-Upload und Zuweisung benutzerdefinierter Attribute ohne Token** gewählt haben.

8. Klicken Sie auf **Fertig**.

Nach dem Upload werden die folgenden Details der hochgeladenen CSV-Datei in einer Tabelle auf der Seite **Massenregistrierung** angezeigt.

Einstellung	Beschreibung
Profil	Der Name des Profils.
Beschreibung	Eine Beschreibung des Profils.
Letzte Änderung	Das letzte Änderungsdatum der CSV-Datei.
TYP	Für selbstgewartete Profile → Selbstwartung
Anzahl der Geräte	Die Anzahl der Geräte in der Massenregistrierung.
Assoziierter Benutzer	Der Name des zugeordneten Benutzers.
Benutzername	Gibt den Benutzer an, der dem Gerät zugeordnet ist. Erforderlich, wenn die Gerät-zu-Benutzer-Zuordnung aktiviert ist. Der Benutzer muss in Ivanti Neurons for MDM vorhanden sein.
Aktionen	Sie können eine der folgenden Aktionen ausführen: **Vorhandenen Bestand herunterladen** – Klicken Sie auf diese Schaltfläche, um Details zu den im Profil verfügbaren Geräten herunterzuladen. **Anzeigen** - Klicken Sie auf diesen Link, um die Details der Geräte anzuzeigen, die zur Massenregistrierung hochgeladen wurden. **Bearbeiten** – Klicken Sie auf diese Schaltfläche, um die Profildetails zu bearbeiten. Diese Option ist nur dann verfügbar, wenn die Einzelgerätoption ausgewählt wurde. **Löschen** - Klicken Sie auf diesen Link, um die hochgeladene CSV-Datei zu löschen. Klicken Sie im Bestätigungsfenster auf **Ja**, um das Löschen der hochgeladenen CSV-Datei zu bestätigen.

Token, die beim Hochladen von CSV-Daten generiert werden, müssen für die Registrierung verwendet werden. Bei Eingabe des falschen Tokens erfolgt eine Umleitung zum normalen IReg-Fluss, und es muss die ID/das Passwort eingegeben werden.

Aktionen

Beim Anzeigen der Profile für die Massenregistrierung im Detailabschnitt "Profil anzeigen" können Sie andere Aufgaben über die Registerkarte "Aktionen" der Detailseite "Profil anzeigen" durchführen.

- **Weitere Geräte hinzufügen** – Verwenden Sie diese Option, um einem Profil weitere Geräte hinzuzufügen. Geben Sie die **IMEI-Nummer** und/oder **Seriennummer**, den **Hersteller** und optional die Informationen bei **Benutzerdefinierte Attribute** an und klicken Sie anschließend auf **Speichern**.
- **Konfiguration ändern** – Mit dieser Option modifizieren Sie eine vorhandene Konfiguration. Sie können **Ivanti-spezifische Schlüssel** hinzufügen, Änderungen an **vordefinierten Extras für das Android-System** oder an **benutzerdefinierten Schlüsseln für das Android-System** vornehmen und dann auf **Aktualisieren** klicken.
- **QR-Code generieren** – Mit dieser Option generieren Sie einen QR-Code für die Massenregistrierung von Profilen.
- **Token aktualisieren** – Mit dieser Option aktualisieren Sie ein Token oder verlängern seine Gültigkeit. Die Gültigkeit kann innerhalb eines Bereichs von 7 bis 999 Tagen festgelegt oder auf **Läuft nie ab** gesetzt werden.
- **Zugeordneten Benutzer ändern** – Mit dieser Option können Sie einen anderen zugeordneten Benutzer festlegen. Machen Sie dazu den Benutzer im Popupfenster **Zugeordneten Benutzer ändern** ausfindig, wählen Sie ihn aus und klicken Sie auf **Anwenden**.
- **Bearbeiten** – Mit dieser Option bearbeiten Sie Geräte im ausgewählten Profil. Wählen Sie die Geräte aus und klicken Sie auf **Bearbeiten**.
- **Löschen** – Mit dieser Option löschen Sie Geräte aus dem ausgewählten Profil. Nachdem Sie die Geräte ausgewählt und auf "Löschen" geklickt haben, wird eine Bestätigungsmeldung im Bildschirm angezeigt. Klicken Sie auf **Löschen**.

> Selbstgewartete Geräte verfügen über unterschiedliche Gerätestatus. Weitere Details finden Sie **hier**.

7.5.16. Device_to_User_BulkEnrollment

File not found!

7.5.17. Verwendung der mobilen Registrierung von Samsung Knox

Bei einer mobilen Registrierung mit Samsung KNOX können Administratoren qualifizierte Samsung-Geräte in Ivanti Neurons for MDM registrieren. Bei Verwendung der mobilen Registrierung mit Knox kann ein Gerät direkt von einem Vertragshändler an einen Endbenutzer ausgeliefert werden. Der Go Android-Client wird automatisch mit vordefinierten Registrierungsdaten heruntergeladen. Einzelheiten finden Sie unter **Mobile Samsung Knox-Registrierung für Android Enterprise**.

Anforderungen

- Geräteliste nach IMEI
- CSV-Datei mit einer Geräteliste und der IMEI bzw. Seriennummer sowie optional einem Benutzernamen und einem Registrierungskennwort
- Ivanti Neurons for MDM (aktuelles Release)
- Für mobile Registrierung zugelassenes Samsung Knox-Konto
- Von Samsung unterstützte Geräte. Eine Liste der von Samsung unterstützten Geräte finden Sie **hier**.

Samsung Knox Mobile Enrollment (KME)-Integration

Die Samsung Knox Mobile Enrollment-Integration lässt sich jetzt über durchführen, ohne dass dazu ein Profil erstellt und Geräte über das Samsung Knox-Portal genehmigt werden müssen.

> Es wird davon abgeraten, dass Administratoren die Daten direkt im Samsung KME-Portal aktualisieren oder modifizieren, nachdem sie in integriert wurden. Dies könnte zu Inkonsistenzen führen. Es wird deshalb dringend empfohlen, für sämtliche Profil- und Geräteaktualisierungen zu verwenden, es sei denn, ein bestimmter Anwendungsfall erfordert die Vornahme direkter Änderungen im Samsung KME-Portal. Aktualisierungen, die im Samsung KME-Portal vorgenommen wurden, werden in planbaren Intervallen mit synchronisiert.

Verfahren

1. Wechseln Sie zu **Admin** > **Samsung** > **Knox-Integration**.
2. Geben Sie bei den **Einstellungen** den **Integrationsnamen** und eine **Beschreibung** ein.
3. Klicken Sie auf **Aktivieren**, um die Samsung-KME-Integration zu aktivieren.
4. Wechseln Sie zu **Geräte** > **Massenregistrierung**.

Das Samsung KME-Standardprofil wird erstellt. Die Anzahl der Geräte beträgt weiterhin 0, da die Geräte noch nicht genehmigt wurden. Sobald Geräte genehmigt wurden, wird die entsprechende Anzahl hier angezeigt. Den Schritten 16 bis 18 entnehmen Sie weitere Details zum Samsung KME-Standardprofil.

> Das Samsung KME-Standardprofil wird in der Liste der Profile der Seite "Massenregistrierung" stets ganz oben angezeigt.

> Sie müssen die Geräte in das Samsung-Händlerkonto hochladen, damit sie auf der Registerkarte "Uploads" angezeigt werden.

5. Wechseln Sie zu **Admin** > **Samsung** > **Knox-Integration**.

6. Auf der Registerkarte **Uploads** können Sie die Geräte anzeigen, die vom Samsung-Händlerkonto hochgeladen wurden.
7. Klicken Sie bei den **Details** auf **Anzeigen**. Die Geräteansicht mit der Liste der zu genehmigenden Geräte wird im Bildschirm angezeigt.
8. Klicken Sie auf **Alle Geräte genehmigen**. Es wird ein Bestätigungsdialogfeld im Bildschirm angezeigt. Klicken Sie auf **Genehmigen**.
9. Klicken Sie zum Herunterladen der Liste der nicht genehmigten Geräte auf **Geräte als CSV herunterladen**.
10. Wechseln Sie zu **Geräte** > **Massenregistrierung**. Sie können die Anzahl der genehmigten Geräte im **Samsung KME-Standardprofil** anzeigen.
11. Folgende Gerätestatus sind in Samsung-KME-/selbstgewarteten Profilen verfügbar:

> Das Samsung KME-Standardprofil enthält eine Liste aller Geräte, die keinem der Samsung KME-Profile zugewiesen sind. Die Geräteregistrierung funktioniert nur dann, wenn das Samsung-Gerät einem Samsung-KME-Profil zugewiesen ist.

- Registrierung ausstehend
- Aktiv
- Wipe abgeschlossen
- Wipe ausstehend
- Außer Dienst gestellt
- Stilllegung ausstehend

Nachdem Sie die Samsung Knox-Integration aktiviert und auf der Seite "Massenregistrierung" auf **Hinzufügen** geklickt haben, werden Ihnen folgende Optionen angeboten:

- **Selbstwartung**
- **Mobile Registrierung von Samsung Knox**

Wählen Sie **Samsung Knox Mobile Enrollment** aus und klicken Sie auf **Weiter**.

Die Option **Geräteregistrierung ohne Token** ist nicht standardmäßig aktiviert. Wenn Sie mit der Standardoption fortfahren möchten, wechseln Sie zu den Schritten 11-14. Wenn Sie die Standardoption nicht verwenden möchten, wählen Sie **Geräteregistrierung ohne Token** aus und klicken Sie auf **Fertig**.

12. Wählen Sie im Feld **Benutzer auswählen** einen Benutzer aus.
    Das Registrierungstoken wird in der Spalte „Registrierungstoken“ angezeigt. Klicken Sie zum Aktualisieren des Registrierungstokens auf **Aktualisieren**.
    Das Ablaufdatum des Tokens wird im Abschnitt **Tokenablauf** angezeigt. Klicken Sie auf **Erweitern**, um den Ablaufzeitraum für das Token zu verlängern. Geben Sie in dem Feld **Verlängern bis** die Anzahl der Tage ein, die das Token verlängert werden soll.

> Die angegebene Anzahl der Tage sollte zwischen 7 und 999 liegen. Das Token läuft standardmäßig nach 7 Tagen ab.

Diese Seite wird nicht angezeigt, wenn Sie die Option **Geräteregistrierung ohne Token** ausgewählt haben.

13. Sie können **Ivanti-spezifische Schlüssel** hinzufügen, Änderungen an **vordefinierten Extras für das Android-System** oder an **benutzerdefinierten Schlüsseln für das Android-System** vornehmen.
14. Klicken Sie auf **Fertig**.

Nach der Erstellung des Samsung-Profils werden die folgenden Details in einer Tabelle auf der Seite **Massenregistrierungsprofile** angezeigt.

Einstellung	Beschreibung
Profil	Der Name des Profils.
Beschreibung **Letzte Änderung** **TYP** **Anzahl der Geräte**	Eine Beschreibung des Profils. Das Datum der zuletzt vorgenommenen Änderung. Für Samsung-KME-Profile – Samsung Knox Mobile Enrollment Die Anzahl der Geräte in der Massenregistrierung.
Assoziierter Benutzer	Der Name des zugeordneten Benutzers.
Aktionen	Sie können eine der folgenden Aktionen ausführen: **Vorhandenen Bestand herunterladen** – Klicken Sie auf diese Schaltfläche, um Details zu den im Profil verfügbaren Geräten herunterzuladen. **Anzeigen** - Klicken Sie auf diesen Link, um die Details der Geräte anzuzeigen, die zur Massenregistrierung hochgeladen wurden. **Bearbeiten** – Klicken Sie auf diese Schaltfläche, um die Profildetails zu bearbeiten. Diese Option ist nur dann verfügbar, wenn die Einzelgerätoption ausgewählt wurde. **Löschen** - Klicken Sie auf diesen Link, um die hochgeladene CSV-Datei zu löschen. Klicken Sie im Bestätigungsfenster auf **Ja**, um den Vorgang zu bestätigen.

15. Klicken Sie auf der Seite "Massenregistrierung" auf das Augensymbol, um die Details zum Samsung-Profil anzuzeigen. Folgende Details zur Registrierung werden angezeigt:

- Name, Anzahl der Geräte, Registrierungstoken, Registrierte Geräte, Tokenablauf, Geräte mit ausstehender Registrierung, Profiltyp und Synchronisierungsstatus.

16. Beim Anzeigen der Profile für die Massenregistrierung im Detailabschnitt "Profil anzeigen" können Sie andere Aufgaben über die Registerkarte "Aktionen" der Detailseite "Profil anzeigen" durchführen.

- **Geräte verschieben** (gilt nur für Samsung KME-Profile) – Zum Verschieben von Geräten zwischen zwei verschiedenen Samsung KME-Profilen. Bei Auswahl dieser Option wird ein Popupfenster angezeigt, in dem Sie das Zielprofil aus einer Liste auswählen und den Vorgang mit **Verschieben** bestätigen können.
- **Konfiguration ändern** – Mit dieser Option modifizieren Sie eine vorhandene Konfiguration. Sie können **Ivanti-spezifische Schlüssel** hinzufügen, Änderungen an **vordefinierten Extras für das Android-System** oder an **benutzerdefinierten Schlüsseln für das Android-System** vornehmen und dann auf **Aktualisieren** klicken.
- **Token aktualisieren** – Mit dieser Option aktualisieren Sie ein Token oder verlängern seine Gültigkeit. Die Gültigkeit kann innerhalb eines Bereichs von 7 bis 999 Tagen festgelegt oder auf **Läuft nie ab** gesetzt werden.
- **Zugeordneten Benutzer ändern** – Mit dieser Option können Sie einen anderen zugeordneten Benutzer festlegen. Machen Sie dazu den Benutzer im Popupfenster **Zugeordneten Benutzer ändern** ausfindig, wählen Sie ihn aus und klicken Sie auf **Anwenden**.

- **Bearbeiten** – Mit dieser Option können Sie benutzerdefinierte Attribute hinzufügen/ändern.
- **Zuweisung aufheben** – Mit dieser Option können Sie die Zuweisung eines Geräts zu einem Profil aufheben. Wenn Sie nach Auswahl des Geräts auf **Zuweisung aufheben** klicken, wird das Gerät aus dem vorhandenen Profil entfernt und in das Samsung KME-Standardprofil verschoben.

> Wenn die **Samsung Knox Mobile Enrollment-Integration** gelöscht wird, werden die zu dieser Integration gehörenden Profile **30 Tage lang** in **aufbewahrt**. Nach diesem 30-Tage-Zeitraum werden die Profile **dauerhaft aus gelöscht. Die Profile werden jedoch nicht aus dem Samsung Knox Mobile Enrollment-Portal gelöscht.**

Einstellung	Beschreibung
Profil	Der Name des Profils.
Beschreibung	Eine Beschreibung des Profils.
Letzte Änderung	Das Datum der zuletzt vorgenommenen Änderung.
TYP	Für Samsung-KME-Profile – Samsung Knox Mobile Enrollment
Anzahl der Geräte	Die Anzahl der Geräte in der Massenregistrierung.
Assoziierter Benutzer	Der Name des zugeordneten Benutzers.
Aktionen	Sie können eine der folgenden Aktionen ausführen: **Vorhandenen Bestand herunterladen** – Klicken Sie auf diese Schaltfläche, um Details zu den im Profil verfügbaren Geräten herunterzuladen. **Anzeigen** - Klicken Sie auf diesen Link, um die Details der Geräte anzuzeigen, die zur Massenregistrierung hochgeladen wurden. **Bearbeiten** – Deaktiviert für Samsung KME-Standardprofil. **Löschen** – Deaktiviert für Samsung KME-Standardprofil.

Nach der Erstellung des Samsung-KME-Standardprofils werden die folgenden Details in einer Tabelle auf der Seite **Massenregistrierungsprofile** angezeigt.

Klicken Sie auf der Seite "Massenregistrierung" auf das Augensymbol, um die Details zum Samsung KME-Standardprofil anzuzeigen. Folgende Details zur Registrierung werden angezeigt:

Name, Anzahl der Geräte, Registrierungstoken, Registrierte Geräte, Tokenablauf, Geräte mit ausstehender Registrierung, Profiltyp und Synchronisierungsstatus.

Menü "Aktionen" – Über das Aktionenmenü können Sie die folgenden Aufgaben durchführen:

Geräte verschieben (gilt nur für Samsung KME-Profile) – Zum Verschieben von Geräten vom Samsung KME-Standardprofil in ein anderes Samsung KME-Profil. Bei Auswahl dieser Option wird ein Popupfenster angezeigt, in dem Sie das Zielprofil aus einer Liste auswählen und den Vorgang mit **Verschieben** bestätigen können.

Löschen – Zum Löschen des Geräts.

7.5.18. Registrieren von Oculus-Geräten

Ivanti Neurons for MDM unterstützt ab sofort Geräte des Typs "Quest for Business" (Oculus-Geräte). Derzeit unterstützt Meta Geräte des Typs "Oculus for Business" (OFB) und "Quest for Business" (QFB) für MDM. Sie müssen einige grundlegende Aufgaben in der Meta-Konsole ausführen, um die Geräte für MDM zu aktivieren und sie für Ivanti Neurons for MDM zu registrieren.

Sie können die Oculus-Geräteflotte in der Meta Workplace-Konsole im Device Manager registrieren. Sie müssen sich über die Anmeldeinformationen, die Sie in Ihrer Registrierungs-E-Mail erhalten haben, bei Oculus Business Workplace anmelden. Auf der Startseite werden im Abschnitt "Geräteflotte" Informationen zu allen Geräten angezeigt. Der Abschnitt "Geräteflotte" bietet einen Überblick über alle in der Geräteverwaltung verfügbaren Geräte. Zu diesen Details gehört der Gerätename, der Gerätestatus, das BS (Betriebssystem), das Modell usw.

Dieser Abschnitt enthält die folgenden Themen:

- Voraussetzungen für das Registrieren von Oculus-Geräten
  - Einrichten einer MDM-App im Device Manager
  - Einrichten des Oculus-Geräts

OFB-Gerät in MobileIron Go registrieren

  - Auf der Ivanti Neurons for MDM-Konsole
  - On Go-Client

Voraussetzungen für das Registrieren von Oculus-Geräten

Einrichten einer MDM-App im Device Manager

Die Geräte/Headsets werden bereitgestellt und auf mindestens **Version 28** von **Oculus for Business** aktualisiert. Auf der Metakonsole muss der Administrator im Device Manager einen MDM einrichten und die Oculus-Geräte diesem MDM-Dienst zuordnen.

Verfahren

1. Wählen Sie auf der Startseite von **Oculus Business Workplace Apps** aus.
2. Klicken Sie unter **App-Bibliothek** auf die zu installierende Drittanbieter-MDM-App, und klicken Sie dann auf **Aktualisieren**.
3. Wählen Sie den entsprechenden MDM-Eintrag für die App aus der Liste unter **Mobilgeräteverwaltung** aus, und klicken Sie dann auf **App aktualisieren**.
4. Klicken Sie auf das Oculus-Geräte-Headset, auf dem MDM installiert werden soll. Die Geräteinformationen werden auf dem Bildschirm angezeigt.
5. Führen Sie auf der Registerkarte **Info** einen Bildlauf zu **Mobile Device Manager** aus.
6. Klicken Sie auf die Schaltfläche **Bearbeiten**, die neben der Option **MDM Authority** angezeigt wird.

> Die Oculus Device Manager-Option wird standardmäßig ausgewählt. Sie müssen die MDM Authority-App und **MobileIron Go** aus der MDM Authority-App-Liste auswählen.

Klicken Sie auf **Speichern**. Nachdem das Gerät automatisch zurückgesetzt wurde, müssen Sie das Oculus-Gerät über die Setup-App einrichten.

Einrichten des Oculus-Geräts

Sie können Oculus Quest 2-Headset-Geräte über die Geräte-Setup-App hinzufügen. Diese App muss mit den erforderlichen Benutzern geteilt werden, damit die Benutzer die App auf ihre Android-Geräte herunterladen und dort installieren können.

Verfahren

1. Klicken Sie im Abschnitt **Geräteflotte** auf **Nicht konfigurierte Geräte**.
2. Klicken Sie auf **Setup-App abrufen**. Die Seite **Download-Link senden** wird auf dem Bildschirm angezeigt.
3. Wählen Sie mindestens ein Teammitglied aus der Liste aus, oder klicken Sie auf **Empfänger hinzufügen**, um ein Element aus der Liste auszuwählen.
4. Klicken Sie auf **Link senden**. Die ausgewählten Benutzer erhalten eine E-Mail mit einem Link zum Installieren der **Geräte-Setup-App**.
5. Klicken Sie auf den Link **Geräte-Setup-App herunterladen** in der E-Mail, um die **Geräte-Setup-App** auf Ihrem Android-Gerät zu installieren.

> Nach dem Download wird diese App nicht im App Store auf Ihrem Gerät angezeigt. Sie müssen sie über den Abschnitt "Downloads" auf Ihrem Gerät abrufen und anschließend installieren.

Öffnen Sie die App **Oculus for Business** auf Ihrem Android-Gerät.

7. Schalten Sie die Oculus-Geräte ein, indem Sie 2 Sekunden lang auf die Ein-/Aus-Taste drücken.
8. Schalten Sie Bluetooth ein, und positionieren Sie das Android-Gerät in der Nähe der Oculus-Geräte, bis die Einrichtung abgeschlossen ist.
9. Verwenden Sie zum Suchen von Oculus-Geräten die Bluetooth-Funktion auf Ihrem Android-Gerät.
10. Sobald das erforderliche Oculus-Gerät gefunden wurde, müssen Sie es mit einem WLAN-Netzwerk verbinden und die Einrichtung abschließen.
11. Klicken Sie auf **WLAN-Informationen eingeben**, stellen Sie den Netzwerknamen und das Passowort bereit, und klicken Sie dann auf **Speichern**. Das Oculus-Gerät ist nun mit dem WLAN-Netzwerk verbunden.
12. Klicken Sie auf **Einrichtung starten**. Es wird eine Benachrichtigung auf dem Bildschirm angezeigt, aus der hervorgeht, dass die Einrichtung läuft. Sie sollten die App während der Einrichtung nicht schließen und die Headsets nicht verwenden.
    Es wird eine Bestätigung auf dem Bildschirm angezeigt. Sie können die Suche nach weiteren Geräten über die Schaltfläche **Weitere Geräte suchen** fortsetzen.

Registrieren eines OFB-Geräts mit MobileIron Go

Auf der Ivanti Neurons for MDM-Konsole

Ein OFB-Gerät kann mit MobileIron Go auf Ivanti Neurons für die MDM-Konsole bereitgestellt werden. Allerdings muss die Work Managed-Gerät, nicht GMS-Modus (AOSP)-Konfiguration (unter **Konfigurationen**) an diese OFB-Gerätegruppen verteilt werden.

On Go-Client

Ein OFB-Gerät kann auf dem MobileIron Go-Client registriert werden. Sie müssen die folgenden Aufgaben abschließen, um das OFB-Gerät zu registrieren:

- Fahren Sie nach Abschluss der Einrichtung über die OFB-Setup-App mit den Bildschirmanweisungen auf dem OFB-Headset fort, um die Einrichtung des Geräts abzuschließen.

- Die MobileIron Go-App wird automatisch gestartet, und Sie müssen die Anmeldeinformationen eingeben und die Registrierung abschließen, indem Sie den MDM-Anweisungen folgen.

Das Gerät wurde im DO-Modus bereitgestellt und kann nun von MDM verwaltet werden.

7.5.19. Bluetooth auf einem Gerät aktivieren

Gilt für:

- iOS 11.3+
- macOS 10.13.4+

Sie können Bluetooth auf einem Gerät aktivieren oder deaktivieren.

Verfahren

1. Wählen Sie auf der Seite **Geräte** das Gerät aus.
2. Führen Sie eine der folgenden Aktionen aus:
    - Wählen Sie die Geräte in der Liste aus.
    - Klicken Sie auf den Gerätenamen, um die Seite mit den Gerätedetails anzuzeigen.
3. Klicken Sie im Menü **Aktionen** auf **Bluetooth aktivieren/deaktivieren**.
4. Klicken Sie auf **OK**.

Die Änderungen werden per Push auf die Geräte übertragen, sobald diese sich das nächste Mal anmelden.

7.5.20. iOS-Update planen

Gilt für:

- iOS 9.0+ Überwachte Geräte für Device Enrollment
- Überwachte Geräte mit iOS 10.3.

Planen Sie die Aktualisierung eines iOS-Geräts auf die letzte verfügbare iOS-Version. Unter **Gerät** > **Aktionen** zeigt die Menüoption **Betriebssystemversion aktualisieren** für überwachte iOS-Geräte eine Liste derjenigen iOS-Versionen an, die für das Gerät relevant sind.

Verfahren

1. Wählen Sie auf der Seite **Geräte** das Gerät aus.
2. Klicken Sie auf den Gerätenamen, um die Seite mit den Gerätedetails anzuzeigen.
3. Klicken Sie im Menü **Aktionen** auf **Betriebssystemversion aktualisieren**.
4. Überprüfen Sie im Assistenten **Betriebssystemversion aktualisieren** die iOS-Version und wählen Sie die Betriebssystemversion aus der Dropdownliste **Aktualisieren auf Version** aus.

> Falls Sie eine identische oder eine ältere Version eingeben, weist eine Meldung darauf hin, dass die iOS-Zielversion höher sein muss als die aktuelle Version.

5. Klicken Sie auf **Aktualisieren**.

Das iOS-Gerät wird zur Aktualisierung auf die letzte derzeit verfügbare iOS-Version eingeplant, sobald sich das Gerät anmeldet. Wenn das Gerät über einen Passcode verfügt, stellt das Gerät, sobald MDM das Update an das Gerät gesendet hat, das Update in die Warteschlange. Der Benutzer wird dann aufgefordert, seinen Passcode einzugeben, um die Installation zu starten. Weitere Informationen finden Sie unter **Software-Aktualisierungen**.

7.5.21. Installieren Sie die iOS System-Apps neu.

Gilt für:

- Geräte unter iOS 11.3+.

Installieren Sie gelöschte iOS System-Apps auf iOS-Geräten neu.

Verfahren

1. Navigieren Sie zur Seite **Geräte**. Sie können auch auf den Namen des Geräts klicken und diese Aktion über die Seite Gerätedetails ausführen.
2. Wählen Sie mindestens ein iOS-Gerät aus.
3. Klicken Sie im Menü **Aktionen** auf **iOS-System-Apps neu installieren**.
4. Wählen Sie im Anzeigefeld iOS-System-Apps neu installieren eine oder mehrere verfügbare System-Apps für die Installation auf den Geräten aus.
5. Klicken Sie auf **Apps neu installieren**.

Die Apps werden auf den ausgewählten und kompatiblen iOS-Geräten installiert, sobald die Geräte einchecken. Auf diese Weise installierte System-Apps gelten nicht als verwaltete Apps. Wenn keine kompatiblen Geräte ausgewählt sind, erhalten Sie eine Meldung, dass die System-Apps nicht auf diesen Geräten installiert werden.

Weitere Informationen finden Sie unter **Software-Aktualisierungen**.

7.5.22. Zuweisen eines neuen Benutzers für ein Gerät

Ein vorhandenes, registriertes Gerät muss gegebenenfalls einem neuen Benutzer übergeben werden, wenn der alte Benutzer eine andere Rolle erhalten hat oder nicht mehr im Unternehmen beschäftigt ist. Mit den folgenden Schritten vermeiden Sie eine Abschaltung mit anschließender Neuregistrierung des Geräts.

Schritte:

1. Wählen Sie auf der Seite **Geräte** das Gerät aus.
2. Klicken Sie auf den Gerätenamen, um die Seite mit den Gerätedetails anzuzeigen.
3. Klicken Sie auf das Symbol **Benutzer zuweisen** .

> Alternativ können Sie ein Gerät auf der Seite **Geräte** auswählen und die Option **Benutzer zuweisen** im Menü **Aktionen** auswählen.

Beginnen Sie mit der Eingabe des Benutzernamens im Feld **Benutzer suchen ...**. Feld.

5. Wählen Sie den gewünschten Benutzer aus.
6. Klicken Sie auf **Benutzer zuordnen.**
   Das Gerät wird für diesen Benutzer bereitgestellt.

> Sie werden feststellen, dass Sie in den Szenarien mit Benutzer- und Gerätelizenzen ein Gerät einem Benutzer zuordnen können, auch wenn dessen Limit für zugeordnete Geräte überschritten ist. Der Grund liegt darin, dass mit der Funktion zur Begrenzung der Gerätezahl die Registrierung der Geräte limitiert werden soll, die im Rahmen von BYOD-Initiativen ("jeder bringt sein eigenes Gerät mit") unterstützt werden.

Sowohl bei Gerätelizenzen als auch bei Benutzerlizenzen ist die Durchsetzung des Gerätelimits inkonsequent. Bei Gerätelizenzen ändern sich die Kosten für den Endkunden nicht, weil sich die Gesamtzahl der Geräte im System nicht ändert. Bei Benutzerlizenzen profitiert von der fehlenden Prüfung derzeit der Kunde. Angenommen, Sie haben fünf Benutzer U1 bis U5 mit jeweils 5 Geräten. Bei der Benutzerlizenzierung entspräche dies fünf Lizenzen. Wenn stattdessen zwei der Geräte von U4 und U5 an U1 und U2 übergeben werden, werden WENIGER Lizenzen benötigt, statt fünf nur drei.

7.5.23. Neuzuweisen eines Android-Geräts

Der Administrator kann den Besitz eines Android-Geräts zwischen zwei Benutzern übertragen. Während des Prozesses der Neuzuweisung wird das Verwaltungsprofil des Geräts im Android Enterprise-Modus neu konfiguriert oder vom aktuellen Benutzer einem neuen Benutzer zugeordnet. Die Neuzuweisung kann auf allen Android Enterprise-Geräten außer Android Management API (AMAPI)-Geräten und nicht auf Google Domain Android Enterprise-Geräten durchgeführt werden.

> Die Gerätezuweisung kann nur dann durchgeführt werden, wenn sich die Geräte im gleichen Modus befinden. Beispiel: Ein Gerät im Work Managed Device-Modus kann einem anderen Benutzer in diesem Modus zugeordnet werden.

Der Prozess der Geräteneuzuweisung durchläuft folgende Status:

- Initiiert
- Erfolg
- Fehlgeschlagen
- Ausstehend

Sie können den letzten Neuzuweisungsstatus eines Geräts auf der Seite **Gerätedetails** → Registerkarte **Übersicht** → **Letzter Neuzuweisungsstatus** anzeigen.

Verfahren

1. Gehen Sie zu **Geräte**.
2. Wählen Sie einen oder mehrere Geräte aus der Liste aus.
3. Klicken Sie in der Liste **Aktionen** auf **Einem Benutzer zuweisen**.
4. Alternativ können Sie auf einen Gerätenamen klicken. Die Seite **Gerätedetails** wird geöffnet. Klicken Sie auf das Symbol für **Einem Benutzer zuweisen**, um den gleichnamigen Bildschirm aufzurufen und den gewünschten Benutzer auszuwählen.
5. Klicken Sie auf **Einem Benutzer zuweisen**. Die ausgewählten Optionen werden validiert, um zu prüfen, ob die ausgewählten Geräte dem ausgewählten Benutzer neu zugewiesen werden können.
   Nach erfolgreicher Validierung und Neuzuweisung wird eine Bestätigungsmeldung im Bildschirm angezeigt.

> Wenn Sie maximal 10 Geräte ausgewählt haben, wird die Meldung "Zuweisung initiiert" im Bildschirm angezeigt. Wenn Sie 11 oder mehr Geräte ausgewählt haben, wird die Popup-Meldung "Validierung wird gerade durchgeführt" angezeigt.

> Die Neuzuweisung von Android-Geräten ist eine innovative Lösung, die speziell dazu entwickelt wurde, Restdaten von ehemals zugewiesenen Benutzern zu eliminieren und ist nur in SUEM-Premium SKU verfügbar.

7.5.24. Erzwingen einer Geräteanmeldung

Geräte müssen Kontakt mit der Cloud haben (sich anmelden), um Informationen zu senden und zu empfangen. Anmeldungen werden in regelmäßigen Abständen veranlasst. Sie können ein Gerät auch dazu auffordern, einen Anmeldung bei Bedarf auszuführen. Eine erzwungene Geräteanmeldung kann den Prozess der Übernahme von Konfigurationen u.ä. beschleunigen.

Verfahren

1. Gehen Sie zu **Geräte > Geräte**.
2. Wählen Sie die entsprechenden Geräte aus.
3. Klicken Sie auf **Aktionen**.
4. Wählen Sie **Anmeldung erzwingen**.
5. Sie können auch auf den Link mit dem Gerätenamen klicken, um die Seite mit den Gerätedetails aufzurufen. Klicken Sie dann auf das Symbol **Anmeldung erzwingen**  und dann auf **OK**.

Wenn bei der Verarbeitung des Konfigurationsinstallationsbefehls bei der Anmeldung auf dem Gerät ein Fehler auftritt, versucht die Cloud nicht erneut, die Konfiguration auf dem Gerät zu installieren, wenn es sich später automatisch anmeldet. Der Administrator muss dann die Installation der Konfiguration manuell über die Seite Gerätedetails des Geräts ausführen. Gehen Sie dazu zur Registerseite Konfiguration, wählen Sie die Fehlerkonfiguration aus und klicken Sie auf **Installation wiederholen**.

7.5.25. Lokalisierung eines Geräts

Wenn Sie die Lokalisierungsfunktion für ein Geräts aktiviert haben, können Sie den letzten bekannten Standort dieses Geräts sehen. Sie müssen die **Datenschutzkonfiguration** bearbeiten, um die Erfassung von Standortdaten zu aktivieren und die Konfiguration für das Gerät übernehmen, damit es diese Funktion aktivieren kann. Das Gerät muss diese Funktion auch unterstützen und der Benutzer muss zustimmen, dass seine Standortdaten geteilt werden.

Verfahren

1. Wählen Sie auf der Seite **Geräte** das Geräts aus.
2. Klicken Sie in der Spalte **Name** auf den Link.
3. Klicken Sie auf der Registerkarte**Überblick**auf den Link unter **Standort des Gerätes**.

Folgende Details werden auf der Seite angezeigt:

Feldname	Beschreibung
Zuletzt lokalisiert am	Zeigt Datum und Uhrzeit der letzten Lokalisierung des Gerätes an.
Koordinaten	Zeigt den Breitengrad (Nord-Süd-Position) und den Längengrad (Ost-West-Position) des Gerätes an.

Sie können den Gerätestandort auch in der auf der Seite angezeigten Karte suchen.

7.5.26. Gerät sperren

Sie können die Bildschirmsperre auf einem Gerät aktivieren. Bei verschiedenen Geräten unterscheidet sich die Aktivierung der Sperre jeweils etwas.

Verfahren

1. Gehen Sie zu **Geräte > Geräte**.
2. Wählen Sie das entsprechende Gerät aus.
3. Klicken Sie auf **Aktionen**.
4. Wählen Sie **Sperren**.
5. Sie können auch auf den Link mit dem Gerätenamen klicken, um die Seite mit den Gerätedetails aufzurufen, und anschließend auf das Symbol für **Sperren**  und dann auf **OK** klicken.
6. Bei AppConnect Android-Apps sperrt der Sperrbefehl den Benutzer aus dem Container aus und sperrt zudem das Gerät. Die Benutzer können sich erneut bei dem Gerät und der AppConnect-App anmelden, indem sie den Gerätepasscode bzw. den AppConnect-Passcode verwenden.
7. Bei iOS 7-Geräten können Sie eine Display-Nachricht und eine Telefonnummer (optional) eingeben.
   Durch diese Optionen erhalten die Benutzer des Gerät Informationen dazu, warum das Gerät gesperrt wurde, und erfahren die Nummer, die sie anrufen müssen, um das Gerät zu entsperren.
8. Bei macOS-Geräten wird der Benutzer aufgefordert, als Passcode für den Zugriff auf das Gerät eine sechsstellige PIN einzugeben. Um trotz Bildschirmsperre weiterzuarbeiten, muss der Gerätebenutzer folgende Schritte ausführen:
   1. Geben Sie die PIN ein.
   2. Wählen Sie das Kontrollkästchen zur Bestätigung der Gerätesperre aus.
   3. Klicken Sie auf **Ja, Sperrbefehl senden**.

> In macOS kann der Benutzer eine optionale Meldung und eine Telefonnummer für den Sperrbildschirm hinzufügen, wenn der Passcode für die Gerätesperre eingestellt wird.

9. Bei der Durchführung eines Sperrvorgangs auf einem ChromeOS-Gerät wird folgende Meldung angezeigt: "Nach dem Sperren eines Gerätes muss der Benutzer eventuell einen Passcode eingeben, um auf das Gerät zugreifen zu können". Wenn Sie auf **Sperren** klicken, wechselt der Gerätestatus in **Deaktivierung gesendet**. Der aktualisierte Gerätestatus wird nach der regelmäßigen Gerätesynchronisierung angezeigt.

Alternative Verfahren zum Sperren eines Gerätes:

- Ein Gerätebenutzer kann die Sperraktion auch über das Selbstbedienungsportal auslösen.
- Ein Administrator kann die Sperrfunktion über das Administratorportal aufrufen.

7.5.27. Verwalten von Apple-Geräten im Verloren-Modus

Dieser Abschnitt enthält die folgenden Themen:

- Lost Mode aktivieren
- Lost Mode-Aktionen durchführen
- Lost Mode deaktivieren

Gilt für: überwachte Geräte mit iOS 10.3+

Sie können ein überwachtes Gerät über die Cloud in den Verloren-Modus schalten. Das heißt, Sie melden den Apple-Servern, dass das Gerät verloren gegangen ist. Dadurch können Sie den letzten erfassten Standort des Geräts anzeigen sowie den „Verloren-Modus“ deaktivieren, sobald das Gerät gefunden wurde.

Lost Mode aktivieren

Sie können ein verloren gegangenes Gerät den Apple-Servern melden, indem Sie das Gerät in den Verloren-Modus schalten. Sobald Sie ein Gerät in den "Verloren-Modus" geschaltet haben, gilt Folgendes:

- Wenn das Gerät abgeschaltet ist, können Sie den Verloren-Modus nicht deaktivieren.
- Wenn das Gerät komplett gelöscht ist, können Sie das Gerät weder lokalisieren, noch verfolgen.

Verfahren

1. Gehen Sie zu **Geräte**.
2. Klicken Sie in das Kontrollkästchen für das Gerät.
3. Wählen Sie die Option **Aktionen** > **Allgemein** > **Verloren-Modus aktivieren** aus.
4. Navigieren Sie alternativ zur Seite **Gerätedetails**, indem Sie den Link mit dem Gerätenamen auswählen. Klicken Sie auf das Aktionssymbol des Geräts und wählen Sie **Verloren-Modus aktivieren** aus.

Lost Mode-Aktionen durchführen

Sobald der Verloren-Modus aktiviert ist, können Sie im Abschnitt für den Verloren-Modus:

- eine Nachricht/Mobil-Telefonnummer per Push an das iPhone senden
  - eine Nachricht eingeben, die auf dem Sperrbildschirm des verlorenen Geräts angezeigt werden soll
  - eine Kontaktnummer eingeben, die auf dem Sperrbildschirm des verlorenen Geräts angezeigt werden soll. Wenn jemand das Gerät findet, kann er die Rufnummer verwenden, um seinen Fund zu melden.

Gerät sperren

- **Gerätestandort aktualisieren**

> Wenn das Gerät komplett gelöscht ist, können Sie das Gerät nicht lokalisieren.

- **Klang im Verloren-Modus abspielen.**

> Der Klang wird abgespielt, bis das Gerät sich nicht mehr im Verloren-Modus befindet oder ein Benutzer den Klang am Gerät deaktiviert.

- **Standort aktualisieren**
  Die Option **Standort aktualisieren** wurde zum **Verlustmodus** hinzugefügt, um den Standort des Geräts anzuzeigen. Folgende Details werden angezeigt:
  - **Breitengrad**: Der Breitengrad des Gerätestandorts.
  - **Zeitstempel**: Uhrzeit und Datum der Payload werden angezeigt.
  - **Längengrad**: Der Längengrad des Gerätestandorts.

Lost Mode deaktivieren

Wenn ein Gerät im Verloren-Modus gefunden wurde oder der Verloren-Modus irrtümlich aktiviert wurde, können Sie den Verloren-Modus deaktivieren.

> Wenn das verloren gegangene Gerät in Ivanti Neurons for MDM stillgelegt wurde, können Sie den Verloren-Modus nicht deaktivieren.

Verfahren

1. Gehen Sie zu **Geräte**.
2. Klicken Sie in das Kontrollkästchen für das Gerät.
3. Wählen Sie die Option **Aktionen** > **Allgemein** > **Verloren-Modus deaktivieren** aus.
4. Navigieren Sie alternativ zur Seite **Gerätedetails**, indem Sie den Link mit dem Gerätenamen auswählen, und wählen Sie **Verloren-Modus für Gerät: Aktiviert** > **Verloren-Modus deaktivieren** aus.

7.5.28. Verwalten von Android-Geräten im Verloren-Modus

Dieser Abschnitt enthält die folgenden Themen:

- Aktivieren des Verloren-Modus
- Deaktivieren des Verloren-Modus

Aktivieren des Verloren-Modus

Gilt für: Geräte mit Android 8+

Sie können über Ivanti Neurons for MDM mehrere Android-Geräte gleichzeitig in den Verloren-Modus versetzen. Sie können den Verlust eines Geräts an Ivanti Neurons for MDM melden, indem Sie das Gerät (oder mehrere) in den Verloren-Modus versetzen. Für diesen Modus können Sie eine benutzerdefinierte Meldung, eine Telefonnummer und eine Fußnote im Bildschirm definieren sowie optional die Wiedergabe eines Sounds festlegen.

> Diese Funktionalität unterstützt nur vollständig verwaltete Geräte sowie Nicht-GMS-Geräte.

Verfahren

1. Gehen Sie zu **Geräte**.
2. Markieren Sie das Kontrollkästchen für das Gerät/die Geräte.
3. Wählen Sie die Option **Aktionen > Verloren-Modus aktivieren** aus.
4. Sie können auch auf den Link mit dem Gerätenamen klicken, um die Seite mit den Gerätedetails aufzurufen und dann auf das Symbol ⋮ klicken. Wählen Sie die Option **Verloren-Modus aktivieren** aus.
5. Geben Sie eine Bildschirmsperre-Meldung und/oder eine Telefonnummer ein, die auf dem Sperrbildschirm des/der verlorenen Geräts/Geräte angezeigt werden soll. Administratoren können außerdem die Fußnote festlegen und die Option **Sound für Verloren-Modus wiedergeben** auswählen. Wenn jemand das Gerät/die Geräte findet, kann er den Fund über die angezeigte Rufnummer melden.

> Es muss entweder eine Meldung oder eine Telefonnummer in das jeweilige Feld eingetragen werden, um die Option **Verloren-Modus aktivieren** aufzurufen.

> Der Sound für den Verloren-Modus ertönt 5 Minuten lang, es sei denn, das Telefon wird innerhalb dieser Zeit entsperrt oder der Verloren-Modus wird vom Administrator deaktiviert. Um den Sound wieder zu aktivieren, muss der Verloren-Modus auf dem Gerät/den Geräten erneut aktiviert werden.

6. Wählen Sie **Verloren-Modus aktivieren**, um das oder die Android-Geräte in den Verloren-Modus zu versetzen.

Durch Aktivieren des Verloren-Modus werden folgende Aktionen deaktiviert:

- Entsperren
- Kiosk aufrufen/beenden
- Abmeldung vom gemeinsam genutzten Kiosk erzwingen

- Benutzer zuweisen
- Nachricht senden
- Eigentumsstatus definieren

> Sobald der Verloren-Modus auf einem Gerät aktiviert wurde, wird die Option "Verloren-Modus" auf dem Server deaktiviert.

Deaktivieren des Verloren-Modus

Wenn ein Gerät im Verloren-Modus wieder gefunden oder der Verloren-Modus irrtümlich aktiviert wurde, können Sie den Verloren-Modus deaktivieren.

> Wenn das verloren gegangene Gerät in Ivanti Neurons for MDM komplett gelöscht wurde, können Sie den Verloren-Modus nicht deaktivieren.

Verfahren

1. Gehen Sie zu **Geräte**.
2. Markieren Sie das Kontrollkästchen für das Gerät/die Geräte.
3. Wählen Sie die Option **Aktionen > Verloren-Modus deaktivieren** aus.
4. Sie können auch auf den Link mit dem Gerätenamen klicken, um die Seite mit den Gerätedetails aufzurufen und dann **Verloren-Modus: Aktiviert > Verloren-Modus deaktivieren** auswählen.

> Im Abschnitt **Details** ist die Option **Verloren-Modus deaktivieren** nur dann sichtbar, wenn zuvor **Verloren-Modus aktivieren** aktiviert wurde. Nachdem die Option **Verloren-Modus deaktivieren** gewählt wurde, ist das Feld **Verloren-Modus für Gerät: Aktiviert**, in dem auch die Option **Verloren-Modus deaktivieren** enthalten ist, ausgeblendet.

> Geräte, die sich vorher im Kiosk-Modus befanden, müssen nach dem Deaktivieren des Verloren-Modus wieder in den Kiosk-Modus versetzt werden.

7.5.29. Debug-Protokolle anfordern

Sie können eine Anfrage an verwaltete Geräte mit iOS, MacOS und Android senden, um Debug-Protokolle zur Fehlerbehebung bei Geräteproblemen abzurufen. Mit dem Befehl "Debug-Protokolle anfordern" auf der Seite "Geräte" werden die Aktionen und der Erfolg oder Misserfolg eines Ereignisses in den Debug-Protokollen erfasst.

Für diese Funktionalität werden folgende Clients benötigt:

- iOS-Geräte benötigen Go 5.3.0 für iOS oder unterstützte neuere Versionen. Für Geräte, die von Ivanti EPMM auf Ivanti Neurons for MDM migriert werden, erfordert diese Funktion Mobile@Work 12.2.0 für iOS oder unterstützte neuere Versionen.
- macOS-Geräte benötigen Mobile@Work 1.5 für macOS oder unterstützte neuere Versionen.
- Verwaltete betriebliche Android-Geräte benötigen Go 65 für Android oder eine unterstützte neuere Version.

Verfahren

1. Gehen Sie zu **Geräte > Geräte**.
2. Wählen Sie das Gerät aus und klicken Sie auf den Link "Gerätename", um zur Seite mit den Gerätedetails zu gelangen.
3. Klicken Sie auf das ⋮-Symbol.
4. Wählen Sie die Option **Debug-Protokolle anfordern** und klicken Sie auf **OK**.

Wenn die Anforderung gesendet wird und die Protokolle auf dem Gerät verfügbar sind, wird eine Benachrichtigung an den Administrator gesendet und in den Geräteprotokollen angezeigt. Die Geräteprotokolle können auch durch Klicken auf den Link heruntergeladen werden.

7.5.30. Apple_Enhanced_Logging

File not found!

7.5.31. Gerät außer Dienst stellen

Mit dem Stilllegen eines Geräts endet die Beziehung zu Ivanti Neurons for MDM. Mögliche Gründe für die Außerdienststellung eines Geräts:

- Der Benutzer hat das Unternehmen verlassen.
- Der Benutzer hat das Gerät ausgetauscht.
- Sie müssen Ihre bisher erledigten Verwaltungsaufgaben rückgängig machen (erneut beginnen).

Verfahren

1. Gehen Sie zu **Geräte > Geräte**.
2. Wählen Sie das entsprechende Gerät aus.
3. Klicken Sie (oben rechts) auf **Aktionen**.
4. Wählen Sie **Außer Dienst stellen**.
5. Sie können auch auf den Link mit dem Gerätenamen klicken, um die Seite mit den Gerätedetails aufzurufen und auf das Symbol ⋮ klicken.
6. Wählen Sie **Abschalten** und klicken Sie auf **OK**.

Wenn Sie eine Operation vom Typ "Stilllegen" auf einem Gerät im aktiven Status ausführen, wird das Gerät sofort stillgelegt.

7.5.32. Verzichten auf Gerätebesitz

Gilt für Android-Geräte im Modus „Arbeitsprofil auf unternehmenseigenem Gerät“.

Wenn Sie auf den Besitz eines Geräts im Modus „Arbeitsprofil auf unternehmenseigenem Gerät“ verzichten, wird das Arbeitsprofil entfernt und das Gerät in der Cloud außer Dienst gestellt, ohne dass private Apps und Daten verändert werden. Der Endbenutzer kann das Gerät dann als privates Gerät verwenden, mit vollem Zugriff auf alle Gerätesteuerungen und -einstellungen.

> Das Gerät muss aus Google Zero Touch oder dem Knox Mobile Enrollment Portal entfernt werden.

Sie können in folgenden Fällen den Besitz eines Geräts oder darauf verzichten:

- Der Benutzer hat das Unternehmen verlassen.
- Der Benutzer hat das Gerät ausgetauscht.

Verfahren

1. Gehen Sie zu **Geräte > Geräte**.
2. Wählen Sie das entsprechende Gerät aus.
3. Klicken Sie auf **Gerätedetailseite** und auf das Symbol ⋮.
4. Wählen Sie **Auf Besitz verzichten** aus.

7.5.33. Gerät „wipen“

Bei der Komplettlöschung eines Geräts werden alle Daten entfernt und das Gerät wird wieder auf die Werkeinstellung zurückgesetzt.

Verfahren

1. Gehen Sie zu **Geräte > Geräte**.
2. Wählen Sie das entsprechende Gerät aus.
3. Klicken Sie (oben rechts) auf **Aktionen**.
4. Wählen Sie Wipe durchführen.
5. Sie können auch auf den Link mit dem Gerätenamen klicken, um die Seite mit den Gerätedetails aufzurufen und dann auf das Symbol ⋮ klicken. Wählen Sie die Option **Wipe durchführen** und klicken Sie auf **OK**.
6. Die Option **Datentarif beibehalten** ist standardmäßig ausgewählt.
   (Optional, gilt für iOS 11.3+ Geräte). Wählen Sie die Option **Nachbarschafts-Setup überspringen**.
7. Wählen Sie **Wiederinbetriebnahme** aus, um das Gerät automatisch neuzuregistrieren, nachdem Daten gelöscht wurden, sodass Sie nach einer Komplettlöschung das Gerät nicht manuell neuregistrieren müssen. Dies gilt nur für iOS-Geräte ab Version 17, die im DEP-Modus registriert wurden.
   1. Wählen Sie die **WLAN-Konfiguration** aus dem Dropdownmenü aus. Der Benutzer muss sämtliche Aktivierungssperren deaktivieren. Dies gilt nur für iOS-Geräte ab Version 17, die im DEP-Modus registriert wurden.
   2. Wählen Sie optional **Apps beibehalten** aus, wenn Sie möchten, dass die Geräte mit den vorhandenen, beibehaltenen Apps wieder in Betrieb genommen werden. Es werden nur diejenigen Apps beibehalten, die unter Verwendung von Ivanti N-MDM mit hoher Priorität installiert wurden. Gilt nur für iOS 26.+-Geräte.
8. Bei macOS-Geräten können Sie eine 6-stellige PIN als Passcode an das Gerät senden. Auf dem Gerät wird der Benutzer aufgefordert, die PIN einzugeben, um auf das Gerät zuzugreifen. Um die Löschaktion fortzusetzen, muss der Gerätebenutzer folgende Schritte ausführen:
   1. Geben Sie die PIN ein.
   2. Er muss das Kontrollkästchen markieren, um die Löschaktion des Geräts zu bestätigen.
   3. Klicken Sie auf **Ja, dieses Gerät komplett löschen.**
9. Wenn Sie auf einem ChromeOS-Gerät eine Komplettlöschung über die Seite **Gerätedetails** oder **Geräteliste** durchführen, wird folgende Meldung angezeigt: "Bei einer Komplettlöschung wird das Gerät auf die Werkseinstellungen zurückgesetzt. Dadurch können auf dem Gerät gespeicherte Daten verloren gehen. Die Durchführung einer Komplettlöschung unterscheidet sich je nach Plattform."
   1. Markieren Sie das Kontrollkästchen "Ich habe verstanden, dass eine Komplettlöschung nicht rückgängig gemacht werden kann", um die Komplettlöschung des Geräts zu bestätigen.
   2. Klicken Sie auf **Komplett löschen**, um das Gerät vollständig zurückzusetzen.

Der Gerätestatus wechselt in **Komplettlöschung gesendet**. Der aktualisierte Gerätestatus wird nach der regelmäßigen Gerätesynchronisierung angezeigt.

Auf Geräten mit Android Enterprise können Sie die Aktion **Komplettlöschung** auch dann ausführen, wenn das Gerät neu gestartet wurde und gesperrt bleibt.

Android-Geräte mit dem Status **Komplettlöschung ausstehend** können jetzt mithilfe der Option **Gerät löschen** der Seite **Gerätedetails** gelöscht werden. Nachdem ein Gerät gelöscht wurde, wird es vom Server getrennt und ist nicht mehr konform. Nach dem Zurücksetzen auf die Werkseinstellungen muss der Benutzer das Gerät neu registrieren.

7.5.34. Löschen von Geräten

Nachdem Sie ein Gerät außer Dienst gestellt haben, können Sie es löschen. Durch das Löschen wird es von allen Seiten entfernt. Sie können ein Gerät nur löschen, wenn sein Status "Stillgelegt", "Stilllegung ausstehend", "Komplett gelöscht" oder "Komplettlöschung ausstehend" lautet.

Verfahren

1. Wechseln Sie zu **Geräte > Geräte**. Die Geräteliste wird angezeigt.
2. Wählen Sie das zu löschende Geräte aus.
3. Klicken Sie auf **Aktionen**.
4. Wählen Sie im Abschnitt **Allgemein** die Option **Geräte löschen** aus. Ein Popup-Fenster wird angezeigt.
5. Wählen Sie "Ich bin mir darüber im Klaren, dass der Löschvorgang nicht rückgängig gemacht werden kann" aus und klicken Sie anschließend auf **Gerät(e) löschen**.
6. Alternativ können Sie ein Gerät löschen, indem Sie folgende Schritte durchführen:
   - Gehen Sie zu **Geräte** > **Geräte**.
   - Klicken Sie in der Spalte **Anzeigename des Benutzers** auf einen Link. Die Seite **Gerätedetails** wird angezeigt. Klicken Sie auf **Gerätedetails**. Ein Popup-Fenster wird angezeigt. Wenn Sie die Warnmeldung bestätigen und auf **OK** klicken, wird das betreffende Gerät gelöscht.

Löschen mehrerer Geräte

Sie können mehrere Geräte löschen, indem sie die betreffenden Geräte auswählen.

Verfahren

1. Gehen Sie zu **Geräte > Geräte**.
2. Wählen Sie die Geräte in der Liste der verfügbaren Geräte aus.
3. Klicken Sie auf die Registerkarte **Aktionen** und wählen Sie unter dem Titel **Allgemein** die Option **Geräte löschen** aus.
4. Gehen Sie im Fenster **Gerät(e) löschen** folgendermaßen vor:
   1. Markieren Sie das Kontrollkästchen **Ich bin mir darüber im Klaren, dass der Löschvorgang nicht rückgängig gemacht werden kann**.
   2. Klicken Sie auf **Gültige(s) Gerät(e) löschen**, um die ausgewählten Geräte zu löschen.

7.5.35. Gerät entsperren

Dieser Abschnitt enthält die folgenden Themen:

- Android-Geräte entsperren
- AppConnect für Android-Apps entsperren
- iOS-Gerät entsperren
- Entsperren von ChromeOS-Geräten

So entsperren Sie ein Gerät:

Sie können die Bildschirmsperre auf einem Gerät deaktivieren. Bei verschiedenen Geräten unterscheidet sich die Deaktivierung der Sperre jeweils etwas.

Verfahren

1. Gehen Sie zu **Geräte > Geräte**.
2. Wählen Sie die entsprechenden Geräte aus.
3. Klicken Sie auf **Aktionen**.
4. Wählen Sie **Entsperren**.
5. Sie können auch auf den Link mit dem Gerätenamen klicken, um die Seite mit den Gerätedetails aufzurufen und dann auf das Symbol für **Entsperren** und dann auf **OK** klicken.

Android-Geräte entsperren

Wenn die Android-App einen Entsperrbefehl empfängt, versucht sie, den Passcode zurückzusetzen. In den Modi Geräte-Admin und Geräteeigentümer wird der Entsperrcode zurückgesetzt. In den Modi Profileigentümer und COPE wird der Entsperrcode des Arbeitsprofils zurückgesetzt.

Der Entsperrbefehl bietet dem Administrator die Option, den Entsperrcode als Kombination aus alphanumerischen Zeichen zu definieren. Die Standardoption, über die der Entsperrcode auf '0000' gesetzt wird, kann auf mehreren Geräten durchgeführt werden. Die neue Option "Benutzerdefinierter Entsperrcode für Android" kann jedoch immer nur auf einem Gerät gleichzeitig durchgeführt werden. Die Mindestzahl der Zeichen ist 6, die Höchstzahl 8. Diese Option ist auf der Registerkarte **Aktionen** und auf der Seite **Gerätedetails** verfügbar. Wenn Sie die Entsperrfunktion auf der Registerkarte **Aktionen** oder auf der Seite **Gerätedetails** auswählen, werden folgende Optionen angeboten:

- Standard
- (Nur Android) Geben Sie einen Entsperrcode an. Sie können einen Entsperrcode über diesen Abschnitt bereitstellen und auf **Sperre aufheben** klicken.
    - Geräteaufforderung zum Zurücksetzen des Passcodes überspringen – Wählen Sie diese Option, um das Zurücksetzen des Passcodes zu überspringen, wenn die Passcode-Konfiguration via Push an ein Gerät übertragen wird.

Nach Festlegen des Entsperrcodes kann der Administrator diesen auf den Seiten **Audit-Protokolle** und **Geräteprotokolle** anzeigen.

> Die Directboot-Entsperrung funktioniert nur für die Standard-Entsperroption mit dem Entsperrcode '0000'. Der benutzerdefinierte Entsperrcode für direktes Starten wird nicht unterstützt.

AppConnect für Android-Apps entsperren

Bei AppConnect-Apps können Sie mit dem Befehl **AppConnect entsperren** Container entsperren, die gesperrt wurden, weil die Benutzer sich mehrmals mit falschen Passcodes angemeldet haben. Durch diese Entsperrung wird das Gerät selbst nicht entsperrt.

iOS-Gerät entsperren

Wenn ein Unlock-Befehl empfangen wird, entfernt die iOS App den Passcode vom Gerät. Wenn die **Passwortkonfiguration** festlegt, dass ein neues Passwort benötigt wird, wird der Gerätebenutzer aufgefordert, ein neues Passwort entsprechend den für die Passwortkonfiguration definierten Regeln einzugeben. Der Benutzer muss diese Änderung innerhalb von 60 Minuten vornehmen, anderenfalls erzwingt die App vom Benutzer die Definition eines neuen Passworts.

Entsperren von ChromeOS-Geräten

Wenn ein ChromeOS-Gerät ausgewählt und auf die Option **Entsperren** geklickt wird, wird ein Popup-Fenster mit folgender Meldung angezeigt: "Durch das Entsperren wird eventuell ein bestehender Passcode gelöscht, um einem Benutzer den Zugang zum Gerät zu ermöglichen. Entsperrungen unterscheiden sich je nach Plattform." Wenn Sie auf **Entsperren** klicken, wechselt der Gerätestatus in "Entsperren gesendet". Der aktualisierte Status wird nach der regelmäßigen Gerätesynchronisierung angezeigt.

7.5.36. Geräte neu starten und herunterfahren

Dieser Abschnitt enthält die folgenden Themen:

- Gerät neu starten
- Gerät ausschalten

Gilt für: Android 7.0+ (verwaltete Geräte), iOS 10.3+ überwacht, tvOS 10.3+ überwacht, macOS 10.13+ und Windows 10+-Geräte.

Administratoren können ein überwachtes iOS-Gerät einzeln oder über die Gerätedetailseite oder als Gruppe über die Gerätelistenseite neu starten oder herunterfahren.

Gerät neu starten

Verfahren

1. Gehen Sie zu **Geräte**.
2. Navigieren Sie zu dem Gerät.
3. Klicken Sie in der Spalte **Name** auf den Link.
4. Klicken Sie auf die Schaltfläche **Aktionen**.
5. Klicken Sie auf **Gerät neu starten/herunterfahren**.

> Nicht unterstützte Geräte können nicht neu gestartet werden.

6. Lesen Sie die angezeigte Warnung.
7. (Optional) Wählen Sie die Option aus, um den Passcode beim Neustart von dem Gerät zu löschen. Wenn der Passcode nicht gelöscht wird, fordert das Gerät einen Passcode an und stellt nach dem Neustart keine Verbindung mit dem WLAN her.
8. Wählen Sie, sofern noch nicht geschehen, **Gerät neu starten**.
9. Wenn Sie das Gerät trotzdem neu starten wollen, klicken Sie auf **An Gerät senden**. Andernfalls klicken Sie auf **Abbrechen**.

> Bei Android-Geräten können Administratoren die Startzeit des Geräts unter Uptime auf der Seite „Gerätedetails“ einsehen.

Sie können mehrere unterstützte Geräte über die Listenseite **Geräte** neu starten. Wählen Sie dazu die Geräte aus, klicken Sie auf **Aktionen > Gerät neu starten/herunterfahren** und folgen Sie den Anweisungen auf dem Bildschirm.

Gerät ausschalten

Verfahren

1. Gehen Sie zu **Geräte**.
2. Navigieren Sie zu dem Gerät.
3. Klicken Sie in der Spalte **Name** auf den Link.
4. Klicken Sie auf die Schaltfläche **Aktionen**.
5. Klicken Sie auf **Gerät neu starten/herunterfahren**.

> Nicht unterstützte Geräte können nicht neu gestartet werden.

6. Lesen Sie die angezeigte Warnung.
7. Wählen Sie die Option **Gerät herunterfahren**.
8. Wenn Sie das Gerät trotzdem noch herunterfahren wollen, klicken Sie auf die Option **An Gerät senden**. Andernfalls klicken Sie auf **Abbrechen**.

Sie können mehrere unterstützte Geräte über die Listenseite **Geräte** herunterfahren. Wählen Sie dazu die Geräte aus, klicken Sie auf **Aktionen > Gerät neu starten/herunterfahren** und folgen Sie den Anweisungen auf dem Bildschirm.

7.5.37. Passwort-Einschränkungen löschen (nur iOS)

Sie können ein Beschränkungs-Passwort löschen, das der Benutzer auf einem überwachten Gerät mit iOS 8 gesetzt hat. Diese Aktion steht nur für aktive Geräte zur Verfügung.

Verfahren

1. Gehen Sie zu Geräte > Geräte.
2. Wählen Sie den Geräteeintrag.
3. Wählen Sie [Actions > Clear Restrictions Password]
4. Bestätigen Sie auf Aufforderung die Aktion.

7.5.38. Sentry-Zuordnung für ein Gerät löschen

Die Sentry-Zuordnung erfolgt für Geräte mit aktivierter Tunneling-App oder aktivierter ActiveSync für das E-Mail-System und kontrolliert den Zugriff der Geräte auf E-Mails. Falls erforderlich, kann für jedes Gerät, das Sentry zugeordnet ist, die Zuordnung wie folgt aufgehoben werden:

Verfahren

1. Gehen Sie zu **Geräte.**
2. Klicken Sie in der Spalte **Name** auf den Gerätelink des Gerätes, dessen Sentry-Zuordnung Sie löschen wollen.
3. Klicken Sie auf die Registerkarte "**Sentry**".
4. Klicken Sie in der Spalte **Aktionen** auf **Löschen**.

7.5.39. Anpassbare Attribute für Geräte zuweisen

Sie können für eines oder mehrere Geräte angepasste Attribute zuweisen, beispielsweise eine interne ID. Jedes Attribut hat einen entsprechenden Wert, den Sie für Aufgaben wie die Erstellung von Konfigurationen und Gerätegruppen verwenden können. Nachdem Sie benutzerdefinierte Attribute erstellt haben, können Sie sie Geräten zuweisen. Weitere Informationen zum Verwalten von Attributen finden Sie unter **Attribute**.

Verfahren

1. Melden Sie sich beim Administrationsportal an.
2. Gehen Sie zu **Geräte**.
3. Wählen Sie mindestens ein Gerät aus.
4. Klicken Sie auf **Aktionen**.
5. Wählen Sie die Option **Benutzerdefinierte Attribute zuweisen**.
6. Wählen Sie *eine* der folgenden Optionen aus:
    - Zuweisung (Überschreiben) aller Attribute erzwingen, selbst wenn Werte vorhanden sind.
    - Nur überschreiben, wenn der Wert leer ist, Attribute mit vorhandenen Werten überspringen

Wählen Sie die Attribute aus, die Sie zuweisen wollen, und geben Sie deren Werte ein (leere Werte sind nicht zulässig).

8. Klicken Sie auf **Zuweisen**.

> Die **benutzerdefinierten Geräteattribute** und ihre Werte lassen sich über die Seite **Gerätedetails** in das CSV-Format exportieren.

7.5.40. Anpassbare Attribute von Geräten entfernen

Arbeiten Sie überlegt, da diese Aktion nicht rückgängig gemacht werden kann. Zur Entfernung kundenspezifischer Attribute von einem oder mehreren Geräten gehen Sie wie folgt vor:

Verfahren

1. Gehen Sie zu **Geräte**.
2. Wählen Sie mindestens ein Gerät aus.
3. Klicken Sie auf **Aktionen**.
4. Wählen Sie die Option **Angepasste Attribute entfernen**.
5. Wählen Sie die Attribute aus, die Sie entfernen möchten.
6. Klicken Sie auf **Entfernen**.

7.5.41. App-Feedback synchronisieren und abrufen

Sie können eine Anfrage an eine auf Android-Geräten installierte App senden, um Details des aktuellen App-Konfigurationsstatus der App zu erhalten. Wenn eine Anforderung gesendet wird, erhalten Sie einen Bericht über die App-Konfiguration für das Gerät.

Verfahren

1. Gehen Sie zu **Geräte**.
2. Klicken Sie auf das Gerät, für das Sie die Anfrage senden möchten.
3. Klicken Sie auf **Aktionen**.
4. Wählen Sie **App-Feedback synchronisieren und holen**. Die Anforderung wird gesendet, um die App zu synchronisieren und das App-Konfigurations-Feedback zu holen. Das Feld „App Feedback letzte Synchronisation“ neben dem Feld „Client letzte Anmeldung“ wird aktualisiert.
5. Klicken Sie auf der Registerkarte Installierte Apps auf den Link Details anzeigen für die App in der Spalte App-Feedback.Das Fenster **App Feedback** wird angezeigt.
   Schlüssel – Bietet ausführliche Informationen und ermöglicht die Platzierung gemeldeter Einstellungen (in der verwalteten App-Konfiguration der App) basierend auf dem Feedback, das von den Apps eingeht.
   Zeitstempel - Zeit und Datum des Schlüssels.
   Schweregrad - Gibt den Schweregrad des Schlüssels an. Beispiel: „Info“, „Fehler“.
   Nachricht - Art der Nachricht, die als Rückmeldung der App-Konfiguration empfangen wird. Beispiel: „Fehler“.
   Daten - Details der Daten, die als Rückmeldung von der App-Konfiguration empfangen wurden.

App-Konfigurations-Feedback aus dem App-Katalog anzeigen

Sie können den Feedback-Bericht zur App-Konfiguration für die jeweilige App im App-Katalog einsehen.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Wählen Sie eine App aus, für die Sie Details anzeigen möchten.
3. Klicken Sie auf die Registerkarte **App-Konfigurations-Feedback**. Die Spalte **Geräteanzahl** zeigt die Anzahl der Geräte (Hyperlink) für jeden Schlüssel des Feedback-Berichts der App-Konfiguration.
4. Klicken Sie auf den Hyperlink zur Anzahl der Geräte, um die Details der Geräte anzuzeigen. Wenn Sie beispielsweise auf Hyperlink 5 klicken, werden die Details von 5 Geräten angezeigt. Für die Kombination aus „Schlüssel“ und „Schweregrad“ über der Tabelle werden folgende Details angezeigt:
   E-Mail-Adresse - gibt den Benutzernamen an. Wenn Sie auf den Link „Benutzername“ klicken, gelangen Sie zur Registerkarte **Installierte Apps** unter **Geräte> Gerätedetails**.
   Gerätetyp - gibt das Gerätemodell an.
   OS - Android OS-Versionsnummer.
   Seriennummer - Die Seriennummer des Geräts.
   Zeitstempel - Uhrzeit und Datum der letzten Aktualisierung.
   Nachricht - Art der Nachricht, die als Rückmeldung der App-Konfiguration empfangen wird. Beispiel: „Fehler“.
   Daten - Details der Daten, die als Rückmeldung von der App-Konfiguration empfangen wurden.

Sie können die Fehlerbenachrichtigungen der App-Konfiguration für das Android-Gerät anzeigen, indem Sie auf das Glockensymbol (oben rechts) oder auf der Seite **Dashboard > Benachrichtigungen** klicken. Wenn Sie auf den Link zur Benachrichtigung klicken, wird die Registerkarte **App-Konfigurations-Feedback** aufgerufen und der Feedback-Bericht der App angezeigt.

Der App-Config-Feedback-Bericht wird entfernt und nicht mehr angezeigt, wenn das Gerät gelöscht oder außer Dienst gestellt wird. Ein Hintergrundjob, der alle 24 Stunden gestartet wird, bereinigt Daten, die älter als 7 Tage sind.

7.5.42. Definition des Firmware-Passworts

Gilt für: macOS 10.13 oder unterstützte neuere Versionen.

Der Administrator kann das Firmware-Passwort (EFI) für ein macOS-Gerät konfigurieren oder aktualisieren. Ein Firmware-Passwort verhindert, dass das macOS-Gerät über ein internes oder externes Speichergerät gestartet wird, das nicht das vom Gerätebenutzer ausgewählte Startlaufwerk ist. Infolge dessen lassen sich auch die meisten Start-Tastenkombinationen nicht verwenden.

Schritte:

1. Gehen Sie zu **Geräte**.
2. Firmware-Passwort für ein einzelnes Gerät konfigurieren oder ändern:
    1. Klicken Sie auf den Benutzernamen, dem das Gerät zugeordnet ist, um die Gerätedetailseite anzuzeigen.
    2. Erweitern Sie im Abschnitt Allgemein die Anzeige für **Firmware-Passwort** und klicken Sie auf **Passwort einstellen** oder im Aktionsmenü des Geräts auf **Firmware-Passwort einstellen/ändern**.
    3. Folgende Informationen werden in diesem Abschnitt angezeigt:
        1. **Passwort:** Das Passwort bzw. eine Liste möglicher Passwörter

        > Wenn ein Administrator das Firmware-Passwort konfiguriert, wird der Befehl an das Gerät gesendet. Wenn das Gerät nicht rechtzeitig reagiert, wird das Passwort temporär gespeichert und in diesem Feld angezeigt. Das neue Passwort wird erst wirksam, wenn eine Bestätigung von dem Gerät eingeht und das Gerät neu startet. Bis dahin werden alle möglichen Passwörter angezeigt. Nach dem Neustart des Geräts und Bestätigung der Passwort-Änderung werden alle nicht gewünschten Passwörter gelöscht.

        2. **Änderung ausstehend:** Gibt an, dass die Kennwortänderung noch aussteht.
        3. **Befehlsstatus:** Gibt an, ob die Kennwortänderung erfolgreich oder erfolglos war.
        4. **Option ROMs zulassen:** Gibt an, ob die Option ROMs aktiviert werden soll. Standardmäßig ist die Option auf Nein eingestellt.

Firmware-Passwort für mehr als ein Gerät einstellen oder ändern:

1. Wählen Sie die entsprechenden Geräte aus.
2. Klicken Sie im Aktionsmenü auf **Firmware-Passwort konfigurieren/ändern**.

Geben Sie das aktuelle und das neue Passwort ein.

Wenn Sie das Passwort erstmals definieren, kann das aktuelle Passwort leer sein.

Lassen Sie zum Zurücksetzen des Passworts das Feld für das neue Passwort leer.

5. Klicken Sie auf **Speichern**.

> Nur Geräte mit unterstützten macOS-Versionen werden mit dem neuen Passwort aktualisiert. Nicht unterstützte Geräte werden übersprungen.

7.5.43. Neuen persönlichen Wiederherstellungsschlüssel ausstellen

Gilt für: macOS-Geräte mit Mobile@Work für macOS 1.66 oder unterstützte neuere Versionen.

Bei der Migration von anderen MDM-Lösungen zu Ivanti Neurons for MDM können Administratoren das Betriebssystem auffordern, bei der Registrierung einen neuen Personal Recovery Key (PRK) auszustellen, wenn vor der Registrierung bereits ein PRK ausgestellt wurde. Dies ermöglicht die Speicherung des Schlüssels in Ivanti Neurons for MDM.

Sie können die Audit-Protokolleinträge für die PRK-Aktivitäten wie folgt anzeigen:

1. Gehen Sie zu **Dashboard > Audit-Protokolle**.
2. Wählen Sie im Filter „Typ“ die Option Persönlicher Wiederherstellungsschlüssel. PRK-Einträge werden in der Kategorie „Geräteverwaltung und Aktivitäten“ beispielsweise als „Angezeigter persönlicher Wiederherstellungsschlüssel“ angezeigt.

Voraussetzung

Verteilen Sie die folgenden Konfigurationen auf die Geräte, bevor Sie diesen Vorgang durchführen:

- Mobile@Work für die macOS-Konfiguration.
- FileVault-Wiederherstellungsschlüssel-Konfiguration.

Verfahren

1. Wenden Sie sich an den **Support**, um das Skript zur Erzeugung neuer PRK auf dem Gerät anzufordern.
2. Erstellen Sie ein benutzerdefiniertes Geräteattribut mit dem Namen „deviceprk“, das im Skript verwendet wird.
3. Laden Sie das Skript in das Repository unter **Admin > Skripte und Dateien > Alle Skripte hoch**. Wählen Sie dabei das benutzerdefinierte Attribut „deviceprk“ aus.
4. Erstellen Sie eine dynamische Gerätegruppe für Geräte, deren PRK nicht von der alten MDM-Lösung abgerufen wurde. Wählen Sie die Gerätegruppenregeln wie folgt aus: **Plattform=macOS** und **Verschlüsselung aktiviert ist gleich Ja** und **Persönlicher Wiederherstellungsschlüssel für macOS ist gleich Nein** und **Wiederherstellungsschlüssel für macOS ist gleich Persönlich**.“
5. Erstellen Sie eine Mobile@Work für macOS Skript-Konfiguration, in der Sie das PRK-Skript aus dem Repository auswählen können. Verteilen Sie die Konfiguration auf die neue Gerätegruppe.
6. Planen Sie das Skript so, dass es einmal täglich oder nach Wunsch ausgeführt wird. Dieses Skript fragt bei jeder Ausführung nach dem Benutzer-Passwort. Standardmäßig beträgt die Timeout-Periode für die Skriptausführung 60 Sekunden. Sie sollten die Timeout-Zeit in der entsprechenden Mobile@Work für MacOS-Konfiguration verlängern, indem Sie das **Feld Max. Startzeit** auf 300 Sekunden setzen.

- Der entschlüsselte Schlüssel ist auf der Gerätedetailseite eines Gerätes im Abschnitt „Geräteverschlüsselungsstatus“ verfügbar. Klicken Sie neben dem Feld **FileVault-Verschlüsselung aktiviert** auf „Anzeigen“.
- Nach Erhalt des PRKs verlässt das Gerät die Gerätegruppe. Die Skriptkonfiguration ist dann nicht mehr anwendbar und wird vom Gerät gelöscht.
- Nachdem MDM den Wiederherstellungsschlüssel eines Geräts mit Hilfe des Skripts abgerufen hat, wird das Skript vom Gerät deinstalliert.

Verwandte Themen:

- **Attribute**
- **Alle Skripte**
- **Gerätegruppen**
- **Mobile@Work für macOS**
- **FileVault-Wiederherstellungsschlüssel**

7.5.44. Wiederherstellungssperre einstellen oder ändern

Gilt für: macOS 11.5+

Der Administrator kann die Wiederherstellungssperre für den Neustart eines macOS-Geräts mit Apple Silicon einstellen oder ändern. Eine Wiederherstellungssperre verhindert den Start der macOS-Geräte im Wiederherstellungsmodus, es sei denn, der Passcode wird eingegeben.

Schritte:

1. Gehen Sie zu **Geräte**.
2. So können Sie die Wiederherstellungssperre für den Neustart einstellen oder ändern:
    1. Klicken Sie auf den Anzeigenamen des Benutzers, dem das Gerät zugeordnet ist, um die Gerätedetailseite anzuzeigen. Führen Sie eine der folgenden Schritte aus:
    2. Erweitern Sie im AbschnittÜbersichtden EintragWiederherstellungssperreund klicken Sie aufPasswort einstellenoder aufPasswort ändern. Oder klicken Sie auf die Ellipse nebenAktionenund dann aufWiederherstellungssperre einstellen/ändern.
    3. Gehen Sie im Dialogfeld **Wiederherstellungssperre einstellen/ändern** wie folgt vor:
        1. Aktuelles Passwort: Geben Sie hier das aktuelle Passwort ein. Lassen Sie das Feld leer, wenn Sie das Passwort erstmalig einstellen.
        2. Passwort: Geben Sie das einzustellende Passwort ein.
        3. Passwort bestätigen: Geben Sie das einzustellende Passwort erneut ein.

Klicken Sie aufWiederherstellungssperre einstellen/ändern.

> In der Übersicht zeigtWiederherstellungssperre aktiviertden Status des Passcodes für die Wiederherstellungssperre.

> Administratoren können den Passcode bei Bedarf löschen. Entfernen Sie hierzu den vorhandenen Passcode und klicken Sie aufWiederherstellungssperre einstellen/ändern.

7.5.45. Apple-Zugriffsverwaltung

Voraussetzungen:

- Überprüfen und sperren Sie die Domäne in Apple Business Manager oder Apple School Manager.
- Konfigurieren Sie mindestens einen MDM-Server über die Apple Business Manager- oder Apple School Manager-Organisation, wenn verwaltete Apple-IDs in Ivanti Neurons for MDM vorhanden sind.

Mit der Anmeldung bei einer verwalteten Apple-ID können Organisationen steuern, auf welche Apple-Dienste und -Funktionen Benutzer Zugriff haben.

In Apple Business Manager oder Apple School Manager wird über die Einstellung **Verwalteten Apple Account zulassen auf** gesteuert, wo sich Benutzer mit ihrer verwalteten Apple-ID anmelden können. Administratoren können diese Einstellung konfigurieren, um die Anmeldung auf verwaltete oder überwachte Geräte zu begrenzen oder auf einem beliebigen Gerät zuzulassen.

- **Beliebiges Gerät** (Standard): Benutzer können sich auf einem beliebigen Gerät mit ihrer verwalteten Apple-ID anmelden, unabhängig davon, ob dieses von einer MDM-Lösung verwaltet wird.
- **Nur verwaltete Geräte**: Benutzer können sich nur bei Geräten anmelden, die von einer MDM-Lösung mit Unterstützung für den Get Token-Endpunkt verwaltet werden.
- **Nur überwachte Geräte**: Benutzer können sich nur bei Geräten anmelden, die von einer MDM-Lösung mit Unterstützung für den Get Token-Endpunkt überwacht (und verwaltet) werden.

Diese Einstellungen sind Teil der allgemeineren "Zugriffsverwaltung" für Apple-Dienste innerhalb von Apple Business Manager und Apple School Manager.

> Mit erweiterter Sicherheit lässt sich durch das Einschränken der Anmeldung auf verwaltete oder überwachte Geräte die Datensicherheit verbessern, indem sichergestellt wird, dass berufliche Daten nur auf kontrollierten Geräten verfügbar sind.

Die Anmeldung beim verwalteten Apple Account schlägt fehl, wenn null oder mehrere Geräteregistrierungs-MDM-Server-Organisationen auf der Registerkarte **Geräteregistrierung** vorhanden sind und der Administrator in Apple Business Manager oder Apple School Manger die Einstellung **Verwalteten Apple Account zulassen auf** unter **Zugriffsverwaltung** > **Apple-Dienste** auf "Nur überwachte Geräte" oder "Nur verwaltete Geräte" gesetzt hat.

> Die Geräte können sich nicht anmelden, wenn der **Verwaltete Apple Account** nicht auf dem Ivanti Neurons for MDM Geräteregistrierungs-MDM-Server vorhanden ist.

7.5.46. Registrierung über Gruppenrichtlinie

Windows 10/11-Geräte können unter Verwendung einer Gruppenrichtlinie bei Ivanti Neurons for MDM registriert werden. Durch Erstellen einer Gruppenrichtlinie werden automatisch alle Geräte mit Hybrid-Beitritt zu Azure AD registriert.

ProcedureSo registrieren Sie Geräte mit einer Gruppenrichtlinie:

1.	**Stellen Sie sicher, dass Ihre Geräte hybrid in Azure AD eingebunden wurden. Weitere Informationen finden Sie in der Microsoft-Dokumentation zum Thema Hybrides Einbinden von Geräten in Azure AD.**
2.	**Erstellen Sie ein Gruppenrichtlinien-Objekt (GPO). Weitere Informationen finden Sie in der Microsoft-Dokumentation zum Thema Konfigurieren der automatischen Registrierung für eine Gerätegruppe.**
3.	**Erstellen Sie eine Sicherheitsgruppe, in der die Geräte, die Sie registrieren möchten, enthalten sind. Weitere Informationen finden Sie in der Microsoft-Dokumentation zum Thema Active Directory-Sicherheitsgruppen.**
4.	**Verknüpfen Sie das Gruppenrichtlinien-Objekt mit der Sicherheitsgruppe. Weitere Informationen finden Sie in der Microsoft-Dokumentation zum Thema Verknüpfen des Gruppenrichtlinien-Objekts (GPO) mit der Domäne.**

Benutzererfahrung

Wenn sich ein Benutzer unter Verwendung von Anmeldeinformationen in Azure AD am Gerät anmeldet, erkennt Microsoft die zu dessen Unternehmen gehörige Azure AD-basierte MDM-Konfiguration. Das Gerät wird bei Ivanti Neurons for MDM registriert und kann Richtlinien und Befehle empfangen.

8. Apps

Dieser Abschnitt enthält die folgenden Themen:

- App-Katalog
- Apps@Work
- iOS Apps@Work AppStore-Funktionen
- Anzeige der App-Details
- App-Konfiguration
- Zuweisen benutzerdefinierter Attribute zu Apps
- Verwaltete Konfigurationen für Android
- Verwaltung von Google Play-Apps
- Löschen von Apps aus dem App-Katalog
- Upgrading von hauseigenen Apps
- Suche des Paketnamens für eine Android App
- Kategorien
- Verteilungsfilter
- Ausschließen oder Verteilen von Apps
- Rezensionen
- Apple Apps and Books
- Katalogeinstellungen
- App-Abhängigkeiten bereitstellen
- Bereitstellen von Divide Productivity mit Android Enterprise
- Konfiguration der Provisioner-App
- Verwalten von Windows-Anwendungen
- Ivanti Bridge

8.1. App-Katalog

Dieser Abschnitt enthält die folgenden Themen:

- Lizenzierung für App-Funktionen
- Zwischen Listen- und Rasteransicht umschalten
- App aus dem Google Play Store in Android Enterprise hinzufügen
- App aus einem öffentlichen Store hinzufügen
- Hinzufügen einer internen App
- Geräteberechtigungen für interne Android Enterprise Apps delegieren
- Bereitstellungsprofilstatus für eigene iOS-Apps anzeigen
- Bereitstellungsprofil für eigene iOS-Apps aktualisieren
- Hauseigene App in Google Play bereitstellen
- Web-App für Geräte mit Android Enterprise hinzufügen
- Web-App für iOS-Geräte hinzufügen
- Erweiterte Suche verwenden
- Exportieren von Apps in eine CSV-Datei

Ihren App-Katalog verwalten Sie mit der Seite "App-Katalog".Der App-Katalog listet die mobilen Apps auf, die Sie Ihren Benutzern zur Verfügung gestellt haben. Dazu gehören Apps, die Benutzer von öffentlichen App Stores herunterladen können, und Apps, die Sie mithilfe von Cloud verteilen möchten (interne Apps). Über AppConnect aktivierte Apps, GoClient for iOS und M@W for macOS sind ebenfalls als Business-Apps auf der Seite "App-Katalog" verfügbar. Dadurch ist es einfacher, sie für Konfigurations- und Verteilungszwecke zu importieren. Bei MAM-Only-Geräten werden iOS-Benutzer aufgefordert, das Zertifikat auszuwählen, um den Zugriff auf diese Apps zu authentifizieren, wenn sie den App Catalog öffnen.

MacBooks von Apple mit M1-Chipset unterstützen iPhone- und iPad-VPP-Apps. Nur der Administrator kann die unterstützten iPhone- und iPad-VPP-Apps per Push übertragen. Diese Option ist nicht für die Installation durch Benutzer über den App Catalog verfügbar.

Für Ivanti Neurons for MDM-Mandanten mit Android-Geräten gilt: Wenn Android Enterprise nicht bis Ende März 2021 aktiviert wird, können Administratoren nicht mit den Namen nach Apps suchen. Der Hinweis auf diese Änderung wird beim Aufruf der Anwendungskatalogseite mit einem Banner angezeigt. Dieses Banner wird so lange angezeigt, bis Android Enterprise bei diesen Mandanten aktiviert wird bzw. bis die Option 'Diese Meldung nicht mehr anzeigen' aktiviert wird.

- Die Installation der App im Hintergrund ist für öffentliche macOS-Apps nicht verfügbar. Die macOS-Apps können auch über Apple Apps and Books als Gerätelizenzen sowie bei Registrierungen durch Installation der App im Hintergrund bereitgestellt werden.
- Beim Hochladen der Ivanti Go-App auf den Ivanti Neurons for MDM-Server müssen Sie, wenn Sie die Option **In verwaltete App konvertieren** benötigen, außerdem die Option **Auf Gerät installieren** aktivieren.
- App-Katalog und App-Installation werden für SonimXP5S-Geräte nicht unterstützt.
- Android gestattet nicht, dass Apps mit aktiven Administratorrechten deinstalliert werden. Gehen Sie zur Deinstallation einer solchen App zu **Geräteinstellungen > Sicherheit > Geräteadministratoren** und deaktivieren Sie die Geräteadministratorrechte. Deinstallieren Sie dann die App.
- Wenn eine Android Enterprise-App manuell mithilfe des Android Enterprise Play Store auf dem Gerät installiert wird und der Administrator später die Verteilung der App wieder aufhebt, muss die App auch manuell deinstalliert werden.
- Interne Android-Apps können nicht hochgeladen werden, wenn die App komprimiert oder verschleiert ist.

- Öffentliche Apps werden auf **gemeinsam genutzten iPads** nicht unterstützt.
- Aufgrund einer von Apple definierten Einschränkung für Business-to-Business (B2B)-iOS-Apps, die im App-Katalog verfügbar sind, sind Beschreibungen und Screenshots der Apps auf der Registerkarte **Details** nicht verfügbar.
- Wenn Sie im App-Katalog oder im Administrationsportal nach einer App suchen, basieren die Suchergebnisse auf den Feldern **App-Name**, **Kommentar**, **Beschreibung**, **Anzeigeversion** und **Neuigkeiten**. Wenn die gesuchten App-Daten mit einem dieser Felder übereinstimmen, werden sie als Suchergebnisse angezeigt.

Lizenzierung für App-Funktionen

Die folgenden App-Funktionen benötigen eine zusätzliche Lizenzierung:

- Installation/-Deinstallation von Apps im Hintergrund: Silver-Lizenz
- Konfiguration pro Anwendung: Gold Lizenz
- Kundenspezifische AppConnect-Konfiguration: Gold-Lizenz
- Benutzerdefinierte **Android Enterprise**-Konfiguration: Silver-Lizenz

Wenn sich ein Android-Gerät im Kiosk-Modus befindet:

Wenn das Gerät im Kiosk-Modus arbeitet, können nur hauseigene Apps installiert werden. Sie können öffentliche Apps installieren, das Gerät muss jedoch den Kiosk-Modus beenden, um die betreffenden Apps zu installieren. Sie können auch die für die Nutzung auf Geräten im Kiosk-Modus verfügbaren Apps auf die Apps begrenzen, die von Ihrem Unternehmen genehmigt oder in der Whitelist enthalten sind. Bei Geräten mit Android 4.1 wird beim Start einer App, die nicht in der Whitelist enthalten ist, durch eine genehmigte App die betreffende App gestartet und dann sofort zum Symbol verkleinert. Bei Geräten mit Android 5.0 bleibt die nicht genehmigte App nach dem Start durch eine App aus der Whitelist weiter verfügbar.

Zwischen Listen- und Rasteransicht umschalten

Klicken Sie auf das Symbol für Liste oder Raster auf der rechten Seite des App-Katalogbildschirms.

App aus dem Google Play Store in Android Enterprise hinzufügen

- Sie können eine App aus dem Google Play Store zum App-Katalog hinzufügen und den Benutzern zur Verfügung stellen. Um eine App aus dem Google Play Store in Android Enterprise hinzuzufügen, müssen Sie die Aufnahme einer App in den App Catalog genehmigen lassen.
- Das Google Play Store-Layout für Android Enterprise-Geräte verfügt über eine Startseite für migrierte Geräte, die von einer Core-Instanz aus verwaltet werden, und einen Quick-Link zu Cloud, der alle Anwendungen anzeigt, die von der Cloud aus verwaltet werden. Wenn Sie Android Enterprise-Geräte von Core zu Ivanti Neurons for MDM migrieren, werden nur die gemeinsamen Anwendungen von Core und dem Ivanti Neurons for MDM-App-Katalog im Arbeitsprofil Google Play Store des Geräts aufgeführt. Sie können auf die Cloud-Schaltfläche klicken, um eine Liste aller Anwendungen anzuzeigen, die im Cloud App Catalog verfügbar sind.

Das Google Play Store-Layout für Android Enterprise-Geräte verfügt über eine Startseite für migrierte Geräte, die von einer Core-Instanz aus verwaltet werden, und einen Quick-Link zu Cloud, der alle Anwendungen anzeigt, die von der Cloud aus verwaltet werden. Wenn Sie Android Enterprise-Geräte von Core zu Ivanti Neurons for MDM migrieren, werden nur die gemeinsamen Anwendungen von Core und dem Ivanti Neurons for MDM-App-Katalog im Arbeitsprofil Google Play Store des Geräts aufgeführt. Sie können auf die Ivanti Neurons for MDM-Schaltfläche klicken, um alle Anwendungen anzuzeigen, die im Ivanti Neurons for MDM-App-Katalog verfügbar sind.

Voraussetzung

- Sie müssen Android Enterprise aktivieren, um auf Google Play Store-Anwendungen zuzugreifen und diese dem App-Katalog hinzuzufügen.

ProcedureVerfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Klicken Sie auf **[Add]** (oben links).

> Klicken Sie in der Dropdown-Liste auf Google Play und suchen Sie nach einer App im Google Play Store. Wenn Android Enterprise registriert ist, wird Google Play iFrame angezeigt.

3. Suchen Sie in dem Suchfeld nach der App und klicken Sie auf die App.
4. Klicken Sie auf **Fertig**.

> Die Genehmigung für eine genehmigte App kann durch Klicken auf **NICHT GENEHMIGT** wieder zurückgezogen werden.

Option	Beschreibung
Genehmigungseinstellungen	
Genehmigung beibehalten, wenn die App neue Berechtigungen verlangt. App-Genehmigung zurücknehmen, wenn diese App neue Berechtigungen verlangt **Genehmigungseinstellungen**	Erlaubt Benutzern, die aktualisierte App zu installieren. **Die App wird aus dem Store entfernt, bis sie erneut genehmigt wird.**
Teilnehmer hinzufügen	Geben Sie die E-Mail-Adresse ein, um Teilnehmer für die E-Mail-Benachrichtigungen zu ergänzen, wenn die Apps, die Sie genehmigt haben, neue Berechtigungen verlangen.

App aus einem öffentlichen Store hinzufügen

Können Sie eine App aus einem öffentlichen Store im App-Katalog ergänzen und den Benutzern zur Verfügung stellen.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Klicken Sie auf **[Add]**.
3. Gewünschte App auswählen:
4. Öffnen Sie den öffentlichen App-Store.
5. Geben Sie den Namen der App ein.
6. Wählen Sie die App in der Liste aus.
7. Klicken Sie auf **Weiter**.
8. App für Benutzer beschreiben:

9. Entfernen bzw. fügen Sie Kategorien hinzu.
10. Geben Sie eine optionale Beschreibung ein.
11. Klicken Sie auf **Weiter**.
12. App-Verteilung bestimmen:
13. Wählen Sie eine Verteilungsoption aus.
14. Erweitern Sie den Abschnitt **Erweiterte Optionen und App-Konfiguration**.
15. Beachten Sie für die Optionen die folgenden Anleitungen:

Einstellung	So gehen Sie vor
Auf einem Gerät installieren	Wählen Sie diese Option aus, um die Installation sofort nach der Registrierung zu beginnen. Der Benutzer wird aufgefordert, die Installation der App zu bestätigen, sofern nicht folgende Bedingungen erfüllt sind: • Das Gerät ist ein überwachtes iOS-Gerät für neue App-Installationen und App-Updates. • Das Gerät ist ein für App-Updates nicht überwachtes iOS-Gerät. • Die Benutzer haben sich für das Programm Apps and Books registriert. • Die Gerät ist ein Samsung Knox-Gerät und es wurde die Option für die Installation im Hintergrund ausgewählt. Bei öffentlichen iOS-Apps, die erstmalig auf dem Gerät installiert werden, zeigt der App-Katalog die Schaltfläche „Neu installieren“ an, damit der Benutzer die App erneut installieren kann. Die Neuinstallation wird durchgeführt, wenn sich die App-Version auf dem Gerät von der Version im iOS-App-Store unterscheidet.
App nicht im App-Katalog des Endbenutzers anzeigen	Wählen Sie diese Option aus, wenn Sie nicht wollen, dass der Benutzer die App im App-Katalog des Gerätes sieht.
Priorität für die Installation von Anwendungen festlegen	Wählen Sie „Hoch“, „Mittel“ oder „Niedrig“ für die Priorität der App-Installation während des Benutzer-Onboardings. Nur Apps mit hoher Priorität werden während des Benutzer-Onboardings installiert.
Erneute Push-Übertragung der App nach einer bestimmten Zahl fehlgeschlagener Versuche aussetzen (nur iOS)	Schalten Sie den Kippschalter auf ON, um eine erneute Push-Übertragung der App nach einer bestimmten Zahl fehlgeschlagener Versuche mit den folgenden Einstellungen auszusetzen: **Erneute Push-Übertragung stoppen** - Geben Sie die Anzahl der fehlgeschlagenen Push-Übertragungsversuche ein, nach denen die Push-Übertragung gestoppt werden soll. Die eingegebenen Werte sollten zwischen **1** und **999** liegen. **fehlgeschlagene Versuche, erneut versuchen nach** - Geben Sie ein, wie viele Stunden nach einem fehlgeschlagenen Neustart die Push-Übertragung erneut durchgeführt werden soll. Die eingegebenen Werte sollten zwischen **3** und **48** Stunden liegen.
(Nur Android) Bei Samsung-Knox-Geräten im Hintergrund installieren	Diese Option gilt nicht für öffentliche Apps.
(nur iOS und macOS) Per-App-VPN für diese App aktivieren	Wählen Sie diese Option aus, um für diese App eine Per-App-VPN-Konfiguration zu verwenden. Wählen Sie die Per-App-VPN-Konfiguration aus der Dropdownliste, die verwendet werden soll. Wählen Sie bei macOS nur die Tunnel-per-App-VPN-Konfiguration aus.
(Nur iOS): Backup in der iCloud und iTunes sperren.	Wählen Sie diese Option aus, um zu verhindern, dass Daten dieser App in der iCloud und iTunes gesichert werden.
(Nur iOS): Apps entfernen, wenn eine Registrierung rückgängig gemacht	Wählen Sie diese Option aus, um diese App zu entfernen, sobald das Gerät nicht mehr über die Cloud verwaltet wird.

Einstellung	So gehen Sie vor
wird.	
(Nur iOS): Anpassbare AppConnect-Konfiguration	Geben Sie für die AppConnect-fähige App die Schlüssel und die Werte ein, die die Präferenzen Ihrer kundenspezifischen Konfiguration definieren. Informationen zu den verfügbaren Schlüsseln finden Sie in der Dokumentation der App.
Verwaltete Einstellungen in iOS 7+	Geben Sie die für diese App definierten Schlüssel und Werte für eine unter iOS 7+ verwaltete App ein. Weitere Informationen über unterstützte Schlüssel finden Sie in der Dokumentation der App.

> Für **Android Enterprise**-Apps gibt es andere Optionen.

Klicken Sie auf **Weiter**

4. Wählen Sie eine Verteilungsoption aus:
5. Klicken Sie auf **+ Beschreibung hinzufügen**, um eine Kurzbeschreibung der Konfiguration einzugeben.

- Nicht empfohlen
- Empfohlene Liste
- Empfohlenes Banner
- Wenn Sie Empfohlenes Banner auswählen, geben Sie bitte Folgendes an:
    1. **Titel** – Geben Sie den Titel der Anwendung an.
    2. **Beschreibung** – Geben Sie Details zur Anwendung an.
    3. **Bannerstil** – Wählen Sie einer Bannerfarbe aus.

6. Sie können auch die Verteilung der Konfiguration ändern.
7. Klicken Sie auf **Fertig**, um die App-Konfiguration zu speichern.
8. Klicken Sie auf **Fertig**.

> Wenn Sie im App-Katalog nach einer Windows-App suchen, können Sie auch nach einer annähernd übereinstimmenden App suchen, indem Sie die Option **App-Name** oder **AppStore-ID** aus der Dropdownliste auswählen:

- **App-Name** – Wählen Sie diese Option aus und geben Sie den Namen der App an.
- **AppStore-ID** – Wählen Sie diese Option aus und geben Sie die AppStore-ID an.

Die Suche in der Windows Store-App unterstützt Win32-Store-Apps.

Stellen Sie sicher, dass das Winget-Tool zum Verwalten der Win32-Store-Apps auf dem Gerät verfügbar ist.

Hinzufügen einer internen App

Sie können eine interne App in den App-Katalog in den folgenden Dateiformaten hochladen. Das Hochladen einer großen Datei kann mehrere Minuten dauern. Die Anzahl der Versionen der internen Anwendungen ist auf 100 begrenzt. Wenn diese Zahl überschritten wird, löscht das Cloud-System die ältesten Versionen der Anwendung. Der Status des Anwendungsuploads und der Bereinigung wird aufgelistet und ist auf der Seite Audit-Protokolle sichtbar.

Der von Mobile@Work zurückgegebene MIP-App-Bestand ist bei einigen wenigen Apps möglicherweise nicht korrekt. Mobile@Work kann u. U. den Installationsstatus von Apps, die nicht am Standardspeicherort installiert sind, nicht erkennen. Bei diesen Apps trägt das Erkennungsskript bei, den richtigen App-Status auf dem Gerät zu ermitteln. Mobile@Work stellt das Vorliegen der App fest, wenn das Erkennungsskript den Exit-Code 0 zurückgibt. Bei allen anderen Exit-Codes gilt die App als nicht installiert. Mobile@Work stellt den Bestandsbericht für das Gerät anhand der erkannten Apps zusammen.

- IPA (iOS)
- MIP (Packager macOS-App)
- PKG (macOS)
- APK (Android)
- APPX, APPXBUNDLE, EXE und MSI (Windows)

> Bei Anwendungen wie PKG mit Skripten oder DMGs mit PKG und Skripten kann Mobile@Work für macOS nur eine Installationsanforderung erkennen. Es wird nicht gemeldet, ob die App gelöscht wurde oder ob die installierten Skripte entfernt wurden. Deshalb kann der Ivanti Neurons for MDM Server einen Installationsbefehl nicht erneut senden. Wenn die Verbindung beim Herunterladen der Apps getrennt wird, wiederholen Sie die App-Installation, indem Sie sich anmelden. Bei MIP-Anwendungen installiert Mobile@Work die MIP-Anwendung selbst dann nicht, wenn die Anwendung von dem Gerät entfernt wird, auf dem es von PKG oder DMG mit PKG und Skript installiert wurde, aber der PKG-Eintrag im Empfangsordner des Client-Geräts vorhanden ist.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Klicken Sie auf **[Add]** (oben links).
3. Wählen Sie unter **Plattformen für das Hochladen der Datei auswählen** Ihre Plattform (z. B. **Apple Apps**) und dann das spezifische Betriebssystem (z. B. iOS oder macOS) aus dem Dropdownmenü von Apple Apps aus.

> Wenn ein Benutzer eine Plattform auswählt und versucht, einen abweichenden Dateityp hochzuladen (wenn er z. B. Apple auswählt, aber dann eine .apk-Datei hochladen möchte), löst das System einen Fehler vom Typ "Ungültiges Dateiformat" aus.

4. Ziehen Sie die App-Datei in das gepunktete Feld oder klicken Sie auf **Datei auswählen** , um sie aus dem Dateisystem auszuwählen und zu bestätigen.
5. Klicken Sie auf **Weiter** (unten rechts).
6. Beschreiben Sie die App für die Benutzer und konfigurieren Sie vorausgesetzte Apps:
7. Fügen Sie Kategorien hinzu.
8. Wenn Sie ein macOS-Paket ergänzen und die Paketdatei mehr als eine App enthält (beispielsweise Pakete mit Microsoft Office und Cisco AnyConnect), werden die ausgewählten primären Apps zur Identifikation des installierten Pakets verwendet. Sofern konfiguriert, wird die VPN-Verbindung per App für diese Apps verwendet.
9. Geben Sie eine optionale Beschreibung ein.
10. **MSI-Produktcode**: Beim Hochladen der MSI-Apps wird der Produktcode der MSI-App automatisch in dieses Feld eingetragen.

> Markieren Sie die Option "Ich habe den MSI-Produktcode geprüft", um zu bestätigen, dass die richtige GUID eingetragen wird.

URL überschreiben: Geben Sie eine optionale URL zum Überschreiten der App-Quelle ein, wenn Apps aus einer anderen Quelle heruntergeladen oder große Dateien, wie Microsoft Office Installationsdateien, aus einem lokalen Netzwerk (HTTP und HTTPS) bezogen werden sollen. Für diese Optionen ist der Zugriff auf ein sicheres internes Netzwerk und die manuelle Synchronisation eines alternativen Servers erforderlich, auf dem die Apps gespeichert sind. Geben Sie erst einen Wert ein, wenn Sie die erforderliche Infrastruktur aufgebaut haben. Sie können diesen Wert bearbeiten, wenn Sie die App-Einstellungen für die spezifische App bearbeiten.

- Bei iOS-Apps müssen die URLs, mit denen die Original-URL überschrieben werden kann, das Format HTTP oder HTTPS aufweisen.
- Bei Apps für Android und macOS ist für die URLs zum Überschreiben nur das HTTPS-Format zulässig.
- Bei macOS-Apps muss die URL mit der Dateierweiterung ".pkg" enden.

6. **Befehlszeile** (Nur für 32-Bit-MSI-Apps für Windows) Geben Sie einen optionalen Befehlszeilenparameter ein, um Zusatzinformationen zu definieren, die bei der Bereitstellung der MSI-Dateien nicht Teil des Pakets sind. Um beispielsweise Installationsprotokolle in eine Ausgabedatei zu schreiben, können Sie in diesem Feld "/log output.txt" eingeben. Dadurch wird eine Datei output.txt im Ordner C:\Windows\System32 angelegt. Standardmäßig wird die Befehlszeilenoption /qn für die Installation im Hintergrund während des Hochladens von MSI-Anwendungen automatisch eingetragen.

> Der Paketname der hochzuladenden MSI-App sollte nicht als Teil der Befehlszeilenparameter hinzugefügt werden. Falls er hinzugefügt wird, wird der Upload blockiert, bis der Paketname der Anwendung aus den Befehlszeilenargumenten entfernt wird. Eine Liste aller unterstützten Befehlszeilenoptionen finden Sie unter dem zusätzlichen Link. Dieser Link wird im Ansichts- und Bearbeitungsmodus der App sichtbar sein.

.exe für Win32: Die Installation erfolgt über Bridge unter Verwendung des Admin PowerShell-Modus. Die Bridge-Funktionalität wird automatisch verwendet, falls verfügbar.

- Aktualisieren Sie die Version, um die Konsistenz zwischen **Anzeigeversion** und **Bundle-Version** zu gewährleisten.
- Speicherort des Installationsprogramms (.exe)
- Befehlszeilenparameter im Installationsprogramm: Argument zum Ausführen der Datei im Hintergrund (z. B. /SILENT oder /VERY SILENT) muss zwingend angegeben werden.
- Installationsprogramm als Benutzer ausführen: Wählen Sie 'Als Benutzer ausführen' aus, um die Installation mit den Anmeldeinformationen des Benutzers auszuführen.

Für Win32-Store-Apps: Die Installation erfolgt über Bridge unter Verwendung des Admin PowerShell-Modus.

9. Für Packager macOS-Apps konfigurieren Sie die als Voraussetzung benötigten Apps (optional). Einen Überblick über die Funktionalität der als Voraussetzung benötigten Apps finden Sie unter „interne Packager-macOS-Apps verstehen“.
10. **URL starten**: Geben Sie die benutzerdefinierte URL zum Start der App in AppStation ein. Nur erforderlich, wenn Nicht-AppConnect-Apps für die Verteilung in einer reinen MAM-only-Bereitstellung mit AppStation hinzugefügt werden. Gilt nur für iOS-Apps.
11. Konfigurieren Sie die **App-Delegierung**.

> Sobald Sie eine als Voraussetzung benötigte App delegiert haben und diese für die App aus dem Nicht-Standard-Space zu einer als Voraussetzung benötigte App wird, können Sie die Delegierung dieser App nur noch aufheben, wenn Sie zuerst die als Voraussetzung definierte Beziehung entfernen.

Klicken Sie auf **Weiter**.

13. Klicken Sie auf **Weiter**.
14. (Optional) Fügen Sie Screenshots der App hinzu.
15. (Optional) Fügen Sie Symbole für die App hinzu oder ersetzen Sie diese (iOS-, macOS- und Windows-Apps).
16. Klicken Sie auf **Weiter**.
17. Definieren oder wählen Sie für Packager macOS-Apps Installationsskripte, die vor und/oder nach der App-Installation ausgeführt werden. Wählen Sie eines oder beide der folgenden Skripte aus, indem Sie etwas in dem Suchfeld eingeben oder auf den Link klicken, um die Liste der Skripte anzuzeigen. Klicken Sie auf **Weiter**.
18. Sie können die Skripte auf der Seite **Admin > Skripte und Dateien > Alle Skripte** erstellen. Wenn Sie die Anwendung aktualisieren, können Sie die Skripte der älteren Anwendung kopieren und die Skripte für die aktualisierte Anwendung ausführen. Wenn Sie diesen Abschnitt überspringen, können Sie Skripte konfigurieren, indem Sie die App später bearbeiten.

- **Vorinstallations-Skripts** - Geben Sie den Skriptnamen ein, um das Skript auszuwählen, das vor der Installation der App ausgeführt werden soll. Die vorinstallierten Skripte werden ausgeführt oder erneut getestet, bis der Kunde den Erfolgsstatus der Skriptausführung empfängt. Erst danach wird der Befehl zur Installation der Anwendung gesendet. Sie können den Status der Skriptausführung auf der Gerätedetailseite auf der Registerkarte **Protokolle** anzeigen.
- **Post-Installations-Skripte** - Geben Sie den Skriptnamen ein, um das Skript auszuwählen, das nach der Installation der App ausgeführt werden soll.
- **Deinstallationsskripte**: Geben Sie den Skriptnamen ein, den der Server an ein Gerät sendet, wenn er erkennt, dass eine App nicht mehr an das Gerät verteilt wird.
- **Erkennungsskripte**: Geben Sie den Skriptnamen ein, den der Server an ein Gerät sendet, um eine App zu erkennen. Das Ergebnis des Erkennungsskripts für die App überschreibt das standardmäßige Bestandsergebnis für die App auf dem Gerät. Unabhängig davon, ob die App an das Gerät verteilt wurde oder nicht, wird das Erkennungsskript für alle Apps an das Gerät gesendet, um das Vorhandensein der Apps auf dem Gerät zu prüfen.
  Beispiel für ein Erkennungsskript:

```
#!/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
```

App-Verteilung bestimmen:

12. Wählen Sie eine Verteilungsoption aus:
13. Wählen Sie eine Verteilungsoption aus.
14. Erweitern Sie den Abschnitt **Erweiterte Optionen und App-Konfiguration**.
15. Beachten Sie für die Optionen die folgenden Anleitungen:
16. Klicken Sie auf **Weiter**.

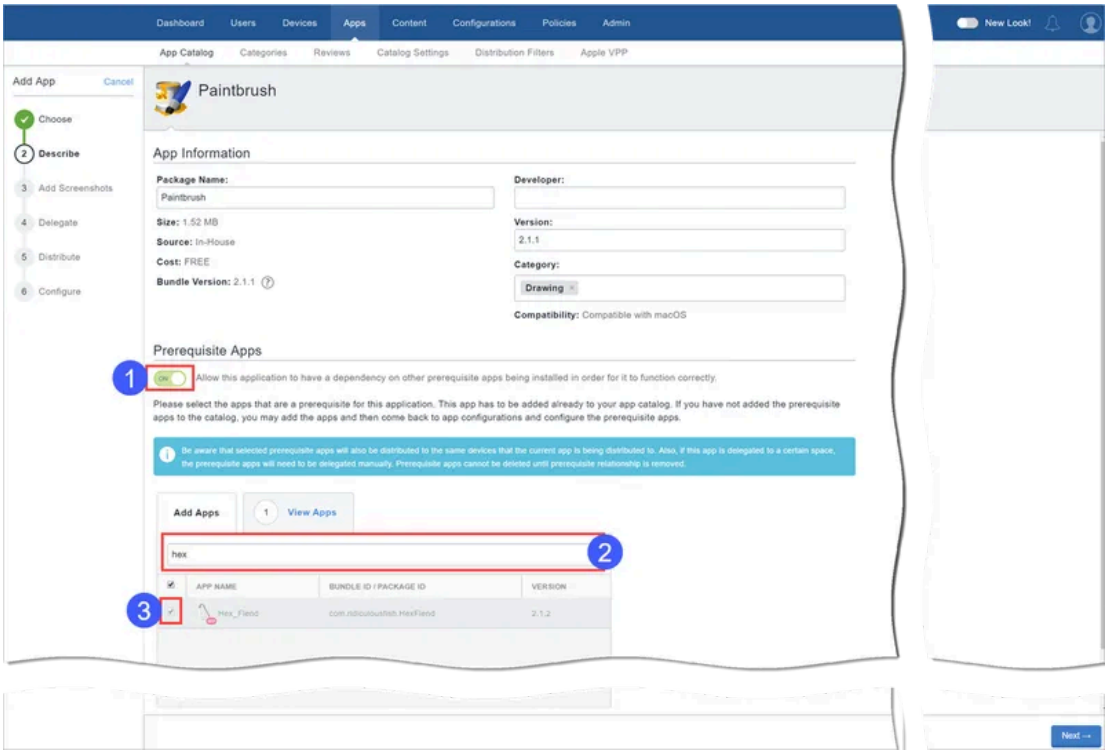
Einstellung	So gehen Sie vor
Auf einem Gerät installieren	Wählen Sie diese Option aus, um die Installation sofort nach der Registrierung zu beginnen. Der Benutzer wird aufgefordert, die Installation der App zu bestätigen, sofern nicht folgende Bedingungen erfüllt sind: • Die Gerät ist ein überwachtes iOS-Gerät. • Die Gerät ist ein Samsung Knox-Gerät und es wurde die Option für die Installation im Hintergrund ausgewählt.
App nicht im App-Katalog des Endbenutzers anzeigen	Wählen Sie diese Option aus, wenn Sie nicht wollen, dass der Benutzer die App im App-Katalog des Gerätes sieht.
Priorität für die Installation von Anwendungen festlegen	Wählen Sie „Hoch“, „Mittel“ oder „Niedrig“ für die Priorität der App-Installation während des Benutzer-Onboardings. Nur Apps mit hoher Priorität werden während des Benutzer-Onboardings installiert.
Erneute Push-Übertragung der App nach einer bestimmten Zahl fehlgeschlagener Versuche aussetzen (nur iOS)	Schalten Sie den Kippschalter auf ON, um eine erneute Push-Übertragung der App nach einer bestimmten Zahl fehlgeschlagener Versuche mit den folgenden Einstellungen auszusetzen: **Erneute Push-Übertragung stoppen** - Geben Sie die Anzahl der fehlgeschlagenen Push-Übertragungsversuche ein, nach denen die Push-Übertragung gestoppt werden soll. Die eingegebenen Werte sollten zwischen **1** und **999** liegen. **fehlgeschlagene Versuche, erneut versuchen nach** - Geben Sie ein, wie viele Stunden nach einem fehlgeschlagenen Neustart die Push-Übertragung erneut durchgeführt werden soll. Die eingegebenen Werte sollten zwischen **3** und **48** Stunden liegen.
(Nur Android) Bei Samsung-Knox-Geräten im Hintergrund installieren	Wählen Sie die Option, wenn Sie nicht wollen, dass der Benutzer zur Bestätigung der Installation auf Samsung Knox-Geräten aufgefordert wird.
(nur iOS und macOS) Per-App-VPN für diese App aktivieren	Wählen Sie diese Option aus, um für diese App eine Per-App-VPN-Konfiguration zu verwenden. Wählen Sie die Per-App-VPN-Konfiguration aus der Dropdownliste, die verwendet werden soll. Wählen Sie bei macOS nur die Tunnel-per-App-VPN-Konfiguration aus.
(Nur iOS): Backup in der iCloud und iTunes sperren.	Wählen Sie diese Option aus, um zu verhindern, dass Daten dieser App in der iCloud und iTunes gesichert werden.
(Nur iOS): Apps entfernen, wenn eine Registrierung rückgängig gemacht wird.	Wählen Sie diese Option aus, um diese App zu entfernen, sobald das Gerät nicht mehr über die Cloud verwaltet wird.
(Nur iOS): Anpassbare AppConnect-Konfiguration	Geben Sie für die AppConnect-fähige App die Schlüssel und die Werte ein, die die Präferenzen Ihrer kundenspezifischen Konfiguration definieren. Informationen zu den verfügbaren Schlüsseln finden Sie in der Dokumentation der App.
Verwaltete Einstellungen in iOS 7+	Geben Sie die für diese App definierten Schlüssel und Werte für eine unter iOS 7+ verwaltete App ein. Weitere Informationen über unterstützte Schlüssel finden Sie in der Dokumentation der App.

17. Klicken Sie auf **Fertig**.

- Nicht empfohlen
- Empfohlene Liste
- Banner

Interne Packager-macOS-Apps verstehen

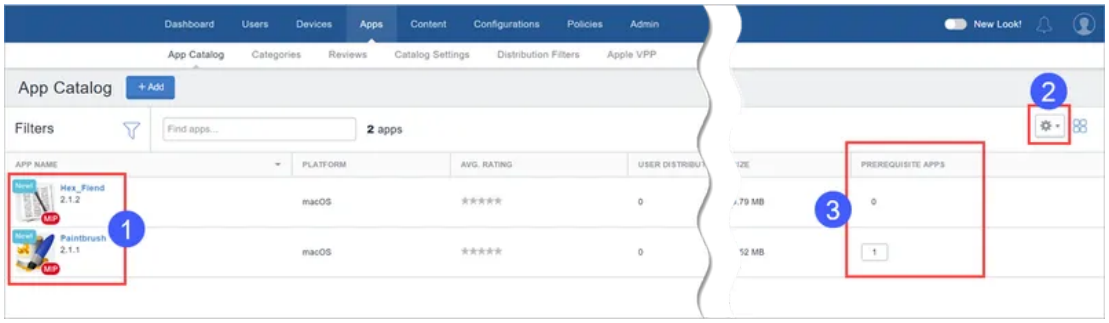
Beim Import von Packager-internen macOS-Apps kann der Administrator die Funktion „Als Voraussetzung benötigte Apps“ aktivieren (1), um nach Apps zu suchen, die als Voraussetzung benötigt werden (2) und die Apps auswählen (3), die auf den Clients installiert sein müssen, bevor die vom Administrator importierte App installiert werden kann.



Nach dem Import wird die interne Packager macOS-App im App Catalog mit dem Badge MIP angezeigt, 1, siehe unten. Sie können dann mit der Spalteneinstellungen 2 die Spalte PREREQUISITE APPS hinzufügen, 3 damit Sie auf einen Blick die Apps mit Abhängigkeiten, d.h. die Apps mit obligatorischen Apps sehen.

- Sie können nach MIP-, Nicht-MIP- und öffentlichen Apps (Apps and Books und öffentliche Apps des macOS App Store) suchen und diese als Voraussetzung auswählen.
- Benutzer müssen die Lizenz für Apps and Books akzeptieren, damit Apps and Books im Hintergrund installiert werden kann.
- Bei den öffentlichen, obligatorischen Apps, die keine Apple Apps and Books-Apps sind, müssen die Administratoren die öffentlichen Apps explizit verteilen und der Benutzer muss die öffentlichen Apps installieren. Die öffentlichen Apps (Apps and Books und andere Apps, die keine Apps and Books Apps sind) müssen in den App Catalog importiert werden, damit sie in der Liste der obligatorischen Apps angezeigt werden. Die Spalte „Quelle“ gibt die Art der obligatorischen App an.
- Eine MDM-Anmeldung ist erforderlich, um eine interne nicht-MIP-App zu installieren, für die keine MIP-Apps obligatorisch sind.
- Benutzer müssen die öffentlichen Anwendungen, die keine Apple Apps and Books sind, manuell installieren.
- Wenn das Token für Apps and Books entfernt wird oder die Lizenzen erschöpft sind, werden die ausgewählten obligatorischen Apps and Books und damit die Hauptanwendung nicht installiert. Für den Administrator hat es sich bewährt, die Benutzer in

jedem dieser Fälle über Apps and Books Apps im Voraus zu informieren.

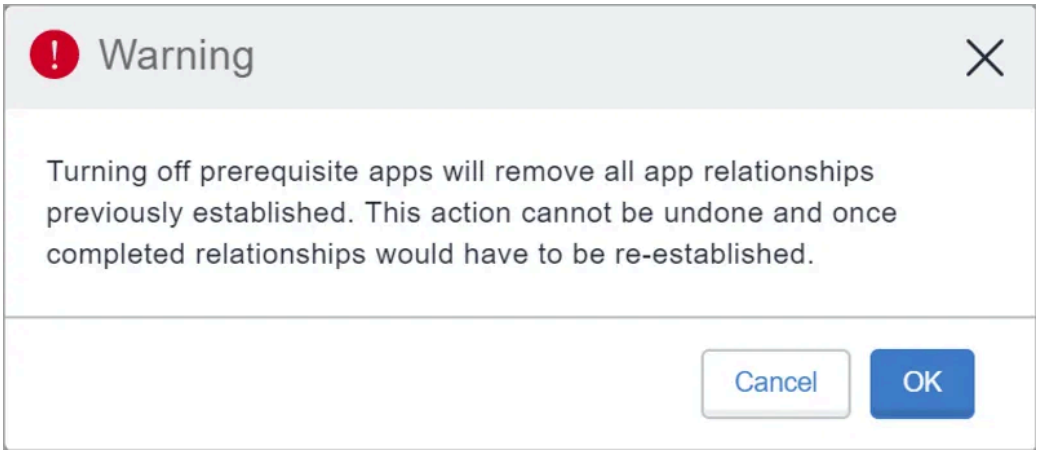


Obligatorische Apps stehen dem Benutzer auch als eigenständige Apps zum Download zur Verfügung, wenn sie explizit verteilt werden. Wenn der Benutzer versucht, eine obligatorische App zu deinstallieren:

- Stellen Sie sicher, dass die erforderliche App beim nächsten Geräte-Check-in erneut installiert wird.
- Die obligatorische App wird deinstalliert, wenn keine abhängigen Haupt-Apps auf dem gleichen Gerät installiert sind.
- Wenn die obligatorische App nicht explizit verteilt wird, wird die obligatorische App zusammen mit der Haupt-App deinstalliert.
- Wenn die obligatorische App explizit verteilt wird, bleibt die obligatorische App auf dem Gerät.
- Wenn die obligatorische App eine abhängige App hat, bleibt die obligatorische App auf dem Gerät.

Funktion „Obligatorische Apps“ deaktivieren

Bei der Interaktion mit Apps mit Abhängigkeiten und vorausgesetzten Apps, z. B. beim Aktualisieren, Löschen oder Delegieren solcher Apps, weisen Systemanweisungen Sie darauf hin, wie sich die Abhängigkeit oder der Voraussetzungsstatus der App auf die Aktionen auswirken können, die Sie ausführen wollen. Wenn Sie beispielsweise versuchen, die Funktion „Vorausgesetzte Apps“ für eine App zu deaktivieren, wird folgende Eingabeaufforderung angezeigt:



- Wenn Sie die Funktion für obligatorischen Apps für eine App deaktivieren, werden Details zu den obligatorischen Apps gelöscht. Dazu gehört auch die automatische Delegation und Aufhebung der Delegation von Apps aus Sub-Spaces.
- In Apps@Work erscheint die Installationsschaltfläche nicht für abhängige Apps, wenn die obligatorischen Apps nicht bereits auf dem betreffenden Client installiert sind.
- Wenn ein Benutzer auf den Benutzergeräten versucht, eine interne App mit Abhängigkeiten zu installieren, werden zuerst die obligatorischen Apps installiert (falls nicht bereits geschehen), und anschließend die Haupt-App, was einige Minuten dauern kann. Die Liste der obligatorischen Apps wird dem Benutzer zusammen mit dem Installationsstatus angezeigt.

Obligatorische Apps aus Spaces delegieren und Delegierung aufheben

- Obligatorische Apps, die an eine App (die Haupt-App) gebunden sind, werden automatisch delegiert, wenn die Haupt-App an einen Subspace delegiert wird.
- Wenn die Haupt-App nicht aus einem Sub-Space delegiert wird, werden auch die obligatorischen Apps delegiert, wenn die obligatorischen Apps nicht explizit verteilt werden. Die Delegation der obligatorischen Apps, die an mehr als eine Haupt-App gebunden sind, wird jedoch nicht zurückgenommen.
- Wenn die obligatorischen Apps explizit delegiert werden, wird die Delegation nicht automatisch aufgehoben.

Geräteberechtigungen für interne Android Enterprise Apps delegieren

Delegierte Berechtigungen können internen Apps zugewiesen werden, die sich auf verwaltete Android Enterprise-Geräte und AMA-Geräte anwenden lassen.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Wählen Sie im **App-Katalog** eine App aus, für die Sie Geräteberechtigungen delegieren möchten.
3. Klicken Sie auf die Registerkarte **App-Konfigurationen**.
4. Wählen Sie in den delegierten Berechtigungen (interne Android Enterprise-App) die erforderlichen Berechtigungen für die Apps aus:

> Nur die COSU-Bereitstellung verwendet AMAPI. Weitere Informationen finden Sie im Abschnitt über AMAPI.

   - **Laufzeitberechtigungen von Drittanbieter-Apps konfigurieren**
   - **Apps von Drittanbietern ausblenden und vorübergehend sperren**
   - **Zertifikate verwalten**
   - **App-Konfigurationen verwalten**
   - **Blockierung der App-Deinstallation verwalten**
   - **Aktivierung von System-Apps verwalten**
   - **Zertifikatauswahl verwalten** (nicht im AMAPI-Modus unterstützt)
   - **Beibehaltung von deinstallierten Apps verwalten** (nicht im AMAPI-Modus unterstützt)
   - **Netzwerkprotokollerfassung verwalten** (wird immer nur in einer App gleichzeitig unterstützt)
   - **Sicherheitsprotokollerfassung verwalten** (wird immer nur in einer App gleichzeitig unterstützt)
   - **Installation von vorhandenen Apps verwalten** (nicht im AMAPI-Modus unterstützt)
   - **Pakete installieren und entfernen** (nicht im AMAPI-Modus unterstützt)

Die Option zum Installieren und Entfernen von Paketen ist auf allen unterstützten Geräten des Android Geräteeigentümermodus (7.0 oder höher) verfügbar. Andere delegierte Berechtigungen gelten nur für Android 8.0 oder höher.
Konfigurieren Sie Verteilungsoptionen durch Auswahl von **Jeder mit App**, **Keiner** oder **Benutzerdefiniert**.

6. Klicken Sie auf **Speichern**.

Bereitstellungsprofilstatus für eigene iOS-Apps anzeigen

Zeigen Sie den Bereitstellungsprofilstatus auf der App-Katalogseite für eigene iOS-Apps an. Der Tool-Tipp neben dem Profilnamen zeigt an, in wie vielen Tagen das Profil abläuft. Diese Statusangabe kann nützlich sein, um zu überprüfen, wann Bereitstellungsprofile

für eigene Apps ablaufen.

Der Status ist bei der Fehlerbehebung von Apps hilfreich, die nicht installiert werden können, weil das Profil abgelaufen ist. Die Apps würden installiert werden, lassen sich aber nicht öffnen oder starten, wenn kein geeignetes Bereitstellungsprofil vorhanden ist.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Klicken Sie auf das Zahnradsymbol oben rechts, um die Spalten anzuzeigen.
3. Wählen Sie diese Option **Bereitstellungs-Profil**, um die Spalte für die Liste der Apps in der App-Katalogseite anzuzeigen.

Die Details des Bereitstellungsprofils finden Sie auch auf der Seite mit den App-Details im Abschnitt „Bereitstellungs-Profileinstellungen“.

Bereitstellungsprofil für eigene iOS-Apps aktualisieren

Das Bereitstellungs-Profil wird auf eine bestimmte interne iOS-App angewendet. Die Details des Bereitstellungs-Profils einer App sind auf der Seite mit den Details der App verfügbar. Damit eine hauseigene iOS-App auf dem Gerät gestartet werden kann, muss ein nicht abgelaufenes Bereitstellungs-Profil vorhanden sein. Wenn die Berechtigung abgelaufen ist, können Sie ein Bereitstellungsprofil aktualisieren, indem Sie das Profil auf der Seite App-Details hochladen.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Klicken Sie auf die App, bei der eine Aktualisierung des Bereitstellungsprofils erforderlich ist. Die Seite mit den App-Details wird angezeigt.
3. Klicken Sie auf **Bearbeiten**.
4. Klicken Sie im Abschnitt **Bereitstellungs-Profil** auf **Datei auswählen**.
5. Wählen Sie die Datei für das Bereitstellungsprofil (Dateierweiterung .mobileprovision) aus, die hochgeladen werden soll, und klicken Sie auf **Speichern**.

Hauseigene App in Google Play bereitstellen

Laden Sie Ihre internen Apps in den privaten Kanal von Google Play hoch und importieren Sie diese in Ivanti Neurons for MDM, um sie für Geräte bereitzustellen, die Android Enterprise unterstützen.

Verfahren

1. Melden Sie sich bei der Goople-Konsole für private Apps an: **https:// .play.google.com/apps/publish**.
2. Klicken Sie im linken Menü auf **Alle Anwendungen**.
3. Klicken Sie auf **Neue Anwendung erstellen** und geben Sie einen Namen für die Anwendung ein.
4. Klicken Sie auf **APK hochladen**, um die erzeugte APK-Datei hochzuladen.
5. Klicken Sie auf **Listing speichern**:
    - Geben Sie eine Kurzbeschreibung und eine ausführliche Beschreibung ein.
    - Laden Sie für alle Registerkarten Bildschirmfotos hoch.
    - Laden Sie ein Symbol mit hoher Auflösung hoch.
    - Laden Sie ein Grafiksymbol für eine Funktion hoch (graphic.png).

- Geben Sie die benötigten Informationen für Kategorisierung, Kontaktdetails und Datenschutzrichtlinie ein.
- Füllen Sie den Fragebogen für eine App-Bewertung aus.

6. Klicken Sie auf **Tarife & Verteilung**.
   Wenn alle erforderlichen Informationen eingegeben wurden, erscheint am oberen Rand der Seite die Meldung "Fertig zum Veröffentlichen".
7. Wechseln Sie in Ivanti Neurons for MDM zur Registerkarte "Apps".
8. Klicken Sie auf **Verfügbare Kataloge aktualisieren**, um Ihre privaten Apps zu synchronisieren.

> Es kann mehrere Stunden dauern, bis Ihre Apps veröffentlicht sind.

Web-App für Geräte mit Android Enterprise hinzufügen

Eine Web-App ist ein Link zu einer beliebigen Website, der als Shortcut auf dem Gerät installiert wird. Web-Apps verhalten sich ähnlich wie andere Apps, d. h. die Web-App kann nach den gleichen Kriterien verteilt werden wie eine App. Sie erscheint im App-Katalog und kann von den Benutzern wie jede andere App installiert werden. Web-Apps gibt es jedoch nur als Einzelversion, eine Installation im Hintergrund wird nicht unterstützt. Web-Apps nutzen Web-Clips und werden als Konfigurationen auf dem Gerät installiert, verhalten sich aber wie Apps.

Konfigurieren Sie einen Web-Clip als App im App-Katalog, um die Web-App für die Benutzer im App-Katalog zur Verfügung zu stellen. Der Web-Clip kann als Konfiguration definiert werden, eine Konfiguration kann jedoch nur vom Administrator verteilt werden. Benutzer können die Web-App auf ihren Geräten installieren oder die Installation ablehnen. Eine Webclip-Konfiguration dagegen können die Benutzer nicht ablehnen.

In Android Enterprise ist eine Web-App eine eingebettete Form einer Web-App, die über Google Chrome innerhalb des Arbeitsprofils ausgeführt wird. Sie kann mit einer VPN- oder SSO-Lösung in Android Enterprise kombiniert werden. Nach der Erstellung einer Web-App funktioniert die App wie jede andere Android-App, die Sie bei Bedarf verteilen können. Web-Apps erfordern die Installation von Chrome im Arbeitsprofil des unternehmenseigenen Geräts, damit sie ausgeführt werden können.

> Wenn es Probleme bei der Verwendung dieser Funktion gibt, können sich Administratoren an den **Support**wenden.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie in der Dropdown-Liste auf **Google Play** und suchen Sie nach einer App im Google Play Store. Wenn Android Enterprise registriert ist, wird Google Play iFrame angezeigt.
4. Klicken Sie auf **Webanwendung**.
5. App für Benutzer beschreiben:
   1. Titel oder Name der App.
   2. App-URL
   3. Darstellungsart der Web-App.
   4. Laden Sie das Symbol hoch, dies kann ein 512px großes, quadratisches PNG- oder JPEG-Bild sein.

Klicken Sie auf **Erstellen**. Warten Sie auf die Veröffentlichung der App im iFrame. Es kann ein paar Minuten dauern. Sie können die App schließen und später wieder aufrufen.

7. Importieren Sie nach dem Import der Web-App die Anwendung zur Verteilung in den App-Katalog. Klicken Sie auf das Symbol der Web-App.
8. Scrollen Sie nach unten und klicken Sie auf **Auswählen**.
9. Fügen Sie Kategorien und eine optionale Beschreibung hinzu.
10. Klicken Sie auf **Weiter**.
11. Wählen Sie eine der folgenden Optionen für die App-Delegation:
    - Diese App für alle Spaces delegieren.
    - Diese App nicht für alle Spaces delegieren.

Klicken Sie auf **Weiter**.

13. Wählen Sie eine Verteiloption für die Anwendung.
14. Klicken Sie auf **Fertigstellen**.

Sobald Sie eine Web-App hinzugefügt haben, können Sie die Web-App nach Belieben bearbeiten. Gehen Sie dazu wie folgt vor:

1. Klicken Sie auf der Seite **App-Katalog** auf den Namen der vorhandenen Web-App.
2. Klicken Sie auf **Bearbeiten**, um die Felder der Web-App zu bearbeiten.

Web-App für iOS-Geräte hinzufügen

Eine Web-App ist ein Link zu einer beliebigen Website, der als Shortcut auf dem Gerät installiert wird. Web-Apps verhalten sich ähnlich wie andere Apps, d. h. die Web-App kann nach den gleichen Kriterien verteilt werden wie eine App. Sie erscheint im App-Katalog und kann von den Benutzern wie jede andere App installiert werden. Web-Apps gibt es jedoch nur als Einzelversion, eine Installation im Hintergrund wird nicht unterstützt. Web-Apps nutzen Web-Clips und werden als Konfigurationen auf dem Gerät installiert, verhalten sich aber wie Apps.

Konfigurieren Sie einen Webclip als App im App-Katalog, um die Web-App für die Benutzer im App-Katalog zur Verfügung zu stellen. Der Web-Clip kann als Konfiguration definiert werden, eine Konfiguration kann jedoch nur vom Administrator verteilt werden. Benutzer können die Web-App auf ihren Geräten installieren oder die Installation ablehnen. Eine Webclip-Konfiguration dagegen können die Benutzer nicht ablehnen.

> Wenn es Probleme bei der Verwendung dieser Funktion gibt, können sich Administratoren an den **Support**wenden.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Klicken Sie auf **+ Hinzufügen** (oben links).
3. Klicken Sie auf **Web-Apps**.
4. App für Benutzer beschreiben:
    1. App-Name
    2. App-URL
    3. Plattformart
    4. App-Symbol
    5. Entfernen bzw. fügen Sie Kategorien hinzu.
    6. Vollbild - Wählen Sie die Anzeige der Web-App im Vollbildmodus aus.

7. Entfernbar - Wählen Sie aus, ob die Web-App entfernbar sein soll.
8. Klicken Sie auf **Weiter**.

Wählen Sie eine der folgenden Optionen für die App-Delegation:

- Diese App für alle Spaces delegieren.
- Diese App nicht für alle Spaces delegieren.

Klicken Sie auf **Weiter**.

7. Wählen Sie eine Verteiloption für die Anwendung.
8. Klicken Sie auf **Fertigstellen**.

Bearbeiten einer Web-App

Sobald Sie eine Web-App hinzugefügt haben, können Sie die Web-App nach Belieben bearbeiten.

Verfahren

1. Klicken Sie auf der Seite **App-Katalog** auf den Namen der vorhandenen Web-App.
2. Klicken Sie auf **Bearbeiten**, um die Felder der Web-App zu bearbeiten.

Langsamer Rollout

Mit der Einstellung **Langsamer Rollout** können Administratoren neue Versionen von Anwendungen automatisch schrittweise auf Geräten implementieren. Die Option „Verteilung als langsamer Roll-Out“ ist verfügbar, wenn Sie das nächste Release der App installieren. Über das Ivanti Neurons for MDM-Administrationsportal können Sie Anwendungen auch dann bearbeiten, wenn der langsame Rollout angehalten ist.

Nachdem der langsame Roll-Out für ein Release definiert wurde, gilt er für die nachfolgenden Releases mit dem zuletzt von Ihnen eingestellten Prozentsatz. Sie können die Verteilung einer Anwendung unterbrechen, wenn die Verteilung auf 100 % eingestellt ist. Wenn Sie jedoch das Verteilungsziel auf 100 % setzen, müssen Sie den Prozentsatz des Verteilungsziels für die nächste Version manuell festlegen, da die Benutzeroberfläche den Prozentsatz auf 0 % zurücksetzt.

Verfahren

	1.	**Gehen Sie zu App Catalog, Apps und wählen Sie eine der Optionen für den Verteilungsmodus.**
	2.	**Wählen Sie die Option Benutzerdefiniert % der Geräte in Auswahlübersicht (langsamer Rollout).**
	3.	**Ziehen Sie in den Einstellungen für langsamen Rollout den Schieberegler in Verteilungsziel% angeben.**
	4.	**Klicken Sie auf Bestätigen und dann auf Fertig. Der Status der neuesten App-Version wird angezeigt. Auf der Seite "App-Katalog" wird der Status SLOW ROLLOUT in der Tabelle angezeigt.**

Wenn Sie auf der Seite **App Catalog** keine Aufgaben ausführen können, kann es sein, dass Sie nicht über die erforderlichen Berechtigungen verfügen. Sie benötigen die Rolle "Verwaltung von Apps und Inhalten".

Erweiterte Suche verwenden

Mit der Option "Erweiterte Suche" können Sie anhand von Regeln nach Apps suchen, um die Apps nach bestimmten Kriterien zu identifizieren und anzuzeigen. Diese Regeln können mit den entsprechenden Operatoren erstellt werden, einschließlich der Operatoren "entspricht", "ist kleiner als", "ist größer als", "ist im Bereich", "ist gleich" und "ist nicht gleich". Die Regeln können miteinander mit den Optionen ANY (OR) oder ALL (AND) verschachtelt werden. Mit den Regeln übereinstimmenden Apps werden unterhalb des Abschnitts angezeigt.

> Bei den in der Suche verwendeten benutzerdefinierten Attributwerten wird zwischen Groß- und Kleinschreibung unterschieden.

Verfahren

1. Klicken Sie auf der Seite „App-Katalog“ auf den Link **Erweiterte Suche**. Der Assistent für die erweiterte Suche wird aufgerufen.
2. Klicken Sie auf eine der folgenden Optionen:
    - Klicken Sie auf **Beliebig**, wenn die Apps mindestens eine der Regeln erfüllen müssen.
    - Klicken Sie auf **Alle**, wenn die Geräte alle Regeln erfüllen müssen.

Wählen Sie zum Erstellen einer Regel zum Definieren der Suchkriterien eine der folgenden Optionen und die zugehörige Aktion aus:

- AppConnect aktiviert
- Durchschnittliche Bewertung
- Bundle-ID
- Kategorie
- Kosten
- Benutzerdefinierte Attribute
- Datum der Hinzufügung zum App-Katalog
- Änderungsdatum
- Geräteverteilung
- Gerätegruppenverteilung
- Gerätetyp
- Gruppenverteilung
- Mindestversion Betriebssystem
- [Name]
- Betriebssystemplattform
- Bereitstellungsprofil
- Größe
- Quelle
- Benutzerverteilung
- Name der Benutzergruppen
- Version

4. (Optional): Klicken Sie auf +, um weitere Richtlinien zu erstellen.
5. Klicken Sie auf **Suchen**. Die Liste der Apps, die den Suchkriterien entsprechen, wird angezeigt.

Suchanfragen laden

Liste der gespeicherten Suchanfragen anzeigen.

Verfahren

1. Klicken Sie auf "Erweiterte Suche" und dann auf das Ordnersymbol. Die Liste der erstellten Suchanfragen wird im Abschnitt **Abfrage laden** angezeigt.
   - **Abfragename** - Der Name der geladenen Abfrage.
   - **Abfrageinhalt** - Zeigt den Inhalt der Regeln an, die die Suchabfrage definieren.
   - **Aktionen** - Wählen Sie die Aktion aus, die mit der Abfrage ausgeführt werden soll.
2. Klicken Sie in der Spalte **Aktionen** auf **Abfrage laden**, um die Liste der Apps anzuzeigen, die mit den in der geladenen Abfrage definierten Kriterien übereinstimmen.
3. Klicken Sie auf **Löschen**, um eine geladene Abfrage zu löschen.

Exportieren von Apps in eine CSV-Datei

Sie können die Apps mithilfe der Option "Als CSV-Datei exportieren" der Seite "App-Katalog" exportieren.

Verfahren

1. Gehen Sie zu **Apps** > **App-Katalog**.
2. Klicken Sie auf die Option **Als CSV-Datei exportieren**, um die Liste der Apps und die zugehörigen Details in eine CSV-Datei zu exportieren.

> Es werden nur die im ausgewählten Space aufgeführten Apps berücksichtigt, wobei alle paginierten Ergebnisse in eine einzige Datei kompiliert werden.

> Beim Verwenden von Filtern und Suchergebnissen werden nur die relevanten Apps exportiert.

3. Es wird eine Popup-Meldung mit den Schaltflächen **Weiter** und **Abbrechen** angezeigt, die darauf hinweist, dass der Exportvorgang begonnen hat und in Kürze ein Bericht verfügbar sein wird.
4. Klicken Sie auf **Weiter** und warten Sie, bis die Anforderung abgeschlossen ist, bevor Sie eine weitere Anforderung übermitteln.
5. Eine Meldung zeigt **App-Katalog – CSV-Bericht fertiggestellt** sowie die Schaltflächen **Herunterladen** und **Löschen** an.
6. Klicken Sie auf **Herunterladen**, um den Bericht herunterzuladen.
7. (Optional) Klicken Sie zum Löschen des Berichts auf **Löschen**.

> Die Option **Als CSV-Datei exportieren** wird erst wieder aktiviert, wenn die Option **Herunterladen** oder die Option **Löschen** gewählt wird.

> Falls mehrere Versionen einer App vorhanden sind, wird nur ein Eintrag pro App-Version angezeigt.

Verwandte Themen

- Benutzerrollen
- Löschen von Apps aus dem App-Katalog

- App-Abhängigkeiten bereitstellen

8.2. App-Verwaltung mit DDM (deklarativer Geräteverwaltung)

Übersicht

App-Verwaltung mit DDM (Deklarative Geräteverwaltung) bietet Unterstützung für das Apple Declarative Management Framework für die Anwendungsbereitstellung und das Lebenszyklusmanagement auf iOS- und iPadOS-Geräten. DDM verlässt sich nicht auf kontinuierliche Befehlszustellung und periodische Abfragen, sondern ermöglicht es den Geräten, Deklarationen lokal anzuwenden und Statusänderungen proaktiv zu melden.

Mit DDM sendet der Server nur einmal eine Deklaration an das Gerät. Das Gerät wendet dann die Konfiguration an, überwacht den Status und meldet Statusänderungen zurück an den Server. Dieser gerätebezogene Ansatz reduziert die Serverkommunikation, verbessert die Skalierbarkeit und bietet zeitnahere Statusaktualisierungen für Anwendungsbereitstellungen.

Die DDM-App-Verwaltung konzentriert sich derzeit auf zentrale Funktionen der Anwendungsverwaltung für unterstützte Apple-Geräte.

DDM-App-Verwaltung – Workflow

In einem DDM-Workflow liefert der Server den gewünschten Status an das Gerät und überträgt ihm die Zuständigkeit für die Wartung und Meldung dieses Status.

Folgendes geschieht, wenn eine Anwendung einem DDM-fähigen Gerät zugewiesen wird:

1. Der Server sendet eine Anwendungsdeklaration an das Gerät.
2. Das Gerät verarbeitet die Deklaration lokal.
3. Das Gerät installiert, aktualisiert oder wartet die Anwendung basierend auf der zugewiesenen Konfiguration.
4. Das Gerät überwacht kontinuierlich den Anwendungsstatus.
5. Alle Installationsstatus- oder Statusänderungen werden sofort an den Server zurückgemeldet.

Dieses deklarative Modell bietet nahezu in Echtzeit Einblick in den Fortschritt der Anwendungsbereitstellung, ohne dass regelmäßige Statusabrufe erforderlich sind.

Aktivieren der DDM-App-Verwaltung

Die DDM-App-Verwaltung wird über die Benutzereinstellungen aktiviert und bestimmten Benutzergruppen zugewiesen.

So aktivieren Sie die DDM-App-Verwaltung:

1. **Gehen Sie zu Benutzer** > **Benutzereinstellungen**.
2. Klicken Sie unter **Apple DDM-Einstellung** für eine bestimmte Benutzergruppe auf **+Hinzufügen**. Die Seite **Apple-DDM-Einstellung** wird geöffnet.
3. Geben Sie einen Namen ein und aktivieren Sie den Schieberegler **DDM-App-Verwaltung aktivieren**.
4. Klicken Sie auf **Weiter**. Die Seite **Verteilung der Benutzereinstellung** wird aufgerufen.
5. Wählen Sie die Benutzergruppe aus, die die DDM-App-Verwaltung verwenden soll.
6. Klicken Sie auf **Fertig**.

Nachdem DDM für eine Benutzergruppe aktiviert wurde, werden alle unterstützten Anwendungen, die den Benutzern in dieser Gruppe zugewiesen sind, über die DDM-App-Verwaltung verarbeitet. Die DDM-Konfiguration ist mandantenweit, wird jedoch über Benutzer-

Gruppen-Zuweisungen angewendet, sodass Organisationen DDM schrittweise für ausgewählte Benutzer oder Gruppen bereitstellen können.

Unterstützte Registrierungsmethoden

Die DDM-App-Verwaltung unterstützt iOS-/iPadOS-Geräte, die wie folgt registriert wurden:

- iReg/verwalteter Ivanti Go-Client
- Device Enrollment-Profil (DEP) hinzufügen
- Kontogesteuerte Geräteregistrierung

Unterstützte Anwendungstypen

Die DDM-App-Verwaltung unterstützt die folgenden Anwendungstypen:

- Öffentliche Anwendungen
- VPP-Anwendungen (nur für die Geräteregistrierung)
- Interne Anwendungen

Der Workflow für die Anwendungszuweisung und -bereitstellung unterscheidet sich kaum von herkömmlichen N-MDM-Bereitstellungen. Bestehende Prozesse der Anwendungsverteilung sind weiterhin funktional und profitieren gleichzeitig von den erweiterten Statusberichtfunktionen von DDM.

8.2.1. Einstellungen für DDM-App-Verwaltung

Im Allgemeinen beinhaltet die App-Verwaltung folgende Einstellungen:

- Backup in iCloud verhindern
- App nicht auf neu registrierten Geräten installieren
- Mobilfunk 5G
- DNS-Proxy
- Konfiguration für verwaltete App
- Geschäftliche Apps – Apps@Work, Email+ usw.
- VPN pro App
- Netzwerkrelais
- Web-Content-Filter
- App Store-Updates zulassen

Zusätzlich zu den oben aufgeführten Einstellungen führt die DDM-App-Verwaltung mehrere Funktionen ein, die nur für über DDM verwaltete Geräte verfügbar sind.

App-Version anheften

Das Anheften der App-Version (Pinning) ermöglicht Administratoren das Bereitstellen und Warten einer bestimmten Anwendungsversion auf Geräten mit DDM-Verwaltung.

Folgendes geschieht, wenn Version Pinning aktiviert ist:

- Die Geräte installieren die angegebene Anwendungsversion.
- Automatische Upgrades auf neuere Versionen werden verhindert.
- Die Anwendungen verbleiben in der zugewiesenen Version, bis ein Administrator explizit eine neue Version auswählt.

Diese Funktion ermöglicht eine engere Kontrolle über die Konsistenz der Anwendungsversion und gestaffelte Upgrade-Bereitstellungen.

Verfahren

1. Gehen Sie zu **Apps** > **App-Katalog**.
2. Klicken Sie in der angezeigten Liste auf eine App. Die Seite **App-Details** wird geöffnet.
3. Klicken Sie auf der Registerkarte **App-Konfigurationen** auf **Apple-App-Einstellungen**.
4. Klicken Sie auf eine der aufgeführten vorhandenen Einstellungen.
5. Klicken Sie auf **Bearbeiten**.
6. Wählen Sie im Abschnitt **App-Version an ein Gerät anheften** die Option **App-Version anheften** aus.
7. Wählen Sie aus der Liste **App-Version auswählen** die gewünschte App-Version aus.

> Wenn auf dem Gerät bereits eine Version der App vorhanden ist, können Sie sie nicht durch eine ältere Version ersetzen.

8. Klicken Sie auf **Aktualisieren**.

Automatisierte App Store-Updatekontrollen (automatische App-Updates)

Administratoren können konfigurieren, wie App Store-Updates für verwaltete Anwendungen gehandhabt werden. Diese Funktion bietet eine umfassendere Kontrolle über das Verhalten bei Anwendungsupdates und hilft der IT, Updates an internen Validierungs- und Rolloutprozessen auszurichten.

Downloads über Mobilfunk zulassen

Mit DDM verfügen Sie jetzt über eine dedizierte Einstellung, die es ermöglicht, Anwendungsdownloads und Updates über das Mobilfunknetz zu steuern.

Verfahren

1. Gehen Sie zu **Apps** > **App-Katalog**.
2. Klicken Sie in der angezeigten Liste auf eine App. Die Seite **App-Details** wird geöffnet.
3. Klicken Sie auf der Registerkarte **App-Konfigurationen** auf **Auf Gerät installieren**.
4. Klicken Sie auf eine der aufgeführten vorhandenen Einstellungen.
5. Klicken Sie auf **Bearbeiten**.
6. Wählen Sie im Abschnitt **Zulässige Downloads über Mobilfunk** eine der folgenden Optionen aus:
    - **Speicher-Einstellungen** – Die Standardoption. Das Gerät verwendet beim Herunterladen von Apps die Einstellungen für den entsprechenden Speicher.
    - **Immer Ein** – App-Downloads sind zulässig, auch wenn für das Gerät keine WLAN-Verbindung besteht.
    - **Immer Aus** – App-Downloads sind nicht zulässig, wenn für das Gerät keine WLAN-Verbindung besteht.
7. Klicken Sie auf **Aktualisieren**.

Anwendungsinstallation – Workflow

Der Prozess zum Verteilen von Anwendungen ist dem der herkömmlichen N-MDM-App-Verwaltung ähnlich.

Administratoren können Folgende Aktionen durchführen:

- Apps zuweisen
- Apps verteilen
- Apps installieren

Mit DDM ändert sich jedoch, wie der Bereitstellungsstatus kommuniziert wird. Anstatt sich auf Serverabrufe zu stützen, melden Geräte Änderungen des Anwendungsstatus, sobald eine Aktion abgeschlossen ist. Dadurch stehen genauere und frühzeitigere Informationen über den Installationsfortschritt und die Bereitstellungsergebnisse zur Verfügung.

Statusberichte und Überwachung

Einer der Hauptvorteile der DDM-App-Verwaltung ist die proaktive Statusberichterstattung.

Mit DDM:

- Die Geräte überwachen den Anwendungsstatus lokal.
- Installations- und Aktualisierungsereignisse werden sofort erkannt.
- Statusänderungen werden automatisch an den Server gemeldet.

- Informationen werden verfügbar, ohne dass auf geplante Abfrageintervalle gewartet werden muss.

Dadurch erhalten Administratoren schneller Einblick in:

- Fortschritt der Anwendungsinstallation
- Erfolgreiche Installationen
- Abschluss von Anwendungupdates
- Änderungen des Anwendungsstatus
- Bereitstellungsfehler

Echtzeitberichte verbessern die Fehlerbehebung und bieten eine reaktivere Anwendungsverwaltung.

Anforderungen

DDM-App-Verwaltung wird nur unterstützt auf:

- iOS 26 oder höher
- iPadOS 26 oder höher
- Verwalteter Ivanti Go-Client 126 oder höher

Geräte, die diese Anforderungen nicht erfüllen, verwenden weiterhin die herkömmliche N-MDM-App-Verwaltung.

> Sobald ein Gerät über die DDM-App-Verwaltung verarbeitet wurde, lässt sich das Gerät durch Deaktivieren oder Aktualisieren der Richtlinienverteilung nicht auf die MDM-App-Verwaltung zurücksetzen. Um für das Gerät wieder die MDM-App-Verwaltung zu aktivieren, entfernen Sie die Richtlinienzuweisung und registrieren Sie das Gerät erneut.

8.3. Apps@Work (iOS, Android, Windows und macOS)

Apps@Work ist eine Storefront für Unternehmens-Apps, die die sichere Verteilung von Software und Apps vereinfacht. Apps@work ist für iOS-, Android-, macOS- und Windows-Geräte verfügbar. Der Apps@Work Corporate Appstore ist in Ivanti Go app und in Mobile@Work-Clients für iOS, Android und macOS integriert. Für Windows-Geräte ist es eine native, eigenständige Anwendung. Dieser Abschnitt enthält die folgenden Themen:

- **iOS Apps@Work**
- **Android Apps@Work**
- **macOS Apps@Work**
- **Windows Apps@Work**

iOS Apps@Work

Der native Apps@work Appstore wird automatisch mit dem Go-Client bereitgestellt. Der Administrator muss keine Aktion ausführen. Die Registerkarte Apps@work wird auf der Go-Client-Taskleiste angezeigt. Endbenutzer können auf dieser Registerkarte die vom Unternehmen genehmigten Apps anzeigen und installieren. Weitere Informationen finden Sie unter **iOS Apps@Work AppStore-Funktionen**.

Die iOS Apps@Work-Endbenutzerbenachrichtigungen für App-Updates sind standardmäßig aktiviert. Informationen zum Ändern der Einstellungen finden Sie unter dem Thema **Benachrichtigungen** bei den **Katalogeinstellungen**.

Bestehende Kunden mit iOS Apps@Work Webclip

Die Kunden, die den Legacy-iOS-Apps@Work-Webclip bereitgestellt haben, erhalten nicht standardmäßig den nativen integrierten App-Katalog. Führen Sie folgende Schritte durch, wenn Sie zum nativen Katalog von iOS Apps@Work wechseln und den Apps@work Webclip von den Geräten entfernen möchten:

Pushen von Konfigurationen

Der Administrator muss den App-Katalog für die Konfiguration des nativen Clients via Push auf die Geräte übertragen, damit Apps@Work als native Appstore-Erfahrung über die Go-Client-Anwendung verfügbar ist. Weitere Informationen finden Sie unter **Arbeiten mit Konfigurationen**.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Wechseln Sie zu **Konfigurationen > Filter** und wählen Sie **Clientdienste** aus. Alle Clientkonfigurationen werden aufgeführt.
3. Wählen Sie **App-Katalog für nativen Client** aus. Die Seite mit der Konfiguration "App-Katalog für nativen Client" wird geöffnet.
4. Klicken Sie auf das Symbol für **Verteilung bearbeiten**. Die Seite "Verteilung bearbeiten" wird geöffnet.
5. Wählen Sie eine der folgenden Optionen aus:
    - **Alle Geräte**
    - **Keine Geräte** – Wählen Sie diese Option aus, wenn Sie an kein Gerät etwas verteilen möchten.
    - **Benutzerdefiniert** – Mit dieser Option wählen Sie Geräte, Gerätegruppen, Benutzer und Benutzergruppen aus.

6. Nach der Verteilung der Konfiguration muss der Benutzer ein Upgrade auf die Go-Clientversion 83 oder höher durchführen. Die Registerkarte "Apps@Work" ist jetzt im Go app-Client sichtbar.

> Die Konfiguration lässt sich nicht via Push auf Geräte übertragen, die mithilfe von iReg registriert wurden, da der Go-Client auf solchen Geräten nicht verfügbar ist. Zum Abrufen des nativen App-Katalogs müssen Sie den Go app-Client installieren. Weitere Informationen finden Sie unter **Geräteregistrierung (iOS, macOS und Android)**.

Entfernen von iOS Apps@Work Webclip

Kunden, an deren Geräte Apps@Work Webclip verteilt wurde und die bereits zur nativen Apps@Work-Erfahrung migriert sind, können iOS Apps@Work Webclip entfernen.

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Filtern Sie die Konfiguration – **Apple App-Katalog**.
3. Klicken Sie auf **Bearbeiten**.
4. Wählen Sie bei **Verteilung** die Option **An keine Geräte verteilen** aus.
5. Klicken Sie auf **Speichern**.

Android Apps@Work

Der native Apps@work Appstore wird automatisch mit dem MI Go-Client bereitgestellt. Der Administrator muss keine Aktion ausführen. Die Registerkarte Apps@work wird auf der MI Go-Client-Taskleiste angezeigt. Endbenutzer können auf dieser Registerkarte die vom Unternehmen genehmigten Apps anzeigen und installieren. Weitere Informationen finden Sie unter **Administration > Android Enterprise**.

macOS Apps@Work

MacOs Apps@work ist in den macOS M@W-Client integriert. Sobald das Gerät in Ivanti Neurons for MDM registriert wurde, wird der Client umgeschaltet und als Apps@Work angezeigt. Für neu erstellte Mandanten wird die Apple App-Katalog Webclip-Konfiguration nicht via Push an macOS-Geräte übertragen. Bei Bedarf kann der Administrator die Apps@work Webclip-Konfiguration an macOS-Geräte verteilen. Weitere Informationen finden Sie unter **macOS-Geräte konfigurieren**.

macOS-Apps verteilen

- Ivanti unterstützt die Verteilung von macOS-Apps über das MDM-Protokoll von Apple und die Verwendung der Mobile@Work-App. Administratoren können sich für eines oder beide der folgenden Konzepte entscheiden:
  - MDM-Protokoll von Apple - Administratoren können nur bestimmte PKG-Formate (Verteilungsformate) als interne Apps hochladen und auch Apps aus dem Mac App Store verteilen (mit Unterstützung der Lizenzierung für „Apps and Books“ von Apple). Dieses Konzept erlaubt es Administratoren jedoch nicht, DMG- und andere PKG-Formate zu verteilen.
  - Die App Mobile@Work for macOS – Um Apps an Benutzer zu verteilen, können Administratoren mit dem MobileIron Packager (MIP) beliebige PKG-, DMG- oder .app-Dateien in eine MIP-Datei konvertieren. Laden Sie die MIP-Datei als interne App nach Ivanti Neurons for MDM hoch.

Sie können das Dienstprogramm von der **Website für Softwaredownloads** herunterladen.

- Administratoren können mit Mobile@Work hauseigene Apps verteilen, die im DMG-, PKG- oder .app-Format vorliegen. Für Apps, die nur im Mac App Store erhältlich sind, können Administratoren weiterhin die nativen MDM-Funktionen von Apple nutzen, unter anderem auch die Funktionen der Apps and Books-Lizenzen. Weitere Informationen finden Sie unter **macOS-Geräte konfigurieren**.

Windows Apps@Work

Apps@Work ist eine eigenständige native App, die vom Microsoft Store heruntergeladen oder direkt via Push von Ivanti Neurons for MDM übertragen werden kann. Sie ermöglicht die Verwendung von öffentlichen und internen Windows-Apps auf Windows 10+-Geräten in Ivanti Neurons for MDM. Apps@Work wird auf unterstützten Geräten ab Windows 10 im Hintergrund installiert.

Weitere Informationen finden Sie unter **App-Konfiguration**.

Verwenden von Windows Apps@Work

Apps@Work ermöglicht die Verwendung von öffentlichen und internen Windows-Apps auf Windows 10-Geräten in Ivanti Neurons for MDM. Apps@Work wird auf unterstützten Windows 10-Geräten automatisch installiert.

Authentifizierungszertifikat

So verwenden Sie die Authentifizierung per Zertifikat mit Apps@Work:

1. Wechseln Sie zu **Admin > Windows > Apps@Work – Authentifizierung per Zertifikat**.
2. Setzen Sie die Einstellung auf **EIN**.

> Wenn Sie die Einstellung auf **AUS** setzen, wird die Verwendung von Benutzername und Kennwort erzwungen.

> SAML wird für Apps@Work für Windows nicht unterstützt.

So konfigurieren Sie eine App für Apps@Work:

1. Wählen Sie eine Windows-App aus.
2. Klicken Sie auf die Registerkarte **App-Konfiguration**.
3. Klicken Sie auf **Auf Gerät installieren**.
   Die Konfiguration für eine eigene App unter Windows kann so eingestellt werden, dass die Installation im Hintergrund oder über Apps@Work erfolgt. Öffentliche Apps können nicht im Hintergrund installiert werden.
4. Sie können die Apps auch im Apps@Work-Katalog anzeigen oder ausblenden.
   Diese Option gilt nur für interne Apps.
5. Klicken Sie auf die Registerkarte **Werbung**.

> Apps@Work unterstützt derzeit keine Bannerwerbung. Die verfügbaren Optionen lauten **Featured** und **Not Featured**.
>
> Für öffentliche Apps wird nur die Option **Werbung** angezeigt.

8.4. iOS Apps@Work AppStore-Funktionen

Die Registerkarte "Apps@Work" bietet folgende Funktionen:

- Aufrufen der Registerkarte "Apps@Work" über die Go-Anwendung
- Suchen
- Installieren einer App – Schaltfläche "Status"
- Empfohlene Anwendungen und Banner
- Update-Benachrichtigung für Anwendung
- Einstellungen – Meine Geräte

Aufrufen der Registerkarte "Apps@Work" über die Go-Anwendung

Verfahren

1. Melden Sie sich über Ihr iOS-Gerät bei Go app an.
2. Tippen Sie auf das Symbol für **Apps@Work**. Zwei Standardregisterkarten sind verfügbar: "Alle Apps" und "Kategorien".

3. Tippen Sie auf die Registerkarte **Alle Apps**. Auf der Registerkarte "Alle Apps" werden alle Apps in alphabetischer Reihenfolge aufgeführt.
4. Tippen Sie auf die Registerkarte **Kategorien**. Auf der Registerkarte "Kategorien" werden nur die Kategorien angezeigt, die Anwendungen enthalten:
    - Jede Kategorie zeigt die Anzahl der Anwendungen an, die in ihr enthalten sind.
    - Die Zeile "Meine Apps" unter der Registerkarte "Kategorien" ist eine Position, die alle installierten Anwendungen enthält. Die Zeile "Meine Apps" ist stets die erste Kategorie, alle anderen Kategorien sind alphabetisch darunter aufgeführt.
    - Wenn keine Anwendungen installiert sind, wird in der Liste "Meine Apps" der Wert "Keine" angezeigt.
    - Wenn Sie auf eine Kategorie klicken, werden alle in der Kategorie enthaltenen Anwendungen mit einer Installationsoption aufgelistet. Klicken Sie auf **Installieren**, um jede Anwendung einzeln zu installieren, oder klicken Sie auf **Alle installieren**, um alle Anwendungen der Kategorie zu installieren. Sie werden aufgefordert, die Installation jeder einzelnen Anwendung zu erlauben.

Suchen

Verfahren

1. Melden Sie sich über Ihr iOS-Gerät bei Go app an.
2. Tippen Sie auf das Symbol für **Apps@Work**.
3. Tippen Sie auf das Suchsymbol (Lupe), um nach Folgendem zu suchen:
    - **Neue Release** – Eine Liste neu veröffentlichter Apps wird angezeigt, wenn kein Text in die Suchleiste eingegeben wurde.

    - Geben Sie beliebigen Text in das Suchfeld ein, um dynamisch Vorschläge übereinstimmender Anwendungen zu erhalten.
    - Die Anzahl der Suchergebnisse wird als Unterüberschrift angezeigt.
    - Durch Tippen auf die Schaltfläche **Installieren** können Sie eine Anwendung installieren, ohne auf die Seite mit den Details wechseln zu müssen.



Installieren einer App – Schaltfläche "Status"

Da der Server für die App-Installation die Anforderung verarbeiten und die Anwendung via Push an das Gerät übertragen muss, zeigt die Installationsschaltfläche den Fortschritt nicht in Echtzeit an. Der Status der Schaltfläche "Installieren" wechselt von "Installieren" zu "Angefordert" zu "Installiert".

Verfahren

1. Melden Sie sich über Ihr iOS-Gerät bei Go app an.
2. Tippen Sie auf das Symbol für **Apps@Work**.
3. Tippen Sie auf **Installieren**, um die Statusbenachrichtigungen wie folgt anzuzeigen:
    - Eine Alarmmeldung wird erstmals angezeigt, wenn eine Installation angefordert wurde.
    - Tippen Sie auf die Registerkarte "Angefordert". Eine Alarmmeldung wird angezeigt.

    > Der Status "Installiert" ist keine Schaltfläche.



Empfohlene Anwendungen und Banner

Die Registerkarte "Empfohlen" wird je nach der vom Administrator via Push übertragenen Konfiguration angezeigt. Die Registerkarte "Empfohlen" ist die Standardlandinpage, wenn keine Updates verfügbar sind.



Verfahren

1. Melden Sie sich über Ihr iOS-Gerät bei Go app an.
2. Tippen Sie auf das Symbol für **Apps@Work**.
3. Tippen Sie auf die Registerkarte **Empfohlen**.
    - Der empfohlene App-Banner zeigt eine Anwendung an.
    - Unter "Empfohlene App" ist eine Liste aller empfohlenen Apps enthalten.



Update-Benachrichtigung für Anwendung

Der Endbenutzer erhält eine Benachrichtigung, sobald Updates für Anwendungen verfügbar sind. Die Benachrichtigung enthält die Anzahl der Anwendungen, für die Updates verfügbar sind. Wenn der Benutzer auf die Benachrichtigung klickt, wird Apps@Work geöffnet.

Verfahren

1. Melden Sie sich über Ihr iOS-Gerät bei Go app an. Das Symbol für Apps@Work zeigt die Anzahl der Anwendungen an, für die Updates ausstehen.
2. Wenn Sie auf die Update-Benachrichtigung tippen, werden Sie zur Registerkarte "Alle Apps" in Apps@Work weitergeleitet. Die folgenden Indikatoren werden angezeigt:

- Der Unterabschnitt "Updates verfügbar" der Registerkarte "Alle Apps" zeigt die Anzahl der Anwendungen an, für die ein Update verfügbar ist.
- Für jede Anwendung, die aktualisiert werden muss, wird ein Symbol mit einem roten Punkt angezeigt.



Einstellungen – Meine Geräte

Verfahren

1. Melden Sie sich über Ihr iOS-Gerät bei Go app an.
2. Tippen Sie auf das Symbol für **Einstellungen**.
   - Die Registerkarte "Meine Geräte" ist bei den Einstellungen verfügbar.
   - "Meine Geräte" wird jetzt als Position unter "Authentifizieren" aufgeführt.

8.5. iOS Go – Erweiterte Funktionen

Schlüssel-Wert-Paare (Key-Value Pairs, KVPs) sind einfache Anwendungseinstellungen, die aus einem Schlüssel (Name der Einstellung) und einem Wert (anzuwendende Konfiguration) bestehen. In Ivanti Go for iOS können Unternehmen mit KVPs Funktionen aktivieren oder deaktivieren und das App-Verhalten anpassen, ohne dass dazu ein App-Update erforderlich ist.

Wenn Ivanti Go auf vom Unternehmen verwalteten iPhones oder iPads ausgeführt wird, werden diese KVP-Einstellungen beim Start oder während eines Check-ins gelesen. Die App wendet die Updates sofort an und stellt sicher, dass Konfigurationsänderungen schnell, konsistent und an die richtigen Benutzer geliefert werden.

Verwenden von KVPs in Ivanti Go-App-Konfigurationen

KVPs zum Anpassen von Meldungen bei Verletzungen werden in der Ivanti Go-App unterstützt. Sie können KVPs in den Einstellungen der Ivanti Go-App konfigurieren, um die Anwendung anzupassen.

Verfahren

1. Öffnen Sie die **Ivanti Go-App** in Ihrem App-Katalog.
2. Klicken Sie auf **Konfigurationen**.
3. Klicken Sie auf **Hinzufügen**, um eine neue **Apple App-Konfiguration** zu erstellen.
4. Fügen Sie Ihre KVPs manuell hinzu:
    - Geben Sie in der Spalte **Schlüssel** den Konfigurationsschlüssel ein, den Sie anpassen möchten.
    - Geben Sie in der Spalte **Wert** den Wert ein, den Sie auf den Geräten durchsetzen möchten.
5. (Optional) Laden Sie eine vorhandene *.plist*-Datei hoch, in der die vordefinierten KVPs enthalten sind, die Sie anwenden möchten.
6. **Speichern** Sie die Konfiguration.
7. Die aktualisierten KVPs werden beim nächsten Check-in auf die Geräte angewendet.

Hinzufügen einer Liste zu einer bestimmten iOS-App (für mehrere Schlüssel-Wert-Paare)

Administratoren können mehrere Key-Value Pairs (KVPs) für eine iOS-App mithilfe von App-Seriennummern, Bundle-Kennungen, Versionsdetails oder anderen Metadaten konfigurieren. Eine effiziente Methode dafür ist das Hochladen einer .plist-Datei über die Ivanti Neurons for MDM-Konsole.

Verfahren

1. Gehen Sie zu **Apps**.
2. Öffnen Sie den **App-Katalog**.
3. Wählen und öffnen Sie die **spezifische iOS-App**, die Sie konfigurieren möchten.
4. Wechseln Sie zur Registerkarte "App-Konfigurationen".
5. Wählen Sie **Von Apple verwaltete App-Konfiguration** aus.
6. Klicken Sie auf die Schaltfläche **Hinzufügen**.
7. Geben Sie einen **Namen** für Ihre Konfiguration ein.
8. Klicken Sie auf **.plist verwenden**.
9. Wählen Sie **eine der folgenden Optionen** aus.

10. Navigieren Sie zu Ihrer .plist-Datei, wählen Sie sie aus und klicken Sie auf **Öffnen**. Das System füllt die Konfigurationstabelle automatisch mit den Schlüssel-Wert-Paaren der Liste aus.
11. Wählen Sie die Benutzergruppen oder Geräte aus, die die Konfiguration empfangen sollen.
12. Klicken Sie auf **Diese App-Konfiguration verteilen**.
13. Klicken Sie auf **Speichern**, um den Vorgang abzuschließen.

Die hochgeladene Datei über eine .plist-Erweiterung verfügen. Wenn Sie die Datei manuell erstellt haben (Beispiel in einem Texteditor), stellen Sie sicher, dass Sie die Erweiterung vor dem Hochladen von *.txt* in *.plist* ändern.

Starten von Ivanti Go im Single-App-Modus während der Registrierung

Mit dieser Funktion können Administratoren Schlüssel-Wert-Paare während der Geräteregistrierung verwenden, um Ivanti Go für iOS automatisch im Single App-Modus (SAM) zu starten. Wenn ein Gerät mit der Registrierung beginnt, lösen die konfigurierten Schlüssel-Wert-Paare Ivanti Go sofort aus. Während dieses Vorgangs wird dem Benutzer folgende Meldung angezeigt:

Bitte warten Sie, während Ihr Gerät konfiguriert wird.

Um dieses Verhalten zu aktivieren, muss die Konfiguration des Single App-Modus installiert und explizit auf Ivanti Go für iOS vor oder während des Registrierungsablaufs ausgerichtet sein. Sobald die Registrierung abgeschlossen ist, wird der Single App-Modus automatisch beendet. Anschließend wird das Gerät für den normalen Betrieb an den Endbenutzer freigegeben, wodurch eine sichere Einrichtung gewährleistet ist, ohne dass die Verwendung nach der Registrierung eingeschränkt wäre.

Diese Funktion unterstützt Ivanti Mobile@Work-Umgebungen und bietet einen sicheren Registrierungsablauf für überwachte iOS-Geräte.

Einrichten der Zero Touch-Aktivierung

So aktivieren Sie die Zero Touch-Aktivierung für Ivanti Go:

1. Richten Sie eine Gruppe ein, die nur Geräte enthält, bei denen *Client registriert = Nein* ist.
2. Erstellen Sie eine Single App-Modus (SAM)-Konfiguration für die Ivanti Go-Anwendung. Weisen Sie diese Konfiguration nur der in *Schritt 1* erstellten Gerätegruppe zu.
3. Fügen Sie das Schlüssel-Wert-Paar (KVP) zero_touch_activation zur Konfiguration der Ivanti Go-App hinzu. Verwenden Sie als Ziel die gleiche Gerätegruppe, die bereits in den vorherigen Schritten verwendet wurde.

KVP-Konfiguration

Schlüssel	Wert	Typ	Beschreibung
zero_touch_activation	Wahr	Boolesch	Wenn der Wert auf "wahr" gesetzt ist, erkennt die Ivanti Go-App, dass sie über die SAM-Konfiguration im Single-App-Modus (SAM) ausgeführt wird. Die SAM-Konfiguration startet die Ivanti Go-App, wobei dieser Wert als zusätzliche Einstellung dient, die dafür sorgt, dass die App im SAM-Modus ordnungsgemäß funktioniert. Nach erfolgreicher Registrierung beendet das Gerät den Single-App-Modus und steht dem Endbenutzer für den normalen Gebrauch zur Verfügung.

Aktivieren der Schaltfläche "Wiederinbetriebnahme" in Ivanti Go (iOS 18+)

Die Funktion **Wiederinbetriebnahme** ermöglicht es dem Gerät, sich automatisch neu zu registrieren, nachdem die Daten komplett gelöscht wurden, sodass das Gerät nach dem Komplettlöschen nicht mehr manuell neu registriert werden muss.

Administratoren können die Schaltfläche "Wiederinbetriebnahme" mithilfe eines konfigurierbaren Schlüssel-Wert-Paars (KVP) aktivieren oder deaktivieren. Folgendes gilt, wenn das KVP als Teil der App-Konfiguration für Ivanti Go bereitgestellt wird:

- Die Option "Wiederinbetriebnahme" wird für den Endbenutzer sichtbar.
- Der Benutzer kann den Prozess des Zurücksetzens direkt über Ivanti Go initiieren.
- Das Gerät führt eine von Apple verwaltete Wiederinbetriebnahme durch.
- Verwaltungsprofile und erforderliche Apps bleiben erhalten.
- Das Gerät schließt den Re-Provisionierungsablauf ab und ist wieder einsatzbereit.

Diese Funktion wird auf Ivanti Go für iOS-, iOS 18 und neueren Geräten unterstützt, die im DEP-Modus registriert sind.

KVP-Konfiguration

Fügen Sie den folgenden KVP zu der von Ivanti Go verwalteten App-Konfiguration in Ivanti Neurons for MDM hinzu:

Schlüssel	Wert	Beschreibung
ReturnToServiceEnabled	wahr	Aktiviert die Schaltfläche **Wiederinbetriebnahme** in Ivanti Go. Wenn diese Funktion auf falsch gesetzt ist oder nicht definiert ist, bleibt sie ausgeblendet.

Deaktivieren des Screenshot-Schutzes im Bildschirm "SAML-Authentifizierung"

Ivanti Go for iOS enthält einen integrierten Screenshot-Schutz, um die Sicherheit während der Geräteregistrierung zu erhöhen. Standardmäßig wird durch die Registrierung mit SAML-Authentifizierungsbildschirm Folgendes blockiert:

- Screenshots
- Bildschirmaufzeichnungen
- Bildschirmfreigabe

Dieser Schutz stellt sicher, dass vertrauliche Authentifizierungsdaten, wie Benutzernamen, Passwörter und SAML-basierte Anmeldeinhalte, nicht ohne Autorisierung erfasst oder weitergegeben werden können.

Administratoren können den Screenshot-Schutz auf verwalteten Geräten mithilfe einer KVP-Konfiguration deaktivieren. Wenn diese Konfiguration angewendet wird, lässt die Ivanti Go-App Screenshots und Aufzeichnungen nur im Bildschirm "SAML-Authentifizierung" zu, während alle anderen Sicherheitsmechanismen in der App beibehalten werden.

KVP-Konfiguration

Um den Screenshot-Schutz für den Bildschirm "SAML-Authentifizierung" zu deaktivieren, wenden Sie das folgende KVP auf die Ivanti Go-App-Konfiguration in Ihrer MDM an:

Schlüssel	Wert	Beschreibung
SCREENSHOT_PROTECTION_DISABLED	Wahr	Deaktiviert den Screenshot-, Bildschirmerfassungs- und Bildschirmfreigabeschutz im Bildschirm "SAML-Authentifizierung". Wenn der Schutz nicht definiert oder auf "falsch" gesetzt ist, bleibt der Schutz standardmäßig aktiviert.

KVPs zum Anpassen von Meldungen zu Richtlinienverletzungen

Mithilfe deiser KVPs können Administratoren die Meldungen anpassen, die an Endbenutzer gesendet werden, wenn Richtlinienverletzungen erkannt werden.

Diese KVPs zur Anpassung beschreiben die KVPs und Verletzungsarten, die Administratoren zum Anpassen des Ivanti Go for iOS-App-Verhaltens zur Verfügung stehen. Diese KVPs definieren das App-Verhalten, wie z. B. die Bereitstellung detaillierter Benachrichtigungen an die Gerätebenutzer und den Export von Kontakten aus Ivanti Go for iOS.

Die Verletzungsarten sind kombinierbar. Wenn mehrere Verstöße vorliegen, wird eine Liste mit Meldungen in Ivanti Go for iOS angezeigt.

Schlüssel-Wert-Paare (KVPs)	Standardmeldungen
compliance.message.COMPROMISED	• Ihr Gerät wurde kompromittiert. Es wurde ein Jailbreak festgestellt. Versetzen Sie Ihr Gerät wieder in den Zustand "Kein Jailbreak" oder wenden Sie sich an Ihren Administrator, um Hilfe bei der Lösung dieses Problems zu erhalten.
compliance.message.DATA_PROTECTION_DISABLED	• Der Unternehmenszugriff wurde aus Datenschutzgründen deaktiviert. Wenden Sie sich an Ihren Administrator, um Unterstützung bei der Lösung dieses Problems zu erhalten.
compliance.message.OUT_OF_CONTACT	• Ihr iOS-Gerät ist nicht erreichbar. Wenden Sie sich an Ihren Administrator, um Unterstützung bei der Lösung dieses Problems zu erhalten.
compliance.message.APPS	• Auf Ihrem Gerät fehlen erforderliche Apps und/oder es sind nicht zulässige Apps auf Ihrem Gerät vorhanden. Bitte fügen Sie notwendige Apps hinzu/entfernen Sie sie oder wenden Sie sich an Ihren Administrator, um Unterstützung bei der Lösung dieses Problems zu erhalten.
compliance.message.MDM_DISABLED compliance.message.ROAMING	• Ihr Gerät ist nicht mehr konform, da die MDM-Funktion deaktiviert wurde. Bitte registrieren Sie Ihr Gerät erneut oder wenden Sie sich an Ihren Administrator, um Unterstützung bei der Lösung dieses Problems zu erhalten.
compliance.message.generic	• Der Unternehmenszugriff wurde ohne Angabe eines Grunds deaktiviert. Wenden Sie sich an Ihren Administrator, um Unterstützung bei der Lösung dieses Problems zu erhalten.
compliance.message.header compliance.message.CUSTOM	Ihr Gerät ist aus folgenden Gründen nicht mehr konform: Wenn die Verletzungsart CUSTOM oder CUSTOM_NOTIFY_ONLY lautet, zeigt das System eigenständige Meldungen ohne Header an. Möglicherweise ist eine Aktion auf Ihrem Gerät erforderlich. Bitte wenden Sie sich bei Bedarf an Ihren Administrator.
compliance.message.CUSTOM_NOTIFY_ONLY	Ihr Gerät ist nicht mehr konform, und es wurde eine Benachrichtigung gesendet. Weitere Informationen finden Sie auf der Registerkarte "Benachrichtigungen" oder in Ihrer E-Mail.

Wenn die Liste der Verletzungsarten keine Verletzung mit zugeordneter Meldung, aber mindestens eine Verletzung ohne zugeordnete Meldung enthält, zeigen Sie die Standardmeldung an:

- Firmenzugriff wurde ohne Angabe eines Grunds deaktiviert. Wenden Sie sich an Ihren Administrator, um Unterstützung bei der Lösung dieses Problems zu erhalten.

Wenn die Meldungsliste mindestens eine Verletzungsmeldung enthält, zeigen Sie die folgende Kopfzeile über der Liste an:
Ihr Gerät ist aus folgenden Gründen nicht mehr konform:

Wenn Sie eine Standardmeldung nicht ändern möchten, fügen Sie kein Schlüssel-Wert-Paar (KVP) hinzu. Definieren Sie KVPs nur für diejenigen Meldungen, die Sie ändern möchten.

Konfigurieren von Standardbrowser und E-Mail-Clients unter Verwendung der verwalteten App-Konfiguration

Mit Key Value Pairs (KVP) können Administratoren konfigurieren, welchen Browser und E-Mail-Client **Ivanti Go** beim Öffnen von Weblinks und Erstellen von E-Mails über die verwaltete App-Konfiguration verwendet.

Als Administrator können Sie anhand der verwalteten App-Konfigurations-KVPs steuern, wie die Links auf der Registerkarte **Support** gehandhabt werden:

Schlüssel	Werte	Typ	Beschreibung
default_browser	safari, edge, chrome, firefox, brave, opera, webatwork, duckduckgo	Zeichenfolge	Browser, den Ivanti Go verwendet, um Weblinks auf der Registerkarte "Support" zu öffnen. http/https-Links werden zum Schema des konfigurierten Browsers umgeleitet. **Standard, falls nicht konfiguriert**: Systemstandardbrowser.
Allow_browser_fallback	true, false	Boolesch	**Verhalten, wenn der Standardbrowser nicht installiert ist**: **Wahr**: Es wird der Standardbrowser des Systems verwendet. **Falsch**: Der Link wird nicht geöffnet, dem Benutzer wird die Meldung "<Browser> nicht installiert" angezeigt. **Standard, wenn nicht konfiguriert:** Wahr
restrict_log_sharing_to_email	true, false	Boolesch	Gibt an, ob die Protokoll-/Supportfreigabe auf E-Mail beschränkt ist (unter Verwendung von default_email). Das automatisches Anhängen von Protokollen funktioniert mit Email+ und nativer E-Mail. Funktioniert mit **allow_email_fallback**. **Wahr**: Nur für E-Mail freigeben. **Falsch**: Standard-Freigabeoptionen sind verfügbar. **Standard, wenn nicht konfiguriert**: falsch.
default_email	nativemail, outlook, gmail, yahoo, citrixmail.emailplus, spark, protonmail	Zeichenfolge	E-Mail-Client, den Ivanti Go verwendet, um E-Mails von mailto-Links auf der Registerkarte "Support" zu verfassen. mailto wird in die Erstellungs-URL des Clients **Standard, wenn nicht konfiguriert** umgewandelt: Standard-E-Mail-Anwendung. Doppelte Rolle bei der Verbindungsauflösung und Protokollfreigabe, wenn der Standard-E-Mail-Client nicht installiert ist.
Allow_email_fallback	true, false	Boolesch	**Verhalten, wenn Standard-E-Mail nicht installiert ist**. **Wahr**: Die E-Mail-Erstellung nutzt die Standard-E-Mail-Anwendung, wenn der konfigurierte E-Mail-Client nicht installiert ist; die Protokollfreigabe kann eine alternative Zustellungsmethode verwenden. **Falsch**: Die E-Mail-Erstellung wird blockiert und dem Benutzer wird die Meldung **Nicht installiert** angezeigt, wenn der konfigurierte E-Mail-Client nicht verfügbar ist. Logsharing-Beschränkungen werden ohne Fallback-Option durchgesetzt. **Standard, wenn nicht konfiguriert**: wahr. (Fallback-Verhalten ist aktiviert)

8.6. Anzeige der App-Details

Sie können im App-Katalog mit der Detailsuche App-Details zu jeder App im Katalog abfragen. Auf der Seite „App-Details“ werden die Details zu den Apps wie Anzeigeversion (z. B. 1.5.0), Bundle-Version (z. B. 1.5.0.42) und die erforderliche Mindest-OS-Version (z. B. 5.0 für Android) angezeigt.

Apps, die nicht die in dem Feld „Erforderliche Mindest-OS-Version“ angegebene Version besitzen, werden im Apps@Work-Katalog nicht angezeigt. Daher können solche Apps nicht an die Geräte verteilt werden. Das Feld „Erforderliche Mindest-OS-Version“ wird auch als Teil der **Audit-Protokolle** für die Apps angezeigt.

Verfahren

1. Klicken Sie auf **Apps**.
2. Klicken Sie auf **App-Katalog**.
3. Wählen Sie die App aus.

Das Fenster "App-Details" wird angezeigt.

> Für interne iOS-Apps können Sie das **Ablaufdatum des Bereitstellungsprofils** auf der Seite mit den App-Details prüfen.

> In den App-Informationen wird nun **App-Installation auf M1-Geräten bei Verteilung zulassen** als Option für alle iOS- und iPadOS-VPP-Apps angezeigt. Der Administrator muss die Option **App-Installation auf M1-Geräten bei Verteilung zulassen** nur für iOS- oder iPad-VPP-Anwendungen aktivieren, die auf einem M1-macOS-Gerät installiert werden können. Erst wenn diese Option aktiviert wurde, kann der Administrator die M1-macOS-Geräte während der Anwendungsinstallation sehen. Die verwaltete App-Konfiguration wird für iOS-VPP-Anwendungen auf M1-Mac-Geräten unterstützt.

> Bei iOS- und macOS-App Store-Apps, einschließlich Business-to-Business, prüft die Funktion **Neue Version synchronisieren**, ob App-Updates im App Store vorhanden sind, und synchronisiert diese ggf. Die aktualisierte App-Version wird innerhalb von 12 bis 24 Stunden, basierend auf dem App-Synchronisierungsplan, angezeigt.

> Die Gerätedetails wurden mit einer Umschalt-Schaltfläche für **Vorausgesetzte Apps** ergänzt. Administratoren können diese Option wählen und Apps als Voraussetzungen für eine Haupt-App hinzufügen.

Sobald eine App an unterschiedliche Geräte verteilt wird, kann der Verteilungsstatus auf der Registerkarte **Geräteübersicht** verfolgt werden. Die Registerkarte "Geräteübersicht" zeigt außerdem die Anzahl der geeigneten Geräte an sowie die Anzahl der Geräte, auf denen die App installiert wurde, die Installation aussteht oder die Installation fehlgeschlagen ist. Die Anzahl der Geräte in diesen Feldern basiert auf den Geräten, auf denen die App-Installation erforderlich ist. Auf diese Weise können Administratoren die erste Bereitstellung obligatorischer Apps nachverfolgen.

Informationen zu den Zahlen allgemeiner Apps (einschließlich zu von Benutzern installierten Apps) erhalten Sie, indem Sie eine App-Inventar-Suche durchführen.

> Apps, die vom Gerät ausgeschlossen wurden, haben den Verteilungsstatus "Ausstehend".

Die folgende Tabelle enthält mögliche Gründe für das Fehlschlagen der App-Installation auf iOS-/OSX-Geräten:

Grund	Beschreibung
App bereits installiert	Die App ist bereits installiert.
App Store deaktiviert	Der App Store ist deaktiviert.
App-ID nicht verifizierbar	Die App-ID konnte nicht verifiziert werden.
Fehlgeschlagen	Die App-Installation ist aufgrund eines unbekannten Fehlers fehlgeschlagen.
Verwaltet aber deinstalliert	Die App wird verwaltet, wurde aber vom Benutzer entfernt. Wenn die App wieder installiert wird (auch vom Benutzer), wird sie erneut verwaltet.
Verwaltung abgelehnt	Der Benutzer hat die Konvertierung einer nicht verwalteten App zu einer verwalteten App abgelehnt.
Keine App	Der Befehl zum Installieren der App wurde aufgrund einer ungültigen Anwendungskennung abgelehnt, welche zur Auflösung in eine Ressource führen würde, die keine App ist.
Nicht unterstützt	Die App wird nicht unterstützt.
Sonstiges	Der Grund für neu hinzugefügte Fehler.
Kaufmethode wird nicht unterstützt	Ab iOS 7 kann die App aufgrund einer ungültigen Kaufmethode (die nur für VPP-Apps gilt) nicht installiert werden.
Vom Benutzer installierte App	Der Benutzer hat die App installiert, bevor die verwaltete App-Verwaltung starten konnte.
Vom Benutzer abgelehnt	Der Benutzer hat das Angebot zum Installieren der App abgelehnt.
Update abgelehnt	Der Benutzer hat das Angebot zum Aktualisieren der App abgelehnt.

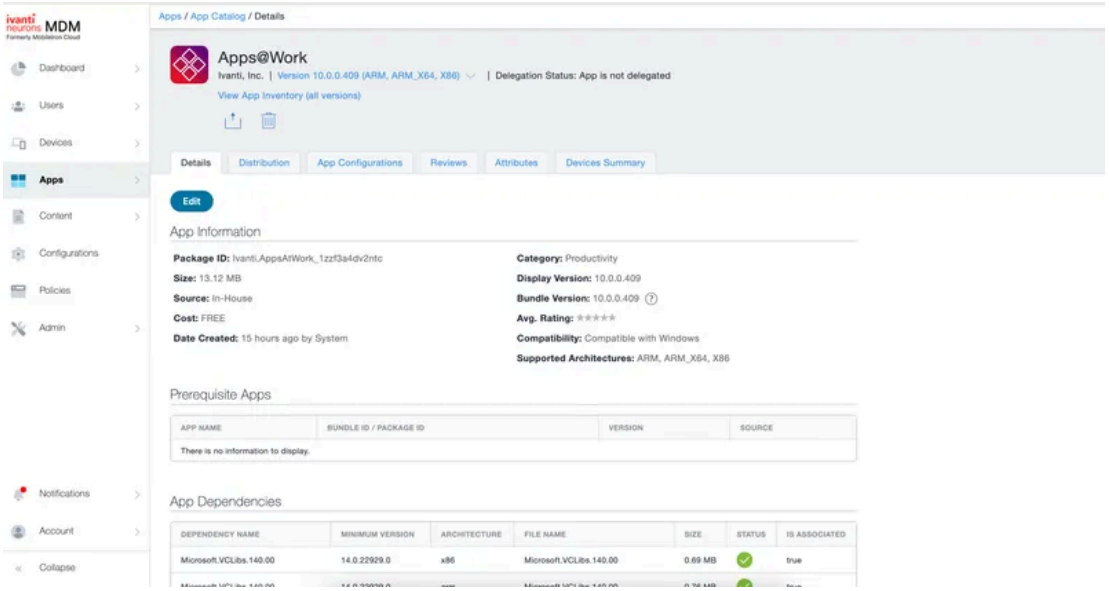
Die folgende Tabelle enthält mögliche Gründe für das Fehlschlagen der App-Installation auf Android-Geräten:

Grund	Beschreibung
VOM BENUTZER INSTALLIERT	Die App wurde bereits auf dem Gerät installiert (außerhalb von MDM).
NICHT UNTERSTÜTZT	Der Vorgang wird nicht unterstützt.
INSTALLATION VOM BENUTZER ABGELEHNT	Der Benutzer hat die Installation der Anwendung abgelehnt.
INSTALLATIONSFEHLER	Beim Versuch, die Anwendung zu installieren, wurde ein Fehler erkannt. Installation fehlgeschlagen.
NICHT ERKANNT	Das Element wurde nicht gefunden oder wird nicht mehr verfolgt (z. B. Fehler/Deinstalliert und aus der Verfolgung entfernt).
INSTALLATION NICHT UNTERSTÜTZT	Aktualisiert für 3.0 Android-Client/22.0.0-Server: Bestimmter Status zur Installationsverfolgung oder Deinstallation erforderlich.
AUSGEBLENDET	Während der Quarantäne wird der Status AUSGEBLENDET/DEINSTALLIERT gesendet. Bei Aufhebung der Quarantäne wird erneut "Installiert" angezeigt.
SONSTIGES	Der Grund für neu hinzugefügte Fehler.

Bei Windows-Geräten wird, sofern die App bei den App-Konfigurationen für die Installation im Hintergrund festgelegt ist, in der Geräteübersicht die Anzahl der geeigneten, installierten, ausstehenden oder fehlgeschlagenen Geräte für die App angezeigt.

Anzeigen von App-Inventar-Informationen über die Seite "App-Details"

Klicken Sie zum Anzeigen der App-Inventar-Informationen auf **App-Inventar anzeigen (alle Versionen)**. Unter **Geräte > App-Inventar** wird daraufhin eine nach Bundle-ID gefilterte Liste der App angezeigt.



8.7. App-Konfiguration

Dieser Abschnitt enthält die folgenden Themen:

- Lizenzierung für App-Funktionen
- Gemeinsame Konfigurationsschritte für mehrere Apps
- Apps ausblenden und vorübergehend anhalten (nur Android)
- Konfigurieren des Netzwerkrelais
- Konfigurieren von 5G-Mobilfunk-Slicing
- Verteilen einer Anwendung unter Verwendung der Konfiguration "Web-Content-Filter"
- Verteilen einer Anwendung unter Verwendung von DNS-Proxy
- App-Cache für Android Enterprise-Geräte löschen

Mit der App-Konfiguration können Sie die Installation, Werbung und Verteilung für jede App, die Sie auf den Benutzergeräten bereitstellen, nach Wunsch anpassen. Bei den Apps kann es sich um interne Apps, Apps aus einem öffentlichen Store oder Cloud-Apps handeln. Sie können die Apps flexibel für die verschiedensten Benutzer und Benutzergruppen mit eindeutigen Namen und für jeden Empfänger speziell angepassten Konfigurationen bereitstellen. Die Anzahl der Versionen der internen Anwendungen ist auf 100 begrenzt. Wenn diese Zahl überschritten wird, löscht das Cloud-System die ältesten Versionen der Anwendung. Der Status des Anwendungsuploads und der Bereinigung wird aufgelistet und ist auf der Seite Audit-Protokolle sichtbar.

> Wenn Sie die Werte für die App-Konfiguration einer App im App-Katalog oder in dem verwalteten App-Konfigurationsprofil ändern, muss sich das Gerät ein- oder zweimal anmelden, um die neuen Konfigurationswerte zu erhalten.

Lizenzierung für App-Funktionen

> Die folgenden Funktionen erfordern eine zusätzliche Lizenzierung:

- Installation/-Deinstallation von Apps im Hintergrund: Silver-Lizenz
- Konfiguration pro Anwendung: Gold Lizenz
- Kundenspezifische AppConnect-Konfiguration: Gold-Lizenz

Mehrere App-Pakete erfordern ein gutes Gruppenmanagement, da zukünftige Gerätearten möglicherweise nicht durch das Windows-Betriebssystem definiert werden können. Die einzige Möglichkeit zur Installation der richtigen Version der App ist in diesem Fall die Verwendung der korrekten Gruppe für die korrekte Anwendung durch den Administrator.

Gemeinsame Konfigurationsschritte für mehrere Apps

Führen Sie zuerst diese Schritte aus und setzen Sie dann mit den Konfigurationsschritten für jede einzelne App fort, die Sie bereitstellen wollen. Sie können mehrere Konfigurationen der gleichen App definieren und jeder Konfiguration einen eindeutigen Namen geben. Für jede Konfiguration können eigene Verteilungs- und Werberegeln entsprechend Ihrer Bereitstellungsstrategie gelten. Die Anzahl der Versionen der internen Anwendungen ist auf 100 begrenzt. Wenn diese Zahl überschritten wird, löscht das Cloud-System die ältesten Versionen der Anwendung. Der Status des Anwendungsuploads und der Bereinigung wird aufgelistet und ist auf der Seite Audit-Protokolle sichtbar. Sie können eine Anwendung für maximal 100 Benutzer, Benutzergruppen, Geräte oder Gerätegruppen auf einmal bereitstellen. Sie können eine App auswählen, um sie zum App-Katalog hinzuzufügen.
Ivanti Neurons for MDM verfügt über einen asynchronen Prozess für den Befehl Installation senden/Aktualisierung anfordern für iOS-

Apps. Wenn Sie den Befehl Installation senden/Aktualisierung anfordern verwenden, zeigt das Ivanti Neurons for MDM-Administrationsportal eine Meldung an, die darüber informiert, dass:

- der Prozess weiterhin im Hintergrund ausgeführt wird
- der Prozess abgeschlossen ist
- der Prozess erfolgreich durchgeführt wurde bzw. Fehler vorhanden sind

Verfahren

1. Gehen Sie zu **Apps > Apps-Katalog** und klicken Sie auf **+Hinzufügen**.
2. Benutzen Sie das Pulldown-Menü, um entweder den App Store, Google Play oder Ihren eigenen App-Store auszuwählen und eine App im Katalog zu ergänzen.
   Wenn es Ihre Lizenzvereinbarung zulässt, können Sie auch Apps in Ihrem Katalog hinzufügen.
3. Sie können auch die Kategorie für die App bearbeiten.
4. Optional können Sie auch eine Kurzbeschreibung der App in dem Feld **Beschreibung** einfügen.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie eine Verteilungsebene für diese Konfiguration der App:
   - **Für alle** - Die App wird bei allen benutzerkompatiblen Geräten hinzugefügt.
   - **Für niemand** - Die Verteilung der App wird auf später verschoben.
   - **Benutzerdefinierte Verteilung** - Wählen Sie eine der folgenden Optionen:
     - **Benutzer/Benutzergruppen** - Die Anwendung wird nur an die von Ihnen ausgewählten Benutzer oder Benutzergruppen verteilt.
       Klicken Sie auf die Registerkarte **Benutzer**, um die Benutzer auszuwählen.
       Klicken Sie auf die Registerkarte **Benutzergruppen**, um die Benutzergruppe(n) auszuwählen.
     - **Geräte/Gerätegruppen** - Die App wird nur an die von Ihnen ausgewählten Geräte oder Gerätegruppen verteilt
       Klicken Sie auf die Registerkarte **Geräte**, um die Geräte auszuwählen.
       Klicken Sie auf die Registerkarte **Gerätegruppen**, um die Gerätegruppe(n) auszuwählen.
7. Klicken Sie auf **Weiter**.

Installationsoptionen konfigurieren

Sie können die Installationskonfigurationsoptionen auswählen.

Verfahren

1. Klicken Sie auf **Anwendungskonfigurationseinstellungen installieren** oder auf das Symbol **+**, um eine weitere Konfiguration hinzuzufügen und die Seite **Konfigurations-Setup** anzuzeigen.
2. Geben Sie einen Namen für die Konfiguration im Feld **Name** ein.
3. Sie können auch eine Kurzbeschreibung der Installationskonfiguration in dem Feld **Beschreibung** eingeben.
4. Wählen Sie die Option **Konfigurationen für die Geräteinstallation** aus.
5. Wählen Sie eine der folgenden Optionen aus:
   - **Installation auf Gerät verlangen**
   - **Nur einmalig bei der Geräteregistrierung installieren**

6. Wählen Sie die Option **Keine bestimmte App-Version erforderlich**, aus, um zu verhindern, dass eine bereits installierte App auf eine niedrigere Version zurückgestuft wird. Diese Option ist nur für moderne Apps verfügbar.
7. Wählen Sie aus den folgenden Optionen:
    - **Installation im Hintergrund in Samsung KNOX Workspaces und auf Zebra-Geräten**
    - **App nicht im App-Katalog des Endbenutzers anzeigen**
    - **App nicht auf neu registrierten Geräten installieren**: Vorhandene Geräte sind nicht betroffen und zeigen die App weiterhin im App-Katalog des Geräts an.
        - Für neu registrierte Geräte dieser Verteilung wird die App nicht aufgeführt oder via Push übertragen.
        - Wenn der Administrator einen Installations-/Aktualisierungsbefehl auslöst, wird der Befehl an das Gerät gesendet.
    - **App-Update verschieben um**: Mit dieser Option verzögern Sie die Installation der neuen App-Version. Diese Einstellung verzögert die automatische Installation neuer App-Versionen basierend auf der konfigurierten Dauer.
    - **App-Update-Modus** (auch für AMAPI-Geräte unterstützt). (nur Android)
      Verwenden Sie diese Option, um eine App auf die neueste Version zu aktualisieren, indem Sie einen der folgenden drei Modi verwenden:
        - Standard: Dieser Modus wird ausgewählt, sobald Sie die Option „App-Update-Modus“ auswählen. In diesem Modus erfolgt die Aktualisierung innerhalb von 24 Stunden ab dem Zeitpunkt der Verfügbarkeit der App.
        - Für 90 Tage aufschieben: Wenn Sie diesen Update-Modus auswählen, können Sie die App-Updates 90 Tage aufschieben. Nach 90 Tagen werden die Apps automatisch aktualisiert, entsprechend den anderen Einstellungen, die in der Konfiguration für Managed Google Play vorgenommen wurden.
        - Hohe Priorität: Wenn Sie diesen Aktualisierungsmodus auswählen und das Gerät des Benutzers online ist, wird die App sofort aktualisiert, sobald sie im Google Play Store verfügbar ist.
    - **App-Installationspriorität festlegen** – Weitere Details finden Sie unter dem Thema "Konfigurieren der App-Priorität".

> Auf Android-Geräten sind App-Updates über die Option für automatische Updates auch dann erlaubt, wenn die Option für die Installation im Hintergrund nicht ausgewählt wurde. Der Administrator kann App-Updates auf Apps steuern, die nicht obligatorisch sind, oder auf Apps, die vom Benutzer selbst installiert wurden.

    - **Während der Verwendung der App nicht aktualisieren**: Wählen Sie diese Option aus, um zu verhindern, dass eine Anwendung aktualisiert wird, während der Benutzer die Anwendung aktiv verwendet. Diese Option bewirkt Folgendes:
        - Anwendungsupdates werden verschoben, während die Anwendung im Vordergrund ausgeführt wird.
        - Der Benutzer kann die Anwendung ohne Unterbrechung weiterverwenden.
        - Das ausstehende Update wird automatisch installiert, sobald die Anwendung geschlossen oder in den Hintergrund verschoben wird.

Anwendungen entfernen, wenn Verteilung entfernt wird (Android)
Bei verwalteten Google Play-Anwendungen entfernt Ivanti Neurons for MDM automatisch eine Anwendung von Android-Geräten, wenn die Anwendung nicht mehr dem Gerät zugewiesen ist.
Eine Anwendung wird in den folgenden Szenarien entfernt:

- Die Anwendungsverteilung wird auf "Niemand" geändert.
- Die Anwendung wird aus dem App-Katalog gelöscht.
- Das Gerät ist von der Anwendungsverteilung ausgeschlossen.

Ihnen werden je nach der gewählten App gegebenenfalls weitere Konfigurationsoptionen angezeigt. Eine solche Option ist beispielsweise die Möglichkeit, mehrere Schlüssel-Wert-Paare zu ergänzen. Klicken Sie in solchen Fällen auf **+Hinzufügen**, um Schlüssel-Wert-Paare zu ergänzen. Weitere Informationen finden Sie unter **Hinzufügen einer App über einen öffentlichen Store** im App-Katalog.

9. (macOS 11+) Wählen Sie die Optionen für die Installation und Konfiguration der Apps als verwaltete Apps:
   - **Als verwaltete App installieren**
   - **In verwaltete App konvertieren**

   > In macOS 12.0+ werden verwaltete Apps auf benutzerregistrierten Geräten unterstützt.

Apps ausblenden und vorübergehend anhalten (nur Android)

Für Android-Geräte in den Modi **Arbeitsprofil**, **Vollständig verwaltetes Gerät**, **Vollständig verwaltetes Gerät mit Arbeitsprofil** und **Arbeitsprofil auf firmeneigenem Gerät** können Sie jetzt Apps nach der Installation ausblenden oder vorübergehend anhalten.

Verfahren

	1.	**Installieren Sie eine oder mehrere Apps auf dem Gerät, auf dem Sie die Aktion "Ausblenden" oder "Vorübergehend anhalten" anwenden möchten.**
	2.	**Erstellen Sie eine App Control-Konfiguration und fügen Sie die verwalteten Apps zur Liste "Ausblenden" oder "Vorübergehend anhalten" hinzu.**
	3.	**Wenden Sie die Änderungen auf das Gerät an.**

> Ist eine App sowohl in der Liste "Ausblenden" als auch in der Liste "Vorübergehend anhalten" vorhanden, wird sie ausgeblendet, da diese Liste Vorrang hat.

App-Priorität konfigurieren

Sie können die Reihenfolge festlegen, in der Apps auf dem Gerät empfangen werden, wenn es zum ersten Mal registriert wird (insbesondere innerhalb der ersten 20 Minuten nach Registrierungsdatum und -zeit) und in der die obligatorischen Apps per Push für die Installation übertragen werden. Sie können festlegen, mit welcher Priorität bestimmte Anwendungen vor anderen Anwendungen heruntergeladen werden. Zum Beispiel können Sie festlegen, dass Downloads von Tunnel- und E-Mail-Anwendungen gegenüber anderen, unkritischen Apps Priorität haben. Diese Funktion ist sowohl für öffentliche als auch für private Apps anwendbar. Obligatorische Apps werden vor abhängigen Apps per Push übertragen.

Diese Funktion wird auf Geräten mit iOS (außer AppStation für iOS), Android (außer Android Enterprise), macOS (interne PKG-Apps und Apple Apps and Books-Apps) und Windows unterstützt.

> Diese Funktion ist für neue Registrierungsgeräte verfügbar. Standardmäßig sind alle Apps auf mittlere Priorität eingestellt. Während dieses Prozesses kann der Benutzer wahlweise jede App im Katalog manuell installieren, auch wenn eine solche App dann um Ressourcen konkurriert und eventuell vor Apps mit hoher Priorität in die Warteschlange eingereiht wird.

> Bei Windows-Apps hat Bridge gegenüber allen anderen Apps die höchste Priorität.

Im vorherigen Abschnitt "Installationsoptionen konfigurieren" finden Sie die Schritte zum Festlegen der Priorität einer Anwendung mit der Option **App-Installationspriorität** festlegen. Sie können für eine Anwendung eine hohe, mittlere oder niedrige Priorität festlegen. Apps mit gleicher Priorität werden nicht in einer bestimmten Reihenfolge installiert. Bei App-Updates wird, wenn der Benutzer die App bereits installiert hat, die App-Priorität ignoriert.

Auswählen von Konfigurationseinstellungen zur Apple-Anwendungsverwaltung

Diese Einstellungen gelten nur für diese App und überschreiben globale Einstellungen, die unter **Apps > Katalogeinstellungen** ausgewählt sind. Sie können Einstellungen für **Apple App Management** auswählen.

Verfahren

1. Klicken Sie auf **Apple Apps Einstellungen** oder auf das Symbol **+**, um eine weitere Konfiguration hinzuzufügen und die Seite **Konfigurationssetup** anzuzeigen.
2. Geben Sie einen Namen für die Konfiguration im Feld **Name** ein.
3. Geben Sie eine Kurzbeschreibung der Konfiguration im Feld **Beschreibung** ein.
4. Aktivieren oder deaktivieren Sie eine oder mehrere der folgenden Optionen, bei den **Apple-Verwaltungseinstellungen**:
   - **Datensicherung in iCloud und iTunes verhindern**
   - **Apps bei Deregistrierung entfernen**
   - (iOS 14.0+) Entfernen und Entladen dieser App zulassen - Sie können diese Option deaktivieren, wenn Sie verhindern wollen, dass ein Benutzer eine verwaltete Anwendung entfernt und entlädt.
   - (Optional) **Von Apple verwaltete App-Konfiguration** hinzufügen
5. Klicken Sie auf **Aktualisieren**.

App-Promotionsebenen auswählen

Sie können die Werbeebene für die App definieren.

Verfahren

1. Klicken Sie auf **Werbeverteilungskonfigurationseinstellungen** oder auf das Symbol **+**, um eine weitere Konfiguration hinzuzufügen und die Seite **Werbekonfiguration** anzuzeigen.
2. Klicken Sie auf **Bearbeiten**.
3. Geben Sie einen Namen für die Konfigurationseinstellungen zur Werbeverteilung in dem Feld **Name** ein.
4. Sie können auch eine Kurzbeschreibung der Konfiguration in dem Feld **Beschreibung** eingeben.
5. Wählen Sie die Werbeebene aus, die die App erhalten soll: **Nicht empfohlen**, **Funktionsliste**, oder **Funktionsbanner**. Eine App mit der Option **Nicht empfohlen** wird nicht in der Liste angezeigt.
6. Wenn Sie Empfohlenes Banner auswählen, geben Sie bitte Folgendes an:
   1. **Titel** – Geben Sie den Titel der Anwendung an.
   2. **Beschreibung** – Geben Sie Details zur Anwendung an.
   3. **Bannerstil** – Wählen Sie einer Bannerfarbe aus.
7. Klicken Sie auf **+ Beschreibung hinzufügen**, um eine Kurzbeschreibung der Konfiguration einzugeben.

8. Sie können auch die Verteilung der Konfiguration ändern.
9. Klicken Sie auf **Fertig**, um die App-Konfiguration zu speichern.

AppTunnel-Traffic-Regeln konfigurieren

Definieren Sie mit AppTunnel die Traffic-Regeln, die den Zugriff auf Dienste über Sentry zulassen.

Informationen zum Hinzufügen einer AppTunnel-Konfiguration finden Sie unter „AppTunnel-Konfiguration hinzufügen“ in der *AppConnect-Anleitung für Cloud*.

Verwaltete App konfigurieren

Verfahren

1. Klicken Sie auf das **+** Symbol, um die Konfigurationsseite zu öffnen.
2. Klicken Sie auf **+ Beschreibung hinzufügen**, um eine Kurzbeschreibung der Konfiguration einzugeben.
3. Klicken Sie auf **+ Hinzufügen**, um Schlüssel und Wert einzugeben.
4. Wählen Sie eine Verteilungsebene.
5. Klicken Sie auf **Weiter**.

Konfiguration einer VPN-Verbindung für jede App mit Per-App-VPN

Verfahren

1. Klicken Sie auf das **+** Symbol, um die Konfigurationsseite zu öffnen.
2. Geben Sie einen Namen für die VPN-Verbindung dieser App im Feld **Name** ein.
3. Klicken Sie auf **+ Beschreibung hinzufügen**, um eine Kurzbeschreibung der Konfiguration einzugeben.
4. Klicken Sie auf das Kontrollkästchen **Per-App-VPN für diese App aktivieren** und wählen Sie eine verfügbare Per-App-VPN-Konfiguration aus.
5. (Optional) Für macOS-Anwendungen geben Sie den String **Designierte Anforderung** im Format Bezeichner „\%s\“ ein. Benutzen Sie als Bezeichner zum Beispiel „com.google.Chrome“. Verwenden Sie dieses Feld, damit eine macOS-App mit mehreren Paketen ein Pro-App-VPN wie Tunnel verwenden kann.
6. Wählen Sie aus, wie **diese App-Konfiguration verteilt werden soll**.
7. Klicken Sie auf **Weiter**.

Konfiguration für von Apple verwaltete App verwenden

Über die Konfiguration für die von Apple verwaltete App können spezifische Einstellungen der installierten verwalteten App definiert werden. Bei einer Anwendung können bestimmte Konfigurationsparameter vom Entwickler implementiert oder beschränkt sein. Bei Anwendungen mit solchen Einschränkungen sind Ihre Konfigurationsoptionen möglicherweise begrenzt. Sie können von Apple verwaltete Apps konfigurieren.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Wählen Sie eine App aus.
3. Klicken Sie auf die Registerkarte **App-Konfigurationen**.

4. Klicken Sie auf **Konfiguration für von Apple verwaltete App** oder klicken Sie auf die Schaltfläche **+**.
   In der Konfiguration für die von Apple verwaltete App sind einige Standardeinstellungen vorhanden.
5. Klicken Sie auf **Hinzufügen**, um gegebenenfalls eine andere Konfiguration hinzuzufügen. Sie können auch auf den Namen der Konfiguration klicken, um die Konfiguration zu bearbeiten.
6. Wählen Sie unter **Konfigurationsquelle** eine der Optionen für den **Quellentyp**.

- **AppConfig Community** - Diese Option ist nur für Apps verfügbar, für die in der Community-Repository eine Spezifikation der App-Konfiguration verfügbar ist. Wenn diese Option verfügbar ist, ist sie standardmäßig ausgewählt.
- **.xml spec verwenden** - Mit dieser Option können Sie das Schema für die App hochladen, um eine bestimmte Version der App-Konfiguration per Push zu übertragen. Klicken Sie auf **Datei auswählen**, um die .xml-Datei hochzuladen. Stellen Sie sicher, dass die .xml-Datei die Bundle-ID und die Version enthält. Eine Fehlermeldung wird angezeigt, wenn die Bundle-ID in der Datei nicht mit der Bundle-ID der App übereinstimmt.
- **Keine** - Wählen Sie diese Option, wenn Sie kein Schema für die Anwendung übernehmen möchten. Diese Option ist standardmäßig ausgewählt, wenn die Option **AppConfig Community** nicht verfügbar ist.
  Die hochgeladene .xml-Datei wird im Abschnitt **Konfigurationsquelle** angezeigt. Klicken Sie auf das Löschsymbol, um die hochgeladene .xml-Datei zu löschen.

7. In den **Einstellungen der von Apple verwaltete App** können Sie die Konfigurationsoptionen zur Eingabe von Schlüssel-Wert-Paaren einstellen.

- Klicken Sie auf **Hinzufügen**, um die Schlüssel-Wert-Paare zu der verwalteten App-Konfiguration hinzuzufügen und die Registrierungsnamen-Identität des Go-Clients während iReg oder Apple Device Enrollment abzurufen.
  Sie können die Datentypen (String, Integer, Boolean, Long Float, Double, Date, String Array, Integer Array, Double Array, Float Array, Long Array) für die Schlüsselwertpaare auswählen.

Fügen Sie die folgenden Schlüssel-Wert-Paare zur Konfiguration der verwalteten App hinzu, um die Registrierungsnamen-Identität des Go-Client während iReg oder Apple Device Enrollment abzurufen:

Schlüssel	Wert	Typ
registration.username	$	ZEICHENFOLGE
registration.token	$	STRING
registration.token.expirationSeconds	$	ZEICHENFOLGE
registration.url	$	ZEICHENFOLGE

Fügen Sie die folgenden Schlüssel-Wert-Paare zur Konfiguration der verwalteten App hinzu, um die Registrierungsnamen-Identität während iReg oder Apple Device Enrollment über den Mac-Agenten (Mobile@Work) abzurufen:

Schlüssel	Wert	Typ
ClientRegistrationUrl	$	ZEICHENFOLGE
Token	$	ZEICHENFOLGE
TokenExpiresAt	$	ZEICHENFOLGE

Falls der Endbenutzer die Ivanti Go-Anwendung beendet, klicken Sie auf **Bearbeiten**, um die Anwendung für eine der folgenden Aktionen zu konfigurieren:

Schlüssel	Wert	Typ
Verwenden Sie zum Anzeigen der Standardbenachrichtigung folgende Werte:		
enableAppTerminationNotification	wahr/falsch ODER 1/0	Boolescher Wert ODER Zeichenfolge
Verwenden Sie zum Anzeigen einer benutzerdefineirten Benachrichtigung folgende Werte:		
appTerminationNotificationMessage	Benutzerdefinierte Benachrichtigung	Zeichenfolge
enableAppTerminationNotification	wahr/falsch ODER 1/0	Boolescher Wert ODER Zeichenfolge

- **.plist verwenden** - .plist-Dateien enthalten mehrere Schlüssel-Wertepaare, die in einem Durchgang hochgeladen werden sollen. Klicken Sie auf **Datei auswählen**, um die .plist-Datei hochzuladen. Die validierten Plist-Daten werden in der Tabelle **Einstellungen für die von Apple verwaltete App** angezeigt.

plists mit verschachtelten Wörterbüchern sind ungültig.

8. Klicken Sie auf **Aktualisieren**, um die Einträge zu speichern.

Konfigurieren des Netzwerkrelais

Relais machen den Netzwerkverkehr Ihrer App privater und sicherer, ohne Verbindung zu einem VPN. Weitere Informationen finden Sie unter Netzwerkrelais-Konfiguration.

1. Klicken Sie auf das Symbol **Netzwerkrelais +**, um die Konfigurationsseite zu öffnen.
2. Geben Sie einen Namen für das **Netzwerkrelais** der App in das Namensfeld ein.
3. Klicken Sie auf **+ Beschreibung hinzufügen**, um eine Kurzbeschreibung der Konfiguration einzugeben.
4. Klicken Sie auf **Netzwerkrelais aktivieren** für diese App-Option und wählen Sie eine verfügbare **Netzwerkrelais-Konfiguration** aus.
5. Wählen Sie aus, wie **diese App-Konfiguration verteilt werden soll**.
6. Klicken Sie auf **Weiter**.

Konfigurieren von 5G-Mobilfunk-Slicing

Mit der Unterstützung für 5G-Mobilfunk-Slicing können einzelne verwaltete Apps (für alle iOS-Apps)einem Netzwerksegment zugewiesen werden, wodurch möglicherweise bestimmte Netzwerkfunktionen und Eigenschaften für eine optimierte App-Erfahrung verfügbar werden. Die Zuweisung erfolgt über das neue App-Attribut **CellularSliceUUID** entweder im Installationsbefehl der MDM-App

oder in einer deklarativen App-Konfiguration. Der in den Schlüssel zu platzierende Zeichenfolgewert des Netzwerksegments muss vom unterstützenden Betreiber bereitgestellt werden.

> 5G-Network-Slicing wird nicht verwendet, wenn entweder die konkrete App oder das ganze Gerät für die Verwendung von VPN konfiguriert ist.

ProcedureVerfahren

1. Wechseln Sie zu **Apps > App-Katalog > App-Konfigurationen > 5G-Mobilfunk-Slicing** und klicken Sie auf **Hinzufügen**.
2. Aktualisieren Sie im Abschnitt **Konfigurations-Setup** folgende Felder:
   - [Name]
   - Wählen Sie die Option **5G-Network-Slicing aktivieren** aus.
   - Wählen Sie den **DNN** oder die **App-Kategorie** aus (je nach Netzwerkanbieter).
3. Wählen Sie eine Verteilungsebene für diese Konfiguration der App:
4. Klicken Sie auf **Speichern**.

Verteilen einer Anwendung unter Verwendung der Konfiguration "Web-Content-Filter"

Sie können eine Anwendung statt mit einem DNS-Proxyserver auch mit der Konfiguration "Web-Content-Filter" verteilen. Nachdem Sie die Konfiguration "Web-Content-Filter" erstellt haben, können Sie sie einer Anwendung hinzufügen, um die Anwendung zu verteilen. Weitere Informationen zur Konfiguration "Web-Content-Filter" finden Sie unter **Web-Content-Filter**.

Verfahren

1. Gehen Sie zu **Apps** > **App-Katalog**.
2. Wählen Sie eine App aus.
3. Klicken Sie auf Weiter.
4. Wählen Sie die Delegierungsoption aus und klicken Sie auf **Weiter**.
5. Wählen Sie die Verteilungsoptionen aus und klicken Sie auf **Weiter**.
6. Wählen Sie die **Konfiguration "Web-Content-Filter** aus und klicken Sie auf das Pluszeichen (**+**).
7. Geben Sie den **Namen** an.
8. Markieren Sie das Kontrollkästchen **Web-Content-Filter für diese Anwendung aktivieren**.
9. Wählen Sie den Web-Content-Filter aus dem Dropdownmenü aus.
10. Wählen Sie eine Verteilungsebene für diese Konfiguration der App:
    1. **Für alle** - Die App wird bei allen benutzerkompatiblen Geräten hinzugefügt.
    2. **Für niemand** - Die Verteilung der App wird auf später verschoben.
    3. **Benutzerdefinierte Verteilung** - Wählen Sie eine der folgenden Optionen:
       - **Benutzer/Benutzergruppen** - Die Anwendung wird nur an die von Ihnen ausgewählten Benutzer oder Benutzergruppen verteilt.
         Klicken Sie auf die Registerkarte **Benutzer**, um die Benutzer auszuwählen.
         Klicken Sie auf die Registerkarte **Benutzergruppen**, um die Benutzergruppe(n) auszuwählen.

- **Geräte/Gerätegruppen** – Die App wird nur an die von Ihnen ausgewählten Geräte oder Gerätegruppen verteilt.
  Klicken Sie auf die Registerkarte **Geräte**, um die Geräte auszuwählen.
  Klicken Sie auf die Registerkarte **Gerätegruppen**, um die Gerätegruppe(n) auszuwählen.

11. Klicken Sie auf **Weiter**.
12. Klicken Sie auf **Fertig**. Die ausgewählte App wird über die Konfiguration "Web-Content-Filter" an bestimmte Benutzer verteilt.

Verteilen einer Anwendung unter Verwendung von DNS-Proxy

Sie können eine Anwendung mit der Konfiguration "DNS-Proxy" verteilen. Nachdem Sie die Konfiguration "DNS-Proxy" erstellt haben, können Sie sie einer Anwendung hinzufügen, um die Anwendung zu verteilen. Weitere Informationen zur Konfiguration "DNS-Proxy" finden Sie unter Erstellen der DNS-Proxykonfiguration.

Verfahren

1. Gehen Sie zu **Apps** > **App-Katalog**.
2. Wählen Sie eine App aus.
3. Klicken Sie auf Weiter.
4. Wählen Sie die Delegierungsoption aus und klicken Sie auf **Weiter**.
5. Wählen Sie die Verteilungsoptionen aus und klicken Sie auf **Weiter**.
6. Wählen Sie die **Konfiguration "DNS-Proxy** aus und klicken Sie auf das Pluszeichen (**+**).
7. Geben Sie den **Namen** an.
8. Markieren Sie das Kontrollkästchen **DNS-Proxy für diese Anwendung aktivieren**.
9. Wählen Sie den DNS-Proxy aus dem Dropdownmenü aus.
10. Wählen Sie eine Verteilungsebene für diese Konfiguration der App:
    1. **Für alle** - Die App wird bei allen benutzerkompatiblen Geräten hinzugefügt.
    2. **Für niemand** - Die Verteilung der App wird auf später verschoben.
    3. **Benutzerdefinierte Verteilung** - Wählen Sie eine der folgenden Optionen:
       - **Benutzer/Benutzergruppen** - Die Anwendung wird nur an die von Ihnen ausgewählten Benutzer oder Benutzergruppen verteilt.
         Klicken Sie auf die Registerkarte **Benutzer**, um die Benutzer auszuwählen.
         Klicken Sie auf die Registerkarte **Benutzergruppen**, um die Benutzergruppe(n) auszuwählen.
       - **Geräte/Gerätegruppen** – Die App wird nur an die von Ihnen ausgewählten Geräte oder Gerätegruppen verteilt.
         Klicken Sie auf die Registerkarte **Geräte**, um die Geräte auszuwählen.
         Klicken Sie auf die Registerkarte **Gerätegruppen**, um die Gerätegruppe(n) auszuwählen.
11. Klicken Sie auf **Weiter**.
12. Klicken Sie auf **Fertig**. Die ausgewählte App wird über die Konfiguration "DNS-Proxy" an bestimmte Benutzer verteilt.

Klonen von App-Konfigurationseinstellungen

Sie können die Konfigurationseinstellungen einer verwalteten App klonen, um die Einstellungen auf andere Geräte anzuwenden. Sie können die geklonten Einstellungen auch umbenennen und Änderungen daran vornehmen.

Android-

Sie können Konfigurationseinstellungen auf Android-Geräten klonen.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Wählen Sie die App aus, über die Sie die Konfigurationseinstellungen klonen möchten.
3. Klicken Sie auf **App-Konfigurationen**.
4. Im Abschnitt **Übersicht über App-Konfigurationen** finden Sie die Liste der für Android-Geräte verfügbaren Konfigurationen (**Verwaltete Konfigurationen für Android**, **Auf Gerät installieren**, **Werbung**, **Delegierte Geräteberechtigungen** und **Google Play Release**).
5. Klicken Sie auf eine der verfügbaren Konfigurationen.
6. Klicken Sie unter **Aktionen** auf **Klonen**, um den Klonvorgang zu starten.
7. Standardmäßig lautet der Name der geklonten Konfiguration <Copy of the Cloned Configuration name>. Sie können jedoch den Namen ändern, indem Sie in das Feld **Name** einen Namen Ihrer Wahl eingeben.
8. (Optional) Machen Sie Angaben zu der geklonten Einstellung im Feld **Beschreibung**.
9. Klicken Sie auf **Weiter**.

Ein Bestätigungsdialogfeld weist darauf hin, dass das Klonen der App-Konfigurationseinstellungen abgeschlossen ist. Sie können die geklonte Version im Abschnitt "Übersicht über App-Konfigurationen" und innerhalb der geklonten App anzeigen.

iOS-

So können Konfigurationseinstellungen für verwaltete Apps auf iOS-Geräten klonen.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Wählen Sie die App aus, über die Sie die Konfigurationseinstellungen klonen möchten.
3. Klicken Sie auf **App-Konfigurationen**.
4. Im Abschnitt **Übersicht über App-Konfigurationen** finden Sie die Liste der für iOS-Geräte verfügbaren Konfigurationen (**Auf Gerät installieren**, **Apple-App-Einstellungen**, **Werbung**, **Benutzerdefinierte AppConnect-Konfiguration**, **App-Tunnel**, **Von Apple verwaltete App-Konfiguration** und **Per-App-VPN**).
5. Klicken Sie auf die Konfiguration, die Sie klonen möchten.
6. Klicken Sie unter **Aktionen** auf **Klonen**, um den Klonvorgang zu starten.
7. Standardmäßig lautet der Name der geklonten Konfiguration <Copy of the Cloned Configuration name>. Sie können jedoch den Namen ändern, indem Sie in das Feld **Name** einen Namen Ihrer Wahl eingeben.
8. (Optional) Machen Sie Angaben zu der geklonten Einstellung im Feld **Beschreibung**.
9. Wählen Sie aus der Liste **Quelltyp** eine Konfigurationsquelle aus.
10. Geben Sie im Abschnitt **Apple Managed App Settings** section, enter **Key**, **Value**, and select **Type** from the list.
    Informationen zu **Schlüssel**, **Wert** und **Typ** finden Sie unter **Verwenden der von Apple verwalteten App-Konfiguration**.
11. Klicken Sie auf **Weiter**.
    Ein Bestätigungsdialogfeld weist darauf hin, dass das Klonen der App-Konfigurationseinstellungen abgeschlossen ist. Sie können die geklonte Version im Abschnitt **Von Apple verwaltete App-Konfiguration** anzeigen.

Windows

Sie können App-Konfigurationseinstellungen auf Windows-Geräten klonen:

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Wählen Sie die App aus, über die Sie die Konfigurationseinstellungen klonen möchten.
3. Klicken Sie auf **App-Konfigurationen**.
4. Im Abschnitt **Übersicht über App-Konfigurationen** finden Sie die Konfigurationen **Auf Gerät installieren** und **Werbung**.
5. Klicken Sie auf die Konfiguration, die Sie klonen möchten.
6. Klicken Sie unter **Aktionen** auf **Klonen**, um den Klonvorgang zu starten.
7. Standardmäßig lautet der Name der geklonten Konfiguration <Copy of the Cloned Configuration name>. Sie können jedoch den Namen ändern, indem Sie in das Feld **Name** einen Namen Ihrer Wahl eingeben.
8. (Optional) Machen Sie Angaben zu der geklonten Einstellung im Feld **Beschreibung**.
9. Klicken Sie auf **Weiter**.

Ein Bestätigungsdialogfeld weist darauf hin, dass das Klonen der App-Konfigurationseinstellungen abgeschlossen ist. Sie können die geklonte Version im Abschnitt "Übersicht über App-Konfigurationen" und innerhalb der geklonten App anzeigen.

Auswahl der Apps für Windows 10 in Ihrem internen Katalog.

Wählen Sie die Apps aus, die Sie in Ihrem internen Katalog hinzufügen wollen. Interne, Microsoft Store- und Microsoft for Business-Apps werden auf Windows 10 unterstützt. Windows 10 erzwingt die Compliance direkt auf dem Gerät in Abhängigkeit von den Apps, die Sie zulassen bzw. nicht zulassen.

> Das Anmeldeintervall für Windows 10 ist standardmäßig auf jeweils 60 Minuten eingestellt. Möglicherweise wollen Sie die Anmeldung eines Geräts erzwingen, um ein Update des Geräts durchzuführen und den App-Status zu kontrollieren.

Folgende Aktionen werden unterstützt:

- Hochladen neuer Apps
- Installation im Hintergrund
- Manuelle Installation mit Apps@Work
- Hinzufügen einer neuen Version der App
- Löschen einer App

Folgende Formate werden unterstützt:

- APPX
- APPXBUNDLE
- MSI-gepackte Win32 - mitgelieferte Win32-App
- MSIX (wird bei Geräten mit Windows 10 ab RS5 und höher unterstützt)
- .EXE (unter Verwendung von Bridge)

> Die App **Ivanti Neurons Agent** ist im **App-Katalog** für **Windows**-Geräte verfügbar. Der Administrator kann die App **Ivanti Neurons Agent** als interne App bereitstellen und entsprechend an Windows-Geräte verteilen.

Konfigurieren von Windows 10-Apps

Verfahren

1. Klicken Sie in der Hauptnavigationsleiste auf Geräte.
2. Wählen Sie ein Gerät mit Windows 10, das Sie in der Cloud registriert haben.
3. Klicken Sie auf Apps > App-Katalog.
4. Wählen Sie eine App aus.
5. Ergänzen Sie mit dem Pulldown-Menü Aktionen die App oder löschen Sie die App aus Ihrem Katalog.
   Sie können auch eine neue App-Version hinzufügen.
   - Klicken Sie auf das Pull-down-Menü Aktionen.
   - Wählen Sie die Option Neue Version hinzufügen.
   - Gehen Sie zum Katalog und wählen Sie eine neue Version der App aus.
   - Klicken Sie auf Aktualisieren und Speichern, um den Bildschirm mit den App-Informationen anzuzeigen.
6. Wählen Sie über das Pull-down-Menü **Version** die gewünschte Version aus.
7. Klicken Sie auf Bearbeiten , um mit Änderungen an den Details zu beginnen.
   - Bearbeiten Sie gegebenenfalls die Kategorie.
   - Geben Sie bei Bedarf eine Beschreibung ein.
   - Ergänzen Sie ggf. Bildschirmfotos.
8. Klicken Sie auf Speichern.
9. Klicken Sie auf die Registerkarte Verteilung und dann auf Bearbeiten, um Änderungen auf der Verteilungsebene vorzunehmen.
10. Klicken Sie auf Speichern.
11. Klicken Sie auf die Registerkarte App-Konfigurationen, um eine Übersicht der aktuellen Konfiguration anzuzeigen.
12. Geben Sie ggf. eine Beschreibung der App ein.
13. Klicken Sie in der Übersichtsseite "App-Konfigurationen" auf die Option Auf Gerät installieren.
    Standardmäßig erfolgt die Installation im Hintergrund. Diese Einstellung kann nicht geändert werden.
14. Klicken Sie auf der linken Navigationsseite auf Werbung, und dann auf die Option Werbungsverteilung-Konfigurationseinstellungen, um die Werbungsebene zu ändern.
    - Klicken Sie auf Bearbeiten, um Änderungen an den Einstellungen der Werbeebene vorzunehmen.
    - Geben Sie einen Namen für die Konfiguration ein.
    - Geben Sie eine Beschreibung für die Konfiguration ein.
    - Wählen Sie eine Promotionsoption aus.
    - Klicken Sie auf **Aktualisieren,** um die Änderungen zu speichern.
15. Klicken Sie auf die Registerkarte Bewertungen, um Informationen zu den Bewertungen anzuzeigen.
    Exportieren Sie die Rezensionsdaten ggf. in eine Tabellenkalkulation.

App-Konfigurationseinstellungen für Windows 10 bearbeiten

Verfahren

1. Klicken Sie auf Richtlinien > Konfiguration.
2. Klicken Sie auf +Add.
3. Wählen Sie die Option Windows- App-Kontrolle aus, um den Bildschirm Windows-Appkontrollkonfiguration erstellen anzuzeigen.

4. Geben Sie für die Konfiguration einen Namen und eine Beschreibung ein.
5. Definieren Sie den App-Typ wie folgt:
    - Zulässig (Whitelist) – Nur diese Apps sind zulässig. Diese Apps werden im Hintergrund installiert, wenn sie noch nicht auf dem Gerät vorhanden sind.
    - Nicht erlaubt (Blacklist) – Wenn diese Apps aus der Blacklist auf dem Gerät vorhanden sind, werden sie beim Start gesperrt.
6. Definieren Sie die Regeln für den App-Typ und den App-Identifikator.
7. Klicken Sie auf Apps suchen, um den Bildschirm Windows 10 Apps suchen anzuzeigen.
8. Geben Sie den Namen der App ein, die Sie im Windows Store suchen.
9. Wählen Sie aus den angezeigten Optionen die App aus, um sie zum App-Identifikator hinzuzufügen.
10. Sie können auch über das Pulldown-Menü "App-Typ" einen Pfad zum App-Identifikator definieren, um die Installation von Apps über den definierten Pfad zu erlauben oder zu verweigern oder alle in diesem Pfad installierten Apps zu blockieren.
    Der App-Typ **Publisher/PFN Equals** gilt für Windows 10+-Geräte und unterstützt PFN. **EXE/Win32 Equals**.
11. Klicken Sie auf Weiter.
12. Wählen Sie eine Verteilungsoption aus.
    - **Alle Geräte** .
    - **Keine Geräte**.
    - **Benutzerdefiniert** – Geben Sie die Benutzer oder Benutzergruppen ein, die die App erhalten sollen.
13. Klicken Sie auf Fertig.
14. Sie können die Regeldefinitionen bearbeiten und einen App-Typ auswählen sowie einen App-Identifikator festlegen.
    - Klicken Sie auf das Pull-down-Menü Aktionen.
    - Wählen Sie die Option Neue Version hinzufügen.
    - Wählen Sie eine neue Version der App aus.
    - Klicken Sie auf Aktualisieren und Speichern, um den Bildschirm mit den App-Informationen anzuzeigen.

Konfigurieren der Option "Gerät nach der Installation neu starten" für Windows

Sie können ein Gerät so konfigurieren, dass es nach einer App-Installation neu gestartet wird. Verwenden Sie dazu die Option **Gerät nach der Installation neu starten**.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Wählen Sie eine beliebige Windows-spezifische App aus der Liste aus.
3. Gehen Sie zu **App-Konfigurationen > Auf Gerät installieren > Anwendung installieren – Konfigurationseinstellung**.
4. Klicken Sie auf **Bearbeiten**, und aktivieren Sie die Option **Gerät nach der Installation neu starten**.
5. Wählen Sie eine der folgenden Zeitplanoptionen aus, um festzulegen, wann das Gerät neu gestartet werden soll:

Einstellung	Aktion
Direkt nach der Installation	Wählen Sie diese Option aus, um das Gerät unmittelbar nach Installation der Anwendung neuzustarten.
Zu einer bestimmten Uhrzeit an dem Tag	Wählen Sie diese Option aus, um das Gerät am Tag der Installation zu einer bestimmten Uhrzeit nach Installation der Anwendung neuzustarten.
Nach einigen Minuten	Wählen Sie diese Option aus, um das Gerät **15**, **30**, **60** oder **120** Minuten nach Installation der Anwendung neuzustarten.

6. Klicken Sie auf **Aktualisieren**.

Das Gerät wird zur geplanten Uhrzeit neu gestartet.

> Im Kontext von öffentlichen Apps und Microsoft Store for Business (MSB)-Apps müssen Sie die Einstellung **Auf Windows-Geräten automatisch installieren** über den Abschnitt **App-Konfigurationen** aktivieren.

Apps mit Apps@Work installieren

So installieren Sie eine App mit Apps@Work:

1. Klicken Sie auf den App Apps@Work.
   Ihre Administrator-E-Mail-Adresse und die Server-URL sind in dem Anmeldedialog für Apps@Work bereits eingetragen.
2. Geben Sie Ihr Passwort ein und klicken Sie auf "Anmelden", um die App-Seite anzuzeigen.
3. Wählen Sie eine App zur Installation aus. Sie können keine Apps installieren, die vorausgesetzte Apps benötigen, wenn diese vorausgesetzten Apps nicht bereits auf dem Client installiert sind.
   Bei Apps@Work für iOS-Geräte können Sie optional auf die Schaltfläche **Alles installieren** klicken, um alle Apps zu installieren. Diese Option ist in den Bildschirmen **Neue Freigaben**, **Empfohlene Apps** und **Kategorien** verfügbar.

> Apps and Books-Apps werden erst installiert, wenn die Apps and Books App-Lizenz akzeptiert wurde.

4. Klicken Sie auf Aktualisieren und Speichern, um den Bildschirm mit den App-Informationen anzuzeigen.

App-Installation und Updates für Android Enterprise-Geräte

Administratoren können eine App im Katalog für den allgemeinen Zugriff veröffentlichen und sie gleichzeitig zur sofortigen Nutzung auf einem bestimmten Gerät bereitstellen. Somit können Benutzer die App direkt empfangen, während sie gleichzeitig im Katalog zur Verfügung steht, wo sie von anderen Benutzern nach Bedarf installiert werden kann.

Zur Installation von Apps und Updates

1. Wechseln Sie zu **Apps > App-Katalog**.
2. Wählen Sie die gewünschte App.
3. Klicken Sie im Bildschirm **Details** auf **Aktionen**. Der Eintrag **Installations-/Update-Anfrage senden** wird angezeigt.
4. Klicken Sie auf "Installations-/Update-Anfrage senden". Das Dialogfeld **Installations-/Update-Anfrage senden** wird angezeigt.
5. Führen Sie unter **Installations- und Update-Benachrichtigungen an Geräte für diese Anwendung senden** folgende Schritte durch:

- Markieren Sie das Kontrollkästchen **Anfrage für neue Anwendung senden** (für Geräte, auf denen die App noch nicht installiert ist), um die neue Anwendung zu installieren.
- Wählen Sie **Anfrage für Updates senden** (für Geräte, auf denen die App installiert, aber ein Update verfügbar ist) aus.

6. Führen Sie unter **Benutzer für Anfrageversand auswählen** folgende Schritte aus:
   - Klicken Sie auf **Jeder**, um die Konfiguration an alle kompatiblen Benutzer zu verteilen. Die App wird im App-Katalog der Benutzer aufgeführt.
   - Klicken Sie auf **Benutzerdefiniert**, um die Benutzergruppe oder den Benutzer zu definieren, die/der die Anwendung im App-Katalog anzeigen kann.

> Die Verteilung **Installations-/Update-Anfrage senden** ist Bestandteil des Verteilungsprozesses. Die Einstellungen, die Sie im Bildschirm **Verteilung** wählen, bestimmen darüber, welche Geräte die App empfangen.

Ein Bestätigungsdialogfeld weist darauf hin, dass die Installation der App abgeschlossen ist.

Änderungen an neuen Installationen oder Updates werden unter **Dashboard** > **Audit-Protokolle** angezeigt.

> Für öffentliche und private Apps ist **Anfrage für Updates senden** (für Geräte, auf denen die App installiert, aber ein Update verfügbar ist) deaktiviert. Es ist nur **Anfrage für neue Anwendung senden** erlaubt.

Verwandte Themen:

- App-Katalog

App-Cache für Android Enterprise-Geräte löschen

Mit der **Anfrage zum Löschen des App-Caches** können Administratoren zwischengespeicherte Daten für eine ausgewählte Anwendung, die auf Android Enterprise-Geräten installiert ist, unter Verwendung von Ivanti Neurons for MDMim Remoteverfahren löschen. Diese Aktion unterstützt die Behebung häufiger Probleme mit der App, z. B. langsame Leistung, unerwartete Fehler oder veraltete temporäre Daten, ohne die App zu deinstallieren oder neu zu installieren. Die Anfrage löscht lediglich den App-Cache. Benutzerdaten, App-Einstellungen und Konfigurationen werden beibehalten. Administratoren können mithilfe dieser Funktion das normale App-Verhalten schnell wiederherstellen und dabei Unterbrechungen für Endbenutzer auf ein Minimum reduzieren.

Verfahren

1. Wechseln Sie zu **Apps** > **App-Katalog**.
2. Wählen Sie die App aus und öffnen Sie sie.
   Die Seite **Details** der App wird angezeigt.
3. Klicken Sie auf das Aktionsmenü (**?**) der Seite **Details** der App.
4. Wählen Sie die Option **Anfrage zum Löschen des App-Caches** aus.
   Der Bereich **Anfrage zum Löschen des App-Caches** wird angezeigt.
5. Führen Sie eine der folgenden Aktionen im Abschnitt **Benutzer für Anfrageversand auswählen** aus, um die Anfrage zum Löschen des App-Caches zu verteilen:
   - Wählen Sie **Alle**, um die Anfrage an alle kompatiblen Geräte zu senden, auf denen die App installiert ist.
   - Wählen Sie **Benutzerdefiniert** aus, um die Anfrage an bestimmte Benutzer, Benutzergruppen, Geräte oder Gerätegruppen zu senden.
6. (Optional) Suchen Sie nach einer vorhandenen Verteilerliste unter **Andere Verteilerfilteroptionen**.

7. (Optional) Wählen Sie **+ Verteilungsfilter hinzufügen** aus, um einen Verteilungsfilter im Bereich **Verteilungsfilter erstellen** anzulegen.

Verwenden Sie diese Option, um die **Anfrage zum Löschen des App-Caches** an einen bestimmten Satz von Geräten zu senden, z. B. Geräte im DO- oder EPO-Modus.

8. Klicken Sie auf **Senden**.
9. Klicken Sie im Bestätigungsdialogfeld **App-Cache löschen** auf **OK**.
   Ivanti Neurons for MDM zeigt eine Benachrichtigung mit der Anzahl der Geräte an, die die **Anfrage zum Löschen des App-Caches** erhalten haben.

Nach Abschluss der Anforderung **App-Cache löschen** werden alle App-Details (version, name, platformAppId, displayVersion und bundleVersion) auf der Seite **Audit-Protokolle** protokolliert.

8.8. Zuweisen benutzerdefinierter Attribute zu Apps

Nachdem Sie benutzerdefinierte Attribute erstellt haben, können Sie sie einer oder mehreren Anwendungen zuweisen. Jedes Attribut hat einen entsprechenden Wert, den Sie für Aufgaben wie die Erstellung von Anwendungsgruppen verwenden können. Weitere Informationen zum Verwalten von Attributen finden Sie unter **Attribute**.

Erstellen und Zuweisen eines benutzerdefinierten Attributs für eine einzelne Anwendung

Sie können einer einzelnen Anwendung ein benutzerdefiniertes Attribut hinzufügen.

Verfahren

1. Melden Sie sich beim Administrationsportal an.
2. Wechseln Sie zu **Apps** > **App-Katalog**.
3. Wählen Sie eine Anwendung aus und klicken Sie auf **Attribute**.
4. Klicken Sie auf **+Neu hinzufügen** und wählen Sie einen Wert aus dem Dropdown-Menü **Attributname** aus.
5. Geben Sie im Feld **Wert** den Attributwert an.
6. Klicken Sie auf **Speichern**. Das benutzerdefinierte Attribut wird zur Anwendung hinzugefügt.

Zuweisen eines benutzerdefinierten Attributs zu mehreren Anwendungen

Sie können benutzerdefinierte Attribute einer oder mehreren Anwendungen zuweisen. Wenn Sie mehrere Anwendungen auswählen, wird das benutzerdefinierte Attribut auf jede Version der Anwendung angewendet. Sie können eine bestimmte Anwendung auswählen und dann auf der Registerkarte "Attribute" die Details des benutzerdefinierten Attributs für eine bestimmte Anwendungsversion ändern.

Verfahren

1. Melden Sie sich beim Administrationsportal an.
2. Wechseln Sie zu **Apps** > **App-Katalog**.
3. Markieren Sie die Kontrollkästchen für eine oder mehrere Anwendungen.
4. Klicken Sie auf **Aktionen**.
5. Wählen Sie **Benutzerdefinierte Attribute zuweisen** aus. Der Assistent zum Zuweisen benutzerdefinierter Attribute zu Apps wird angezeigt.
6. Wählen Sie *eine* der folgenden Optionen aus:
   - Zuweisung (Überschreiben) aller Attribute erzwingen, selbst wenn Werte vorhanden sind.
   - Nur überschreiben, wenn der Wert leer ist, Attribute mit vorhandenen Werten überspringen
7. Markieren Sie die Kontrollkästchen für ein oder mehrere Attribute.
8. Geben Sie den Wert in den betreffenden Wertfeldern an (Feld muss ausgefüllt werden).
9. Klicken Sie auf **Zuweisen**. Das benutzerdefinierte Attribut wird allen Versionen der ausgewählten Anwendungen zugewiesen.
10. (Optional) Wenn Sie das benutzerdefinierte Attribut für eine einzelne Anwendungsversion ändern möchten, wählen Sie die gewünschte Version aus der Dropdownliste für die Version aus und klicken Sie auf "Bearbeiten".

Mithilfe der **benutzerdefinierten App-Attribute** und ihrer Werte lassen sich über die Seite **Gerätedetails** Berichte erstellen und in das CSV-Format exportieren.

8.9. Verwaltete Konfigurationen für Android

Dieser Abschnitt enthält die folgenden Themen:

- Verwaltete Konfigurationen für Android Enterprise verwenden
- App-Beschränkungen und -Berechtigungen für interne Apps
- Gmail für Android Enterprise einrichten

Wenn für Ivanti Neurons for MDM Android Enterprise aktiviert ist, ist die Android Enterprise-Konfiguration für die Verwendung pro App verfügbar.

Verwaltete Konfigurationen für Android Enterprise verwenden

1. Klicken Sie auf **Apps**.
2. Klicken Sie auf **App-Katalog**.
3. Wählen Sie eine App aus, für die Sie die Konfiguration für Android Enterprise erstellen wollen.
4. Klicken Sie auf **App-Konfigurationen**.
5. Klicken Sie auf die Option **Verwaltete Konfigurationen für Android**.
6. Geben Sie einen Namen für die Konfiguration ein.
7. Geben Sie ggf. eine Beschreibung ein.
8. Konfigurieren Sie mit den Feldern für die verwalteten Konfigurationen das Verhalten verwalteter Konfigurationen:
9. Verwenden Sie die **Tunnel-Konfigurationseinstellungen**, um die Tunnel-App direkt in die Ivanti Go-App für Android-Geräte zu integrieren. Wählen Sie die Option **Tunnel-Konfiguration aktivieren**, um diese Einstellung anzuwenden. Mit dieser Verbesserung können Administratoren Tunnelfunktionen über Ivanti Go aktivieren und sichere Konnektivität mithilfe der vorhandenen Tunnelkonfigurationen einrichten. Die Funktion ist für neu registrierte Android-Geräte verfügbar. Um einen nahtlosen Übergang zu gewährleisten, wird die eigenständige Tunnel-App weiterhin unterstützt. Geräte, auf denen die eigenständige Tunnel-App installiert ist, zeigen jedoch nicht das integrierte Tunnel-Erlebnis in Ivanti Go an. Nachdem die eigenständige Tunnel-App entfernt wurde, wird die integrierte Tunnel-Funktionalität in der Go-App verfügbar. Es kann immer nur eine Tunnelkonfiguration gleichzeitig auf ein Gerät angewendet werden.

Einstellung	Beschreibung
Apps dürfen Widgets nicht profilübergreifend teilen	Aktivieren Sie diese Option, damit Apps Widgets nicht profilübergreifend teilen können, wenn die App nicht im Hintergrund installiert wird. Lassen Sie die Option deaktiviert, wenn vertrauenswürdige Apps, die im Profil von Android Enterprise installiert sind, Widgets auf dem Homescreen anzeigen dürfen, damit Benutzer Informationen abrufen können. ohne sich anzumelden.
Verhindert, dass der Benutzer die App deinstalliert	Aktivieren Sie die Option, um zu verhindern, dass der Benutzer die (öffentliche, private oder interne) App deinstalliert, nachdem Ivanti Neurons for MDM die App im Hintergrund installiert hat.
Mindestversionscode	Legen Sie einen Mindestversionscode für die App fest, um das Standard-Update-Verhalten zu überschreiben. Wenn der Versionscode der derzeit auf dem Gerät installierten App kleiner als der angegebene Mindestversionscode ist, wird die App sofort auf die neueste Version aktualisiert.
Automatischer Start bei der Installation	Wählen Sie diese Option, wenn Sie eine Anwendung nach der Installation automatisch starten möchten. Diese Funktion ist nur verfügbar, wenn die App neu auf dem Gerät installiert wird (nicht bei einem Versions-Update). Bei Arbeitsprofilen und Arbeitsprofilen auf firmeneigenen Geräten sollte die Go-App aktiv sein und sich im Vordergrund befinden. Aufgrund von Einschränkungen bei Android 10+ wird bei Arbeitsprofil und Arbeitsprofil auf firmeneigenen Geräten nur eine App automatisch gestartet, wenn der Benutzer mehrere Apps aktiviert.

10. Der Administrator kann steuern, welche App-Konfigurationsfelder an die Geräte gesendet werden und welche nicht. Im Allgemeinen werden bei der Push-Übertragung der Konfigurationen an die Geräte die Standardeinstellungen verwendet. Wählen Sie im Abschnitt "Verwaltete Konfigurationen" innerhalb der Einstellung **Via Push an das Gerät senden** die Option **Alle Einstellungen via Push senden** oder **Nur Einstellungen mit definierten Werten via Push senden** aus.

Verwaltete Domainkonfiguration

In jeder App-Konfiguration von Android Enterprise wird für jedes Textfeld die Schaltfläche "Zertifikat aktivieren" angezeigt. Wenn Sie darauf klicken, wird das Textfeld durch eine Dropdown-Liste mit Zertifikaten ersetzt. Nach der Konfiguration werden diese Zertifikate im Hintergrund ohne Benutzereingriff verwendet.

Ein vorhandenes zertifikatsaktiviertes Feld kann durch Klicken auf die gleiche Schaltfläche neben dem Feld in ein textaktiviertes Feld geändert werden. Ein textaktiviertes Feld, das in ein zertifikatsaktiviertes Feld geändert wurde, kann durch Klicken auf dieselbe Schaltfläche wieder in ein textaktiviertes Feld geändert werden. (Standard-Dropdown-Felder können nicht in Textfelder umgewandelt werden.)

> Wenn im Mandanten keine ID-Zertifikate konfiguriert sind und Sie mit der Schaltfläche „Zertifikat aktivieren“ von Text auf Dropdown umschalten, wird in der Dropdown-Liste nur die Option „Keine“ angezeigt.

Klicken Sie auf die Option **Berechtigungen verwalten**, um die Runtime-Berechtigungen für Anwendungen auszuwählen und zu konfigurieren, die API 23 oder höher und Android 6.0+ betreffen.

Zur Auswahl aufgelistet werden nur die gefährlichen Berechtigungen für die spezifische Anwendung. https://developer.android.com/guide/topics/permissions/requesting.html#perm-groupsDie komplette Liste gefährlicher Berechtigungen (beispielsweise zum Auslesen Ihrer Kontakte, zur Suche von Konten auf dem Gerät, zur Erfassung eines Anrufprotokolls usw.) finden Sie unter https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups.

11. Sie können jeder Berechtigung folgende Rechte zuordnen:
    - Die Berechtigungen werden nur übernommen, wenn die Anwendung Berechtigungen anfordert.
    - Die Berechtigungen werden nicht übernommen, wenn die Benutzer die Berechtigungen bereits akzeptiert oder verweigert haben.
    - Automatisch erteilen
    - Automatisch verweigern: Verwenden Sie diese Einstellung mit Vorsicht.
    - Standard/Global

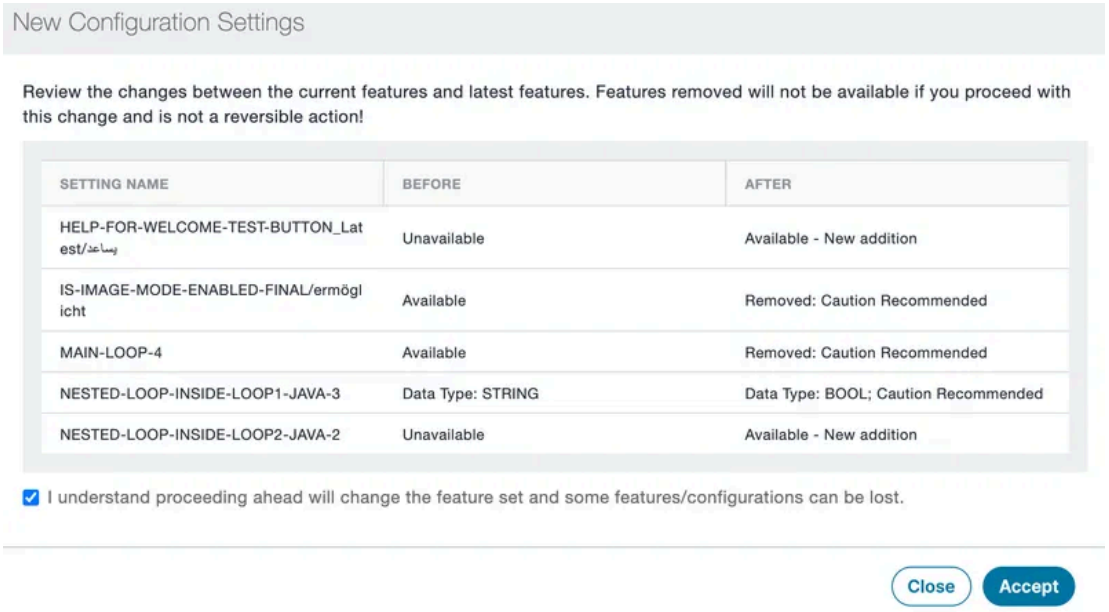
Konfigurieren Sie Verteilungsoptionen durch Auswahl von **Jeder mit App**, **Keiner** oder **Benutzerdefiniert**.

12. Klicken Sie auf **Speichern**.

Neue Konfigurationseinstellungen

Wenn eine App-Version aktualisiert wird und Änderungen an vorhandenen Konfigurationen vorhanden sind, wird nach dem Bearbeiten der Seite "Konfigurationsdetails" die Schaltfläche **Auf neueste Funktionen aktualisieren** angezeigt.

1. Klicken Sie auf **Auf neueste Funktionen aktualisieren**.
   Es wird eine Warnmeldung angezeigt, die darauf hinweist, dass Benutzer nach dem Aktualisieren auf die neuesten Funktionen keinen Zugriff mehr auf ältere Versionen der Anwendung haben werden. Die Warnmeldung beinhaltet Empfehlungen zum nahtlosen Integrieren der neuesten Version der Anwendung.
2. Klicken Sie auf **Weiter**.
3. Das Fenster **Neue Konfigurationseinstellungen** wird angezeigt.



Das Fenster **Neue Konfigurationseinstellungen** führt die Einstellungen auf, die in der Konfiguration vorhanden waren, sowie den Status jeder Einstellung nach dem Update. Das Fenster "Neue Konfigurationseinstellungen" führt alle Einschränkungen der Datenbank auf. Das Google-Schema gibt den folgenden Status an:

- Hinzugefügt
- Entfernt
- Geändert

Markieren Sie das Kontrollkästchen und klicken Sie auf **Annehmen**, um mit dem Update fortzufahren.
Eine Bestätigungsmeldung weist darauf hin, dass die Konfiguration erfolgreich mit den neuesten Funktionen aktualisiert wurde. Sie können die Konfigurationen jetzt verteilen und speichern, damit die Änderungen wirksam werden.

App-Beschränkungen und -Berechtigungen für interne Apps

Der Administrator kann einige App-Beschränkungen einrichten und Berechtigungen für interne Apps einräumen oder verweigern. Diese Funktionalität war nur für öffentliche Apps verfügbar. Diese Funktionalität wurde nun auf die internen Apps erweitert.

> Der Administrator muss die internen Apps erneut hochladen, um auf die Funktionen **App-Beschränkungen** und **-Berechtigungen** in den Apps verfügbar zu machen. Es wird empfohlen, die vorhandene App vor dem Hochladen einer neuen Version zu löschen.

Verfahren

1. Gehen Sie zu **Apps** > **App-Katalog**.
2. Wählen Sie eine **interne** App aus der Liste aus.
3. Klicken Sie auf **App-Konfigurationen**.
4. Klicken Sie auf **Verwaltete Konfigurationen für Android**.
5. Klicken Sie auf **[Add]**.
6. Der Abschnitt **App-Beschränkungen** wird auf dem Bildschirm angezeigt.
   Geben Sie die erforderlichen Werte für die verfügbaren Beschränkungen ein.
7. Wählen Sie **Berechtigungen verwalten**.
8. Das Fenster **Berechtigungen auswählen** wird auf dem Bildschirm angezeigt.
   Wählen Sie die erforderlichen Berechtigungen aus der Liste aus, und klicken Sie auf **Auswählen**.
9. Legen Sie im Abschnitt **Laufzeitberechtigungen** die Werte für die ausgewählten Berechtigungen fest.
10. Wählen Sie im Abschnitt **Diese App-Konfiguration verteilen** eine der folgenden Optionen für die **App-Verteilung** aus:
    - **Jeder mit der App**
    - **Keine/r**
    - **Anpassbar**
11. Klicken Sie auf **Speichern**.
    Die ausgewählten Beschränkungen und Berechtigungen werden auf die internen Apps angewendet.

Gmail für Android Enterprise einrichten

Sie können Gmail auf Geräten mit Android Enterprise bereitstellen, wenn Sie die Cloud für Android Enterprise eingerichtet haben.
Gmail für Android Enterprise einrichten

1. Gehen Sie zu **Apps > App-Katalog**.
2. Wählen Sie die Gmail-App aus, für die Sie Android Enterprise konfigurieren möchten. Der Abschnitt mit dem Konfigurationssetup wird angezeigt.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie ggf. eine Beschreibung ein.
5. Konfigurieren Sie mit den Feldern **Verwaltete Konfigurationen** das Verhalten verwalteter Konfigurationen:

Die Optionen **Alle erweitern** und **Alle ausblenden** sind nur für verschachtelte oder hierarchische Einschränkungen verfügbar.

Einstellung	Beschreibung
Via Push an das Gerät senden	Alle Einstellungen via Push senden – Wählen Sie diese Option aus, um alle Umschalter zu senden, auch solche ohne Werte. Nur Einstellungen mit definierten Werten via Push senden – Wählen Sie diese Option aus, um alle Umschalter mit definierten Werten zu senden und die Umschalter für Einstellungen ohne Werte zu deaktivieren. In vielen Fällen sind die Standardeinstellungen bereits verfügbar. Der Administrator hat jedoch die Möglichkeit, die erforderlichen App-Konfigurationseinstellungen auszuwählen oder die Variablen zu bearbeiten, die an die Geräte gesendet werden müssen.
E-Mail-Adresse	Geben Sie Ersatzvariablen zur Definition der E-Mail-Adresse ein. Normalerweise geben Sie $emailaddress$ ein$. UEMs können dieses Feld verwenden, um Benutzeranmeldeinformationen aus Active Directory zu holen.
Hostname oder Host	Geben Sie den Hostnamen für den Active Sync-Server ein, z. B. hostname.company.com:443/pfad.
Benutzername	Verwenden Sie die Variable für den Active Directory-Benutzernamen des Benutzers, der als direkter Benutzername (janaschmitt) oder als Wert in Form einer Schablone ($username$) angegeben werden kann.
Authentifizierungsarten	Wählen Sie die Liste der Zeichenfolgen, die die zulässigen Authentifizierungsarten enthalten.
SSL erforderlich	Wenn diese Option ausgewählt ist, aktiviert und erfordert SSL für die mit dem Hostnamen verwendeten Portnummern.
Allen Zertifikaten vertrauen	Wählen Sie die Option nur aus, wenn die App nicht vertrauenswürdige Zertifikate automatisch akzeptieren soll. Verwenden Sie diese Option nur zum Debuggen oder zur Entwicklung, wenn Sie in einer Testumgebung arbeiten.
Anmeldezertifikat-Alias	Geben Sie den Alias für das Anmeldezertifikat ein, das zur Authentifizierung bei ActiveSync-Servern verwendet wird.
Nicht verwaltete Konten zulassen	Wählen Sie diese Option, damit Benutzer ein anderes Exchange-Konto als das in dieser verwalteten Konfiguration angegebene Konto hinzufügen oder entfernen können.
Standard-E-Mail-Signatur	Geben Sie die Zeichenfolge der Standard-E-Mail-Signatur ein, die am Ende des gesamten ausgehenden E-Mail-Nachrichtentextes angehängt werden soll.
Standard-Synchronisationsfenster	Geben Sie als Zeitfenster für die Synchronisierung mit EAS (Exchange Active Sync) einen Wert von 0-5 ein.

Klicken Sie auf **Weiter**.

7. Konfigurieren Sie Verteilungsoptionen durch Auswahl von **Jeder mit App**, **Keiner** oder **Benutzerdefiniert**.

8. Klicken Sie auf **Speichern**.

8.10. Verwaltung von Google Play-Apps

Sie können festlegen, welche Binärdatei der Google App für bestimmte Gruppen oder Einzelpersonen bereitgestellt werden soll. Diese Bereitstellung gilt für Bereitstellungen mit Android für Unternehmen. Der App-Entwickler muss außerdem Ihr Unternehmen in die Whitelist eintragen, damit Apps im Alpha- oder Beta-Kanal bereitgestellt werden können.

1. Klicken Sie auf **Apps**.
2. Wählen Sie im **App-Katalog** eine App aus, für die Sie die Google Play-Freigabekonfiguration erstellen wollen.
3. Klicken Sie auf die Registerkarte **App-Konfigurationen.**
4. Klicken Sie auf **Google Play Release**.

> Die Konfiguration für Google Release wird nur für Apps unter Android Enterprise verwendet. Standardmäßig werden die Produktionsoptionen verwendet, wenn die Google Release-Konfiguration für neu ergänzte Apps nicht ausgewählt wurde.

Klicken Sie auf **[Add]**.

6. Geben Sie einen Namen für die Konfiguration ein.
7. Geben Sie ggf. eine Beschreibung ein.
8. Wählen Sie mit einer Option aus der Dropdown-Liste die Binärdatei für die Benutzer und Geräte, welche diese App erhalten. Die Optionen sind:
   - Produktion
   - Alpha
   - Beta

   > Die Produktionsoption wird standardmäßig für Apps übernommen, die bereits per Push auf das Gerät übertragen wurden.
9. Konfigurieren Sie Verteilungsoptionen durch Auswahl von **Jeder mit App**, **Keiner** oder **Benutzerdefiniert**.
10. **Benutzerdefiniert** verteilt die App innerhalb der Benutzergruppe entsprechend dem Gerätefilter.
    Klicken Sie auf **Speichern**.

Priorisierung mehrerer Freigabekonfigurationen

Wenn mehrere Google-Freigabekonfigurationen ergänzt werden, können Sie die Reihenfolge festlegen, in der die Google-Freigabekonfigurationen verwendet werden sollen.

1. Klicken Sie in **App-Konfigurationen** auf **Konfigurationen priorisieren**.

> Diese Schaltfläche wird nur angezeigt, wenn mehrere Konfigurationen aufgelistet sind.

Übernehmen Sie aus den aufgelisteten Konfigurationen per Drag&Drop die Konfiguration, die als erste in der Liste angewendet werden soll.

3. Klicken Sie auf **Aktualisieren**.

Wenn die erste eingestellte Konfiguration gelöscht ist, erhält die nächste Konfiguration in der Liste die höchste Priorität.

8.11. Löschen von Apps aus dem App-Katalog

Sie können öffentliche und hauseigene Apps aus dem App-Katalog löschen. Sie können vorausgesetzte Apps nicht löschen. Sie müssen die Apps bearbeiten und die als Voraussetzung definierten Beziehungen entfernen, wenn Sie solche Apps löschen wollen. Wenn eine App auf dem Gerät installiert ist, wird sie entfernt, wenn diese Geräte sich das nächste Mal anmelden,. Die Installation/Deinstallation im Hintergrund wird auf Samsung- und Zebra-Geräten im Geräteadmininistratormodus oder auf allen Geräten im Geräteeigentümermodus unterstützt.

Bei internen Apps wird ein Bestätigungsfenster im Bildschirm angezeigt. Sie müssen bestätigen, dass Sie den Löschvorgang fortsetzen möchten und anschließend auf **App löschen** klicken. Wenn Sie versuchen, mehrere Apps zu löschen und dies bei einigen Apps nicht gelingt, wird ein Fenster mit Hinweisen angezeigt. Diese geben Aufschluss darüber, welche Apps nicht gelöscht werden können und weshalb.

Folgendes gilt, wenn Sie versuchen, eine oder mehrere Apps aus dem App-Katalog zu löschen:

- Wenn eine Version der internen App nicht gelöscht werden kann, dann kann keine Version gelöscht werden.
- Falls es sich bei einer der Versionen der internen App um eine erforderliche App handelt, dann kann weder die App noch eine der Versionen gelöscht werden.
- Wenn Sie alle oder einige der internen Apps zum Löschen aus dem Katalog auswählen, werden alle Versionen der ausgewählten internen Apps gelöscht.
- Eine von einem Space delegierte interne App kann nicht gelöscht werden.

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Klicken Sie auf den Link für die App.
3. Klicken Sie auf **Aktionen > Aus Katalog löschen**.
4. Beachten Sie den Warnhinweis zu den Konsequenzen beim Löschen einer App.
5. Die Warnung weist darauf hin, dass auch Apps and Books-Lizenzen (iOS) und App-Rezensionen (alle Betriebssysteme) gelöscht werden.
   Markieren Sie das Kontrollkästchen "Die mit dem Löschen einer App verbundenen Folgen sind mir bekannt", um mit dem Löschvorgang fortzufahren.
6. Klicken Sie auf **Anwendung löschen**.

8.12. Upgrading von hauseigenen Apps

Verwenden Sie das folgende Verfahren, um eine unternehmensinterne App zu aktualisieren:

1. Gehen Sie zu **Apps > App-Katalog**.
2. Wählen Sie die App aus, die aktualisiert werden soll.
3. Klicken Sie auf **Aktionen > Neue Version hinzufügen**.
4. Laden Sie per Drag and Drop die App in dem Bereich **App hochladen** oder klicken Sie auf **Datei auswählen**, um die App in Ihrem Dateisystem auszuwählen.
5. Klicken Sie auf eine der folgenden Optionen, je nachdem, wie Sie mit der Vorversion der App verfahren wollen:
   - **Beschreibung, Screenshots, Verteilung, App-Voraussetzungen und App-Konfigurationen unverändert übernehmen:** Ersetzt die vorherige Version im App-Katalog.
   - **Beschreibung, Screenshots, Verteilung, App-Voraussetzungen oder App-Konfigurationen ändern**: Enthält beide Versionen im App-Katalog.
6. Geben Sie unter **Was ist neu** Text ein, der den Benutzern erläutert, was in der neuen Version anders ist.
7. Dieser Text wird auf dem Gerät angezeigt, wenn der Benutzer die App für die Installation auswählt.
   Wenn Sie Beschreibungen, Screenshots oder Verteiloptionen ändern wollen, müssen Sie diese Änderungen abschließen.
8. Klicken Sie auf **Fertig**.

Wenn Sie ältere Versionen der App im Katalog behalten wollen, wird unter **Apps > App-Katalog** nur ein Eintrag angezeigt. Das Feld ganz links zeigt die Anzahl der Apps an, für die der Eintrag gilt. Wenn Sie später die neuere Version löschen wollen, wird diese Installation auf den Geräten automatisch durch die ältere Version ersetzt.

Anzeige einer Liste der App-Versionen

Administratoren dürfen Apps mit der gleichen Version und unterschiedlichen Architekturen hochladen.

ProcedureVerfahren

1. Klicken Sie auf den Link für die App unter **Apps > App-Katalog**.
2. Klicken Sie auf die Registerkarte Version.
   Wenn mehrere Versionen der App im Katalog vorhanden sind, werden die Versionen in einer Dropdown-Liste angezeigt. Wenn mehrere Anwendungen mit der gleichen Versionsnummer, aber unterschiedlichen Architekturen hochgeladen werden, zeigt das Dropdown-Menü die unterstützten Architekturdetails an. Die für die Apps unterstützten Architekturen werden auch unter **App-Informationen** angezeigt.

8.13. Suche des Paketnamens für eine Android App

Für öffentliche Apps, die auf dem Google Play Store verfügbar sind:

1. Verwenden Sie einen Web-Browser, um die App im Google Play Store zu finden.
2. Wählen Sie die App aus.
3. Untersuchen Sie die URL, die im Browser angezeigt wird.

Der Paketname steht in der URL nach id= wie in dem folgenden Beispiel:

https://play.google.com/store/apps/details?id=<package name>

Versuchen Sie für unternehmensinterne Apps und andere Apps, die nicht im Play Store verfügbar sind, **Package Name Viewer** oder eine ähnliche App aus dem Google Play Store herunterzuladen.

8.14. Kategorien

Dieser Abschnitt enthält die folgenden Themen:

- Kategorie hinzufügen
- Kategorie entfernen

Kategorien beschreiben die App-Arten und helfen bei der Organisation von Apps, wenn Benutzer den App-Katalog durchblättern.Jeder App muss mindestens eine Kategorie zugewiesen sein. Eine Liste häufiger App-Kategorien wird Ihnen bei der ersten Arbeit mit der Cloud angeboten. Nutzen Sie diese Seite zur Verwaltung der App-Kategorien.

Kategorie hinzufügen

Neue Kategorien können Sie entweder hier hinzufügen oder wenn Sie eine App im App-Katalog hinzufügen.

1. Klicken Sie auf Hinzufügen (unten links).
2. Geben Sie den Kategorienamen ein.
3. Bei Kategorien muss Groß- und Kleinschreibung nicht beachtet werden, d. h., „MEINE“ und „Meine“ unterscheiden sich nicht. Klicken Sie auf **Speichern**.

Kategorie entfernen

- Klicken Sie auf das X neben der Kategorie.

Wenn Sie keine Aufgaben auf der Seite **App-Kategorien** ausführen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie benötigen eine der folgenden Rollen:

- Verwaltung von Apps und Inhalten

8.15. Verteilungsfilter

Dieser Abschnitt enthält die folgenden Themen:

- Verteilungsfilter konfigurieren
- Verteilungsfilter für den delegierten Administrator konfigurieren

Begrenzen Sie mit Verteilungsfiltern die Zahl der Apps, die installiert werden können. Verteilungsfiltern begrenzen die im App-Katalog angezeigten Apps auf die Apps, die für das Gerät geeignet sind.

Lizenz: Silver

Diese Filter sind standardmäßig verfügbar:

- **Apps für Android Enterprise** - begrenzt die App-Verteilung auf Geräte, bei denen Android Enterprise aktiviert ist.
- **Nur iPad-Apps** - begrenzt die App-Verteilung auf iPad-Geräte.
- **Nur iPhone-Apps** - begrenzt die App-Verteilung auf iPhone-Geräte.

Verteilungsfilter konfigurieren

1. Gehen Sie zu **Apps > Verteilungsfilter**.
   Die Standard-App-Filter und erstellte App-Filter werden hier aufgelistet.
2. Klicken Sie auf **+Hinzufügen**, um den Dialog **Verteilungsfilter erstellen** aufzurufen.
3. Geben Sie einen Namen und eine Beschreibung in den entsprechenden Feldern ein.
4. Wählen Sie Regeldefinitionen aus. Diese Regeln können mit den entsprechenden Operatoren erstellt werden, einschließlich der Operatoren „enthält“, „ist kleiner als“, „ist größer als“, „ist im Bereich“, „ist gleich“ und „ist nicht gleich“. Die Regeln können miteinander mit den Optionen ANY (OR) oder ALL (AND) verschachtelt werden. Es gibt folgende App-Verteilungsfilter:
   - Von Access blockiert
   - APNS-fähig
   - Verwaltetes Android-Gerät mit Arbeitsprofil
   - Android Enterprise aktiviert
   - Android Sicherheits-Patchlevel (für Android-Geräte)
   - In Android Enterprise verwaltete Geräte aktiviert (Geräteeigentümer)
   - Android-Arbeitsprofil auf unternehmenseigenen Geräten aktiviert
   - Letzter Check-in durch Client
   - Client registriert
   - Compliance
   - Von Compliance-Aktion blockiert
   - Aktueller Ländername
   - Aktueller MCC-Code
   - Aktueller MNC-Code
   - Kundenspezifisches Geräteattribut
   - Benutzerdefiniertes LDAP-Attribut

- Kundenspezifisches Benutzerattribut
- Benutzerdefiniertes IDP-Attribut
- Gerätetyp
- Heimatlandname
- Eigener MCC-Code
- Eigener MNC-Code
- IMEI
- IMEI2 (nur auf Android-Geräten mit dualem SIM-Port und ab Version 8.0)
- Kiosk-Modus
- Hersteller
- Betriebssystemversion
- Verantwortung
- Telefonnr.
- Roaming
- Secure Apps Status
- Überwacht
- Von Sentry blockiert
- User Enrollment Registriert
- Automatische Geräteregistrierung eingereicht
- Automatische Geräteregistrierung aktiviert

5. Klicken Sie auf **Verteilungsfilter erstellen**.
6. Wählen Sie bei Bedarf einen benutzerspezifischen Filter für die Aktualisierung aus.
    1. Klicken Sie auf **Bearbeiten**, um die Seite **Verteilungsfilter aktualisieren** anzuzeigen.
    2. Geben Sie einen Namen und eine Beschreibung in den entsprechenden Feldern ein.
    3. Definieren Sie die Regeln für den Filter über die Pulldown-Menüs.
    4. Klicken Sie auf **Verteilungsfilter aktualisieren**.
7. Wählen Sie eine App aus.
8. Wählen Sie auf der Seite mit den App-Details die Registerkarte **Verteilung** aus.
9. Klicken Sie auf **Bearbeiten**.
10. Wählen Sie eine App-Verteilungsoption aus:
    - **Jeder**
    - **Keiner**
    - **Anpassbar**

    > Der Bereich für den Verteilungsfilter ist nur sichtbar, wenn für die Verteilung die Option Jeder bzw. Benutzerdefiniert ausgewählt ist.

11. Wählen Sie eine Verteilungsfilteroption:

1. Geben Sie einen Filternamen in das Feld Suche nach den vorhandenen Verteilungsfiltern ein, um einen bereits erstellten Filter zu finden.
2. Klicken Sie auf die Option **+Verteilungsfilter hinzufügen**, um einen neuen Filter zu ergänzen.

Sie können Verteilungsfilter für eine App erstellen oder zuweisen, bevor diese im Katalog ergänzt wird. Änderungen an den Verteilungsfiltern beeinflussen die Verteilung der Apps, die diesen Filter verwenden (in allen Spaces).

Wenn der Filter eingestellt und **App-Installation auf M1-Geräten bei Verteilung zulassen** aktiviert ist, werden macOS-M1-Geräte eingetragen. Die iOS-VPP-App ist für alle Mac-Geräte verfügbar, wenn **App-Installation auf M1-Geräten bei Verteilung zulassen** aktiviert ist und der Verteilungsfilter entweder **Jeder** oder **Benutzerdefiniert** lautet. Verteilungsfilter für macOS-bezogene Attribute werden nicht für iOS-Apps unterstützt.

Verteilungsfilter für den delegierten Administrator konfigurieren

Der delegierte Administrator kann erstellte Filter verwalten und bearbeiten, die bei der Verteilung in dem delegierten Space einzelnen Apps hinzugefügt wurden. Der delegierte Administrator kann Verteilungsfilter, die im Standard-Space erstellt wurden, nicht in anderen Spaces verwenden, sondern nur für delegierte Apps.

Delegierte Administratoren können Verteilungsfilter in dem spezifischen Space erstellen, verwalten und bearbeiten, auf die sie Zugriff haben. Der Verteilungsfilter ist nur für den Space verfügbar, für den er erstellt wurde. App-Verteilungsfilter können nicht delegiert werden.

Wenn ein delegierter Administrator mit Rechten zur App- und Systemverwaltung eine App mit einem Verteilungsfilter in einem delegierten Space ergänzt, kann er die Gerätedetails für die Geräte in seinem Space und für die Geräte in anderen Spaces sehen.

Benutzer mit Rechten zur Systemverwaltung bzw. zum Lesen der Systemeinstellungen können in Spaces keine Verteilungsfilter erstellen, aktualisieren oder löschen.

Der delegierte Administrator mit Rechten zur App- und Content-Verwaltung hat möglicherweise keinen Zugriff auf den Verteilungsfilter. Aus diesem Grunde können Sie Folgendes nicht tun:

- Apps mit Verteilungsfiltern erstellen. Dies ist der Fall, wenn Sie als delegierter Administrator angemeldet sind und eine App hinzufügen.
- Ein delegierter Administrator mit Systemleserechten oder höheren Rechten kann Apps mit Verteilungsfilter hinzufügen. Ein delegierter Administrator ohne Systemverwaltungsrechte kann Apps ohne Verteilungsfilter hinzufügen.

Der delegierte Administrator kann den Delegationsstatus im App-Katalog durch Auswahl folgender Optionen filtern:

- Delegiert
- Nicht delegiert

8.16. Ausschließen oder Verteilen von Apps

Schließen Sie verwaltete Apps von einem Gerät aus oder verteilen Sie verwaltete Apps, ohne die Konfiguration für die App-Verteilung zu ändern, für interne und öffentliche Apps auf iOS-, macOS- und Windows-Geräten. Bei allen verwalteten Apps befinden sich diese Optionen für alle Geräte in der Spalte **Aktionen** im Abschnitt **Verfügbare Apps**.

Berechtigungen

Sie benötigen folgende Berechtigungen, um eine Anwendung von einem Gerät auszuschließen bzw. an ein Gerät zu verteilen:

- Gerätezugriff im Space (Partition)
- Zugriff auf verfügbare Apps für das Gerät

Ausschließen

Mit der Option "Ausschließen" für eine ausgewählte App wird die App deinstalliert und die zugehörigen Daten werden vom Gerät entfernt. Gehen Sie folgendermaßen vor, um eine erforderliche App auszuschließen: Eine Popup-Benachrichtigung weist darauf hin, dass Sie im Begriff sind, eine erforderliche App auszuschließen und dass dies dazu führt, dass die Haupt-App auf dem Gerät ausgeschlossen wird.

Wenn Sie interne Apps mit mehreren Versionen ausschließen, werden auch alle nicht verteilten App-Versionen auf dem Gerät ausgeschlossen. Wenn Sie eine App vom Gerät ausschließen, wird sie in Apps@Work und Ivanti Go gelöscht. Wenn Sie eine App ausschließen und aus dem App-Katalog löschen und dann erneut hinzufügen, ist die App für das Gerät nicht mehr ausgeschlossen. Wenn Sie eine App vom Gerät ausschließen, wird sie normalerweise unter **Geräte** > **Geräte** > **Verfügbare Apps** angezeigt. Der Administrator kann sie somit nach dem Ausschließen direkt an das Gerät verteilen.

Verteilen

Löst der Administrator den Befehl **Installation senden** über die App aus, wird die App erst installiert, wenn der Administrator sie über die **verfügbaren Apps** des Geräts verteilt. Es wird eine Ausschlussmeldung für diejenigen Geräte angezeigt, die die App nicht empfangen. Wenn der Administrator eine verfügbare Anwendung verteilt, wird sie bei der nächsten Synchronisierung auf dem Gerät installiert.

8.17. Rezensionen

Dieser Abschnitt enthält die folgenden Themen:

- Bewertungen und Rezensionen anzeigen
- Bewertungen und Rezensionen deaktivieren
- Rezension löschen
- Exportieren von Rezensionen in eine CSV-Datei

Rezensionen sind Anmerkungen und Bewertungen (Sterne), die ihre Benutzer für Apps im App-Katalog vergeben.Rezensionen bieten wertvolle Informationen für Sie und Benutzer, die die Installation einer App in Betracht ziehen. Verwenden Sie die Seite Rezensionen zum Anzeigen bzw. Löschen von Bewertungen und Rezensionen. Eine Rezension oder Bewertung kann gelöscht werden, wenn sie alt oder unzutreffend ist.

- Nur Benutzer von Geräten können Bewertungen und Rezensionen von Apps erstellen oder bearbeiten.
- Benutzer von Geräten können ihre eigenen Bewertungen und Rezensionen bearbeiten, aber nicht löschen.
- Nur die Administratoren können Rezensionen von Apps löschen.
- Bewertungen von Apps können nicht gelöscht werden. Bewertungen (Sterne) von Apps bleiben auf der Seite Apps > App-Katalog selbst wenn die Bewertungs- und Rezensions-Funktion für Ihre Benutzer zu einem späteren Zeitpunkt deaktiviert wird.

Bewertungen und Rezensionen anzeigen

- Gehen Sie zu Apps > Rezensionen, um vollständige Benutzerkommentare und Bewertungen (Sterne) für von Ihnen verteilte Apps anzuzeigen.
- Gehen Sie zu **Apps > App Catalog**, um die Spalte mit den **Durchschn. Bewertungen** für alle Rezensionen und die durchschnittliche Bewertung anzuzeigen.
- Gehen Sie zu Apps > App-Katalog, klicken Sie auf den Namen der App, um die Registerkarte Rezensionen mit den Bewertungen und Rezensionen für eine bestimmte App anzuzeigen.

Bewertungen und Rezensionen deaktivieren

1. Gehen Sie zu **Apps > Katalogeinstellungen**.
2. Deaktivieren Sie Aktivierung von Bewertungen und Rezensionen im Endbenutzer-App-Katalog.
3. Klicken Sie auf **Speichern**.

Rezension löschen

1. Gehen Sie zu **Apps > Rezensionen**.
2. Wählen Sie die Rezension aus.
3. Klicken Sie auf die Schaltfläche Aktionen oben rechts auf der Seite.
4. Wählen Sie **Löschen**.
5. Klicken Sie im **Rezension löschen** Bestätigungsdialog auf **Ja**.

Wenn Sie keine Aufgaben auf der Seite **Reviews** ausführen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie benötigen eine der folgenden Rollen:

- Verwaltung von Apps und Inhalten

Exportieren von Rezensionen in eine CSV-Datei

Sie können App-Rezensionen mithilfe der Option **Nach CSV exportieren** der Seite **Rezensionen** exportieren.

Verfahren

1. Gehen Sie zu **Apps > Rezensionen**.
2. Klicken Sie auf die Option **Nach CSV exportieren**, um die Liste der Rezensionen und die zugehörigen Details in eine CSV-Datei zu exportieren.
3. Es wird eine Popup-Meldung mit den Schaltflächen **Weiter** und **Abbrechen** angezeigt, die darauf hinweist, dass der Exportvorgang begonnen hat und in Kürze ein Bericht verfügbar sein wird.
4. Klicken Sie auf **Weiter** und warten Sie, bis die Anforderung abgeschlossen ist, bevor Sie eine weitere Anforderung übermitteln.
5. Eine Meldung zeigt **App-Rezensionen – CSV-Bericht fertiggestellt** sowie die Schaltflächen **Herunterladen** und **Löschen** an.
6. Klicken Sie auf **Herunterladen**, um den Bericht herunterzuladen.
7. (Optional) Klicken Sie zum Löschen des Berichts auf **Löschen**.

8.18. Apple Apps and Books

Dieser Abschnitt enthält die folgenden Themen:

- Lizenzen für Apps auf mehrere Apple Apps and Books-Konten in einem Space verteilen
- Geräte- und Benutzerlizenzverteilung
- Option für Gerätelizenzen verwenden
- Option für Benutzerlizenzen verwenden
- Apps and Books-App im Katalog hinzufügen
- Apps and Books-Konten hinzufügen
- Sichere Token für Apps and Books aktualisieren
- Priorität eines Apps and Books-Kontos aktualisieren
- Sicheres Token für Apps and Books löschen
- Lizenzen für eine Apps and Books-App im Katalog verteilen
- App-Lizenzen pro Benutzer anzeigen
- Benachrichtigungen über Lizenznutzungsbeschränkungen für Apps and Books
- Lizenznutzung für Apps and Books ansehen
- Apps and Books-Lizenz für eine App widerrufen
- Apps und Books-Verhalten für macOS- und iOS-Geräte
- Lizenzberechtigung für Apps and Books, wenn ein Gerät in Spaces verschoben wird.

Lizenz: Silver

Der Bildschirm **Apple Apps and Books** ist nur verfügbar, wenn Sie Apple Apps and Books in Ihren App-Katalogeinstellungen eingerichtet haben. Dieser Bildschirm zeigt an, welche App-Lizenzen für Apple-Geräte über Apple Apps and Books gekauft wurden und wie viele davon genutzt werden. Nutzen Sie diesen Bildschirm, um:

- die Apps and Books-Apps auszuwählen, die in Ihren Katalog aufgenommen werden sollen;
- Lizenzen für Apps and Books-Apps verteilen.

Weitere Informationen zum Verteilen von Apps mit Apps and Books finden Sie in der Ivanti Community im Artikel **Cloud: Anleitung zum Verteilen von Apps mit VPP**.

> Apple Books ist möglicherweise nicht in allen Ländern oder Regionen erhältlich. Um Lizenzen für Apps über Apps and Books von Apple zu verteilen, müssen Sie das von Apple bereitgestellte sToken eingeben.

Lizenzen für Apps auf mehrere Apple Apps and Books-Konten in einem Space verteilen

- Wenn die gleiche App in mehreren Apps and Books-Konten existiert, wird die Lizenz vom Konto entsprechend der Priorität der Konten verteilt.
- Wenn dieselbe App in mehreren Apps and Books-Konten vorhanden ist und die App-Lizenz in dem Apps and Books-Konto mit höherer Priorität erschöpft ist, erhält die App nur dann eine Lizenz vom nächsten priorisierten Konto, wenn der Benutzer oder das Gerät in der Lizenzverteilungsliste des nächsten priorisierten Kontos enthalten ist.

- Eine Lizenz wird nicht widerrufen und neu zugewiesen, wenn die Priorität der Apps and Books-Konten geändert wird. Die App würde eine Lizenz vom ersten Konto erhalten. Wenn die Lizenzen des ersten Kontos erschöpft sind, erhält die App eine Lizenz des Kontos mit der nächstniedrigeren Priorität usw.
- Ein Benutzer kann alle Lizenzen einer App auf der Seite des App-Katalogs widerrufen. Diese Aktion würde die Lizenz dieser App allen verfügbaren Apps and Books-Konten entziehen.
- Reservierte Lizenzen haben Vorrang vor der Priorität der Apps and Books-Konten.

Geräte- und Benutzerlizenzverteilung

Ob die Lizenz für eine App eine Gerätelizenz oder eine Benutzerlizenz ist, hängt von der Vergabe ab. Wenn Sie eine App-Lizenz für ein Gerät vergeben, wird sie zu einer Gerätelizenz. Wenn Sie eine App-Lizenz an einen Benutzer vergeben, wird sie zu einer Benutzerlizenz.

Es wird eine Lizenz verteilt, wenn die App "Apps and Books" auf einem Gerät installiert wird oder wenn ein Token für diese App generiert wird. Wenn keine Lizenzen für die App verfügbar sind, kann der Benutzer die App selbst installieren und bezahlen. Wenn ein Benutzer bereits eine Benutzerlizenz für eine angeforderte Apps and Books-App erhalten hat, wird die App mit der vorhandenen Benutzerlizenz und nicht mit der Apps and Books-Lizenz installiert.

> Bei **gemeinsam genutzten iPads**werden Apps and Books als Gerätelizenzen installiert, unabhängig davon, ob die Option für Gerätelizenzen ausgewählt wurde.

Option für Gerätelizenzen verwenden

Bei Gerätelizenzen müssen sich die Benutzer nicht bei Apps and Books registrieren. Die benötigten Apps werden automatisch installiert. Vom Unternehmen verwaltete Geräte benötigen keine Apple-ID für die IT-Abteilung.

Bei der Geräteanmeldung wird das Gerät anhand der Seriennummer identifiziert und die benötigte App installiert, wenn die Lizenzen verfügbar sind. Wenn keine Lizenzen verfügbar sind, wird die App nicht installiert. Wenn eine Lizenz für eine App reserviert ist, erfolgt bei der App-Installation keine Gerätelizenzzuordnung.

> App-Aktualisierungen für Apps, die mit der Gerätelizenz für Apps and Books bereitgestellt werden, werden vom Administrator kontrolliert.

Um zu kontrollieren, wie eine App aktualisiert wird, navigieren Sie unter **Apps > App-Katalog** zu der Registerkarte **App-Konfigurationen/Auf Gerät installieren**. Sie können auswählen, ob die Aktualisierung sofort bei der nächsten Anmeldung des Geräts erfolgen soll oder ob die App automatisch aktualisiert werden soll, sobald neue Versionen verfügbar sind.

Wichtig: Bevor Sie eine Gerätelizenz einer Business-to-Business- (B2B) oder Produktivitäts-App zuordnen, müssen Sie überprüfen, ob die App zur Gerätelizenzierung vom App-Entwickler freigegeben ist.

Option für Benutzerlizenzen verwenden

Eine Benutzerlizenz bleibt für einen Benutzer auch dann gültig, wenn sie von einem Gerät auf ein anderes Gerät übernommen wird, weil das alte Gerät verloren gegangen ist oder gestohlen wurde oder der Benutzer ein neues Gerät erwirbt. Bei Benutzerlizenzen muss sich der Benutzer zunächst bei Apple Apps and Books registrieren. Die Registrierung erfolgt manuell durch den Endbenutzer, der die Registrierung im App-Katalog ausfüllt. Obligatorische Apps and Books-Apps werden erst auf dem Gerät installiert, wenn der Benutzer sich bei Apps and Books anmeldet.

Wenn eine App eine obligatorische Apps and Books-App ist und die Lizenzvergabe als Benutzerlizenz erfolgt:

- Wird die benötigte App erst installiert, wenn der Benutzer sich für das Apps and Books-Programm registriert hat.
- Benötigte Apps können installiert werden, wenn der Benutzer sich für das Apps and Books-Programm registriert hat und eine Lizenz frei ist.
- Wenn der Benutzer sich für das Apps and Books-Programm registriert hat, aber keine Lizenzen frei sind, wird die App nicht installiert.

Apps and Books-App im Katalog hinzufügen

Verfahren

1. Gehen Sie zu **Apps > App-Katalog**.
2. Wählen Sie eine App aus und klicken Sie auf **Zum Katalog hinzufügen**. Klicken Sie auf **Weiter**.
3. Sie können optional eine Beschreibung der App ergänzen . Klicken Sie auf **Weiter**.
4. Wählen Sie eine Verteilungsoption aus. Klicken Sie auf **Weiter**.
5. Klicken Sie auf die Registerkarte **App-Konfiguration**.
6. Sie können auch **Auf Gerät installieren** auswählen. Diese Konfigurationsoption installiert die App auf überwachten iOS-Geräten im Hintergrund unabhängig vom Benutzer.
7. Wählen Sie gegebenenfalls weitere Konfigurationsoptionen aus.

Auf der Info-Seite für sichere Token von Apps and Books werden die folgenden Token-Details angezeigt:

- Erstellungsdatum
- Standort (wenn das Token diese Informationen enthält)
- Verfallsdatum

Apps and Books-Konten hinzufügen

Ivanti Neurons for MDM ermöglicht es, mehrere Apps and Books-Konten durch das Hinzufügen mehrerer sicherer Token für Apps and Books in einem einzigen Space zu ergänzen.

Führen Sie die folgenden Schritte aus, um ein sicheres Token für Apps and Books in einem Space hinzuzufügen:

1. Gehen Sie zu **Apps > Apple Apps and Books**.
2. Klicken Sie auf **Apps and Books sToken hinzufügen**.
3. Geben Sie einen Namen ein und wählen Sie eine Token-Datei aus.
4. Deaktivieren Sie bei Bedarf die Option **Apps and Books automatisch an alle Benutzer** verteilen. Diese Option ist standardmäßig ausgewählt. In diesem Fall wird die Gruppe „Alle Benutzer“ zum Verteilen der FCFS-Lizenzen verwendet.
5. Wählen Sie optional die Option **Alle Daten aus früheren Apps and Books-Lizenzen** löschen, um alle mit diesem Token verknüpften App-Lizenzen zu entfernen.
6. Klicken Sie auf **Speichern**.

Sobald das Konto hinzugefügt wurde, wird in der Tabelle eine Liste aller hinzugefügten Apps and Books-Konten angezeigt.

Sichere Token für Apps and Books aktualisieren

Verfahren

1. Gehen Sie zu **Apps > Apple Apps and Books**.
2. Klicken Sie auf den Namen des Apps and Books-Kontos.
3. Klicken Sie auf der Registerkarte Token auf **SToken aktualisieren** (.stoken-Datei).
4. Geben Sie den Token-Namen ein und wählen Sie eine Token-Datei aus.
5. Deaktivieren Sie bei Bedarf die Option **Apps and Books automatisch an alle Benutzer** verteilen. Diese Option ist standardmäßig ausgewählt. In diesem Fall wird die Gruppe „Alle Benutzer“ zum Verteilen der FCFS-Lizenzen verwendet.
6. Wählen Sie optional die Option **Alle Daten aus früheren Apps and Books-Lizenzen** löschen, um alle mit diesem Token verknüpften App-Lizenzen zu entfernen.
7. Klicken Sie auf **Aktualisieren**.

Klicken Sie auf der Registerkarte „Token“ auf **Apps and Books-Lizenznutzungsinformationen für Apps and Books neu synchronisieren**, um eine vollständige Synchronisierung aller App- und Lizenzinformationen des Apple Apps and Books Service durchzuführen. Diese Aktion ist nur notwendig, wenn die Informationen zur Lizenzzuordnung in der Ivanti Neurons for MDM nicht korrekt sind. Diese Ungenauigkeit kann aufgrund von Inkonsistenzen in den Apple APIs für Apps and Books auftreten.

Priorität eines Apps and Books-Kontos aktualisieren

Administratoren können jedem Apps and Books-Konto in einem Space eine Priorität zuweisen, je nachdem, welche Lizenzen verbraucht werden sollen. Mit Prioritäten der Apps and Books-Konten lässt sich die Lizenzverteilung planen und es können Konflikte gelöst werden, wenn ein Benutzer oder ein Gerät eine Lizenz von mehreren Apps and Books-Konten für die gleiche App erhalten darf.

Verfahren

1. Gehen Sie zu **Apps > Apple Apps and Books**.
2. Klicken Sie bei dem gewünschten Apps and Books-Konto auf **Priorität bearbeiten**.
3. Wählen Sie im Fenster „Priorität bearbeiten“ eine neue Priorität aus.
4. Klicken Sie auf **Speichern**.

Sicheres Token für Apps and Books löschen

Die Entfernung eines sicheren Apps and Books-Tokens ist irreversibel und zerstörerisch. Wenn ein Token entfernt wird, gilt:

- Bei Apps mit reservierten Tokens werden die Tokens entfernt.
- Apps, die bezahlt wurden, bleiben im Katalog, die Benutzer können diese auf eigene Rechnung kaufen.
- Apps, die von Endbenutzern über dieses Firmen-Konto für Apps and Books installiert wurden, müssen die Benutzer in ihre Privatkonten übernehmen, wenn sie diese verwenden wollen. Benutzer erhalten dafür eine 30-tägige Nachfrist.

Verfahren

1. Gehen Sie zu **Apps > Apple Apps and Books**.
2. Klicken Sie auf den Namen des Apps and Books-Kontos.
3. Klicken Sie auf der Registerkarte „Token“ auf **Löschen**.
4. Wählen Sie zur Bestätigung im Fenster „Sicheres Token für Apps and Books löschen“ die Option **Ja, das sichere Token für Apps and Books löschen** aus.
5. Klicken Sie auf **Löschen**.

Lizenzen für eine Apps and Books-App im Katalog verteilen

1. Wählen **Sie Apps > Apple Apps and Books** aus dem Hauptmenü.
2. Eine Liste der Apps and Books-Konten wird angezeigt. Für jedes Konto wird eine Liste der über das Programm Apps and Books gekauften Apps angezeigt.
   Wählen Sie eine App aus und klicken Sie auf **Lizenzen verteilen.**
3. Wählen Sie in dem Abschnitt für die Apps and Books-Lizenzen eine Verteilungsoption, d. h. entweder **First-come, first-served**, **Reserviert** oder **Nicht erlaubt**.

App-Lizenzen pro Benutzer anzeigen

Sie können die Lizenzpräferenz für Ihre Benutzer auf der Registerkarte „Lizenznutzung“ festlegen.

1. Klicken Sie auf die Registerkarte **Benutzer**
2. Wählen Sie einen Benutzer aus.
3. Klicken Sie auf die Registerkarte **Lizenznutzung**.
   Es wird eine App-Liste mit der Lizenzart für Apps and Books und den Lizenzzuordnungsdetails angezeigt.

So zeigen Sie die Lizenznutzung für jede App und jeden Benutzer an:

1. Wechseln Sie im Hauptmenü von Ivanti Neurons for MDM zu **Benutzer**.
2. Wählen Sie einen Benutzer aus.
3. Die Registerkarte **Geräte** wird standardmäßig angezeigt.
   Klicken Sie auf die Registerkarte **Lizenznutzung**.
   Es wird eine Liste aller auf dem Benutzergerät installierten Apps einschließlich Lizenzstatus angezeigt. Die Seriennummer des Geräts wird in der Spalte „Apps and Books Lizenztyp“ für Gerätelizenzen angezeigt.
   - App-Name
   - Version der App
   - Kosten der App
   - Datum der App-Zuweisung
   - Lizenzart für Apps and Books
   - Aktionen (Lizenzstatus)
   - Plattforminformationen für Lizenzdetails.

Sie können die Nutzung von Apps and Books-Lizenzen für jede App auch wie folgt anzeigen:

1. Wechseln Sie im Hauptmenü von Ivanti Neurons for MDM zu **App > App-Katalog**.
2. Wählen Sie eine App aus.
3. Klicken Sie auf die Registerkarte **Apps and Books Licenses**, falls vorhanden.
4. Klicken Sie auf einen Kontonamen. In dieser Registerkarte werden nur Apps angezeigt, die über das Programm Apps and Books gekauft wurden.

Für jede Apps and Books-Lizenzart wird eine separate Registerkarte angezeigt.

Lizenzart und Protokoll	Beschreibung
Wer zuerst kommt, malt zuerst (FCFS) - Sie können auswählen, welche Benutzergruppen diesen Lizenztyp erhalten.	• Vom Benutzer angeforderte Apps - Apps, die der Benutzer für die Installation ausgewählt hat. Die Standardeinstellung ist Benutzerlizenz. • Erforderliche Apps – Apps, die benötigt werden und durch die Administratorkonfiguration mit der Einstellung **Auf Gerät installieren** installiert werden. Für diese Apps werden standardmäßig Gerätelizenzen verwendet.
Reserviert	Reservierte Lizenzen haben Priorität vor Lizenzen nach dem Prinzip "Wer zuerst kommt, malt zuerst". Hier können Sie die Benutzer oder Geräte auswählen, die eine reservierte Lizenz für die App erhalten sollen.
Nicht erlaubt	Geben Sie die Benutzer ein, die keine Lizenz für diese App erhalten sollen. Der Benutzer kann die App trotzdem installieren, muss die Lizenz jedoch kaufen.
Aktivitätsprotokoll	Zeigt den Benutzer, die Lizenzart der zugewiesenen Apps and Books, das Datum der Zuweisung und die letzte Aktion für die Lizenz.

So zeigen Sie die detaillierte Lizenznutzung für jede App pro Gerät an:

1. Wechseln Sie im Hauptmenü von Ivanti Neurons for MDM zu **Geräte**.
2. Wählen Sie ein Gerät.
3. Klicken Sie auf die Registerkarte **Installierte Apps.**
4. Eine Liste aller auf dem ausgewählten Gerät verwalteten Apps wird mit dem Lizenzstatus angezeigt.
    - App-Name
    - Version der App
    - Unterstützte Plattformen
    - Quelle der App
    - Größe der App
    - Lizenzart für Apps and Books
    - Datum der für iOS-Apps gemeldeten (installierten) App

Durchsuchen Sie die installierten Apps wie folgt nach dem Gerät:

- App-Name
- Bundle-ID oder Paket-ID

Benachrichtigungen über Lizenznutzungsbeschränkungen für Apps and Books

Benachrichtigungen über Apps and Books helfen Ihnen, die Nutzung der Apps and Books-Lizenz zu verfolgen. Die Schwellenwerte für die Benachrichtigung sind wie folgt definiert:

- Es wird eine Information versendet, wenn über 50 % der Lizenzen verbraucht sind.
- Es wird ein Warnhinweis versendet, wenn 70 bis 80 % der Lizenzen verbraucht sind.
- Es wird eine Warnung mit Hinweis auf den kritischen Zustand versendet, wenn 90 bis 100 % der Lizenzen verbraucht sind.
- Die Benachrichtigungen werden gelöscht, wenn die Nutzung unter 50 % sinkt.

So zeigen Sie die Lizenzinformationen für jede App an:

1. Klicken Sie auf **Apps > Apple Apps and Books**.
2. Die Lizenzinformationen werden mit folgenden Angaben angezeigt:
    - Name der App
    - Kosten der Lizenz
    - Anzahl der verfügbaren Lizenzen
    - Anzahl der zurückgegebenen Lizenzen

Gehen Sie zu **Dashboard > Benachrichtigungen,** um Details einer Lizenzbenachrichtigung anzuzeigen.

3. Die Seite mit den Benachrichtigungen wird angezeigt.
   Klicken Sie auf den Titel der Benachrichtigung, um die Details anzuzeigen. Die verfügbaren Benachrichtigungen finden Sie im Dashboard.

Benachrichtigungen über Lizenznutzungsbeschränkungen für Apps and Books

Auslöser	Schweregrad	Benachrichtigungstyp	Komponententyp
50 % zurückgegeben	[Info]	Lizenznutzung	Apps and Books
70 % zurückgegeben	Warnung	Lizenznutzung	Apps and Books
80 % zurückgegeben	Warnung	Lizenznutzung	Apps and Books
90 % zurückgegeben	Warnung	Lizenznutzung	Apps and Books
100 % zurückgegeben	Warnung	Lizenznutzung	Apps and Books

Lizenznutzung für Apps and Books ansehen

In der Lizenznutzungstabelle der Lizenzspalte werden die Details der Lizenznutzung für den jeweiligen Benutzer angezeigt.

1. Klicken Sie auf eine App.
2. Klicken Sie auf die Registerkarte **Lizenznutzung**.
3. Geben Sie einen Benutzernamen im Suchfeld ein.

Apps and Books-Lizenz für eine App widerrufen

Apps and Books Lizenzen werden widerrufen, wenn:

- Wenn das Gerät inaktiv ist (abgeschaltet oder gelöscht).
- Eine Apps and Books-App gelöscht wird.
- Eine Gerätelizenz wird zurückgezogen, wenn das Gerät abgeschaltet wird.
- Ein Apps and Books-Token gelöscht wird.

Apps and Books-Lizenz für eine App widerrufen:

1. Wählen Sie die App unter **Apps > App-Katalog** aus.

2. Klicken Sie auf die Registerkarte **Apple Apps and Books Licenses**, falls vorhanden.
3. Führen Sie eine der folgenden Aktionen aus:
    1. Klicken Sie auf **Alle Lizenzen widerrufen**, um alle Lizenzen von allen Benutzern oder Geräten zu widerrufen.
    2. Klicken Sie auf die Registerkarte **Aktivitätsprotokoll** . Widerrufen Sie in der Spalte **Aktionen** einzelne Lizenzen pro Benutzer oder pro Gerät.

- Für iOS-Geräte gewährt Apple eine 30-tägige Nachfrist für Apps and Books-Apps, wenn die Apps and Books-Lizenz zurückgezogen wurde. Daher lässt sich die Apps and Books-App installieren.
- Bei macOS-Geräten bleibt die App auch nach Rücknahme der Apps and Books-Lizenz noch auf dem Gerät.

Apps and Books-Lizenz für einen Benutzer widerrufen:

1. Klicken Sie auf eine App.
2. Klicken Sie auf die Registerkarte **Lizenznutzung**.
3. Klicken Sie auf den Link **Lizenz widerrufen** für den Benutzer, dessen Zugang zu der Lizenz entfernt werden soll.

> Apps and Books-Lizenzen werden automatisch zurückgezogen, wenn der Benutzer gelöscht wird oder der Benutzer das MDM-Profil vom Gerät entfernt.

Fehlerbenachrichtigungen bei der Authentifizierung von Apps and Books

Bei Verwendung des Apps and Books-Dienstes von Apple können Authentifizierungsfehler auftreten. Diese Benachrichtigungen über Authentifizierungsfehler bei Apps and Books sind:

Fehlermeldung	Aktion
Ungültiges Authentifizierungs-Token	Gültiges Apps and Books-sToken hochladen
Token abgelaufen	Erstellen Sie online ein neues Token mit Ihrem Unternehmenskonto.
Das sToken wurde zurückgezogen.	Gültige Apps and Books hochladen
Anmeldung erforderlich	Beim Dienst Apps and Books anmelden

Apps und Books-Verhalten für macOS- und iOS-Geräte

Apps and Books für iOS

Aktion	Geräte-Lizenz	Benutzer-Lizenz
Apps and Books-App aus der Distribution für einen Benutzer entfernen	Die App wird auf dem Benutzer-Gerät deinstalliert	Die App wird auf dem Benutzer-Gerät deinstalliert
Delegierung einer Apps and Books-App aufheben	Die App wird von allen Geräten aus allen Spaces außer dem Standard-Space deinstalliert.	Die App wird von allen Geräten aus allen Spaces außer dem Standard-Space deinstalliert.
Apps and Books-App aus dem Standard- oder benutzerdefinierten Bereich löschen	Die App wird von allen Geräten deinstalliert	Die App wird von allen Geräten deinstalliert

Apps and Books für macOS

Aktion	Geräte-Lizenz	Benutzer-Lizenz
Apps and Books-App aus der Distribution für einen Benutzer entfernen	Die App wird nicht vom Benutzergerät deinstalliert.	Entfällt
Delegierung einer Apps and Books-App aufheben	Die App wird nicht von allen Geräten in Nicht-Standard-Spaces deinstalliert.	Entfällt
Apps and Books-App aus dem Standard- oder benutzerdefinierten Bereich löschen	Die App wird nicht von allen Geräten deinstalliert.	Entfällt

Lizenzberechtigung für Apps and Books, wenn ein Gerät in Spaces verschoben wird.

Wenn ein Gerät in einen neuen Space verschoben wird, wird die dem Gerät/Geräteeigentümer zugeordnete Apps and Books-Lizenz zurückgezogen. Unter Berücksichtigung der Verfügbarkeit in dem neuen Space wird eine neue Apps and Books-Lizenz zugewiesen.

Im Folgenden werden die Szenarien für die Lizenzberechtigung von Apps and Books beschrieben:

Szenario	Berechtigung
Eine Apps and Books-Lizenz wird einem Gerät oder einem Gerätebesitzer im Ausgangs-Space zugewiesen und eine Apps and Books-Lizenz für dieselbe App ist im Ziel-Space verfügbar.	Weisen Sie eine Lizenz mit dem Apps and Books-Token im Ziel-Space zu.
Im Ausgangs-Space wird eine Apps and Books-Lizenz einem Gerät oder einem Gerätebesitzer zugewiesen, aber im Ziel-Space ist keine Apps and Books-Lizenz für diese App verfügbar.	Ziehen Sie die Lizenz aus dem Apps and Books-Token im Ausgangs-Space zurück.
Im Quellbereich wird einem Gerät oder Gerätebesitzer keine Apps and Books-Lizenz zugewiesen, und im Ziel-Space ist eine Apps and Books-Lizenz für alle installierten Apps and Books-Apps verfügbar.	Weisen Sie eine Lizenz mit dem Apps and Books-Token im Ziel-Space zu.

Wenn Sie keine Aufgaben auf der Seite **App-Kategorien** ausführen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie benötigen eine der folgenden **Rollen**:

- Verwaltung von Apps und Inhalten

8.19. Katalogeinstellungen

Dieser Abschnitt enthält die folgenden Themen:

- Einstellungen der Apple-App-Verwaltung auswählen
- Festlegen der Standard App-Store-Region
- iOS-App-Updates aktivieren/deaktivieren
- App-Bewertungen und -Rezensionen aktivieren/deaktivieren
- iOS/macOS Apps and Books sToken hochladen oder aktualisieren (Lizenz: Gold)
- iOS/macOS Apps and Books sToken aus Ihrem Cloud-Dienst entfernen

Konfigurieren Sie auf der Seite "Apps > Katalogeinstellungen" die Einstellungen, die Sie auf alle Apps in Ihrem App-Katalog anwenden. Sie können folgende Aktionen durchführen:

- App-Updates bei der Anmeldung des Geräts einbeziehen
- Verhindern von Backups in iCloud und iTunes (nur iOS)
- Standard-App-Store-Region festlegen (Apple und Microsoft)
- Entfernen von iOS-Apps, wenn das Gerät nicht angemeldet ist
- Ivanti Neurons for MDM "Ratings und Bewertungen" aktivieren
- iOS und macOS Apps and Books-Tokens hochladen (erfordert Gold-Lizenz)

Einstellungen der Apple-App-Verwaltung auswählen

Diese Einstellungen gelten für alle Apps, sofern keine App-Verwaltungskonfiguration für einzelne Apps erstellt wurde.

1. Aktivieren oder deaktivieren Sie eines der folgenden Kontrollkästchen:
    - **Apps bei der Geräteanmeldung aktualisieren**(standardmäßig ausgewählt)
    - **Datensicherung in iCloud und iTunes verhindern**
    - **Apps bei Deregistrierung entfernen**

Klicken Sie auf **Speichern**.

Benachrichtigungen

1. Klicken Sie auf die Dropdownliste unter **Systembenachrichtigung generieren, wenn neue App-Versionen in Apple App Store und Google Play Store verfügbar sind**, und wählen Sie eine der folgenden Optionen aus:
    - **Wöchentlich**
    - **Einmal am Tag**

Klicken Sie auf die Dropdownliste unter **Endbenutzerbenachrichtigungen generieren, wenn neue App-Updates im App-Katalog verfügbar sind**, und wählen Sie eine der Optionen aus:

- **Wöchentlich**
- **Einmal am Tag**

Festlegen der Standard App-Store-Region

Legen Sie in den Einstellungen des App-Katalogs die Standardregion für den App Store von Apple und Microsoft fest.

1. Im Abschnitt Standard-App-Store-Region:
    - Wählen Sie die **Region des Apple App Store** aus.
    - Wählen Sie die Region des Microsoft App Store aus.
2. Wählen Sie die Option aus oder deaktivieren Sie diese, um die zuletzt gewählte App-Store-Region als Standardregion für jeden Administrator zu verwenden. Wenn diese Option ausgewählt wird, wird als Region des App-Stores diejenige Region festgelegt, die von den einzelnen Administratoren zuletzt ausgewählt wurde, und setzt die vorherigen Einstellungen außer Kraft. Wenn ein Administrator diese Funktion zum ersten Mal verwendet, werden die Standard-Speicherregionen der App auf die vorherigen Einstellungen gesetzt.
3. Klicken Sie auf **Speichern**.

iOS-App-Updates aktivieren/deaktivieren

1. Aktivieren oder deaktivieren Sie das Kontrollkästchen Apps bei Geräteregistrierung aktualisieren.
    - Diese Option ist standardmäßig aktiviert.
    - Wenn Sie diese Option deaktivieren, wird bei Geräteanmeldungen (auch bei vom Administrator erzwungenen Anmeldungen) nicht auf App-Updates geprüft.
    - Der Benutzer kann jedoch die App auch manuell aktualisieren, indem er im Geräte-App-Katalog auf die Aktion "Anmeldung erzwingen" klickt.
    - Neue App-Installationen und alle sonstigen Konfigurationen und Einstellungen werden bei der Geräteanmeldung aktualisiert.

Klicken Sie auf **Speichern**.

Bei einer verwalteten App kann der Administrator auf die Aktion **Aktualisierung** auf der Seite mit den App-Details klicken, um die App manuell auf die neueste Version aus dem App Store zu aktualisieren.

Auf einem Benutzergerät kann der Benutzer auf die Option **Anmeldung erzwingen** im App-Katalogmenü klicken, damit sich das Gerät anmeldet und die Apps zusammen mit anderen Konfigurationen und Updates aktualisiert werden.

Durch diese Einstellungen können die Endbenutzer auswählen, wann ihre Apps aktualisiert werden sollen:

- Warten Sie, bis Sie Verbindung mit einem WLAN haben, um Kosten bei Datentarifen zu vermeiden.
- Vermeiden Sie eine Aussperrung zur falschen Zeit, d.h. während der Aktualisierung der App.

App-Bewertungen und -Rezensionen aktivieren/deaktivieren

Dies ermöglicht es Benutzern, sowohl diese App zu bewerten und eine Rezension zu schreiben, als auch anderen Benutzern, diese Rezension zu lesen.

1. Aktivieren oder deaktivieren Sie die Option **Bewertungen und Rezensionen im App-Katalog für Endbenutzer aktivieren**.
2. Klicken Sie auf **Speichern**.

> Das Format des sToken für Apps and Books hat sich geändert. Statt einer Zeichenkette wie in den früheren Releases wird jetzt eine Zeichenkette in einer Textdatei im vpptoken-Dateiformat gespeichert. Laden Sie diese Datei zur Verarbeitung direkt in die Administratorkonsole hoch. Die Seite mit dem Konto für Apps and Books wurde aktualisiert und zeigt jetzt den Firmennamen und das Ablaufdatum für Apps and Books an.

iOS/macOS Apps and Books sToken hochladen oder aktualisieren (Lizenz: Gold)

1. Wählen Sie **Apps and Books sToken hinzufügen**.
2. Geben Sie einen Namen für die sToken Datei in dem Feld **Alias Name** ein.
3. Ziehen Sie die sToken-Datei per Drag & Drop in den angegebenen Bereich oder klicken Sie auf **Datei auswählen**, um die sToken-Datei zu suchen.
4. Klicken Sie auf **Speichern** oder, wenn Sie eine sToken-Datei aktualisieren, auf **Update**.
5. Wechseln Sie auf die Seite **Apple Apps and Books**, um die Apps anzuzeigen, die diesem Token zugewiesen sind.

> Ivanti Neurons for MDMWenn die Token von Apps and Books in einer früheren Version von für einzelne Benutzer reserviert waren, müssen Sie überprüfen, ob die Token noch immer für diese Benutzer reserviert sind und sie bei Bedarf erneut reservieren.

iOS/macOS Apps and Books sToken aus Ihrem Cloud-Dienst entfernen

Sie können eine App zurückgeben, die ein Benutzer nicht länger benötigt, und bei Bedarf neu zuweisen. Wenn die App als verwaltete App mit MDM für iOS/macOS bereitgestellt wurde, können Sie die App und all ihre Daten sofort entfernen.

1. Wählen Sie eine App aus, die Sie entfernen wollen.
2. Klicken Sie auf **Löschen**.
   Es erscheint ein Warndialog.
3. Optional können Sie dem Benutzer einen 30-tägigen Verlängerungszeitraum einräumen, damit dieser:
   - die Daten speichern kann,
   - eine persönliche Kopie der App kaufen kann,
   - Apps, die der Benutzer über dieses Apps and Books-Konto installiert hat, zur weiteren Nutzung in sein Privatkonto übertragen kann.

Wenn Sie keine Aufgaben auf der Seite **Katalogeinstellungen** ausführen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie benötigen folgende **Rolle**:

- Verwaltung von Apps und Inhalten

8.20. App-Abhängigkeiten bereitstellen

Wenn Sie ein internes Anwendungs-Bundle hochladen, scannt die Cloud die Anwendung auf Abhängigkeiten. Wenn App-Abhängigkeiten gefunden werden, werden diese als dritter Schritt durch den Assistenten „App hinzufügen“ aufgelistet. Zu jeder Anwendungsabhängigkeit können die Administratoren eine Abhängigkeitsdatei hochladen. Manche Anwendungen lassen sich nicht installieren, wenn die Abhängigkeitsdatei nicht hochgeladen wird.

Der Administrator kann beim Installieren einer App die App-Abhängigkeit festlegen. In einem solchen Fall können eine oder mehrere Apps mit der Haupt-App gekennzeichnet sein. Wenn ein Benutzer versucht, die Haupt-App zu installieren, wird er darüber informiert, welche abhängigen Apps zusammen mit der Haupt-App installiert werden.

> Diese Funktion auf Geräten mit iOS, Android, Windows und macOS unterstützt.

Beachten Sie folgende Punkte zu den Anwendungsabhängigkeiten und Voraussetzungen:

- Der Administrator kann die abhängigen Anwendungen festlegen, die vorausgesetzt sind, bevor eine Anwendung auf einem Gerät installiert werden kann. Eine erforderliche Anwendung kann eine interne, öffentliche, private (Android) oder eine VPP-Anwendung sein.
- Die Anzahl der vorausgesetzten Anwendungen wird nun in der Spalte „Vorausgesetzte Apps“ auf der Seite des App Catalog angezeigt. Wenn Sie mit der Maus auf die Zahl zeigen, wird die Liste der vorausgesetzten Anwendungen eingeblendet.
- Eine vorausgesetzte Anwendung wird direkt heruntergeladen, sobald die Installation der Hauptanwendung ausgelöst wird.
- Wenn eine Hauptanwendung delegiert wird, werden die zugewiesenen vorausgesetzten Anwendungen automatisch delegiert.
- Sie können eine vorausgesetzte Anwendung erst dann aus dem App Catalog löschen, wenn die Voraussetzungsbeziehung entfernt wird.
- Verschiedene Versionen einer Anwendung können verschiedene Anwendungen voraussetzen.
- Auf der Seite mit den Audit-Protokollen werden Hinzufügungen, Entfernungen und automatische Delegierungen von erforderlichen Anwendungen für iOS, Android und macOS erfasst.
- Wenn der Administrator oder der Endbenutzer eine Anwendung installiert, die bestimmte Anwendungen voraussetzt, werden die vorausgesetzten Anwendungen installiert, bevor die Hauptanwendung installiert wird. Wenn sich das Gerät anmeldet, bevor alle vorausgesetzten Anwendungen installiert wurden, werden alle vorausgesetzten Anwendungen deinstalliert.

> Obwohl eine Anwendung eine Abhängigkeitsdatei benötigt, müssen Sie in der Cloud keine der Dateien hochladen, um eine App bereitzustellen.

> Bei Geräten von Samsung sollte der Administrator erforderliche Apps zur Liste der im Kiosk-Modus zulässigen Apps hinzufügen. Die zur Liste der zulässigen Apps hinzugefügten erforderlichen Apps werden nicht zur Liste der verweigerten Apps hinzugefügt.

> Bei Geräten, die nicht von Samsung sind, müsste die erforderliche App unbeaufsichtigt im Hintergrund ausgeführt werden, falls die Haupt-App zur Liste der im Kiosk-Modus zulässigen Apps hinzugefügt wird. Sie können die erforderliche App nur dann im Kioskmodus anzeigen, wenn der Administrator die App in den Kioskmodus versetzt.

Windows-Geräte – Wenn die Bridge-App eine erforderliche App ist und nicht verteilt wird und wenn die Haupt-App eine im Hintergrund verteilte .exe-Datei ist. Nach Entfernen der Abhängigkeit wird die Bridge-App deinstalliert, aber die .exe-Datei schlägt nach diesem Schritt fehl. Der Administrator sollte sicherstellen, dass die Verteilung der Bridge-App nicht standardmäßig aufgehoben wird.

Windows-Geräte – Wenn die Haupt-App nicht im Hintergrund verteilt wird und über eine erforderliche App verfügt, die nicht verteilt wird, wird die erforderliche App zuerst installiert und erfolgreich ausgeführt. Wenn jedoch die Installation der Haupt-App fehlschlägt, wird die erforderliche App sofort deinstalliert. Ein erneuter Installationsversuch einer fehlgeschlagenen Haupt-App findet nur dann statt, wenn der Benutzer eine Installationsanforderung auslöst.

Interne Anwendung hinzufügen

1. Gehen Sie zu **Apps > App-Katalog**.
2. Klicken Sie aufHinzufügen.
3. Ziehen Sie die App-Datei in das gepunktete Feld oder klicken Sie auf **Datei auswählen** , um sie aus dem Dateisystem auszuwählen und zu bestätigen.
4. Klicken Sie auf **Weiter** (unten rechts). Cloud durchsucht die App nach Abhängigkeitsdateien und listet sie in der Tabelle **App-Abhängigkeiten** auf.
5. Prüfen Sie die App-Informationen und die Auswahl der richtigen App.
6. Klicken Sie auf das Hochlade-Symbol in der Spalte **Aktionen**. Das Fenster **Abhängigkeit hochladen** wird angezeigt.
7. Klicken Sie auf **Datei auswählen**, um eine lokale Kopie der Datei zu suchen und klicken Sie dann auf **Hochladen**.
8. Cloud scannt optionale Pakete für die App, falls vorhanden, und listet sie in der Tabelle „Optionale Pakete“ auf. Ist die App aufgelistet, klicken Sie auf das Hochlade-Symbol in der Spalte „Aktionen“. Das Fenster „Optionales Paket hochladen“ wird angezeigt.
9. Prüfen Sie die App-Informationen und die Auswahl der richtigen App.
10. Klicken Sie auf **Datei auswählen**, um eine lokale Kopie der Datei zu suchen und klicken Sie dann auf „Hochladen“.
11. Klicken Sie auf **Weiter**.
12. (Optional) Ergänzen Sie Screenshots der App und klicken auf **Weiter**
13. Wenn die Anwendung weitere Anwendungen voraussetzt.
    1. Wählen Sie die Option **Ein** im Abschnitt **Vorausgesetzte Apps**.
    2. Suchen Sie die vorausgesetzte Anwendung auf der Registerkarte **Apps hinzufügen**.
    3. Wählen Sie die Anwendungen aus.
    4. Klicken Sie auf **Speichern**.
14. Definieren Sie die App-Verteilung und klicken Sie auf **Weiter**.
15. Definieren Sie den Abschnitt App-Konfiguration und klicken Sie auf **Fertig**. Wenn die Geräte das nächste Mal mit der Cloud synchronisiert werden, wird die App zusammen mit den abhängigen Dateien auf dem Gerät bereitgestellt.

Sie können weitere Abhängigkeiten hinzufügen, indem Sie auf die Schaltfläche „Abhängigkeiten hinzufügen“ klicken. Nach dem Hochladen werden auch diese zusätzlichen Abhängigkeiten in der Tabelle App-Abhängigkeiten aufgelistet. Der Administrator kann auch manuell optionale Pakete des Typs „Nur Content“ hinzufügen. Dieser Pakettyp ist nicht versionsabhängig.

Vorausgesetzte Anwendung hinzufügen

Sie können eine vorausgesetzte Anwendung zu einer Hauptanwendung hinzufügen. Sie können verschiedene vorausgesetzte Anwendungen für verschiedene Versionen einer Hauptanwendung hinzufügen. Auf der Seite des App Catalog können Sie entweder angeben, dass Beschreibung, Skripten, Bildschirmfotos, Verteilung, App-Voraussetzungen und App-Konfigurationen der vorhandenen Anwendungsversion beibehalten werden sollen, oder die zugewiesenen vorausgesetzten Anwendungen ändern. Sie können eine vorausgesetzte Anwendung nicht löschen, ohne die Zuweisung zur Hauptanwendung zu entfernen.

Die Seite „Audit-Protokoll“ zeigt nun die unterstützten vorausgesetzten Anwendungen in speziellen Feldern an:

Im Abschnitt "Erforderliche Anwendungen" für die unterstützten iOS-, Android- und macOS-Anwendungen auf der Seite "Audit-Protokolle" werden folgende Felder angezeigt:

appVersionId

Name

platformAppId

Die vorausgesetzten Anwendungen, die automatisch delegiert oder deren Delegierung aufgehoben wurden und folgende Felder enthalten, werden angezeigt:

dmPartitionDistributionType

dmPartitionDistributionReason

Verfahren

1. Wählen Sie eine Anwendung im **App Catalog** aus.
2. Klicken Sie auf **Bearbeiten**.
3. Scrollen Sie nach unten zu **App-Delegation** und wählen Sie die Option **Diese App für alle Spaces delegieren**.
4. Klicken Sie auf **Speichern**.

> Wenn Sie mehrere Apps delegieren und die Delegation aus der Hauptanwendung entfernen, wird die vorausgesetzte Anwendung nicht automatisch aus der Delegation entfernt.

8.21. Bereitstellen von Divide Productivity mit Android Enterprise

Divide Productivity ist eine PIM-App, die Sie für Geräte mit Android Enterprise bereitstellen können.

1. Gehen Sie zu **Apps > App-Katalog**.
2. Klicken Sie unter **Business-Apps** auf **Divide Productivity**.
3. Geben Sie zusätzliche Kategorien oder eine Beschreibung ein.
4. Klicken Sie auf **Weiter**.
5. Akzeptieren Sie die angezeigten Berechtigungen.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine Verteilungsoption aus.
8. Zeigen Sie **Erweiterte Optionen & App-Konfiguration** an.
9. Beachten Sie beim Aktivieren von Optionen die folgenden Leitlinien:
10. Wählen Sie eine Verteilungsoption aus.

Einstellung	So gehen Sie vor
Verhindert, dass der Benutzer die App deinstalliert.	Wählen Sie diese Option aus, um zu verhindern, dass der Endbenutzer die App deinstalliert, nachdem diese im Hintergrund installiert wurde.
E-Mail Adresse	Definieren Sie mit Variablen die E-Mail-Adresse, die mit der App verbunden werden soll.
Passwort	Definieren Sie mit Variablen das Passwort für das E-Mail Konto. Wenn Sie dieses Feld leer lassen, wird der Benutzer nach dem Passwort gefragt.
Host	Geben Sie den Host-Namen des Mailservers an, den Sie verwenden wollen. Geben Sie den vollqualifizierten Domainnamen des ActiveSync-Servers ein. Wenn Sie ein Standalone-Sentry verwenden, geben Sie stattdessen den vollqualifizierten Domainnamen des Sentry (FQDN) ein. Beispiel: mySentry.mycompany.com
Servertyp	Wählen Sie die Art des Mail-Servers aus.
Benutzername	Definieren Sie mit Variablen den Benutzernamen für das E-Mail Konto.
Ist SSL erforderlich?	Wählen Sie diese Option aus, wenn Sie die Kommunikation mit https für den Server absichern wollen, den Sie im Feld "Host" angegeben haben.
Allen Zertifikaten vertrauen	Wählen Sie die Option nur aus, wenn die App nicht vertrauenswürdige Zertifikate automatisch akzeptieren soll. In der Regel wählen Sie die Option nur, wenn Sie in einer Testumgebung arbeiten.
Standard-E-Mail-Signatur	Dies ist die Standard-E-Mail-Signatur für alle E-Mails. Der Endbenutzer kann diese Einstellung jederzeit ändern. Sobald der Gerätebenutzer diese Einstellung ändert, haben spätere Änderungen dieses Felds keinen Einfluss mehr.
Maximale Größe von E-Mail-Anhängen	Geben Sie die maximale Größe für angehängte Dateien ein.
Aufgabe aktivieren	Klicken Sie auf die Option, um Aufgaben zu synchronisieren.
Anmeldezertifikat-Alias	Geben Sie den Alias für das Anmeldezertifikat ein.
S-MIME-Signaturzertifikat – Alias	Derzeit nicht unterstützt.
S-MIME-Verschlüsselungszertifikat – Alias	Derzeit nicht unterstützt.
Erweiterte Optionen	

Einstellung	So gehen Sie vor
Auf einem Gerät installieren	Wählen Sie diese Option aus, um den Benutzer zur Installation der App aufzufordern.
Bei Samsung-Knox-Geräten im Hintergrund installieren	Wählen Sie die Option, um die App automatisch auf Samsung-Knox-Geräten zu installieren.
App nicht im App-Katalog des Endbenutzers anzeigen	Wählen Sie diese Option aus, wenn Sie nicht wollen, dass diese App im App-Katalog des Geräts angezeigt wird.

11. Klicken Sie auf **Fertig**.

8.22. Konfiguration der Provisioner-App

Dieser Abschnitt enthält die folgenden Themen:

- Anforderungen für die Bereitstellung
- Android-Beam für die Verwendung von NFC-Bump freischalten
- Unternehmenseigenes Gerät bereitstellen
- Gerät registrieren
- Registrierungsstatus des Geräts überprüfen

Provisioner ist eine Ivanti Neurons for MDM-App zur Bereitstellung firmeneigener Geräte, sodass diese als betrieblich verwaltete Geräte registriert und im Gerätebesitzermodus betrieben werden können.

Ein vom Unternehmen verwaltetes Gerät besitzt nur ein Unternehmensprofil und kein privates Profil. Der Administrator kann über 20 Sperren für das Gerät einstellen, die Gerätefunktionen wie Kamera, Telefonanrufe, SMS, Netzwerkanbindung usw. betreffen.

Die Provisioner-App wird von dem Gerät benötigt, das die Konfiguration auf dem Android Enterprise-Zielgerät mit einem NFC-Bump einleitet. Um unternehmenseigene Geräte bereitzustellen, installieren Sie die Provisioner-App auf dem Mastergerät und stellen dann per NFC-Bump (über die Nahfeldkonfiguration) neue Geräte bereit. Beim NFC-Bump werden die beiden Geräte mit den Rückseiten aneinander gelegt. Die Geräte können so bereitgestellt werden, dass sie eine der folgenden Client-Apps verwenden:

- Go für die Verwendung mit Ivanti Neurons for MDM
- At Work UEM ist eine Client-App ohne Branding für die Cloud.

Anforderungen für die Bereitstellung

So stellen Sie ein firmeneigenes Gerät mit Android Enterprise als betrieblich verwaltetes Gerät bereit:

- Firmeneigene native Geräte mit Android Enterprise müssen vor der Bereitstellung auf die Werkseinstellungen zurückgesetzt werden.
- Die Konfiguration für Android Enterprise muss für die Android-Gerätegruppe definiert und übernommen worden sein.
- Eine NFC-fähiges Android-Gerät dient als Master oder Vorlage; auf diesem Gerät wird die App Provisioner installiert.
- Android Enterprise geeignete Geräte, die bereitgestellt werden sollen
- Die App Provisioner
  Laden Sie die Provisioner-App für Android von Google Play herunter.

Android-Beam für die Verwendung von NFC-Bump freischalten

Verfahren

1. Gehen Sie auf dem Gerät zu **Einstellungen**.
2. Gehen Sie zur Option **Drahtlos & Netzwerke** und klicken Sie auf **Weiter**.
3. Aktivieren Sie das Kontrollkästchen **NFC**.
4. Klicken Sie auf **Android Beam** und schieben Sie den Schalter in die Stellung **On**.

> Die genauen Schritte weichen je nach dem verwendeten Gerät leicht ab.

Unternehmenseigenes Gerät bereitstellen

Verfahren

1. Installieren Sie die App Provisioner auf dem Gerät, das als Android-Mastergerät verwendet werden soll.
2. Starten Sie den Provisioner auf dem Mastergerät.
3. Wählen Sie eine App aus dem Dropdown-Menü.
4. Geben Sie die Informationen für die App Provisioner ein. Manche Felder werden automatisch ausgefüllt, wenn ein unterstütztes WLAN erkannt wird. Beachten Sie die folgenden Richtlinien:

Feld	Wert
Wählen Sie die App für die Bereitstellung aus.	Los (für die Verwendung mit Ivanti Neurons for MDM auswählen) @Work UEM (Noname-Client-App zur Verwendung mit einer anderen Cloud)
WLAN SSID	Geben Sie SSID des WLANs ein, die das Mastergerät verwenden soll.
WLAN-Sicherheitsprotokoll	Geben Sie das WLAN-Sicherheitsprotokoll ein.
WLAN-Passwort	Geben Sie das Passwort für das WLAN ein.
Zeitzone	Geben Sie die lokale Zeitzone ein.
Region	Geben Sie die Regions- und Spracheinstellungen ein.

5. Klicken Sie auf **Weiter**.
   Der Bildschirm NFC-Bump wird auf dem Mastergerät angezeigt.
6. Sobald das Zielgerät eingeschaltet ist und den Android-Begrüßungsbildschirm anzeigt, drücken Sie die Rückseite des Mastergeräts gegen die Rückseite des Zielgeräts, um eine Nahfelddatenübertragung zu starten.
   Wenn die NFC-Übertragung erfolgreich war, gibt das Zielgerät einen Piepton aus und lädt anschließend die ausgewählte Client-App herunter. Wenn das Gerät nicht verschlüsselt ist, verschlüsselt es sich zunächst, bevor es mit dem nächsten Vorgang fortsetzt.
7. Stellen Sie weitere Geräte bereit, indem Sie einen neuen NFC-Bump durchführen. Das Zielgerät muss den Begrüßungsbildschirm anzeigen, und auf dem Mastergerät muss der Bildschirm **NFC-Bump starten** angezeigt werden.

Gerät registrieren

Sobald das unternehmensfirmeneigene Gerät mit einem NFC-Bump bereitgestellt ist, ist auch die ausgewählte Client-App installiert. Starten Sie die Client-App und registrieren Sie das Gerät.

Registrierungsstatus des Geräts überprüfen

Verfahren

1. Gehen Sie zu **Geräte > Geräte**.
2. Klicken Sie auf den Link für das Gerät, um die Details anzuzeigen.
3. Der Status des Geräts wird in dem linken Feld angezeigt.

8.23. Verwalten von Windows-Anwendungen

Benutzer haben die Möglichkeit, den kompletten App-Lebenszyklus (Importieren, Konfigurieren, Planen, Verteilen, Aktualisieren und Entfernen) für Windows-Anwendungen zu verwalten. App-Verteilung und App-Aktualisierung werden über die MDM-Konsole unterstützt. Weitere Einzelheiten zum Verwalten von Windows-Apps und anderen Anwendungen finden Sie unter **App-Konfiguration**, **App-Einblicke** und **App-Katalog**.

Unterstützte App-Typen

- Intern (prüfen Sie die Optionen unter **Hinzufügen einer internen App** im Abschnitt **App-Katalog**)
- MSB (Microsoft Store für Unternehmen-Integration)
- Öffentlicher Store (über native Microsoft Store-Integration); Microsoft Store-Region kann unter Apps > Katalogeinstellungen festgelegt werden. Weitere Informationen finden Sie unter **Hinzufügen einer App über einen öffentlichen Store** im Abschnitt **App-Katalog**.

Unterstützte App-Erweiterungen

- MSI
- MSIX
- APPX
- APPX-Bündel
- EXE (über **Ivanti Bridge**)

App-Kontrolle

Die Konfiguration "App-Steuerung" steuert die App-Installation pro Gerät. Weitere Informationen finden Sie unter **Konfiguration der App-Kontrolle: Kontrolle der Apps, die auf dem Gerät installiert sind**.

Pakete und Abhängigkeiten

Folgende Funktionen sind verfügbar:

1. Windows-Apps können für alle Anwendungstypen als erforderlich (Voraussetzung) festgelegt werden. Weitere Informationen zum Festlegen von App-Voraussetzungen finden Sie unter **App-Abhängigkeiten bereitstellen**.
2. App-Abhängigkeiten von APPX und APPX-Bundles und weitere Paketabhängigkeiten. Überprüfen Sie auf der Seite **Anzeige der App-Details** den Abschnitt **App-Abhängigkeiten und andere Pakete**.
3. Win32-Apps unterstützen die Auswahl des richtigen Produktcodes (MSIs) sowie der Befehlszeilen und Variablen. Eine Liste der häufigsten Befehlszeilenoptionen finden Sie **hier**.

Skripte

Skripte werden über Ivanti Bridge Client unterstützt. Informationen zum Einrichten der Skripte finden Sie unter **Ivanti Bridge**.

Nachdem Ivanti Bridge auf den Geräten installiert wurde, können die Skripte wie folgt verteilt werden:

- Auf Geräteebene mit Skripten und Aktionen über Ivanti Bridge-Aktion
- Über die Ivanti Bridge-Konfiguration (**Konfigurationen** > **Bridge**)

Das Kontrollkästchen **Vorhandene Version auf Gerät prüfen** der Registerkarte **Skripte und Dateien** für interne MSI- und EXE-Anwendungen steuert, wie die App auf Windows-Geräten installiert wird. Wenn Sie diese Option aktivieren, führt das Gerät einen Check-in aus, um zu überprüfen, ob die App bereits installiert ist, und falls ja, welche Version. Ivanti Neurons for MDM installiert oder aktualisiert die App nur dann, wenn sie nicht vorhanden ist oder wenn die installierte Version älter ist als die erforderliche Version. Wenn die gleiche oder eine neuere Version vorhanden ist, wird die Installation übersprungen. Diese Option setzt voraus, dass die App auf mindestens einem Gerät installiert ist, bevor Sie sie aktivieren.

Skripte und Dateien vor und nach der Installation

Für EXE- und MSI-Dateien

Sie können die der PowerShell-Installation vor- und nachgelagerten Skripte, Registrierungsskripte und ausführbaren Windows-Dateien (.exe) konfigurieren und andere Dateitypen für Windows-Apps auf App-Detailebene herunterladen.

Beim Hinzufügen eines neuen Skriptes oder einer neuen Datei vor oder nach der Installation wird der Bildschirm "Ivanti Bridge" angezeigt. Sie können das Skript oder die Datei anhängen, Skriptargumente hinzufügen und einen Zielspeicherort für die Dateien angeben. Das der Installation vorgelagerte Skript muss erfolgreich auf dem Gerät ausgeführt worden sein, damit der Befehl zur App-Installation an das Gerät ausgegeben werden kann. Die der Installation vor- und nachgelagerten Skripte und Dateien werden in der Reihenfolge installiert bzw. ausgeführt, in der sie zur Konsole hochgeladen wurden. Wenn das Herunterladen des der Installation vorgelagerten Skriptes oder die Installation fehlschlägt, kann der App-Installationsvorgang nicht fortgesetzt werden.

Wenn das der Installation nachgelagerte Skript fehlschlägt, können Sie die Fehler auf der Seite mit den Gerätedetails unter dem Abschnitt "Geräteprorokolle" anzeigen. Falls die der Installation nachgelagerten Aktionen fehlschlagen, können die vor der Installation ausgeführten Skripte bzw. die heruntergeladenen und installierten .exe-Dateien nicht rückgängig gemacht werden.

Sie können die der Installation vor- oder nachgelagerten Skripte und Dateien neu anordnen, indem Sie die Option "Skripte und Dateien priorisieren" verwenden. Diese Option ist nur verfügbar, wenn mindestens zwei Skripte oder Dateien vorhanden sind. Mithilfe dieser Option können Sie die Dateien und Skripte innerhalb ihres jeweiligen Abschnitts vor oder nach der Installation verschieben, jedoch nicht abschnittsübergreifend.

Installationsverhalten und Konfigurationen

Windows-Anwendungen unterstützen die folgenden Funktionen:

- Installationen im Hintergrund
- **Zeitplanung von Windows Apps**
- Neustartoptionen

Weitere Einzelheiten zu Optionen für das Installationsverhalten finden Sie unter **App-Konfiguration**.

> MSI-Apps und EXE-Apps (die mit Bridge installiert wurden) unterstützen Installationen mit benutzerlosen MDM-Sitzungen.

Mögliche Szenarien:

- Das Gerät wurde neu gestartet und es ist noch kein Benutzer angemeldet.
- Der Benutzer hat sich von der Windows-Sitzung abgemeldet.
- Das Gerät wurde im benutzerlosen Autopilot-Modus (Selbstbereitstellung oder Pre-Provisioning) registriert.
- Die Anwendungen werden auf Geräteebene installiert.

Dank der Funktion lassen sich die MSI-Apps effizienter installieren, beispielsweise während des Autopilot-Registrierungsprozesses oder nachts, wenn niemand an dem Windows-Gerät arbeitet. Wenn einfaches Umpacken für EXEs in MSI verwendet wird, kann dies installiert jedoch nicht aktualisiert oder gelöscht werden. Das echte MSI-Paket verfügt über eine Verbindung mit CSP. Weitere Anwendungstypen werden installiert, nachdem sich der Benutzer angemeldet hat.

Tunnel for Windows (Per-App-VPN)

Tunnel ist eine eigenständige native Windows-Anwendung. Sie steht derzeit zur Verteilung an Geräte im Microsoft Store zur Verfügung. Erstellt eine Per-App VPN-Konfiguration. Sentry-Bereitstellung ist erforderlich. Zum Konfigurieren der Tunnel-App wechseln Sie zu **Konfigurationen** > **+Hinzufügen** > Nach Tunnel suchen (wählen Sie die Konfigurationen, die Windows-Geräte unterstützen). Wählen Sie das Sentry-Profil aus und konfigurieren Sie die Einstellungen zum Starten der Tunnelverbindung für die App-Daten über Sentry. Wechseln Sie zum Einrichten eines Sentry-Servers zu **Admin** > **Infrastruktur** > **Sentry**.

App-Inventar

Das Anwendungs- und Softwareinventar Ihrer Windows-Geräteflotte kann auch zwei Ebenen verfolgt werden:

- Wechseln Sie zum Überprüfen der auf all Ihren Geräten installierten Anwendungen zu **Geräte** > **App-Inventar**.
- Wechseln Sie zum Überprüfen des Inventars auf Geräteebene zu "Geräte", wählen Sie ein Gerät und klicken Sie auf "Installierte Apps".

Administratoren haben die Möglichkeit, Intervalle für die Erfassung des Windows-Anwendungsinventars festzulegen. Wechseln Sie zu "Admin > Windows > App-Inventarisierungsintervalle". Die Intervalle werden verwendet, wenn die Datenschutzkonfiguration so eingestellt ist, dass sie alle Apps des Geräts erfasst. Wechseln Sie zum Konfigurieren der Datenschutzkonfiguration zu "Konfigurationen", wählen Sie "+Hinzufügen" aus, suchen Sie nach "Datenschutz" und wählen Sie "App-Inventar für alle Apps auf dem Gerät erstellen". Wählen Sie die zu erfassenden App-Typen aus.

Unternehmens-App-Katalog (Apps@Work)

Kunden können mithilfe von Apps@Work einen Unternehmenskatalog auf Windows-Geräten aktivieren. Apps@Work ist über den App-Katalog in Neurons for UEM verfügbar und kann von dort bereitgestellt werden. Weitere Informationen finden Sie unter **Apps@Work (iOS, Android, Windows und macOS)**.

8.24. Ivanti Bridge

Dieser Abschnitt enthält die folgenden Themen:

- Bridge unterstützte Dateitypen
- Bridge-Setup
- Bridge-Protokolle
- Letzter Check-in von Bridge
- Wiederherstellung nach Ausfall des Bridge-Dienstes

Ivanti Bridge vereinheitlicht Operationen auf Mobilgeräten und Desktopgeräten unter Windows 10 über eine einzige Konsole und einen einzigen Kommunikationskanal. Damit werden die UEM-Fähigkeiten auf die Verwaltung von PCs erweitert. Unternehmen können damit die Kosten signifikant senken, die höhere Effizienz nutzen und für PCs und Mobilgeräte eine konsistente Sicherheit gewährleisten. Mit Ivanti Bridge kommen Unternehmen für Desktops unter Windows 10 mit einem einzigen Protokoll aus, so wie sie es von mobilen Windows-Geräten gewohnt sind, um im Betriebssystem Informationen an die alten Anwendungen zu senden.

Mit Ivanti Bridge kann die IT Windows-Operationen auf UEM-Plattformen modernisieren, ohne auf kritische Funktionalität zu verzichten. Die IT kann bereits verfügbare Richtlinien und Scripte verwenden, ohne dass ein System-Image, ein Domänenbeitritt oder mehrere Kommunikationskanäle mit dem Gerät benötigt werden.

Mit Ivanti Bridge können Unternehmen jetzt:

- Die komplette Kontrolle über PCs mit UEM sicherstellen
- PCs aus der Ferne over-the-air verwalten
- Die Anfertigung von Desktop-Images reduzieren
- Umfassend GPO-Befehle mit PowerShell Scripts für UEM nutzen
- Die Registry bequem bearbeiten und verwalten
- mühelos nicht in MSI gekapselte Win32-Apps und Win32-Store-Apps bereitstellen
- Das Dateisystem transparent machen

> Ivanti Bridge wird auf Windows 11+-Geräten und ARM-Prozessoren unterstützt. Ivanti Bridge unterstützt keine Desktops mit Windows 10 Home.

Bridge unterstützte Dateitypen

Ivanti Bridge unterstützt folgende Dateitypen:

- PowerShell
  Die PowerShell-Scripts werden durch die von Bridge benannten Argumente per Push übertragen.
  64 Bit-PowerShell-Scripts werden auf Desktop-Geräten mit Windows 10 für 64 Bit unterstützt.

> Die serverseitige Bridge-Zeitüberschreitung für das Warten auf das Ergebnis eines PowerShell-Skripts beträgt etwa 20 Minuten. Die Zeitüberschreitung wird als Fehler protokolliert. Das Skript auf dem Gerät funktioniert jedoch weiterhin.

> Die geräteseitige Bridge-Zeitüberschreitung für das Warten auf eine PowerShell-Skriptausführung beträgt etwa 60 Minuten. Nach 60 Minuten wird der Vorgang abgebrochen, es wird keine Skriptausgabe gespeichert und ein neuer Fehler wird an den Server gesendet.

> Die serverseitige und die geräteseitige Zeitüberschreitung werden als Fehler protokolliert. Läuft die zweite Zeitüberschreitung ab und das Skript generiert eine Ausgabe, wird auf dem Server nichts protokolliert.

Registrierung

- VB-Skripte
- .EXE für Win32-Anwendungsinstallation
- Win32-Store-Apps verwenden zum Installieren und Deinstallieren der Apps das WinGet-Tool.

> Wenn Administratoren per Push Win32-Dateien (.EXE-Dateien) auf ein Gerät übertragen müssen (beispielsweise als interne Windows-App), wird die Bridge-Funktionalität automatisch verwendet, sofern sie verfügbar ist. Damit die Datei im Hintergrund gestartet wird, müssen Sie beim Start unbedingt einen Parameter angeben (beispielsweise /SILENT oder /VERYSILENT).
> Die .EXE-Apps werden über Bridge unter Verwendung des Admin PowerShell-Modus installiert. Bei Windows-Geräten wählen Sie die Option 'Als Benutzer ausführen' aus, um die Installation mit den Anmeldeinformationen des Benutzers auszuführen.

> Administratoren sollten zum Installieren der Apps für einen Benutzer das Kontrollkästchen **Installationsprogramm wird als Benutzer ausgeführt** bei **App-Installationsprogramm – Einstellungen** markieren. Markieren Sie das Kontrollkästchen nicht, wenn Sie möchten, dass die Apps auf Systemebene installiert werden.

Mit Ivanti Bridge können Sie das Gerät in folgenden wichtigen Bereichen optimieren:

- **Registry:** Sie können Registry-Werte lesen, schreiben und aktualisieren.
- **Dateien:** Sie können den Inhalt einer Datei überprüfen, lesen und aktualisieren.
- **Anwendungsinstallation:** Sie können .EXE-Anwendungen auf dem Desktop installieren. Diese Anwendungen können sich entweder auf den Ivanti Neurons for MDM-Servern oder in einem Content Delivery Network (CDN) in der Cloud befinden.

Bridge-Setup

Zum Einrichten von Ivanti Bridge müssen Administratoren zuerst folgende Schritte in der angegebenen Reihenfolge abschließen:

1. **Aktivieren von Bridge-Lizenzen**
2. **Installieren der Bridge-Anwendung**
3. **Scripts für die Geräte hochladen** für die permanente oder einmalige Verwendung mit den Geräten.

Aktivieren von Bridge-Lizenzen

Ivanti Bridge ist Teil des älteren Gold-Pakets und des aktuellen Secure UEM-Pakets.

Installieren der Bridge-Anwendung

Nach dem Aktivieren der Ivanti Bridge-Lizenzen kann die mobile Bridge-App wie folgt installiert werden:

1. Gehen Sie zu **Apps > App-Katalog**.

2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie im Abschnitt für geschäftliche Apps auf **Ivanti Bridge**.
4. Ergänzen Sie Details entsprechend den bereitgestellten Lizenzen, passen Sie diese an und verteilen Sie die mobile Bridge-App an die betreffenden Geräte.
   Wenn Sie die Option **Auf Windows-Geräten im Hintergrund installieren** aktiviert haben, wird die mobile Bridge-App im Hintergrund installiert und der Bridge-Dienst auf den Geräten gestartet.

> Die Bridge-App wird standardmäßig zum App Catalog hinzugefügt und auch standardmäßig an alle Geräte verteilt.

> Nach dem Importieren der neuesten Version von Ivanti Bridge in den Katalog des Mandanten kann der Administrator die neue Version der App anzeigen.

Scripts für die Geräte hochladen

Administratoren können Scripts in Geräte hochladen, die dann permanent verwendet werden, indem sie eine neue Bridge-Konfiguration erstellen:

1. Gehen Sie zu Konfiguration > +Hinzufügen.
2. Wählen Sie die Konfiguration **Ivanti Bridge für Windows-Skripte und -Aktionen** aus.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Verwenden Sie im Abschnitt "Ivanti Bridge konfigurieren" eine der folgenden zwei Optionen, um Skripte hochzuladen:
   - Skripte aus der Skriptbibliothek auswählen – Wählen Sie eines der verfügbaren Skripte aus der Liste aus.
   - Oder
     Skripte hochladen – Geben Sie die Einstellungen an, wie in der Tabelle unter Schritt 7 beschrieben.
     - Geben Sie die Kategorieeinstellungen für **Skriptdatei** ein, um ein Installationsskript festzulegen, das per Push auf die Geräte übertragen oder dort ausgeführt werden soll.
     - (Optional) Geben Sie die Kategorieeinstellungen für **Skriptdatei rückgängig machen** ein, um ein Deinstallationsskript festzulegen, das per Push auf die Geräte übertragen oder dort ausgeführt werden soll. Diese Option ist zweckmäßig, wenn Sie ein Gerät löschen oder eine Konfiguration löschen wollen.
     - (Optional) Klicken Sie auf die Option **Outlook konfigurieren**, um Microsoft Outlook für ein Gerät zu konfigurieren, das Bridge verwendet.

       > Unterstützung nur mit Outlook 2010 und 2013

Klicken Sie auf Weiter.

7. Wählen Sie eine Verteilungsebene für diese Konfiguration aus.
   Bei diesen Geräteaktionen wird automatisch eine Anmeldung erzwungen.

Kategorie	Einstellung	So gehen Sie vor
	[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
	Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Script-Datei	**Alle Versionen (Windows 10+ Desktop)**	
	Script-Datei	Wählen Sie ein gültiges Script oder eine gültige ausführbare Datei aus (.ps1, .reg, .exe). • Die definierte Script-Datei bzw. ausführbare Datei (.ps1, .reg, .exe) wird automatisch ausgeführt. • Andere Dateiarten werden nur in den Zielordner kopiert.
	Script-Parameter	Definieren Sie die Liste der Argumente für die Script-Datei. • Bei Win32-Dateien (.exe-Dateien) müssen Sie einen Parameter eingeben, damit die Datei im Hintergrund gestartet wird (beispielsweise, /SILENT oder /VERYSILENT). Diese Eingabe ist obligatorisch.
Script-Datei rückgängig machen **Alle Versionen (Windows 10+ Desktop)**	Zielordner	Definieren Sie den Zielordner für die Script-Datei. • Wenn der Zielordner nicht definiert ist, wird der Wert der Systemumgebungsvariable %TEMP% als Zielordner verwendet.
	Script-Datei	Wählen Sie ein gültiges Script oder eine gültige ausführbare Datei aus (.ps1, .reg, .exe). • Die definierte Script-Datei bzw. ausführbare Datei (.ps1, .reg, .exe) wird automatisch ausgeführt. • Andere Dateiarten werden nur in den Zielordner kopiert.
	Script-Parameter	Definieren Sie die Liste der Argumente für die Script-Datei. • Bei Win32-Dateien (.exe-Dateien) müssen Sie einen Parameter eingeben, damit die Datei im Hintergrund gestartet wird (beispielsweise, /SILENT oder /VERYSILENT). Diese Eingabe ist obligatorisch.
	Zielordner	Definieren Sie den Zielordner für die Script-Datei. • Wenn der Zielordner nicht definiert ist, wird standardmäßig der Wert der Systemumgebungsvariable %TEMP% verwendet.

Scripts auf Geräte zur einmaligen Verwendung hochladen

Administratoren können ein Script in Geräte zur einmaligen Verwendung hochladen.

1. Gehen Sie zu **Geräte > Geräte**.
2. Klicken Sie auf den Link mit dem Gerätenamen, um die Seite mit den Gerätedetails aufzurufen. Dies ist ein Desktopgerät mit Windows 10, auf dem ein Script zur einmaligen Ausführung per PUSH übertragen und ausgeführt wird.

3. Klicken Sie auf das Symbol ⋮ und dann auf **Skripte und Aktionen über Ivanti Bridge**.
4. Geben Sie einen Namen ein.
5. Geben Sie in dem Abschnitt Script-Datei ein Script an, das per PUSH auf das Gerät übertragen und wie in der Tabelle beschrieben ausgeführt werden soll.
6. Klicken Sie auf [Apply.
   Die Ausführung des Scripts wird in eine Warteschlange gestellt. Es kann eine gewisse Zeit dauern, bis sie abgeschlossen ist. Rufen Sie die Registerkarte "Protokolle" auf, um den Status zu überprüfen (Ausgabe oder Fehlermeldung). Bei diesen Geräteaktionen wird automatisch eine Anmeldung erzwungen.

Bridge-Protokolle

Mit dieser Funktion können Sie zur Fehlerbehebung und Diagnose von Anwendungen Ivanti Bridge-Protokolle für einzelne Geräte laden. Die Protokolle werden bei der nächsten Geräteanmeldung versendet. Sie können die nächste geplante Synchronisierung abwarten oder einen Geräte-Check-in erzwingen, um die Protokolle schneller zu erhalten.

Protokolle von einem Gerät laden:

1. Gehen Sie zu **Geräte > Geräte**.
2. Klicken Sie auf den Link mit dem Gerätenamen, um die Seite mit den Gerätedetails aufzurufen. Dies ist ein Desktopgerät mit Windows 10, auf dem ein Script zur einmaligen Ausführung per PUSH übertragen und ausgeführt wird.
3. Klicken Sie auf das Symbol ⋮ und dann auf **Ivanti Bridge-Protokoll abrufen**. Das Fenster **Ivanti Bridge-Protokoll abrufen** wird angezeigt.
4. Wählen Sie eine der folgenden Optionen aus:
   Einzelprotokoll - Fordert von der Cloud das aktuellste Bridge-Protokoll auf dem Gerät an.
   Alle Protokolle - Fordert von der Cloud alle Protokolle (für bis zu 30 Tage) auf dem Gerät an.
5. Klicken Sie auf **Protokoll laden**. Sobald das Protokoll von einem Gerät an die Cloud gesendet wurde, können Sie das Bridge-Protokoll über die Registerkarte „Protokolle“ auf der Seite „Gerätedetails“ aufrufen.

> Nur mit der Option Alle Protokolle versendete Protokolle können als ZIP-Datei heruntergeladen werden.

Letzter Check-in von Bridge

In der Spalte "Letzter Check-in von Bridge" der Geräteseite wird das Datum und die Uhrzeit aufgeführt, zu der sich der Bridge Service zuletzt angemeldet hat. Die Spalte kann über die Option "Spalten anpassen" zur Geräteseite hinzugefügt werden. Sie wird standardmäßig nicht angezeigt.

Um diese Spalte einzublenden, wählen Sie **Geräte** > **Spalten anpassen** > **Bridge Check-in** aus.

> In den exportierten Daten sind auch die Details zum letzten Check-in von Bridge enthalten, falls zutreffend.

Wiederherstellung nach Ausfall des Bridge-Dienstes

Die Wiederherstellung nach einem Bridge-Serviceausfall wurde mit Bridge-Version 2.1.14 eingeführt. Standardmäßig wird diese Version für alle Benutzer in den App-Katalog importiert. In seltenen Fällen kann es vorkommen, dass der Bridge Service ohne erkennbaren Grund stoppt. In derartigen Fällen steht ab Bridge 2.1.14 Support zur Verfügung.

9. Inhalt

Verwenden Sie die Content-Seite, um Content zu verteilen, die auf einer externen Quelle gehostet werden. Der Content kann Dateien umfassen, welche die Benutzer herunterladen können, z. B. Verkaufspräsentationen, Bilder, Tabellenkalkulationen und Dokumente.

Dieser Abschnitt enthält die folgenden Themen:

- Inhalte verwalten
- Kategorien

9.1. Inhalte verwalten

Dieser Abschnitt enthält die folgenden Themen:

- Gehosteten Content verteilen
- Content löschen

Gehosteter Content unterstützt die Verteilung von Inhalten, die über externe URLs heruntergeladen werden können. Die externe URL sollte nur zu herunterladbaren PDF-, EPUB- oder IBOOK-Dateien führen und die externe URL muss diese Erweiterung besitzen.

Die Verteilung von VPP-Buchlizenzen wird nicht unterstützt; daher wird auch die Verteilung von Apple Books anhand der iTunes Store-ID nicht unterstützt.

Greifen Sie über die Books- oder Pages-App, die sich auf dem Gerät befindet, auf den aus der Cloud übertragenen Content zu. Sie stehen im Abschnitt „Bibliothek“ zur Verfügung.

Content für iBook und EPUB können Sie an iPads und Geräte mit iOS 8+ verteilen (Gold-Lizenz). Diese Formate sind auf das iPad beschränkt, weil Apple die interne Verteilung dieser Formate nur beim iPad unterstützt. Die Beschränkung gilt nicht für Geräte mit iOS 9.

> Eine Inhaltsvorschau ist für diese Formate nicht verfügbar.

Bei **PDF**-Content haben Sie die Möglichkeit, das Dokument nach dem Push-Verfahren in die iBook-App bei Geräten mit iOS 8+ zu übertragen.

Gehosteten Content verteilen

Sie können zwar keine neuen Dokumente in die Ivanti Neurons for MDM hochladen, aber einen Pfad (URL) zu dem Host angeben, wo der Inhalt gespeichert wird, und an die Gerätegruppen verteilen.

Verfahren

1. Gehen Sie zu **Content > Gehosteter Content**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie folgende Informationen ein:
    - Titel
    - Autor
    - Kategorie
    - (Optional) Beschreibung
4. Geben Sie in das Feld **Gehosteter Content-Pfad** eine URL für die Datei ein, die Sie hochladen möchten.
5. Klicken Sie auf **Weiter**.
6. Nehmen Sie nötige Änderungen an der Verteilung vor.
7. Klicken Sie auf **Fertig**.

Um gehosteten Content zu ändern, muss der bisherige Content gelöscht werden, neuer gehosteter Content hinzugefügt und verteilt werden.

Andere Einstellungen als die URL modifizieren:

1. Gehen Sie zu Content > Gehosteter Content.
2. Klicken Sie in der Spalte **Name** auf den Link zum Dokument.
3. Klicken Sie auf das Symbol [Edit].
4. Nehmen Sie die nötigen Änderungen vor.
5. Klicken Sie auf **Weiter**.
6. Nehmen Sie nötige Änderungen an der Verteilung vor.
7. Klicken Sie auf **Fertig**.

Content löschen

1. Klicken Sie in der Spalte **Name** auf den Link zum Dokument.
2. Wählen Sie **Aktionen > Dieses Dokument löschen**.
3. Klicken Sie zur Bestätigung auf „Weiter“.
4. Klicken Sie auf „Dokument löschen“.

Wenn Sie ein Dokument löschen:

- wird es aus dem System gelöscht.
- steht es nicht länger im Content-Katalog zur Verfügung.
- wird es von allen Geräten gelöscht, auf denen es vorher heruntergeladen wurde.

Wenn Sie keine Aufgaben auf der Seite **Content** ausführen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie benötigen folgende **Rolle**:

- Verwaltung von Apps und Inhalten

9.2. Kategorien

Dieser Abschnitt enthält die folgenden Themen:

- Kategorie hinzufügen
- Kategorie entfernen

> Mit dem am 15. April 2017 angekündigten Ende des Supports für Content wurde die Möglichkeit zur Ergänzung von neuem Content deaktiviert. Derzeit hochgeladener Content kann weiter an die App Apple iBooks verteilt und verwendet werden.

Kategorien beschreiben die Arten des Contents im Content-Katalog. Kategorien ermöglichen die Verwaltung von Inhalten, damit Benutzer bei Bedarf schnell finden, was sie brauchen. Jedem zum Inhaltskatalog hinzugefügten Objekt muss mindestens eine Kategorie zugewiesen sein.

Kategorie hinzufügen

Verfahren

1. Klicken Sie auf Hinzufügen (unten links).
2. Geben Sie den Kategorienamen ein. Bei den Kategorien wird nicht zwischen Groß- und Kleinschreibung unterschieden.
3. Klicken Sie auf **Speichern**.

Kategorie entfernen

Durch Klicken auf das X neben einer Kategorie können Sie die betreffende Kategorie entfernen.

Wenn Sie auf der Seite **Content (Content)** keine Aufgaben ausführen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie benötigen folgende Rolle:

- Verwaltung von Apps und Inhalten

10. Konfigurationen

Konfigurationen sind Sammlungen von Einstellungen, die Sie an Geräte senden. Sie können zum Beispiel Konfigurationen verwenden, um automatisch VPN-Einstellungen und Passcodeanforderungen auf den Geräten einzurichten. Die vorhandenen Konfigurationen für Ihr System sind auf der Konfigurationsseite aufgelistet.

Dieser Abschnitt enthält die folgenden Themen:

- Arbeiten mit Konfigurationen
- Konfiguration für das Benutzer-Selbstbedienungsportal erstellen
- Anpassbare Konfiguration
- Übertragen von SyncML via Push auf Geräte mit benutzerdefinierten Konfigurationen
- Konfiguration des Startbildschirm-Layouts
- Konfiguration der App-Kontrolle: Kontrolle der Apps, die auf dem Gerät installiert sind
- App-Benachrichtigungen - Konfiguration
- Export von Konfigurationen
- Prioritätenvergabe für Konfigurationen
- Konfigurationen verwalten

10.1. Arbeiten mit Konfigurationen

Dieser Abschnitt enthält die folgenden Themen:

- Konfigurationsanzeige filtern
- Konfiguration hinzufügen
- Konfiguration verteilen
- Langsamer Rollout von Konfigurationen
- Konfigurationen auf mehrere Geräte übertragen
- Konfigurationen ausschließen
- Ausgeschlossene Konfiguration übertragen
- Konfigurationen exportieren
- Importieren von Konfigurationen
- Bearbeiten einer Konfiguration
- Löschen von Konfigurationen
- Interne Anwendungsaktualisierungen planen
- Windows-Konfigurationen, die eine aktive Benutzersitzung erfordern

-Konfigurationen sind Sammlungen von Einstellungen, die Sie als Administrator an Geräte senden. Sie können zum Beispiel Konfigurationen verwenden, um automatisch VPN-Einstellungen und Passcodeanforderungen auf den Geräten einzurichten. Die vorhandenen Konfigurationen für Ihr System sind auf der Konfigurationsseite aufgelistet. Sie können mehrere Konfigurationen auf der Seite "Konfigurationen" auswählen und via Push gleichzeitig auf mehrere Geräte übertragen. Diese Konfigurationen können via Push an Geräte in ausgewählten Spaces übertragen werden, ohne die in anderen Spaces zu beeinträchtigen. Konfigurationen können auf einem einzelnen Space, auf mehrere oder auf allen Spaces gleichzeitig bereitgestellt werden.

Configuration_types.htmEs stehen viele Konfigurationstypen zur Verfügung. Diese fallen unter die folgenden grundlegenden Kategorien:

- Sicherheit
- Benutzerressourcen
- Zugriff auf Unternehmensnetzwerk
- Mobilfunknetz
- Sonstige (weitere Konfigurationen)

Sie können für die meisten Konfigurationen folgende Aktionen durchführen:

- Hinzufügen
- Bearbeiten
- Klonen
- Löschen
- Schließen Sie eine oder mehrere Konfigurationen bei einem bestimmten Gerät aus.
- Übertragen Sie per PUSH eine oder mehrere ausgeschlossene Konfigurationen auf ein bestimmtes Gerät.

Bei bestimmten Konfigurationen existieren Einschränkungen der Aktionen:

- Manche Konfigurationen können nicht ergänzt oder geklont werden. Die iOS-Aktivierungssperre ist ein Beispiel für eine solche Konfiguration. Diese Konfigurationen erscheinen daher nicht unter den Kacheln, die beim Hinzufügen einer Konfiguration aufgelistet werden. Diese Konfigurationen werden nur auf der Konfigurationsseite aufgelistet.
- Systemdefinierte Konfigurationen können Sie nicht bearbeiten oder löschen. SCEP für iOS Enrollment ist ein Beispiel für eine solche Konfiguration.
- Manche Konfigurationen können zwar markiert, aber nicht von einem Gerät gelöscht bzw. nicht neu installiert werden. Solche Konfigurationen können nicht ausgeschlossen und nicht auf per PUSH auf das Gerät übertragen werden.

Konfigurationsanzeige filtern

Wenn Sie die Seite **Konfigurationen** anzeigen, werden alle Konfigurationen aufgelistet. Verwenden Sie die Filter (linker Bereich) unter OS und Konfigurationstyp, um diese Liste auf bestimmte Konfigurationen einzuschränken. Um zum Beispiel die Liste einzugrenzen und nur die macOS-Konfigurationen anzuzeigen, wählen Sie **macOS** im Abschnitt **OS**.

Sie können die Konfiguration für alle oder mehrere Space-Geräte anzeigen, indem Sie mehrere Spaces in der Dropdown-Liste auswählen. Wenn Sie den Mauszeiger über den angezeigten Konfigurationen bewegen, wird ein Popup-Fenster mit einer Liste von Spaces angezeigt. Sie können auf einen Space klicken, um die Seite mit den Konfigurationsdetails anzuzeigen.

Wenden Sie den Filter **Unterstützt** unter **Apple DDM** an, um DDM-bezogene Konfigurationen einfacher zu identifizieren und von anderen Konfigurationstypen zu unterschieden.

Um eine vorhandene Konfiguration anhand ihres Namens zu suchen, geben Sie den Konfigurationsnamen in das **Suchfeld** ein.

Ab Ivanti Neurons for MDM Release 81 können globale Administratoren Space-Administratoren mit der Bearbeitung des dynamisch generierten Identitätszertifikats für alle Geräte und für die Option zur benutzerdefinierten Verteilung beauftragen.

Konfiguration hinzufügen

Diese Option ist nur aktiviert, wenn in der Dropdown-Liste ein einzelner Space ausgewählt ist.

> Sie können bis zu 100 Konfigurationsdateien auf einmal verteilen.

Verfahren

1. Klicken Sie aufHinzufügen.
2. Wählen Sie den Konfigurationstyp aus, den Sie erstellen möchten.
3. Klicken Sie auf **Weiter**.
4. Wenn Sie die Konfiguration nicht sofort vornehmen wollen, löschen Sie die Option **Diese Konfiguration aktivieren**.
5. Wählen Sie eine Verteilungsebene für die Konfiguration:
    - **Alle Geräte** – verteilt die Konfiguration an alle verfügbaren Geräte. Um Konfigurationen für Spaces zu delegieren, wählen Sie eine der folgenden Optionen aus:
        - **Nicht für andere Spaces übernehmen**.
        - Um Konfigurationen für Spaces zu delegieren, klicken Sie auf **Verteilungsübersicht** > **Für Geräte in anderen Spaces übernehmen**.
            - Aktivieren Sie das Kontrollkästchen **Space Admin zur Bearbeitung der Verteilung zulassen**, um den delegierten Space-Administratoren die Bearbeitung der Verteilung für den jeweiligen Space zu ermöglichen.
    - **Keine Geräte** – Wählen Sie diese Konfiguration, wenn die Verteilung später erfolgen soll.

- **Benutzerdefiniert** - Definieren Sie eine bestimmte Gruppe von Geräten, an die diese Konfiguration gesendet werden soll. Um Konfigurationen für Spaces zu delegieren, wählen Sie eine der folgenden Optionen aus:
  - **Nicht für andere Spaces übernehmen**.
  - **Verteilungsübersicht** > **Auf Geräte in anderen Spaces anwenden**.
    - Aktivieren Sie das Kontrollkästchen **Space Admin zur Bearbeitung der Verteilung zulassen**, um den delegierten Space-Administratoren die Bearbeitung der Verteilung für den jeweiligen Space zu ermöglichen.

  > Der Administrator kann die Option zur benutzerdefinierten Verteilung verwenden, um die benutzerdefinierte Konfiguration an Geräte, Gerätegruppen, Benutzer und Benutzergruppen zu verteilen. Die Konfigurationszuweisung oder -verteilung an Benutzer oder Benutzergruppen ist für die folgenden Konfigurationen nicht verfügbar:

  - Android Enterprise: Arbeitsprofil (Android for Work)
  - Android Enterprise: Vom Unternehmen verwaltetes Gerät (Android for Work)
  - Android Enterprise: Verwaltetes Gerät mit Arbeitsprofil/Arbeitsprofil auf firmeneigenem Gerät
  - Android Work Managed-Geräte (Geräteeigentümer) und Work Managed-Geräte, nicht GMS-Modus (AOSP)

6. Wenn für Ihren Dienst Geräte-Spaces definiert sind, müssen Sie festlegen, ob und mit welcher Priorität die Konfiguration auch für die anderen Spaces verwendet werden soll.
7. Klicken Sie auf **Fertig**.

> Bei Konfigurationen, die einen Befehl für das Gerät eingeben, statt ein Profil auf dem Gerät zu installieren, listen die Konfigurationsdetails die Konfiguration für andere Geräte nicht auf.

Konfiguration verteilen

Globale Administratoren können Space-Administratoren zur Bearbeitung des dynamisch generierten Identitätszertifikats für alle Geräte und für die Option zur benutzerdefinierten Verteilung delegieren. Für die dynamisch erzeugten Zertifikate können Sie bei Bedarf die Option **Diese Konfiguration in allen Spaces verfügbar machen** auswählen. Mit dieser Option werden dynamisch erzeugte Identitätszertifikate allen Spaces zur Verfügung gestellt. Diese können damit in Exchange, WLAN, VPN und anderen geeigneten Konfigurationen, beispielsweise verwalteten App-Konfigurationen, genutzt werden. Diese Option eignet sich für Szenarien, in denen das dynamisch erzeugte Identitätszertifikat nur auf Geräte (in Nicht-Standard-Spaces) als Teil der zugeordneten Konfigurationen verteilt werden muss und nicht als Einzelkonfiguration.

Verfahren

1. Spezifizieren Sie die Einstellungsfelder anhand der Informationen der Tabelle für die jeweilige Konfiguration nach Bedarf.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie die Option **Diese Konfiguration aktivieren**.
4. (Optional) Wählen Sie **Diese Konfiguration in allen Spaces zur Verfügung stellen**.
5. Wählen Sie eine der folgenden Verteilungsoptionen aus:
   - **Alle Geräte** . Wählen Sie eine der folgenden Optionen aus:
     - **Nicht für andere Spaces übernehmen**.
     - **Auf Geräte in anderen Spaces anwenden**.

        - **Für alle Geräte in anderen Geräte-Spaces als höchste Priorität übernehmen**. (Dies gilt nur für die WLAN-Konfiguration.)
        - **Für alle Geräte in anderen Geräte-Spaces als geringste Priorität übernehmen**. (Dies gilt nur für die WLAN-Konfiguration.)
            - Aktivieren Sie das Kontrollkästchen **Space Admin zur Bearbeitung der Verteilung zulassen**, um den delegierten Space-Administratoren die Bearbeitung der Verteilung für den jeweiligen Space zu ermöglichen.
    - **Keine Geräte** (Standard)
    - **Benutzerdefiniert** Wählen Sie eine der folgenden Optionen aus:
        - **Nicht für andere Spaces übernehmen**.
        - **Auf Geräte in anderen Spaces anwenden**.
        - **Für alle Geräte in anderen Geräte-Spaces als höchste Priorität übernehmen**. (Dies gilt nur für die WLAN-Konfiguration.)
        - **Für alle Geräte in anderen Geräte-Spaces als geringste Priorität übernehmen**. (Dies gilt nur für die WLAN-Konfiguration.)
            - Aktivieren Sie das Kontrollkästchen **Space Admin zur Bearbeitung der Verteilung zulassen**, um den delegierten Space-Administratoren die Bearbeitung der Verteilung für den jeweiligen Space zu ermöglichen.

> Unabhängig von Spaces kann das dynamisch generierte Identitätszertifikat für alle Spaces konfiguriert, an alle Geräte verteilt und für alle Geräte in anderen Geräte-Spaces übernommen werden.

6. Klicken Sie auf **Fertig**.

Langsamer Rollout von Konfigurationen

Beim Verteilen von Konfigurationen mit der Option **Benutzerdefiniert** können Sie die Konfigurationen mithilfe des langsamen Rollout-Prozesses verteilen, sodass die Konfigurationen nach einem bestimmten Zeitplan bereitgestellt werden. Sie können den langsamen Rollout von Verteilungen entweder manuell oder nach Zeitplan durchführen.

> Der langsame Rollout von Verteilungen wird derzeit nur für VPN- und WLAN-Konfigurationen unterstützt.

Verfahren

1. Wechseln Sie zu **Konfigurationen** > **Hinzufügen**.
2. Machen Sie die gewünschte Konfiguration ausfindig.
3. Geben Sie die Details ein wie **Name**, **Beschreibung** usw. je nach Konfiguration und klicken Sie auf **Weiter**.
4. Wählen Sie **Benutzerdefiniert** als Verteilungsoption aus. Der Abschnitt **Langsamer Rollout** wird angezeigt.
5. Wählen Sie **Langsame Verteilungsmethode für die Bereitstellung verwenden** aus. Die Optionen **Manueller Rollout** und **Geplanter Rollout** werden angezeigt.
    - **Manueller Rollout** – Mit dieser Option können Sie den Prozentsatz des Verteilungsziels manuell festlegen. Es wird nur der angegebene Prozentsatz der Verteilung durchgeführt. Alternativ können Sie **Alle Geräte in der Auswahlübersicht** auswählen , um die Konfiguration an alle Geräte zu verteilen.
    - **Geplanter Rollout** – Verwenden Sie diese Option, um die Verteilung in vier Phasen bereitzustellen. Sie können für jede Phase den Rollout-Prozentsatz angeben, wobei jede nachfolgende Phase einen höheren Prozentsatz als die vorherige aufweisen

muss. Die Dauer zwischen den Phasen muss zwischen 1 Tag und 30 Tagen liegen. Die zuletzt gespeicherte Konfiguration wird automatisch als editierbare Vorlage für zukünftige Konfigurationen vorinstalliert.

6. Wählen Sie die gewünschten Gruppen aus, an die die Konfiguration verteilt werden soll.
7. Klicken Sie auf **Fertig**.

Sie können die Details unter **Konfigurationen** > Neu erstellte Konfiguration > **Details** anzeigen. Auf der Seite "Details" können Sie den Rollout pausieren und fortsetzen.

> Wenn Sie eine neue Konfiguration mit geplantem Rollout erstellen, werden die Prozentsätze, die Sie beim Erstellen der vorhandenen Konfiguration angegeben haben, auf die neue übertragen. Sie können die Details bearbeiten oder mit den gleichen Prozentsätzen fortfahren.

Konfigurationen auf ein Gerät übertragen

Wenn Sie ausgeschlossene Konfigurationen auf einem Gerät neu installieren wollen, übertragen Sie die Konfigurationen per Push.

Verfahren

1. Gehen Sie zu **Geräte** > **Geräte**.
2. Klicken Sie auf einen Gerätenamen, um die Seite mit den Details aufzurufen.
3. Gehen Sie zu **Konfigurationen**.
4. Aktivieren Sie die Kontrollkästchen für die entsprechenden Konfigurationen, die auf das Gerät übertragen werden sollen.
5. Klicken Sie auf **Profile per Push übertragen**.
6. Um eine Einzelkonfiguration per Push zu übertragen, klicken Sie in der Spalte **Aktionen** auf **Push**.

Konfigurationen auf mehrere Geräte übertragen

Sie können mehrere Konfigurationen auf der Seite „Konfigurationen“ auswählen und gleichzeitig auf mehrere Geräte übertragen.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administratorportal an.
2. Gehen Sie zu **Konfigurationen**.
3. Aktivieren Sie die Kontrollkästchen für die entsprechenden Konfigurationen.
4. Klicken Sie auf **Aktionen** und wählen Sie **Ausgewählte Konfigurationen per Push auf Geräte übertragen**. Der Assistent für die Push-Übertragung von Konfigurationen wird geöffnet und alle Konfigurationen werden zusammen mit ihrem Push-Status angezeigt.
5. Klicken Sie auf **Gültige Konfiguration(en) per Push übertragen**. Die Konfigurationen werden in einem Massenvorgang per Push auf alle Geräte übertragen. Konfigurationen, die auf der Registerkarte **Geräte** > **Konfigurationen** für bestimmte Geräte ausgeschlossen wurden, werden nicht übertragen.

Konfigurationen ausschließen

Bestimmte, zuvor verteilte Konfigurationen können Sie manuell von dem Gerät entfernen, indem Sie sie ausschließen.

Verfahren

1. Gehen Sie zu **Geräte** > **Geräte**.

2. Klicken Sie auf einen Gerätenamen, um die Seite mit den Details aufzurufen.
3. Gehen Sie zu **Konfigurationen**.
4. Aktivieren Sie die Kontrollkästchen für die entsprechenden Konfigurationen.
5. Klicken Sie auf **Profile ausschließen**.

Um eine Einzelkonfiguration auszuschließen, klicken Sie in der Spalte **Aktionen** auf **Ausschließen**. Die ausgewählten Konfigurationen werden auf der Registerkarte „Ausgeschlossene Konfigurationen“ angezeigt.

Ausgeschlossene Konfiguration übertragen

Verfahren

1. Gehen Sie zu **Geräte** > **Geräte**.
2. Klicken Sie auf einen Gerätenamen, um die Seite mit den Details aufzurufen.
3. Gehen Sie zu **Konfigurationen** > **Ausgeschlossene Konfigurationen**.
4. Wählen Sie eine oder mehrere Konfigurationen aus, die Sie per Push auf das Gerät übertragen wollen.
5. Klicken Sie auf **Profile per Push übertragen**.
6. Um eine Einzelkonfiguration per Push zu übertragen, klicken Sie in der Spalte **Aktionen** auf **Push**.

Konfigurationen exportieren

Sie können die Details ausgewählter Konfigurationen oder auch alle Konfigurationen aus ausgewählten Spaces in einzelne Dateien exportieren

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Aktivieren Sie die Kontrollkästchen für die entsprechenden Konfigurationen.
3. Klicken Sie auf **Aktionen** > **Ausgewählte Konfigurationen mit Details exportieren**. Wenn Sie alle Konfigurationen exportieren möchten, wählen Sie **Alle Konfigurationen mit Details exportieren**.
   Eine Reihe von YAML-Dateien wird in einer ZIP-Datei gespeichert. Der Bericht enthält Details zu allen vorhandenen Konfigurationen in den ausgewählten Spaces.

Exportieren aller Konfigurationen

Exportieren Sie Ihre Konfigurationsdateien, um diese als Diagnosehilfe an den Support zu senden. Sie können eine einzelne Konfigurationsdatei als YAML-Datei oder all Ihre Konfigurationen als ZIP-Datei exportieren. Sie können Dateien aus verschiedenen Bereichen der Konfigurationsseite exportieren, je nachdem, welche Konfigurationen Sie exportieren wollen.

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Aktivieren Sie die Kontrollkästchen für die entsprechenden Konfigurationen.
3. Klicken Sie auf **Aktionen** > **Ausgewählte Konfigurationen mit Details exportieren**. Wenn Sie alle Konfigurationen exportieren möchten, wählen Sie **Alle Konfigurationen mit Details exportieren**.
   Eine Reihe von YAML-Dateien wird in einer ZIP-Datei gespeichert. Der Bericht enthält Details zu allen vorhandenen Konfigurationen in den ausgewählten Spaces.

Exportieren einer benutzerdefinierten Konfiguration

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**, um eine Konfiguration auszuwählen.
3. Folgen Sie den Schritten zur Anpassung der Konfiguration.
4. Klicken Sie auf **Weiter**.
5. Wählen Sie eine Verteilungsebene.
6. Klicken Sie auf **Fertig**.
7. Wählen Sie die Konfiguration aus, die Sie gerade aus der Liste auf der Seite **Konfiguration** erstellt haben.
8. Klicken Sie auf das Pull-Down-Menü **Aktionen** und dann auf **Export.**

Eine Datei mit dem Namen der Konfiguration und einem Zeitstempel _yyyymmdd.yaml wird heruntergeladen.

Exportieren einer vorhandenen Konfiguration

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Wählen Sie eine vorhandene Konfiguration aus.
3. Klicken Sie auf das Pull-Down-Menü **Aktionen** und dann auf **Exportieren**.
   Eine Datei mit dem Namen der Konfiguration und einem Zeitstempel _yyyymmdd.yaml wird heruntergeladen.

Importieren von Konfigurationen

Sie haben die Möglichkeit, eine YAML-Datei zu importieren, in der die Konfigurationsdetails enthalten sind. Zum Bearbeiten einer Konfiguration können Sie die Details in der YAML-Datei bearbeiten, eine Konfiguration auswählen und die Datei importieren. Die aktualisierten Werte werden in der Konfiguration angezeigt. Werden mehrere Konfigurationen oder Spaces ausgewählt, wird die Schaltfläche zum Importieren deaktiviert. Wird ein falscher Dateityp ausgewählt, wird eine Fehlermeldung angezeigt. Wenn Sie eine YAML-Datei auswählen, die andere Details enthält als für die Konfiguration erforderlich, wird eine Fehlermeldung angezeigt.

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Wählen Sie eine Konfiguration aus, klicken Sie auf **Importieren** und dann auf **Datei wählen**, wählen Sie die YAML-Datei aus und klicken Sie anschließend auf **Importieren**. Die YAML-Datei mit den Konfigurationsdetails wird importiert.

Unterstützte Whitelist-Konfigurationen

- CERTIFICATE
- VPN
- WEBCLIP
- IDENTITY_CERTIFICATE_DG
- RESTRICTIONS
- ANDROID_WORK_DEVICE_OWNER_LOCKDOWN

- PASSCODE
- HOME_SCREEN_LAYOUT
- ANDROID_ADVANCED_PASSCODE_AND_LOCK_SCREEN
- IOS_APP_CONTROL
- SCEP
- ANDROID_SAMSUNG_SAFE_LOCKDOWN
- ANDROID_WORK_DEVICE_OWNER_WITH_WORK_PROFILE_LOCKDOWN
- ANDROID_WORK_LOCKDOWN
- DEVICE_NAME
- MOBILE_THREAT_DEFENSE
- PRIVACY
- APP_LOCK
- GOOGLE_ACCOUNT
- ANDROID_WORK_APP_RUNTIME_PERMISSION
- IDENTITY_PREFERENCE
- MAC_OS_AGENT
- MANAGED_GOOGLE_PLAY
- ANDROID_MI_TUNNEL
- ANDROID_ENCRYPTION
- ANDROID_APP_CONNECT
- APPCONNECT_DEVICE_SETTINGS
- ANDROID_WORK_DEVICE_OWNER_SYSTEM_UPDATE
- DOMAINS
- END_USER_PRIVACY
- EXCHANGE
- MI_CLIENT_PRIVACY
- APP_UPDATE_SCHEDULE
- ZERO_PASSWORD
- WINDOWS_PRINTER
- PRINTING
- AUTH_ONLY
- SAFETYNET
- OSX_RESTRICTIONS
- WATCH_OS_RESTRICTIONS
- VISION_OS_RESTRICTIONS
- ANDROID_APP_CONTROL
- WINDOWS_APP_CONTROL

- ANDROID_SAMSUNG_PHONE_RESTRICTIONS
- Mobile Application Management (MAM)
- ANTI_PHISHING
- SETUP_ASSISTANT
- DNS_SETTINGS
- WINDOWS_KIOSK
- FIDO_AGENT
- WINDOWS_BITLOCKER
- WINDOWS_DEVICE_ADMIN_RESTRICTIONS
- TELECOM_SETTINGS
- IDENTITY_CERTIFICATE_UP
- IDENTITY_CERTIFICATE_DC
- WIFI
- NOTIFICATIONS
- WEB_CONTENT_FILTER
- WINDOWS_AI_MANAGEMENT
- WINDOWS_ENERGY_SAVER
- WINDOWS_BROWSER
- WINDOWS_DESKTOP
- WINDOWS_PHONE_RESTRICTIONS
- WINDOWS_UPDATE
- WINDOWS_GPO_ADMX
- WINDOWS_LICENSE
- WINDOWS_ATP
- WINDOWS_LAPS
- WINDOWS_EDP
- WINDOWS_BIOS
- WINDOWS_BLOATWARE_REMOVER
- WINDOWS_HELLO
- WINDOWS_START_MENU

Erstellen einer Konfiguration unter Verwendung einer YAML-Datei

Sie können eine Konfiguration über eine YAML-Datei erstellen. Die Angaben zur Verteilung sind nicht Bestandteil der YAML-Datei. Die Verteilung ist standardmäßig auf "Keine Geräte" gesetzt.

Verfahren

1. Gehen Sie zu **Konfigurationen**.

2. Klicken Sie auf **Importieren** und dann auf **Datei wählen**, wählen Sie die YAML-Datei aus und klicken Sie anschließend auf **Importieren**. Die YAML-Datei mit den Konfigurationsdetails wird importiert. Die Seite "Konfiguration erstellen" wird mit allen Details geöffnet, die der YAML-Datei hinzugefügt wurden.
3. Wählen Sie *einen* der folgenden Verteilungstypen aus:
    - **Alle Geräte**
    - **Keine Geräte**
    - **Anpassbar**
4. Überprüfen Sie die Details der Konfiguration und wählen Sie *eine* der folgenden Optionen für die Verteilungsübersicht aus:

> Die Verteilungsübersicht ist nicht für alle Konfigurationen verfügbar.

    - **Nicht auf andere Spaces anwenden**
    - **Auf Geräte in anderen Spaces anwenden**
5. Stimmt der neue Name der Konfiguration mit dem Namen einer bereits vorhandenen Konfiguration überein, wird eine Fehlermeldung angezeigt. Klicken Sie auf **OK** und dann auf **Zurück** und bearbeiten Sie den Namen der Konfiguration.
6. Klicken Sie auf **Weiter** und dann auf **Fertig**.

Bearbeiten einer Konfiguration

Sie können eine Konfiguration öffnen und deren Details direkt bearbeiten oder aber eine YAML-Datei mit den benötigten Details importieren. Werden mehrere Konfigurationen oder Spaces ausgewählt, wird die Schaltfläche zum Importieren deaktiviert.

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Wählen Sie eine Konfiguration aus, öffnen Sie sie, klicken Sie auf das Bearbeitungssymbol (Stift) und bearbeiten Sie die Konfiguration.
3. Klicken Sie alternativ auf der Seite für die Konfigurationsbearbeitung auf das Symbol **Importieren**, wählen Sie die YAML-Datei aus und klicken Sie auf **Importieren**. Die Seite "Konfiguration bearbeiten" wird mit allen Details geöffnet, die der YAML-Datei hinzugefügt wurden.
4. Überprüfen Sie die Details der Konfiguration und wählen Sie eine der folgenden Optionen für die Verteilungsübersicht aus:

> Die Verteilungsübersicht ist nicht für alle Konfigurationen verfügbar.

    - **Nicht für andere Spaces übernehmen**.
    - **Auf Geräte in anderen Spaces anwenden**

        > Die Verteilung ist standardmäßig auf "Keine Geräte" gesetzt.
5. Klicken Sie auf **Fertig**.

Löschen von Konfigurationen

Sie haben die Möglichkeit des Löschens ausgewählter Konfigurationen.

Verfahren

1. Aktivieren Sie die Kontrollkästchen für die entsprechenden Konfigurationen.
2. Wählen Sie **Aktionen** > **Löschen**.

Interne Anwendungsaktualisierungen planen

Ivanti Neurons for MDM aktualisiert interne Anwendungen automatisch, wenn ein Gerät eincheckt. Administratoren können jetzt interne Anwendungsupdates basierend auf der Serverzeitzone planen. Die Anwendung wird nur dann aktualisiert, wenn das Gerät innerhalb der geplanten Zeit eincheckt. Standardmäßig ist die Planung von Anwendungsaktualisierungen deaktiviert.

> Diese Konfiguration gilt nur für Updates und nicht für eine Neuinstallation. Sie können mit dem Befehl Installation/Aktualisierung senden den Zeitplan für die automatische Aktualisierung von iOS-Anwendungen außer Kraft setzen. Falls "Automatisch aktualisieren" auf App- oder Katalog-Ebene aktiviert wurde, hat diese Einstellung Vorrang gegenüber der Konfiguration für geplante Apps und die App wird unmittelbar nach dem Einchecken aktualisiert.

Die Konfiguration ist nur für folgende App-Typen anwendbar:

- Interne iOS-Apps.
- Interne Android-Apps, die sich nur im DO-Modus befinden.
- macOS-Anwendungen im PKG- oder MIP-Format.
- Windows-Anwendungen.

Voraussetzungen

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind, damit die Konfiguration wie erwartet funktioniert:

- Die Anwendung muss für iOS und Android verwaltet werden. Unter macOS kann sich die Anwendung entweder im verwalteten oder im nicht verwalteten Zustand befinden.
- Stellen Sie sicher, dass die Option „Auf dem Gerät installieren“ in der App-Konfiguration aktiviert ist.
- Das Gerät muss während der vorgesehenen Zeit angemeldet werden.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administratorportal an.
2. Gehen Sie zu **Konfigurationen**.
3. Klicken Sie auf **Hinzufügen**. Die Seite „Konfiguration hinzufügen“ wird geöffnet.
4. Suchen Sie nach **App Auto Update**. Die Konfigurationsseite „Automatische App-Aktualisierung erstellen“ wird geöffnet.
5. Geben Sie einen Namen in dem Feld **Name** ein.
6. Wählen Sie im Abschnitt **Konfiguration-Setup** die **Zeitzone** aus der Dropdown-Liste aus.
7. Wählen Sie die **Startzeit** in der Dropdown-Liste und dann die **Dauer** in der Dropdown-Liste aus.
8. Klicken Sie auf **Weiter**.
9. Wählen Sie die gewünschte Benutzer- und Gerätegruppe aus und klicken Sie dann auf das Kontrollkästchen **Diese Konfiguration aktivieren**.
10. Klicken Sie auf **Fertig**. Die Konfiguration wird übernommen, die Anwendung wird nun nur noch nach dem angegebenen Zeitplan aktualisiert.

Wenn Sie die Seite „Konfigurationen“ nicht sehen können, kann es sein, dass Sie nicht über die erforderlichen Berechtigungen verfügen. Sie brauchen eine der folgenden **Rollen**:

- Geräteverwaltung
- Geräts schreibgeschützt

Verwandte Themen:

- Räume
- Konfigurationen priorisieren

Windows-Konfigurationen, die eine aktive Benutzersitzung erfordern

Einige Windows-Konfigurationen erfordern eine aktive Benutzersitzung (ein Benutzer, der sich am Gerät angemeldet hat), damit sie bereitgestellt werden können. Wenn gerade kein Benutzer angemeldet ist, werden diese Konfigurationen angewendet, sobald sich ein MDM-Benutzer am Gerät anmeldet.

Die folgenden Konfigurationen erfordern eine aktive Benutzersitzung:

- Passwort
- Benutzerzertifikat (Identitätszertifikat im Benutzerbereich)
- Windows-Firewall
- [Exchange]
- VPN
- Windows-Lizenz
- Microsoft Defender for Endpoint
- Windows-Einstellungen (Benutzerbereich)
- Vom Bridge-Dienst abhängige Konfigurationen
- Moderne/UWP-Anwendungen

Vom Bridge-Dienst abhängige Konfigurationen

Konfigurationen, die den Ivanti Bridge-Dienst erfordern, werden nur bereitgestellt, wenn eine aktive Benutzersitzung verfügbar ist. Beispiele hierfür sind Windows Desktop-Einschränkungen, Browsereinstellungen, Startmenü, Kiosk, BIOS, Windows-Skripte, GPO und andere vom Bridge-Dienst abhängige Konfigurationen.

Ausnahme: Die folgenden Standard-Bridge-Skripte erfordern keine aktive Benutzersitzung und werden unabhängig davon, ob ein MDM-Benutzer angemeldet ist, an das Gerät gesendet:

- get-device-data.ps1
- get-bitlocker-status.ps1
- device-hardware.ps1

Moderne/UWP-Anwendungen

Moderne/UWP-Anwendungen werden nur bereitgestellt, wenn eine aktive Benutzersitzung verfügbar ist. Dazu gehören:

- Interne Anwendungen, die als .appx oder .appxbundle verpackt sind
- Microsoft Store/UWP-Anwendungen

Herkömmliche MSI- und EXE-Anwendungen unterliegen nicht dieser Anforderung.

Wenn eine erforderliche Benutzersitzung nicht verfügbar ist, wenn eine Konfiguration für die Bereitstellung geplant ist, dann wird die Konfiguration automatisch bereitgestellt, sobald sich ein MDM-Benutzer beim Gerät anmeldet.

10.2. Konfiguration für das Benutzer-Selbstbedienungsportal erstellen

Als Unternehmensbenutzer verwalten Sie im Selbstbedienungsportal Ihre Geräte und Zertifikate. Auf der Registerkarte „Meine Geräte“ werden die Geräte angezeigt, die Sie registriert haben.

Sie können die folgenden Aufgaben auf der Registerkarte „Meine Geräte“ durchführen:

- Sperren
- Entsperren
- Gerät löschen
- Secure Apps-Passcode zurücksetzen

Sie können die folgenden Aufgaben auf der Registerkarte „Meine Zertifikate“ durchführen:

- Zertifikat hochladen

> Sie können bis zu 100 Konfigurationsdateien auf einmal verteilen.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administratorportal an.
2. Klicken Sie aufHinzufügen.
3. Suchen Sie den Eintrag **Konfiguration für Benutzer-Selbstbedienungsportal erstellen**.
4. Klicken Sie auf **Weiter**.
5. Wenn Sie die Konfiguration nicht sofort vornehmen wollen, löschen Sie die Option **Diese Konfiguration aktivieren**.
6. Wählen Sie eine Verteilungsebene für die Konfiguration:
    - **Alle Geräte** – verteilt die Konfiguration an alle verfügbaren Geräte. Um Konfigurationen für Spaces zu delegieren, wählen Sie eine der folgenden Optionen aus:
        - **Nicht für andere Spaces übernehmen**.
        - Um Konfigurationen für Spaces zu delegieren, klicken Sie auf **Verteilungsübersicht** > **Für Geräte in anderen Spaces übernehmen**.
            - Aktivieren Sie das Kontrollkästchen **Space Admin zur Bearbeitung der Verteilung zulassen**, um den delegierten Space-Administratoren die Bearbeitung der Verteilung für den jeweiligen Space zu ermöglichen.
    - **Keine Geräte** – Wählen Sie diese Konfiguration, wenn die Verteilung später erfolgen soll.
    - **Benutzerdefiniert** - Definieren Sie eine bestimmte Gruppe von Geräten, an die diese Konfiguration gesendet werden soll. Um Konfigurationen für Spaces zu delegieren, wählen Sie eine der folgenden Optionen aus:
        - **Nicht für andere Spaces übernehmen**.
        - **Verteilungsübersicht** > **Auf Geräte in anderen Spaces anwenden**.
            - Aktivieren Sie das Kontrollkästchen **Space Admin zur Bearbeitung der Verteilung zulassen**, um den delegierten Space-Administratoren die Bearbeitung der Verteilung für den jeweiligen Space zu ermöglichen.
7. Wenn für Ihren Dienst Geräte-Spaces definiert sind, müssen Sie festlegen, ob und mit welcher Priorität die Konfiguration auch für die anderen Spaces verwendet werden soll.

8. Klicken Sie auf **Fertig**.

> Bei Konfigurationen, die einen Befehl für das Gerät eingeben, statt ein Profil auf dem Gerät zu installieren, listen die Konfigurationsdetails die Konfiguration für andere Geräte nicht auf.

10.3. Anpassbare Konfiguration

Dieser Abschnitt enthält die folgenden Themen:

- Definition einer benutzerspezifischen Konfiguration
- Einstellungen der anpassbaren Konfiguration

Lizenz: Silver

Gilt für: iOS, macOS, tvOS, Android und Windows

Beschreibung

Sie können eine vordefinierte Konfigurationsdatei importieren und verteilen.

Es sind folgende Konfigurationsdateiformate zulässig:

BETRIEBSSYSTEM	Gültige Konfigurationsdateiformate
iOS und tvOS	• .plist • .mobileconfig • .xml
macOS	• .plist • .mobileconfig
Android-	.xml. Zurzeit unterstützt diese Funktion nur die .xml-Konfigurationsdateien für Zebra-Geräte.
Windows	SyncML.

Definition einer benutzerspezifischen Konfiguration

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie in dem Suchfeld „custom“ ein, und klicken Sie dann auf die Konfiguration **Anpassbar**.
   Die Seite mit den Details der anpassbaren Konfiguration wird angezeigt.
4. Konfigurieren Sie die Einstellungen auf dieser Seite. Hinweise zu den Werten finden Sie in der Tabelle im Abschnitt Einstellungen der anpassbaren Konfiguration.
5. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
6. (macOS-Geräte): Wählen Sie eine zusätzliche Option für die Einstellung **Für wen gilt diese Konfiguration** entsprechend dem gewünschten Verhalten dieser Konfiguration aus:
   - Geräteweit (wird am häufigsten verwendet).
   - Benutzerspezifisch (für den derzeit registrierten Benutzer).

Klicken Sie auf **Fertig**.

Einstellungen der anpassbaren Konfiguration

Einstellung	So gehen Sie vor
[Name] Beschreibung	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet. Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Betriebssystem wählen	Klicken Sie auf ein Betriebssystemsymbol, um eine Konfigurationsdatei hochzuladen, die dem ausgewählten Symbol entspricht.
Datei auswählen	Diese Option wird angezeigt, wenn Sie ein Betriebssystem ausgewählt haben. Ziehen Sie eine Konfigurationsdatei in die Drag-and-Drop-Box oder klicken Sie auf die Schaltfläche **Datei auswählen**, um eine Konfigurationsdatei auszuwählen.

Benutzerdefinierte CSP-Konfiguration (nur Windows)

Eine benutzerdefinierte CSP-Konfiguration kann nur auf Windows-Geräten erstellt werden. Wenn Sie im Abschnitt für die Auswahl des Betriebssystems Windows auswählen, werden Ihnen zwei Optionen angeboten:

Option 1 – CSP XML-Datei – Wählen Sie diese Option aus und folgen Sie dem gleichen Prozess wie für die Einstellung **Datei wählen**.

Option 2 – Benutzerdefinierter CSP OMA-URI-Schemaknoten

Verfahren

1. Wählen Sie die Option "Benutzerdefinierter CSP OMA-URI-Schemaknoten" aus der Liste aus. Der Abschnitt "Benutzerdefinierte CSP-Konfiguration" wird im Bildschirm angezeigt.
2. Klicken Sie unter **AKTIONEN** auf die Schaltfläche mit dem Pluszeichen (+), um die Konfiguration mit anderen OMA-URI-Feldern zu starten.
3. Das Popup-Fenster **Zeile hinzufügen** wird mit den folgenden Feldern im Bildschirm angezeigt:
    - Beschreibung – Geben Sie allgemeine Informationen zur Einstellung ein.
    - OMA-URI – Geben Sie die OMA-URI ein, die Sie als Einstellung verwenden möchten.
    - Datentyp – Wählen Sie den Datentyp aus, den Sie für diese Einstellung verwenden möchten – DATUM, FLOAT, BASE64, KNOTEN, XML, BINÄR, ZEICHEN, UHRZEIT, BOOLESCH, GANZZAHL
    - Wert – Geben Sie einen Wert ein, der mit dem ausgewählten Datentyp verknüpft ist.
    - Zugriffstyp – Hinzufügen, Löschen, Ausführen, Ersetzen, Abrufen

Klicken Sie auf **Speichern und schließen**, um das Fenster mit den angegebenen Details zu schließen. Klicken Sie auf **Speichern und hinzufügen**, um eine neue Zeile zu erstellen.

5. Klicken Sie auf **Weiter**.
6. Wählen Sie den Verteilungsmodus aus und klicken Sie auf **Fertig**.

Verwandte Themen

- Übertragung von SyncML per Push auf Geräte mit benutzerspezifischer Konfiguration
- Erstellen einer Konfiguration

10.4. Übertragen von SyncML via Push auf Geräte mit benutzerdefinierten Konfigurationen

Sie können Konfigurationsdateien für die Synchronization Markup Language (SyncML) selbst erstellen oder von einem Dritten beziehen, um kundenspezifische Funktionen in einer anpassbaren Konfiguration zu ergänzen.

Unterstützte Plattformen:

- Windows

Unterstützte Geräte:

- Windows 10+
- Microsoft HoloLens 2

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie auf **Anpassbare Konfiguration,** um die Seite **Anpassbare Konfiguration erstellen** anzuzeigen.
4. Geben Sie einen Namen für die Konfiguration ein.
5. Klicken Sie auf das Symbol für das Windows-Betriebssystem.
6. Ziehen Sie mit Drag&Drop die SyncML-Datei in die Schnittstelle oder klicken Sie auf **Datei wählen**, um nach der Datei zu suchen, die Sie in das Gerät hochladen wollen.

> Cloud führt keine Validierungsprüfungen des Codes in der Datei durch.

7. Klicken Sie auf **Weiter**.

Benutzerdefiniertes SyncML-Protokoll

Die an das Windows-Gerät gesendeten SyncML-Befehle und die SyncML-Antworten des Geräts auf diese Befehle werden auf der Registerkarte "Geräteprotokolle" angezeigt. Diese Protokollinformationen sind verfügbar, nachdem die Konfiguration **Benutzerdefiniertes Windows-SyncML** gesendet wurde. Wenn das System eine benutzerdefinierte SyncML-Konfiguration sendet, lautet der Status der Konfiguration, der auf der Registerkarte "Konfiguration" des Geräts angezeigt wird, unabhängig von den SyncML-Antworten, immer "Installiert".

10.5. Konfiguration des Startbildschirm-Layouts

Die Startbildschirm-Layoutkonfiguration legt das Layout für die Apps, Ordner und Webclips auf dem Startbildschirm fest.

Dieser Abschnitt enthält die folgenden Themen:

- Definition einer Konfiguration für das Startbildschirm-Layout
- Einstellungen zur Konfiguration des Startbildschirm-Layouts

Lizenz: Silver

Geeignete Geräte:

- iOS 9.3+, nur auf überwachten Geräten
- tvOS nur auf überwachten Geräten

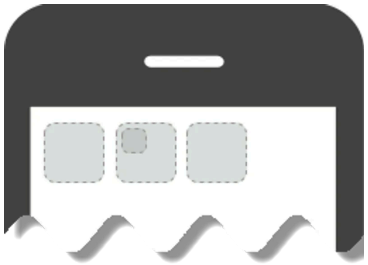
Definition einer Konfiguration für das Startbildschirm-Layout

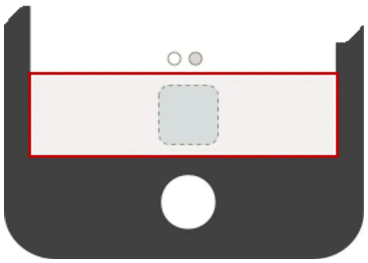
Verfahren

1. Gehen Sie zu **Konfigurationen** > **+ Hinzufügen**.
2. Geben Sie "Start" in das Suchfeld ein, und klicken Sie dann auf die Konfiguration **Startbildschirmlayout**. Die Detailseite "Konfiguration des Layoutbildschirms" wird angezeigt.
3. Konfigurieren Sie die Einstellungen auf dieser Seite. Hinweise zu den Werten finden Sie in der Tabelle im Abschnitt Einstellungen zur Konfiguration des Startbildschirm-Layouts.
4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren. Wählen Sie bei gemeinsam verwendeten iPad-Geräten den Kanal **Gerät** oder den Kanal **Benutzer** aus. Weitere Informationen finden Sie unter Arbeiten mit Konfigurationen.
5. Klicken Sie auf **Fertig**.

Einstellungen zur Konfiguration des Startbildschirm-Layouts

Einstellung	Aktion
[Name] Beschreibung	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet. Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Dock	Um eine App oder einen Webclip zum Startbildschirm hinzuzufügen (hier hervorgehoben), klicken Sie auf das Pluszeichen (+) und folgen den Anweisungen auf den nachfolgenden Bildschirmen: Sie können System-Apps durch das Eingaben der Apple-Bundle-ID manuell hinzufügen (beginnend mit "com.apple"). Geben Sie beispielsweise com.apple.DocumentsApp ein, wenn Sie die App "Files" ergänzen wollen.
Seite 1	Um eine App oder einen Webclip wie hier dargestellt zum Seitenbereich des Startbildschirms hinzuzufügen, Klicken Sie auf ⊕ und folgen den Anweisungen der folgenden Bildschirme: Wenn Sie auf "Seite hinzufügen" klicken, wird eine weitere Seite zur Telefonanzeige hinzugefügt.







10.6. Konfiguration der App-Kontrolle: Kontrolle der Apps, die auf dem Gerät installiert sind

Mit der Konfiguration der App-Kontrolle können Sie Apps auf Geräteebene als Whitelist oder Blacklist kategorisieren. Bereits installierte Apps werden ausgeblendet und können nicht gestartet werden. Apps sind im App Store weiter sichtbar, können jedoch nicht gestartet oder heruntergeladen werden. Jedes Gerät, an das diese Konfiguration verteilt wird, nutzt diese Konfiguration und ignoriert eventuelle Einstellungen der Richtlinie für zulässige Apps. Diese Konfiguration überschreibt alle App-relevanten Richtlinien, die sich auf die gleichen Anwendungen auf den Zielgeräten beziehen.

Diese Konfiguration überschreibt alle App-relevanten Richtlinien, die sich auf die gleichen Anwendungen auf den Zielgeräten beziehen. Bei Geräten mit Windows 10 erfolgen Einschränkungen auf Geräteebene, daher ist eine Konfiguration die einzige Möglichkeit, App-Regeln zu erzwingen.

Mit der App-Control-Konfiguration können Sie Folgendes erstellen:

- **eine Whitelist:** Es werden nur Apps zugelassen, die ausdrücklich in dieser Liste eingetragen sind. Auf den Geräten können keine anderen Apps installiert werden.
- **eine Blacklist:** Bestimmte Apps dürfen nicht auf den Geräten installiert werden.

Unterstützte Geräte

Sie können die Konfiguration der App-Kontrolle verwenden, um verschiedene Apps auf den folgenden Geräten auf eine Blacklist oder Whitelist zu setzen:

- Android-Arbeitsprofil auf firmeneigenen Geräten
- Nur überwachte Geräte unter iOS9.3+
- tvOS 11+
- Windows

Konfiguration der App-Kontrolle erstellen

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Add**
3. Geben Sie **App-Kontrolle** in dem entsprechenden Feld **Konfiguration auswählen** ein und wählen Sie dann die Konfiguration **App-Kontrolle**.
4. Geben Sie für die Konfiguration einen Namen und eine Beschreibung ein.
5. Wählen Sie ein Betriebssystem aus und setzen Sie dann mit dem Abschnitt für Ihr Betriebssystem fort.

Android-Arbeitsprofil auf firmeneigenen Geräten

Benutzer können bis zu 50 Anwendungs-IDs zur Whitelist- oder Blacklist-Gruppe hinzufügen.

Verfahren

1. Wählen Sie **Whitelist für private Apps erstellen** oder **Blacklist für private Apps erstellen**, um die Liste der Apps hinzuzufügen, die in die Whitelist oder Blacklist gestellt werden sollen.

2. Geben Sie die Anwendungs-ID (com.example.com) ein und klicken Sie auf Hinzufügen.
3. Klicken Sie auf **Weiter** und wählen Sie eine Verteilungsoption.
4. Klicken Sie auf **Fertig**.

Überwachte Geräte in iOS 9.3

Verfahren

1. Wählen Sie diese Option, um eine Whitelist oder Blacklist zu erstellen.
2. Klicken Sie auf **Apps hinzufügen**.
3. Wählen Sie die Apps aus, die Sie in die Whitelist oder Blacklist stellen wollen, indem Sie auf eine oder beide der folgenden Registerkarten klicken:
    - Klicken Sie auf die Option **Durch Suche hinzufügen**, um nach Apps im App Store oder App-Katalog zu suchen und auszuwählen.
    - Klicken Sie auf Manuell hinzufügen um System-Apps durch Eingabe der Apple-Bundle-ID zu wählen (beginnt mit "com.apple").

Klicken Sie auf die Registerkarte **Whitelist** oder **Blacklist**, um die Liste der ausgewählten Apps anzuzeigen, die in der Whitelist oder Blacklist eingetragen sind.

5. (Optional) Wählen Sie die Option **Alle Webclips einschließen**.
6. Klicken Sie auf **Weiter** und wählen Sie eine Verteilungsoption aus.
7. Klicken Sie auf **Fertig**.

Windows-Geräte

Verfahren

1. Wählen Sie **Erlaubt** oder **Nicht erlaubt**, um die Liste der entsprechenden Anwendungen hinzuzufügen, die auf die Whitelist oder Blacklist gesetzt werden sollen.
2. Wählen Sie unter dem Abschnitt **Regeldefinition** den **App-Typ** aus der Liste aus.
3. Geben Sie einen Identifikatornamen in das Feld **App-Identifikator** ein, um nach einer bestimmten App zu suchen. Sie können auch den Link **Apps suchen** verwenden, um einen neuen Dialog zu öffnen und nach Windows-spezifischen App-Identifikatoren zu suchen.
4. (Optional) Geben Sie eine Beschreibung der App in das Feld **App-Beschreibung** ein.
5. Verwenden Sie den Link **+Hinzufügen**, um weitere Regeldefinitionen für die Whitelist oder Blacklist der Apps hinzuzufügen.
6. Klicken Sie auf **Weiter** und wählen Sie eine Verteilungsoption.
7. Klicken Sie auf **Fertig**.

10.7. App-Benachrichtigungen - Konfiguration

Wählen Sie aus, wie die Benutzer Benachrichtigungen von ausgewählten Apps erhalten sollen.

Gilt für: überwachte Geräte mit iOS 9.3+.

Erstellen einer Konfiguration für App-Benachrichtigungen

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie in dem Suchfeld Notifications ein und klicken Sie dann auf die Konfiguration **App-Benachrichtigungen**. Die Setup-Seite für die Konfiguration der App-Benachrichtigungen wird angezeigt.
4. Bezeichnen und beschreiben Sie die Konfiguration.
5. Fügen Sie Apps hinzu, indem Sie im App Store suchen oder die Bundle-ID manuell eingeben.
6. Wählen Sie eine App aus, für die die App- Benachrichtigungseinstellungen gelten sollen.
7. Konfigurieren Sie die Benachrichtigungseinstellungen. Folgende Benachrichtigungen können Sie auswählen:
    - Benachrichtigungen zulassen
        - Im Benachrichtigungszentrum anzeigen
        - Töne
        - Badge-App-Symbol
        - Auf dem Sperrbildschirm anzeigen
        - (iOS 12.0+ überwacht) Kritische Warnung bei Verwendung von CarPlay anzeigen
        - (iOS 12.0+ überwacht) Kritische Warnungen aktivieren ("Nicht stören" ignorieren).
    - Warnung entsperren
        - Banner
        - Bedingte Warnung
        - Kein/e
    - (iOS 12.0+ überwacht) Gruppierungsart
        - Automatisch
        - Nach App
        - [Off]
    - (iOS 14.0+) Benachrichtigungsvorschau-Typ - Wählen Sie einen Vorschau-Typ, der in der Vorschau der Gerätebenachrichtigungen angezeigt werden soll.
        - Benutzergesteuert - Anzeige von Nachrichtenvorschauen gemäß den Benutzereinstellungen für die Apps auf dem Gerät.
        - Immer - Nachrichtenvorschauen anzeigen.
        - Wenn entsperrt - Die Nachrichtenvorschau wird nur angezeigt, wenn ein Gerät entsperrt ist.
        - Niemals - Verhindern Sie, dass Apps Nachrichtenvorschauen in Benachrichtigungen anzeigen.

8. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
9. Klicken Sie auf Fertig.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.8. Export von Konfigurationen

Exportieren Sie Ihre Konfigurationsdateien, um diese als Diagnosehilfe an den Support zu senden. Sie können eine einzelne Konfigurationsdatei im Yaml-Format als Datei oder all Ihre Konfigurationen in einer .ZIP-Datei exportieren.

Verfahren

[Export Configuration]

Sie können Dateien aus verschiedenen Bereichen der Konfigurationsseite exportieren, je nachdem, welche Konfigurationen Sie exportieren wollen.

Alle Konfigurationen exportieren:

1. Gehen Sie zu **Konfigurationen**.
2. Aktivieren Sie die Kontrollkästchen für die entsprechenden Konfigurationen.
3. Klicken Sie auf **Aktionen** > **Ausgewählte Konfigurationen mit Details exportieren**. Wenn Sie alle Konfigurationen exportieren möchten, wählen Sie **Alle Konfigurationen mit Details exportieren**.
   Eine Reihe von YAML-Dateien wird in einer ZIP-Datei gespeichert. Der Bericht enthält Details zu allen vorhandenen Konfigurationen in den ausgewählten Spaces.

Kundenspezifische Konfiguration exportieren:

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**, um eine Konfiguration auszuwählen.
3. Folgen Sie den Schritten zur Anpassung der Konfiguration.
4. Klicken Sie auf **Weiter**.
5. Wählen Sie eine Verteilungsebene.
6. Klicken Sie auf **Fertig**.
7. Wählen Sie die Konfiguration aus, die Sie gerade aus der Liste auf der Seite **Konfiguration** erstellt haben.
8. Klicken Sie auf das Pull-Down-Menü **Aktionen** und dann auf **Export.**

Eine Datei mit dem Namen der Konfiguration und einem Zeitstempel _yyyymmdd.yaml wird heruntergeladen.

Vorhandene Konfiguration exportieren

1. Gehen Sie zu **Konfigurationen**.
2. Wählen Sie eine vorhandene Konfiguration aus.
3. Klicken Sie auf das Pull-Down-Menü **Aktionen** und dann auf **Exportieren**.
   Eine Datei mit dem Namen der Konfiguration und einem Zeitstempel _yyyymmdd.yaml wird heruntergeladen.

10.9. Prioritätenvergabe für Konfigurationen

Wenn Sie mehrere Gerätegruppen für eine Konfiguration auswählen, werden einem bestimmten Gerät möglicherweise mehrere Konfigurationen desselben Typs zugewiesen. In diesem Fall bestimmt die definierte Priorität, welche Konfiguration angewendet wird. Die Konfiguration mit der höchsten Priorität hat die niedrigste Nummer. Zum Beispiel hat die Konfiguration mit der Priorität 1001 eine höhere Priorität als die Konfiguration mit der Priorität 1002. Der Dienst weist die Nummern automatisch zu.

> Die WLAN-Priorität kann nicht für das Gerät übernommen werden und ist von der Priorität ausgenommen.

Diese Option ist nur verfügbar, wenn die Seite mindestens zwei Konfigurationen desselben Typs enthält und wenn in der Dropdown-Liste ein einzelner Space ausgewählt ist. Sie können die Priorität der Konfigurationen ändern.

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Wählen Sie **Aktionen > Konfigurationen priorisieren** , wenn keine Konfiguration ausgewählt ist.
   Wenn die Option **Aktionen** nicht angezeigt wird, haben Sie maximal eine Konfiguration eines Typs, der Prioritäten erfordert.
3. Verwenden Sie die Pfeile, um die Konfigurationen zu verschieben, damit die Konfiguration, die die höchste Priorität haben soll, oben erscheint.

> Ein Schlosssymbol zeigt an, dass Sie die Priorität der Konfiguration nicht ohne Bearbeitung der Verteilungseinstellungen für alle Geräte in dieser Konfiguration ändern können.

Klicken Sie auf **Speichern**.

> Die Priorisierung kann für bis zu 400 Konfigurationen erfolgen.

Wenn Sie die Seite „Konfigurationen“ nicht sehen können, kann es sein, dass Sie nicht über die erforderlichen Berechtigungen verfügen. Sie brauchen eine der folgenden Rollen:

- Geräteverwaltung
- Geräts schreibgeschützt

10.10. Konfigurationen verwalten

Dieser Abschnitt enthält die folgenden Themen:

- AppConnect-Konfigurationen
- Sicherheitskonfiguration
- Konfigurationen für Benutzerressourcen
- Konfiguration des Unternehmensnetzwerkzugangs
- Mobilfunk
- Andere Konfiguration

10.10.1. Konfigurationstypen

Dieser Abschnitt enthält die folgenden Themen:

- Durchsuchen einer Konfiguration
- Sicherheit
- Benutzerressourcen
- Unternehmensnetzwerkzugriff
- Mobilfunknetz
- Weitere Konfigurationen
- Konfiguration der Gerätesynchronisation

Durchsuchen einer Konfiguration

Mithilfe der Such- und Filterfunktion der Seite **Konfigurationen wählen** ermitteln Sie die gewünschte Konfiguration.

Verfahren

1. **Konfigurationen** auswählen.
2. Wählen Sie eine der Konfigurationen in der Liste oder klicken Sie auf die Schaltfläche **+Hinzufügen** .
3. Die Seite **Konfiguration wählen** wird angezeigt.
   Klicken Sie auf eine der aufgelisteten Konfigurationen oder:
   - Geben Sie den Namen der Konfiguration in dem Suchfeld ein.
   - Klicken Sie auf ein Filtersymbol in dem Suchfeld auf der rechten Seite, um die Konfigurationstypen anzuzeigen, die mit der Plattform kompatibel sind.

Klicken Sie auf eine Konfigurationsschaltfläche, um auf die Konfigurationseinstellungen zuzugreifen.

Weitere Informationen finden Sie unter **Arbeiten mit Konfigurationen**.

Sicherheit

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
Android Enterprise	Definiert die Optionen für Android Enterprise.	Android Enterprise	hinzufügen
AppConnect-fähiges Gerät	Definiert die Sicherheitseinstellungen für AppConnect-fähige Apps auf Geräten.	• Android- • iOS-	hinzufügen
Apple PassKeys-Bescheinigung	Aktivieren Sie die WebAuthn-Unternehmensbescheinigung für bestimmte Passkeys auf Apple-Geräten.	• macOS	
Entra ID (Azure-Mandant)	Durch Verbinden von Ivanti Neurons for MDM mit Entra ID können Sie den Geräte-Compliance-Status der verwalteten Geräte für den bedingten Zugriff auf Microsoft 365-Apps nutzen.	• iOS- • Android	• https://www.mobileiron.com/en/pricing#Für Neukunden:Secure UEM Premium • Für Bestandskunden: Platinum
Zertifikat	Stellt die Vertrauensstellung mit Servern her.	• Android • iOS- • macOS • watchOS • visionOS • tvOS	
Zertifikatstransparenz	Kontrolliert die Durchsetzung der Zertifikatstransparenz, die nur in einem Geräteprofil erscheinen darf.	• iOS- • macOS • tvOS • watchOS • visionOS	

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
Geräteprotokollierung	Ruft zusätzliche Protokolle von den Geräten ab, wie Netzwerk- und Sicherheitsprotokolle.	• Android Enterprise	
Konfiguration "Datenträgerverwaltung"	Definiert die Richtlinien zum Verwalten externer und im Netzwerk befindlicher Speichergeräte.	• Überwachtes macOS 15.0+	
Android-Verschlüsselung	Fordert Benutzer zur Durchführung der Verschlüsselung auf.	Android-	
Verschlüsselter DNS	Ermöglicht die Erhöhung der Sicherheit, ohne dass ein VPN konfiguriert werden muss.	• iOS- • macOS • visionOS	hinzufügen
Externe Intelligence-Einstellungen	Lässt externe Intelligence-Integrationen zu.	• iOS 26.4+ • macOS 26.4+ • visionOS 26.4+	
Abwehr mobiler Bedrohungen	Schützt verwaltete Geräte vor mobilen Bedrohungen und Sicherheitslücken, die die Sicherheit des Geräts, des Netzwerks und von Anwendungen beeinträchtigen.	• Android • iOS-	
Lokale Aktionen von Threat Defense	Erstellen und verteilen Sie eine Gerätekonfiguration, die die lokalen Aktionen festlegt, welche auf unterstützten Android-Geräten ausgeführt werden sollen, wenn der Threat Defense-fähige Client eine Bedrohung erkennt.	Android-	
FileVault 2	Bietet die Möglichkeit, eine vollständige XTS-AES 128-Bit-Festplattenverschlüsselung eines Datenträgers auszuführen.	macOS	hinzufügen
FileVault-Wiederherstellungsschlüssel	Ermittelt die Einstellungen für die Umleitung der FileVault-Wiederherstellungsschlüssel auf einen Firmenserver.	macOS	hinzufügen

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
Identitätszertifikat	• Authentifiziert das Gerät für Server. • Authentifiziert das Gerät für Netzwerkressourcen.	• Android- • iOS- • macOS • watchOS • visionOS	
iOS-Aktivierungssperre	Aktiviert die Funktion Apple-Aktivierungssperre auf überwachten Geräten.	iOS-	hinzufügen
Individuelle iOS-Konfiguration	Verteilt ein iOS-Konfigurationsprofil, das von einer anderen App erstellt wurde.	iOS-	
iOS-Einschränkungen	• Sperrt Gerätefunktionen. • Aktiviert Gerätefunktionen.	• iOS- • watchOS • visionOS	
Intelligence-Einstellungen	Ermöglicht Apple Intelligence-Integrationen.	• iOS 26.4+ • macOS 26.4+ • visionOS 26.4+	
Konferenzraum-Anzeige	Schaltet den Konferenzraum-Anzeigemodus auf Apple TV ein.	tvOS 10.2+	
Tastatureinstellungen	Ermöglicht die Verwaltung des Tastaturverhaltens, der Eingabeoptionen und der zugehörigen Einstellungen für die Benutzererfahrung.	• iOS 26.4+ • macOS 26.4+	
Sperre & Kiosk: Android	• Sperrt Gerätefunktionen. • Reaktiviert Gerätefunktionen. • Wendet die Kiosk-Funktion an.	Android-	

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
Sperre & Kiosk: Android Enterprise	• Definiert die Eigenschaften und die Apps, die auf Geräten mit Android Enterprise Einschränkungen unterliegen. • Wendet die Kiosk-Funktion an.	Android 5.0 +	
Sperre & Kiosk: Samsung Knox Standard	• Definiert die Eigenschaften und Apps, die auf Geräten mit Samsung Knox Standard Einschränkungen unterliegen. • Wendet die Kiosk-Funktion an.	Samsung Knox	
Konfiguration "Local Administrator Password Solution"	Ermöglicht es Administratoren, das lokale Administratorkennwort auf verwalteten macOS-Geräten zu bestimmten Intervallen automatisch erneut zu generieren.	macOS	
macOS-Firewall	Verwaltet die Einstellungen der Anwendungs-Firewall. Diese Einstellungen sind über das Fenster mit den Sicherheitspräferenzen auf macOS-Geräten zugänglich. Der Administrator kann den Stealth-Modus aktivieren, indem er festlegt, dass das Gerät auf einen Ping-Befehl nicht reagiert.	macOS 10.12+	hinzufügen
Einschränkungen für macOS	Ermittelt die auf macOS-Geräten aktivierten Einschränkungen.	macOS	hinzufügen
macOS AppStore-Einschränkungen	Definiert im macOS AppStore aktivierte Einschränkungen.	macOS	hinzufügen
Beschränkungen beim Brennen von CDs/DVDs in macOS	Verwaltet die Einschränkungen beim Brennen von Datenträgern in macOS.	macOS	hinzufügen
Mobile@Work für macOS	Ausführungsregeln für Mobile@Work für macOS erstellen und verteilen.	macOS	hinzufügen
Mobile@Work für macOS Script	Erstellt Skripte zur Verteilung an Mobile@Work für macOS.	macOS	hinzufügen
Identitätspräf	Identifizieren Sie einen Identitätspräferenzeintrag in der Schlüsselkette des Benutzers, der sich auf die Identitäts-Payload in	macOS	hinzufügen

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
erenz	dem gleichen Profil bezieht.		
Zertifikatspräferenz	Identifizieren Sie einen Zertifikatspräferenzeintrag in der Schlüsselkette des Benutzers, der sich auf die Zertifikats-Payload in dem gleichen Profil bezieht.	• macOS	hinzufügen
Zulässige Medien	Konfiguriert Anmelde-, Abmelde- und Auswurfoptionen für physische Datenträger.	macOS	hinzufügen
Einstellungen für macOS Finder	Verwaltet Einstellungen der Finder-App in macOS.	macOS	hinzufügen
Erweiterungsrichtlinie für den macOS Kernel	Beschränkungen der Kontrollen und Einstellungen zum Laden der vom Benutzer genehmigten Kernel-Erweiterungen.	macOS	hinzufügen
Active Directory (macOS)	Konfigurieren Sie erweiterte Optionen, um macOS-Geräte an eine Domain mit Active Directory (AD) zu binden, damit Sie auf Softwaredienste zugreifen können, die Active Directory für die Authentifizierung und Sicherheit benötigen.	macOS	hinzufügen
Automatische Kontoerstellung für Office 365 (macOS)	Konfigurieren Sie die Benutzerinformationen und Optionen für die Erstkonfiguration aller Anwendungen von Microsoft Office 365.	macOS	hinzufügen
Apple App-Katalog	Verwaltet den Zugriff auf den Apple App-Katalog über einen Web-Clip.	• iOS- • macOS	
Verwaltete Domains	Definiert vertrauenswürdige E-Mail- und Web-Domänen.	• iOS 8 ausgeliefert+ • visionOS 1.1+	hinzufügen
Passwort	• Schreibt die Eingabe eines Passworts vor. • Bestimmt Länge und Zeichen des Passworts. • Ändert die Passwortanforderungen.	• Android- • iOS- • macOS • watchOS	

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
Datenschutzpräferenz (macOS)	Konfiguriert, welche Anwendungen Zugriff auf Systemdienste, Systemdateien und Systemressourcen erhalten.	macOS	hinzufügen
Authentifizieren	Bietet kennwortlose Authentifizierung für Cloud-Dienste und/oder Desktop-Anmeldungen.	• macOS • Windows	
Datenschutzeinstellungen	Bestimmt, ob Standortdaten gesammelt werden.	• iOS- • Android- • Windows	
Informationen zur Datenschutzerklärung für Kunden	Zeigt die Datenschutzrichtlinie für den Benutzer im Go-Client an.	• Android- • Android Enterprise • iOS-	
Einstellungen für Ivanti Go-Client	Konfigurieren Sie die Erhebung von Daten über MixPanel, beispielsweise von Geräte- und Nutzungsinformationen, um Fehler zu beheben und die Qualität der Dienste zu erhalten.	• iOS- • macOS	
Konfiguration "Einstellungen für Safari-Erweiterung"	Verwaltet Erweiterungen des Safari-Browsers über verschiedene Domänen.	• Überwachtes iOS 18.0+ • Überwachtes macOS 15.0+	
Siri-Einstellungen	Definiert, wie Geräte auf die Siri-Einstellungen zugreifen und sie verwenden.	• iOS 26.4+ • macOS 26.4+ • watchOS 26.4+	

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
		• visionOS 26.4+	
Konfiguration "Dienstkonfigurationsdateien"	Administratoren können Konfigurationsdateien für verschiedene Systemdienste zentral verwalten und bereitstellen.	macOS	
Software-Updates	Erstellt und verteilt die Regeln für Betriebssystemaktualisierungen.	• iOS- • macOS • Windows	
Konfiguration "Einstellungen für Softwareupdate"	Erstellt und aktualisiert Einstellungen zur Durchsetzung von Softwareupdates.	• Überwachtes iOS 18.0+ • Überwachtes macOS 15.0+	
Zeitserver	Geräten die Verbindung zu benutzerdefinierten Zeitservern erlauben.	macOS	hinzufügen
Web-Content-Filter	Kontrolliert Content von Safari.	• Überwachtes iOS 7 • visionOS 1.1+	Silver
Windows-Firewall	Für die Windows-Firewall-Konfiguration gelten verschiedene Firewall-Einschränkungen. Je nachdem, welche Firewall-Einschränkungen vom Administrator angewendet wurden, entspricht der Firewall-Status im Bereich "Sicherheitsvorgaben" von Windows-Geräten einem der folgenden Werte: • Firewall ist aktiviert und im Überwachungsmodus. • Firewall wurde deaktiviert. • Die Firewall überwacht nicht alle Netzwerke oder es wurden einige Regeln deaktiviert. • Die Firewall überwacht vorübergehend nicht alle Netzwerke. • Nicht anwendbar.	Windows 10+	

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
Schutz von Windows-Informationen	Definiert die Einstellungen für den Windows Informationsschutz (WIP) zum Schutz von Unternehmensdaten.	Windows 10+	hinzufügen
Windows-Einschränkungen	Definiert, welche Funktionen auf Windows 10+-Geräten verfügbar sind.	Windows 10+	
Konfiguration "Windows KI-Verwaltung"	Mit dieser Konfiguration verwalten Sie Windows KI-Einstellungen und -Konfigurationen.	Windows 10+	

Benutzerressourcen

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
CalDAV	• Konfiguriert den Zugriff auf einen CalDAV-Server (z. B. Google Kalender)	• iOS- • visionOS	
CardDAV	• Konfiguriert den Zugriff auf einen CardDAV-Server (z. B. Google Kalender)	• iOS- • visionOS	
E-Mail	• richtet Zugriff für POP/IMAP-E-Mail (z. B. Gmail) ein	• iOS- • visionOS	
[Exchange]	• Konfiguriert eine ActiveSync-E-Mail (ähnlich Outlook) für Android- und iOS-Mobilgeräte. • Konfiguriert die Exchange-Web-Dienste (EWS) für E-Mails auf macOS-Geräten. • definiert, wie viel mit dem Gerät synchronisiert werden soll • bestimmt Sicherheit für E-Mail	• Android- • iOS- • macOS • visionOS	• Exchange über Sentry wird in macOS nicht unterstützt. • Das E-Mail-Flag für die Synchronisation seit einer bestimmten Anzahl von Tagen steht für macOS nicht zur Verfügung.
Google	• Erstellt die Google-Kontokonfigurationen, mit denen Geräte mit iOS 9.3.2+ mit Google-Konten eine Verbindung aufbauen. • Gibt an, welche App für Gespräche mit Kontakten im Google-System verwendet werden soll.	• iOS- • visionOS	
Schriftart	• installiert für eine ordnungsgemäße Anzeige von Dokumenten erforderliche Nicht-Standard-Schriftarten	• iOS-	
Abonnierter Kalender	• richtet ein Abonnement für einen Internetkalender ein	• iOS- • visionOS	
Web-Clip	• zeigt einen Schnellzugriff (Symbol) auf eine Internetseite an	• iOS- • macOS	
Content-Caching	• bietet einen Dienst zur Zwischenspeicherung von Inhalten, um lokale Kopien der App Store Software zu aktivieren und	• macOS	

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
	• aktiviert verbundene Clients für schnellere Software- und App-Downloads.		

Unternehmensnetzwerkzugriff

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
AirPlay-	• richtet Zugriff auf Ersatzgeräte zum Anzeigen von Medien ein	• iOS- • macOS	Silver
AirPrint	• ermöglicht Einrichtung zum drahtlosen Drucken	• iOS- • macOS	Silver
Always On VPN	• Konfiguriert den Zugang zu einem VPN-Server ohne Benutzereingriff.	• Android 7.0+ • iOS 8 ausgeliefert+	• Gold für Android für Unternehmen • Silver-Lizenz für iOS
Standard-App-Runtime-Berechtigungen	• Definiert die Runtime-Rechte in der Konfiguration für Apps, die für Geräte mit Android für Unternehmen bereitgestellt werden.	• Apps für die Android API 23+ und Android 6.0+ auf Geräten mit Android für Unternehmen.	
Bildung	• Konfiguriert die Apple Education Payload sowie die ClassRoom-App für Lehrer und Schüler.	• supervised iOS 9.3+	hinzufügen
Globaler Proxy	• konfiguriert Geräte für Weiterleitung von HTTP-Verkehr an einen Proxy-Server	• iOS 7 auf überwachten Geräten • Überwachte Geräte mit tvOS	Silver
LDAP,	• richtet Zugriff auf ein Unternehmensverzeichnis ein	• iOS- • visionOS	
Tunnel	• definiert eine App-bezogene VPN-Verbindung zwischen einem Client und Sentry mithilfe von Tunnel	• iOS 7 ausgeliefert+ • macOS 10.13+ • Windows 10+ • Android-	
Bridge	• erlaubt der IT, Windows-Operationen auf UEM-Plattformen zu modernisieren, ohne auf kritische Funktionalität zu verzichten.	• Windows 10 Desktop	Lizenz für Bridge
macOS-Server	• Definiert ein macOS-Server-Konto mit den konfigurierten Kontoarten und den entsprechenden	• iOS 10+	

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
	Einstellungen. Erlaubt dem Benutzer die Aktivierung der Dateifreigabe auf dem Server.		
Per-App VPN	• stellt Verbindungen zwischen bestimmten Apps und einem VPN-Server her	• iOS- • watchOS • visionOS • tvOS	Silver
Netzwerkrelais-Konfiguration	• Fügt eine Konfiguration hinzu, um Einstellungen für Netzwerkrelais zu definieren.	• iOS- • macOS • visionOS	
Single Sign-On	• richtet Single Sign-On für bestimmte verwaltete Apps ein	• iOS- • macOS • visionOS	
Sichere Anmeldung für mehrere Benutzer	• Konfiguriert einen sicheren Zugriff für viele Benutzer über Web-clip.	• iOS-	
VPN	• richtet Zugriff auf einen VPN-Server ein	• Android- • Windows • iOS- • macOS • visionOS • tvOS	
VPN-on-Demand	• richtet basierend auf Domänen, Host-Namen usw. Zugriff auf einen VPN-Server ein	• iOS-	
WLAN	• richtet Zugriff auf ein Wireless-Netzwerk ein	• Android- • Windows • iOS- • macOS • watchOS • visionOS • tvOS	

Mobilfunknetz

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
APN	• richtet den Mobilfunk-Zugangspunktnamen für das Gerät ein	• iOS-	
Mobilfunk	• richtet Zugriff auf Mobilfunknetz ein	• iOS- • watchOS	
Konfiguration "Privates Mobilfunknetz"	• Weist die Payload an, Geräteinformationen zu privaten Netzwerkbereitstellungen anzugeben.	• iOS-	
Konfiguration für iOS Telecom-Voreinstellungen	• bestimmt Standardwerte für Roaming-Einschränkungen • bestimmt Standardwerte für persönliche Hotspot-Einschränkungen	• iOS-	

Weitere Konfigurationen

Typ	Vorgesehene Funktion	Für diese Geräte	Benötigte Lizenz
Apple TV	• definiert Sprache und Ort für Apple TV	• iOS 7 auf überwachten Geräten	Silver
Standardgerätename	• Definiert einen Standardgerätenamen mit Hilfe von Variablen.	• Überwachte Geräte mit iOS 8	Silver
iOS-Hintergrund	• Installiert einen Startbildschirm und einen Sperrbildschirmhintergrund	• iOS 7 auf überwachten Geräten	Silver
macOS-Hintergrundbild	• Installiert ein Startbildschirm- und Sperrbildschirm-Hintergrundbild auf den Geräten. Hintergründe können vom Benutzer geändert, aber nach der Verteilung nicht mehr von dem Gerät entfernt werden.		Nicht erforderlich
Einstellungen für den Migrationsassistenten	Unterstützt Administratoren und Benutzer bei der Übertragung von Daten, Apps und Einstellungen während der Geräteeinrichtung oder -migration.	• macOS 26.4+	
Single-App-Modus	• beschränkt das Gerät auf die Nutzung der angegebenen App	• iOS 7 auf überwachten Geräten • Überwachte Geräte mit tvOS	Silver
Konfiguration verknüpfter Domänen	• Die Konfiguration verknüpfter Domänen ist ein Wörterbuch, das Apps den zugehörigen Domänen zuordnet. • Verknüpfte Domänen können mit Funktionen wie Extensible AppSSO, universelle Links und Kennwort-AutoFill verwendet werden.	• macOS 10.15+	Gold
Konfiguration "Hosteinstellungen für Bildschirmfreigabe"	• Ermöglicht Administratoren das sichere Steuern von macOS-Bildschirmfreigabefunktionen für verwaltete Geräte.	• macOS 14+	

Konfiguration der Gerätesynchronisation

Die Einstellungen zur Gerätesynchronisation enthalten eine Liste von Datenpunkten, die Sie auf Geräten überwachen können. Die Konfigurationen für die Gerätesynchronisation lassen sich nicht bearbeiten. Sie können eine Liste der überprüften Einstellungen anzeigen.

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **Konfiguration der Gerätesynchronisation**. Die Registerkarte "Details" der Seite **Konfiguration der Gerätesynchronisation** wird mit einer Liste markierter Einträge angezeigt.

Einstellungen	Zeit zwischen den Messungen in Minuten
Zertifikatliste	
Geräteinformationen	60
Liste der installierten Apps	60
Liste der verwalteten Apps	60
Profilliste	60
Liste der Provisionierungsprofile	60
Einschränkungen	60
Sicherheitsinformationen	60
iOS9+ Nach Updates prüfen	 1440

Verwandte Themen

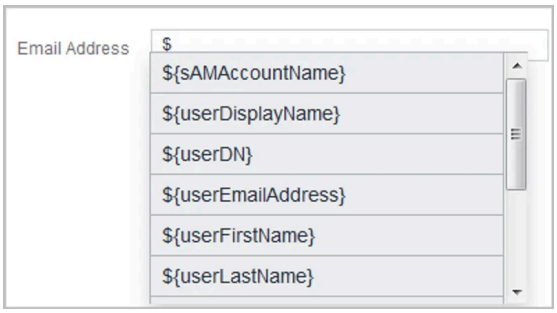
- Variablen
- Arbeiten mit Konfigurationen

10.10.2. Variablen

Variablen können in bestimmten Konfigurationsfeldern eingesetzt werden, wo sie bestimmte Angaben eines beliebigen Benutzers repräsentieren. Jedes Feld, in dem Variablen unterstützt werden, zeigt eine Liste unterstützter Variablen an, wenn Sie in das Feld "$" eingeben. Dieser Abschnitt enthält die folgenden Themen:

Unterstützte Variablen für Benutzerkonten

Benutzervariablen

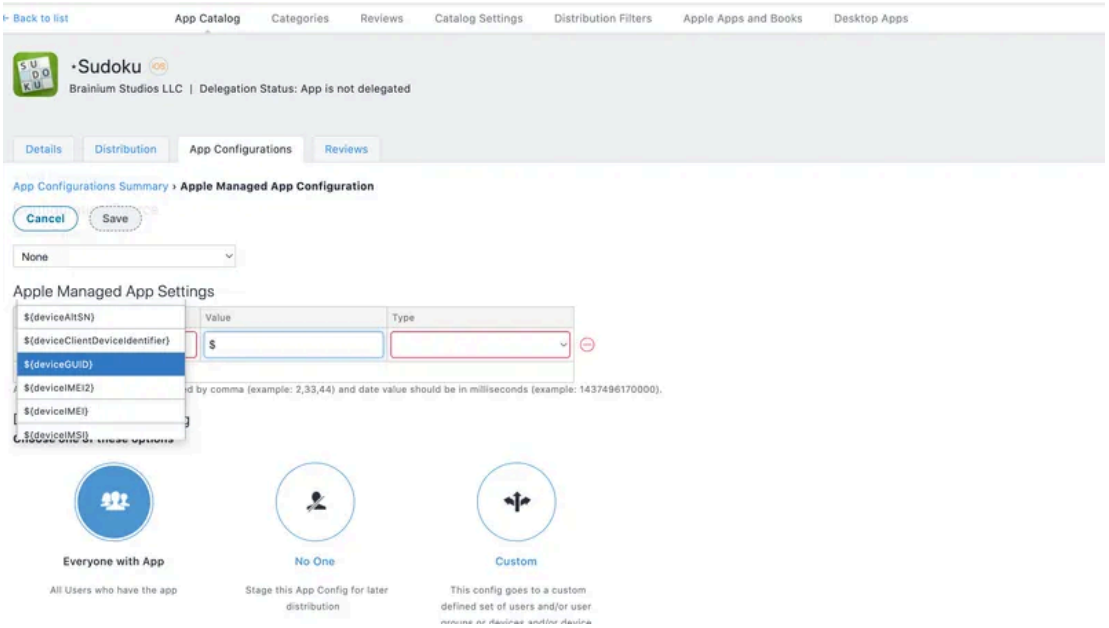


Variablenschlüssel	Beschreibung des Werts
$	Abteilungsattribut (erfordert Entra ID)
$	Persönliche Kennung für den elektronischen Datenaustausch
$	Verwaltete Apple-ID des Benutzers
$	sAMAccountName-Attribut (erfordert Active Directory)
$	Das Attribut Allgemeiner Name (CN) extrahiert aus dem Eindeutigen Namen (erfordert LDAP)
$	Anzeigename
$	Eindeutiger Name (erfordert LDAP)
$	Der Domänenabschnitt der E-Mail-Adresse (der Teil nach dem '@')
$>	Der lokale Abschnitt der E-Mail-Adresse (der Teil vor '@')
$	E-Mail-Adresse
$	Vorname
$	Nachname
$	Gebietsschema
$	Attribut Organisationseinheit (OU) extrahiert aus dem Eindeutigen Namen (erfordert LDAP)
$	Kerberos-Bereichsinformationen (erfordert Active Directory)
$	Der Domänenabschnitt der Anmelde-ID (der Teil nach dem '@')
$	Der lokale Abschnitt der Anmelde-ID (der Teil vor dem '@')
$	Anmelde-ID (E-Mail-Adressformat)
$	Attribut userPrincipalName (erfordert Active Directory)

Unterstützte Gerätevariablen

Mithilfe von Gerätevariablen legen Sie Informationen zu einem Mobilgerät fest.

Gerätevariablen


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

Variablenschlüssel	Beschreibung des Werts
$	Datum des letzten Client-Anmeldung (letzte Anmeldung - entweder MDM oder Client)
$	Alternative Seriennummer
$	Von der Client-Anwendung verwendete Kennung
$	Global eindeutige Gerätekennung
$	ICCID
$	IMEI2
$	IMEI
$	IMSI
$	Datum der letzten Geräteanmeldung (letzte Anmeldung von MDM oder Client)
$	Interne Gerätekennung
$	Für MDM verwendete Kennung
$	MEID
$	Modell
$	Gerätename
$	Telefonnummer des Geräts
$	Clustereigene Gerätekennung
$	Seriennummer
$	iOS UDID
$	WLAN-MAC-Adresse

E-Mail-Vorlagenvariablen

Variablenschlüssel	Beschreibung des Werts
$	E-Mail-Textteil
$	E-Mail-Betreff

Zeitstempelvariablen

Variablenschlüssel	Beschreibung des Werts
$	Aktueller Zeitstempel (Millisekunden seit Epoch)

Richtlinien-Vorlagenvariablen

Variablenschlüssel	Beschreibung des Werts
$	Name der verletzten Richtlinie
$	Nächste mehrstufige Compliance-Aktion (außer Warten und Stilllegen) nach dem Senden der Nachricht
$	Anzahl der Tage, an denen das Gerät nicht konform war.
$	Zeitstempel der ersten erkannten Richtlinienverletzung (Format UTC TT-MM-JJJJ)
$	Regeldefinition (Abfragezeichenfolge, wie sie jetzt erscheint)

Verwandte Themen:

- **Attribute**

10.10.3. AppConnect-Konfigurationen

Dieser Abschnitt enthält die folgenden Themen:

- Übersicht über AppConnect
- AppConnect-Passcode

10.10.3.1. Übersicht über AppConnect

AppConnect ist eine Funktion, die Apps in Containern kapselt, um Daten auf iOS- und Android-Geräten zu schützen. Jede AppConnect-fähige App wird zu einem sicheren Container, dessen Daten verschlüsselt, gegen den Zugriff Unbefugter geschützt und entfernbar sind. Da jeder Benutzer über mehrere geschäftliche Apps verfügt, sind die sicheren App-Container miteinander verbunden. Diese Verbindung ermöglicht den AppConnect-fähigen Apps, Daten wie Dokumente zu teilen. Die Cloud verwendet Richtlinien zur Verwaltung der AppConnect-fähigen Apps.

Weitere Informationen zu AppConnect und zur Konfiguration und Bereitstellung von AppConnect-Apps finden Sie in der *AppConnect-Anleitung für Cloud*.

Status sicherer Apps

Klicken Sie auf der Seite **Geräte > Geräte** auf ein Gerät, um die **Übersichtsseite** anzuzeigen. Auf dieser Seite können die Benutzer den Status der sicheren Apps mit folgenden Informationen überprüfen:

- **Status sicherer Apps** – gibt an, ob AppConnect aktiviert oder deaktiviert ist.
- Verschlüsselungsstatus sicherer Apps - Gibt an, ob der AppConnect-Passcode aktiviert oder deaktiviert ist.
- **Verschlüsselungsmodus für sichere Apps** – gibt an, ob der Verschlüsselungsmodus (beispielsweise AES 256) aktiviert ist.

Außerdem können folgende Felder verwendet werden:

- Als Filter (linke Ansicht), um die angezeigten Geräteeinträge einzugrenzen, wenn Benutzer versuchen, Geräte zu finden und zu filtern.
- Als Regeln bei der Erstellung einer dynamisch verwalteten Gerätegruppe.
- Als Verteilungsfilter, welche die Geräte festlegen, für die Apps nach bestimmten Regeln verteilt werden.

Administratoren können für jede sichere App den Status der Container-Richtlinie und der Konfiguration überprüfen (installiert, übernommen, gesendet oder laufende Installation). Sie finden diese Informationen auf der Registerkarte **Konfigurationen** der Seite "Gerätedetails".

10.10.3.2. AppConnect-Passcode

Dieser Abschnitt enthält die folgenden Themen:

- Passcode ändern/zurücksetzen
- Einmal-PIN zum Zurücksetzen eines Passcodes für abgesicherte Apps für iOS-Geräte erzeugen

Sie können einen AppConnect-Passcode anfordern, auch bezeichnet als Passcode für sichere Apps. Mit einer einzigen Anmeldung mit dem AppConnect-Passcode kann der Gerätebenutzer auf alle sicheren Apps zugreifen. Im Admin-Portal können Sie die Regeln für das Single-Sign-On-Passwort konfigurieren. Das AppConnect-Passwort ist nicht identisch mit dem Zugangscode zum Entsperren des Gerätes.

Passcode ändern/zurücksetzen

Benutzer können den Passcode für sichere Apps im Secure Apps Manager für Android-Geräte und in der Go for iOS-App ändern oder zurücksetzen, sofern dies in der AppConnect-Konfiguration erlaubt wurde. Für iOS-Geräte:

Verfahren

1. Öffnen Sie die Go for iOS-App.
2. Klicken Sie auf **Sichere Apps**.
3. Klicken Sie auf **Authentifizierung**.
4. Klicken Sie auf **Sicheren Apps Passcode ändern** und folgen Sie den Anweisungen zur Änderung/zum Zurücksetzen des Passcodes.

Für Android-Geräte:

1. Öffnen Sie den Secure Apps Manager.
2. Klicken Sie im Optionsmenü auf **Passcode ändern**.
3. Klicken Sie auf **Passwort vergessen**, um den Passcode zurückzusetzen.

Einmal-PIN zum Zurücksetzen eines Passcodes für abgesicherte Apps für iOS-Geräte erzeugen

Administratoren können die Cloud so konfigurieren, dass iOS-Gerätebenutzer den Passcode für ihre sicheren Apps (AppConnect) zurücksetzen können, wenn sie ihn vergessen haben. Wenn Sie diese Option konfiguriert haben, können in der Cloud mit Benutzername und Passwort registrierte Gerätebenutzer diese Anmeldeinformationen in der Go for iOS-App Version 3.1.0 bzw. für neuere und unterstützte Versionen eingeben, um sich selbst zu authentifizieren und dann ihren sicheren Apps-Passcode zurückzusetzen. Gerätebenutzer, die das Passwort und die PIN vergessen haben, benötigen jedoch einen anderen Mechanismus, um sich selbst zu authentifizieren.

Verfahren

1. In der Cloud aktiviert der Administrator die Option **Passcode für sichere Apps** in der Standardkonfiguration für iOS AppConnect (oder in einer anderen Konfiguration für iOS AppConnect).
2. Der Benutzer generiert einmalig eine PIN für ein bestimmtes iOS-Gerät im Benutzer-Selbstbedienungsportal, indem auf die Option Passcode für sichere Apps zurücksetzen klickt und den Anweisungen folgt. Die einmalig verwendbare PIN gilt für 30 Minuten.

3. In der Go for iOS-App auf einem Gerät folgt der Benutzer den Anweisungen zum Zurücksetzen eines vergessenen Passcodes für sichere Apps.
4. Wenn er zur Eingabe seiner Benutzeranmeldedaten aufgefordert wird, gibt der Benutzer seinen Benutzernamen und die einmalig verwendbare PIN anstelle des regulären Passcodes ein.
5. Damit setzt der Benutzer seinen Passocde für sichere Apps zurück.

10.10.4. Sicherheitskonfiguration

Dieser Abschnitt enthält die folgenden Themen:

- Android Enterprise
- Bearbeiten der Android Enterprise-Standardkonfiguration
- Einrichten von Android Enterprise
- Android Work Challenge
- Zertifikatskonfiguration
- Zertifikatstransparenz
- Konfiguration der Zertifikatswiderrufsprüfung
- Erstellen einer Konfiguration für den autonomen Einzel-App-Modus
- Erstellen der DNS-Proxykonfiguration
- Konfigurieren der Geräteprotokollierung
- Konfiguration "Datenträgerverwaltung"
- Android-Verschlüsselung
- Verschlüsselter DNS
- Externe Intelligence-Einstellungen
- Bedrohungsabwehr
- FileVault 2
- FileVault-Wiederherstellungsschlüssel
- Konfiguration der FileVault-Optionen
- Identitätszertifikat
- Konfiguration der iOS-Aktivierungssperre
- Individuelle iOS-Konfiguration
- Intelligence-Einstellungen
- Tastatureinstellungen
- iOS-Einschränkungen
- Konferenzraum-Anzeige
- Sperre & Kiosk: Android-Geräte Administratormodus
- Konfiguration des Kiosk-Modus für Android
- Kiosk für unter Android freigegebenes Gerät konfigurieren
- Sperre & Kiosk: Android Enterprise
- Sperre & Kiosk-Modus: Samsung Knox Standard
- macOS-Firewall
- Einschränkungen für macOS
- macOS AppStore-Einschränkungen
- Beschränkungen beim Brennen von CDs/DVDs in macOS

- Kontrolle zulässiger Medien (zurückgestuft)
- Einstellungen für macOS Finder
- Erweiterungsrichtlinie für den macOS Kernel
- Mobile@Work für macOS
- Konfiguration der Update-Regeln für macOS Software
- Zertifikatspräferenz
- Active Directory (macOS)
- Identitätspräferenz
- Automatische Kontoerstellung für Office 365 (macOS)
- Authentifizieren
- Apple App-Katalog
- Verwaltete Domänen
- Passwortkonfiguration
- Datenschutzpräferenz (macOS)
- Einstellungen für Ivanti Go-Client
- Datenschutzeinstellungen
- Informationen zur Datenschutzerklärung für Kunden
- Konfiguration "Einstellungen für Safari-Erweiterung"
- [Software Updates]
- Konfiguration "Einstellungen für Softwareupdate"
- Konfiguration der Sicherheitspräferenzen
- Siri-Einstellungen
- Zeitserver
- Web-Content-Filter
- Windows-Firewall
- Schutz von Windows-Informationen
- Windows-Einschränkungen
- Einschränkungen für Windows Desktop
- Desktop-Einstellungen für Windows 10
- Konfiguration von Windows Hello for Business
- Konfiguration "Windows KI-Verwaltung"
- Play Integrity (ehemals SafetyNet-Bestätigung)
- Erweiterter Android-Passcode und Sperrbildschirm
- Microsoft Defender for Endpoint
- Zertifikat-basierte Authentifizierung

10.10.4.1. Android Enterprise

Lizenz: Silver

Eine Konfiguration für Android Enterprise definiert die Optionen für **Android Enterprise**, die für unterstützte Geräte aktiviert sind. Sie können alternative Konfigurationen für andere Gerätegruppen erstellen oder einfach die Standardkonfiguration bearbeiten. Eine Liste der Geräte, die Android Enterprise unterstützen, finden Sie auf der offiziellen Seite von **Android**.

Android Enterprise-Einstellungen

Einstellung	Aktion
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Screenshots deaktivieren (Android 5.0 +)	Wählen Sie diese Option, um zu verhindern, dass Geräte die native Bildschirmaufnahmefunktion verwenden.
Apps-Kontrolle deaktivieren (Android 5.0+)	Wählen Sie diese Option, um zu verhindern, dass Benutzer Apps in den Einstellungen oder Anwendungsstartern (Launchern) modifizieren.
Konfigurieren der Anmeldeinformationen nicht zulassen (Android 5.0+)	Wählen Sie diese Option aus, um zu verhindern, dass die Benutzer die Anmeldeinformationen selbst konfigurieren.
Profilübergreifendes Kopieren und Einfügen nicht zulassen (Android 5.0+)	Wählen Sie diese Option, damit Geräte Arbeitsprofile nicht kopieren und in andere Android Enterprise-Arbeitsprofile einfügen können.
Modifizieren von Konten nicht zulassen (Android 5.0+)	Wählen Sie diese Option, um zu verhindern, dass Benutzer Konten hinzufügen und entfernen können.
Ausgehenden Beam verweigern (Android 5.0 +)	Wählen Sie diese Option, um zu verhindern, dass Benutzer mit NFC App-Daten übertragen können.
Standortfreigabe verweigern (Android 5.0+)	Wählen Sie diese Option aus, um zu verhindern, dass Websites und Apps den Gerätebenutzer auffordern, den Gerätestandort freizugeben.
Eingabemethoden beschränken (Android 5.0+)	Wählen Sie diese Option, um die Eingabemethoden zu beschränken, indem Sie eine Liste mit zulässigen Paketnamen festlegen. Wenn keine Pakete in der Liste aufgeführt sind, ist nur die Eingabe über die Systemtastatur zulässig. Die Eingabemethoden gelten nicht nur für geschäftliche Apps, sondern für das gesamte Gerät.
Zugangsdienste beschränken (Android 5.0 +)	Wählen Sie diese Option, um die Eingabemethoden zu beschränken, indem Sie eine Liste mit zulässigen Paketnamen festlegen. Wenn keine Pakete eingetragen sind, sind nur systemseitige Services für Barrierefreiheit zulässig. Die Eingabemethoden gelten nicht nur für geschäftliche Apps, sondern für das gesamte Gerät.
Anrufer-ID deaktivieren (Android 6,0 +)	Legt fest, ob die Anrufer-ID-Informationen aus dem Arbeitsprofil bei eingehenden Anrufen auf dem Gerät angezeigt werden.

Verwandte Themen

- Einrichten von Android Enterprise

10.10.4.2. Apple PassKeys-Bescheinigung

Verwenden Sie die Konfiguration "Passkey-Bescheinigung", um das Gerät für das Zulassen der WebAuthn-Unternehmensbescheinigung für bestimmte Passkeys zu konfigurieren.

Wenn ein Benutzer einen Passkey zum Authentifizieren und Registrieren seiner Geräte verwendet, greift die Konfiguration "Apple Passkey-Bescheinigung" auf vom Unternehmen verwaltete Anmeldedaten zu, um den Passkey mit einem Unternehmenszertifikat zu bestätigen. Zu den unterstützten Anmeldeinformationen gehören SCEP, ACME sowie Identitätsanmeldeinformationen.

Die Passkey-Bescheinigung unterstützt Folgendes:

- Unterstützte Mindestversionen von Betriebssystemen: macOS 14
- Unterstützte Registrierungsmethoden: Geräteregistrierung
- Zum Synchronisieren von Passkeys sind verwaltete Apple Accounts erforderlich.
- Können zusammen mit der Zugriffsverwaltung über ABM verwendet werden.

> Die Passkeys-Payload schlägt auf Mac fehl.

Zum Erstellen einer Passkey-Konfiguration müssen Sie zuerst eine Identitätszertifikat-Konfiguration erstellen und diese dann mit der Passkey-Konfiguration verknüpfen. Machen Sue außerdem folgende Angaben im Abschnitt "Konfiguration 'Sicherheits-Passkey-Bescheinigung'":

Feld	Beschreibung
[Name]	Name des Passkeys.
Beschreibung	Beliebige Informationen zur Konfiguration.
Bescheinigung Identität Asset-Referenz • Bescheinigung Identität Schlüssel ist extrahierbar	Geben Sie die von Ihnen erstellte Asset-Referenz-Identität an, um die Verknüpfung zur Passkey-Konfiguration herzustellen. Wählen Sie diese Option aus, um anzugeben, dass der Identitätsschlüssel extrahierbar ist.
Vertrauende Parteien	Geben Sie die Details für authentifizierte Domänen ein.

10.10.4.3. Standardeinstellungen für App-Datenschutz

Verwenden Sie die **App-Datenschutz-Standardeinstellungen**, um standardmäßige Datenschutzberechtigungen für Apps auf überwachten Geräten zu definieren. Administratoren können die Datenschutzkomponenten identifizieren, die eine App verwendet, die App und ihre Komponenten in der Konfiguration auflisten und Datenschutz-Standardeinstellungen festlegen. Wenn Benutzer die App starten, überprüft die App die konfigurierten Datenschutz-Standardeinstellungen und fordert die Benutzer auf, Berechtigungen zu gewähren. Die Berechtigungen können jedoch auch später bei den Geräteeinstellungen verschoben oder verwaltet werden.

Gilt für:

- iOS 27.0+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- iPad 27.0+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- macOS 27.0+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Suchen Sie nach der Konfiguration **App-Datenschutz-Standardeinstellungen** und wählen Sie sie aus.
3. Geben Sie in das Feld **Name** eine Bezeichnung ein, mit der Sie die Konfiguration identifizieren können.
4. Geben Sie in das Feld **Beschreibung** eine Beschreibung ein, die den Zweck der Konfiguration erläutert.
5. Wählen Sie im Bereich **Konfigurationseinstellungen** die Option **Durch Suche hinzufügen** aus.
6. Geben Sie den Namen der App ein, für die Sie **App-Datenschutz-Standardeinstellungen** konfigurieren möchten, indem Sie eine der folgenden Optionen auswählen:

- iOS Store
- App-Katalog
- visionOS Store
- OS X Store (macOS)

> Sie können mehrere Apps auswählen.

7. (Optional) Wählen Sie **Manuell hinzufügen** aus, um eine App auszuwählen.
8. (Optional) Geben Sie den **Paketnamen** der App ein.
9. (Optional) Klicken Sie auf **App hinzufügen**.
10. Wählen Sie **App anzeigen** aus.

Der Bereich **App anzeigen** listet alle ausgewählten Anwendungen auf.

11. Klicken Sie bei jeder Anwendung auf **Standardeinstellungen hinzufügen**, um die Standardeinstellungen für den App-Datenschutz individuell zu konfigurieren.

Der Bereich **Standardeinstellungen hinzufügen** wird angezeigt.

12. Wählen Sie die **Standardwerte** und **Einschränkungen** gemäß der folgenden Tabelle aus:

Standard einstellungen	Einschränkungen festlegen
Kamera	Wählen Sie eine der folgenden Optionen aus: • Zulassen • Kein/e
Bluetooth	Wählen Sie eine der folgenden Optionen aus: • Zulassen • Kein/e
Barrierefreiheit	Wählen Sie eine der folgenden Optionen aus: • Zulassen • Kein/e
Diktat	Wählen Sie eine der folgenden Optionen aus: • Zulassen • Kein/e
Mikrofon	Wählen Sie eine der folgenden Optionen aus: • Zulassen • Kein/e
Standort	Wählen Sie eine der folgenden Optionen aus: • Während der Verwendung • Kein/e • Immer
Standortgenauigkeit	Wählen Sie eine der folgenden Optionen aus: • Ungefähr • Genau • Kein/e
Lokales Netzwerk	Wählen Sie eine der folgenden Optionen aus: • Zulassen • Kein/e
Begründung Unternehmen	Die **Begründung Unternehmen** kann den Namen des Unternehmens, den App-Namen, die vom Administrator bereitgestellte Begründung und Details für jede Komponente mit einer empfohlenen Datenschutz-Standardeinstellung anzeigen. Wenn der Benutzer **Zulassen** auswählt, wendet das System die empfohlenen Datenschutz-Standardeinstellungen an. Wenn der Benutzer **Nicht jetzt auswählt**, werden die Eingabeaufforderungen zur Erteilung der Zustimmung angezeigt, wenn die App auf die angegebenen Komponenten auf dem Gerät des Benutzers zugreift.

13. Klicken Sie auf **Speichern**.
14. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.

15. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **App-Datenschutz-Standardeinstellungen** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
16. Klicken Sie auf **Fertig**.

10.10.4.4. Bearbeiten der Android Enterprise-Standardkonfiguration

Globale Administratoren können Space-Administratoren gestatten, die Verteilung für der folgenden Android Enterprise-Standardkonfigurationen im angepassten Space zu bearbeiten.

- Android Enterprise: Arbeitsprofil auf unternehmenseigenem Gerät (Android for Work)
- Android Enterprise: Vom Unternehmen verwaltetes Gerät (Android for Work)
- Android Enterprise: Verwaltetes Gerät mit Arbeitsprofil
- Android Enterprise: AOSP

Verteilung für jede der oben genannten Konfigurationen bearbeiten

Verfahren

1. Wählen Sie auf der Registerkarte „Konfigurationen“ die zu bearbeitende Konfiguration aus.
2. Klicken Sie auf das Bearbeitungssymbol.
3. Klicken Sie auf **Weiter**
4. Wählen Sie eine der folgenden Verteilungsebenen auf der Verteilungsseite aus, um sie zu bearbeiten und zu konfigurieren:
    - **Alle Geräte**: Wählen Sie eine der folgenden Optionen, um die Konfiguration an alle kompatiblen Geräte zu verteilen:
        1. Nicht auf andere Spaces anwenden
        2. Auf Geräte in anderen Spaces anwenden
    - **Keine Geräte** (Standard)
    - **Benutzerdefiniert**: Wählen Sie eine der folgenden Optionen, um die Konfiguration an alle kompatiblen Geräte oder Benutzer zu verteilen:
        1. **Benutzer/Benutzergruppen**: Markieren Sie das Kontrollkästchen neben den Benutzern oder Benutzergruppen. Alternativ können Sie nach den Benutzern oder Benutzergruppen suchen, indem Sie sie eingeben.
        2. **Geräte/Gerätegruppen**: Markieren Sie das Kontrollkästchen neben den Geräten oder Gerätegruppen. Alternativ können Sie nach den Geräten oder Gerätegruppen suchen, indem Sie sie eingeben.
           Wählen Sie in der **Verteilungsübersicht** eine der folgenden Optionen, um Konfigurationen für mehrere Spaces zu aktivieren oder zu deaktivieren:
            - Nicht für andere Spaces übernehmen.
            - Auf Geräte in anderen Spaces anwenden

        > Das Kontrollkästchen **Space-Admin das Bearbeiten der Verteilung erlauben** wird angezeigt, wenn Sie die Option **Auf Geräte in anderen Spaces anwenden** ausgewählt haben. Es ermöglicht delegierten Space-Administratoren das Bearbeiten der Verteilung für den jeweiligen Space.

> Wenn Sie die Verteilungsoption bearbeiten, müssen Sie das Kontrollkästchen **Mir ist bekannt, dass eine Änderung der Verteilung der Android Enterprise-Device Mode-Konfiguration dazu führen kann, dass Geräte stillgelegt oder gelöscht werden, wenn die Konfiguration von bestehenden Geräten entfernt wird** markieren.

5. Klicken Sie auf **Fertig**.

Wenn diese Konfiguration auf Spaces angewendet wird, können die Space-Administratoren die Verteilung bearbeiten, indem sie auf das Verteilungssymbol im angepassten Space klicken.

10.10.4.5. Einrichten von Android Enterprise

Dieser Abschnitt enthält folgendes Thema:

- Unterstützte Geräte
- Verbinden von Ivanti Neurons for MDM mit Android Enterprise
- Anfordern der Anmeldeinformationen für Android Enterprise
- Hinzufügen Ihres Android Enterprise MDM-Tokens zu Ivanti Neurons for MDM
- Synchronisieren von Benutzern zwischen Ivanti Neurons for MDM und Google
- Active Directory/LDAP-Benutzer
- Lokale Benutzer
- Bereitstellen von Android Enterprise für unterstützte Geräte
- Registrierte Geräte abschalten
- Gerät bereitstellen
- Bereitstellung bestätigen
- Apps für Android Enterprise bereitstellen
- Unternehmens-Apps konfigurieren

Lizenz: Silver

Android Enterprise ist ein von Google angebotenes Programm, das Mobility-Administratoren Folgendes ermöglicht:

- Betriebliche und private Daten trennen
- Unternehmens-Apps absichern und verwalten
- System-Apps kontrollieren (beispielsweise Kamera und Galerie)
- Apps zentral im Android Enterprise-Container bereitstellen und konfigurieren
- Datenverlust verhindern (durch Bildschirmfotos)

Sie können Ivanti Neurons for MDM als den UEM-Server konfigurieren, auf dem Android Enterprise verwaltet wird. Android Enterprise erfordert mindestens Android 3.0. Es werden zwei Konfigurationen von Android Enterprise unterstützt: Geräteeigentümer und Verwaltetes Profil – Mitarbeitereigentum.

Unterstützte Geräte

Ivanti Neurons for MDM unterstützt Android Enterprise derzeit nur auf Geräten, die Android 5.0 ausführen und auf denen Android Enterprise durch den Hersteller aktiviert wurde. Android Enterprise ist für den Kiosk-Modus auf Geräten mit Android 5.0 erforderlich.

Voraussetzung

Wenn Sie Ihre Domain bei Google registriert haben, müssen Sie sich zuerst für das Programm auf der Google-Website anmelden:

https://admin.google.com.

Während dieses Vorgangs führen Sie folgende Schritte aus:

- Domain anfordern (diese muss identisch sein mit der Domain der Benutzer-E-Mail-Adresse)
- Token erhalten

- JSON Client-ID herunterladen

Beide Elemente sind erforderlich, wenn Sie Android Enterprise auf Ivanti Neurons for MDM einrichten.

Danach erhalten Sie eine E-Mail mit Anweisungen, mit denen überprüft wird, ob Sie die Domain besitzen, die Sie angegeben haben.

Wenn das Unternehmen diesen Domain-Namen bereits zur Anmeldung für Google-Apps for Work verwendet hat, finden Sie Informationen zur Aktivierung von Android Enterprise unter **https://support.google.com/work/android/answer/6174062**.

Verbinden von Ivanti Neurons for MDM mit Android Enterprise

Sobald Sie sich bei Android Enterprise angemeldet haben, richten Sie Ivanti Neurons for MDM als UEM-Server ein.

Anfordern der Anmeldeinformationen für Android Enterprise

Verfahren

1. Wechseln Sie zu **Admin > Android Enterprise**.
2. Klicken Sie auf die **Google Developers Console**.
3. Klicken Sie auf die erste angezeigte Verknüpfung, um zur Google Developers Console zu wechseln.
4. Wählen Sie aus dem DropDown-Menü die Option **Projekt erstellen**.
5. Geben Sie einen Namen für das Projekt ein.
6. Akzeptieren Sie die Nutzungsbedingungen.
7. Klicken Sie auf **Erstellen**.
8. Klicken Sie auf **API** .
9. Wählen Sie die **APIs** aus.
10. Geben Sie in dem Suchfeld „**emm**“ ein, um die EMM-API in Google Play zu finden.
11. Klicken Sie auf den Link **Google Play EMM API**.
12. Klicken Sie auf**API aktivieren**.
13. Klicken Sie auf **Anmeldeinformationen**.
14. Wählen Sie das **Dienstkonto**.
15. Klicken Sie auf **Erstellen**, um die JSON-Datei zu speichern.

Hinzufügen Ihres Android Enterprise MDM-Tokens zu Ivanti Neurons for MDM

Verfahren

1. **https://admin.google.com**Melden Sie sich unter **https://admin.google.com** an.
2. Klicken Sie auf Sicherheit.
3. Falls die Android Enterprise-Einstellungen nicht angezeigt werden, klicken Sie auf **Mehr anzeigen**.
4. Wählen Sie **Android Enterprise-Einstellungen** aus.
5. Kopieren Sie unter Enterprise Mobility Management-Anbieter verwalten das MDM-Token.
6. Kehren Sie zum Ivanti Neurons for MDM-Portal zurück.
7. Klicken Sie auf Fertig.
8. Fügen Sie in Feld 2 das MDM-Token ein, das Sie gerade kopiert haben.

9. Geben Sie in dem Feld Domain die Domain ein, die Sie bei Google angegeben haben.
10. Klicken Sie auf Datei auswählen und laden Sie die JSON-Datei hoch, die Sie zuvor heruntergeladen haben.
11. Klicken Sie auf Verbinden.
    Sobald die Verbindung aufgebaut ist, erscheint die Mitteilung Mit Google verbunden.
12. Klicken Sie im Feld 3 auf **Autorisieren**, um anzugeben, dass Sie Ivanti Neurons for MDM Zugriff auf Ihre Google-Benutzerdaten einräumen möchten.
13. Klicken Sie auf Akzeptieren.
    Die Meldung **Mit Benutzern verbunden** wird im Ivanti Neurons for MDM-Portal angezeigt.

Synchronisieren von Benutzern zwischen Ivanti Neurons for MDM und Google

Damit Sie Android Enterprise für von Ivanti Neurons for MDMIvanti Neurons for MDM verwaltete Android-Benutzer bereitstellen können, muss jeder Benutzer über einen entsprechenden Datensatz im Google Admin Portal verfügen. Die Schritte, die erforderlich sind, um die Benutzerinformationen zwischen Ivanti Neurons for MDM und dem Google Admin-Portal zu synchronisieren, richten sich danach, ob Sie eine Integration mit den Verzeichnisdiensten (AD/LDAP) in Ihrem Unternehmen eingerichtet haben.

Active Directory/LDAP-Benutzer

Wenn Sie eine AD/LDAP-Integration mit Ivanti Neurons for MDM eingerichtet haben, müssen Sie Google Apps Directory Sync verwenden und eine AD/LDAP-Integration with dem Google Admin-Portal einrichten. Weitere Informationen finden Sie unter https://support.google.com/a/answer/106368?hl=en.

Lokale Benutzer

Wenn Sie nur lokale Benutzer in Ivanti Neurons for MDM erstellt haben und keine Integration mit einem Verzeichnisdienst planen, führen Sie die folgenden Schritte zum Synchronisieren dieser Benutzer über das Google Admin-Portal aus:

Verfahren

1. https://admin.google.comMelden Sie sich im Google Admin-Portal unter https://admin.google.com an.
2. Klicken Sie auf **Users**.
3. Klicken auf das Symbol **"Benutzer hinzufügen"** oder **"Mehrere Benutzer hinzufügen"** unten rechts.
4. Fügen Sie für jeden Ivanti Neurons for MDM-Benutzer, der Android Enterprise verwenden wird, einen Google-Benutzer mit demselben Benutzernamen und derselben E-Mail-Adresse wie beim Ivanti Neurons for MDM-Benutzer hinzu.
5. Im Portal Ivanti Neurons for MDM für die einzelnen Ivanti Neurons for MDM-Benutzer, die gerade zum Google Admin-Portal hinzugefügt wurden:
   a. Klicken Sie auf der Registerkarte "Benutzer" auf den Link mit dem Namen des Benutzers, um dessen Benutzerdetails anzuzeigen.
   b. Wählen Sie die Option Benutzer mit Google-Benutzerverzeichnis synchronisieren.
   c. Klicken Sie auf die Option Mit Google-Benutzerverzeichnis synchronisieren.
   T. Überprüfen Sie, ob der Google-Status als "Aktiviert" angezeigt wird.

Bereitstellen von Android Enterprise für unterstützte Geräte

Zum Bereitstellen von Android Enterprise sind zwei Konfigurationen erforderlich:

- Android Enterprise: Die Konfiguration "Arbeitsprofil auf unternehmenseigenem Gerät" aktiviert Android Enterprise.

- Eine Sperr- und Kiosk-Konfiguration definiert die anzuwendenden Android Enterprise-Einschränkungen.

Registrierte Geräte abschalten

In BYOD-Szenarien ist aufgrund des Wechsels von Geräteadmin zu Android Enterprise-Arbeitsprofil auf firmeneigenem Gerät kein Stilllegen und erneutes Registrieren der Gräte erforderlich. Eine Komplettlöschung oder Außerdienststellung des Geräts ist nur beim Wechsel vom Geräteadministrator- in den Geräteeigentümermodus erforderlich.

Wenn Sie ein im Modus Gerätebesitzer/Besitzer erweitertes Profil/Company-Owned Personally Enabled (COPE) registriertes Gerät für die Stilllegung auswählen, wird im Bildschirm eine Popup-Meldung angezeigt. Diese weist darauf hin, dass der Stilllegungsbefehl für firmeneigene Geräte nicht unterstützt wird.

Gerät bereitstellen

Verfahren

1. Gehen Sie im Ivanti Neurons for MDM-Portal zu **Konfigurationen**.
2. Klicken Sie auf **Android Enterprise: Arbeitsprofil**.
3. Klicken Sie auf Bearbeiten.
4. Klicken Sie auf Weiter.
5. Wählen Sie die Option Alle Geräte oder Anpassbar.
6. Nachdem Sie Anpassbar ausgewählt haben, suchen Sie die Gerätegruppen, die die Einstellungen für Android Enterprise empfangen sollen, und wählen diese aus.
7. Klicken Sie auf Fertig.
8. Klicken Sie auf die Option Zurück zur Liste (oben links).
9. Klicken Sie auf +Add.
10. Klicken Sie auf **Sperre & Kiosk: Android Enterprise**.
11. Geben Sie in dem Feld Name den Text ein, mit dem Sie die Konfiguration identifizieren können.
12. Wählen Sie unter Sperrart auswählen die Option Arbeitsprofil.
13. Wählen Sie die Sperr-Einstellungen, die Sie für die Zielgeräte verwenden wollen.
14. Klicken Sie auf Weiter.
15. Wählen Sie die Option Alle Geräte oder Anpassbar.
16. Nachdem Sie "Anpassbar" ausgewählt haben, suchen Sie die Gerätegruppen, die die Einstellungen für Android Enterprise empfangen sollen, und wählen diese aus.
17. Klicken Sie auf Fertig.

> Sie können keine Änderungen an dem Profil mehr vornehmen, sobald es bereitgestellt ist. Stattdessen müssen Sie eine neue Android Enterprise-Konfiguration erstellen und diese bereitstellen.

Bereitstellung bestätigen

Sie können über die folgenden Optionen bestätigen, dass Android Enterprise bereitgestellt wurde:

- Suchen Sie unter **Benutzer > Benutzer**den Eintrag für einen Benutzer und prüfen Sie dann, ob die Option **Google Status aktiviert ist**.

- Klicken Sie unter **Geräte > Geräte** auf den Link eines Geräts und prüfen Sie, ob der Status von **Android Enterprise** auf **Aktiviert** gesetzt ist.

Der Google Status für einen Benutzer sollte als **aktiviert** angezeigt werden. Ist er nicht aktiviert, kann der Benutzer keine Geräte registrieren.

> Bei Unternehmen, die GSuite nicht abonniert haben, ermöglicht die verwaltete Google Play Accounts-Methode, dass Benutzer sich bei Android Enterprise registrieren können. Wenn Android Enterprise als Google Play Accounts eingerichtet wurde, wird der Benutzer erst nach der Registrierung eines Android Enterprise-Geräts als **Google-Status: Aktiviert** angezeigt. Weitere Informationen über **Verwaltete Google Play-Konten** finden Sie unter verwaltete Google Play-Konten.

Apps für Android Enterprise bereitstellen

Jede für Android Enterprise entwickelte App kann Optionen enthalten, die Sie über Ivanti Neurons for MDM konfigurieren können.

Verfahren

1. Gehen Sie im Ivanti Neurons for MDM-Portal zu **Apps >App-Katalog**.
2. Suchen Sie die App im Google Play Store.
3. Klicken Sie auf den App-Eintrag.
4. Berechtigungen für die Benutzer von Android Enterprise akzeptieren.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie eine Verteilungsoption aus.
7. Zeigen Sie **Erweiterte Optionen & App-Konfiguration** an.
8. Beachten Sie für die Optionen die folgenden Anleitungen:
9. Klicken Sie auf **Weiter**.

Einstellung	Beschreibung
Auf einem Gerät installieren	Wählen Sie diese Option aus, um die Installation sofort nach der Registrierung zu beginnen. Der Benutzer wird aufgefordert, die Installation der App zu bestätigen, sofern es sich nicht um ein Gerät von Samsung Knox handelt und die nachstehende Option für die Installation im Hintergrund ausgewählt wurde.
App nicht im App-Katalog des Endbenutzers anzeigen	Wählen Sie diese Option aus, wenn Sie nicht wollen, dass der Benutzer die App im App-Katalog des Gerätes sieht.
Bei Samsung-Knox-Geräten im Hintergrund installieren	Wählen Sie die Option, wenn Sie nicht wollen, dass der Benutzer zur Bestätigung der Installation auf Samsung Knox-Geräten aufgefordert wird.
Installationspriorität für Apps festlegen	Bei Android Enterprise-Apps können Sie festlegen, mit welcher Priorität bestimmte Anwendungen vor anderen Anwendungen heruntergeladen werden. Zum Beispiel können Sie festlegen, dass Downloads der Apps Tunnel und Email gegenüber anderen, unkritischen Apps Priorität haben. Folgende Optionen sind für die Prioritätsebenen verfügbar: • **Hoch** • Mittel (standardmäßig ausgewählt) • **Niedrig** Diese Einstellung gilt für interne, öffentliche, private und Web-Apps. Die hausinternen Apps werden über den Client und die öffentlichen und privaten Apps über Google installiert. Die Anwendungspriorität gilt nur für diejenigen Apps, die über denselben Kanal installiert werden.
Nur bei Verbindung über WLAN installieren	Wählen Sie diese Option, um die App nur dann zu installieren, wenn das Gerät mit dem WLAN verbunden ist.
Nur beim Aufladen installieren	Wählen Sie diese Option, um die App nur dann zu installieren, wenn das Gerät gerade aufgeladen wird.
Nur im Leerlauf installieren	Wählen Sie diese Option, um die App nur zu installieren, wenn sich das Gerät im Leerlauf befindet (vom Benutzer nicht aktiv genutzt wird).
Automatischer Start bei der Installation	Wählen Sie diese Option, um eine Anwendung nach der Installation automatisch zu starten. Diese Funktion ist nur verfügbar, wenn die App neu auf dem Gerät installiert wird (nicht bei einem Versions-Update).

10. Wählen Sie eine Verteilungsoption aus.
11. Klicken Sie auf **Fertig**.

Unternehmens-Apps konfigurieren

Android Enterprise-Apps sind im Abschnitt "Business-Apps" des App-Kataologs verfügbar, darunter die folgenden Apps:

- **Divide Productivity**
- Email+
- Tunnel
- Gmail

10.10.4.6. Android Enterprise: Work Managed-Gerät, nicht GMS-Modus (AOSP)

Ivanti Neurons for MDM unterstützt die Registrierung des Geräteeigentümers von Work Managed, nicht GMS-Modus (AOSP)-Geräten, ohne dass dafür Google Mobile Services (GMS) erforderlich sind. Es handelt sich um eine Systemkonfiguration, Administratoren können die Konfiguration nicht hinzufügen. Administratoren können sie verteilen oder die Verteilung rückgängig machen.

Verfahren

1. Melden Sie sich mit Benutzeranmeldedaten bei Ivanti Neurons for MDM an.
2. Konfigurationen durchsuchen für Android Enterprise: Work Managed-Gerät, nicht GMS-Modus (AOSP).
3. Bearbeiten Sie die Konfiguration und verteilen Sie sie an die entsprechenden Gerätegruppen. Beispiel: Android-Geräte.
4. Klicken Sie auf **Fertig**.

10.10.4.7. Android Work Challenge

Dieser Abschnitt enthält folgendes Thema:

- Challenge-Konfiguration für Android für Unternehmen erstellen:
- Einstellungen für das Konfigurations-Setup

Lizenz: Silver

Eine Konfiguration für Android Work Challenge (Android-Unternehmens-Herausforderung) definiert sichere Passwörter für die Benutzer, die auf Arbeitsprofil, Daten und Apps zugreifen wollen. Erfordert ein Android Enterprise-Arbeitsprofil.

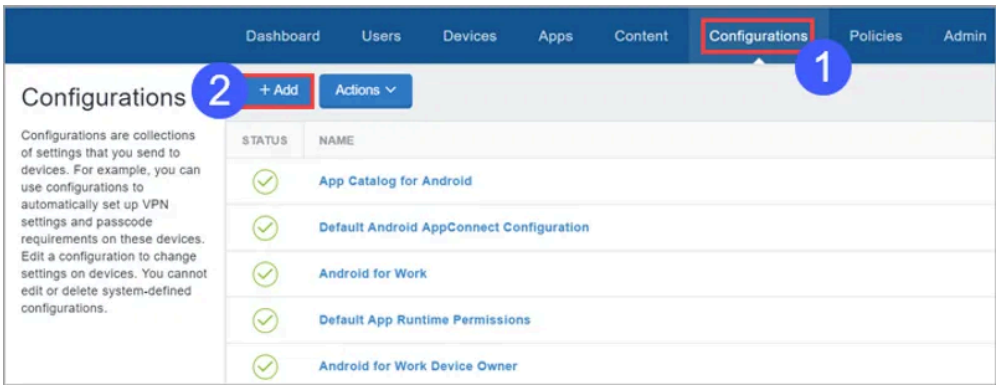
Hinweise zur Implementierung:

- Administratoren können eine Gerätepasswortrichtlinie und eine Arbeitsprofilpasswortrichtlinie unabhängig voneinander verwenden.
- Die Cloud sendet diese Konfiguration nur an Clients mit älteren Versionen als Android 7.0, weil diese Geräte diese Funktion nicht unterstützen.
  Ivanti Neurons for MDM sendet diese Konfiguration nur an Geräte mit einem Arbeitsprofil für Android Enterprise.

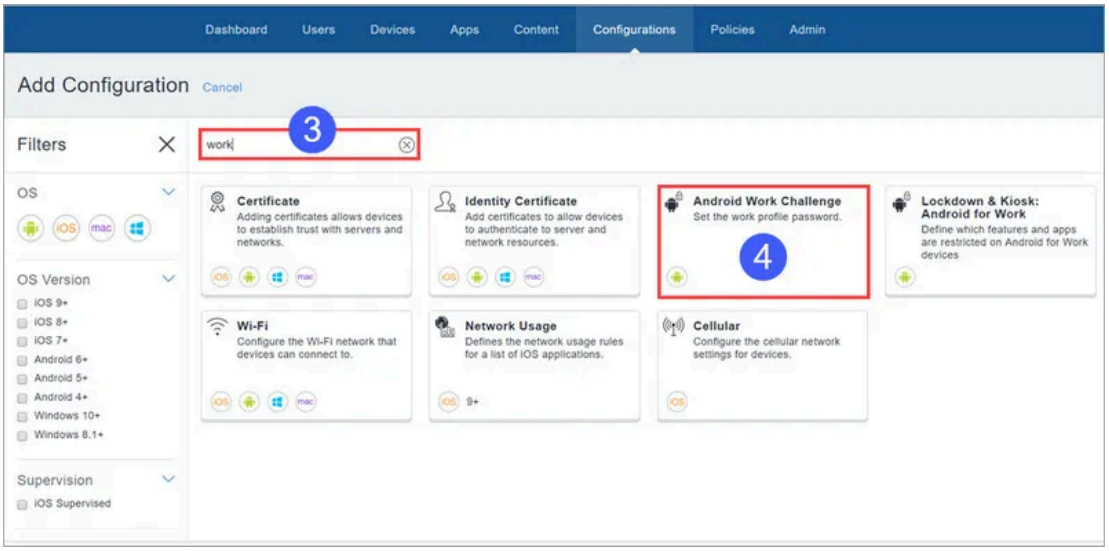
Challenge-Konfiguration für Android für Unternehmen erstellen:

Verfahren

1. Klicken Sie auf **Konfigurationen**.

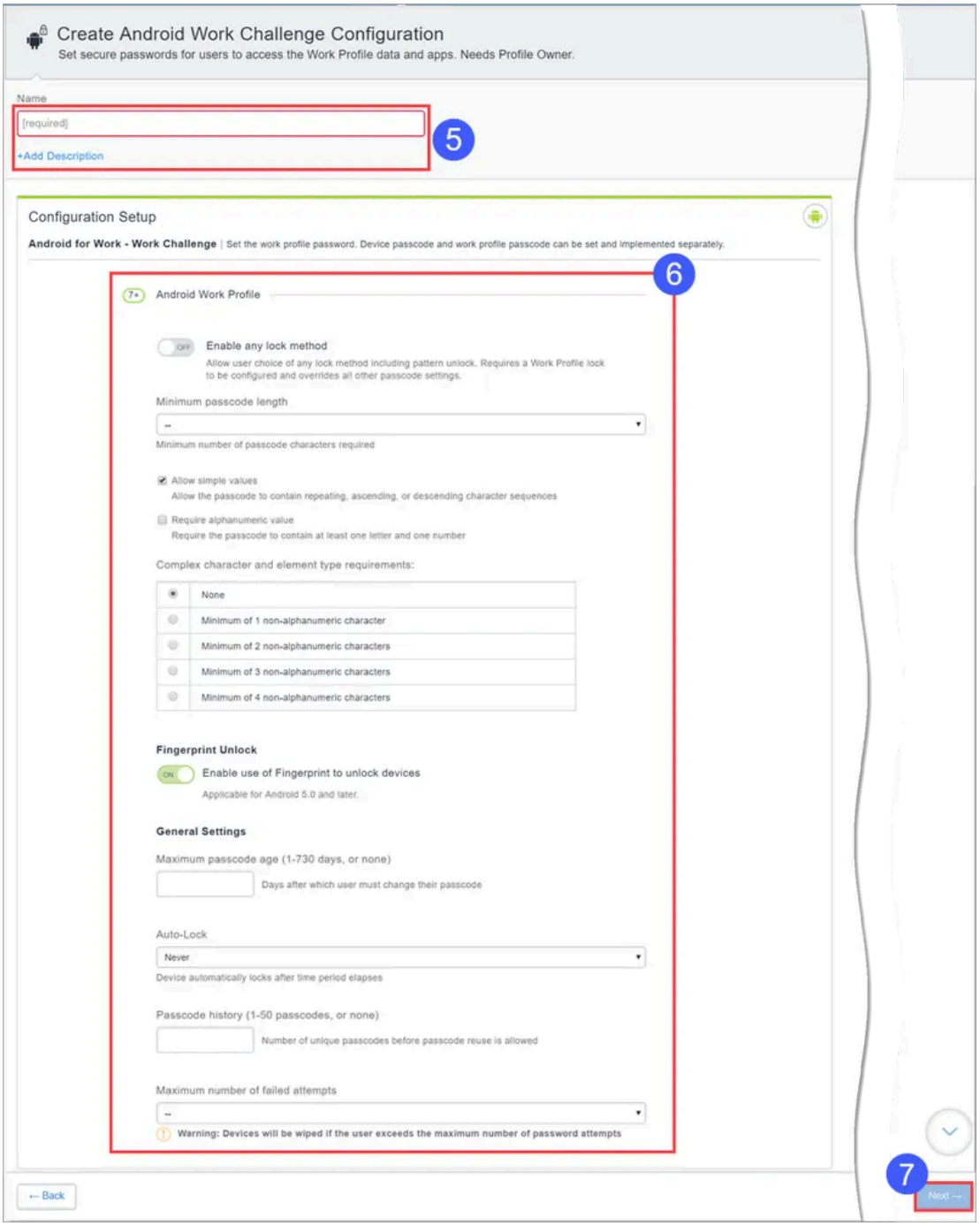


Klicken Sie auf **+Hinzufügen**.



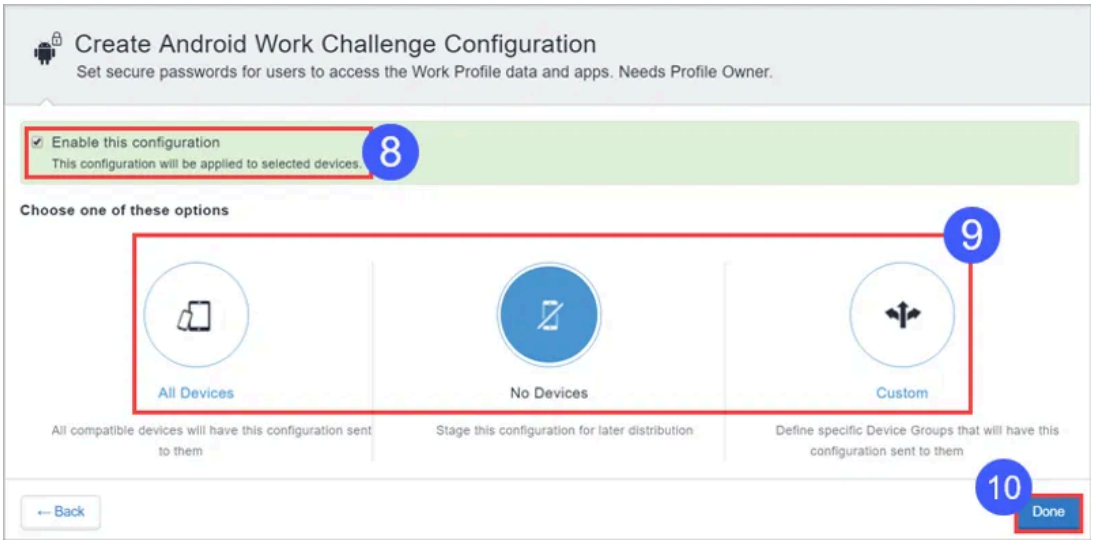
Geben Sie in dem Suchfeld „Work“ ein.

4. Wählen Sie die **Android Work Challenge (Android-Unternehmens-Herausforderung)** aus.



Geben Sie einen Namen für die Konfiguration und ggf. eine Beschreibung ein.

6. Verwenden Sie die Konfigurations-Setup-Felder, um die Konfiguration zu erstellen. Details zu den Einstellungen finden Sie unter **Konfigurations-Setup-Einstellungen**.
7. Klicken Sie auf **Weiter →**.



Aktivieren Sie gegebenenfalls die Konfiguration.

9. Konfigurieren Sie die Verteilungseinstellungen für alle Geräte, keine Geräte oder eine benutzerdefinierte Reihe von Geräten.
10. Klicken Sie auf **Fertig**.

Einstellungen für das Konfigurations-Setup

Einstellung	Aktion
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Alle Sperrmethoden aktivieren	Erlaubt dem Benutzer die Auswahl einer beliebigen Sperrmethode, beispielsweise eine Entsperrung mit Hilfe von Mustern. Überschreibt alle anderen Passcodeeinstellungen.
Minimale Passcodelänge	Wählen Sie für den Passcode eine Mindestlänge von 4 bis 16 Zeichen.
Einfache Werte zulassen	Sich wiederholende, aufsteigende oder absteigende Zeichenfolgen für das Passwort zulassen.
Alphanumerischer Wert erforderlich	Das Passwort muss mindestens einen Buchstaben und eine Zahl enthalten.
Komplexe Zeichen und Elementtypeneigenschaften	Konfigurieren Sie die Anforderungen für komplexe Zeichen und Elementtypen in folgender Reihenfolge: • Kein/e • Mindestens ein nicht-alphanumerisches Zeichen • Mindestens 2 Sonderzeichen • Mindestens 3 Sonderzeichen • Mindestens 4 Sonderzeichen
Entsperrung per Fingerabdruck	Benutzer können damit ihre Geräte per Fingerabdruck entsperren.
Maximale Gültigkeitsdauer des Passworts	Konfigurieren Sie ein maximales Passwortalter von 0 bis 730 Tagen.
Automatische Sperre	Wählen Sie einen Zeitraum aus, nach dem sich das Gerät automatisch sperrt. Ein solcher Zeitraum kann zwischen null und fünfzehn Minuten liegen.
Passwortverlauf	Geben Sie an, wie viele verschiedene Passcodes definiert werden müssen, bevor ein alter Passcode wiederverwendet werden darf. Der Bereich kann zwischen 0 und 50 Passcodes liegen.
Maximale Anzahl an Fehlversuchen	Definieren Sie die maximal zulässige Anzahl der Fehlversuche. **WARNUNG: Ivanti Neurons for MDM löscht Geräte komplett, wenn der Benutzer die maximale Anzahl falscher Kennworteingaben überschreitet!**

10.10.4.8. Zertifikatskonfiguration

Eine Zertifikatskonfiguration bestimmt ein Zertifikat zur Verteilung an Geräte. Zertifikate ermöglichen sichere Verbindungen zwischen den Geräten und Server- und Netzwerkressourcen. Ab Version 76 unterstützen wir nur noch v3-Zertifikate.

Als Administrator können Sie jetzt Cloud-Zertifikate für die Smartcard-Anmeldung und benutzerdefinierte Objekt-IDs (OIDs) erzeugen. Sie können Zertifikate für die folgenden Authentifizierungsoptionen erzeugen:

- Client-Authentifizierung - standardmäßig aktiviert
- IPSEC - optional, kann vom Administrator aktiviert werden
- Smartcard-Anmeldung - optional, der Administrator kann diese aktivieren.
- Benutzerdefinierte OIDs - optional, Administrator kann diese aktivieren.

Diese Funktion ist nur für die folgenden Zertifizierungsstellen (CA) verfügbar:

- Lokale Zertifikatsautorität
- Zwischengeschaltete Zertifizierungsstelle
- Externe Zertifizierungsstelle - Konfiguration der Anwendungsrichtlinien der CA-Vorlage im NDES-Server zur Unterstützung von IPSEC, Smartcard-Anmeldung und benutzerdefinierten OIDs
- SCEP-Zertifizierungsstelle vor Ort

Konfiguration verteilen

Ab Ivanti Neurons for MDM Release 91 können globale Administratoren Space-Administratoren zur Bearbeitung der Zertifikatkonfiguration für alle Geräte und für die Option zur benutzerdefinierten Verteilung delegieren. Für die Zertifikatkonfiguration können Sie optional "Diese Konfiguration in allen Spaces verfügbar machen" auswählen. Mit dieser Option wird die Zertifikatkonfiguration allen Spaces zur Verfügung gestellt. Sie kann dann in Exchange, WLAN, VPN, Per-App VPN und anderen geeigneten Konfigurationen, genutzt werden. Diese Option eignet sich für Szenarien, in denen die Zertifikatkonfiguration nur an Geräte (in Nicht-Standard-Spaces) als Teil der zugeordneten Konfigurationen verteilt werden muss und nicht als Einzelkonfiguration.

Verfahren

1. Geben Sie einen Namen in das Feld Name ein.
2. Laden Sie die Zertifikatdatei hoch.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie die Option **Diese Konfiguration aktivieren**.
5. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - **Alle Geräte** . Wählen Sie eine der folgenden Optionen aus:
        - **Nicht für andere Spaces übernehmen**.
        - **Auf Geräte in anderen Spaces anwenden**.
            - Aktivieren Sie das Kontrollkästchen **Space Admin zur Bearbeitung der Verteilung zulassen**, um den delegierten Space-Administratoren die Bearbeitung der Verteilung für den jeweiligen Space zu ermöglichen.
    - **Keine Geräte** (Standard)
    - **Benutzerdefiniert** Wählen Sie eine der folgenden Optionen aus:

10.10.4.9. Zertifikatstransparenz

Gilt für: iOS 12.1.1, macOS 10.14.2, tvOS 12.1.1, watchOS 10.0+, visionOS 1.1+ und unterstützte neuere Versionen.

Kontrolliert die Durchsetzung der Zertifikatstransparenz, die nur in einem Geräteprofil erscheinen darf. Sie können mehrere Zertifikate hinzufügen und bei Bedarf Domains deaktivieren.

Konfiguration für die Zertifikatstransparenz erstellen

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie in dem Suchfeld **certificate** ein und klicken Sie dann auf die Konfiguration **Zertifikatstransparenz**.
4. Geben Sie einen Namen ein und beschreiben Sie die Konfiguration.
5. Geben Sie die **Domains an, die deaktiviert werden sollen**. Klicken Sie auf **+Domäne** hinzufügen, um mehr als eine Domäne hinzuzufügen. Für Subdomains kann ein vorangestellter Punkt verwendet werden, jedoch darf eine Domainabgleichsregel nicht für alle Domains einer Top-Level-Domain gelten. So sind beispielsweise „.example.com“ und „.example.co.uk“ erlaubt, „.com“ und „.co.uk“ dagegen nicht. Domains mit Jokerzeichen werden nicht unterstützt.
6. Geben Sie den Zertifikatshash nach Auswahl eines Algorithmus (SHA 256) an. Klicken Sie auf **+ Hinzufügen**, um mehr als einen Zertifikatshash hinzuzufügen.
7. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
8. Klicken Sie auf **Fertig**.

Um die durch den Hash-Schlüssel im subjectPublicKeyInfo-Dictionary spezifizierten Daten zu erzeugen, benötigen Sie den folgenden Befehl für ein PEM-codiertes Zertifikat:

```
openssl x509 -pubkey -in example_certificate.pem -inform pem | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

Wenn Ihr Zertifikat DER-kodiert ist, verwenden Sie den folgenden Befehl:

```
openssl x509 -pubkey -in example_certificate.der -inform der | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.4.10. Konfiguration der Zertifikatswiderrufsprüfung

Diese Konfiguration ermöglicht es den Administratoren, eine Reihe von Zertifikaten zu prüfen, die von einem Gerät entfernt wurden. Administratoren können eine Zertifizierungsstelle (CA) angeben, die es der Konfiguration ermöglicht, die Widerrufsprüfung für alle Zertifikate zu aktivieren, die mit dieser CA verknüpft sind.

Gilt für: iOS 14.2+ und visionOS 1.1+

Verfahren

1. Gehen Sie zu Konfigurationen > +Hinzufügen.
2. Geben Sie Zertifikat in das Suchfeld ein, und klicken Sie dann auf die Konfiguration Zertifikatswiderrufsprüfung.
3. Geben Sie einen Namen und eine Beschreibung der Konfiguration ein.
4. Wählen Sie als Algorithmus SHA 256 und geben Sie den Hash des Stammzertifikats ein.

> Unter „Hash“ müssen Sie einen Base64-kodierten (binären) SHA-256-Hash des öffentlichen Zertifikatschlüssels eingeben. **https://support.apple.com/en-us/HT209143**Unter Apple-Dokumentation finden Sie die verfügbaren vertrauenswürdigen Stammzertifikate für Apple-Betriebssysteme. Sie können in dieser Konfiguration mehrere Stammzertifikate hinzufügen.

5. Klicken Sie auf Weiter.
6. Wählen Sie die Option Diese Konfiguration aktivieren.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
8. Klicken Sie auf Fertig.

10.10.4.11. Erstellen einer Konfiguration für den autonomen Einzel-App-Modus

Anhand der Konfiguration "Autonomer Einzel-App-Modus" lässt sich sicherstellen, dass nur bestimmte Anwendungen auf einem Gerät ausgeführt werden. Auch wenn der Benutzer versucht, eine andere Anwendung zu starten, lässt die Konfiguration immer nur die festgelegte Anwendung zu.

Verfahren

1. Wechseln Sie zu **Konfigurationen** > **Hinzufügen** > **Autonomer Einzel-App-Modus**.
2. Definieren Sie mit den folgenden Richtlinien die App- und zugehörige Einstellungen.
3. Klicken Sie auf **Weiter**.

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Konfigurations-Setup	**Bundle-ID** – (Erforderlich) Die eindeutige Kennung für das Bundle. Wenn zwei Wörterbücher denselben BundleIdentifier-Wert, aber einen unterschiedlichen TeamIdentifier-Wert enthalten, wird dies als Fehler interpretiert und das Profil wird nicht installiert. **Team-ID** – (Erforderlich) Die Teamkennung des Entwicklers, die beim Signieren der App verwendet wurde.

4. Wählen Sie im Bildschirm **Verteilung** die Gruppen aus, die diese Konfiguration erhalten sollen.
5. Klicken Sie auf **Fertig**.

10.10.4.12. Erstellen der DNS-Proxykonfiguration

Als Ivanti Neurons for MDM-Administrator können Sie die DNS-Proxyeinstellungen konfigurieren, indem Sie für Benutzer von iPhone- und iPad-Geräten die DNS-Proxykonfiguration verwenden. Anhand der DNS-Proxy-Payload legen Sie die App fest, die die DNS-Proxy-Netzwerkerweiterung und andere anbieterspezifische Werte bereitstellt.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Wechseln Sie zu **Konfigurationen**.
3. Geben Sie **DNS** in das Suchfeld ein und klicken Sie dann auf **DNS-Proxykonfiguration**.
4. Geben Sie einen Namen ein und beschreiben Sie die Konfiguration.
5. Machen Sie folgende Angaben für die DNS-Proxykonfiguration:
    - App-Bundle-Kennung (erforderlich)
    - Anbieter-Bundle-Kennung
    - Anbieterkonfiguration (Schlüssel-Wert)
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Option **Diese Konfiguration aktivieren**.
8. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar

Klicken Sie auf **Fertig**.

10.10.4.13. Konfigurieren der Geräteprotokollierung

Über die Konfiguration der Geräteprotokollierung aktivieren Sie Netzwerk- und Sicherheitsprotokolle für Android-Geräte.

Erstellen einer Konfiguration für die Geräteprotokollierung

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie in das Suchfeld **Geräteprotokollierung** ein und wählen Sie die Konfiguration aus.
4. Geben Sie einen Namen ein und beschreiben Sie die Konfiguration.
5. Wählen Sie unter dem Abschnitt **Konfigurations-Setup** eine oder beide der folgenden Optionen aus:
    - Netzwerkprotokollierung aktivieren
    - Sicherheitsprotokollierung aktivieren

> Welche Android-Versionen für die Sicherheits- und Netzwerkprotokollierung unterstützt werden, ist in den Tabellen unter **Matrix für Sicherheitsprotokollierung** angegeben.

Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.

7. Klicken Sie auf **Fertig**.

Matrix für Sicherheitsprotokollierung

Gerätetyp	Unterstützte Android-Versionen
Work Managed-Geräte und Work Managed-Geräte, nicht GMS-Modus (AOSP)	7, 8, 9, 10, 11, 12, 13
Verwaltete Geräte mit Arbeitsprofil	8, 9, 10
Arbeitsprofil	Entfällt
Arbeitsprofil auf unternehmenseigenem Gerät	11, 12, 13

Matrix für Netzwerkprotokollierung

Gerätetyp	Unterstützte Android-Versionen
Work Managed-Geräte und Work Managed-Geräte, nicht GMS-Modus (AOSP)	8, 9, 10, 11, 12, 13
Verwaltete Geräte mit Arbeitsprofil	8, 9, 10
Arbeitsprofil	12, 13
Arbeitsprofil auf unternehmenseigenem Gerät	12, 13

Nach dem Installieren der Konfiguration für die Geräteprotokollierung auf dem Gerät erhält der Benutzer eine Benachrichtigung mit Infos zur Geräteverwaltung und Netzwerkprotokollierung. Klicken Sie zum Bestätigen der Benachrichtigung auf **OK**.

Anfordern von Debugprotokollen

Verfahren

1. Melden Sie sich bei Ivanti Neurons for MDM an.
2. Wechseln Sie zu **Geräte** > **Gerätedetails**.
3. Klicken Sie im Abschnitt **Übersicht** auf die drei vertikalen Punkte neben der Schaltfläche **Anmeldung erzwingen**.
4. Wählen Sie **Debugprotokolle anfordern** aus.
5. Wählen Sie eine der folgenden zwei Optionen aus:
    - Fehlerbericht ausschließen – Wenn Sie diese Option auswählen und auf "Weiter" klicken, wird ein Bestätigungsfenster im Bildschirm angezeigt. Klicken Sie auf **Debugprotokolle anfordern**. Benutzer müssen keine Zustimmung zu dieser Option erteilen. Die Protokolle schließen den Fehlerbericht für die ausgewählten Android-Geräte aus.
    - Fehlerbericht einschließen – Wenn Sie diese Option auswählen und auf "Weiter" klicken, wird ein Bestätigungsfenster im Bildschirm angezeigt. Klicken Sie auf **Debugprotokolle anfordern**. Benutzer müssen ihre Zustimmung zur Freigabe des Fehlerberichts erteilen. Bei Android-Geräten werden die Benutzer aufgefordert, die Geräteprotokolle mit Fehlerbericht einzureichen.

10.10.4.14. Konfiguration "Datenträgerverwaltung"

Ivanti Neurons for MDM Die Konfigurationseinstellungen für die Datenträgerverwaltung definieren die Richtlinien für das effektive Verwalten von Daten in externen und netzwerkinternen Speichergeräten.

Gilt für: macOS 15.0 überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird.

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Datenträgerverwaltung** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie die Einstellungen für die **Datenträgerverwaltung** gemäß der folgenden Tabelle:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Datenträgerverwaltung	
Externer Speicher	Wählen Sie einen der folgenden Werte aus der Dropdownliste aus: • **Zulässig**: Erlaubt das Lesen und Beschreiben des Speichers. • **Schreibgeschützt**: Erlaubt das Lesen des Speichers. • **Nicht erlaubt**: Unterbindet den Zugriff auf den Speicher.
Netzwerkspeicher	Wählen Sie einen der folgenden Werte aus der Dropdownliste aus: • **Zulässig**: Erlaubt das Lesen und Beschreiben des Speichers. • **Schreibgeschützt**: Erlaubt das Lesen des Speichers. • **Nicht erlaubt**: Unterbindet den Zugriff auf den Speicher.

4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
5. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Datenträgerverwaltung** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
6. Klicken Sie auf **Fertig**.

10.10.4.15. Android-Verschlüsselung

Eine Verschlüsselungskonfiguration definiert die Anforderungen für die Geräteverschlüsselung für Android-Geräte im Geräteverwaltungsmodus. Die Geräteverschlüsselung stellt sicher, dass über bekannte Jailbreak- oder Root-Exploits nicht auf vertrauliche Unternehmensdaten zugegriffen werden kann. Eine Verschlüsselung speichert die Daten eines Gerät in unlesbarer Form, sodass im Fall eines Diebstahls niemand auf die Daten zugreifen kann.

Bei Aktivierung der Verschlüsselung wird der Benutzer aufgefordert, das Gerät zu verschlüsseln und ein Gerätepasscode einzurichten. Mit dem Passwort werden die Daten entschlüsselt und lesbar gemacht. Die Geräteverschlüsselung wird auf Android Enterprise (Arbeitsprofil oder verwaltete Geräte) oder iOS-Geräten automatisch aktiviert, wenn ein Passcode festgelegt ist. Das Gerät kann nicht verwendet werden, während es verschlüsselt wird. Sobald die Verschlüsselung aktiv ist, muss das Gerät zum Ausschalten auf die Werkseinstellungen zurückgesetzt werden.

Verschlüsselungseinstellungen

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Geräteverschlüsselung aktivieren	Bestimmen Sie die Einstellung zur Aktivierung der Verschlüsselung für alle verschlüsselungsfähigen Android-Geräte, die diese Konfiguration erhalten.

> Die Android-Verschlüsselungskonfiguration ist für Samsung-Geräte im Geräte-Admin-Modus auf Android 11 veraltet. Die Verschlüsselung wird auf Android Enterprise-Geräten standardmäßig unterstützt, wenn ein Passcode für das Gerät festgelegt ist.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.4.16. Verschlüsselter DNS

Lizenz: Gold

Gilt für:

- iOS 14.0 oder unterstützte neuere Versionen.
- macOS 11.0 oder unterstützte neuere Versionen.
- visionOS 1.1 oder unterstützte neuere Versionen

Konfigurieren Sie einen verschlüsselten DNS, um die Sicherheit zu erhöhen, ohne VPN zu konfigurieren.

Dieser Abschnitt enthält die folgenden Themen:

- Verschlüsselte DNS-Konfiguration
- Verschlüsselte DNS-Konfigurationseinstellungen

Verschlüsselte DNS-Konfiguration

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie in dem Suchfeld **DNS** ein und klicken Sie dann auf die Konfiguration **Verschlüsselter DNS**.
4. Geben Sie einen Namen ein und beschreiben Sie die Konfiguration.
5. Geben Sie die Konfigurationseinstellungen für Verschlüsselter DNS ein.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Option **Diese Konfiguration aktivieren**.
8. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
9. Klicken Sie auf **Fertig**.

Verschlüsselte DNS-Konfigurationseinstellungen

Verwenden Sie die Einstellungen in der folgenden Tabelle, um verschlüsselte DNS zu konfigurieren. Weitere Informationen zu diesen Einstellungen finden Sie in der Apple-Dokumentation.

Einstellung	Beschreibung
DNS-Einstellungen	Ein Wörterbuch, das eine Konfiguration für einen verschlüsselten DNS-Server definiert.
DNS-Protokoll	Legen Sie das verschlüsselte Transportprotokoll für die Kommunikation mit dem DNS-Server fest. Wählen Sie eines der folgenden Protokolle aus: • HTTPS • TLS
Server-URL	Die URI-Vorlage eines DNS-over-HTTPS-Servers entsprechend der Definition in RFC 8484. Diese URL muss das Schema https:// verwenden, der Hostname oder die Adresse in der URL werden zur Validierung des Serverzertifikats verwendet. Wenn keine Serveradressen angegeben sind, werden der Hostname oder die Adresse in der URL zur Ermittlung der Serveradressen verwendet. Dieser Schlüssel muss nur vorhanden sein, wenn das DNS-Protokoll HTTPS ist.
Server-Adressen	Eine ungeordnete Liste von DNS-Server-IP-Adress-Strings. Diese IP-Adressen können sowohl IPv4- als auch IPv6-Adressen sein. Klicken Sie auf **Hinzufügen**, um eine oder mehrere Serveradressen hinzuzufügen.
Ergänzende Match-Domains	Eine Liste von Domain-Strings, mit denen festgelegt wird, welche DNS-Anfragen den DNS-Server verwenden. Wenn dieses Array nicht angegeben wird, verwenden alle Domains den DNS-Server. Klicken Sie auf **Hinzufügen**, um eine oder mehrere Domains hinzuzufügen.
Benutzer an der Deaktivierung von DNS-Einstellungen hindern.	Hindert Benutzer an der Deaktivierung von DNS-Einstellungen. Diese Funktion gibt es nur bei überwachten Geräten.
Demand-Regeln	Ein Array von Regeln, die die DNS-Einstellungen definieren. Wenn keine Regeln vorhanden sind, verwendet das System immer die DNS-Einstellungen. Klicken Sie auf **+ Demand-Regeln hinzufügen**, um mindestens einen Satz von Demand-Regeln hinzuzufügen.
[Network]	Die Aktion, die ausgeführt werden soll, wenn dieses Wörterbuch zum aktuellen Netzwerk passt. Wählen Sie eine der folgenden Aktionen: • **Verbinden:** DNS-Einstellungen übernehmen, wenn das Wörterbuch einen passenden Eintrag enthält. • **Trennen:** DNS-Einstellungen nicht übernehmen, wenn das Wörterbuch einen passenden Eintrag enthält. • **Verbindung prüfen:** DNS-Einstellungen mit Ausnahmen pro Domain anwenden, wenn das Wörterbuch einen passenden Eintrag enthält.
[Evalutate Connection]	Diese Netzwerkoption hat folgende Einstellungen: • **Domain-Aktion** - Das Verhalten der DNS-Einstellungen für die angegebenen Domains. Wählen Sie eine der folgenden Aktionen: ◦ **Niemals verbinden** - Die DNS-Einstellungen für die angegebenen Domains nicht verwenden. ◦ **Bei Bedarf verbinden**- Die Verwendung der DNS-Einstellungen für die angegebenen Domains erlauben.

Einstellung	Beschreibung
	• **Domains** - Die Domains, für die diese Prüfung gilt. Klicken Sie auf **+ Hinzufügen**, um eine oder mehrere Domains hinzuzufügen.
Regeln	Klicken Sie auf **+ Hinzufügen**, um mindestens eine Regel hinzuzufügen, die die folgenden Parameter mit den angegebenen Werten abgleicht.
DNS-Domänen-Abgleich	Ein Array von Domainnamen. Diese Regel passt, wenn einer der Domainnamen in der angegebenen Liste mit einer Domain in der Liste der Suchdomains des Geräts übereinstimmt.
DNS-Serveradressen-Abgleich	Ein Array von IP-Adressen. Diese Regel passt, wenn einer der angegebenen DNS-Server des Netzwerks mit einem Eintrag im Array übereinstimmt.
SSID-Abgleich	Ein Array von SSIDs zum Abgleich mit dem aktuellen Netzwerk. Wenn es sich bei dem Netzwerk nicht um ein WLAN handelt oder wenn SSID nicht in diesem Array erscheint, schlägt der Abgleich fehl. Lassen Sie diesen Schlüssel und das entsprechende Array weg, um einen Abgleich mit jeder SSID durchzuführen.
Schnittstellentyp-Abgleich	Ein Schnittstellentyp. Wenn diese Regel definiert ist, wird sie nur erfüllt, wenn die Hardware der primären Netzwerkschnittstelle dem angegebenen Typ entspricht. Klicken Sie auf eine der folgenden Typen: • Ethernet • WLAN • Mobilfunk
URL-Zeichenfolgen-Test	Eine URL zum Prüfen. Wenn diese URL erfolgreich aufgerufen wird (und als HTTP-Statuscode 200 zurückgibt), ohne dass eine Umleitung erfolgt, ist diese Regel erfüllt.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.4.17. Externe Intelligence-Einstellungen

Mithilfe von **Externe Intelligence-Einstellungen** konfigurieren Sie externe Intelligence-Integrationen auf überwachten Geräten. Diese Konfiguration hilft Administratoren, konsistente, richtlinienbasierte Einstellungen anzuwenden, die steuern, wie Geräte unterstützte externe Intelligence-Dienste verbinden und verwenden.

Gilt für:

- iOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- macOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- visionOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Externe Intelligence-Einstellungen** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie **Externe Intelligence-Einstellungen** gemäß der folgenden Tabelle:

Einstellung	Aktion
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Externe Datenintegrationen zulassen	Aktivieren Sie das Kontrollkästchen, um External Intelligence-Integrationen zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um externe Intelligence-Integrationen auf überwachten Geräten zu aktivieren.
Anmeldung externer Intelligence-Integrationen zulassen	Aktivieren Sie das Kontrollkästchen, um die Anmeldung von External Intelligence-Integrationen zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um die Anmeldung von externen Intelligence-Integrationen auf überwachten Geräten zu aktivieren.
Externe Intelligence Workspace-IDs zulassen	Geben Sie die Workspace-IDs ein, um External Intelligence zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um externe Intelligence für die eingegebenen Workspace-IDs auf überwachten Geräten zu aktivieren.

4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
5. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Externe Intelligence-Einstellungen** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
6. Klicken Sie auf **Fertig**.

10.10.4.18. Bedrohungsabwehr

Gilt für:

- Wählen Sie die iOS-Client-Version 3.2.0 oder eine unterstützte neuere Version.
- Wählen Sie die Android-Client-Version 52 oder eine unterstützte neuere Version.

Cloud bietet die Möglichkeit, Aktivierungs-Tokens zu verteilen, um die in Go integrierte Threat Defense-Technologie für Android- und iOS-Clients zu aktivieren. Threat Defense schützt verwaltete Geräte vor mobilen Bedrohungen und Sicherheitslücken, die die Sicherheit des Geräts, des Netzwerks und der Anwendungen gefährden.

Wenn diese Konfiguration in der Cloud aktiviert ist und für die Geräte übernommen wird, werden die Bibliotheken von Threat Defense auf den GO-Clients aktiviert. Den Dienst Threat Defense können Sie durch Entfernung des Lizenz-Tokens und erneuten Versand der Lizenzkonfiguration an den Client deaktivieren.

Threat Defense überwacht:

- Auf Geräteebene: Systemparameter, Konfiguration, Firmware und Bibliotheken zur Identifikation verdächtiger oder Schadsoftware-Aktivitäten.
- Auf Netzwerkebene: Netzwerk-Traffic und verdächtige Verbindungen zu und von mobilen Geräten.
- Auf App-Ebene: unsichere Apps (die möglicherweise Unternehmensdaten gefährden) sowie Apps mit Schadsoftware durch Risikobewertung und Code-Analyse.

Aktuelle Dokumentation

Die neuesten Anweisungen zu Threat Defense finden Sie im *Ivanti Neurons for MDM Threat Defense Solution Guide* auf der Website für Produktdokumentationen unter **Ivanti Neurons for MDM-Produktdokumentation**.

10.10.4.19. FileVault 2

Lizenz: Gold

Mit FileVault 2 kann eine vollständige XTS-AES 128-Bit-Verschlüsselung des Datenträgerinhalts erfolgen.

Wenn Sie die Option „FileVault 2“ aktivieren, können Sie folgende Einstellungen konfigurieren:

Kategorie	Einstellungen
FileVault-Benutzereinstellungen	• FileVault bei SetupAssist aktivieren **Standard:** Falsch • Falls wahr, und wenn die Payload nach dem Registrieren bei Ivanti Neurons for MDM in Setup Assistant installiert wird, wird Setup Assistant veranlasst, FileVault beim Setup zu aktivieren. Das System ignoriert außerdem alle anderen Schlüssel der Payload, mit Ausnahme von ShowRecoveryKey. **Voraussetzung**: Stellen Sie vor dem Aktivieren von FileVault in Setup Assistant sicher, dass die Option **Gerätekonfiguration während der Geräteregistrierungseinrichtung abwarten** im Geräteregistrierungsprofil aktiviert ist. • FileVault erst aktivieren, wenn der betreffende Benutzer sich abgemeldet hat. ◦ Benutzer immer zur Aktivierung von FileVault auffordern. ◦ Höchste Zahl der Nichtaktivierungen von FileVault durch den Benutzer Keine Aktivierung von FileVault beim Abmelden des Benutzers verlangen.
Ausgabepfad Persönlicher Wiederherstellungsschlüssel	Geben Sie den Pfad zu dem Ort ein, an dem der Wiederherstellungsschlüssel und die plist mit den Computerdaten gespeichert werden. • Erstellen Sie einen persönlichen Wiederherstellungsschlüssel. • Zeigen Sie den persönlichen Wiederherstellungsschlüssel dem Benutzer an, sobald FileVault aktiviert ist. Diese Option ist nur sichtbar, wennPersönlichen Wiederherstellungsschlüssel erstellenaktiviert ist. Die Option ist standardmäßig deaktiviert. • Wiederherstellungsschlüssel für Institutionen aktivieren: Verwendung von Keychain - wenn bei diesem Payload keine keine Zertifikatsinformationen angegeben sind, wird die bereits erstellte Keychain unter /Library/Keychains/FileVaultMaster.keychain verwendet. Wählen Sie eine der folgenden Optionen aus: ◦ Zertifikat hochladen ◦ Zertifikat ◦ Keychain im Benutzersystem verwenden.
FileVault-Schlüssel nach __ Tagen rotieren	Administratoren können eine regelmäßige Rotation der FileVault-Schlüssel für macOS-Geräte konfigurieren, um das Sicherheitsrisiko für bereitgestellte Geräte zu reduzieren. Administratoren können das Rotationsintervall in Tagen festlegen. Es werden nur persönliche Wiederherstellungsschlüssel rotiert.

10.10.4.20. FileVault-Wiederherstellungsschlüssel

Lizenz: Gold

Die Konfiguration des FileVault-Wiederherstellungsschlüssels prüft auf Umleitung und Treuhänder für die FileVault-Wiederherstellungsschlüssel auf einem Unternehmensserver.

> Die Option zum Ausschluss mit erneuter Übertragung der Konfiguration des File Vault Recovery Key ist deaktiviert, da ein macOS-Gerät bei erneuter Übertragung der Konfiguration keinen Wiederherstellungsschlüssel mehr sendet.

Sie können folgende Optionen einstellen:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	(Optional) Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Konfigurationseinstellungen für macOS <10.13	
Wiederherstellungsschlüssel im Ivanti Neurons for MDM-Mandanten speichern	Klicken Sie auf die Option, damit die Cloud die Schlüssel für Ihren Mandanten speichern kann. Bei Bedarf kann der Schlüssel über die Seite mit den Gerätedetails entschlüsselt werden.
URL auf Server umleiten	Geben Sie die folgenden Einstellungen ein: • Geben Sie den Befehl Redirect URL ein und legen Sie fest, an welche FDE statt an Apple Wiederherstellungsschlüssel gesendet werden sollen. Die URL muss mit https:// beginnen. • Wählen Sie ein Zertifikat aus der Dropdown-Liste. Unterstützt wird nur das Zertifikat im PKCS1-Format.
Konfigurationseinstellungen für macOS 10.13+	
Standort	(Erforderlich) Geben Sie eine Kurzbeschreibung des Ortes ein, an dem der Wiederherstellungsschlüssel verwahrt wird. Dieser Text wird in die Mitteilung eingefügt, die dem Benutzer bei Aktivierung von FileVault angezeigt wird.
Geräteschlüssel	(Optional) Geben Sie einen String ein, der in dem Hilfetext angezeigt werden soll, wenn der Benutzer anscheinend sein Passwort vergessen hat.

10.10.4.21. Konfiguration der FileVault-Optionen

Mit dieser Konfiguration kann der Administrator FileVault aktivieren oder deaktivieren sowie den FileVault-Schlüssel zerstören, wenn das System in den Standby-Modus wechselt.

Gilt für: macOS 10.7+

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Geben Sie in dem Suchfeld FileVault ein und klicken Sie dann auf die Konfiguration FileVault-Optionen.
3. Geben Sie einen Namen und eine Beschreibung der Konfiguration ein.
4. Wählen Sie im Konfigurations-Setup die erforderlichen Einstellungen:
    - FileVault-Schlüssel zerstören, wenn System in den Standby-Modus wechselt
    - Deaktivierung der Festplattenverschlüsselung nicht erlauben
    - Aktivierung der Festplattenverschlüsselung nicht erlauben
5. Klicken Sie auf Weiter.
6. Wählen Sie die Option Diese Konfiguration aktivieren.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
8. Klicken Sie auf Fertig.

10.10.4.22. Identitätszertifikat

Dieser Abschnitt enthält die folgenden Themen:

- Identitätszertifikat – Einstellungen
- Konfiguration verteilen

Eine Identitätszertifikat-Konfiguration definiert einen Authentifizierungszertifikats-Mechanismus für Mobilgeräte. Identitätszertifikate sind X.509-Zertifikate (.p12 oder .pfx). Certificate Management.htmDie Identitätszertifikate können dynamisch mit der Zertifizierungsstelle als Quelle erzeugt werden. Bevor Sie beginnen, sollten Sie bereits wissen, wie Sie die Zertifikate auf Ihre Mobilgeräte verteilen möchten. Sie sollten auch bereits jede nötige Zertifizierungsstelle konfiguriert haben.

> Ab Release 91 wird das Zertifikat "Geräteidentität" für Apple-Geräte automatisch innerhalb von 30 Tagen nach Ablauf verlängert. iOS-Geräte erhalten im Rahmen des regulären Eincheckens des Geräts verlängerte MDM-Zertifikate von Ivanti Neurons for MDM. iOS-Geräte müssen jedoch erneut bei Ivanti Neurons for MDM registriert werden, wenn sie so lange offline waren, dass das MDM-Zertifikat abgelaufen ist, bevor das Einchecken erfolgen konnte, wodurch das Zertifikat vor dem Ablauf verlängert worden wäre.

- SHA-1-Zertifikate werden bei der Erstellung der Identitätszertifikate abgelehnt. Sie können andere Algorithmen auswählen. Bei der Aktualisierung der Zertifikate kann der gleiche SHA-1-Algorithmus verwendet werden, wenn die älteren Zertifikate SHA-1 verwenden. Wenn die älteren Zertifikate einen stärkeren Algorithmus als SHA-1 verwenden, ist eine Umschaltung auf SHA-1 nicht möglich.
- Nach der Konfiguration eines Identitätszertifikats können Sie auf die Option **Konfiguration testen und fortfahren** klicken, um das Prüfzertifikat auszustellen und dessen Gültigkeit zu überprüfen. Bei diesem Test für eine neue oder eine bestehende dynamisch generierte Identitätszertifikatskonfiguration kann ein Fehler angezeigt werden, wenn der Betreffname mit dem der lokalen Zertifizierungsstelle übereinstimmt. Wenn diese Fehlermeldung angezeigt wird, sollten Sie den Betreffnamen des Identitätszertifikats ändern; er sollte sich vom Betreffnamen der lokalen Zertifizierungsstelle unterscheiden. Bei bestehenden Identitätszertifikatskonfigurationen, die mit dem Betreffnamen geändert werden, werden die Zertifikate neu ausgestellt und die Konfigurationen neu per Push übertragen.
  Wenn Sie die Option eingerichtet haben, eine Konfiguration ohne ausgestelltes Testzertifikat für **Dynamisch generierte** Zertifikatsverteilung zu erstellen, klicken Sie auf **Weiter**.
- Zertifikate werden implizit neu ausgestellt.
- Wenn Android-Apps Identitätszertifikate zugeordnet sind, holt sich die App des Benutzers die Identitätszertifikate, ohne dass der Benutzer die Berechtigung zur Verwendung des Zertifikats erteilen muss (übernimmt die App). Dazu gehören alle Apps wie Email+, Gmail usw.
- Email+ kann mit einem vom Benutzer zur Verfügung gestellten Identitätszertifikat konfiguriert und als App-Konfiguration auf Android-Unternehmensgeräte per Push übertragen und zugewiesen werden. Sie gilt nur für die Modi „Arbeitsprofil auf unternehmenseigenem Gerät“ und „Geräteeigentümer“.

Identitätszertifikat – Einstellungen

Einstellung	Aktion
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Verteilung von Zertifikaten	Wählen Sie die Art der einzurichtenden Verteilung von Zertifikaten. • **Einzelne Datei**: Laden Sie ein bestehendes Zertifikat zur Verteilung auf Geräte hoch. • **Dynamisch generiert**: Erstellen Sie Zertifikate auf Anfrage mit einer lokalen oder externen Zertifikatsautorität. • **Vom Benutzer**: Erstellen Sie Labels für die Art der Zertifikate, die der Benutzer hochladen soll. Nach der Erstellung kann der Benutzer die erstellten Labels (Optionen) im Selbstbedienungsportal sehen und für diese Label entsprechende Zertifikate hochladen. • **Abgeleitete Anmeldeinformationen:** Geben Sie eine der folgenden Verwendungen für die abgeleiteten Anmeldeinformationen an: ◦ Authentifizierung ◦ Verschlüsselung ◦ Signieren ◦ Entschlüsseln • **SCEP-Konfig.**: Legt fest, wie ein Zertifikat vom SCEP-Server angefordert werden soll. Klicken Sie auf eine der folgenden Konfigurationen: ◦ Apple-Konfiguration ◦ Windows-Konfiguration Ihre Auswahl bestimmt, welche weiteren Optionen im Formular angezeigt werden.
Allen Apps den Zugriff auf den privaten Schlüssel gestatten (macOS 10.10+)	**Gilt für:** Einzeldatei, dynamisch erzeugte, vom Benutzer bereitgestellte und SCEP Apple Config-Identitätszertifikate. (Optional) Aktivieren Sie für PKCS#12-Zertifikate die Option Allen Anwendungen Zugriff auf den privaten Schlüssel gestatten, um allen Anwendungen den Zugriff auf den privaten Schlüssel zu erlauben. Dieser Schlüssel kann beispielsweise verwendet werden, wenn vom Benutzer ein Passwort angefordert wird, um den Zugriff auf ein für VPN verwendetes Zertifikat zu ermöglichen.
Einzelne Datei	
Daten des Identitätszertifikats	Ziehen Sie die Zertifikatsdatei in das gepunktete Feld oder klicken Sie auf **Datei auswählen**, um sie aus Ihrem Dateisystem auszuwählen.
Passwort	Geben Sie das Passwort zum Schutz der PKCS#12-Zertifikatsdatei ein. Dieses Passwort wird für die Installation ohne Aufforderung verwendet.
Dynamisch erzeugt	
Quelle	Wählen Sie die lokale Zertifizierungsstelle aus der Dropdown-Liste aus. Sie sollten diese Zertifizierungsstelle bereits unter **Admin >** Zertifizierungsverwaltung erstellt haben.

Einstellung	Aktion
Konfiguration ohne Ausstellung eines Testzertifikats erstellen.	Aktivieren Sie das Kontrollkästchen, um eine Konfiguration zu erstellen, ohne ein Prüfzertifikat auszustellen.
Nur Windows - Zielzertifikatspeicher	Admins können jetzt den Zielzertifikatspeicher auf Windows-Geräten auswählen.
Vom Benutzer bereitgestellt Zertifikat-Anzeigename Privaten Schlüssel löschen	 Geben Sie den Namen des Zertifikats ein. Dieser Zertifikatname ist für den Mandanten eindeutig; der Benutzer kann den Namen im Selbstbedienungsportal sehen, wenn er das Zertifikat hochlädt. Wählen Sie diese Option, um den privaten Schlüssel des Zertifikats nach *n* (1-30) Tagen zu löschen. Sie können die für diese Operationen auch die durch die Cloud bereitgestellten APIs verwenden. Weitere Informationen über die Ivanti Neurons for MDM*API* finden Sie in dem API-Leitfaden. Wenn Sie versuchen, dieses Zertifikat in einer Konfiguration zu verwenden (z. B. zur Authentifizierung einer App oder zur Push-Übertragung einer WLAN- oder VPN-Konfiguration), nachdem der private Schlüssel gelöscht wurde, schlägt die Aufgabe fehl. Sie müssen diese Aufgabe ausführen, bevor Sie den privaten Schlüssel löschen.
Tage bis zum Löschen des privaten Schlüssels **Abgeleitete Anmeldeinformationen**	Wählen Sie die Frist in Tagen (1-30), nach deren Ablauf die privaten Schlüssel des Zertifikats gelöscht werden. Der Standardwert ist 2 Tage.
Verwendung abgeleiteter Zugangsdaten	Wählen Sie eine der folgenden Optionen aus: • **Authentifizierung** - Gibt an, dass die abgeleiteten Anmeldeinformationen zur Authentifizierung verwendet werden. • **Verschlüsselung** - Gibt an, dass die abgeleiteten Anmeldeinformationen zur Verschlüsselung verwendet werden. • **Signieren** - Gibt an, dass die abgeleiteten Anmeldeinformationen zum Signieren verwendet werden. • **Entschlüsselung** - Gibt an, dass die abgeleiteten Anmeldeinformationen zur Entschlüsselung verwendet werden.
Marke	Wählen Sie aus den folgenden Optionen den von Ihnen verwendeten Anbieter abgeleiteter Anmeldeinformationen aus: • **Entrust** • **Intercede** • **Purebred** Weitere Informationen zur Ergänzung der benutzerdefinierten Anbieter abgeleiteter

Einstellung	Aktion
	Anmeldeinformationen, die Sie verwenden, finden Sie unter **Anbieter abgeleiteter Anmeldeinformationen**.
ACME-Konfiguration – gilt nur für iOS/iPadOS16+/macOS14+.	
Client-ID	Eine eindeutige Zeichenfolge zur Identifizierung eines bestimmten Geräts.
Verzeichnis-URL	(Erforderlich) Die Verzeichnis-URL des ACME-Servers. Die URL muss das https-Schema verwenden.
Erweiterte Schlüsselnutzung	Der Wert wird als Bereich von Zeichenfolgen angegeben. Jede Zeichenfolge ist eine OID in punktierter Standardschreibweise. Beispiel: [”1.3.6.1.5.5.7.3.2”, “1.3.6.1.5.5.7.3.4”] steht für Client-Authentifizierung und E-Mail-Schutz. Das Gerät fordert dieses Feld für das vom ACME-Server ausgestellte Zertifikat an. Der ACME-Server kann dieses Feld bei dem von ihm ausgestellten Zertifikat übersteuern oder ignorieren.
Schlüssellänge	(Erforderlich) Die gültigen Werte für die Schlüssellänge richten sich nach den Werten für "Schlüsseltyp" und "Hardwaregebunden". Spezifische Anforderungen sind den betreffenden Schlüsseln zu entnehmen.
Schlüsseltyp	(Erforderlich) Der Typ des zu generierenden Schlüsselpaares.
Betreff	(Erforderlich) Geben Sie einen X.500-Namen als kommagetrenntes Array von OIDs und Werten ein. Normalerweise steht im Betreff der vollqualifizierte Domänenname (FQDN) des Benutzers. Zum Beispiel C=US,DC=com,DC=MobileIron,OU=InfoTech oder CN=www.mobileiron.com. Sie können den Betreff auch anpassen und der Objektkennung eine Variable hinzufügen. Zum Beispiel: CN=www.mobileiron.com-${{deviceGUID}}. Zur Erleichterung der Konfiguration können Sie auch die Variable $ verwenden, um den Betreff mit dem FQDN des Benutzers auszufüllen. Verwenden Sie nicht den umgekehrten Schrägstrich (\) im Betreff.
Alternativer Name für Betreff	Das Gerät fordert den alternativen Namen für den Betreff für das vom ACME-Server ausgestellte Zertifikat an. Der ACME-Server kann dieses Feld bei dem von ihm ausgestellten Zertifikat übersteuern oder ignorieren.
Schlüsselnutzung	Dieses Feld ist ein Bit-Wert. Bit 0x01 steht für digitale Signatur. Bit 0x10 steht für Schlüsselvereinbarung. Das Gerät fordert diesen Schlüssel für das vom ACME-Server ausgestellte Zertifikat an. Der ACME-Server kann dieses Feld bei dem von ihm ausgestellten Zertifikat übersteuern oder ignorieren.
Hardwaregebunden	Wenn "Hardwaregebunden" auf "wahr" gesetzt ist, ist der private Schlüssel an das Gerät gebunden. Nur dann muss der Schlüsseltyp ECSECPrimeRandom lauten und die Schlüssellänge muss 256 oder 384 sein.
Bescheinigung	Falls auf "wahr" gesetzt, stellt das Gerät Bescheinigungen für den ACME-Server bereit, die das Gerät und den generierten Schlüssel beschreiben. Wenn "Bescheinigung" auf "wahr" gesetzt ist, muss auch

Einstellung	Aktion
	"Hardwaregebunden" auf "wahr" gesetzt sein.
SCEP-Konfiguration – Apple-Konfiguration	
Identitätszertifikat (SCEP)	Wählen Sie diese Option, um einen SCEP-Server anzugeben.
Lokale Zertifikatsautorität	Wählen Sie diese Option, um eine lokale Zertifizierungsstelle zu bestimmen, die Sie bereits unter **Administration >** Zertifikatsverwaltung erstellt haben. Wählen Sie die lokale Zertifikatsautorität aus dem Dropdown-Menü aus, das angezeigt wird, wenn Sie diese Option wählen.
[URL]	Geben Sie die URL für den SCEP-Server ein.
CA-ID	Geben Sie die von der Zertifikatsautorität gelieferte Kennung ein.
Betreff	Geben Sie einen X.500-Namen als durch Kommas getrenntes Array von OIDs und Werten ein. Normalerweise steht im Betreff der vollqualifizierte Domänenname (FQDN) des Benutzers. Zum Beispiel C=US,DC=com,DC=MobileIron,OU=InfoTech oder CN=www.mobileiron.com. Sie können den Betreff auch anpassen und der Objektkennung eine Variable hinzufügen. Zum Beispiel CN=www.mobileiron.com-$DEVICE_CLIENT_ID$. Zur Erleichterung der Konfiguration können Sie auch die Variable $USER_DN$ verwenden, um den Betreff mit dem FQDN des Benutzers auszufüllen. Verwenden Sie nicht den umgekehrten Schrägstrich (\) im Namen für den Betreff.
Typ des alternativen Namens für Betreff	Wählen Sie RFC 822 Name, DNS Name, Uniform Resource Identifier oder nichts aus; basierend auf den Attributen der Zertifikatsvorlage.
Wert des alternativen Namens für Betreff	Geben Sie den Wert für den entsprechenden Typ ein. Wenn Sie als erstes Zeichen '$' eingeben, wird eine Dropdownliste mit möglichen benutzerdefinierten LDAP- und Entra ID-Attributen angezeigt. Wählen Sie ein geeignetes, anpassbares Attribut aus der Liste. Wenn der Entra ID-Wert verwendet wird, wird nur 'onPremisesImmutableId' unterstützt. Geben Sie fn:base64tohex($) ein.
NT-Principal-Name	Geben Sie einen alternativen Betreff-Namen für die Microsoft-Umgebung ein. Normalerweise müsste die Konfiguration den UPN (User Principal Name) des Benutzers einschließen.
Herausforderung	(Optional) Wird als vorab geteiltes Gruppenpasswort für die automatische Registrierung verwendet.
Wiederholungen	Wählen Sie eine Zahl aus der Liste aus, um zu bestimmen, wie oft der Versuch der Authentifizierung wiederholt wird, nachdem zum ersten Mal der Status „Ausstehend“ angegeben wird.
Wartezeit für Wiederholung	Wählen Sie eine Zahl aus der Liste aus, um zu bestimmen, wie viele Sekunden vor einer Wiederholung gewartet werden soll.
Schlüssellänge	Wählen Sie 1024, 2048 oder 4096 Bits.
Als digitale Signatur verwenden	Wählen Sie aus, ob das Zertifikat zum Signieren verwendet werden darf.

Einstellung	Aktion
Als Verschlüsselung für den Schlüssel verwenden	Wählen Sie, ob das Zertifikat zur Verschlüsselung verwendet werden darf.
CA-Fingerabdruck	Wenn Ihre Zertifizierungsstelle HTTP verwendet, geben Sie den Hex-String ein, der als Fingerabdruck des Zertifikats der Zertifizierungsstelle verwendet werden soll. MD5-Fingerabdrücke werden unterstützt. Sie können auch einen Fingerabdruck des Zertifikats erstellen. Legen Sie das Zertifikat einfach mit Drag and Drop im entsprechenden Bereich ab, oder klicken Sie auf **Von Zertifikat erstellen**, um das Zertifikat aus Ihrem Dateisystem auszuwählen.
SCEP-Konfiguration - Windows-Konfiguration	
CA (Zertifizierungsstelle)	Wählen Sie die Option, um eine Zertifizierungsstelle zu bestimmen, die Sie bereits unter **Administration > Zertifikatsverwaltung erstellt haben**. Wählen Sie die Zertifizierungsstelle aus der Dropdown-Liste aus, die bei Auswahl dieser Option angezeigt wird.
Betreff	Geben Sie einen X.500-Namen als durch Kommas getrenntes Array von OIDs und Werten ein. Normalerweise steht im Betreff der vollqualifizierte Domänenname (FQDN) des Benutzers. Zum Beispiel C=US,DC=com,DC=MobileIron,OU=InfoTech oder CN=www.mobileiron.com. Sie können den Betreff auch anpassen und der Objektkennung eine Variable hinzufügen. Zum Beispiel CN=www.mobileiron.com-$DEVICE_CLIENT_ID$. Zur Erleichterung der Konfiguration können Sie auch die Variable $USER_DN$ verwenden, um den Betreff mit dem FQDN des Benutzers auszufüllen. Verwenden Sie nicht den umgekehrten Schrägstrich (\) im Namen für den Betreff.
Typ des alternativen Namens für Betreff	Klicken Sie auf **+ Hinzufügen**, um den RFC 822-Namen, DNS-Namen, den Uniform Resource Identifier oder „Keine“ anhand der Attribute der Zertifikatsvorlage auszuwählen.
Wiederholungen	Wählen Sie eine Zahl aus der Liste aus, um zu bestimmen, wie oft der Versuch der Authentifizierung wiederholt wird, nachdem zum ersten Mal der Status „Ausstehend“ angegeben wird.
Wartezeit für Wiederholung	Wählen Sie eine Zahl aus der Liste aus, um zu bestimmen, wie viele Sekunden vor einer Wiederholung gewartet werden soll.
Schlüssellänge	Wählen Sie als Schlüsselgröße 1024, 2048 oder 4096 Bit.
Verwendung auswählen	Wählen Sie mindestens eine Option aus: • Als digitale Signatur verwenden - Wählen Sie, ob das Zertifikat zum Signieren verwendet werden darf. • Als Verschlüsselungsschlüssel verwenden - Wählen Sie, ob das Zertifikat zur Verschlüsselung verwendet werden darf.
Gültigkeit	Wählen Sie die Gültigkeit in Tagen, Monaten oder Jahren.

Einstellung	Aktion
CA Thumbprint	Wenn Ihre Zertifizierungsstelle HTTP verwendet, geben Sie den Hex-String ein, der als Fingerabdruck des Zertifikats der Zertifizierungsstelle verwendet werden soll. MD5-Fingerabdrücke werden unterstützt. Sie können auch einen Fingerabdruck des Zertifikats erstellen. Legen Sie das Zertifikat einfach mit Drag and Drop im entsprechenden Bereich ab, oder klicken Sie auf **Von Zertifikat erstellen**, um das Zertifikat aus Ihrem Dateisystem auszuwählen.
Hash-Algorithmus-Familie	Wählen Sie SHA-2- oder SHA-3-Algorithmen.

> Wenn ein Identitätszertifikat für ein Arbeitsprofil auf einem Gerät verwendet wird, ohne dass ein Work-Challenge-Passcode eingestellt ist, verlangt das Gerät statt eines Work-Challenge-Passcodes einen Geräte-Passcode.

Weitere Informationen finden Sie unter **Arbeiten mit Konfigurationen**.

10.10.4.23. Konfiguration der iOS-Aktivierungssperre

Lizenz: Silver

Dieser Abschnitt enthält die folgenden Themen:

- iOS-Aktivierungssperre aktivieren
- iOS-Aktivierungssperre auf überwachten Geräten aktivieren
- macOS-Aktivierungssperre aktivieren
- macOS-Aktivierungssperre auf überwachten Geräten aktivieren
- Bypass-Code für die iOS-Aktivierungssperre verwenden
- Bypass-Code für die iOS-Aktivierungssperre löschen

Die Aktivierungssperre ist eine Apple-Funktion, die verhindern soll, dass jemand ein verloren gegangenes oder gestohlenes Gerät verwendet. Nach der Aktivierung von Find My wird eine Zuordnung zwischen dem iCloud-Konto und einer Hardware-Kennung für dieses Gerät auf den Aktivierungsservern von Apple gespeichert. Von diesem Moment an kann niemand mehr die Funktion „Find My“ abschalten, das Gerät löschen oder neu aktivieren, wenn er die vorhandene Apple-ID und das Passwort nicht kennt. Wenn jemand anders als der Benutzer das Gerät löscht und dann versucht, es neu zu aktivieren und zu verwenden, werden die Apple-ID und das Passwort im Setup Assistant abgefragt.

Die Deaktivierung der Aktivierungssperre deaktiviert diese Funktion bei überwachten Geräten nicht, wenn der Endbenutzer die Funktion „Find My Device“ aktiviert hat. Der Setup-Assistent fordert den Benutzer auf, entsprechend zu reagieren, wenn das Gerät zurückgesetzt oder aus der Ferne komplett gelöscht wird.

Die Aktivierungssperre gibt den Administratoren weitere Möglichkeiten, den Diebstahl von überwachten Geräten zu erschweren. Die meisten Administratoren in Unternehmen lassen die Aktivierungssperre jedoch deaktiviert, weil es vor allem eine Funktion für Verbraucher ist. Die folgende Tabelle fasst die Funktionen für Unternehmensbereitstellungen zusammen:

Gerätetyp	Ergebnis
Überwachung und Haftung durch das Unternehmen	• Die Aktivierungssperre ist standardmäßig für überwachte Geräte deaktiviert. • Die Gerätebenutzer können die Aktivierungssperre nicht einschalten.
Nicht überwachte Geräte mit Haftung durch das Unternehmen	• Die Aktivierungssperre wird eingeschaltet, sobald der Endbenutzer sich in iCloud mit seiner Apple-ID anmeldet und die Funktion "Find My Device" einschaltet. • MDM-Server, beispielsweise Cloud, können die Aktivierung der Sperre auf nicht überwachten Geräten nicht kontrollieren. Gerätebenutzer können die Aktivierung mit ihren persönlichen Anmeldeinformationen sperren, sodass Sie als Administrator keinen Zugriff mehr haben, wenn diese Benutzer aus dem Unternehmen ausscheiden sollten.

iOS-Aktivierungssperre aktivieren

Gilt für: überwachte Geräte mit iOS 7+

Diese Konfiguration gilt für überwachte Geräte (iOS7 und höher), bei denen die Funktion Find My aktiviert ist. Wenn ein Administrator oder ein anderer Benutzer versucht, auf dem Gerät die Funktion zum Suchen des Geräts zu deaktivieren oder das Gerät komplett zu

löschen oder zu aktivieren, wird ein Apple-Aktivierungssperrbildschirm angezeigt. Um fortzufahren, muss der Benutzer die iTunes-Anmeldeinformationen oder einen Bypass-Code eingeben.

Der Bypass-Code für überwachte Geräte wird nach der Aktivierung gespeichert und kann in den Gerätedetails eingesehen werden. Der Bypass-Code kann für überwachte Geräte aus der Ferne mit dem Befehl „Aktivierungssperre löschen“ versendet werden. Der Code muss bei Neuaktivierung des Geräts bzw. bei Deaktivierung der Funktion zum Suchen des Geräts jedoch manuell eingegeben werden.

> Sie können nur eine Aktivierungssperrkonfiguration für alle Spaces erstellen.

iOS-Aktivierungssperre auf überwachten Geräten aktivieren

Verfahren

1. Aktivieren Sie die Funktion **Find My** auf Ihrem Gerät.
2. Gehen Sie zu **Konfigurationen**.
3. Wählen Sie die Konfiguration **iOS-Aktivierungssperre** aus der Liste der vorhandenen Konfigurationen.
4. Klicken Sie auf **Bearbeiten**.
5. Klicken Sie im Bereich iOS 7+ Supervised auf **Aktivierungssperre aktivieren**.
6. Klicken Sie auf **Fertig**.
7. Registrieren Sie das Gerät.

macOS-Aktivierungssperre aktivieren

Gilt für: überwachte Geräte mit iOS 10.15+

Diese Konfiguration wird für die überwachten Geräte mit macOS 10.15 und höher verwendet. Die Aktivierungssperre für macOS gilt nur für Macs mit einem Apple T2 Security Chip. Bei überwachten Geräten und bei aktualisierten, aktuell registrierten Geräten ist die Aktivierungssperre unabhängig davon, ob sie aktualisiert oder neu installiert wurden, standardmäßig deaktiviert. Wenn Sie „Find My“ aktivieren, wird die Aktivierungssperre auf diesen Geräten nicht automatisch aktiviert.

Wenn ein Administrator oder ein anderer Benutzer versucht, auf dem Gerät die Funktion Find My zu deaktivieren, zu aktivieren oder das Gerät komplett zu löschen, wird ein Apple-Aktivierungssperrbildschirm angezeigt. Um fortzufahren, muss der Benutzer die iTunes-Anmeldeinformationen oder einen Bypass-Code eingeben. Der Bypass-Code für überwachte Geräte wird nach der Aktivierung gespeichert und kann in den Gerätedetails eingesehen werden. Der Bypass-Code kann für überwachte Geräte aus der Ferne mit dem Befehl „Aktivierungssperre löschen“ versendet werden. Der Code muss bei Neuaktivierung des Geräts bzw. bei Deaktivierung der Funktion Find My jedoch manuell eingegeben werden.

> Sie können nur eine Aktivierungssperrkonfiguration für alle Spaces erstellen.

macOS-Aktivierungssperre auf überwachten Geräten aktivieren

Verfahren

1. Aktivieren Sie die Funktion „Find My“ auf Ihrem
2. Gehen Sie zu **Konfigurationen**.
3. Wählen Sie die Konfiguration **iOS-Aktivierungssperre** aus der Liste der vorhandenen Konfigurationen.

4. Klicken Sie auf **Bearbeiten**.
5. Klicken Sie im Bereich „macOS 10.15+ Supervised“ auf **Aktivierungssperre aktivieren**.
6. Klicken Sie auf **Fertig**.
7. Registrieren Sie das Gerät.

Bypass-Code für die iOS-Aktivierungssperre verwenden

Wenn das Gerät komplett gelöscht wird und die iOS-Aktivierungssperre aktiviert ist, bleibt der Bypass-Code auf dem Apple Aktivierungsserver sowie auf der Administrationsoberfläche der Cloud erhalten.

Verfahren

1. Gehen Sie zu **Geräte**.
2. Wählen Sie das entsprechende Gerät aus.
3. Klicken Sie auf **Aktionen > Wipe durchführen**. Es kannn einige Minuten dauern, bis das Gerät neu startet.
4. Wenn das Gerät Sie nach der Apple-ID und dem Passwort fragt, lassen Sie das Feld für die **Apple-ID** leer.
5. Geben Sie den Bypasscode in dem Feld **Passwort** ein.
6. Klicken Sie auf **Weiter**.
7. Fahren Sie mit der Einrichtung fort.

Bypass-Code für die iOS-Aktivierungssperre löschen

Wenn die iOS-Aktivierungssperre in der Administrationsoberfläche der Cloud gelöscht wird, wird der Bypasscode vom Apple Aktivierungsserver entfernt, ist aber noch in den Gerätedetails der Administrationsoberfläche der Cloud vorhanden.

Verfahren

1. Gehen Sie zu Geräte.
2. Wählen Sie das entsprechende Gerät aus.
3. Klicken Sie auf **Konfigurationen**.
4. Wählen Sie **Apple Aktivierungssperre**.
5. Klicken Sie auf **Bearbeiten**.
6. Deaktivieren Sie in der Sektion „iOS 7+ überwacht“ die Option **Aktivierungssperre aktivieren**.
7. Klicken Sie auf **Fertig**.
8. Gehen Sie zu Geräte.
9. Wählen Sie das entsprechende Gerät aus.
10. Klicken Sie auf **Aktionen > Wipe durchführen**. Es kannn einige Minuten dauern, bis das Gerät neu startet. Sie können das Gerät jetzt mit der AppleID und dem Passwort des neuen Benutzers konfigurieren.
11. Fahren Sie mit der Einrichtung fort.

Der Status der gelöschten iOS-Aktivierungssperre wird auf der Schnittstelle wie folgt angezeigt:

Bundesland	Ergebnis
Ausstehend	• Der Server sendet den Code zum Löschen der Aktivierungssperre an Apple.
Gesendet	• Apple bestätigt den Erhalt des Codes zum Löschen der Aktivierungssperre.
Fehlgeschlagen	• Der Server konnte den Code nicht an Apple senden. • Apple hat einen Fehler gemeldet.

10.10.4.24. Individuelle iOS-Konfiguration

Eine iOS Custom Configuration ermöglicht Ihnen das Hochladen und Verteilen eines iOS-Konfigurationsprofils, das von einer anderen App, wie z. B. der iPhone Configuration Utility von Apple, erstellt wurde.

Benutzerdefinierte iOS-Einstellungen

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Dateidaten	Ziehen und legen Sie die Konfigurationsdatei ab oder klicken Sie auf **Datei auswählen**, um sie aus Ihrem Dateisystem auszuwählen.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.4.25. Intelligence-Einstellungen

Verwenden Sie die externen Intelligence-Einstellungen, um Apple Intelligence-Einstellungen auf überwachten Geräten zu konfigurieren. Diese Deklaration hilft Administratoren, konsistente, richtlinienbasierte Kontrollen anzuwenden, die steuern, wie Geräte auf Apple Intelligence-Funktionen zugreifen und diese verwenden.

Gilt für:

- iOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- macOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- visionOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Intelligence-Einstellungen** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie die **Intelligence-Einstellungen** gemäß der folgenden Tabelle:

Einstellung	Aktion
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Apple Intelligence-Bericht zulassen	Aktivieren Sie das Kontrollkästchen, um den Apple Intelligence-Bericht zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um Apple Intelligence-Berichte auf überwachten Geräten zu aktivieren.
Genmoji zulassen	Aktivieren Sie das Kontrollkästchen, um Genmoji zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um Genmoji auf überwachten Geräten zu aktivieren.
Image Playground zulassen	Aktivieren Sie das Kontrollkästchen, um Image Playground zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um Image Playground auf überwachten Geräten zu aktivieren.
Image Wand zulassen	Aktivieren Sie das Kontrollkästchen, um Image Wand zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um Image Wand auf überwachten Geräten zu aktivieren. Diese Einstellung gilt nicht für macOS-Geräte.
Personalized Handwriting Results Wand zulassen	Aktivieren Sie das Kontrollkästchen, um Personalized Handwriting Results Wand zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um Personalized Handwriting Results Wand auf überwachten Geräten zu aktivieren. Diese Einstellung gilt nicht für macOS- und visionOS-Geräte.
Zusammenfassung von Visual Intelligence zulassen	Aktivieren Sie das Kontrollkästchen, um die Visual Intelligence-Zusammenfassung zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um Visual Intelligence-Zusammenfassungen auf überwachten Geräten zu aktivieren. Diese Einstellung gilt nicht für macOS- und visionOS-Geräte.
Schreibtools zulassen	Aktivieren Sie das Kontrollkästchen, um Schreibwerkzeuge zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um Schreibwerkzeuge auf überwachten Geräten zu aktivieren.
"Diktat nur auf Gerät" erzwingen	Aktivieren Sie das Kontrollkästchen, um Nur-Gerät-Diktate zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um "Diktat nur auf Gerät" auf überwachten Geräten zu aktivieren.
"Übersetzung nur auf Gerät" erzwingen	Aktivieren Sie das Kontrollkästchen, um "Übersetzung nur auf Gerät" zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um "Übersetzung nur auf Gerät" auf überwachten Geräten zu aktivieren. Diese Einstellung gilt nicht für macOS- und visionOS-Geräte.
Apps	
Kalender	

Einstellung	Aktion
Bearbeiten natürlicher Sprache zulassen	Aktivieren Sie das Kontrollkästchen, um die Bearbeitung natürlicher Sprache im Kalender und in Erinnerungen zu aktivieren. Schalten Sie die Schaltfläche **Via Push an das Gerät senden** um, um die Bearbeitung in natürlicher Sprache im Kalender und in Erinnerungen auf überwachten Geräten zu aktivieren.
E-Mail	
Smart Replies zulassen	Aktivieren Sie das Kontrollkästchen, um Smart Replies zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um Smart Replies auf überwachten Geräten zu aktivieren.
Zusammenfassung zulassen	Aktivieren Sie das Kontrollkästchen, um die Zusammenfassung zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um Zusammenfassungen auf überwachten Geräten zu aktivieren.
Hinweise	
Transkription zulassen	Aktivieren Sie das Kontrollkästchen, um die Transkription zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um die Transkription auf überwachten Geräten zu aktivieren. Diese Einstellung gilt nicht für visionOS-Geräte.
Transcription Summary ulassen	Aktivieren Sie das Kontrollkästchen, um die Transkriptionszusammenfassung zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um die Transkriptionszusammenfassung auf überwachten Geräten zu aktivieren. Diese Einstellung gilt nicht für visionOS-Geräte.
Safari	
Zusammenfassung zulassen	Aktivieren Sie das Kontrollkästchen, um die Zusammenfassung zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um Zusammenfassungen auf überwachten Geräten zu aktivieren.

4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
5. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Intelligence-Einstellungen** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
6. Klicken Sie auf **Fertig**.

10.10.4.26. iOS-Einschränkungen

iOS-Einschränkungen sind Einstellungen, über die der primäre Benutzer des Geräts steuern kann, welche Aktionen andere Benutzer auf iOS-, watchOS- und visionOS-Geräten durchführen können. Diese Einstellungen werden von Apple definiert und über die Cloud verwaltet.

Bei der Verteilung dieser Konfiguration an **Gemeinsam genutzte iPads** können Sie entweder den Gerätekanal oder den Benutzerkanal wählen. Dies ist nützlich, um separate Konfigurationen zu verteilen und Einschränkungen durchzusetzen, die nur für das Gerät oder den Benutzerkanal gelten.

Globale Administratoren können Space-Administratoren zur Bearbeitung der Konfiguration für **Alle Geräte und für die benutzerdefinierten Verteilung** delegieren. Für die Konfiguration der iOS-Einschränkung können Sie optional **Diese Konfiguration in allen Spaces zur Verfügung stellen** auswählen.

> Die Änderungen an der Verteilung gelten nur für den jeweiligen Space. Alle anderen Spaces übernehmen weiterhin die Verteilungseinstellungen des Standard-Space.

iOS-Einschränkungseinstellungen

Kategorie	Einstellung	Aktion
	[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
	Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Gerätefunktionen	**iOS Alle Versionen**	**Verwendung von Gerätefunktionen aktivieren.**
	Bildschirmfotos und Bildschirmaufzeichnungen zulassen.	Wählen Sie die Option, um dem Gerätebenutzer das Erstellen von Screenshots mit der integrierten iOS-Screenshot-Funktion zu gestatten.
	Fernüberwachung zulassen (iOS 9.3 und höher)	Wählen Sie diese Option aus, damit Benutzer den entfernten Bildschirm sehen können.
	Beobachtung des Bildschirms in Classroom ohne Rückfrage erzwingen (nur überwacht - iOS 10.3+)	(Nur für iPads) Wählen Sie diese Option aus, damit Mitteilungen ohne Aufforderung auf dem Display angezeigt werden können, wenn ein überwachter iPad mit verwalteten Klassen konfiguriert wird.
	Automatische Synchronisierung beim Roaming zulassen	Wählen Sie diese Option, um die Synchronisierung von E-Mail-Konten zu gestatten, während sich das Gerät außerhalb seines Heimatlandes befindet.
	Siri zulassen	Wählen Sie diese Option, um die Personal Assistant-App auf unterstützten Geräten zuzulassen.
	Siri während Sperrung des Gerätes zulassen	Wählen Sie diese Option, um zuzulassen, dass die Personal Assistant-App auch während der Sperrung des Geräts Aufgaben erledigt.
	Siri-Profanitätsfilter aktivieren (nur überwachte Geräte)	Wählen Sie die Option aus, um den Siri-Profanitätsfilter zu aktivieren.
	Sprachwahl zulassen	Wählen Sie die Option, um Benutzern zu gestatten, einen Kontakt bzw. eine Nummer durch Sprachwahl anzuwählen.
	In-App-Käufe zulassen	Wählen Sie diese Option, um Benutzern zu gestatten, über auf dem Gerät installierte Apps Käufe zu tätigen.

Kategorie	Einstellung	Aktion
	Passbook während Sperrung des Gerätes zulassen	Wählen Sie die Option, um Passbook-Nachrichten während der Sperrung des Geräts zuzulassen.
	Lock Screen Control Center zulassen	Wählen Sie die Option, um den Zugriff auf das Control Center über den Sperrbildschirm zuzulassen.
	Anzeige von Lock Screen-Benachrichtigungen zulassen	Wählen Sie die Option, um zuzulassen, dass Nachrichten auf dem Sperrbildschirm angezeigt werden.
	Lock Screen Today-Anzeige zulassen	Wählen Sie die Option, um den Zugriff auf die Today-Anzeige über den Sperrbildschirm zuzulassen.
	Open-In von verwalteten in unverwalteten Apps zulassen	**Hierzu ist eine Gold-Lizenz erforderlich**. Wählen Sie diese Option aus, um zu gestatten, dass verwaltete Apps und Konten in nicht verwalteten Apps und Konten geöffnet werden. Durch Deaktivieren dieser Option wird der Austausch von Dokumenten zwischen verwalteten und unverwalteten Apps bzw. Konten verhindert. Beispiel: sollten Sie verhindern, dass Unternehmensdokumente mit privaten Apps geöffnet werden. Sie können diese Option (Deaktivieren) auch gemeinsam mit einer verwalteten Domain-Konfiguration verwenden, damit aus verwalteten Domains heruntergeladene Daten nur in einer verwalteten App geöffnet werden können.
	Open-In von unverwalteten in verwalteten Apps zulassen	**Hierzu ist eine Gold-Lizenz erforderlich**. Wählen Sie diese Option aus, um zu gestatten, dass verwaltete Apps und Konten in nicht verwalteten Apps und Konten geöffnet werden. Durch Deaktivieren dieser Option wird der Austausch von Dokumenten zwischen nicht verwalteten und verwalteten Apps bzw. Konten verhindert. Beispielsweise sollten Sie verhindern, dass Benutzer persönliche Dokumente über Firmen-E-Mail-Adressen versenden. Sie können die Option (Deaktivieren) gemeinsam mit einer verwalteten Domain-Konfiguration verwenden, damit aus nicht verwalteten Domains heruntergeladene Daten nicht in einer verwalteten App geöffnet werden können.
	Passcode für erste AirPlay-Kopplung erforderlich	Wählen Sie diese Option aus, damit Apple TV eine Passwortabfrage anzeigt und der Benutzer auf dem iOS-Gerät ein Passwort für die erste Kopplung der Geräte eingeben muss.
	Bei eingehenden AirPlay-Anfragen Passwort erzwingen (tvOS bis 10.1) **iOS 26+**	Wählen Sie die Option aus, um vom Benutzer die Eingabe eines Passworts für alle eingehenden AirPlay-Anfragen zu verlangen. Standard: nicht ausgewählt
	Apps, die von Bewertungseinschränk	Geben Sie die Liste der Apps ein, die nur dann von altersbasierten Bewertungseinschränkungen ausgenommen werden sollen, wenn ihre Bundle-IDs in der

Kategorie	Einstellung	Aktion
	ungen ausgenommen sind (gilt für iOS 26.1+)	Schnittmenge aller Ausnahmelisten mehrerer Payloads und übergeordneter Steuerungs-Apps wie ScreenTime enthalten sind. Standard: Ausgewählt
	iOS Alle überwachten Versionen	
	Apple Books zulassen	Wählen Sie dies Option aus, um Zugang zu der App Apple Books zuzulassen.
	Sexuellen Content im iBooks Store ausdrücklich zulassen (iOS und tvOS 11.3 und höher)	Wählen Sie diese Option, um Benutzern das Herunterladen von iBooks Store-Inhalten zu gestatten, die als Erotica gekennzeichnet sind.
	Kontenänderung zulassen	Wählen Sie diese Option, um Benutzern mit überwachten iOS 7-Geräten zu gestatten, E-Mail-Konten hinzuzufügen und Änderungen an bereits konfigurierten E-Mail-Konten vorzunehmen.
	App-Gerätedatenänderung zulassen	Wählen Sie die Option, um Benutzern zu gestatten, Änderungen an Mobilgerätedaten für Apps vorzunehmen.
	Find My Friends-Änderung zulassen	Wählen Sie die Option, um Benutzern zu gestatten, Änderungen an den Einstellungen der Find My Friends-App vorzunehmen.
	Koppeln mit Nicht-Configurator-Hosts zulassen	Wählen Sie die Option, um die Host-Kopplung für die Synchronisation mit iTunes zuzulassen. Die Aktivierung dieser Option ermöglicht überwachten Geräten die Synchronisierung mit iTunes auf einem anderen Mac als dem Überwachungscomputer. Durch Deaktivieren dieser Option wird die Host-Kopplung bis auf den Überwachungscomputer deaktiviert. Wenn für den Überwachungscomputer kein Zertifikat konfiguriert wurde, wird die Kopplung vollständig deaktiviert.
	AirDrop zulassen	Wählen Sie die Option, um die Nutzung von AirDrop auf dem Gerät zuzulassen. AirDrop ist das Ad-hoc-WLAN-System von Apple, das den Datenaustausch mit Benutzern in der näheren Umgebung ermöglicht. Durch Einschränken dieser Funktion stellen Sie sicher, dass sensible Dokumente nicht auf nicht autorisierte oder unsichere Geräte gelangen.
	Touch-ID / Face-ID zum Entsperren des Geräts zulassen	Wählen Sie diese Option aus, um Geräte mit Touch-ID oder Face-ID zu entsperren.
	Spotlightsuche nach Internet-Suchergebnissen erlauben.	Wählen Sie diese Option, um die Spotlightsuche nach Internet-Suchergebnissen zuzulassen.

Kategorie	Einstellung	Aktion
	App in Single-App-Modus zulassen	Geben Sie mit Komma als Trennzeichen eine Liste von Bundle-IDs für Apps ein, die auf überwachten iOS-Geräten selbstständig in den Single-App-Modus wechseln. Sie können zum Beispiel individuelle Prüfungs-Apps für Studenten angeben. Sobald der Student die App ausführt, wechselt diese in den Single-App-Modus für , damit der Student während der Prüfung nicht auf andere Ressourcen zugreifen kann. Diese Funktion gilt für Apps, die für den autonomen Single-App-Modus entwickelt wurden. Überwachung erfolgt über Apple Configurator.
	iOS 8 ausgeliefert+	
	Datensicherung von Unternehmens-Büchern erlauben.	Wählen Sie diese Option aus, um ein persönliches Backup von iBooks, ePub und PDF-Dokumenten zu erlauben, die mit MDM auf das Gerät übertragen wurden.
	Synchronisation von Anmerkungen und Markierungen der Unternehmens-Bücher erlauben.	Wählen Sie diese Option aus, wenn Anmerkungen und Hervorhebungen in Enterprise-Books mit iTunes synchronisiert werden dürfen.
	Apple Watch-Handgelenkerkennung erzwingen	Wählen Sie diese Option aus, um Benachrichtigungen auf dem Bildschirm auszublenden, solange niemand die Apple Watch trägt.
	iOS 8+ überwacht	
	Prädiktive Tastatur erlauben	Wählen Sie diese Option aus, damit der Benutzer die Vorschlagoption von iOS beim Eingeben eines Wortes aktivieren kann, sodass der Benutzer nur auf einen der drei Vorschläge tippen muss, um das Wort komplett einzugeben.
	Tastatur-Autokorrektur erlauben	Wählen Sie diese Option aus, um die Autokorrektur mit Bluetooth-Tastaturen zu erlauben.
	Tastatur-Rechtschreibprüfung erlauben	Wählen Sie diese Option aus, um eine Rechtschreibprüfung mit Bluetooth-Tastaturen zu erlauben.
	Tastatur-Definitionsanzeige	Wählen Sie diese Option aus, um die Definitionssuche mit Bluetooth-Tastaturen zu erlauben.
	Modifikation von Touch-ID-Fingerabdrücken / Face-ID-Gesichtern zulassen	Wählen Sie die Option aus, damit die Einstellungen für Touch-ID oder Face-ID geändert werden dürfen.

Kategorie	Einstellung	Aktion
	iOS 9+ überwacht	
	Tastenkombinationen auf iPads zulassen	Klicken Sie auf die Option; um die Verwendung von Tastenkombinationen auf dem iPad zu erlauben.
	Wallpaper-Modifikation zulassen	Klicken Sie auf die Option, um den Benutzern die Änderung der Hintergrundbilder zu erlauben.
	Kopplung mit Apple Watch zulassen	Wählen Sie die Option, um das iPhone mit der Apple Watch zu koppeln.
	Gerätename-Modifikation zulassen	Klicken Sie auf die Option, um dem Benutzer die Änderung des Namens für das Gerät zu erlauben.
	Modifikation der Vertrauenswürdigkeitseinstellungen der Unternehmens-App zulassen.	Wählen Sie die Option aus, um die Einstellungen zur Vertrauenswürdigkeit der Unternehmens-App zu ändern.
	iOS 9.3+-überwacht	
	Modifikation der Benachrichtigungseinstellungen zulassen	Wählen Sie die diese Option aus, damit Benutzer die Benachrichtigungseinstellungen ändern dürfen.
	iOS 9.3.2+-überwacht	
	Diagnoseversand und Modifikation erlauben	Wählen Sie diese Option aus, damit Benutzer Einstellungen zum Versand von Diagnosedaten an Apple ändern können.
	iOS 10+ überwacht	
	Bluetooth-Modifikation erlauben	Wählen Sie diese Option aus, damit die Benutzer die Bluetooth-Einstellung auf den überwachten Geräten modifizieren können. Zweckmäßig ist diese Option in Fällen, bei denen gemeinsam genutzte iPads für die Classroom-App und Apple Education verwendet werden und zum Start der App Bluetooth benötigt wird.
	iOS 10.3+ überwacht	
	Diktieren zulassen	Wählen Sie diese Option aus, damit der Benutzer keine Eingaben tippen muss, sondern stattdessen mit dem iPhone oder iPad sprechen kann (gilt nur für iPads).
	iOS 11+ überwacht	
	AirPrint zulassen	Klicken Sie auf „die Option, um die AirPrint-Funktion für den Druck im WLAN zu erlauben.

Kategorie	Einstellung	Aktion
	Speicherung der AirPrint-Anmeldeinformationen zulassen	Klicken Sie auf die Option, um eine Keychain-Speicherung von Benutzername und Passwort für AirPrint zu erlauben.
	AirPrint iBeacon Discovery zulassen	Klicken Sie auf die Option, wenn Sie dem Benutzer erlauben wollen, die iBeacon-Erkennung von AirPrint-Druckern einzustellen.
	Gold VPN-Konfigurationen zulassen	Klicken Sie auf die Option, wenn der Benutzer die VPN-Konfiguration vornehmen darf.
	Für AirPrint vertrauenswürdiges TLS erzwingen.	Klicken Sie auf die Option, um Vertrauenswürdige Zertifikate für die TLS-Druckkommunikation zuzulassen. Standard: nicht ausgewählt
	Entfernung von System-Apps zulassen	Wählen Sie die Option aus, um die Entfernung der System-App zu erlauben.
	Modifikation der Mobilfunk-Tarifeinstellungen zulassen	Wählen Sie die Option aus, damit die Benutzer die Mobilfunk-Tarifplaneinstellungen ändern können.
	Konfiguration neuer Geräte in der Nähe zulassen	Wählen Sie die Option aus, damit die Benutzer neue Geräte in der Nähe konfigurieren können.
	Classroom-Klassen ohne Aufforderung automatisch beitreten	Wählen Sie die Option aus, damit die Benutzer sich automatisch ohne Eingabeanforderung in Klassen im Unterrichtsraum anmelden können. Standard: nicht ausgewählt
	Classroom erlauben, eine App und das Gerät ohne Aufforderung zu sperren	Wählen Sie die Option aus, damit der Unterrichtsraum eine App und das Gerät ohne Aufforderung an den Benutzer sperren kann. Standard: nicht ausgewählt
	Authentifizierung des Benutzers erzwingen, bevor Kennwörter oder Kreditkarteninformationen automatisch in Safari und Apps eingetragen werden können	Der Geräteeigentümer muss sich zuerst authentifizieren, damit Kennwörter oder Kreditkarteninformationen automatisch in Safari und in Anwendungen eingetragen werden können. Standard: Falsch

Kategorie	Einstellung	Aktion
	iOS 11.3+	
	Kopplung mit entfernter App zulassen (tvOS 11.3 und höher)	Wählen Sie diese Option aus, um die Kopplung des Geräts mit der entfernten App zu erlauben.
	Eingehende AirPlay-Anfragen zulassen (tvOS 11.3 und höher)	Wählen Sie diese Option aus, um eingehende AirPlay-Anforderungen zuzulassen.
	iOS 11.3+ überwacht	
	USB Restricted Mode zulassen	Wählen Sie diese Option, damit der Benutzer den eingeschränkten USB-Modus nutzen kann.
	Software-Updates um 30 Tage verschieben (für iOS 11.3, tvOS 12.2 und später nur auf überwachten Geräten)	Wählen Sie diese Option, um anzugeben, um wie viele Tage Sie Software-Updates verschieben möchten. Die Standardeinstellung ist 30 Tage, und das Maximum sind 90 Tage. Standard: nicht ausgewählt
	Bei nicht verwalteten Klassen ist zum Verlassen des Classroom eine Trainerberechtigung erforderlich.	Klicken Sie auf die Option, damit der Benutzer die benötigte Erlaubnis des Lehrers zum Verlassen des Unterrichtsraums bei nicht verwalteten Klassen erhält.
	iOS 12:3+-überwacht	
	Automatisches Datum und Uhrzeit erzwingen (iOS 12.0 und tvOS 12.2 und höher)	Aktivieren Sie für die Funktion Datum & Uhrzeit "automatisch einstellen". Diese Funktion kann vom Benutzer nicht deaktiviert werden. Standard: Falsch
	Ändern von eSIM-Einstellungen zulassen (iPhone XS, iPhone XS Max und iPhone XR - iOS 12.1 und neuere Versionen)	Wählen Sie diese Option, damit die Benutzer die eSim-Konfiguration auf den überwachten Geräten modifizieren können. Diese Option verhindert außerdem, dass Benutzer in den Einstellungen ihrer Geräte einen Mobiltelefontarif hinzufügen oder entfernen. Standard: Wahr
	iOS 12.2+ überwacht	
	Ändern der Einstellungen für	Wählen Sie diese Option, damit der Benutzer die Einstellungen für den persönlichen Hotspot ändern kann.

Kategorie	Einstellung	Aktion
	persönliche Hotspots zulassen	Standard: Wahr
	iOS 13.0+	
	Files-App Netzwerklaufwerkszugriff erlauben	Wählen Sie diese Option, damit der Benutzer eine Verbindung zu Netzlaufwerken in der Dateianwendung aufbauen kann. Standard: Wahr
	Files-App USB-Laufwerkzugriff erlauben	Aktivieren Sie diese Option, damit der Benutzer eine Verbindung zu allen angeschlossenen USB-Geräten in der Dateianwendung herstellen kann. Standard: Wahr
	iOS 13.0+ überwacht	
	Wischeingabe-Tastatur zulassen	Wählen Sie diese Option, um eine kontinuierliche Tastatur (zum Wischen oder zum Streichen über Buchstaben) zu aktivieren. Standard: Wahr
	Sleep-Modus für Gerät zulassen	Wählen Sie diese Option, um den Ruhezustand des Geräts zu aktivieren. Standard: Wahr
	Gerätesuche erlauben	Wählen Sie diese Option, um die Option Mein Gerät suchen in der App Find My zu aktivieren. Standard: Wahr
	Find My Friends zulassen	Wählen Sie diese Option, um „Meine Freunde finden“ in der App „Find My“ zu aktivieren. Standard: Wahr
	WLAN-Einschalten erzwingen	Wählen Sie diese Option, um die WLAN-Stromversorgung einzuschalten. Standard: Falsch
	iOS 13.4+	
	Gastsitzung für freigegebenes iPad erlauben	Ist diese Option nicht aktiviert („falsch“), sind temporäre Sitzungen auf dem gemeinsam genutzten iPad nicht verfügbar. Standard: Wahr
	iOS 14.0+	
	Personalisierte Apple-Werbung erlauben	Status „falsch“ schränkt die personalisierte Werbung von Apple ein. Dadurch wird verhindert, dass Apple die Informationen des Benutzers zur gezielten Werbung verwendet. Dadurch wird die Anzahl der eingegangenen Werbeanzeigen möglicherweise nicht verringert, aber die Anzeigen werden für den Benutzer weniger relevant sein. Standard: Wahr
	iOS 14.0+ überwacht	

Kategorie	Einstellung	Aktion
	App-Clips zulassen	Ist diese Option nicht aktiviert („falsch“), kann kein Benutzer App-Clips hinzufügen, und alle vorhandenen App-Clips werden von dem Gerät entfernt. Voreinstellung: Wahr
	iOS 14.2+ überwacht	
	NFC zulassen **iOS 14.5+**	Wenn die Einstellung falsch ist, wird NFC deaktiviert. Erfordert ein überwachtes Gerät. Verfügbar ab iOS 14.2 und höher. Voreinstellung: Wahr
	Automatisches Entsperren zulassen	Administratoren können die vorhandene Einschränkung allowAutoUnlock verwenden, um diese Funktion zu verwalten. Ist der Wert „false“, wird die automatische Entsperrung deaktiviert. Verfügbar ab iOS 10.12 und höher sowie macOS 14.5 und höher. Voreinstellung: true
	Diktat nur auf Gerät erzwingen **iOS 14,5+ überwacht** Ungekoppeltes externes Booten zur Wiederherstellung zulassen	Ist der Wert „wahr“, werden Verbindungen zu Siri-Servern zum Diktieren deaktiviert. Voreinstellung: false Bei „true“ können Geräte von einem nicht gekoppelten Gerät in die Wiederherstellung gestartet werden. Voreinstellung: false
	WLAN-Verbindung nur zu erlaubten Netzwerken gestatten	Bei Einstellung „true“ darf das Gerät nur WLAN-Netzwerken beitreten, die über das Konfigurationsprofil eingerichtet wurden. Voreinstellung: false Wenn die Einschränkung **WLAN nur bei zugelassenen Netzwerken erlauben** aktiviert ist und die WLAN-Konfiguration nicht an das Gerät verteilt ist, geht die WLAN-Verbindung verloren.
	iOS15+	
	Übersetzung nur auf Gerät erzwingen Verwaltete Pasteboard anfordern	Wenn die Auswahl „true“ ist, stellt das Gerät keine Verbindung zu Siri-Servern für die Übersetzung her. Voreinstellung: false Wenn die Auswahl „true“ ist, respektiert die Kopier- und Einfügefunktion die Einschränkungen allowOpenFromManagedToUnmanaged und allowOpenFromUnmanagedToManaged. Voreinstellung: false
	iOS 15.2+	
	E-Mail-Datenschutz zulassen	Bei "falsch" wird der E-Mail-Datenschutz auf dem Gerät deaktiviert. Verfügbar ab iOS 14.2 und höher.

Kategorie	Einstellung	Aktion
		Wenn die Konfiguration "E-Mail-Datenschutz zulassen" installiert ist und über das Ivanti Neurons for MDM-Administrationsportal aktiviert wurde, ist der Umschalter für den Schutz der E-Mail-Aktivität aktiviert und folgende Optionen werden angeboten: • **IP-Adresse ausblenden** – Der Absender der E-Mail kann die E-Mail nicht mit Ihrer Online-Aktivität in Verbindung bringen oder Ihren Standort ermitteln. • **Alle Remote-Inhalte blockieren** – Verhindert, dass der Absender der E-Mail Ihre E-Mail-Aktivitäten sieht. Voreinstellung: true
	iOS 15.4+	
	Automatischen Bildschirmschoner von Apple TV zulassen (ab tvOS 15.4)	Bei "falsch" wird der automatische Apple TV-Bildschirmschoner deaktiviert. Verfügbar ab iOS 14.2 und höher. Voreinstellung: true
	iOS 16.0 bis 26.0	
	Installation von Sicherheitsverbesserungen im Hintergrund zulassen	Um die Antworten zu deaktivieren. Der Benutzer kann keine Sicherheitsverbesserungen im Hintergrund installieren.
	Entfernen von Sicherheitsverbesserungen im Hintergrund zulassen	Um den Benutzer darin zu hindern, die Antworten rückgängig zu machen. Der Benutzer kann keine Sicherheitsverbesserungen im Hintergrund entfernen.
	iOS 17.0+ überwacht	
	iPhone-Widgets auf Mac-Geräten zulassen	Wählen Sie diese Option aus, um zuzulassen, dass iPhone-Widgets auf Mac-Geräten angezeigt werden, wobei dieselbe AppleID von iPhone for iCloud auf beiden Geräten verwendet wird.
	iOS 17.2+ überwacht	
	Live Voice Mail zulassen	Wählen Sie diese Option aus, um Live-Voice Mail auf dem Gerät zu aktivieren.
	"ESIM bei Löschung beibehalten" erzwingen	Wählen Sie diese Option aus, um den eSIM beizubehalten, wenn das System das Gerät wegen zu vieler Kennwort-Falscheingaben löscht oder wählen Sie die Option "Alle Inhalte und Einstellungen löschen" unter **Einstellungen** > **Allgemein** > **Zurücksetzen** aus. Das System behält den eSIM nicht bei, wenn **Mein Gerät finden** die Löschung des Geräts initiiert.
	iOS 17.4+ überwacht	

Kategorie	Einstellung	Aktion
	Installation von Marketplace-Apps zulassen	Wählen Sie diese Option aus, um Benutzern das Herunterladen von Apps von alternativen Marketplaces zu erlauben. Wenn diese Einschränkung auf "falsch" gesetzt ist, können Benutzer keine neuen Apps von alternativen Marktplätzen installieren und keine bereits von solchen Marktplätzen installierte Apps verwenden.
	Automatisches Dimmen zulassen **iOS 17.5+ überwacht**	Wählen Sie diese Einstellung aus, um die Option für automatisches Dimmen auf iPads mit OLED-Display zuzulassen.
	Installation der Webverteilungs-App zulassen	Wenn die Einschränkung **allowWebdistributionAppInstallation** auf "falsch" gesetzt ist, können Benutzer Apps von neuen alternativen Websites nicht direkt installieren. Diese Einstellung gilt nur für überwachte Geräte.
	iOS 18.0+ überwacht	
	Ausgehende eSIM-Transfers zulassen	Wählen Sie diese Option aus, um den Transfer eines eSIM an ein anderes Gerät zu erlauben als das, auf dem die Einschränkung installiert ist.
	Genmoji zulassen	Wählen Sie diese Option, um die Erstellung von Genmojis zuzulassen.
	Image Playground zulassen	Wählen Sie diese Option, um die Bildgenerierung zuzulassen.
	Image Wand zulassen	Wählen Sie diese Option, um die Image Wand zuzulassen.
	iPhone-Spiegelung zulassen	Wählen Sie diese Option, um die iPhone-Spiegelung auf einem macOS-Gerät zuzulassen.
	Ergebnisse personalisierte Handschrift zulassen	Wählen Sie diese Option, um zuzulassen, dass das System unter Verwendung der Handschrift des Benutzers Text erstellt.
	Schreibtools zulassen	Wählen Sie diese Option, um Apple Intelligence-Schreibtools zu aktivieren.
	Ausblenden der Apps zulassen	Wählen Sie diese Option aus, wenn Sie möchten, dass Apps ausgeblendet werden können.
	Sperren der Apps zulassen **iOS 18.1+ überwacht**	Wählen Sie diese Option aus, wenn Sie möchten, dass Apps gesperrt werden können.
	Anrufaufzeichnung zulassen	Wählen Sie diese Option aus, um das Aufzeichnen von Anrufen zuzulassen. Standard: Wahr
	E-Mail-Zusammenfassung	Wählen Sie diese Option aus, um das manuelle Zusammenfassen von E-Mail-Nachrichten zuzulassen.

Kategorie	Einstellung	Aktion
	zulassen	Standard: Wahr
	RCS Messaging zulassen	Wählen Sie diese Option aus, um RCS Messaging zuzulassen. Standard: Wahr Auf iOS 26-Geräten und Mobilfunk-iPad-Modellen mit iPadOS 26 kann die RCS Messaging-Nutzung auf Geräten begrenzt sein, deren Mobilfunktarif mit ICCID verknüpft ist.
	iOS 18.2+ überwacht	
	Externe Datenintegrationen zulassen	Wählen Sie diese Option aus, um die Verwendung externer, cloudbasierter Datendienste mit Siri zuzulassen.
	Anmeldung externer Datenintegrationen zulassen	Wählen Sie diese Option aus, um externen Datenanbietern den Wechsel in den anonymen Modus zu erlauben. Wenn ein Benutzer bereits bei einem externen Datenanbieter angemeldet ist, wird er bei Anwendung dieser Einschränkung abgemeldet.
Anwendungen	Änderung des Standardbrowsers zulassen	Wählen Sie diese Option aus, um das Festlegen eines anderen bevorzugten Standardbrowsers zuzulassen. Über die Ivanti Neurons for MDM-Einstellungen können Sie den Standardwebbrowser festlegen.
	iOS Alle Versionen	Zugang zu Anwendungen auf dem Geräte zulassen.
	Installation von Apps zulassen	Wählen Sie die Option, um dem Benutzer zu gestatten, Apps aus dem Apple App Store zu installieren. Heben Sie die Auswahl auf, um den App Store zu deaktivieren und das zugehörige Symbol vom Startbildschirm zu entfernen.
	Verwendung der Kamera zulassen	Wählen Sie diese Option, um dem Benutzer zu gestatten, die Kamera zu bedienen. Heben Sie die Auswahl auf, um die Kamera zu deaktivieren und das zugehörige Symbol vom Startbildschirm zu entfernen. Auf iOS 26+-Geräten wird die Einschränkung "Kamera zulassen" nicht angewendet, wenn die Apps zur Ausnahmeliste hinzugefügt wurden.
	Verwendung von Safari zulassen	Wählen Sie diese Option, um die Nutzung des Web-Browsers Safari zuzulassen. Heben Sie die Auswahl auf, um den Web-Browser Safari zu deaktivieren, das zugehörige Symbol vom Startbildschirm zu entfernen und Benutzer davon abzuhalten, Web-Clips zu öffnen.
	Automatisches Ausfüllen aktivieren	Wählen Sie diese Option, um die Funktion zum automatischen Ausfüllen für Felder in Safari zu aktivieren.
	Betrugswarnung erzwingen	Wählen Sie diese Option, damit Safari verhindert, dass Benutzer als betrügerisch oder schädlich befundene Websites aufrufen.

Kategorie	Einstellung	Aktion
Safari	JavaScript aktivieren	Wählen Sie diese Option, um die Unterstützung von JavaScript für Safari zu aktivieren.
	Popups blockieren	Wählen Sie diese Option, damit Safari Popups gesperrt.
	Nur überwacht – Version 26+	
	Leeren des Safari-Verlaufs zulassen	Wählen Sie diese Option, um Benutzern das Löschen des Browserverlaufs zu erlauben.
	Privates Browsen in Safari zulassen	Wählen Sie diese Option, um privates Browsen zuzulassen.
	iOS Alle überwachten Versionen	
	Deinstallation von Apps zulassen	Wählen Sie diese Option aus, wenn die Benutzer Apps vom Gerät entfernen dürfen.
	Nutzung des Game Center zulassen	Wählen Sie diese Option, um den Zugriff auf das Game Center zuzulassen.
	Hinzufügen von Game-Center-Freunden zulassen	Wählen Sie um Benutzern zu ermöglichen, Freunde zum Game Center hinzuzufügen.
	Multiplayer-Spiele zulassen	Wählen Sie diese Option, um Benutzern zu gestatten, Spiele mit mehreren Spielern zu spielen.
	iMessage zulassen	Wählen Sie diese Option, um die Nutzung von iMessage zuzulassen. Auf iOS 26-Geräten und Mobilfunk-iPad-Modellen mit iPadOS 26 kann die iMessage-Nutzung begrenzt sein, wenn das Gerät zur Verweigerungsliste hinzugefügt wurde.
	Cookies akzeptieren	Wählen Sie als Option "Nie", "Immer" oder "Von besuchten Sites" aus.
	FaceTime zulassen	Wählen Sie diese Option, um dem Benutzer die Ausführung von FaceTime zu gestatten, wenn die Kamera aktiviert ist. Auf iOS 26-Geräten und Mobilfunk-iPad-Modellen mit iPadOS 26 kann FaceTime begrenzt sein, wenn das Gerät zur Verweigerungsliste hinzugefügt wurde.
	iOS 8 ausgeliefert+	
	Cloud-Synchronisation für verwaltete Anwendungen erlauben.	Wählen Sie diese Option aus, wenn verwaltete Apps in der Cloud synchronisiert werden dürfen.

Kategorie	Einstellung	Aktion
	Aktivitätsfortführung erlauben.	Wählen Sie diese Option aus, um die Fortführung von Aktivitäten in Apps zu erlauben, die Handoff unterstützen.
	iOS 8+ überwacht	
	Verwendung von Podcasts erlauben	Wählen Sie diese Option, um die Nutzung von Podcasts zuzulassen.
	iOS9+	
	Neue Unternehmens-App-Autoren als vertrauenswürdig einstufen	Klicken Sie auf die Option, um dem Benutzer den Zugriff auf neue Unternehmens-Apps zu erlauben.
	iOS 9+ überwacht	
	App Store zulassen	Klicken Sie auf die Option, um dem Benutzer den Zugriff auf den Apple Store zu erlauben.
	Automatisches App-Download zulassen	Klicken Sie auf die Option, wenn die App Dateien, Daten und Updates mit Benutzeraufforderung herunterladen darf.
	News-App zulassen	Wählen Sie diese Option, um die Nutzung von YouTube zuzulassen.
	iOS 9.3+-überwacht	
	iTunes Radio zulassen	Wählen Sie diese Option aus, um die Nutzung von iTunes Radio zuzulassen.
	Apple Music zulassen	Wählen Sie diese Option aus, um Apple Music zuzulassen.
	Aufgelistete App-Bundle-IDs zulassen	Aktivieren Sie dieses Kontrollkästchen, damit nur die im Array aufgeführten Bundle-IDs angezeigt oder gestartet werden können. Fügen Sie den Wert com.apple.webapp ein, um alle Webclips zuzulassen.
	Gesperrte App-Bundle-IDs	Aktivieren Sie dieses Kontrollkästchen, damit die im Array aufgeführten Bundle-IDs nicht angezeigt oder gestartet werden können. Fügen Sie den Wert com.apple.webapp ein, um alle Webclips einzuschränken.
	iOS 13.0+ überwacht	
	Verwendung des iTunes Store zulassen	Wählen Sie diese Option, um die Nutzung des iTunes Music Store zuzulassen. Heben Sie die Auswahl auf, um den iTunes Music Store zu deaktivieren und das zugehörige Symbol vom Startbildschirm zu entfernen.

Kategorie	Einstellung	Aktion
iCloud	iOS Alle Versionen Backups zulassen	Zugang zu iCloud-Diensten aktivieren. Wählen Sie diese Option, damit das Gerät Daten über den iCloud-Dienst von Apple sichern kann.
	Dokumentensynchronisierung zulassen	Wählen Sie diese Option, um die Synchronisierung von Dokumenten über den iCloud-Dienst von Apple zuzulassen.
	Fotostream zulassen Gemeinsame Foto-Streams zulassen (eine Verweigerung der Erlaubnis kann zu Datenverlust führen).	Wählen Sie diese Option, um die Synchronisierung von Fotos auf Ihren anderen iOS-Geräten über iCloud von Apple zuzulassen. Wählen Sie diese Option, um die Synchronisierung von freigegebenen Fotos zuzulassen Die Deaktivierung dieser Option kann dazu führen, dass Fotos verloren gehen.
	Keychain-Synchronisation zulassen **iOS9+** iCloud Photo-Bibliothek zulassen **iOS 15+ auf überwachten Geräten**	Wählen Sie die Option, um die Synchronisation Ihres Schlüsselbunds zuzulassen. Klicken Sie auf die Option, um den Zugriff auf die iCloud-Fotobibliothek zu erlauben.
	Cloud-Privat-Relay erlauben	Wenn diese Option auf „false“ eingestellt ist, wird das iCloud Private-Relay deaktiviert. Voreinstellung: true

Kategorie	Einstellung	Aktion
Sicherheit und Privatsphäre	**iOS Alle Versionen**	Richtlinien zur Sicherheit und Privatsphäre aktivieren.
	Over-the-Air-Zertifikat-Updates zulassen	Wählen Sie die Option, um Over-the-Air-Updates für Root-Zertifikate zuzulassen.
	„Ad Tracking beschränken“ erzwingen **iOS Alle überwachten Versionen**	Wählen Sie die Option, um den Einsatz der Funktion „Ad Tracking beschränken“ zu erzwingen.
	Konfigurationsprofil-Installation zulassen	Wählen Sie diese Option, um dem Benutzer zu gestatten, Konfigurationsprofile und Zertifikate interaktiv zu installieren.
	Vom Benutzer des Assistenten erzeugte Inhalte zulassen **iOS 8+ überwacht**	Wählen Sie die Option, um zuzulassen, dass Siri vom Benutzer erzeugte Inhalte aus dem Internet abruft.
	Benutzern dürfen alle Inhalte und Einstellungen in der Reset-Benutzerschnittstelle löschen.	Wählen Sie diese Option aus, um in der iOS-Reset-Benutzeroberfläche des Geräts die Option "Alle Inhalte und Einstellungen löschen" zu aktivieren.
	Bildschirmzeit zulassen	Wählen Sie diese Option, um Bildschirmzeit zuzulassen (Einstellungen > Bildschirmzeit).
	Senden von Diagnosedaten an Apple zulassen	Wählen Sie diese Option, um die automatische Übermittlung von Diagnosedaten an Apple zuzulassen.
	Annahme nicht vertrauenswürdiger TLS-Zertifikate durch den Benutzer zulassen	Wählen Sie diese Option, um dem Benutzer des Geräts die Annahme nicht vertrauenswürdiger HTTPS-Zertifikate zu gestatten. Wenn diese Option nicht ausgewählt ist, lehnt das Gerät nicht vertrauenswürdige HTTPS-Zertifikate automatisch ab, ohne den Benutzer des Geräts dazu aufzufordern.
	Verschlüsselte Backups erzwingen	Wählen Sie die Option, um verschlüsselte Backups über iTunes zu erzwingen. Aufgrund der SCEP-Anforderungen ist die Option automatisch ausgewählt.

Kategorie	Einstellung	Aktion
	Für alle Käufe Eingabe des iTunes-Store-Passworts vom Benutzer erzwingen	Wählen Sie diese Option, damit der Benutzer des Geräts sein iTunes-Passwort für jede Transaktion im App Store eingeben muss. Wenn diese Option nicht ausgewählt ist, kann der Benutzer des Geräts mit einer einzelnen Authentifizierung mehrere Transaktionen tätigen.
	iOS9+	
	AirDrop als nicht verwaltetes Ziel behandeln **iOS 9+ überwacht** Gerätepasscode-Modifikation zulassen iOS 12+	Wählen Sie diese Option aus, um den Benutzerzugang zur AirDrop-Dateifreigabe zu erlauben. Standard: Falsch Klicken Sie auf die Option, um dem Benutzer die Änderung des Passworts für das Gerät zu erlauben.
	Verwaltete Apps dürfen Kontakte in nicht verwaltete Kontaktkonten schreiben. iOS 12:3+-überwacht Automatisches Eintragen der Passwörter zulassen	Wählen Sie diese Option aus, damit verwaltete Apps in Kontakte nicht verwalteter Kontaktkonten schreiben können. Standard: Falsch Wählen Sie diese Option aus, damit Benutzer Passwörter automatisch eintragen können und aufgefordert werden, in Safari oder in Apps ein gespeichertes Passwort zu verwenden.
	In der Nähe befindliche Geräte dürfen Anfragen nach einem Passwort teilen. Passwortteilung zulassen	Wählen Sie diese Option aus, damit ein Benutzergerät Passwörter von Geräten in der Nähe anfordern kann. Wählen Sie diese Option aus, damit die Benutzer ihre Passwörter mit der Funktion "Airdrop Passwords" teilen können.
	Nicht verwaltete Apps dürfen Kontakte aus verwalteten Kontaktkonten lesen. iOS 18.3 Externe Intelligence Workspace-IDs zulassen Zusammenfassung von	Wählen Sie diese Option aus, damit nicht verwaltete Apps verwaltete Kontaktkonten auslesen können. Standard: Falsch Geben Sie die zulässige externe Intelligence Workspace-ID ein. Wählen Sie diese Option, um die Erstellung von Zusammenfassungen aus Transcriptions zuzulassen.

Kategorie	Einstellung	Aktion
	Notiztranskription zulassen	Voreinstellung: Wahr
	Zusammenfassung von Visual Intelligence zulassen	Wählen Sie diese Option, um die Erstellung von Zusammenfassungen aus Apple Visual Intelligence unter Verwendung von Bildern oder visuellen Inhalten zuzulassen. Voreinstellung: Wahr

Kategorie	Einstellung	Aktion
Bewertung von Inhalten		Zugang auf Apps und Medien kontrollieren.
	Explizit die Wiedergabe von Musik, Podcasts und iTune-Medien (nur überwachtes iOS 13+ sowie tvOS 13.11.3 und höher) zulassen.	Eindeutige Inhalte werden beim Verkauf über den iTunes Store von den Anbietern der Inhalte, z. B. Plattenlabels, als solche gekennzeichnet.
	Region für Bewertungen	Wählen Sie eine Region aus der Dropdown-Liste, um die Region zu ändern, die mit den Bewertungen von Apps, Fernsehsendungen und Filmen verbunden ist.
	Filme	Bestimmen Sie eine Bewertungsgrenze für die auf dem Gerät gespeicherten Filme: • Videos nicht zulassen • G • PG • PG-13 • R • NC-17 • Alle Filme zulassen
	Fernsehsendungen	Bestimmen Sie eine Bewertungsgrenze für die auf dem Gerät gespeicherten Fernsehsendungen: • Fernsehsendungen nicht zulassen • TV-Y • TV-Y7 • TV-G • TV-PG • TV-14 • TV-MA • Alle Fernsehsendungen zulassen
	Apps	Bestimmen Sie eine Bewertungsgrenze für die auf dem Gerät gespeicherten Apps: • Apps nicht zulassen • 4+ • 9+ • 12+ • 17+ • Alle Apps zulassen

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.4.27. Konferenzraum-Anzeige

Gilt für tvOS 10.2 und unterstützte neuere Versionen.

Diese Konfiguration schaltet den Konferenzraum-Anzeigemodus auf Apple TV ein. Der Konferenzraum-Anzeigemodus sperrt Apple TV in diesem Modus, um andere Arten der Nutzung zu verhindern.

Ab tvOS 10.2 können Sie für überwachte Apple TV-Geräte den Konferenzraum-Anzeigemodus einstellen. Die Konferenzraumanzeige sperrt Apple TV-Geräte mit einem schwarzen Bildschirmhintergrund und lädt einen Standard-Bildschirmschoner herunter, sofern kein Hintergrundbild und ein Bildschirmschoner manuell in den Apple TV-Geräteeinstellungen definiert sind. In diesem Modus kann auch eine Meldung angezeigt werden, wie sie bei der Konfiguration der Konferenzraumanzeige definiert wird.

Die Konfiguration der Konferenzraumanzeige kann automatisch bereitgestellt werden; Anwendungen können installiert werden, solange sich die Geräte in diesem Modus befinden. Ein Gerät, das auf den Konferenzraum-Anzeigemodus eingestellt ist und neu gestartet wird, zeigt automatisch den gesperrten Bildschirm wieder an, ohne zuerst den Startbildschirm einzublenden.

> Wenn ein Apple TV-Gerät im Single App-Modus läuft oder der Single App-Modus mit der Konferenzraumanzeige bereitgestellt wird, setzt die Konferenzraumanzeige den Single App-Modus außer Kraft. Wenn ein Apple TV-Gerät über Ethernet mit einem Netzwerk verbunden ist, wird auf dem Konferenzraum-Display nicht automatisch ein WLAN-Netzwerk zur Anmeldung für die AirPlay-Freigabe angezeigt. Diese Anweisung kann auf dem Bildschirm über das Feld „Benutzerdefinierte Nachricht“ der Konferenzraum-Anzeigekonfiguration angezeigt werden.

Konferenzraum-Anzeigekonfiguration erstellen

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie **Conference** in das Suchfeld ein und klicken Sie dann auf die Konfiguration der **Konferenzraumanzeige**.
4. Geben Sie einen Namen ein und beschreiben Sie die Konfiguration.
5. Geben Sie die **benutzerdefinierte Nachricht** ein. Dies ist die benutzerdefinierte Nachricht, die im Konferenzraum-Anzeigemodus auf dem Bildschirm angezeigt wird.
6. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
7. Klicken Sie auf **Fertig**.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.4.28. Tastatureinstellungen

Verwenden Sie die **Tastatureinstellungen**, um Tastatureinstellungen auf überwachten Geräten zu konfigurieren. Diese Deklaration hilft Administratoren, konsistente, richtlinienbasierte Kontrollen anzuwenden, die das Tastaturverhalten, Eingabeoptionen und zugehörige Einstellungen für die Benutzererfahrung steuern.

Gilt für:

- iOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- macOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Tastatureinstellungen** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie die **Tastatureinstellungen** gemäß der folgenden Tabelle:

10.10.4.29. Sperre & Kiosk: Android-Geräte Administratormodus

Sperre und Kiosk: Die Android-Konfiguration für den Geräte-Admin-Modus deaktiviert bestimmte Funktionen der Android-Geräte und erstellt eine Whitelist der Apps, die den Benutzern im Kiosk-Modus zur Verfügung stehen.

> Die Android-Konfiguration für den Geräte-Admin-Modus ist veraltet und wird auf Geräten mit Android 8 oder späteren Versionen nicht mehr unterstützt. Für Android 8 und spätere Versionen wird die Verwendung von Android Enterprise-Sperren für Kiosk-Sperren empfohlen.

Sie können die Option zur Änderung der Einstellungen oder Apps beschränken, wenn ein Android-Gerät im Kiosk-Modus arbeitet.

- Ergänzen Sie Apps und wählen Sie Einstellungen auf der Seite „Sperre und Kiosk erstellen“ der Android-Konfigurationsseite für Administratoren.
- Im Kiosk-Modus können Sie über das Symbol für Einstellungen die Einstellungen ändern.
- Wenn Sie nur Apps auswählen, aber keine Einstellungen, werden die Konfigurationsoptionen und das Symbol für die Einstellungen im Kiosk-Modus nicht angezeigt.
- Wenn Sie keine Apps in der Konfiguration eintragen wollen, wird das Symbol für die Einstellungen angezeigt.

Einstellung	So gehen Sie vor
[Name] Beschreibung **Sperr-Einstellungen:** Funktionen für alle Android-Geräte deaktivieren.	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet. Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Wi-Fi deaktivieren	Wählen Sie diese Option, um den Zugriff auf drahtlose Netzwerke zu deaktivieren.
Kamera deaktivieren Bluetooth deaktivieren **Kiosk-Moduseinstellungen:** Ermöglicht die Nutzung des Geräts als Kiosk mit einer beschränkten Anzahl spezifischer Apps. Die Einstellungen des Kioskmodus werden nicht für ein Gerät mit Android 8.0 und höher übernommen. Für solche Geräte wird auf der Seite mit den Gerätedetails als Kioskstatus UNSUPORTED_ON_DEVICE gemeldet.	Wählen Sie diese Option, um den Zugriff auf die Kamera zu deaktivieren. Wählen Sie diese Option, um Bluetooth-Funktionen zu deaktivieren. Seien Sie bei Anwendung dieser Option vorsichtig. Ivanti rät davon ab, Audio-Funktionen zu deaktivieren, da damit auch der Zugriff auf Bluetooth-Freisprecheinrichtungen deaktiviert wird. Gesetzliche Vorschriften zur Nutzung von Freisprechanlagen während des Fahrens sind immer weiter verbreitet.
Kiosk-Modus aktivieren	Klicken Sie auf , um den **Kiosk Mode** auf Android-Geräten zu konfigurieren.
Schnelleinstellungen deaktivieren Benutzerzugriff auf Wi-Fi-Einstellungen zulassen	Wählen Sie diese Option aus, um die Schnelleinstellungen im Kiosk-Modus zu deaktivieren. Wählen Sie diese Option aus, damit ein Benutzer die WLAN-Einstellungen ändern und auf bevorzugte drahtlose Netze zugreifen kann.
Benutzerzugang für Bluetooth-Einstellungen zulassen Benutzerzugang für Standort-Einstellungen zulassen	Wählen Sie diese Option aus, damit ein Benutzer die Bluetooth-Einstellungen ändern und weitere Bluetooth-Geräte koppeln kann. Wählen Sie diese Option aus, damit ein Benutzerzugriff auf die Standorteinstellungen möglich ist.

Einstellung	So gehen Sie vor
Verzögerung der Anwendungs-Updates durch Benutzer zulassen	Wählen Sie diese Option aus, damit ein Benutzer Anwendungsupdates verzögern kann.
PIN zum Beenden des Kiosk-Modus	Geben Sie den vierstelligen Zahlencode ein, den der Endbenutzer eingeben muss, um den Kiosk-Modus zu beenden.
Erstellen Sie eine Whitelist der Apps, die den Benutzern im Kiosk-Modus zur Verfügung stehen, indem Sie Apps zur Liste der zulässigen Apps hinzufügen. Ordnen Sie die Apps per Drag-and-Drop in der Reihenfolge an, in der sie im Launcher für den Kiosk-Modus angezeigt werden sollen. Durch Hinzufügen einer Anwendung zur Liste zulässiger Apps wird die App nicht auf dem Gerät installiert. Achten Sie darauf, jede App an die entsprechenden Benutzer und Benutzergruppen im App-Katalog zu verteilen.	
Vorinstallierte Apps	Klicken Sie auf „+Hinzufügen“, um aufgelistete, native Apps in der für den Kiosk-Modus zugelassenen Gruppe einzuschließen. Wenn Sie Dialer oder Kamera in den Sperreinstellungen oben deaktiviert haben, können Sie diese nicht in der Liste der zulässigen Apps ergänzen.
App-Katalog	Klicken Sie auf „Hinzufügen+“, um aufgelistete Apps aus dem App-Katalog in der für den Kiosk-Modus zugelassenen App-Gruppe einzuschließen.
Sonstige Apps	Klicken Sie auf Hinzufügen+, um den **Paketnamen** einer App einzuschließen, die nicht im Google Play Store verfügbar ist.
Im Kiosk-Modus zulässige Apps	Klicken Sie auf X, um eine App aus der für den Kiosk-Modus zugelassenen App-Gruppe zu entfernen. Ändern Sie mit Drag&drop die Reihenfolge der Apps auf den Kiosk-Geräten.

Bei Samsung-Geräten mit Knox Standard 4.0 oder höher wird die Mehrbenutzerfunktion im Kiosk-Modus automatisch gesperrt.

Bei Nicht-Samsung-Geräten wird der Kiosk-Modus in Version Android 8.0 oder höher nicht unterstützt. Wir empfehlen, bei Android 8.0 oder höher zur Kiosk-Sperre die Sperrfunktionen für Android Enterprise zu verwenden.

Verwandte Themen:

- **Konfiguration des Kiosk-Modus für Android**
- **Erstellen einer Konfiguration**

10.10.4.30. Konfiguration des Kiosk-Modus für Android

Dieser Abschnitt enthält die folgenden Themen:

- Kiosk-Modus aus der Ferne starten
- Kiosk-Modus beenden

Lizenz: Silver

Im Kiosk-Modus für Android-Geräte können Sie die Verwendung eines Geräts auf spezifische Apps beschränken. Sie können mit dem Kiosk-Modus Geräte für Mitarbeiter konfigurieren, die nur arbeitsspezifische Apps enthalten.

Bei der Vorbereitung von Android-Geräten für den Kiosk-Modus oder von Geräteeigentümern mit Kiosk-Modus müssen Sie eine **Whitelist der Apps erstellen**, die Sie den Benutzern im Kiosk-Modus anbieten wollen. Bei Geräten mit der Funktion „Geräteeigentümer" können Sie die Apps bei der Konfiguration der App zur Liste der genehmigten Apps hinzufügen, indem Sie die Apps per Drag&Drop in der Reihenfolge in den Kiosk Mode Launcher ziehen, in der sie dort angezeigt werden sollen. Weitere Informationen finden Sie unter **Sperr- und Kioskkonfiguration**.

Voraussetzungen

Bevor Sie den Kiosk-Modus für Android-Geräte konfigurieren, müssen Sie folgende Aufgaben ausgeführt haben:

- Sie müssen die Go auf den Geräten installiert haben.
- Sie müssen den App-Katalog mit den Apps konfiguriert haben, die Sie für die Kiosk-Konfiguration brauchen.
- Sie müssen den App-Katalog auf die Geräte verteilt haben, die im Kiosk-Modus laufen sollen.

> SonimXP5S-Geräte unterstützen den Kiosk-Modus nicht.

- Sie müssen die Apps installiert haben, die Sie für Ihre Kiosk-Konfiguration brauchen.
- (Optional) Richten Sie **Android Kiosk Branding** ein.

> Der Kiosk-Modus wird auf Android 5.1 und 6.0 unterstützt. Anwendungen außerhalb von Samsung Knox müssen in den Geräteeigentümermodus gesetzt werden, um die Verwendung unerwünschter Anwendungen zu verhindern.

Wichtig: Bei manchen Geräten existieren Funktionen, die den Bildschirm überschreiben oder in anderer Weise den Kiosk-Modus verlassen können. Ein Beispiel für eine derartige Funktion ist die People Edge-Funktion des Samsung Galaxy S6 Edge. Wir empfehlen dem Administrator, solche Funktionen abzuschalten, bevor das Gerät bereitgestellt wird.

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie auf **Sperre & Kiosk: Android-Geräte Administrationsmodus**.
4. Vervollständigen Sie im Bildschirm **Einstellungen erstellen** mindestens den Abschnitt **Kioskmodus-Einstellungen**.
5. Wählen Sie in dem Bildschirm **Verteilung** die Gerätegruppen aus, die diese Konfiguration erhalten sollen.
6. Klicken Sie auf **Fertig**.

7. Bei Nicht-Samsung-Geräten führen Sie außerdem folgende Schritte aus:
    1. Gehen Sie zu **Geräte** > **Geräte**.
    2. Wählen Sie die Geräte aus, die Sie im Kiosk-Modus aktivieren wollen.
    3. Klicken Sie auf **Aktionen** und dann auf **Einchecken erzwingen**.
    4. Tippen Sie auf den Geräten auf die Schaltfläche **Kiosk-Modus**.
    5. Drücken Sie die Taste **Home** auf dem Gerät.
    6. Wenn ein Dialog **Startprogramm auswählen** erscheint, tippen Sie auf **Go Kiosk Launcher** und dann auf **Immer**. Dieser Schritt ist notwendig, damit immer das richtige Startprogramm verwendet wird. Anderenfalls würde der Benutzer aufgefordert, ein Startprogramm auszuwählen.

Kiosk-Modus aus der Ferne starten

Verfahren

1. Gehen Sie zu **Geräte > Geräte**.
2. Ergänzen Sie die Spalte Kiosk-Modus in der Anzeige.
3. Wählen Sie die Geräte aus, bei denen der Kiosk-Modus aktiviert werden soll, die aber zurzeit nicht im Kiosk-Modus arbeiten.
4. Klicken Sie auf **Aktionen > Kiosk-Modus aufrufen**.

Kiosk-Modus beenden

Sie können den Kiosk-Modus auf dem Gerät beenden, wenn Sie eine PIN in der Konfiguration festlegen.

Verfahren

1. Tippen Sie auf das Symbol **Einstellungen**.
2. Wählen Sie **Kiosk-Modus beenden**.
3. Tippen Sie auf das Feld **Kiosk PIN**, wenn Sie dazu aufgefordert werden.
4. Geben Sie die Kiosk-PIN ein.

Sie können den Kiosk-Modus für ein bestimmtes Gerät über das Portal beenden:

Verfahren

1. Gehen Sie zu **Geräte > Geräte**.
2. Zeigen Sie die Details für das Gerät an.
3. Klicken Sie auf **Aktionen > Kiosk-Modus beenden**.

Sie können den Kiosk-Modus auch wie folgt beenden:

- Löschen Sie die Konfiguration.
- Deaktivieren Sie die Konfiguration.
- Entfernen Sie die Gerätegruppe aus der Konfiguration.

10.10.4.31. Kiosk für unter Android freigegebenes Gerät konfigurieren

Für spezifische Arbeitsaufgaben können Unternehmen dedizierte Android-Geräte bereitstellen, die für eine spezifische Benutzerrolle angepasst sind. Je nach Benutzerprofil können verschiedene Apps und Konfigurationen auf dem Gerät angezeigt werden. Einem Benutzer, der Techniker ist, können beispielsweise spezifische Apps für seine Arbeitsaufgaben angezeigt werden, während ein Wartungstechniker Zugriff auf andere Apps hat.

Der freigegebene Kiosk-Modus unter Android dient als App-Filter für verschiedene Benutzergruppen, die Geräte gemeinsam verwenden. Ein Benutzer, der bei einem freigegebenen Gerät im Kiosk-Modus angemeldet ist, sieht nur die Apps, die seiner Rolle entsprechen. Einer der Hauptvorteile des Kiosk-Modus mit gemeinsam verwendeten Geräten ist, dass verschiedenen Benutzergruppen Zugriff auf verschiedene App-Gruppen auf dem gleichen Gerät eingeräumt werden kann. Wenn ein Benutzer sich im Kiosk-Modus von einem gemeinsam verwendeten Android-Gerät abmeldet, werden die Apps und Benutzerdaten einschließlich der bisherigen Nutzerdaten aus der Anzeige gelöscht, wenn sich der nächste Benutzer auf dem Gerät anmeldet (und die App zur Neuinstallation markiert ist). Der Kiosk-Modus auf freigegebenen Geräten steht nur in Bereitstellungen von Android Enterprise mit verwalteten Google Play-Konten zur Verfügung.

Der Kiosk-Modus mit freigegebenen Geräten erfordert zwei Arten von Benutzern, einen „Staging User“ und einen Benutzer für den Kiosk-Modus auf dem gemeinsam verwendeten Gerät sowie mindestens zwei Richtlinien für diese Benutzer. Der „Staging User“ veranlasst, dass der Anmeldebildschirm auf dem freigegebenen Gerät angezeigt wird. Der „Staging User“ ist ein spezifischer Administratortyp, der anderen Benutzern gestattet, sich auf dem aktuellen Kiosk-Gerät anzumelden. Nachdem sich der Benutzer auf dem freigegebenen Gerät im Kiosk-Modus erfolgreich angemeldet hat, wird die Staging-Richtlinie durch die Richtlinie für den Kiosk-Modus auf dem freigegebenen Gerät ersetzt. Der Kiosk-Benutzer hat Zugriff auf die auf dem Gerät installierten Apps entsprechend der zugewiesenen Richtlinie. Sie können zwar mehrere Richtlinien für den Kiosk-Modus auf freigegebenen Geräten erstellen, es ist auf dem Kiosk-Gerät jedoch immer nur eine Kiosk-Richtlinie aktiv. Wenn sich der Kiosk-Benutzer von dem freigegebenen Kiosk-Gerät abmeldet, konfiguriert sich das Gerät wieder für den „Staging User“ und damit für die Staging-Richtlinie.

Der „Staging User“ kann nur auf die Anmeldeseite zugreifen. Infolgedessen müssen Sie speziell für diesen Benutzer eine Staging-Richtlinie erstellen. Die Benutzer, die das freigegebene Gerät im Kiosk-Modus nutzen, können dagegen auf die App-Gruppen zugreifen, die in der jeweiligen Richtlinie definiert sind. (Sie müssen natürlich auch die erlaubten Apps auf den gemeinsam genutzten Geräten des Geräte-Kiosks installieren.) Die Richtlinie für den gemeinsam genutzten Geräte-Kiosk ermöglicht Ihnen das Erstellen eines Filters erlaubter Apps aus allen bereits früher installierten Apps. Sie können Apps nicht direkt in eine Kiosk-Richtlinie auf einem freigegebenen Android-Gerät hochladen. Oft wollen Sie eine Kiosk-Richtlinie für ein freigegebenes Gerät für einen bestimmten Benutzertyp im Kiosk-Modus auf dem freigegebenen Gerät reservieren oder für eine bestimmte Benutzergruppe, speziell für Ihr Unternehmen. Beispielsweise kann es in einem Unternehmen Mitarbeiter für die Tagesschicht und für die Nachtschicht geben, die verschiedene Aufgaben haben und Zugriff auf andere Apps benötigen. In diesem Fall müssen Sie eine Richtlinie für die Tagesschicht und eine für die Nachtschicht erstellen.

Weitere Informationen zur Aktivierung von gemeinsam genutzten Geräten im Kioskmodus finden Sie unter **Sperre & Kiosk: Android Enterprise**

10.10.4.32. Sperre & Kiosk: Android Enterprise

Sperre und Kiosk: Diese Android-Konfiguration deaktiviert bestimmte Funktionen auf Android Enterprise-Geräten und erstellt eine Whitelist der Apps, die den Benutzern im Kiosk-Modus zur Verfügung stehen.

Dieser Abschnitt enthält die folgenden Themen:

- Sperreinstellungen
- Arbeitsprofil
- Verwaltete betriebliche Geräte (Geräteeigentümer- und Kiosk-Modus-Einstellungen)
- Sperr-Einstellungen für verwaltetes Gerät mit Arbeitsprofil/firmeneigenes Gerät mit Arbeitsprofil

Sperreinstellungen

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Sperrart auswählen	Wählen Sie die Art der Sperreinstellungen aus, die Sie konfigurieren wollen: • Arbeitsprofil • Verwaltete betriebliche Geräte (Geräteeigentümer- und Kiosk-Modus-Einstellungen) • Sperr-Einstellungen für verwaltetes Gerät mit Arbeitsprofil/firmeneigenes Gerät mit Arbeitsprofil Die Sperr-Einstellungen für ein firmeneigenes Gerät mit Arbeitsprofil sind nur für Geräte mit Android 11+ verfügbar. Es ist nur eine Art pro Konfiguration zulässig. Die angezeigten Optionen hängen von dem ausgewählten Typ ab. Wenn ein betrieblich verwaltetes Gerät (Geräteeigentümer) und ein verwaltetes Gerät mit Arbeitsprofil in der Konfiguration für ein unternehmenseigenes Gerät auf dasselbe Gerät verteilt werden, hat das verwaltete Gerät mit Arbeitsprofil Vorrang.

Arbeitsprofil

Deaktiviert bestimmte Funktionen der Geräte mit Android Enterprise.

Einstellung	Aktion	Für die Geräte
Screenshots deaktivieren	Wählen Sie diese Option, um die integrierte Funktion des Geräts zum Erstellen von Screenshots zu deaktivieren.	• Android 5.0 +
Apps-Kontrolle verweigern	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer Anwendungen in den Einstellungen oder Startkonfigurationen modifiziert.	• Android 5.0 +
Konfigurations-Anmeldeinformationen verweigern	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer Anmeldeinformationen konfiguriert.	• Android 5.0 +
Profilübergreifendes Kopieren und Einfügen verweigern	Wählen Sie diese Option aus, um zu verhindern, dass Informationen zwischen Profilen kopiert und eingefügt werden.	• Android 5.0 +
Kontoänderungen verweigern	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer Konten hinzufügt oder entfernt.	• Android 5.0 +
Outgoing Beam verweigern	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer mit NFC App-Daten überträgt.	• Android 5.1 +
Standortfreigabe verweigern	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer den Gerätestandort für Apps freigibt.	• Android 5.0 +
Debugging-Funktionen nicht zulassen	Wählen Sie diese Option, um die Debugging-Funktionen auf den Geräten zu deaktivieren. Standardmäßig ist diese Option aktiviert.	• Android 5.0 +
Apps-Verifizierung sicherstellen	Wählen Sie diese Option, um Anwendungsverifizierungsfunktionen auf den Geräten zu erlauben. Standardmäßig ist diese Option aktiviert. Wenn diese Option deaktiviert ist, zeigt das Gerät wieder das Standardverhalten, das je nach Gerät abweichen kann.	• Android 5.0 +
Unbekannte Quellen auf Geräten deaktivieren.	Klicken Sie auf die Option, um zu verhindern, dass das Gerät Apps aus unbekannten Quellen installiert. Damit diese Einstellung auf dem Gerät wirksam wird, muss diese Funktion mit einem anstehenden Google Play Update aktiviert werden.	• Android 5.0 +
Eingabemethoden beschränken	Beschränken Sie mit der Option **Paketname** den Zugang auf Unternehmens-Apps auf Pakete in einer Whitelist. Auf den Geräten stehen sowohl die Eingabemethoden der Whitelist als auch die Standard-Eingabemethoden des Systems zur Verfügung. Der Benutzer kann zwischen den Standard-Eingabemethoden des Systems und den Eingabemethoden der Whitelist-Pakete wählen.	• Android 5.0 +

Einstellung	Aktion	Für die Geräte
	Für Android 10+ gilt die Whitelisting-Funktion nur für IME-Apps auf der Arbeitsprofilseite. Für ältere Android-Versionen ist Whitelisting für IME-Apps geräteweit anwendbar (sowohl im als auch außerhalb des Arbeitsprofils).	
Zugangsdienste beschränken	Beschränken Sie mit der Option **Paketname** den Zugang auf Unternehmens-Apps auf Pakete in einer Whitelist. Wenn in der Whitelist keine Programmpakete eingetragen sind, ist nur die Eingabe über die Systemtastatur zulässig.	• Android 5.0 +
Unbekannte Quellen im Arbeitsprofil deaktivieren	Wählen Sie diese Option, um den Download aus unbekannten Quellen innerhalb des Arbeitsprofils zu verbieten.	• Android 5.0 +
System-Apps aktivieren/deaktivieren	Wählen Sie diese Option, um die Systemanwendungen zu aktivieren bzw. zu deaktivieren, die bereitgestellt werden sollen, indem Sie zwei Listen mit Paketnamen über die Felder **System App-Paketname** zuordnen. Mit dieser Funktion können Sie den Zugriff auf Systemanwendungen verwalten, die nicht in Google Play veröffentlicht sind. Die Ergänzung einer App im App-Katalog sowie in der Liste der System-Apps wird nicht unterstützt.	• Android 5.0 +
Anrufer-ID deaktivieren	Legt fest, ob die Anrufer-ID-Informationen aus dem Arbeitsprofil bei eingehenden Anrufen auf dem Gerät angezeigt werden.	• Android 6.0+
Kontaktfreigabe über Bluetooth deaktivieren	Wählen Sie diese Option, um zu verhindern, dass das Gerät Kontakte über Bluetooth mit anderen Geräten teilt.	• Android 6.0+
Kontaktfreigabe über Suche deaktivieren	Wählen Sie diese Option, um zu verhindern, dass Benutzer nach Arbeitskontakten in der privaten Kurzwahlliste suchen.	• Android 7.0 +
Automatisches Ausfüllen nicht zulassen	Wählen Sie diese Option, um ein automatisches Ausfüllen zu verhindern	• Android 8.0 +
Benachrichtigungen über Arbeitsanwendungen im persönlichen Profil deaktivieren	Wählen Sie diese Option, um die Benachrichtigungen über Arbeitsprofile einzuschränken.	• Android 8.0 +
Drucken nicht zulassen	Aktivieren Sie diese Option, um den Druck aus allen Anwendungen einzuschränken.	• Android 9.0 +

Einstellung	Aktion	Für die Geräte
Freigabe im Profil verweigern	Aktivieren Sie diese Option, wenn Benutzer keine personenbezogenen Daten in einem Arbeitsprofil auf dem Gerät freigeben sollen.	• Android 9.0 +
Zugriff zu den Kalendern der Arbeitsprofile erlauben	Wählen Sie eine der folgenden Optionen, um alle Apps zuzulassen, oder eine Reihe von Apps auf der persönlichen Seite, die auf die im Arbeitsprofil vorhandenen Kalenderinformationen zugreifen dürfen: • **Alle Apps im persönlichen Profil** – erlaubt allen Apps den Zugriff auf die im Arbeitsprofil vorhandenen Kalenderinformationen. • **Nur die folgenden Apps im persönlichen Profil** – Geben Sie in das Textfeld unten die Bundle-IDs der Apps durch ein Komma getrennt ein. Nur diesen ausgewählten Apps auf der persönlichen Seite wird der Zugriff auf die im Arbeitsprofil vorhandenen Kalenderinformationen gestattet. Für die App auf der persönlichen Seite sollten spezifische APIs implementiert sein, um auf den gemeinsamen Kalender zuzugreifen.	• Android 10.0 +
Profilübergreifendes Whitelisting von Apps aktivieren	Aktivieren Sie das Kontrollkästchen, um Benutzern die gemeinsame Nutzung von Informationen aus bestimmten Apps aus dem Arbeitsprofil auf der privaten Seite des Geräts zu ermöglichen. Geben Sie in das Feld **Apps in der Whitelist** die Paket-IDs der Apps durch Kommata getrennt ein, die auf die Whitelist gesetzt werden sollen. Diese Option ist standardmäßig deaktiviert.	• Android 11.0+
5G Network Slicing aktivieren	Wählen Sie diese Option aus, um eine 5G Network Slicing-Option auf dem Arbeitsprofil firmeneigener Geräte bereitzustellen. Diese Option ist standardmäßig deaktiviert.	• Android 12.0 +
Teilen der WLAN-Konfiguration des Administrators nicht zulassen	Wählen Sie diese Option, um zu verhindern, dass Benutzer vom Administrator festgelegte WLAN-Konfigurationen teilen können.	• Android 13.0 +
AI Assist deaktivieren	Aktivieren Sie diese Option, um Benutzer von AI Assist-Funktionen auszuschließen. Diese Option ist standardmäßig deaktiviert.	• Android 15.0 +

Verwaltete betriebliche Geräte (Geräteeigentümer- und Kiosk-Modus-Einstellungen)

Deaktiviert bestimmte Funktionen auf verwalteten betrieblichen Geräten (Geräteeigentümer) für Android 5.0+.

Einstellung	Beschreibung
Wi-Fi deaktivieren	Wählen Sie diese Option, um den Zugriff auf drahtlose Netzwerke zu deaktivieren.
WLAN-Einstellungen deaktivieren	Wählen Sie die Option, um den Zugriff auf die Einstellungen für drahtlose Netzwerke zu deaktivieren.
Kamera deaktivieren	Wählen Sie diese Option, um den Zugriff auf die Kamera zu deaktivieren.
Bluetooth deaktivieren (Android 8.0+)	Wählen Sie diese Option, um Bluetooth-Funktionen zu deaktivieren. Seien Sie bei Anwendung dieser Option vorsichtig. Ivanti rät davon ab, Audio-Funktionen zu deaktivieren, da damit auch der Zugriff auf Bluetooth-Freisprecheinrichtungen deaktiviert wird. Gesetzliche Vorschriften zur Nutzung von Freisprechanlagen während des Fahrens sind immer weiter verbreitet.
Bluetooth-Einstellungen nicht zulassen (Android 8.0+)	Wählen Sie diese Option, um den Zugriff auf die Bluetooth-Einstellungen zu deaktivieren.
Screenshots deaktivieren	Wählen Sie diese Option, um die integrierte Funktion des Geräts zum Erstellen von Screenshots zu deaktivieren.
Zurücksetzen des Netzwerks deaktivieren	Wählen Sie diese Option, um das Zurücksetzen des Netzwerks zu verhindern. (Gilt für Android 7.0+-Geräte und wird im Modus "Arbeitsprofil auf unternehmenseigenem Gerät" nicht unterstützt.)
Hauptlautstärke stummschalten	Wählen Sie die Option, um die Hauptlautstärke stumm zu schalten.
Apps-Kontrolle verweigern	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer Anwendungen in den Einstellungen oder Startkonfigurationen modifiziert.
Anmeldeinformationen nicht zulassen	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer Anmeldeinformationen konfiguriert.
Notfallrundsendungen nicht zulassen	Klicken Sie auf die Option, um Notfall-Broadcasts zu verhindern.
Mobile Netzwerke nicht zulassen	Wählen Sie diese Option, um den Zugriff auf mobile Netzwerke zu deaktivieren. Diese Option kann nicht deaktiviert werden, wenn das WLAN deaktiviert ist.
Internetweiterleitung nicht zulassen	Wählen Sie diese Option zur Deaktivierung von Wi-Fi-Tethering, einer Funktion, die die Internetverbindung eines Gerät nutzt, um Internetzugang für ein anderes Gerät herzustellen.
VPN nicht zulassen	Wählen Sie diese Option aus, um die VPN-Verbindungen zu deaktivieren.
Reset auf Werkeinstellung nicht zulassen	Wählen Sie diese Option, um Benutzer daran zu hindern, das Gerät auf die Werkseinstellungen zurückzusetzen.
Zurücksetzen auf die Werkseinstellungen schützen	Wählen Sie diese Option, damit die Benutzer das Gerät nicht auf die Werkseinstellungen zurücksetzen können. Sie können auch eine Liste autorisierter Google-Konto-IDs (als Ganzzahl) angeben, mit denen das Gerät nach einem Reset auf die Werkeinstellungen bereitgestellt

Einstellung	Beschreibung
	werden kann, oder den Mauszeiger über dem Hilfesymbol bewegen, wenn Sie nicht wissen, wie Sie autorisierte Konto-IDs laden.
Kontoänderungen verweigern	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer Konten hinzufügt oder entfernt.
NFC nicht zulassen (abgehender Beam)	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer mit NFC App-Daten überträgt.
Abgehende Gespräche nicht zulassen	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer selbst anrufen kann.
Sicheren Neustart nicht zulassen (Android 6.0+)	Wählen Sie die Option, um zu verhindern, dass ein Benutzer ein Gerät im sicheren Startmodus neu startet.
Standortfreigabe verweigern	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer den Gerätestandort für Apps freigibt.
Debugging-Funktionen nicht zulassen	Wählen Sie diese Option, um die Debugging-Funktionen auf den Geräten zu deaktivieren. Standardmäßig ist diese Option aktiviert.
Apps-Verifizierung sicherstellen	Wählen Sie diese Option, um Anwendungsverifizierungsfunktionen auf den Geräten zu erlauben. Standardmäßig ist diese Option aktiviert. Wenn diese Option deaktiviert ist, zeigt das Gerät wieder das Standardverhalten, das je nach Gerät abweichen kann.
SMS nicht zulassen	Wählen Sie diese Option aus, wenn ein Benutzer keine SMS-Nachrichten senden oder empfangen darf.
Einschalten des Mikrofons nicht zulassen	Wählen Sie diese Option aus, wenn das Mikrofon des Geräts immer eingeschaltet bleiben soll.
Automatische Zeit nicht zulassen	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer die automatische Zeiteinstellung aktiviert.
Automatische Zeitzone nicht zulassen	Wählen Sie diese Option, damit die Gerätezeit bei Zeitzonenänderungen nicht automatisch angepasst wird.
Zeit mit dem Server synchronisieren (Android 9.0+)	Wählen Sie diese Option, damit die Geräte die Zeit mit den MI-Cloud-Servern erstmals bei der Registrierung und danach einmal alle 24 Stunden nach jeder Anmeldung synchronisieren können. Diese Option ist nur verfügbar, wenn die Option **Automatische Zeit deaktivieren** ausgewählt wurde.
Zeitzone einstellen (Android 9.0+)	Geben Sie die Zeichenfolge für die Zeitzone im Olson-Zeitzonen-ID-Format an (z. B. Pacific/Midway).
Daten-Roaming deaktivieren	Wählen Sie diese Option, um den Datenaustausch zu deaktivieren, während sich das Gerät im Roaming-Modus befindet.

Einstellung	Beschreibung
Automatische WLAN-Deaktivierung nicht zulassen	Wählen Sie diese Option aus, wenn das WLAN nicht deaktiviert werden soll, wenn das Gerät in den Sleep-Modus wechselt.
Eingabemethoden beschränken	Beschränken Sie mit der Option **Paketname** den Zugang auf Unternehmens-Apps auf Pakete in einer Whitelist. Auf den Geräten stehen sowohl die Eingabemethoden der Whitelist als auch die Standard-Eingabemethoden des Systems zur Verfügung. Der Benutzer kann zwischen den Standard-Eingabemethoden des Systems und den Eingabemethoden der Whitelist-Pakete wählen. Für Android 10+ ist die Whitelisting-Funktion nur für IME-Apps auf der Geräteseite anwendbar. Bei älteren Android-Versionen gilt die Whitelisting-Funktion für IME-Apps geräteweit.
Zugangsdienste beschränken	Beschränken Sie mit der Option **Paketname** den Zugang auf Unternehmens-Apps auf Pakete in einer Whitelist. Wenn in der Whitelist keine Programmpakete eingetragen sind, ist nur die Eingabe über die Systemtastatur zulässig.
USB-Dateitransfer deaktivieren	Klicken Sie auf die Option, um den USB-Dateitransfer deaktivieren.
Externe Medien deaktivieren	Klicken Sie auf die Option, um externe Medien deaktivieren.
Keyguard deaktivieren (ohne Wirkung, wenn PIN/Passcode eingestellt ist)	Wählen Sie diese Option, um die Tastensperre zu deaktivieren. Diese Option hat keine Auswirkungen, wenn ein Passwort, eine PIN oder ein Muster festgelegt ist. Wenn ein Passwort, eine PIN oder ein Muster nach Deaktivierung der Tastensperre gesetzt wird, wird die Tastensperre nicht mehr deaktiviert.
Der Bildschirm bleibt eingeschaltet, wenn er an die Stromversorgung angeschlossen ist.	Wählen Sie diese Option, wenn der Bildschirm eingeschaltet bleiben soll, wenn er an die Stromversorgung angeschlossen ist. Der Bildschirm wird möglicherweise abgedunkelt, schaltet sich jedoch nicht aus, wenn das Gerät an eine Stromquelle angeschlossen ist. Diese Einstellung wird nur dann wirksam, wenn die automatische Sperrung oder die Inaktivitätszeitüberschreitung in der Passcode-Konfiguration nicht zur Definition einer Zeitüberschreitung verwendet wird.
Erstellung von Fenstern nicht zulassen	Wählen Sie diese Option, um zu verhindern, dass Apps bestimmte Fenster einblenden, z. B. Warnmeldungen und Toasts.
Hinweise für neue Anwender überspringen	Wählen Sie diese Option, um die Systemempfehlung für Apps zu aktivieren und das Benutzer-Lernprogramm und andere einleitende Hinweise beim ersten Start zu überspringen.
Unbekannte Quellen auf Geräten deaktivieren.	Wählen Sie diese Option, um die Installation von Anwendungen aus unbekannten Quellen zu verbieten.
Meldung für Sperrbildschirm einstellen (Android 7.0+)	Wählen Sie diese Option, um festzulegen, welche Meldung auf dem Sperrbildschirm des Geräts angezeigt werden soll. Geben Sie die Meldung für die Displaysperre (maximal 256 Zeichen) in das Textfeld ein. Bei Aktivierung dieser Option kann der Benutzer die Meldung in den Einstellungen nicht ändern, und die vom Admin eingestellte Meldung wird dem Benutzer angezeigt.

Einstellung	Beschreibung
	Wenn der Admin nach der Aktivierung von 'Setze Sperrbildschirmmeldung' keine Sperrmeldung zur Verfügung stellt, wird dem Benutzer die Einstellung der Meldung in den Einstellungen verwehrt, aber es wird keine Meldung an den Benutzer angezeigt.
Bildschirmhelligkeit festlegen	Mit dieser Option legen Sie die Bildschirmhelligkeit auf Ihrem Gerät fest. • Manuell – Wählen Sie diese Option aus, um manuell eine Zahl einzugeben (von 0 bis 255). • Adaptiv – Wählen Sie diese Option aus, um dem Gerät das Festlegen der Helligkeit zu erlauben. Es wird empfohlen, vor dem Einstellen der Bildschirmhelligkeit die Option "Konfigurieren der Helligkeit nicht zulassen" zu aktivieren.
Zeitüberschreitung für Bildschirm festlegen	Mit dieser Option legen Sie die Dauer des Bildschirm-Timeouts (in Sekunden) fest. Es wird empfohlen, vor dem Einstellen des Bildschirm-Timeouts die Option "Konfigurieren der Zeitüberschreitung für Bildschirm nicht zulassen" zu aktivieren.
Bildschirmausrichtung festlegen	Mit dieser Option legen Sie die Bildschirmausrichtung fest. Über die Dropdownliste lässt sich die Ausrichtung auf 0, 90, 180 oder 270 Grad festlegen. Diese Option ist standardmäßig nicht aktiviert. Für die Go-App ab Version 89 müssen Sie diese Option aktivieren und den Wert auf 0 setzen, damit das Gerät in Kiosk im Portraitmodus bleibt.
System-Apps aktivieren/deaktivieren	Wählen Sie diese Option, um die Systemanwendungen zu aktivieren bzw. zu deaktivieren, die bereitgestellt werden sollen, indem Sie zwei Listen mit Paketnamen über die Felder **System App-Paketname** zuordnen. Mit dieser Funktion können Sie den Zugriff auf Systemanwendungen verwalten, die nicht in Google Play veröffentlicht sind. Das Hinzufügen einer App zum App-Katalog sowie zu einer Liste mit System-Apps wird nicht unterstützt.
Android 8.0 +	
Automatisches Ausfüllen nicht zulassen	Aktivieren Sie dieses Kontrollkästchen, um dem Benutzer die Verwendung von Auto-Fill-Diensten zu verbieten.
Bluetooth-Freigabe nicht zulassen	Aktivieren Sie dieses Kontrollkästchen, wenn der Benutzer ausgehendes Bluetooth auf dem Gerät nicht teilen soll.
Sicherungsdienst deaktivieren	Wählen Sie diese Option, um den Backup-Dienst zu deaktivieren.
Android 9.0 +	
Drucken nicht zulassen	Markieren Sie dieses Kontrollkästchen, wenn der Benutzer nicht drucken darf.
Flugzeugmodus nicht zulassen	Aktivieren Sie diese Option, um den Flugzeugmodus auf dem gesamten Gerät zu deaktivieren.

Einstellung	Beschreibung
Umgebungsanzeige nicht zulassen	Aktivieren Sie diese Option, um die Umgebungsanzeige für den Benutzer zu deaktivieren.
Konfigurationshelligkeit nicht zulassen	Aktivieren Sie diese Option, um dem Benutzer die Konfiguration der Helligkeit zu deaktivieren. Es wird empfohlen, vor dem Auswählen dieser Option den Modus "Bildschirmhelligkeit festlegen" zu definieren.
Datum und Uhrzeit der Konfiguration nicht zulassen	Aktivieren Sie diese Option, um die Konfiguration von Datum, Uhrzeit und Zeitzone zu deaktivieren.
Konfigurationsspeicherort nicht zulassen	Aktivieren Sie dieses Kontrollkästchen, um dem Benutzer zu verbieten, Standortbetreiber zu deaktivieren.
Zeitlimit für Konfigurationsbildschirm nicht zulassen	Aktivieren Sie dieses Kontrollkästchen, um dem Benutzer zu verbieten, die Zeitüberschreitung für die Bildschirmabschaltung zu ändern. Es wird empfohlen, vor dem Auswählen dieser Option den Wert "Zeitüberschreitung für Bildschirm festlegen" zu definieren.
Android 12.0+ USB nur zum Laden aktivieren **Android 13.0+** Mindestens erforderliche WLAN-Sicherheit festlegen Teilen der WLAN-Konfiguration des Administrators nicht zulassen **Android 15.0+**	 Wählen Sie diese Option aus, um den USB-Port nur zum Laden zu aktivieren. Mit dieser Option legen Sie die mindestens erforderliche WLAN-Sicherheit fest: • Keine Mindestsicherheit erforderlich – Wählen Sie diese Option aus, wenn keine Mindestsicherheit erforderlich ist. • Sicherheit auf Basis eines persönlichen Netzwerks – Wählen Sie diese Option aus, um persönliche WLAN-Netzwerke zu blockieren, wie WEP, WPA/WPA2/WPA3 usw. • Sicherheit auf Basis eines EAP-Enterprise-Netzwerks – Wählen Sie diese Option aus, um WLAN-Netzwerke auf Basis des EAP-Protokolls zu blockieren. • Sicherheit auf Basis eines 192-Enterprise-Netzwerks – Wählen Sie diese Option aus, um WLAN-Netzwerke auf EAP-Unternehmensbasis zu blockieren. Alle vorhandenen Geräte, die die Mindestkriterien nicht erfüllen, werden getrennt. Bei den Gerätedetails wird die mindestens erforderliche WLAN-Sicherheitsstufe (falls definiert) unter **Allgemein > WLAN-Sicherheitsstufe** angezeigt. Wählen Sie diese Option, um auszuschließen, dass Benutzer die vom Administrator festgelegten WLAN-Konfigurationen teilen können.
AI Assist deaktivieren	Aktivieren Sie diese Option, um Benutzer von AI Assist-Funktionen auszuschließen. Diese Option ist standardmäßig deaktiviert.

Einstellung	Beschreibung
Kiosk-Moduseinstellungen: Im Kiosk-Modus gelten für das Geräte zusätzliche Einschränkungen wie etwa der beschränkte Zugriff auf Apps über einen benutzerdefinierten Launcher.	
Kiosk-Modus aktivieren	Wählen Sie diese Option, um den **Kiosk-Modus** auf Android-Geräten zu konfigurieren. • Wenn ein Benutzer sich im Kiosk-Modus anmeldet und dann wieder abmeldet, bleibt der Benutzername im Go-Client für künftige Anmeldungen verfügbar. Im freigegebenen Kiosk-Modus speichert der Go-Client die sieben zuletzt verwendeten Benutzernamen. • Der freigegebene Kiosk-Modus unterstützt nun die IDP-Authentifizierung. Wenn die Cloud mit IDP konfiguriert wird, kann der freigegebene Shared-Modus also mit der IDP-Authentifizierung genutzt werden.
Aufgaben-Sperr-Modus aktivieren	Wählen Sie diese Option, um den Aufgabensperrmodus auf Android-Geräten zu aktivieren. Bei Aktivierung zeigen die Geräte Keyguard, Statusleiste und Safemode an. Diese Option ist standardmäßig ausgewählt. Im Folgenden finden Sie die zusätzlichen Einstellungen, die angezeigt werden, wenn der Task-Sperrmodus für Android 9 oder unterstützte neuere Versionen aktiviert ist: Symbol „Einstellungen"– Ermöglicht Apps den Zugriff auf Systemfunktionen, die von den Geräteeinstellungen abhängig sind. Wenn die Geräteeinstellungen aktiviert werden, lassen sich Verstöße gegen den Aufgabensperrmodus in verschiedenen Szenarien vermeiden, z. B. bei der Bluetooth-Kopplung über eine App. Es wird empfohlen, diese Einstellung für bestimmte Apps aktiviert zu lassen. **Systeminfo** – Zeigt Datum/Uhrzeit, Konnektivität, Akkustatus und Vibrationsmodus in der Statusleiste an. Diese Option ist standardmäßig ausgewählt. **Keyguard** (standardmäßig aktiviert) – Aktiviert den Keyguard während des Aufgabensperrmodus. **Globale Aktionen** (standardmäßig aktiviert) - Aktiviert das Menü, das angezeigt wird, wenn der Benutzer lange den Ein/Aus-Schalter drückt. Wenn diese Option deaktiviert ist, kann der Benutzer das Gerät möglicherweise nicht ausschalten. **Home-Button** - Aktiviert den Home-Button. Diese Option ist standardmäßig deaktiviert. Bei Aktivierung werden folgende Unteroptionen angezeigt: • **Übersichtsschaltfläche** (standardmäßig deaktiviert) – Aktiviert die Übersichtsschaltfläche und den Übersichtsbildschirm im Aufgabensperrmodus. • **Benachrichtigungen** (standardmäßig deaktiviert) - Erlaubt Benachrichtigungen im Aufgabensperrmodus. Dazu gehören Benachrichtigungssymbole in der Statusleiste, eingeblendete Benachrichtigungen und die erweiterbare Benachrichtigungs-Schattierung. Wenn die Option „Home-Button" nicht aktiviert ist, kann der Benutzer die Mehrfensterfunktion nicht nutzen.

Einstellung	Beschreibung
Kiosk-Modus automatisch aufrufen (nur bei der Erstkonfiguration)	Wählen Sie diese Option, um den Kiosk-Modus automatisch zuzulassen, wenn die Konfiguration angewendet wird.
Kioskmodus nach Richtlinienaktualisierungen beibehalten	Wählen Sie diese Option aus, um das Gerät automatisch in den Kioskmodus zurückzusetzen, nachdem eine Sperrrichtlinie aktualisiert wurde. Diese Einstellung sorgt für einen ununterbrochenen Kioskbetrieb und reduziert die Notwendigkeit manueller Eingriffe im Anschluss an Richtlinienänderungen. Zuvor konnte das Aktualisieren einer Sperrrichtlinie dazu führen, dass das Gerät den Kiosk-Modus beendet. Wenn aktiviert, wechselt das Gerät automatisch zurück in den Kiosk-Modus, nachdem die Aktualisierung der Richtlinie verarbeitet wurde.
Schnelleinstellungen für Geräte mit Android 5 deaktivieren	Wählen Sie diese Option, um die Schnelleinstellungen im Kiosk-Modus für Geräte zu deaktivieren, die unter Android 5 laufen.
Schnelleinstellungen für Geräte mit Android 6+ und alle Samsung-Geräte deaktivieren	Wählen Sie diese Option, um die Schnelleinstellungen im Kioskmodus für Geräte mit Android Enterprise ab Version 6 bis zur letzten freigegebenen Version und alle Samsung-Geräte zu deaktivieren. Eine Deaktivierung dieser Einstellung blockiert keine Benachrichtigungssymbole und -Töne auf dem Gerät.
Benutzerzugriff auf Wi-Fi-Einstellungen zulassen	Wählen Sie diese Option aus, damit ein Benutzer die WLAN-Einstellungen ändern und auf bevorzugte drahtlose Netze zugreifen kann.
Benutzerzugang für Bluetooth-Einstellungen zulassen	Wählen Sie diese Option aus, damit ein Benutzer die Bluetooth-Einstellungen ändern und weitere Bluetooth-Geräte koppeln kann.
Benutzerzugang für Standort-Einstellungen zulassen	Wählen Sie diese Option aus, damit ein Benutzerzugriff auf die Standorteinstellungen möglich ist.
Verzögerung der Anwendungs-Updates durch Benutzer zulassen	Wählen Sie diese Option aus, damit ein Benutzer Anwendungsupdates verzögern kann.
Benutzer darf auf Zugriffsdatums- und -zeiteinstellungen zugreifen.	Klicken Sie auf die Option, wenn ein Benutzer auf die Datums- und Zeiteinstellungen zugreifen darf.
Benutzer darf auf mobile Netzwerkeinstellungen zugreifen.	Klicken Sie auf die Option, wenn ein Benutzer auf die mobilen Netzwerkeinstellungen zugreifen darf.
Sprachauswahl dem Benutzer überlassen	Wählen Sie diese Option, damit der Benutzer auf die Spracheinstellungen zugreifen kann.
Freigegebenes Gerät aktivieren	Im Kiosk-Modus mit freigegebenem Gerät wird das Gerät von mehreren Endbenutzern geteilt. Diese Option ermöglicht es, ein Gerät zu teilen, während das Gerät im Kiosk-Modus betrieben wird: • **Anmelden erlauben**: Diese Option ist für einen Kiosk-Administrator vorgesehen. Wenn ein Gerät mit dieser Option konfiguriert ist, wird der Bildschirm für die Benutzeranmeldung angezeigt, damit sich ein Endbenutzer am gemeinsam genutzten Kiosk-Gerät anmelden kann.

Einstellung	Beschreibung
	Die Option „Anmeldung aktivieren“ ist nur dann sichtbar, wenn der Benutzer als Benutzer eines Android Enterprise-Gerätekontos (Staging-Benutzer) eingerichtet wurde. Wählen Sie Domain-Ersatz verwenden und geben Sie die Domain entsprechend ein. Diese Option prüft den Benutzernamen auf den Domainsuffix. Wenn das Domainsuffix fehlt, hängt das System automatisch das obige Domainsuffix an den Benutzernamen an. • **Abmelden zulassen**: Wenn ein Gerät mit dieser Option konfiguriert ist, hat der angemeldete Endbenutzer Zugriff auf die Apps in der Whitelist. Dieser Benutzer sieht die Option zur Abmeldung, kann den Kiosk jedoch nicht verlassen. Wenn ein Benutzer sich auf dem freigegebenen Gerät im Kiosk-Modus abmeldet, kann sich ein anderer Benutzer im Kiosk-Modus auf dem freigegebenen Gerät anmelden und die vom Administrator konfigurierten Apps sehen. • Die Apps werden mit einem Recyclingsymbol angezeigt, um eine Neuinstallation einer App bei jeder Neuanmeldung zu erzwingen. Diese Option kann für Apps verwendet werden, die lokale Cache-Daten verwenden. Der Benutzer kann den Kioskmodus verlassen, wenn der Administrator die Kiosk-PIN angibt. • **Zeitüberlauf**: Definiert den Zeitüberlauf in Stunden. Wenn der Zeitüberlauf beispielsweise auf zwei Stunden konfiguriert ist und der Endbenutzer sich im Kiosk-Modus nicht von dem freigegebenen Gerät abmeldet, erfolgt die Abmeldung auf dem Gerät automatisch nach Ablauf der beiden Stunden. Das **Timeout**-Feld wird nur angezeigt, wenn die Option **Abmeldung aktivieren** ausgewählt ist, und es ist optional. Sie können Endbenutzer auch aus dem gemeinsamen Kiosk-Modus abmelden, indem Sie auf die Option **Bei Android Enterprise Kiosk abmelden** auf der Seite mit den Gerätedetails klicken.
FIDO-Authentifizierung zulassen (erfordert Google Chrome-App auf dem Gerät)	Wählen Sie diese Option aus, um die FIDO-Authentifizierung für Benutzer bei Verwendung des gemeinsam genutzten Kiosks zu aktivieren. Erlauben Sie Benutzern die Verwendung von FIDO-Schlüsseln für die Anmeldung am Gerät. Google Chrome ist der einzige unterstützte Browser und muss auf dem Gerät vorhanden sein, damit die FIDO-Authentifizierung im gemeinsam genutzten Kiosk verfügbar ist.
Dem Benutzer erlauben, die Helligkeit zu konfigurieren und die Anzeige automatisch zu drehen	Wählen Sie diese Option, damit der Benutzer die Helligkeit und die automatische Drehung konfigurieren kann.
Mehrere Fenster aktivieren	Wählen Sie diese Option, um die gleichzeitige Anzeige von mehr als einer Anwendung bei Samsung-Geräten zu ermöglichen (Kiosk für Gerätebesitzer). Um im Aufgabensperrmodus mehrere Fenster anzuzeigen, sollten auch folgende Optionen für den Aufgabensperrmodus aktiviert werden: • **Schaltfläche Home**

Einstellung	Beschreibung
	• **Schaltfläche Übersicht**
Inaktivitätsschutz aktivieren	Wählen Sie diese Option aus, um den Inaktivitätsschutz im Kiosk-Modus zu aktivieren. Wenn aktiviert, bleibt der Kiosk-Bildschirm standardmäßig 30 Sekunden lang aktiv. Sie können einen beliebigen Wert zwischen 30 und 3600 festlegen.
Kiosk-Branding	Wählen Sie die Standard- oder benutzerdefinierten Branding-Optionen aus der Dropdown-Liste aus.
PIN zum Beenden des Kiosk-Modus	Geben Sie die sechsstellige PIN ein, die der Benutzer eingeben muss, um den Kiosk-Modus zu beenden. Die PIN muss mindestens 6 Ziffern und maximal 10 Ziffern enthalten. Diese PIN gilt für alle Geräte im Kiosk-Modus. Bislang war die Kiosk-PIN nur vierstellig. Der Benutzer kann die vierstellige PIN auch dann weiterbenutzen, wenn ein Upgrade von einer früheren Version auf Cloud 82 vorgenommen wurde. Wenn Änderungen an der Konfiguration anfallen, gelten jedoch die neuen Anforderungen für die PIN-Länge (also mindestens 6 Stellen und maximal 10 Stellen). Die Go-App schützt das Gerät vor Brute-Force-Angriffen. Weitere Informationen finden Sie in der Dokumentation zu Go for Android.
Einzel-App Launcher Kiosk aktivieren	Wählen Sie diese Option aus, um den Kiosk-Modus zu verwenden und eine App auf GMS- und Nicht-GMS-Geräten im Vordergrund zu behalten. Sie müssen eine App aus dem App-Katalog auswählen oder eine Paket-ID eingeben.
Benutzerzugriff auf Ivanti Agent-Einstellungen zulassen	Wählen Sie diese Option, um auf die **Ivanti Agent-Einstellungen** zuzugreifen, während sich das Gerät im **Einzel-App-Kiosk-Modus befindet**. Bisher musste der Administrator den Kiosk-Modus verlassen, um auf Agenteneinstellungen zuzugreifen. Nachdem die Einstellung aktiviert und an Geräte verteilt wurde, können Benutzer die Seite mit den Ivanti Agent-Einstellungen öffnen, indem sie die Tasten für laut und leise gleichzeitig gedrückt halten. Die Funktion wird nur auf Android-Geräten unterstützt, die im Modus für unternehmensseitig verwaltete Geräte registriert sind.
Fahrersicherheit aktivieren	Wählen Sie diese Option, um das Symbol für Fahrersicherheit alle Apps im Abschnitt "Im Kiosk-Modus zulässige Apps" zu aktivieren. Klicken Sie auf das Symbol für Fahrersicherheit, um die App bei Überschreitung der Geschwindigkeitsbegrenzung zu deaktivieren.
Erstellen Sie eine Whitelist der Apps, die den Benutzern im Kiosk-Modus zur Verfügung stehen, indem Sie Apps zur Liste der zulässigen Apps hinzufügen. Ordnen Sie die Apps per Drag-and-Drop in der Reihenfolge an, in der sie im Launcher für den Kiosk-Modus angezeigt werden sollen. Durch Hinzufügen einer Anwendung zur	

Einstellung	Beschreibung
Liste zulässiger Apps wird die App nicht auf dem Gerät installiert. Achten Sie darauf, jede App an die entsprechenden Benutzer und Benutzergruppen im App-Katalog zu verteilen.	
Vorinstallierte Apps	Klicken Sie auf „+Hinzufügen“, um aufgelistete, native Apps in der für den Kiosk-Modus zugelassenen Gruppe einzuschließen. In den Einstellungen für die im Kioskmodus zugelassenen Apps stehen folgende Optionen zur Verfügung: • **App-Benutzerdaten löschen**: Wenn Sie diese Option aktivieren, werden alle Anwendungsdaten automatisch und ohne Aufforderung gelöscht, wenn sich der Benutzer vom Kiosk abmeldet. Wählen Sie in den Einstellungen für den Kioskmodus Gemeinsam genutztes Gerät aktivieren, damit diese Option mit den Anwendungen verfügbar ist. ◦ App-Daten werden für Google Chrome und das Webview-Paket auch dann nicht gelöscht, wenn sie in der App-Whitelist mit aktivierter Benutzerdatenlöschung hinzugefügt wurden. Dies liegt daran, dass das Kiosk-Gerät abstürzen könnte, wenn die App-Daten für diese 2 Pakete gelöscht werden. ◦ App-Daten werden für System-Apps, für die kein App-Launcher verfügbar ist, nicht gelöscht (sowohl innerhalb als auch außerhalb des Kiosks). • **Verbergen**: Wenn Sie diese Option aktivieren, kann die Anwendung zwar von anderen Apps aufgerufen werden, ist aber im Kiosk-Startprogramm nicht sichtbar. Wenn Sie Dialer oder Kamera in den Sperreinstellungen oben deaktiviert haben, können Sie diese nicht in der Liste der zulässigen Apps ergänzen.
App-Katalog Sonstige Apps	Klicken Sie auf „Hinzufügen+“, um aufgelistete Apps aus dem App-Katalog in der für den Kiosk-Modus zugelassenen App-Gruppe einzuschließen. Klicken Sie auf Hinzufügen+, um den **Paketnamen** einer App einzuschließen, die nicht im Google Play Store verfügbar ist. Bei Samsung-Geräten sollten die Administratoren die folgenden Dialer-/Systempakete in die Whitelist aufnehmen, damit sie im Kioskmodus funktionsfähig sind und die Dialer-Funktionalität im Kioskmodus aktiviert werden kann. • Telefonat - com.samsung.android.incallui • Telefon - com.samsung.android.dialer (sollte auf der Whitelist stehen; der Administrator sollte die Option „Verstecken“ für dieses Paket wählen, um Probleme mit zwei Dialer-Optionen für den Benutzer zu vermeiden). • Telefonat - com.sec.phone • Telefonateinstellung - com.samsung.android.app.telephonyui • Unterstützte Anwahl - com.sec.providers.assisteddialing

Einstellung	Beschreibung
	• Telefonatprotokoll sichern/wiederherstellen - com.android.calllogbackup • Dialer-Speicherung - com.android.providers.telephony • Telefon - com.android.server.telecom • Telefon - com.android.phone • Smart Call - com.samsung.android.smartcallprovider • WLAN-Telefonie - com.sec.unifiedwfc
Im Kiosk-Modus zulässige Apps **Erstellen Sie eine Whitelist der Apps,** die den Benutzern im Kiosk-Modus zur Verfügung stehen, indem Sie Apps zur Liste der zulässigen Apps hinzufügen. Ordnen Sie die Apps per Drag-and-Drop in der Reihenfolge an, in der sie im Launcher für den Kiosk-Modus angezeigt werden sollen. Durch Hinzufügen einer Anwendung zur Liste zulässiger Apps wird die App nicht auf dem Gerät installiert. Achten Sie darauf, jede App an die entsprechenden Benutzer und Benutzergruppen im App-Katalog zu verteilen.	Klicken Sie auf „X“, um eine App aus der für den Kiosk-Modus zugelassenen App-Gruppe zu entfernen. Ändern Sie mit Drag&drop die Reihenfolge der Apps auf den Kiosk-Geräten. **Ordner hinzufügen** – Mithilfe dieser Option können Sie einen Ordner in diesem Abschnitt erstellen und eine oder mehrere Apps in diesen Ordner verschieben. Sie können bis zu zwei Ordnerebenen erstellen. Die in einen Ordner kopierten Apps können nicht in einen anderen Ordner kopiert werden. In einem Ordner werden maximal 25 Apps unterstützt.
Vorinstallierte Apps	Klicken Sie auf „+Hinzufügen“, um aufgelistete, native Apps in der für den Kiosk-Modus zugelassenen Gruppe einzuschließen. In den Einstellungen für die im Kioskmodus zugelassenen Apps stehen folgende Optionen zur Verfügung: • **App-Benutzerdaten löschen**: Wenn Sie diese Option aktivieren, werden alle Anwendungsdaten automatisch und ohne Aufforderung gelöscht, wenn sich der Benutzer vom Kiosk abmeldet. Wählen Sie in den Einstellungen für den Kioskmodus Gemeinsam genutztes Gerät aktivieren, damit diese Option mit den Anwendungen verfügbar ist. ◦ App-Daten werden für Google Chrome und das Webview-Paket auch dann nicht gelöscht, wenn sie in der App-Whitelist mit aktivierter Benutzerdatenlöschung hinzugefügt wurden. Dies liegt daran, dass das

Einstellung	Beschreibung
	Kiosk-Gerät abstürzen könnte, wenn die App-Daten für diese 2 Pakete gelöscht werden. ◦ App-Daten werden für System-Apps, für die kein App-Launcher verfügbar ist, nicht gelöscht (sowohl innerhalb als auch außerhalb des Kiosks). • **Verbergen**: Wenn Sie diese Option aktivieren, kann die Anwendung zwar von anderen Apps aufgerufen werden, ist aber im Kiosk-Startprogramm nicht sichtbar. Wenn Sie Dialer oder Kamera in den Sperreinstellungen oben deaktiviert haben, können Sie diese nicht in der Liste der zulässigen Apps ergänzen.
App-Katalog Sonstige Apps	Klicken Sie auf „Hinzufügen+“, um aufgelistete Apps aus dem App-Katalog in der für den Kiosk-Modus zugelassenen App-Gruppe einzuschließen. Klicken Sie auf Hinzufügen+, um den **Paketnamen** einer App einzuschließen, die nicht im Google Play Store verfügbar ist. Bei Samsung-Geräten sollten die Administratoren die folgenden Dialer-/Systempakete in die Whitelist aufnehmen, damit sie im Kioskmodus funktionsfähig sind und die Dialer-Funktionalität im Kioskmodus aktiviert werden kann. • Telefonat - com.samsung.android.incallui • Telefon - com.samsung.android.dialer (sollte auf der Whitelist stehen; der Administrator sollte die Option „Verstecken“ für dieses Paket wählen, um Probleme mit zwei Dialer-Optionen für den Benutzer zu vermeiden). • Telefonat - com.sec.phone • Telefonateinstellung - com.samsung.android.app.telephonyui • Unterstützte Anwahl - com.sec.providers.assisteddialing • Telefonatprotokoll sichern/wiederherstellen - com.android.calllogbackup • Dialer-Speicherung - com.android.providers.telephony • Telefon - com.android.server.telecom • Telefon - com.android.phone • Smart Call - com.samsung.android.smartcallprovider • WLAN-Telefonie - com.sec.unifiedwfc
Im Kiosk-Modus zulässige Apps	Klicken Sie auf „X“, um eine App aus der für den Kiosk-Modus zugelassenen App-Gruppe zu entfernen. Ändern Sie mit Drag&drop die Reihenfolge der Apps auf den Kiosk-Geräten. **Ordner hinzufügen** – Mithilfe dieser Option können Sie einen Ordner in diesem Abschnitt erstellen und eine oder mehrere Apps in diesen Ordner verschieben. Sie können bis zu zwei Ordnerebenen erstellen. Die in einen Ordner kopierten Apps können nicht in einen anderen Ordner kopiert werden. In einem Ordner werden maximal 25 Apps unterstützt.

Einstellung	Beschreibung
Einzel-App Launcher Kiosk aktivieren	Wählen Sie diese Option aus, um den Kiosk-Modus zu verwenden und eine App auf GMS- und Nicht-GMS-Geräten im Vordergrund zu behalten. Sie müssen eine App aus dem App-Katalog auswählen oder eine Paket-ID eingeben.
Erstellen Sie eine Whitelist der Apps, die den Benutzern im Kiosk-Modus zur Verfügung stehen, indem Sie Apps zur Liste der zulässigen Apps hinzufügen. Ordnen Sie die Apps per Drag-and-Drop in der Reihenfolge an, in der sie im Launcher für den Kiosk-Modus angezeigt werden sollen. Durch Hinzufügen einer Anwendung zur Liste zulässiger Apps wird die App nicht auf dem Gerät installiert. Achten Sie darauf, jede App an die entsprechenden Benutzer und Benutzergruppen im App-Katalog zu verteilen.	
Vorinstallierte Apps	Klicken Sie auf „+Hinzufügen“, um aufgelistete, native Apps in der für den Kiosk-Modus zugelassenen Gruppe einzuschließen. In den Einstellungen für die im Kioskmodus zugelassenen Apps stehen folgende Optionen zur Verfügung: • **App-Benutzerdaten löschen**: Wenn Sie diese Option aktivieren, werden alle Anwendungsdaten automatisch und ohne Aufforderung gelöscht, wenn sich der Benutzer vom Kiosk abmeldet. Wählen Sie in den Einstellungen für den Kioskmodus Gemeinsam genutztes Gerät aktivieren, damit diese Option mit den Anwendungen verfügbar ist. ◦ App-Daten werden für Google Chrome und das Webview-Paket auch dann nicht gelöscht, wenn sie in der App-Whitelist mit aktivierter Benutzerdatenlöschung hinzugefügt wurden. Dies liegt daran, dass das Kiosk-Gerät abstürzen könnte, wenn die App-Daten für diese 2 Pakete gelöscht werden. ◦ App-Daten werden für System-Apps, für die kein App-Launcher verfügbar ist, nicht gelöscht (sowohl innerhalb als auch außerhalb des Kiosks). • **Verbergen**: Wenn Sie diese Option aktivieren, kann die Anwendung zwar von anderen Apps aufgerufen werden, ist aber im Kiosk-Startprogramm nicht sichtbar. Wenn Sie Dialer oder Kamera in den Sperreinstellungen oben deaktiviert haben, können Sie diese nicht in der Liste der zulässigen Apps ergänzen.
App-Katalog	Klicken Sie auf „Hinzufügen+“, um aufgelistete Apps aus dem App-Katalog in der für den Kiosk-Modus zugelassenen App-Gruppe einzuschließen.

Einstellung	Beschreibung
Sonstige Apps	Klicken Sie auf Hinzufügen+, um den **Paketnamen** einer App einzuschließen, die nicht im Google Play Store verfügbar ist. Bei Samsung-Geräten sollten die Administratoren die folgenden Dialer-/Systempakete in die Whitelist aufnehmen, damit sie im Kioskmodus funktionsfähig sind und die Dialer-Funktionalität im Kioskmodus aktiviert werden kann. • Telefonat - com.samsung.android.incallui • Telefon - com.samsung.android.dialer (sollte auf der Whitelist stehen; der Administrator sollte die Option „Verstecken" für dieses Paket wählen, um Probleme mit zwei Dialer-Optionen für den Benutzer zu vermeiden). • Telefonat - com.sec.phone • Telefonateinstellung - com.samsung.android.app.telephonyui • Unterstützte Anwahl - com.sec.providers.assisteddialing • Telefonatprotokoll sichern/wiederherstellen - com.android.calllogbackup • Dialer-Speicherung - com.android.providers.telephony • Telefon - com.android.server.telecom • Telefon - com.android.phone • Smart Call - com.samsung.android.smartcallprovider • WLAN-Telefonie - com.sec.unifiedwfc
Im Kiosk-Modus zulässige Apps	Klicken Sie auf „X", um eine App aus der für den Kiosk-Modus zugelassenen App-Gruppe zu entfernen. Ändern Sie mit Drag&drop die Reihenfolge der Apps auf den Kiosk-Geräten. **Ordner hinzufügen** – Mithilfe dieser Option können Sie einen Ordner in diesem Abschnitt erstellen und eine oder mehrere Apps in diesen Ordner verschieben. Sie können bis zu zwei Ordnerebenen erstellen. Die in einen Ordner kopierten Apps können nicht in einen anderen Ordner kopiert werden. In einem Ordner werden maximal 25 Apps unterstützt.
Einzel-App Launcher Kiosk aktivieren	Wählen Sie diese Option aus, um den Kiosk-Modus zu verwenden und eine App auf GMS- und Nicht-GMS-Geräten im Vordergrund zu behalten. Sie müssen eine App aus dem App-Katalog auswählen oder eine Paket-ID eingeben.
Erstellen Sie eine Whitelist der Apps, die den Benutzern im Kiosk-Modus zur Verfügung stehen, indem Sie Apps zur Liste der zulässigen Apps hinzufügen. Ordnen Sie die Apps per Drag-and-Drop in der Reihenfolge an, in der sie im Launcher für den Kiosk-Modus angezeigt werden sollen. Durch Hinzufügen einer Anwendung zur Liste zulässiger Apps wird die App nicht	

Einstellung	Beschreibung
auf dem Gerät installiert. Achten Sie darauf, jede App an die entsprechenden Benutzer und Benutzergruppen im App-Katalog zu verteilen.	
Vorinstallierte Apps	Klicken Sie auf „+Hinzufügen“, um aufgelistete, native Apps in der für den Kiosk-Modus zugelassenen Gruppe einzuschließen. In den Einstellungen für die im Kioskmodus zugelassenen Apps stehen folgende Optionen zur Verfügung: • **App-Benutzerdaten löschen**: Wenn Sie diese Option aktivieren, werden alle Anwendungsdaten automatisch und ohne Aufforderung gelöscht, wenn sich der Benutzer vom Kiosk abmeldet. Wählen Sie in den Einstellungen für den Kioskmodus Gemeinsam genutztes Gerät aktivieren, damit diese Option mit den Anwendungen verfügbar ist. ◦ App-Daten werden für Google Chrome und das Webview-Paket auch dann nicht gelöscht, wenn sie in der App-Whitelist mit aktivierter Benutzerdatenlöschung hinzugefügt wurden. Dies liegt daran, dass das Kiosk-Gerät abstürzen könnte, wenn die App-Daten für diese 2 Pakete gelöscht werden. ◦ App-Daten werden für System-Apps, für die kein App-Launcher verfügbar ist, nicht gelöscht (sowohl innerhalb als auch außerhalb des Kiosks). • **Verbergen**: Wenn Sie diese Option aktivieren, kann die Anwendung zwar von anderen Apps aufgerufen werden, ist aber im Kiosk-Startprogramm nicht sichtbar. Wenn Sie Dialer oder Kamera in den Sperreinstellungen oben deaktiviert haben, können Sie diese nicht in der Liste der zulässigen Apps ergänzen.
App-Katalog	Klicken Sie auf „Hinzufügen+“, um aufgelistete Apps aus dem App-Katalog in der für den Kiosk-Modus zugelassenen App-Gruppe einzuschließen.
Sonstige Apps	Klicken Sie auf Hinzufügen+, um den **Paketnamen** einer App einzuschließen, die nicht im Google Play Store verfügbar ist. Bei Samsung-Geräten sollten die Administratoren die folgenden Dialer-/Systempakete in die Whitelist aufnehmen, damit sie im Kioskmodus funktionsfähig sind und die Dialer-Funktionalität im Kioskmodus aktiviert werden kann. • Telefonat - com.samsung.android.incallui • Telefon - com.samsung.android.dialer (sollte auf der Whitelist stehen; der Administrator sollte die Option „Verstecken“ für dieses Paket wählen, um Probleme mit zwei Dialer-Optionen für den Benutzer zu vermeiden). • Telefonat - com.sec.phone • Telefonateinstellung - com.samsung.android.app.telephonyui • Unterstützte Anwahl - com.sec.providers.assisteddialing • Telefonatprotokoll sichern/wiederherstellen - com.android.calllogbackup

Einstellung	Beschreibung
Im Kiosk-Modus zulässige Apps	• Dialer-Speicherung - com.android.providers.telephony • Telefon - com.android.server.telecom • Telefon - com.android.phone • Smart Call - com.samsung.android.smartcallprovider • WLAN-Telefonie - com.sec.unifiedwfc Klicken Sie auf „X“, um eine App aus der für den Kiosk-Modus zugelassenen App-Gruppe zu entfernen. Ändern Sie mit Drag&drop die Reihenfolge der Apps auf den Kiosk-Geräten. **Ordner hinzufügen** – Mithilfe dieser Option können Sie einen Ordner in diesem Abschnitt erstellen und eine oder mehrere Apps in diesen Ordner verschieben. Sie können bis zu zwei Ordnerebenen erstellen. Die in einen Ordner kopierten Apps können nicht in einen anderen Ordner kopiert werden. In einem Ordner werden maximal 25 Apps unterstützt.

Bei Samsung-Geräten mit Knox Standard 4.0 oder höher wird die Mehrbenutzerfunktion im Kiosk-Modus automatisch gesperrt.

Verwaltete Geräte mit Arbeitsprofil

Deaktiviert bestimmte Funktionen auf einem verwalteten Gerät mit Arbeitsprofil für Android 8.0+.

Bestimmte Funktionen können für das Arbeitsprofil auf firmeneigenen Geräten deaktiviert werden (gilt für Geräte mit Android 11+).

Einstellung	Beschreibung
Verwaltete Geräte-Sperreinstellungen	
Wi-Fi deaktivieren	Wählen Sie diese Option aus, um den Zugriff auf WLANs zu deaktivieren (gilt nicht für Geräte ab Android 11).
WLAN-Einstellungen deaktivieren	Wählen Sie die Option, um den Zugriff auf die Einstellungen für drahtlose Netzwerke zu deaktivieren.
Kamera deaktivieren	Wählen Sie diese Option, um den Zugriff auf die Kamera zu deaktivieren.
Bluetooth deaktivieren	Wählen Sie diese Option, um Bluetooth-Funktionen zu deaktivieren. Seien Sie bei Anwendung dieser Option vorsichtig. Ivanti rät davon ab, Audio-Funktionen zu deaktivieren, da damit auch der Zugriff auf Bluetooth-Freisprecheinrichtungen deaktiviert wird. Gesetzliche Vorschriften zur Nutzung von Freisprechanlagen während des Fahrens sind immer weiter verbreitet.
Bluetooth-Einstellungen nicht zulassen	Wählen Sie diese Option, um den Zugriff auf die Bluetooth-Einstellungen zu deaktivieren.
Zurücksetzen des Netzwerks deaktivieren	Wählen Sie diese Option, um das Zurücksetzen des Netzwerks zu verhindern (gilt für Geräte ab Android 7.0).
Hauptlautstärke stummschalten	Wählen Sie die Option aus, um die Hauptlautstärke stumm zu schalten. (Gilt nicht für Geräte mit Android 11+)
Notfallrundsendungen nicht zulassen	Klicken Sie auf die Option, um Notfall-Broadcasts zu verhindern.
Mobile Netzwerke nicht zulassen	Wählen Sie diese Option, um den Zugriff auf mobile Netzwerke zu deaktivieren. Diese Option kann nicht deaktiviert werden, wenn das WLAN deaktiviert ist.
Internetweiterleitung nicht zulassen	Wählen Sie diese Option zur Deaktivierung von Wi-Fi-Tethering, einer Funktion, die die Internetverbindung eines Gerät nutzt, um Internetzugang für ein anderes Gerät herzustellen.
VPN nicht zulassen	Wählen Sie diese Option aus, um die VPN-Verbindungen zu deaktivieren. (Gilt nicht für Geräte mit Android 11+)
Zurücksetzen auf Werkseinstellungen deaktivieren	Wählen Sie die Option, um Benutzer daran zu hindern, das Gerät auf die Werkeinstellungen zurückzusetzen. (Gilt nicht für Geräte mit Android 11+)
Zurücksetzen auf die Werkseinstellungen schützen	Wählen Sie diese Option aus, damit Benutzer das Gerät auf die Werkeinstellungen zurücksetzen können. Sie können auch eine Liste autorisierter Google-Konto-IDs (als Ganzzahl) angeben, mit denen das Gerät nach einem Reset auf die Werkeinstellungen bereitgestellt werden kann, oder den Mauszeiger über dem Hilfesymbol bewegen, wenn Sie nicht wissen, wie Sie autorisierte Konto-IDs laden.

Einstellung	Beschreibung
Abgehende Gespräche nicht zulassen	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer selbst anrufen kann.
Sicheren Neustart nicht zulassen (Android 6.0+)	Wählen Sie die Option, um zu verhindern, dass ein Benutzer ein Gerät im sicheren Startmodus neu startet.
Debugging-Funktionen nicht zulassen	Wählen Sie diese Option, um die Debugging-Funktionen auf den Geräten zu deaktivieren. Standardmäßig ist diese Option aktiviert.
Apps-Verifizierung sicherstellen	Wählen Sie diese Option, um Anwendungsverifizierungsfunktionen auf den Geräten zu erlauben. Standardmäßig ist diese Option aktiviert. Wenn diese Option deaktiviert ist, zeigt das Gerät wieder das Standardverhalten, das je nach Gerät abweichen kann.
SMS nicht zulassen	Wählen Sie diese Option aus, wenn ein Benutzer keine SMS-Nachrichten senden oder empfangen darf.
Einschalten des Mikrofons nicht zulassen	Wählen Sie diese Option aus, wenn das Mikrofon des Geräts immer eingeschaltet bleiben soll.
Automatische Zeit nicht zulassen	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer die automatische Zeiteinstellung aktiviert.
Automatische Zeitzone nicht zulassen	Wählen Sie diese Option, damit die Gerätezeit bei Zeitzonenänderungen nicht automatisch angepasst wird.
Daten-Roaming deaktivieren	Wählen Sie diese Option, um den Datenaustausch zu deaktivieren, während sich das Gerät im Roaming-Modus befindet.
Zeit mit dem Server synchronisieren (Android 9.0+)	Wählen Sie diese Option, damit die Geräte die Zeit mit den MI-Cloud-Servern erstmals bei der Registrierung und danach einmal alle 24 Stunden nach jeder Anmeldung synchronisieren können. Diese Option ist nur verfügbar, wenn die Option **Automatische Zeit deaktivieren** ausgewählt wurde.
Zeitzone einstellen (Android 9.0+)	Geben Sie die Zeichenfolge für die Zeitzone im Olson-Zeitzonen-ID-Format an (z. B. Pacific/Midway).
Automatische WLAN-Deaktivierung nicht zulassen	Wählen Sie diese Option aus, wenn das WLAN nicht deaktiviert werden soll, wenn das Gerät in den Sleep-Modus wechselt. (Gilt nicht für Geräte mit Android 11+)
Eingabemethoden beschränken	Wählen Sie diese Option aus, um die Eingabemethoden für Arbeits-Apps einzuschränken, indem Sie über das Feld **Paketname** eine Liste der zulässigen Paketnamen angeben (gilt nicht für Geräte ab Android 11). Auf den Geräten stehen sowohl die Eingabemethoden der Whitelist als auch die Standard-Eingabemethoden des Systems zur Verfügung. Der Benutzer kann zwischen den Standard-Eingabemethoden des Systems und den Eingabemethoden der Whitelist-Pakete wählen.

Einstellung	Beschreibung
	In Android 10+ sind die Eingabemethoden nur für die Geräteseite beschränkt, ansonsten gelten die Bechränkungen für das gesamte Gerät.
Zugangsdienste beschränken	Beschränken Sie mit der Option **Paketname** den Zugang auf Unternehmens-Apps auf Pakete in einer Whitelist. Wenn in der Whitelist keine Programmpakete eingetragen sind, ist nur die Eingabe über die Systemtastatur zulässig. In Android 10+ sind die Eingabemethoden nur auf beruflich genutzte Apps beschränkt, ansonsten gelten die Beschränkungen für das gesamte Gerät.
USB-Dateitransfer deaktivieren	Klicken Sie auf die Option, um den USB-Dateitransfer deaktivieren.
Externe Medien deaktivieren	Klicken Sie auf die Option, um externe Medien deaktivieren.
Unbekannte Quellen auf Geräten nicht zulassen.	Klicken Sie auf die Option, um zu verhindern, dass das Gerät Apps aus unbekannten Quellen installiert. Damit diese Einstellung auf dem Gerät wirksam wird, muss diese Funktion mit einem anstehenden Google Play Update aktiviert werden.
Meldung für Sperrbildschirm einstellen (Android 7.0+)	Wählen Sie diese Option, um festzulegen, welche Meldung auf dem Sperrbildschirm des Geräts angezeigt werden soll. Geben Sie die Meldung für die Displaysperre (maximal 256 Zeichen) in das Textfeld ein. Bei Aktivierung dieser Option kann der Benutzer die Meldung in den Einstellungen nicht ändern, und die vom Admin eingestellte Meldung wird dem Benutzer angezeigt. Wenn der Admin nach der Aktivierung von 'Setze Sperrbildschirmmeldung' keine Sperrmeldung zur Verfügung stellt, wird dem Benutzer die Einstellung der Meldung in den Einstellungen verwehrt, aber es wird keine Meldung an den Benutzer angezeigt.
Bildschirmhelligkeit festlegen	Mit dieser Option legen Sie die Bildschirmhelligkeit auf Ihrem Gerät fest. • Manuell – Wählen Sie diese Option aus, um manuell eine Zahl einzugeben (von 0 bis 255). • Adaptiv – Wählen Sie diese Option aus, um dem Gerät das Festlegen der Helligkeit zu erlauben. Es wird empfohlen, vor dem Einstellen der Bildschirmhelligkeit die Option "Konfigurieren der Helligkeit nicht zulassen" zu aktivieren. Falls der Benutzer Änderungen vornehmen darf, werden die Einstellungen beim nächsten Einchecken auf die vom Administrator definierten Einstellungen zurückgesetzt. Diese Einstellung wird auf Geräten mit Android 11 oder später für das Arbeitsprofil im Modus "Firmeneigenes Gerät" nicht unterstützt.
Zeitüberschreitung für Bildschirm festlegen	Mit dieser Option legen Sie die Dauer des Bildschirm-Timeouts (in Sekunden) fest. Es wird empfohlen, vor dem Einstellen des Bildschirm-Timeouts die Option "Konfigurieren der Zeitüberschreitung für Bildschirm nicht zulassen" zu aktivieren. Falls der Benutzer Änderungen vornehmen darf, werden die Einstellungen beim nächsten Einchecken auf die vom Administrator definierten Einstellungen zurückgesetzt. Diese Einstellung wird auf Geräten mit Android 11 oder später für das Arbeitsprofil im Modus "Firmeneigenes Gerät" nicht unterstützt.

Einstellung	Beschreibung
Bildschirmausrichtung festlegen	Mit dieser Option legen Sie die Bildschirmausrichtung fest. Über die Dropdownliste lässt sich die Ausrichtung auf 0, 90, 180 oder 270 Grad festlegen. Diese Einstellung wird auf Geräten mit Android 11 oder später für das Arbeitsprofil im Modus "Firmeneigenes Gerät" nicht unterstützt.
Automatisches Ausfüllen deaktivieren (Android 8.0+)	Aktivieren Sie diese Option, um ein automatisches Ausfüllen zu verhindern. (Gilt nicht für Geräte mit Android 11+)
Bluetooth-Freigabe nicht zulassen (Android 8.0+)	Aktivieren Sie dieses Kontrollkästchen, wenn der Benutzer ausgehendes Bluetooth auf dem Gerät nicht teilen soll.
Datensicherungs-Dienst deaktivieren (Android 8.0+)	Wählen Sie diese Option, um den Backup-Dienst zu deaktivieren. (Gilt nicht für Geräte mit Android 11+)
Drucken verweigern (Android 9.0+)	Wählen Sie diese Option aus, um das Drucken über alle Apps zu unterbinden (gilt nicht für Geräte ab Android 11).
Flugzeugmodus nicht zulassen (Android 9.0+)	Aktivieren Sie diese Option, um den Flugzeugmodus auf dem gesamten Gerät zu deaktivieren.
Umgebungsanzeige nicht zulassen (Android 9.0+)	Aktivieren Sie diese Option, um die Umgebungsanzeige für den Benutzer zu deaktivieren. (Gilt nicht für Geräte mit Android 11+)
Konfigurierte Helligkeit nicht zulassen (Android 9.0+)	Aktivieren Sie diese Option, um zu verhindern, dass Benutzer die Helligkeit konfigurieren können (gilt nicht für Geräte mit Android 11+). Es wird empfohlen, vor dem Auswählen dieser Option den Modus für "Bildschirmhelligkeit festlegen" zu definieren.
Konfiguration von Datum/Uhrzeit nicht zulassen (Android 9.0+)	Aktivieren Sie diese Option, um die Konfiguration von Datum, Uhrzeit und Zeitzone zu deaktivieren.
Standortkonfiguration nicht zulassen (Android 9.0+)	Aktivieren Sie dieses Kontrollkästchen, um dem Benutzer zu verbieten, Standortbetreiber zu deaktivieren.
Zeitüberschreitung des Konfigurationsbildschirms nicht zulassen (Android 9.0+)	Aktivieren Sie diese Option, um zu verhindern, dass Benutzer die Zeitüberschreitung für die Bildschirmabschaltung ändern können. (Gilt nicht für Geräte mit Android 11+) Es wird empfohlen, vor dem Auswählen dieser Option den Wert für "Zeitüberschreitung für Bildschirm festlegen" zu definieren.
Systemfehler-Dialoge nicht zulassen (Android 9.0+)	Wählen Sie diese Option aus, um Dialogfelder zu Systemfehlern zu unterbinden (gilt nicht für Geräte ab Android 11).

Einstellung	Beschreibung
Screenshots deaktivieren (Android 11.0 +)	Wählen Sie diese Option, um die integrierte Funktion des Geräts zum Erstellen von Screenshots zu deaktivieren. Wenn diese Option ausgewählt ist, wird die Bildschirmaufnahme auf der privaten Seite des Geräts deaktiviert.
Android 12.0+	
USB nur zum Laden aktivieren	Wählen Sie diese Option aus, um den USB-Port nur zum Laden zu aktivieren.
Android 13.0+	
Mindestens erforderliche WLAN-Sicherheit festlegen	Mit dieser Option legen Sie die mindestens erforderliche WLAN-Sicherheit fest: • Keine Mindestsicherheit erforderlich – Wählen Sie diese Option aus, wenn keine Mindestsicherheit erforderlich ist. • Sicherheit auf Basis eines persönlichen Netzwerks – Wählen Sie diese Option aus, um persönliche WLAN-Netzwerke zu blockieren, wie WEP, WPA/WPA2/WPA3 usw. • Sicherheit auf Basis eines EAP-Enterprise-Netzwerks – Wählen Sie diese Option aus, um WLAN-Netzwerke auf Basis des EAP-Protokolls zu blockieren. • Sicherheit auf Basis eines 192-Enterprise-Netzwerks – Wählen Sie diese Option aus, um WLAN-Netzwerke auf EAP-Unternehmensbasis zu blockieren. Alle vorhandenen Geräte, die die Mindestkriterien nicht erfüllen, werden getrennt. Bei den Gerätedetails wird die mindestens erforderliche WLAN-Sicherheitsstufe (falls definiert) unter **Allgemein > WLAN-Sicherheitsstufe** angezeigt.
Teilen der WLAN-Konfiguration des Administrators nicht zulassen	Wählen Sie diese Option, um zu verhindern, dass Benutzer vom Administrator festgelegte WLAN-Konfigurationen teilen können.
Arbeitsprofil-Sperreinstellungen	
Screenshots deaktivieren	Wählen Sie diese Option, um die integrierte Funktion des Geräts zum Erstellen von Screenshots zu deaktivieren.
Apps-Kontrolle verweigern	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer Anwendungen in den Einstellungen oder Startkonfigurationen modifiziert.
Konfigurations-Anmeldeinformationen verweigern	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer Anmeldeinformationen konfiguriert.
Profilübergreifendes Kopieren und Einfügen verweigern	Wählen Sie diese Option aus, um zu verhindern, dass Informationen zwischen Profilen kopiert und eingefügt werden.
Kontoänderungen	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer Konten hinzufügt oder entfernt.

Einstellung	Beschreibung
verweigern	
Ausgehende NFC (Outgoing Beam) verweigern (Android 5.1 +)	Wählen Sie diese Option aus, um zu verhindern, dass ein Benutzer mit NFC App-Daten überträgt.
Standortfreigabe verweigern	Wählen Sie diese Option aus, um zu verhindern, dass Websites und Apps den Gerätebenutzer auffordern, den Gerätestandort freizugeben.
Debugging-Funktionen nicht zulassen	Wählen Sie diese Option, um die Debugging-Funktionen auf den Geräten zu deaktivieren. Standardmäßig ist diese Option aktiviert.
Apps-Verifizierung sicherstellen	Wählen Sie diese Option, um Anwendungsverifizierungsfunktionen auf den Geräten zu erlauben. Standardmäßig ist diese Option aktiviert. Wenn diese Option deaktiviert ist, zeigt das Gerät wieder das Standardverhalten, das je nach Gerät abweichen kann.
Unbekannte Quellen im Arbeitsprofil deaktivieren	Wählen Sie diese Option, um den Download aus unbekannten Quellen innerhalb des Arbeitsprofils zu verbieten.
System-Apps aktivieren/deaktivieren	Wählen Sie diese Option, um die Systemanwendungen zu aktivieren bzw. zu deaktivieren, die bereitgestellt werden sollen, indem Sie zwei Listen mit Paketnamen über die Felder **System App-Paketname** zuordnen. Mit dieser Funktion können Sie den Zugriff auf Systemanwendungen verwalten, die nicht in Google Play veröffentlicht sind. Die Ergänzung einer App im App-Katalog sowie in der Liste der System-Apps wird nicht unterstützt.
Anrufer-ID deaktivieren (Android 6,0 +)	Legt fest, ob die Anrufer-ID-Informationen aus dem Arbeitsprofil bei eingehenden Anrufen auf dem Gerät angezeigt werden.
Kontaktfreigabe über Bluetooth deaktivieren (Android 6.0+)	Wählen Sie diese Option, um zu verhindern, dass das Gerät Kontakte über Bluetooth mit anderen Geräten teilt.
Kontaktfreigabe über die Suche deaktivieren (Android 7.0+)	Wählen Sie diese Option, um zu verhindern, dass Benutzer nach Arbeitskontakten in der privaten Kurzwahlliste suchen.
Automatisches Ausfüllen deaktivieren (Android 8.0+)	Aktivieren Sie diese Option, um ein automatisches Ausfüllen zu verhindern. (Gilt nicht für Geräte mit Android 11+)
Benachrichtigungen über Arbeitsanwendungen im persönlichen Profil deaktivieren (Android 8.0+)	Wählen Sie diese Option, um die Benachrichtigungen über Arbeitsprofile einzuschränken.

Einstellung	Beschreibung
Drucken verweigern (Android 9.0+)	Wählen Sie diese Option, um den Druck aus allen Apps zu beschränken. (Gilt nicht für Geräte mit Android 11+)
Freigabe in Profil verweigern (Android 9.0+)	Aktivieren Sie diese Option, wenn Benutzer keine personenbezogenen Daten in einem Arbeitsprofil auf dem Gerät freigeben sollen.
Eingabemethoden beschränken (Android 10.0 +)	Aktivieren Sie dieses Kontrollkästchen, um IME-Paketnamen auf der Whitelist einzuschränken, indem Sie über das Feld **Paketname** eine Liste mit den Namen in der Whitelist angeben (gilt nicht für Geräte mit Android 11+). Auf den Geräten stehen sowohl die Eingabemethoden der Whitelist als auch die Standard-Eingabemethoden des Systems zur Verfügung. Der Benutzer kann zwischen den Standard-Eingabemethoden des Systems und den Eingabemethoden der Whitelist-Pakete wählen. Die Eingabemethoden gelten für IME-Apps, die für das Arbeitsprofil installiert sind. Selbst wenn die auf der Geräteseite installierten Anwendungen für diese Sperre auf der Whitelist stehen, sind sie als Anwendungen auf der Arbeitsprofilseite nicht verfügbar.
Zugriff auf Arbeitsprofilkalender zulassen (Android 10.0 +)	Wählen Sie eine der folgenden Optionen, um alle Apps zuzulassen, oder eine Reihe von Apps auf der persönlichen Seite, die auf die im Arbeitsprofil vorhandenen Kalenderinformationen zugreifen dürfen: • **Alle Apps im persönlichen Profil** – erlaubt allen Apps den Zugriff auf die im Arbeitsprofil vorhandenen Kalenderinformationen. • **Nur die folgenden Apps im persönlichen Profil** – Geben Sie in das Textfeld unten die Bundle-IDs der Apps durch ein Komma getrennt ein. Nur diesen ausgewählten Apps auf der persönlichen Seite wird der Zugriff auf die im Arbeitsprofil vorhandenen Kalenderinformationen gestattet. Für die App auf der persönlichen Seite sollten spezifische APIs implementiert sein, um auf den gemeinsamen Kalender zuzugreifen.
Profilübergreifendes Whitelisting von Apps aktivieren (Android 11.0+)	Aktivieren Sie das Kontrollkästchen, um Benutzern die gemeinsame Nutzung von Informationen aus bestimmten Apps aus dem Arbeitsprofil auf der privaten Seite des Geräts zu ermöglichen. Geben Sie in das Feld **Apps in der Whitelist** die Paket-IDs der Apps durch Kommata getrennt ein, die auf die Whitelist gesetzt werden sollen. Diese Option ist standardmäßig deaktiviert.

Einstellung	Beschreibung
Maximale Profilzeitüberschreitung aktivieren (Android 11.0+)	Wählen Sie diese Option, um ein maximales Zeitfenster festzulegen, in dem das Arbeitsprofil ausgeschaltet werden kann, bevor die Cloud private Apps auf dem Gerät vorübergehend deaktiviert. Sie können eine Zeit zwischen 72 und 8760 Stunden einstellen. 8760 Stunden sind ein Jahr. Standardmäßig sind 72 Stunden eingestellt, wenn die Option ausgewählt ist. Der Gerätebenutzer sieht eine Meldung mit der Aufforderung, das Arbeitsprofil einzuschalten, um zeitweilig deaktivierte Apps zu aktivieren. Für unternehmenseigene Geräte mit Android 11+ im Arbeitsprofil verfügbar Wenn das Profil für längere Zeit deaktiviert ist, werden persönliche Apps auf dem Gerät aufgehoben.
5G Network Slicing aktivieren (Android 12.0+)	Wählen Sie diese Option aus, um eine 5G Network Slicing-Option auf dem Arbeitsprofil firmeneigener Geräte bereitzustellen. Diese Option ist standardmäßig deaktiviert.
AI Assist deaktivieren (Android 15.0+)	Aktivieren Sie diese Option, um Benutzer von AI Assist-Funktionen auszuschließen. Diese Option ist standardmäßig deaktiviert.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.4.33. Sperre & Kiosk-Modus: Samsung Knox Standard

Eine Konfiguration für den Modus Sperre & Kiosk: Samsung Knox Standard deaktiviert bestimmte Funktionen auf Geräten mit Samsung Knox Standard und erstellt eine App-Whitelist für die Benutzer im Kiosk-Modus.

> Die Samsung KNOX Standard-Konfiguration ist veraltet und wird auf Geräten mit Android 9 oder späteren Versionen nicht mehr unterstützt.

Sperr-Einstellungen

Einstellung

So gehen Sie vor

[Name]

Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.

Beschreibung

Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.

Samsung Knox Sperr-Einstellungen: Deaktiviert bestimmte Funktionen auf Samsung Knox-Geräten.

Wi-Fi deaktivieren

Wählen Sie diese Option, um den Zugriff auf drahtlose Netzwerke zu deaktivieren.

Kamera deaktivieren

Wählen Sie diese Option, um den Zugriff auf die Kamera zu deaktivieren.

Bluetooth deaktivieren

Wählen Sie diese Option, um Bluetooth-Funktionen zu deaktivieren.

Bei Bluetooth nur Audio zulassen

Wählen Sie die Option, um nur die Bluetooth-Audiofunktionen zu aktivieren.

Mobile Daten deaktivieren

Wählen Sie diese Funktion, um den Datenaustausch zu deaktivieren, wenn ein Gerät mit einem anderen Gerät in Kontakt kommt.

Diese Option kann nicht deaktiviert werden, wenn das WLAN deaktiviert ist.

GPS deaktivieren

Wählen Sie diese Funktion, um GPS zu deaktivieren.

Wählhilfe deaktivieren

Wählen Sie diese Funktion, um die Telefon-App zu deaktivieren.

SD-Karte deaktivieren

Wählen Sie diese Option, um den zugriff auf die SD-Karte zu deaktivieren.

Google Backup deaktivieren

Wählen Sie diese Option, um Backups auf Google-Servern zu deaktivieren.

Kopieren/Einfügen deaktivieren

Wählen Sie diese Option, um den Zugriff auf die Funktionen Kopieren/Einfügen zu deaktivieren.

NFC deaktivieren

Wählen Sie diese Option, um den Datenaustausch per NFC (Near-field Communication) zu deaktivieren, wenn das Gerät mit einem anderen Gerät in Kontakt kommt.

Mikrofon deaktivieren

Wählen Sie diese Option, um den App-Zugriff auf das Mikrofon des Geräts zu deaktivieren.

Screenshots deaktivieren

Wählen Sie diese Option, um die integrierte Funktion des Geräts zum Erstellen von Screenshots zu deaktivieren. Bei Auswahl dieser Option sind keine Bildschirmfotos der GO-App möglich. Solche Bildschirmfotos werden blockiert.

Bluetooth-Tethering deaktivieren

Wählen Sie diese Option zur Deaktivierung von Bluetooth Tethering, einer Funktion, die die Internetverbindung eines Gerät nutzt, um Internetzugang für ein anderes Gerät herzustellen.

USB-Debugging deaktivieren

Wählen Sie diese Option, um die Funktion USB-Debugging zu deaktivieren.

USB-Tethering deaktivieren

Wählen Sie diese Option zur Deaktivierung von USB Tethering, einer Funktion, die die Internetverbindung eines Gerät nutzt, um Internetzugang für ein anderes Gerät herzustellen.

Wi-Fi-Tethering deaktivieren

Wählen Sie diese Option zur Deaktivierung von Wi-Fi-Tethering, einer Funktion, die die Internetverbindung eines Gerät nutzt, um Internetzugang für ein anderes Gerät herzustellen.

Integrierten Browser deaktivieren

Wählen Sie diese Option, um Benutzer am Zugriff auf den Android-Browser zu hindern.

YouTube deaktivieren

Wählen Sie diese Option, um Benutzer am Zugriff auf YouTube zu hindern.

Zurücksetzen auf Werkseinstellungen deaktivieren

Wählen Sie diese Option, um Benutzer daran zu hindern, das Gerät auf die Werkseinstellungen zurückzusetzen.

OTA-Aktualisierung deaktivieren

Wählen Sie diese Option zur Deaktivierung von Over-the-Air-Upgrades der Geräte-Firmware.

Warnung: Deaktivieren Sie nicht die Funktion **Einstellungsänderungen deaktivieren**, solange **OTA Upgrade** aktiviert ist. Wenn die **Einstellungsänderungen deaktiviert** werden, solange **OTA Upgrade** aktiviert ist, kann dies dazu führen, dass das Gerät nicht mehr funktioniert, da die Einstellungsänderungen für Upgrades benötigt werden.

Sprach-Roaming deaktivieren

Wählen Sie diese Option, um Sprachanrufe zu deaktivieren, während sich das Gerät im Roaming-Modus befindet.

USB-Media-Player deaktivieren

Wählen Sie diese Option, um den USB-Media-Player zu deaktivieren.

Google Play deaktivieren

Wählen Sie diese Option, um den Zugriff auf Google Play zu deaktivieren.

Daten-Roaming deaktivieren

Wählen Sie diese Option, um den Datenaustausch zu deaktivieren, während sich das Gerät im Roaming-Modus befindet.

Unbekannte Quellen deaktivieren

Wählen Sie die Option, um die Installation anderer Apps außer GO aus beliebigen Quellen, beispielsweise aus dem Google Play Store, zu deaktivieren.

Die Entfernung der Geräte-Administratorberechtigungen deaktivieren

Wählen Sie die Option, um Benutzer daran zu hindern, die Administratorrechte der GO-App auf dem Gerät zu deaktivieren.

Einstellungsänderungen deaktivieren

Wählen Sie diese Option, um den Zugriff auf die App für die Geräteeinstellungen zu deaktivieren.

Warnung: Deaktivieren Sie nicht die Funktion **Einstellungsänderungen deaktivieren**, solange **OTA Upgrade** aktiviert ist. Wenn die **Einstellungsänderungen deaktiviert** werden, solange **OTA Upgrade** aktiviert ist, kann dies dazu führen, dass das Gerät nicht mehr funktioniert, da die Einstellungsänderungen für Upgrades benötigt werden.

Kiosk-Moduseinstellungen: Im Kiosk-Modus gelten für das Geräte zusätzliche Einschränkungen wie der beschränkte Zugriff auf Apps über einen benutzerdefinierten Launcher.

Anwendbar auf Android-Versionen bis 8.1. Verwenden Sie für Android-Versionen ab 9.0 die Android Enterprise-Konfiguration für ein verwaltetes Kiosk-Gerät.

Kiosk-Modus aktivieren

Klicken Sie auf , um den **Kiosk Mode** auf Android-Geräten zu konfigurieren.

Benutzerzugriff auf Wi-Fi-Einstellungen zulassen

Wählen Sie diese Option aus, damit ein Benutzer die WLAN-Einstellungen ändern und auf bevorzugte drahtlose Netze zugreifen kann.

Benutzerzugang für Bluetooth-Einstellungen zulassen

Wählen Sie diese Option aus, damit ein Benutzer die Bluetooth-Einstellungen ändern und weitere Bluetooth-Geräte koppeln kann.

Verzögerung der Anwendungs-Updates durch Benutzer zulassen

Wählen Sie diese Option aus, damit ein Benutzer Anwendungsupdates verzögern kann.

GPS-Standorteinstellungen

Wählen Sie eine der folgenden Einstellungen für die GPS-Standortbestimmung:

- Standort deaktivieren
- Standortermittlung aktivieren
- Auswahl dem Benutzer überlassen

PIN zum Beenden des Kiosk-Modus

Geben Sie den vierstelligen Zahlencode ein, den der Endbenutzer eingeben muss, um den Kiosk-Modus zu beenden.

Erstellen Sie eine Whitelist der Apps, die den Benutzern im Kiosk-Modus zur Verfügung stehen, indem Sie Apps zur Liste der zulässigen Apps hinzufügen. Ordnen Sie die Apps per Drag-and-Drop in der Reihenfolge an, in der sie im Launcher für den Kiosk-Modus angezeigt werden sollen.

Durch Hinzufügen einer Anwendung zur Liste zulässiger Apps wird die App nicht auf dem Gerät installiert. Achten Sie darauf, jede App an die entsprechenden Benutzer und Benutzergruppen im App-Katalog zu verteilen.

Vorinstallierte Apps

Klicken Sie auf „+Hinzufügen“, um aufgelistete, native Apps in der für den Kiosk-Modus zugelassenen Gruppe einzuschließen.

Wenn Sie Dialer oder Kamera in den Sperreinstellungen oben deaktiviert haben, können Sie diese nicht in der Liste der zulässigen Apps ergänzen.

App-Katalog

Klicken Sie auf „Hinzufügen+“, um aufgelistete Apps aus dem App-Katalog in der für den Kiosk-Modus zugelassenen App-Gruppe einzuschließen.

Sonstige Apps

Klicken Sie auf Hinzufügen+, um den **Paketnamen** einer App einzuschließen, die nicht im Google Play Store verfügbar ist.

Im Kiosk-Modus zulässige Apps

Klicken Sie auf X, um eine App aus der für den Kiosk-Modus zugelassenen App-Gruppe zu entfernen. Ändern Sie mit Drag&drop die Reihenfolge der Apps auf den Kiosk-Geräten.

> Samsung-Geräte, die mehrere Benutzer unterstützen, sperren bei Verwendung des Kiosk-Modus mit Android 4.4 bis 6.0 automatisch die Funktion für mehrere Benutzer, solange sich das Gerät im Kiosk-Modus befindet.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.4.34. Konfiguration "Local Administrator Password Solution"

Die Konfigurationseinstellungen für **Local Administrator Password Solution (LAPS)** ermöglichen es Ivanti Neurons for MDM-Administratoren, das lokale Administratorkennwort auf verwalteten macOS-Geräten zu bestimmten Intervallen automatisch erneut zu generieren. Weitere Informationen zu LAPS finden Sie unter **Local Admin Password Solution (LAPS)**.

Gilt für: macOS-Geräte, die unter Verwendung der automatischen Geräteregistrierung registriert und verwaltet werden.

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Local Administrator Password Solution** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie die Einstellungen für **LAPS** gemäß der folgenden Tabelle:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Plattform	Wählen Sie macOS-aus der Dropdownliste aus.
Rotationsintervall	Wählen Sie eine der folgenden Optionen aus der Dropdownliste aus, um die automatische Kennwortrotation zu definieren: • Keine Rotation (**Standard**) • 15 Tage • 30 Tage • 60 Tage • 90 Tage • 120 Tage • 180 Tage
Rotation nach Anzeigen des Kennworts	Wählen Sie eine der folgenden Optionen aus der Dropdownliste aus, um die Kennwörter automatisch zu rotieren, nachdem sie auf der Seite **Gerätedetails** angezeigt wurden: • 1 bis 24 Stunden • 36 Stunden • 48 Stunden Der Standardwert ist **2 Stunden**.

4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
5. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Local Administrator Password Solution** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
6. Klicken Sie auf **Fertig**.

10.10.4.35. macOS-Firewall

Lizenz: Gold

Die macOS Firewall verwaltet die Einstellungen der Anwendungs-Firewall, die auf der Seite mit den Sicherheitspräferenzen für macOS-Geräte zugänglich sind.

Gilt für: macOS

- **Integrierter Software den Empfang eingehender Verbindungen erlauben** – Bei "wahr" kann die integrierte Software eingehende Verbindungen empfangen.
- **Heruntergeladener signierter Software den Empfang eingehender Verbindungen erlauben** – Bei "wahr" kann die heruntergeladene signierte Software eingehende Verbindungen empfangen.

Gilt für: macOS

- **Protokollierung aktivieren** – Bei "wahr" ist die Protokollierung möglich.
- **Geben Sie den Protokollierungstyp an.**
  - **Drosseln**
  - **Kurz**
  - **Details**

Gilt für: macOS 10.12+

Wenn Sie die Option **Firewall aktivieren** auswählen, können Sie eine oder mehrere der folgenden Optionen wählen:

- **Alle eingehenden Verbindungen sperren** – Wählen Sie diese Option, um zu verhindern, dass Freigabedienste eingehende Verbindungen auf macOS-Geräten empfangen können, zum Beispiel Bildschirmfreigabe oder Dateifreigabe. Die folgenden Systemdienste können eingehende Verbindungen weiterhin empfangen:
  - configd, der DHCP und andere Netzwerk-Konfigurationsdienste implementiert
  - mDNSResponder, der Bonjour implementiert
  - racoon, der IPSec implementiert
- **Stealth-Mode aktivieren** – Wählen Sie diese Option, um zu verhindern, dass macOS-Geräte auf Testanfragen reagieren. Verwaltete macOS-Geräte beantworten eingehende Anfragen für autorisierte Apps weiterhin, ignorieren jedoch unerwartete Anfragen wie ICMP (ping).
- **Anwendungen** – Die Liste der Anwendungen, deren Verbindungen von der Firewall kontrolliert werden. Wählen Sie die Apps aus, für die Sie eingehende Verbindungen auf macOS-Geräten empfangen möchten.

Wählen Sie **Hinzufügen+** aus, um eine Zeile zur App-Liste hinzuzufügen. Wählen Sie die Zelle unter **Bundle-ID** aus, um die App auszuwählen, deren eingehende Verbindungen Sie explizit zulassen möchten. Markieren Sie das Kontrollkästchen in der Zelle **Verbindungen zulassen**, um eingehende Verbindungen von der ausgewählten App zuzulassen.

> Die Konfiguration muss in einem systemweit geltenden Profil existieren. Wenn mehr als ein Profil in dieser Konfiguration enthalten ist, werden die jeweils restriktivsten Einstellungen verwendet.

> Die Optionen **Heruntergeladene signierte Software automatisch zulassen** und **Integrierte Software automatisch zulassen** werden nicht unterstützt. Wenn die Konfiguration verfügbar ist, werden jedoch beide Optionen erzwungen.

Der Administrator kann den Stealth-Modus aktivieren, indem er festlegt, dass das Gerät auf einen Ping-Befehl nicht reagiert.

10.10.4.36. Einschränkungen für macOS

Lizenz: Gold

Die macOS-Einschränkungen legen fest, welche Einschränkungen an macOS-Geräten aktiv sind.

Sie können die folgenden Funktionen auf macOS-Geräte aktivieren oder deaktivieren:

macOS-Version	Funktionen
macOS 10.11+	
	• [Allow Camera] • iCloud-Dokumentsynchronisation zulassen **Nur überwacht:** • Spotlight der Internetergebnisse zulassen
macOS 10.11.2+	
	• Definitionssuche zulassen
macOS 10.12+	
	• iCloud Keychain-Synchronisation zulassen • Datensicherung auf Mac zulassen • Suche nach Mac zulassen • Freigabe von Notizen, Erinnerungen oder LinkedIn zulassen • Lesezeichensynchronisation zulassen • MacOS-Mail-iCloud-Dienst zulassen • MacOS-iCloud-Kalenderdienst zulassen • MacOS-iCloud-Adressbuchdienst zulassen • iCloud-Erinnerungsdienst zulassen • Automatisches Entsperren zulassen **Nur überwacht:** • Apple Music zulassen
macOS 10.12.4+	
	• Fingerabdruck zum Entsperren zulassen
macOS 10.13+	
	• Dateifreigabe über iTunes zulassen • Content Caching zulassen • Wallpaper-Modifikation zulassen **Nur überwacht:** • AirPrint zulassen • AirPrint iBeacon Discovery zulassen

macOS-Version	Funktionen
	• Vertrauenswürdige TLS-Anforderung für AirPrint erzwingen • AirDrop zulassen • [Allow Game Center]
macOS 10.13.4+	
	Nur überwacht: Software-Updates für einen bestimmten Zeitraum in Tagen (30 bis 90 Tage) aufschieben Standard: 30 Tage.
macOS 10.14+	
	Nur überwacht: Zulassen, dass in der Nähe befindliche Geräte Anfragen nach einem Kennwort teilen
macOS 10.14.4+	
	• Screenshots zulassen • Fernüberwachung des Bildschirms erlauben **Nur überwacht:** • Automatisches Beitreten zum ClassRoom erlauben • Dem ClassRoom erlauben, eine Erlaubnis zum Verlassen des Unterrichts anzufordern. • ClassRoom erlauben, eine App und das Gerät ohne Aufforderung zu sperren. • Beobachtung verwalteter Klassenzimmergeräte ohne Aufforderung erzwingen
macOS 11.0+	
	Nur überwacht: Erzwungene Verzögerung von App-Software-Updates zulassen
macOS 11.3+	
	Erzwungener Fingerabdruck-Timeout Standardwert: 48 Stunden Voraussetzung: Berührungs-ID muss auf dem Gerät konfiguriert sein.
macOS 11.3+	
	Nur überwacht: • Erzwungene Software-Aktualisierung Große Verzögerung bei der Installation von Betriebssystemen

macOS-Version	Funktionen
	• Erzwungene Software-Aktualisierung Geringfügige Verzögerung bei der Installation von Betriebssystemen • Erzwungene Software-Aktualisierung ohne Verzögerung der Installation von Betriebssystemen • Verzögerung größerer Software-Aktualisierungen erzwingen
macOS 12+	• allowCloudPrivateRelay: Wenn Sie das private Relais auf einem macOS-Gerät aktivieren, wird der Netzwerkverkehr verschlüsselt und die Internetaktivität ist privat und sicher. Diese Einschränkung erfordert ein überwachtes Gerät. • iCloud Photo-Bibliothek zulassen **Nur überwacht**: • Löschen von Content und Einstellungen zulassen
macOS 13.0 bis 26.0	• Installation von Sicherheitsverbesserungen im Hintergrund zulassen: Zum Deaktivieren der Reaktionen. Der Benutzer kann keine Sicherheitsverbesserungen im Hintergrund installieren. • Entfernen von Sicherheitsverbesserungen im Hintergrund zulassen: Verhindert, dass Benutzer Reaktionen rückgängig machen können. Der Benutzer kann keine Sicherheitsverbesserungen im Hintergrund entfernen. • Universelle Kontrolle zulassen: ◦ Wenn **"wahr"**, lässt die Konfiguration zu, dass Sie über die Eingabegeräte des primären Geräts das sekundäre Anzeigegerät steuern. ◦ Wenn **"falsch"**, können Sie zwar ein sekundäres Anzeigegerät hinzufügen, dieses jedoch nicht über die primären Eingabegeräte steuern. **Nur überwacht**: • Installation des UI-Konfigurationsprofils zulassen: Wenn "falsch", lässt die Konfiguration keine Installation des Profils, der Konfiguration oder der Zertifikate auf dem macOS-Gerät zu. • Eingeschränkten USB-Modus zulassen: Wenn "wahr", lässt die Konfiguration nicht zu, dass das Gerät remote verbundene Eingabegeräte verwendet. Die Optionen für das Zulassen der Verbindung von Zubehör sind auf dem Gerät ausgegraut.
macOS 14.0+	• Änderung der ARD-Remote-Verwaltung zulassen ◦ Wenn "falsch", kann die Einstellung für die Freigabe der Remote-Verwaltung bei den Systemeinstellungen nicht geändert werden. ◦ Voreinstellung: true • Änderung der Bluetooth-Freigabe zulassen

macOS-Version	Funktionen
	◦ Wenn "falsch", kann die Bluetooth-Einstellung bei den Systemeinstellungen nicht geändert werden. ◦ Voreinstellung: true • Cloud Freeform zulassen ◦ Wenn "falsch", sind iCloud Freeform-Dienste nicht erlaubt. ◦ Voreinstellung: true • Änderung der Dateifreigabe zulassen ◦ Wenn "falsch", kann die Dateifreigabe-Einstellung bei den Systemeinstellungen nicht geändert werden. ◦ Voreinstellung: true • Änderung der Internetfreigabe zulassen ◦ Wenn "falsch", kann die Internetfreigabe-Einstellung bei den Systemeinstellungen nicht geändert werden. ◦ Voreinstellung: true • Lokale Benutzererstellung zulassen ◦ Wenn "falsch", können keine neuen Benutzer in den Systemeinstellungen angelegt werden. ◦ Voreinstellung: true • Änderung der Druckerfreigabe zulassen ◦ Wenn "falsch", kann die Druckerfreigabe-Einstellung bei den Systemeinstellungen nicht geändert werden. ◦ Voreinstellung: true • Ändern von Remote-Apple-Ereignissen zulassen ◦ Wenn "falsch", kann die Einstellung für die Freigabe von Remote-Apple-Ereignissen bei den Systemeinstellungen nicht geändert werden. ◦ Voreinstellung: true • Siri zulassen ◦ Voreinstellung: true • Änderung der Startfestplatte zulassen ◦ Wenn "falsch", kann die Einstellung für die Startfestplatte bei den Systemeinstellungen nicht geändert werden. ◦ Voreinstellung: true • Time Machine Backup zulassen ◦ Wenn "falsch", können die Time Machine-Einstellungen bei den Systemeinstellungen nicht geändert werden. ◦ Voreinstellung: true **Nur überwacht**: • Kontenänderung zulassen ◦ Wenn "falsch", wird die Modifizierung des Kontos verhindert. ◦ Voreinstellung: true • Modifikation des Gerätenamens zulassen

macOS-Version	Funktionen
	◦ Wenn "falsch", wird das Ändern des Gerätenamens verhindert. ◦ Voreinstellung: true • Modifikation von Touch-ID-Fingerabdrücken zulassen ◦ Wenn "falsch", wird das Ändern von Touch-ID-Fingerabdrücken verhindert. ◦ Voreinstellung: true
macOS 15.0+	**Nur überwacht**: • Genmoji zulassen ◦ Wählen Sie diese Option, um die Erstellung von Genmojis zuzulassen. ◦ Voreinstellung: true • Image Playground zulassen ◦ Wählen Sie diese Option, um die Bildgenerierung zuzulassen. ◦ Voreinstellung: true • iPhone-Spiegelung zulassen ◦ Wählen Sie diese Option, um die iPhone-Spiegelung auf einem macOS-Gerät zuzulassen. ◦ Voreinstellung: true • Schreibtools zulassen ◦ Wählen Sie diese Option, um Apple Intelligence-Schreibtools zu aktivieren. ◦ Voreinstellung: true
macOS 15.1+	**Nur überwacht**: • E-Mail-Zusammenfassung zulassen ◦ Wählen Sie diese Option aus, um das manuelle Zusammenfassen von E-Mail-Nachrichten zuzulassen. ◦ Voreinstellung: true • Ändern der Medienfreigabe zulassen ◦ Wählen Sie diese Option aus, um das Ändern der Einstellungen für die Medienfreigabe zuzulassen. ◦ Voreinstellung: true
macOS 15.2+	**Nur überwacht**: • Externe Datenintegrationen zulassen

macOS-Version	Funktionen
	◦ Wählen Sie diese Option aus, um die Verwendung externer, cloudbasierter Datendienste mit Siri zuzulassen. ◦ Voreinstellung: true • Anmeldung externer Datenintegrationen zulassen ◦ Wählen Sie diese Option aus, um das Festlegen eines anderen bevorzugten Standardbrowsers zuzulassen. Der Ivanti Neurons for MDM-Befehl zum Festlegen des bevorzugten Standardbrowsers funktioniert auch bei Anwendung dieser Option. ◦ Voreinstellung: true
macOS 15.3	
	Sicherheit und Privatsphäre: • Externe Intelligence Workspace-IDs zulassen ◦ Geben Sie die zulässige externe Intelligence Workspace-ID ein. • Zusammenfassung der Transskription in Notes zulassen ◦ Wählen Sie diese Option, um die Erstellung von Zusammenfassungen aus Transcriptions zuzulassen. ◦ Voreinstellung: true

10.10.4.37. macOS AppStore-Einschränkungen

Lizenz: Gold

Die macOS AppStore-Einschränkungen legen fest, welche Funktionen im macOS AppStore aktiviert werden.

Sie können folgende Optionen einstellen:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Konfigurations-Setup	
macOS-Version	**Funktionen**
10.9+	App-Installationen nur für Administratoren zulassen.
10.10+	• App-Installationen nur als Software-Updates zulassen. • App-Akzeptanz durch die Benutzer deaktivieren. • Software-Update-Benachrichtigungen deaktivieren.
10.11+	App-Installation auf über MDM-installierte Apps und Software-Updates beschränken.

Konfiguration verteilen

Verfahren

1. Stellen Sie die Optionen anhand der vorstehenden Tabelle ein.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie die Option **Diese Konfiguration aktivieren**.
4. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar

Klicken Sie auf **Fertig**.

10.10.4.38. Beschränkungen beim Brennen von CDs/DVDs in macOS

Lizenz: Gold

Die Beschränkungen beim Brennen von CDs/DVDs in macOS verwalten die Einschränkungen zum Brennen von Datenträgern in macOS. Sie können die **macOS-Findereinstellungen** so konfigurieren, dass Datenträger über die Finder-App in macOS gebrannt bzw. nicht gebrannt werden können.

Sie können folgende Optionen einstellen:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Konfigurations-Setup	
Einstellung	**Aktion**
Brennen von Datenträgern zulassen	• EIN • AUS • [Require Authentication]

Konfiguration verteilen

Verfahren

1. Stellen Sie die Optionen anhand der vorstehenden Tabelle ein.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie die Option **Diese Konfiguration aktivieren**.
4. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar

Klicken Sie auf **Fertig**.

10.10.4.39. Kontrolle zulässiger Medien (zurückgestuft)

Lizenz: Gold

Die Konfiguration für die Kontrolle zulässiger Medien verwaltet die Anmeldung, Abmeldung und den Auswurf nach der Deaktivierung für verschiedene physische Medien in macOS.

Sie können folgende Optionen einstellen:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Konfigurations-Setup **Anmeldekontrolle für Medienarten** Aktivieren Sie die Anmeldekontrolle für jede Medienart und definieren Sie die Anmeldeeinstellungen. Wenn Sie die Anmeldekontrolle deaktivieren, gilt die Standardeinstellung des Betriebssystems.	
Medienart	**Anmeldeeinstellungen**
• CD • DVD • BD	• Schreibgeschützt mit Authentifizierung • Anmeldung verweigern • Datenträger auswerfen
• Leere CD • Leere DVD • Leere BD • DVD-RAM • Festplattenimage • Interne Festplatte • Externe Festplatte • Netzwerk-Laufwerk • Externe Festplatten sind USB-Festplatten, USB-Flash-Speicher und SD-Karten. • Schreibgeschützte Datenträger, wie CD, DVD und BD werden standardmäßig schreibgeschützt angemeldet.	• Schreibgeschützt • Anmeldung verweigern • Datenträger auswerfen • Authentifizieren
Abmeldekontrolle für Medienarten Aktivieren Sie die Abmeldekontrolle für jede Medienart und definieren Sie die Abmeldeeinstellungen. Wenn Sie die Abmeldekontrolle deaktivieren, gilt die Standardeinstellung des Betriebssystems. Überlegen Sie genau, ob und wann Sie die Einstellung „Abmelden verweigern“ für Medienarten definieren.	
Medienart	**Anmeldeeinstellungen**

Einstellung	So gehen Sie vor
• CD • DVD • BD • Leere CD • Leere DVD • Leere BD • DVD-RAM • Festplattenimage • Interne Festplatte • Externe Festplatte • Netzwerk-Laufwerk **Bei Abmeldung auswerfen** Die Medienarten werden automatisch ausgeworfen, wenn sich der Benutzer abmeldet. **Medienart** • CD • DVD • BD • Leere CD • Leere DVD • Leere BD • DVD-RAM • Festplattenimage • Externe Festplatte • Netzwerk-Laufwerk	• Abmelden verweigern • Authentifizieren

Konfiguration verteilen

Verfahren

1. Stellen Sie die Optionen anhand der vorstehenden Tabelle ein.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie die Option **Diese Konfiguration aktivieren**.
4. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar

Klicken Sie auf **Fertig**.

10.10.4.40. Einstellungen für macOS Finder

Lizenz: Gold

Die macOS-Findereinstellungen verwalten die Einstellungen der Finder-App in macOS.

Sie können folgende Optionen einstellen:

Einstellung	**So gehen Sie vor**
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Konfigurations-Setup	
Einstellung	**Aktion**
Unterstützung des Brennens von Datenträgern im Finder deaktivieren	• Einschalten • Ausschalten

Konfiguration verteilen

Verfahren

1. Stellen Sie die Optionen anhand der vorstehenden Tabelle ein.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie die Option **Diese Konfiguration aktivieren**.
4. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar

Klicken Sie auf **Fertig**.

10.10.4.41. Erweiterungsrichtlinie für den macOS Kernel

Gilt für: macOS 10.13.2 oder unterstützte neuere Versionen.

Beschränkungen der Kontrollen und Einstellungen zum Laden der vom Benutzer genehmigten Kernel-Erweiterungen.

Konfiguration für macOS Kernel-Erweiterungsrichtlinie erstellen

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Tippen Sie in dem Suchfeld **Kernel** ein und klicken Sie dann auf die Konfiguration **macOS Kernel Erweiterungsrichtlinie**.
4. Bezeichnen und beschreiben Sie die Konfiguration.
5. Wählen Sie die Option **Überschreiben durch Benutzer zulassen**, damit die Benutzer zusätzliche Kernel-Erweiterungen genehmigen können, die nicht explizit in der folgenden Konfiguration zugelassen sind.
6. Klicken Sie in dem Abschnitt "Erlaubte Teamidentifikatoren und Kernel-Erweiterungen" auf **+Hinzufügen**, damit erlaubte Teamidentifikatoren und Kernel-Erweiterungen ergänzt werden können. Eine Kernel-Erweiterung ist eine Bundle-ID eines Pakets. Für jede Team-ID können Sie mehrere Kernel-Erweiterungsnamen mit gültiger Signatur in dem Popup-Fenster ergänzen.
7. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
9. Klicken Sie auf Fertig.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.4.42. Mobile@Work für macOS

Dieser Abschnitt enthält die folgenden Themen:

- Konfiguration und Skriptausführung von Mobile@Work für macOS
- Mobile@Work für macOS-Konfiguration erstellen
- Benutzer-Onboarding für macOS-Geräte aktivieren
- Konfiguration von Mobile@Work for macOS Script erstellen
- Saubere Deinstallation von Mobile@Work für macOS durchführen
- Anwenden von Skripten über macOS Mobile@Work

Ivanti Neurons for MDM ermöglicht Ihnen, eigene macOS-Shell-Skripte zu erstellen, die Sie dann in Ivanti Neurons for MDM hochladen und auf verwalteten macOS-Geräten starten können. Informationen zum Erstellen, Hochladen und Verwalten der Skript-Repository finden Sie unter Alle Scripts.

Ein macOS-Gerätebenutzer kann die Abschaltung des Geräts mit Mobile@Work für macOS 1.1 oder höher veranlassen. Die Option „Außer Dienst stellen" ist verfügbar, wenn Sie im Bildschirm „Über Mobile@Work" auf **Deinstallieren** klicken. In der Ivanti Neurons for MDM können Sie den Status des Geräts auf der Seite **Geräte** und auf der Seite mit den Gerätedetails überprüfen.

Mobile@Work für macOS 1.5 oder höher öffnet Apps@Work sofort nach der Registrierung, ohne auf den Abschluss der MDM-Registrierung zu warten.

Klicken Sie in Mobile@Work für MacOS auf eine Anwendungskachel, um die Seite App Details für diese Anwendung anzuzeigen. Die Seite enthält App-Beschreibung, Screenshots, Bewertungen und Rezensionen.

Mobile@Work für macOS benachrichtigt den Server Ivanti Neurons for MDM, ob die internen Packager-macOS-Apps im Bestandsbericht installiert sind.

Voraussetzungen

Im App-Katalog ist der Mobile@Work für macOS-Client als Business-App verfügbar. Bevor Sie Shell-Skripte auf MacOS-Geräten ausführen können, weisen Sie die Benutzer an, ihre Geräte mit Ivanti Neurons for MDMMobile@Work für MacOS zu registrieren.

Verfahren

1. Laden Sie Mobile@Work für die macOS-Anwendung herunter. Verfügbar als PKG-Dtaei unter https://support.mobileiron.com/support/CDL.html. In diesem Artikel bei den Ivanti Kundenforen erhalten Sie Informationen zum Erhalt der Anmeldeinformationen für die Download-Site.
2. Laden Sie die PKG-Datei für Mobile@Work für macOS auf einen sicheren Server. Dieser Server muss für die Gerätebenutzer zugänglich sein.
3. Teilen Sie die URL der Installationsdatei für Mobile@Work für macOS mit den Gerätebenutzern per E-Mail oder Mitteilung.
4. Weisen Sie die Benutzer an:
    1. Laden Sie Mobile@Work for macOS herunter und installieren Sie die App auf dem Gerät.
    2. Registrieren Sie die Geräte mit Ivanti Neurons for MDM mit Mobile@Work für macOS.

Konfiguration und Skriptausführung von Mobile@Work für macOS

Verfahren

1. Definieren Sie die Mobile@Work-Konfiguration für MacOS und verteilen Sie diese.
2. Richten Sie eine Mobile@Work for macOS-Skriptkonfiguration ein und verteilen Sie sie, um das Skript zu Ivanti Neurons for MDM hochzuladen. Die Skripts sind verschlüsselt und mit einem signierten Zertifikat gesichert, das für den Mandanten eindeutig ist. Der Schlüssel zur Entschlüsselung des Skripts wird zusammen mit der verschlüsselten und signierten URL zum Download des Skripts an das Gerät gesendet.
3. Ivanti Neurons for MDM führt die Scripts auf macOS-Geräten mit Mobile@Work für macOS aus. Mobile@Work für macOS fragt Ivanti Neurons for MDM regelmäßig ab, um zu prüfen, ob Scripts auf die Ausführung warten. Wenn sich Scripts in der Warteschlange befinden, lädt Mobile@Work die Scripts auf die macOS-Geräte herunter und führt sie entsprechend den von Ihnen in der Ivanti Neurons for MDM festgelegten Einstellungen aus.
4. Mobile@Work für macOS gibt die Ergebnisse der Scriptausführung zurück an Ivanti Neurons for MDM. Diese werden dann in den Geräteprotokollen angezeigt. Sie können die Geräteprotokolle über die Seite Gerätedetails des macOS-Geräts auf der Registerkarte **Protokolle** kontrollieren.

Mobile@Work für macOS-Konfiguration erstellen

Für Mobile@Work und macOS steht eine Standardsystemkonfiguration zur Verfügung. Sie wird jedoch nicht standardmäßig auf die Geräte verteilt.

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie **work** in das Suchfeld ein und klicken Sie dann auf die Konfiguration **Mobile@Work for macOS**.
4. Bezeichnen und beschreiben Sie die Konfiguration.
5. Gebe Sie für **Max. Ausführungszeit** an, wie viele Sekunden ein Script ausgeführt werden darf. Der Standardwert sind 60 Sekunden.
6. Geben Sie die **Max. Antwortgröße** in Kilobyte (KB) ein, um die maximale Antwortgröße der Script-Ausgabe zu begrenzen, die an die Ivanti Neurons for MDM zurückgegeben wird. Dies sind die stdout- bzw. die stderr-Daten, die bei Ausführung des Scripts zurückgeliefert werden. Der Standardwert ist 1 KB.
7. Geben Sie die **Anmeldehäufigkeit** in Minuten ein, um festzulegen, wie oft Mobile@Work für macOS-App sich bei Ivanti Neurons for MDM anmelden muss. Der Standardwert ist 15 Minuten.
8. (Optional) Sie können das Benutzer-Onboarding für macOS-Geräte aktivieren, indem Sie den Abschnitt **Benutzer-Onboarding für macOS-Geräte aktivieren** verwenden.
9. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
    1. Wählen Sie eine Verteilungsebene:
    2. **Für alle** - Die App wird bei allen benutzerkompatiblen Geräten hinzugefügt.
    3. **Für niemand** - Die Verteilung der App wird auf später verschoben.
    4. **Benutzerdefinierte Verteilung** - Wählen Sie eine der folgenden Optionen:
        - **Benutzer/Benutzergruppen** - Die Anwendung wird nur an die von Ihnen ausgewählten Benutzer oder Benutzergruppen verteilt.
          Klicken Sie auf die Registerkarte **Benutzer**, um die Benutzer auszuwählen.
          Klicken Sie auf die Registerkarte **Benutzergruppen**, um die Benutzergruppe(n) auszuwählen.
        - **Geräte/Gerätegruppen** - Die App wird nur an die von Ihnen ausgewählten Geräte oder Gerätegruppen verteilt
          Klicken Sie auf die Registerkarte **Geräte**, um die Geräte auszuwählen.

Klicken Sie auf die Registerkarte **Gerätegruppen**, um die Gerätegruppe(n) auszuwählen.

10. Klicken Sie auf Fertig.

Benutzer-Onboarding für macOS-Geräte aktivieren

Sie können das Benutzer-Onboarding für macOS-Geräte während des automatischen Geräteanmeldungsprozesses wie folgt aktivieren:

- Sobald die Geräteregistrierung abgeschlossen ist, wird Mobile@Work für MacOS (Version 1.68 oder höher erforderlich) zusammen mit den Profilen, Konfigurationen und Anwendungen per Push auf das Gerät übertragen.
- Mobile@Work for macOS-Client und andere Apps werden nur dann per Push auf die Geräte übertragen, wenn:
  - Die Apps entweder unternehmensinterne PKG-Apps oder öffentliche Apps von Apple Apps and Books sind.
  - Die Einstellung für die Installation der Apps im Hintergrund auf „true“ gesetzt ist. Die Einstellung ist auf der Seite **Apps** >App-Details >**App-Konfiguration** >**Auf dem Gerät installieren** verfügbar ist.
  - Die Priorität von **für die Apps** auf „High“ gesetzt ist. Die Mobile@Work for macOS-Client-App hat standardmäßig eine hohe Priorität (die nicht geändert werden kann), **da sonst der Onboarding-Prozess für den Benutzer fehlschlagen kann**.
  - Die Apps sind so konfiguriert, dass sie an die Geräte, Benutzer- oder Gerätegruppen verteilt werden können.
- Sobald Mobile@Work für macOS installiert und registriert ist, geht das macOS-Gerät in den Kiosk-Modus über (der Benutzer hat keine Kontrolle über das Gerät), bis die übrigen Profile, Konfigurationen und Apps konfiguriert und installiert sind. Der Fortschritt schrittweise angezeigt wird.

Für Mobile@Work für macOS 1.73 oder höhere Versionen, die von Ivanti Neurons for MDM unterstützt werden, werden die folgenden Zusatzfunktionen unterstützt:

- Der Onboarding-Prozess für den Benutzer ist abgeschlossen, sobald die Geräteregistrierung für ein Gerät abgeschlossen ist. Der Benutzer-Onboarding-Prozess startet nicht, wenn das Zeitfenster zum Start des Benutzer-Onboarding abgelaufen ist (typischerweise 20 Minuten nach der Geräteregistrierung) selbst wenn ein Administrator das Benutzer-Onboarding in der Mobile@Work-Konfiguration aktiviert. Dadurch wird verhindert, dass ein Gerät in den Kioskmodus für das Benutzer-Onboarding wechselt, wenn das Gerät regelmäßig verwendet wird.
- Der Onboarding-Prozess des Benutzers wird in Mobile@Work for den macOS-Client schrittweise angezeigt. Die Konfigurationen werden als Teil des ersten Schritts installiert.
- Apps mit hoher Priorität werden zuerst installiert. Jede App mit hoher Priorität wird als ein Schritt gezählt. Packager-Apps werden nicht als Teil der Schritte gezählt.
- Die übrigen Apps werden im Hintergrund installiert, auch wenn das Benutzer-Onboarding abgeschlossen ist. Apps werden als installiert markiert, nachdem die Installation auf einem Gerät initialisiert oder die App tatsächlich auf dem Gerät installiert wurde.
- Nach dem Benutzer-Onboarding können Sie zur Seite mit den Gerätedetails gehen, um die Konfigurationen und Apps zu überprüfen, die per Push auf jedes Gerät übertragen wurden. Weitere Informationen finden Sie in den Protokollen.

Verfahren

1. Erstellen Sie eine Mobile@Work für macOS-Konfiguration mit der Option **Mobile@Work für macOS-Konfiguration erstellen**.
2. Wählen Sie die Option Benutzer-Onboarding aktivieren.
3. Geben Sie folgende Details ein:
   - **Timeout-Wert für Benutzer-Onboarding** - Geben Sie die ungefähre Zeit ein, die das Gerät benötigt, um die App und die Konfigurationen bei der Ersteinrichtung des Geräts zu installieren. Standardmäßig dauert der Onboarding-Prozess des Benutzers auf einem macOS-Gerät 120 Sekunden, diese Zeit können Sie nach Bedarf ändern.

- **URL der Benutzer Landing Page**- Geben Sie die URL einer Landing Page an, die dem Benutzer nach dem Onboarding angezeigt wird.

4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
5. Klicken Sie auf Fertig.

Konfiguration für Mobile@Work und macOS Script erstellen

Sie können mehrere Skript-Konfigurationen für Mobile@Work for macOS erstellen und auf den Geräten verteilen. Mit dieser Konfiguration können Sie ein Skript aus dem Repository (**Admin > Skripte und Dateien > Alle Skripte**) auswählen, um es an Mobile@Work for macOS zu verteilen.

Sie können Skriptausführungen auf Geräten mit Mobile@Work für macOS 1.66 oder höher planen. Wenn Sie eine Skriptausführung für die Ausführung auf Geräten mit Mobile@Work für MacOS-Client-Versionen vor 1.66 planen, wird das Skript nur einmal ausgeführt. Wenn der Mobile@Work for macOS-Client von 1.4 auf 1.66 aktualisiert wird, werden alle MacOS-Client-Konfigurationen neu auf die Geräte verteilt.

Voraussetzungen

- Wechseln Sie zu **Admin > Skripte und Dateien > Alle Skripte**, um Skripte hochzuladen und zu verwalten, die in dieser Konfiguration verwendet und auf Geräte verteilt werden können.
- Konfigurieren und verteilen Sie die Mobile@Work for macOS-Konfiguration auf Geräte. Andernfalls meldet die Konfiguration des Skripts Mobile@Work for macOS einen Fehler.

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie **work** in das Suchfeld ein und klicken Sie dann auf die Konfiguration des Skripts **Mobile@Work for macOS**.
4. Bezeichnen und beschreiben Sie die Konfiguration.
5. Geben Sie in dem Feld **Skript auswählen** den Namen des zu suchenden Skripts ein und wählen Sie das Skript aus der Dropdown-Liste aus.
6. Im Abschnitt Skripteingabe werden die Skripteingabe-Labels und Skriptvariablen für das Skript angezeigt. Wenn Sie diese überschreiben müssen, geben Sie alternative Skriptvariablen (z.B. {$userWorkEmailAddress}) und ihre alternativen Standardwerte ein (z.B. john.doe@company.com).
7. Wählen Sie im Abschnitt „Skriptausführung“ eine der folgenden Planungsoptionen aus:
   - Einmalige Ausführung bei der Bereitstellung
   - Wiederkehrende Ausführung
8. Wenn Sie „Wiederkehrende Ausführung“ auswählen, geben Sie die folgenden Details an:
   - Zu verwendende Zeitzone - Wählen Sie die Ortszeit des Geräts oder die UTC-Zeit. Das Skript wird zu dem in diesem Feld ausgewählten Zeitpunkt ausgeführt.
   - Ausführung beginnt am - Wählen Sie das Startdatum aus.
   - Ausführung endet am - Wählen Sie das Enddatum aus (größer oder gleich dem Startdatum).
   - Skript ausführen - Wählen Sie „Täglich“ oder „Wöchentlich“ und geben Sie die Stunden (im 24-Stunden-Format), Minuten bzw. Tage ein.
9. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.

10. Klicken Sie auf Fertig.

Saubere Deinstallation von Mobile@Work für macOS durchführen

Wenn Sie die Option **Apps bei Abmeldung entfernen(Gilt nur für verwaltete Apps)** während der Installation von Mobile@Work für macOS aktiviert haben und wenn Sie das Gerät über das Cloud-Administrator-Portal außer Dienst stellen, wird die Mobile@Work für macOS-Anwendung und das Deinstallationsskript einfach vom Gerät gelöscht. Um zu verhindern, dass die Prozesse und Skripte im Backend ausgeführt werden, stellen Sie sicher, dass Sie während der Geräteregistrierung neuer Benutzer oder der Außerdienststellung bestehender Benutzer die folgende Option im Cloud-Administrator-Portal deaktivieren, damit das Deinstallationsskript ausgeführt wird und die zugehörigen Prozesse und Skripte aus dem Backend löscht.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administratorportal an.
2. Gehen Sie zu **Apps** > **Mobile@Work** > **App-Konfigurationen** > **Zusammenfassung der App-Konfigurationen** > **Apple App-Einstellungen** >**Konfigurationseinstellungen der Apple App-Verwaltung**.
3. Deaktivieren Sie auf der Seite **Konfigurations-Setup** die folgende Option:
    - **Apps bei Abmeldung entfernen (gilt nur für verwaltete Apps)**.

Anwenden von Skripten über macOS Mobile@Work

Mit **Skripte über macOS Mobile@Work** können Administratoren Shell-Skripte remote auf verwalteten macOS-Geräten bereitstellen und ausführen. Dies hilft bei der Automatisierung von Aufgaben, der Anwendung von Korrekturen, der Durchsetzung von Richtlinien und der Optimierung der Konfiguration, ohne dass ein Benutzereingriff erforderlich ist, und gewährleistet eine konsistente und effiziente Geräteverwaltung in großem Maßstab.

Voraussetzungen:

- Auf Geräten muss macOS ausgeführt werden.
- Mobile@Work für macOS muss bereits auf den Geräten installiert sein.
- Stellen Sie sicher, dass die Mobile@Work for macOS-Konfiguration ordnungsgemäß erstellt, verteilt und zugewiesen wurde. Weitere Details finden Sie unter **Erstellen einer Mobile@Work für macOS-Konfiguration**.

> Sie können Skripte nicht über macOS Mobile@Work anwenden, wenn auf dem Gerät der Mobile@Work-Client nicht installiert und konfiguriert ist oder wenn die Geräteplattform keine Skriptausführung unterstützt. Stellen Sie sicher, dass der macOS-Client aktiv ist und dass Sie nur unterstützte macOS-Geräte auswählen.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administratorportal an.
2. Wechseln Sie zu **Geräte** und wählen Sie die Liste der macOS-Geräte aus, für die Sie das Skript ausführen möchten.
3. Navigieren Sie auf der Seite **Geräte** zu **Aktionen** > **macOS** > **Skripte über macOS Mobile@Work**.
   Der Bereich **Skripte über macOS Mobile@Work** wird angezeigt.
4. Geben Sie zum Anwenden der Skripte im Feld **Skript auswählen** den Skriptnamen ein und wählen Sie ihn aus.
   Weitere Informationen zum Erstellen eines Skripts finden Sie unter **Alle Skripte**.
5. Wählen Sie **OK**, um das Skript auf den Geräten auszuführen.

Verwandte Themen:

- Admin > Skripte und Dateien > Alle Skripte
- Erstellen einer Konfiguration

10.10.4.43. Konfiguration der Update-Regeln für macOS Software

Administratoren können die Software-Update-Richtlinie eines Geräts mit den **macOS Software-Aktualisierungsregeln** konfigurieren.

Gilt für: macOS 10.7 bis 26.0.

1. Gehen Sie zu Konfigurationen > +Hinzufügen.
2. Geben Sie macOS in das Suchfeld ein und klicken Sie dann auf die Konfiguration macOS Software-Aktualisierungseinstellungen.
3. Geben Sie einen Namen und eine Beschreibung der Konfiguration ein.
4. Wählen Sie die gewünschten Konfigurationen unter **macOS Software-Aktualisierungsregeln** aus.
5. Klicken Sie auf Weiter.
6. Wählen Sie die Option Diese Konfiguration aktivieren.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
8. Klicken Sie auf Fertig.

macOS Software-Aktualisierungsregeln

Admins können aus der Regelliste wie folgt auswählen:

> Die Benutzer können diese Einstellungen nicht ändern, wenn diese Regeln für das Gerät übernommen werden.

- Installation von Vorabversionen von Software erlauben
- Automatisch:
    - Auf Updates prüfen
    - Neue Updates herunterladen, sobald sie verfügbar sind.
    - macOS-Updates installieren
    - App-Updates aus dem App-Store installieren
    - Systemdateien und Sicherheitsupdates installieren
- App-Installationen nur für Administratoren zulassen
- Option zur Ergänzung der URL des Software-Aktualisierungskatalogs (nicht unterstützt unter macOS 11+).

10.10.4.44. Zertifikatspräferenz

Gilt für:

- macOS 10.12 bis zur letzten aktuellen Version, die von Ivanti Neurons for MDM unterstützt wird.

Identifizieren Sie einen Zertifikatspräferenzeintrag in der Schlüsselkette des Benutzers, der sich auf die Zertifikats-Payload in dem gleichen Profil bezieht.

Mit dieser Funktion wird ein Zertifikat entweder an eine E-Mail-Adresse oder an eine URL gebunden. Sobald Sie ein Zertifikat an eine E-Mail-Adresse gebunden haben, wird es von der Mail-App für dieses E-Mail-Konto verwendet. Wenn ein SSL-Zertifikat für eine Website nicht vertrauenswürdig ist, wird mit einer hinzugefügten Zertifikatspräferenz sichergestellt, dass der Browser keine Warnmeldung einblendet, wenn Sie versuchen, auf die Website zuzugreifen.

> Administratoren benötigen ein Zertifikat. Weitere Informationen zum Hinzufügen und Verteilen eines Zertifikats finden Sie unter **Zertifikatskonfiguration**.

Zertifikatspräferenzkonfiguration erstellen

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie in dem Suchfeld **preference** ein und klicken Sie dann auf die Konfiguration **Zertifikatspräferenz**.
4. Bezeichnen und beschreiben Sie die Konfiguration.
5. Geben Sie im Abschnitt „Konfigurations-Setup“ im Feld **Name** eine E-Mail-ID oder einen Namen ein, für den ein bevorzugtes Zertifikat angefordert wird.
6. Wählen Sie im Feld **Zertifikat-UUID** ein Zertifikat aus.
7. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
8. Klicken Sie auf Fertig.

Verwandte Themen:

- **Identitätspräferenz**
- **Zertifikatskonfiguration**
- **Erstellen einer Konfiguration**

10.10.4.45. Active Directory (macOS)

Gilt für: macOS 10.9 oder unterstützte neuere Versionen.

Konfigurieren Sie erweiterte Optionen, um macOS-Geräte an eine Domain mit Active Directory (AD) zu binden, damit Sie auf Softwaredienste zugreifen können, die Active Directory für die Authentifizierung und Sicherheit benötigen.

Dieser Abschnitt enthält die folgenden Themen:

- Active Directory-Konfiguration erstellen
- Active Directory-Einstellungen

Active Directory-Konfiguration erstellen

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie in dem Suchfeld **Datenschutz** ein und klicken Sie dann auf die Konfiguration **Active Directory**.
4. Bezeichnen und beschreiben Sie die Konfiguration.
5. Geben Sie die Einstellungen wie in der folgenden Tabelle für Active Directory-Einstellungen ein.
6. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
7. Klicken Sie auf **Fertig**.

Active Directory-Einstellungen

Einstellung	Aktion
Active Directory-Einstellungen – Grundlagen	
[Hostname]	(Erforderlich) Geben Sie den Host-Namen ein, das heißt die Active Directory-Domain, der Sie sich anschließen wollen.
Benutzername	Geben Sie den Benutzernamen des Kontos ein, das Sie für die Registrierung bei der Domain verwendet haben.
Passwort	Geben Sie das Passwort des Kontos ein, das Sie bei der Registrierung für die Domain verwendet haben.
AD-Organisationseinheit	Geben Sie die Organisationseinheit (OU) ein, der das betreffende Computerobjekt hinzugefügt wird.
AD-Mount-Stil	Wählen Sie eine der folgenden Optionen aus, um anzugeben, welches Netzwerkprotokoll verwendet werden soll: • AFP • SMB
Active Directory-Einstellungen – erweiterte Einstellungen	
ADCreateMobileAccountAtLogin-Schlüssel aktivieren	Den Schlüssel ADCreateMobileAccountAtLogin aktivieren oder deaktivieren. Zusatzoption: Erstellen Sie ein Mobilgerätekonto bei der Anmeldung.
ADWarnUserBeforeCreatingMA-Schlüssel aktivieren	Den Schlüssel ADWarnUserBeforeCreatingMA aktivieren oder deaktivieren. Zusatzoption: Warnen Sie den Benutzer, bevor ein Mobilgerätekonto erstellt wird.
ADForceHomeLocal-Schlüssel aktivieren	Den Schlüssel ADForceHomeLocal aktivieren oder deaktivieren. Zusatzoption: Lokales Home-Verzeichnis erzwingen.
ADUseWindowsUNCPath-Schlüssel aktivieren	Den Schlüssel ADUseWindowsUNCPath aktivieren oder deaktivieren. Zusatzoption: UNC-Pfad von AD zu dem abgeleiteten Netzwerkstandort verwenden.
ADAllowMultiDomainAuth-Schlüssel aktivieren	Den Schlüssel ADAllowMultiDomainAuth aktivieren oder deaktivieren. Zusatzoption: Authentifizierung von jeder Domain im Forest erlauben.
Standard-Benutzer-Shell	Geben Sie die Standard-Benutzer-Shell ein, beispielsweise /bin/bash.
Ordnen Sie die Benutzer-UID dem Attribut zu.	Wählen Sie diese Option, um die Benutzer-UID dem betreffenden Attribut zuzuordnen.
Benutzer-GID Attribut zuordnen	Wählen Sie diese Option, um die Benutzer-GID dem angegebenen Attribut zuzuordnen.
Gruppen-GID Attribut zuordnen	Wählen Sie diese Option, um die Gruppen-GID dem ausgewählten Attribut zuzuordnen.
Bevorzugter Domainserver	Diesen Domainserver bevorzugen.
Namespace-Konvention	Wählen Sie eine der folgenden Bezeichnungskonventionen für das Benutzerkonto aus:

Einstellung	Aktion
	• Domain (Standard) • Forest
Paketsignierung	Wählen Sie eine der folgenden Paketsignieroptionen aus: • Zulassen (Standard) • Deaktivieren • Erforderlich
Paketverschlüsselung	Wählen Sie eine der folgenden Paketverschlüsselungsoptionen aus: • Zulassen (Standard) • Deaktivieren • Erforderlich • SSL
Verwaltung durch angegebene Active Directory-Gruppen zulassen	Wählen Sie diese Option, wenn Sie die Verwaltung durch bestimmte Active Directory-Gruppen zulassen wollen. Klicken Sie auf **Hinzufügen**, um eine oder mehrere Gruppen hinzuzufügen.
Dynamische DNS beschränken	Wählen Sie diese Option, um dynamische DNS-Updates für die angegebenen Schnittstellen zu beschränken (beispielsweise, en0, en1usw.). Klicken Sie auf **Hinzufügen**, um einen oder mehrere Schnittstellenbezeichnungen hinzuzufügen.
Passwortintervall ändern	Geben Sie an, wie oft (in Tagen) eine Änderung des Passwortes für das vertrauenswürdige Konto des Computers erforderlich ist. Der Wert null ist deaktiviert.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.4.46. Identitätspräferenz

Gilt für: macOS 10.12 oder unterstützte neuere Versionen.

Identifizieren Sie einen Identitätspräferenzeintrag in der Schlüsselkette des Benutzers, der sich auf die Identitäts-Payload in dem gleichen Profil bezieht.

In MacOS können Sie mit einer Identitätspräferenz auswählen, mit welcher Identität (mit welchem Schlüsselpaar) Sie eine Website nutzen wollen. Wenn Sie eine Identitätspräferenz (bestehend aus URL und Identität) per PUSH auf das Gerät übertragen haben, wird diese unter **Keychain-Zugriff → Alle Objekte** angezeigt („Art" ist die „Identitätspräferenz"). Wenn Sie das nächste Mal über Safari diese URL aufrufen, präsentiert das Gerät das konfigurierte Zertifikat.

Ivanti Neurons for MDM erstellt eine Standardkonfiguration für die Systemidentitätspräferenz mit einer Anwendung für die AppStore-URL und das zu verwendende Zertifikat.

Beim Zugriff auf den macOS App-Katalog mit Safari unter macOS 10.12 und höher wird der Benutzer aufgefordert, das Identitätszertifikat mit einem Systempasswort zwischenzuspeichern. Benutzer müssen beim ersten Mal „Immer zulassen" auswählen, um spätere Eingabeaufforderungen beim Zugriff auf den macOS-App-Katalog zu vermeiden.

Safari mit einer MacOS-Version unter 10.12 und andere Browser zeigen in einer neuen Browsersitzung auf MacOS-Geräten Eingabeaufforderungen für das Zertifikat und das Systempasswort an, wenn sie auf den MacOS-App-Katalog zugreifen.

Identitätspräferenzkonfiguration erstellen

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie in dem Suchfeld **preference** ein und klicken Sie dann auf die Konfiguration der **Identitätspräferenz**.
4. Bezeichnen und beschreiben Sie die Konfiguration.
5. Geben Sie im Abschnitt „Konfigurations-Setup" im Feld **Name** eine E-Mail-ID, einen DNS-Hostnamen oder einen Namen ein, der den Dienst eindeutig identifiziert.
6. Wählen Sie im Feld **Zertifikat-UUID** ein Zertifikat aus.
7. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
8. Klicken Sie auf Fertig.

Verwandte Themen:

- Zertifikatspräferenz
- Erstellen einer Konfiguration

10.10.4.47. Automatische Kontoerstellung für Office 365 (macOS)

Gilt für:

- Unterstützte macOS-Geräte.
- Für Microsoft Office 365 werden die Versionen ab 16.13.X empfohlen.

Konfigurieren Sie die Benutzerinformationen und Optionen für die Erstkonfiguration aller Anwendungen von Microsoft Office 365.

Dieser Abschnitt enthält die folgenden Themen:

- Konfiguration zur automatischen Kontoerstellung für Office 365 erstellen
- Einstellungen zur automatischen Kontoerstellung für Office 365

Konfiguration zur automatischen Kontoerstellung für Office 365 erstellen

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie in dem Suchfeld **Office** ein und klicken Sie dann auf die Konfiguration **Automatische Kontoerstellung für Office 365**.
4. Bezeichnen und beschreiben Sie die Konfiguration.
5. Geben Sie die Einstellungen wie in der folgenden Einstellungstabelle für die automatische Kontoerstellung für Office 365 ein.
6. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
7. Klicken Sie auf **Fertig**.

Einstellungen zur automatischen Kontoerstellung für Office 365

Einstellung	Aktion
Office-Aktivierungs-E-Mail-Adresse	Geben Sie die E-Mail-Adresse des Benutzers ein.
Automatische Anmeldung für Office	Wählen Sie die Option, um die Fenster für den Erststart zu unterdrücken. Fragt vom Benutzer nur die obligatorischen Informationen, beispielsweise die Authentifizierung für Office 365 ab.
Standardmäßig lokal öffnen / speichern	Wählen Sie die Option, um in dem Fenster zum Öffnen und Speichern die Option "Auf meinen Mac" statt "Online-Speicher" auszuwählen.
Beim Start anzeigen, was neu ist.	Wählen Sie die Option, um die neuen Funktionsanzeigen beim Start einzublenden.
Visual Basic Macro - Ausführungsstatus	Wählen Sie eine der folgenden Optionen aus: • Mit Warnungen deaktiviert • Ohne Warnungen deaktiviert • Ohne Warnungen aktiviert
Externe dynamische Bibliotheken von Visual Basic deaktivieren	Wählen Sie die Option, um die externen Abhängigkeiten von Visual Basic zu deaktivieren.
Visual Basic zum Binden von System zulassen	Wählen Sie die Option, damit die Macros den Befehl DECLARE verwenden können, um sich mit system () an die API des Betriebssystems zu binden. Mit dieser API können die Macros beliebige externe Prozesse ausführen und beliebige Daten auf der Befehlszeile übergeben.
Visual Basic deaktivieren, um an Popen zu binden	Wählen Sie die Option, damit die Macros den Befehl DECLARE können, um sich mit popen () an die API des Betriebssystems zu binden. Mit dieser API können die Macros beliebige externe Prozesse ausführen und beliebige Daten auf der Befehlszeile übergeben.
Visual Basic-Mac-Script deaktivieren	Wählen Sie die Option, damit die Macros die Apple Script Visual Basic API aufrufen können.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.4.48. Authentifizieren

Gilt für:

- macOS 10.13 und unterstützte neuere Versionen.
- Windows 10 und unterstützte neuere Versionen.

Verwenden Sie die Konfiguration „Authentifizierung“, um eine passwortlose Authentifizierung für Cloud-Dienste und/oder Desktop-Anmeldungen bereitzustellen. Jedes Gerät hat nur eine Authentifizierungskonfiguration.

Voraussetzungen

- Eine Zero-Sign-On-Lizenz ist erforderlich.
- Ivanti Neurons for MDM sollte bei Access registriert sein (das Access-Profil sollte konfiguriert sein).
- Nach der Konfiguration der Authentifizierungskonfiguration können Sie die Registrierung des Zugriffsprofils nicht aufheben, da die Authentifizierungskonfiguration das Zugriffsprofil referenziert.
- Wenn das Zugriffsprofil Änderungen aufweist, verteilen Sie die Authentifizierungskonfiguration erneut an die macOS-Geräte. Für Windows-Geräte kopieren und verwenden Sie die neuen CLI-Werte in den neuen Apps.

Authenticate-Konfiguration erstellen

Procedure

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie im Suchfeld **auth** ein und klicken Sie dann auf die Konfiguration **Authentifizieren**.
4. Bezeichnen und beschreiben Sie die Konfiguration.
5. Wählen Sie ein **Desktop-Identitätszertifikat** aus der Dropdown-Liste aus.
6. Wählen Sie eine oder beide der folgenden OS-Option(en):
    - macOS
    - Windows
7. Für macOS:
    1. Klicken Sie in dem Bereich „Benutzerdefinierte Daten“ auf **+ Hinzufügen**, um Schlüssel und Zeichenkettenwerte für benutzerdefinierte Daten hinzuzufügen, die per Push an die Geräte übertragen werden sollen.
    2. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
    3. Klicken Sie auf **Fertig**.
8. Für Windows 10-Geräte hilft diese Konfiguration bei der Erzeugung von Befehlszeilenargumenten für die Authenticator MSI-App für Windows wie folgt:
    1. Klicken Sie auf **Fertig**, um die Konfiguration der Authentifizierung abzuschließen.
    2. Zeigen Sie auf der Seite **Konfigurationen** die Authentifizierungskonfiguration an, um den angezeigten Befehlszeilentext zu kopieren. Dieser Text wird zur Verteilung der Authentifizierungs-App für Windows-Geräte benötigt.

> Wenn die Konfiguration „Authentifizierung“ für Windows-Geräte übernommen wird, bleibt die Konfiguration im Status „Ausstehende Installation“. Sie können dies ignorieren, da es keine Auswirkungen auf die Funktionalität hat.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.4.49. Apple App-Katalog

Gilt für: iOS und Mac OS

Die Konfiguration des Apple App-Katalogs verwaltet den Zugriff auf den Apple App-Katalog über einen Web-Clip. Ab Cloud Release 83 können Sie von der Go-Anwendung zum nativen Apps@Work wechseln. Für neu erstellte Mandanten wird die Apps@work Webclip-Konfiguration nicht standardmäßig für iOS-Geräte verteilt, die über iReg oder den Client installiert wurden. Der Administrator muss die Webclip-Konfiguration an die über iReg oder den Client registrierten Geräte manuell verteilen.

> Das Apps@Work-Webclip-Suchergebnis zeigt nur 10 Anwendungen auf iOS- und iPad-Geräten an, selbst wenn in der Suchanforderung mehr als 10 Zeilen eingestellt sind.

Verfahren

Administratoren können die Verteilung dieser vom System definierten Konfiguration wie folgt bearbeiten:

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **Apple App Catalog**.
3. Klicken Sie auf die Option **Verteilung bearbeiten**.
4. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte - Alle kompatiblen Geräte erhalten diese an sie gesendete Konfiguration.
    - Keine Geräte - Der Zugriff auf den Apple App-Katalog wird deaktiviert bzw. die Konfiguration für eine spätere Verteilung reserviert.
    - Definieren Sie spezifische Gerätegruppen, an die diese Konfiguration gesendet werden soll.

Klicken Sie auf **Speichern**.

10.10.4.50. Verwaltete Domänen

Lizenz: Silver

Mit einer verwalteten Domänenkonfiguration können Sie angeben, welche Domänen für Mail und Safari auf iOS 8+- und visionOS 1.1+-Geräten als vertrauenswürdig gelten sollen. Sobald die Konfiguration in dem Gerät aktiviert ist, werden nicht in der Konfiguration definierte Domains auf dem Gerät bei E-Mails und Safari als "nicht vertrauenswürdig" hervorgehoben. Kontrollieren Sie mit dieser Konfiguration sowie den **konfigurierten Einschränkungen** die für Safari zulässigen Daten-Downloads.

Verwaltete Domaineinstellungen

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Verwaltete E-Mail-Domänen	Klicken Sie auf **+Hinzufügen**, um eine Domain hinzuzufügen, beispielsweise "Mycompany.com".
Verwaltete Web-Domänen	Klicken Sie auf **+Hinzufügen**, um eine Domain hinzuzufügen, beispielsweise "Mycompany.com".

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.4.51. Passwortkonfiguration

Einer der ersten Schritte bei der Konfiguration in der Ivanti Neurons for MDM (mit dem Startup Wizard) ist die Konfiguration eines Passcodes. Diese Konfiguration definiert Einstellungen für die Bildschirmsperre auf Geräten.

Passworteinstellungen

Einstellung	Aktion
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Einfache Werte zulassen	Legt fest, ob die PIN bzw. das Passwort sortierte Buchstaben oder Ziffern enthalten darf. **Für iOS, macOS, watchOS, und Android:** Wählen Sie die Option aus, um PINs oder Passcodes zu erlauben, die unsicherer sind, weil sie sich wiederholende Zeichen oder Zeichen in aufsteigender oder absteigender Reihenfolge enthalten. Beispiele: 1111, 1234, abcd. Die Deaktivierung dieser Option für Android-Geräte erzwingt Passcodes mit komplexen PINs. Beispielsweise können die Benutzer dann keine Passwörter mit sich wiederholenden oder aufsteigend oder absteigend sortierten Zeichen konfigurieren. **Für Windows 10+:** Wählen Sie diese Option aus, um weniger sichere Passcodes zu erlauben (da sie sich wiederholende oder aufsteigende Ziffernfolgen enthalten). Beispiele: 1111, 1234
Alphanumerischer Wert erforderlich	Verlangt für den Passcode mindestens einen Buchstaben und eine Ziffer. **Für iOS und Android**: Wählen Sie diese Option, wenn in Passcodes Buchstaben und Ziffern enthalten sein sollen. **Für Windows 10+:** Wählen Sie diese Option aus, um starke Kennwörter entsprechend dem Microsoft-Standard zu erzwingen.
Minimale Passcodelänge	Wählen Sie eine Zahl aus der Liste, um eine minimale Passwortlänge festzulegen. **Für Windows 10 Desktops**: Lokale Konten erzwingen als Mindestlänge des Passcodes 6.
Minimale Anzahl komplexer Zeichen	**Für iOS** und Android: Wählen Sie eine Zahl aus der Liste aus, um die Mindestzahl der Zeichen festzulegen, die weder Ziffern noch Buchstaben sein dürfen. **Für Windows 10+**: Lokale Konten erzwingen 3 Sonderzeichen.
Maximale Gültigkeitsdauer des Passworts	Geben Sie eine Zahl für die Anzahl der Tage ein, nach denen der Benutzer des Geräts das Passwort neu einstellen muss. Wenn Sie die Gültigkeitsdauer des Passworts nicht bestimmen möchten, lassen Sie dieses Feld leer.
Automatische Sperre Alle Sperrmethoden	Wählen Sie ein Intervall aus der Liste aus, um zu bestimmen, wie lange das Gerät im Leerlauf bleibt, bevor die Bildschirmsperre automatisch aktiviert wird. **Nur für Android**. Der Benutzer kann damit eine Sperrmethode auswählen, beispielsweise ein Entsperrmuster. Die oben erwähnten Passcodeeinstellungen werden für dieses Gerät nicht verwendet.
Passwortverlauf	Geben Sie eine Zahl ein, um die Anzahl der individuellen Passwörter zu bestimmen, die ein Benutzer eingeben muss, bevor er ein Passwort wieder verwenden kann. Wenn Sie in diesem Feld beispielsweise „4“ eintragen, muss der Benutzer vier Passwörter eingeben, bevor er das erste Passwort wieder verwenden kann.

Einstellung	Aktion
Nachfrist für Sperrung des Geräts	Wählen Sie ein Intervall aus der Liste zur Bestimmung der Zeitspanne zwischen der Aktivierung der Bildschirmsperre und dem Zeitpunkt, zu dem der Benutzer das Gerät mit einem Passwort entsperren kann.
Maximale Anzahl an Fehlversuchen	Stellen Sie mit einer Nummer aus der Liste ein, wie oft der Gerätebenutzer nacheinander einen falschen Passcode eingeben darf, bevor das Gerät zurückgesetzt und komplett gelöscht wird. **Warnung:** Geräte werden gelöscht, wenn der Benutzer die maximal zulässige Anzahl falscher Passworteingaben überschreitet. Verwenden Sie diese Option mit Vorsicht.
(Nur macOS) Regulären Ausdruck für Passcode aktivieren (macOS 14+)	Geben Sie die Zeichenfolge des Ausdrucks an, der mit dem Kennwort übereinstimmt, um festzustellen, ob sie der Richtlinie entspricht.
(nur macOS) Sprache	Geben Sie die Sprache der Beschreibung an.
(nur macOS) Beschreibung	Beschreiben Sie die Kennwortkomplexität. Geben Sie beispielsweise an, ob Zahlen, Sonderzeichen, Zeichenfolgen usw. zu verwenden sind.
(Nur macOS) Passcode-Regel bei der nächsten Anmeldung erzwingen	Wählen Sie diese Option, damit macOS den Benutzer auffordert, das Passwort so zu ändern, dass das Passwort bei der nächsten Anmeldung des Benutzers mit der Passwortrichtlinie übereinstimmt. Diese Option ist standardmäßig nicht aktiviert. Für macOS 10.13 und spätere Versionen
(Nur macOS) Minuten bis zum Zurücksetzen der Anmeldefehlversuche	Legen Sie fest, nach wie vielen Minuten die Anmeldung nach Erreichen der maximalen Anzahl nicht erfolgreicher Anmeldeversuche zurückgesetzt wird. Stellen Sie sicher, dass Sie zur Aktivierung dieses Felds die maximale Anzahl an fehlerhaften Versuchen festlegen. Verfügbar in MacOS ab Version 10.10.
SmartLock	**Für Geräte mit Android 5.0 gilt, sofern es sich nicht um Geräte mit Arbeitsprofilen für Android Enterprise handelt:** **Für Android 6.0 oder höher:** Erlaubt oder verbietet es einem Benutzer, die SmartLock-Funktion zur Entsperrung eines Geräts zu verwenden. Die SmartLock-Funktion entsperrt ein Gerät unter bestimmten Umständen automatisch, beispielsweise, wenn sich der Benutzer in der Nähe des Geräts befindet oder das Gerät an einer bestimmten Stelle oder das Gerät mit einem vertrauenswürdigen Gerät gekoppelt ist.
Fingerabdruck entsperren	**Für Geräte mit Android 5.0 gilt, sofern es sich nicht um Geräte mit Arbeitsprofilen für Android Enterprise handelt:** **Für Android 6.0 oder höher:** Erlaubt oder verbietet dem Benutzer die Verwendung des Fingerabdrucks zur Entsperrung eines Geräts.

Einstellung	Aktion
Sperrbildschirmbenachrichtigungen (nur für Android Enterprise)	**Benachrichtigungen für verwaltete Geräte (für Geräteeigentümer) aktivieren** Bei verwalteten betrieblichen Geräten Benachrichtigungen auf dem Sperrbildschirm zulassen oder nicht zulassen **Nicht überprüfte Benachrichtigungen für Arbeitsprofil aktivieren** **Für Android 6.0 oder höher:** Bei verwalteten betrieblichen Geräten Benachrichtigungen auf dem Sperrbildschirm zulassen oder nicht zulassen. Sobald Sie diese Einstellung aktivieren, erhalten Sie die Benachrichtigung; der Content erscheint jedoch als „Durch die Richtlinie verborgener Content“. Sie können den Content nur in der App sehen (als Mail/ Push-Benachrichtigung).

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.4.52. Datenschutzpräferenz (macOS)

Gilt für: macOS 10.14 oder unterstützte neuere Versionen.

Konfigurieren Sie, welche Anwendungen Zugriff auf Systemdienste, Systemdateien und Systemressourcen erhalten. Diese Konfiguration kontrolliert die Einstellungen auf einem macOS-Gerät unter Systempräferenzen > Sicherheit & Datenschutz > Datenschutz.

Konfiguration für Datenschutzpräferenzen erstellen

Procedure

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie in dem Suchfeld **Datenschutz** ein und klicken Sie dann auf die Konfiguration **Datenschutz-Präferenz**.
4. Bezeichnen und beschreiben Sie die Konfiguration.
5. Wechseln Sie zu einer der Anwendungen, die auf der Seite aufgelistet sind. Weitere Informationen finden Sie in der **Apple-Dokumentation**.
    1. Ab macOS 10.14+ sind folgende Anwendungen und Einstellungen für die Konfiguration verfügbar:
        - Zugänglichkeit - Legt die Richtlinien für die Anwendung über das Teilsystem Zugänglichkeit fest.
        - Adressbuch - Legt die Richtlinien für die von der Contacts.app verwalteten Kontaktinformationen fest.
        - Apple Events - Legt die Richtlinien für die App fest, welche eingeschränkte AppleEvents an einen anderen Prozess sendet.
        - Kalender - Legt die Richtlinien für Kalenderinformationen fest, die von der Kalender-App verwaltet werden.
        - Kamera - Eine Systemkamera. Der Zugriff auf die Kamera kann in einem Profil nicht gewährt, sondern nur verweigert werden.
        - Mikrofon - Ein Systemmikrofon. Der Zugriff auf das Mikrofon kann in einem Profil nicht gewährt, sondern nur verweigert werden.
        - Fotos - Die Bilder, die von der Fotos-App in ~/Pictures/.photoslibrary verwaltet werden.
        - Post-Ereignis - Legt fest, welche Richtlinien für die Anwendung die CoreGraphics-APIs verwenden sollen, um CGE-Ereignisse an den System-Ereignisstrom zu senden.
        - Erinnerungen - Legt die Richtlinien für die von der Erinnerungs-App verwalteten Erinnerungsinformationen fest.
        - Systemrichtlinie (Alle Dateien) - Erlaubt der Anwendung den Zugriff auf alle geschützten Dateien, einschließlich der Systemadministrationsdateien.
        - Systemrichtlinie (Admin-Dateien) - Erlaubt der Anwendung den Zugriff auf bestimmte Dateien in der Systemadministration.
    2. Ab macOS 10.15+ sind folgende Anwendungen und Einstellungen für die Konfiguration verfügbar:
        - Dateinutzung - Zeigt einer File-Provider-Anwendung, ob der Benutzer Dateien verwendet, die vom File-Provider verwaltet werden.
        - Ereignis von allen Prozessen abhören - Erlaubt der Anwendung, die CoreGraphics- und HID-APIs zum Abhören (Empfang) von CGE-Ereignissen und HID-Ereignissen aller Prozesse zu verwenden. Der Zugriff auf diese Ereignisse kann in einem Profil nicht gewährt, sondern nur verweigert werden. Deaktivieren Sie die Option „Erlaubt“.

- Zugriff auf Medienbibliothek - Erlaubt der Anwendung den Zugriff auf Apple Music, Musik- und Videoaktivitäten und die Medienbibliothek.
- Bildschirmfoto der Systemanzeige - Erlaubt der Anwendung, den Inhalt der Systemanzeige zu erfassen und zu lesen. Der Zugriff auf den Content kann in einem Profil nicht gewährt, sondern nur verweigert werden. Deaktivieren Sie die Option „Erlaubt“.
- Sprachdaten erkennen und an Apple senden - Erlaubt dem Programm die Nutzung der Spracherkennungsfunktion des Systems und den Versand der Sprachdaten an Apple.
- Zugriff auf Dateien im Desktop-Ordner des Benutzers - Erlaubt der Anwendung den Zugriff auf Dateien im Desktop-Ordner des Benutzers.
- Zugriff auf Dateien im Dokumenteordner des Benutzers - Erlaubt der Anwendung den Zugriff auf Dateien im Dokumenteordner des Benutzers.
- Zugriff auf Dateien im Download-Ordner des Benutzers - Erlaubt der Anwendung den Zugriff auf Dateien im Download-Ordner des Benutzers.
- Zugriff auf Dateien auf Netzwerklaufwerke - Erlaubt der Anwendung den Zugriff auf Dateien auf Netzwerklaufwerken.
- Zugriff auf Dateien auf Wechselmedien - Erlaubt der Anwendung den Zugriff auf Dateien auf Wechselmedien.

6. Für jede Anwendung, die Sie konfigurieren wollen, klicken Sie auf **Aktionen > Hinzufügen**.
7. Geben Sie die Werte für die folgenden Identitätswörterbuchschlüssel ein:
   - Identifikator: Bezeichnung der Einstellungen Beispiel: „us.zoom.Zoom.ZoomPresence.“
   - Identifikator-Typ - Wählen Sie entweder die Bundel-ID oder den Pfad. Beispiel: „Bundle-ID.“
   - Codeanforderung - Geben Sie den Wert für die Bundle-ID oder den Pfad an. Beispiel: „Bezeichner „us.zoom.Zoom.ZoomPresence“ und „anchor Apple generic“.“
   - Statischer Code (wahr oder falsch)
   - Erlaubt (wahr oder falsch)
   - Kommentieren
8. Klicken Sie auf **Speichern**.
9. (Optional) Klicken Sie bei einer beliebigen Anwendung auf **Aktionen > Löschen**, um vorhandene Datenschutzpräferenzeinstellungen zu entfernen.
10. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
11. Klicken Sie auf **Fertig**.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.4.53. Datenschutzeinstellungen

Eine Datenschutzkonfiguration definiert, ob:

- Standortdaten werden auf dem Gerät erfasst und an das Geräteverwaltungssystem gesendet.
- Administratoren das Gerät löschen dürfen;
- Das App-Inventar des Gerätes für alle Apps erfasst wird oder nur für Apps, die im App-Katalog enthalten sind.

Datenschutzeinstellungen

> Die Geräte-Löschaktion und die Bestandsaufnahme aller Anwendungen auf dem Gerät gilt nicht für benutzerregistrierte Geräte.

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Standortdaten erfassen	Wählen Sie die Option aus, um die Erhebung von Standortdaten zu aktivieren. Die Standortdaten finden Sie auf der „Geräte“-Seite. • Bei iOS-Geräten richtet sich der angezeigte Standort des Gerätes nur nach dem Netzwerkstandort. • Bei Android-Geräten richtet sich die Standortanzeige sowohl nach dem Netzwerkstandort als auch dem GPS-Standort (sofern verfügbar). • Bei Windows-Geräten basiert der Standort auf den Breiten- und Längengradwerten, die während einer Geräte-Anmeldung ermittelt wurden. Wenn die Sammlung von Standortdaten auf einem Gerät aktiviert ist, wird der aktuelle Standort alle vier Stunden aktualisiert. Standortdaten werden aus dem Gerätemanagementsystem gelöscht, wenn das Gerät außer Dienst gestellt wird oder die Datenschutzeinstellungen deaktiviert oder gelöscht werden. Opting Out of Location Data Collection.htmBenutzer von Geräten können die Sammlung von Standortdaten auf dem Gerät deaktivieren.
Wipe-Aktion auf dem Gerät deaktivieren	Wählen Sie die Option aus, um zu verhindern, dass Administratoren das Gerät löschen. Sie sollten diese Option für Geräte auswählen, die privates Eigentum der Benutzer sind (Eigentum der Mitarbeiter).
Benutzer auffordern, Standortdienste zu aktivieren	Wählen Sie diese Option aus, um Benutzern die Möglichkeit zu geben, die Verwendung von Positionsdiensten optional zu erlauben oder zu verweigern, etwa das Lokalisieren von Geräten, Wi-Fi und MTD. Bei vollständig verwalteten Geräten kann dies automatisch gewährt werden, wenn der Administrator sich für die Deaktivierung der Option entschieden hat.
App-Bestand erfassen	Wählen Sie die Option **App-Inventar erfassen**, um Informationen zu allen auf dem Gerät installierten Apps unabhängig davon zu sammeln, ob es sich um eine App aus dem App-Katalog handelt. Klicken Sie auf Für Apps auf dem Gerät, die in dem App-Katalog enthalten sind, um nur Informationen über die installierten Apps zu sammeln, die auf dem Gerät installiert und im App-Katalog enthalten sind. Wählen Sie die Option **Für alle Apps auf dem Gerät**, um Informationen über alle Apps auf dem Gerät zu sammeln. Diese Option gilt für Geräte mit Windows 10+. Die folgenden Bestände des App-Quelltyps werden angezeigt und standardmäßig ausgewählt. • **Bestand aktivieren, der nicht aus dem App Store stammt** - für hauseigene Anwendungen (Universal-Anwendungen), die über MDM oder direkt vom Endbenutzer nach dem manuellen Auspacken auf dem Gerät lokal installiert werden. • **App Store Bestand aktivieren** - für manuell aus Microsoft Store oder über Apps@work Store Front installierte Apps. • **Systembestand aktivieren** für die Apps, die zusammen mit Windows 10 OS von Microsoft als vorinstalliert gemeldet wurden.

Einstellung	So gehen Sie vor
	• **Win32-Inventar aktivieren** – für System-32-basierte Apps wie MSI, EXE, Win32-Store-Apps usw., die via Push über MDM oder direkt durch den Endbenutzer auf dem Gerät installiert werden. Sie können optional auch nur die Bestände der App-Quelltypen auswählen, um Informationen über ausgewählte Apps zu sammeln. MDM-installierte Apps werden im App-Inventar aufgeführt, auch wenn Sie das Inventar für Nicht-App Store-Apps oder Win32-Apps nicht ausgewählt haben. Das EXE-Inventar wird auch erfasst, wenn die Datenschutzkonfiguration die Standardkonfiguration für die Erfassung des App-Inventars nur für den App-Katalog verwendet. Das Inventar muss regelmäßig für alle Apps erfasst werden, wenn das Inventar nur für App-Katalog-Apps erfasst werden soll. Das Inventar für Modern-, MSI- und EXE-Apps, die im App-Katalog verfügbar sind, wird nur abgerufen, wenn mindestens eine App verteilt wird, die einer dieser Varianten angehört.
Einstellungen für Geräte mit Android Enterprise (7.0+)	
Konfigurieren Sie die unten angegebenen Einstellungen, um die Datenschutzrichtlinie für Geräte mit Android Enterprise festzulegen.	
Name des Unternehmens	Geben Sie den Namen des Unternehmens ein, das das Gerät verwaltet.
Unternehmensfarbe	Wählen Sie die Farbe des Unternehmens, die im Hintergrund des Benutzerbildschirms angezeigt werden soll.
Kurznachricht	Geben Sie eine kurze Meldung ein, die angezeigt werden soll, wenn der Benutzer eine Funktion verwenden möchte, die vom Administrator gesperrt wurde.
Lange Nachricht	Geben Sie die lange Nachricht ein, die angezeigt werden soll, wenn der Benutzer auf die Kurznachricht klickt. Diese Meldung enthält weitere Details zu für den Benutzer definierten Einschränkung.
Go-App-Bildschirme ausgeblendet halten	Wählen Sie "wahr" oder "falsch" aus der Liste aus. • **Wahr** – Während der Remote-Freigabe sind die Bildschirme der Ivanti Go-App nicht sichtbar. • **Falsch** – Während der Remote-Freigabe sind die Bildschirme der Ivanti Go-App für Fehlerbehebungszwecke und zum Anzeigen der Dokumentation sichtbar.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.4.54. Informationen zur Datenschutzerklärung für Kunden

Gilt für: Android-, Android Enterprise- und iOS-Geräte oder unterstützte neuere Versionen.

Konfiguration zur Verteilung der Datenschutzerklärung an die Benutzer in Go-Clients Dies ist eine vom System definierte Konfiguration, bearbeitet werden können nur die Verteilereinstellungen.

Die dem Benutzer angezeigten Informationen umfassen die Details der folgenden Konfigurationen:

- Datenschutz
  - Standortdaten erfassen
  - App-Bestandsaufnahme
  - Android 7.0+:
    - Name der Organisation
    - Unternehmensfarbe
    - Kurznachricht
    - Lange Nachricht
- Client-Datenschutz
  - SLC - Signifikanter Standortwechsel, um das Gerät regelmäßig zu aktivieren.
  - Standortabhängiges Mindestaufweckintervall
  - MixPanel-Status aktivieren
- Verwaltung mobiler Geräte - MDM-Zugriffsrechte (gilt nicht für benutzerregistrierte Geräte)
  - Gerätesperre und Entfernen des Passcodes erlauben
  - Gerät löschen
  - Netzwerkinformationen (Telefon-/ SIM-Nummern, MAC-Adressen)

10.10.4.55. Einstellungen für Ivanti Go-Client

Konfigurieren Sie die Erfassung anonymer Daten von Endbenutzern, einschließlich Geräte- und Nutzungsinformationen, um Produktprobleme leichter zu identifizieren und eine hohe Servicequalität zu gewährleisten. Diese Einstellung aktiviert auch Konfigurationsoptionen für Support-Kontakte.

Erstellen der Konfiguration Einstellungen für Ivanti Go-Client

Gilt für:

- Mobile@Work für macOS 1.67 oder unterstützte neuere Versionen.
- Go for iOS 3.5.0 oder unterstützte neuere Versionen.
- Mobile@Work for Android 12.9.0.0 oder unterstützte neuere Versionen.
- Go for Android 124 oder unterstützte neuere Versionen.

Verfahren

1. Wechseln Sie zu **Konfigurationen** > **Konfiguration hinzufügen** > **Einstellungen für Ivanti Go-Client**. Die Seite **Konfiguration "Einstellungen für Ivanti Go-Client" erstellen** wird angezeigt.
2. Geben Sie einen Namen für die Konfiguration im Kästchen **Name** ein.
3. Geben Sie eine **Beschreibung** für die Konfiguration ein.
4. Wählen Sie unter Standortabhängige Aufweckfunktion die Option SLC aktivieren aus. Der signifikante Standortwechseldienst ist eine leistungsfähigere Alternative zu Aktualisierungen des Standorts der GO for iOS-App, wenn die Position des Benutzers sich nach mindestens 15 Minuten deutlich ändert (Standardintervall). Wenn dieser Dienst aktiviert ist, wacht die GO-App bei einer Standardänderung im Hintergrund auf und meldet sich an.
5. Wählen Sie unter **Datenerfassung über Analysen für Clients** die Option **Analysen aktivieren** aus, falls diese deaktiviert ist. Standardmäßig ist diese Option aktiviert.
6. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
7. Klicken Sie auf Fertig.

Setup für Registerkarte "Support" konfigurieren

Gilt für:

- Mobile@Work für macOS 1.67 oder unterstützte neuere Versionen.
- Go for iOS 3.5.0 oder unterstützte neuere Versionen.
- Mobile@Work for Android 12.9.0.0 oder unterstützte neuere Versionen.
- Go for Android 124 oder unterstützte neuere Versionen.

Verfahren

1. Wechseln Sie zu **Konfigurationen** > **Konfiguration hinzufügen** > **Einstellungen für Ivanti Go-Client**. Die Seite **Konfiguration "Einstellungen für Ivanti Go-Client" erstellen** wird angezeigt.
2. Geben Sie einen Namen für die Konfiguration im Kästchen **Name** ein.
3. Geben Sie eine **Beschreibung** für die Konfiguration ein.
4. Wählen Sie bei **Plattform** die jeweilige Plattform aus.

5. Klicken Sie im Abschnitt **Setup für Registerkarte "Support" konfigurieren** auf **Registerkarte "Support" aktivieren**.

> Das Feld **Registerkarte "Support" aktivieren** betrifft nur iOS-Geräte.

> Sie können die **Support-Registerkarte** über Go für iOS, Version 118.0.0 oder höher, und Go für Android, Version 124 oder höher, aktivieren. Geräte mit früheren Versionen zeigen diese Funktion nicht an und unterstützen sie nicht.

Machen Sie im Abschnitt **Konfiguration "Support-Kontakt"** folgende Angaben:

- **Registerkartenname** – Geben Sie den Namen der Registerkarte ein, der in der Ivanti App-Navigation angezeigt werden soll. Der Standardwert ist 'Support' (max. Länge: 10 Zeichen).
- **Anweisungen für Endbenutzer** – Geben Sie Anweisungen zur Verwendung der Support-Kontakte ein (max. Länge: 40 Zeichen).
- **Kontakte hinzufügen** – Klicken Sie auf **+Hinzufügen**, um die Kontakte hinzuzufügen. (Maximale Kontakte: 5)
  - **Name** – Geben Sie den Namen des Kontakts ein. (max. Länge: 20 Zeichen).
  - **Telefonnummer** – Geben Sie eine gültige Telefonnummer ein (mit Landesvorwahl).
- **URL hinzufügen** – Klicken Sie auf **+Hinzufügen**, um die URLs hinzuzufügen. (Maximale URLs: 5)
  - **URL-Name** – Geben Sie den Namen der URL ein. (max. Länge: 20 Zeichen).
  - **URL** – Geben Sie eine gültige URL ein.
- **Zusätzliche Informationen** – Geben Sie hier etwaige zusätzliche Support-bezogene Nachrichten ein, die angezeigt werden sollen (max. Länge: 120 Zeichen).
- **E-Mail-Adresse** – Geben Sie die E-Mail-Adresse ein, an die Support-Anfragen gesendet werden sollen (max. Länge: 40 Zeichen).

  > Geben Sie eine gültige E-Mail-Adresse im Format alias@domainname.com ein.

- **Support Ticketing System-URL** – Fügen Sie die Schaltfläche **Support-Ticket erstellen** zur Registerkarte **Support** von **Ivanti Go for iOS** und der App **Ivanti Go for Android** hinzu. Aktivieren Sie den Umschalter, um die Schaltfläche auf der Registerkarte "Support" anzuzeigen, und geben Sie die entsprechende URL in das vorgesehene Feld ein, um Benutzer zu Ihrem Supportsystem weiterzuleiten.

  > Diese URL wird auf der Ivanti Go **Support-Registerkarte** verwendet, um Benutzer zum angegebenen Supportsystem umzuleiten. Für eine verbesserte Sicherheit wird empfohlen, URLs zu verwenden, die mit *https://* statt mit *http://* beginnen.

Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.

8. Klicken Sie auf Fertig.

Weitere Informationen finden Sie unter **Konfigurationen**.

10.10.4.56. Siri-Einstellungen

Mithilfe der **Siri-Einstellungen** können Sie Siri-Einstellungen auf überwachten Geräten konfigurieren. Diese Konfiguration hilft Administratoren, konsistente, richtlinienbasierte Kontrollen anzuwenden, die steuern, wie Geräte auf Siri-Funktionen zugreifen und diese verwenden.

Gilt für:

- iOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- macOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- watchOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- visionOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- Überwachte Geräte mit tvOS 27.0+ bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Siri-Einstellungen** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie die **Siri-Einstellungen** gemäß der folgenden Tabelle:

Einstellung	Aktion
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Aktiviert	Aktivieren Sie das Kontrollkästchen, um Siri zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um Siri auf überwachten Geräten zu aktivieren.
Siri-KI zulassen	Aktivieren Sie das Kontrollkästchen, um **Siri AI**-Funktionen zu aktivieren. Schalten Sie die Schaltfläche **Via Push an das Gerät senden** um, um die **Siri AI**-Funktionen auf überwachten Geräten zu aktivieren.
Vom Benutzer erstellten Inhalt zulassen	Aktivieren Sie das Kontrollkästchen, um vom Benutzer erstellten Inhalt zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um benutzergenerierten Inhalt auf überwachten Geräten zu aktivieren. Diese Einstellung gilt nicht für macOS- und visionOS-Geräte.
Während der Sperre zulassen	Aktivieren Sie das Kontrollkästchen, um "Während der Sperre" zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um "Während der Sperre" auf überwachten Geräten zu aktivieren. Diese Einstellung gilt nicht für macOS- und visionOS-Geräte.
Profanitätsfilter erzwingen	Aktivieren Sie das Kontrollkästchen, um das Erzwingen des Profanitätsfilters zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um das Erzwingen des Profanitätsfilters auf überwachten Geräten zu aktivieren. Diese Einstellung gilt nicht für visionOS-Geräte.
Reduzierung sensibler Inhalte erzwingen	Aktivieren Sie das Kontrollkästchen, um Siri zu zwingen, sensible Inhalte zu reduzieren. Schalten Sie die Schaltfläche **Via Push an das Gerät senden** um, um Siri zu zwingen, sensible Inhalte auf überwachten Geräten zu reduzieren.

4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
5. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Siri-Einstellungen** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
6. Klicken Sie auf **Fertig**.

10.10.4.57. Konfiguration "Dienstkonfigurationsdateien"

Mithilfe der Konfiguration **Dienstkonfigurationsdateien** können Administratoren Konfigurationsdateien für verschiedene Systemdienste zentral auf verwalteten Geräten verwalten und bereitstellen. Darüber hinaus können Administratoren anhand der Konfiguration sicherstellen, dass die Diensteinstellungen konsistent bleiben und vor unerlaubter Modifizierung geschützt sind, indem sie Dateien in sichere, dienstspezifische Verzeichnisse in einer manipulationssicheren Umgebung senden.

Gilt für macOS-Geräte

Vorbereitung:

- Sie können verschiedene Konfigurationen als *ZIP*-Datei hochladen. Weitere Informationen zum Hinzufügen einer Datei finden Sie unter **Dateien**.
- Alle Dateien im erweiterten Archiv werden auf *-r–r–r– unix*-Dateiberechtigungen gesetzt. Etwaige Links im Archiv können nur auf Dateien innerhalb des dienstspezifischen Speicherorts verweisen.
- Die Dateien im .zip-Archiv müssen die Ordnerstruktur und Konfigurationsdateien spiegeln, die der Dienst erwartet, wobei der Stamm des Dateisystems den Anfang bildet. Der Dienst verwendet nur die von der Deklaration bereitgestellten Dateien und ignoriert die Dateien in den Standardverzeichnissen.

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Dienstkonfigurationsdateien** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie die Einstellungen für die **Dienstkonfigurationsdateien** gemäß der folgenden Tabelle:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Datei auswählen	Geben Sie den Dateinamen ein.
Diensttyp wählen	Wählen Sie einen der **Diensttypen** aus der Dropdownliste aus: • SSHD • SUDO • PAM • CUPS • HTTP_D • BASH • ZSH

4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
5. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Dienstkonfigurationsdateien** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.

6. Klicken Sie auf **Fertig**.

10.10.4.58. [Software Updates]

Gilt für:

- Überwachte Geräte mit iOS 10.3 bis 26.0 und tvOS 12.0 bis 26.0
- macOS-Geräte
- Geräte mit Windows 10+

Regeln für Betriebssystemaktualisierungen erstellen und verteilen

Dieser Abschnitt enthält die folgenden Themen:

- **Software-Updates für iOS/tvOS-Geräte konfigurieren**
- **Software-Updates für iOS/tvOS-Geräte konfigurieren**
- **Software-Updates für Windows-Geräte konfigurieren**
- **Durchsetzen von Softwareupdates unter Verwendung der deklarativen Geräteverwaltung**

Softwareupdates für iOS-Geräte konfigurieren

Verfahren

Gesendete Betriebssystemaktualisierungen bei iOS-Geräten erlauben, wenn es sich um überwachte Geräte handelt:

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie auf **Software-Updates**.
4. Klicken Sie auf **iOS/tvOS**, um das Konfigurations-Setup anzuzeigen.
5. Klicken Sie auf die Option **Betriebssystemaktualisierungen können automatisch auf überwachten Geräten installiert werden.**
6. Wählen Sie eine der folgenden Optionen aus:
   - Auf die aktuellste Version aktualisieren
   - Update auf eine bestimmte Version - Geben Sie beispielsweise die iOS-Versionsnummer 11.3.0 ein.
7. Wählen Sie eine der folgenden Installationsaktionen:
   - Standard
   - Nur herunterladen
   - So schnell wie möglich installieren
8. Wählen Sie die folgenden Zeitoptionen für die Updates aus:
   - [Start Time]
   - [End Time]
   - Zeitzone
9. Klicken Sie auf **Weiter**.
10. Wählen Sie die Option **Diese Konfiguration aktivieren**.
11. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte

- Keine Geräte (Standard)
- Anpassbar

12. Klicken Sie auf **Fertig**.

- Wenn Sie eine bestimmte Version des Betriebssystem-Updates für iOS-Geräte installieren, müssen Sie eine Version auswählen, die für das Gerät verfügbar ist. Wenn Sie eine ungültige oder nicht verfügbare Version auswählen, wird die Software-Aktualisierung des Geräts ignoriert.
- Wenn das Gerät über einen Passcode verfügt, stellt das Gerät, sobald MDM das Update an das Gerät gesendet hat, das Update in die Warteschlange; der Benutzer wird dann aufgefordert, seinen Passcode einzugeben, um die Installation zu starten.
- Aktivieren Sie `enforcedSoftwareUpdateDelay` bei den **iOS-Einschränkungen**, um sicherzustellen, dass durch einen manuellen Scan auf Geräten nach Softwareupdates nicht die spezifischen, von dieser Konfiguration heruntergeladenen Versionen gelöscht werden.

Softwareupdates für iOS-Geräte konfigurieren

Mit dem Device Enrollment Program (DEP), das Teil von Apple Business Manager ist, können Kunden Geräte in großen Mengen kaufen und diese Geräte während der Aktivierung automatisch bei MDM anmelden. Weitere Informationen finden Sie unter **Geräteregistrierung**.

Mithilfe des folgenden Verfahrens können Sie Betriebssystemaktualisierungen an macOS-Geräte mit und ohne DEP senden.

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie auf **Software-Updates**.
4. Klicken Sie auf **macOS**, um das Konfigurations-Setup anzuzeigen.
5. Wählen Sie die Option **macOS-Softwareupdates zulassen**.
6. Wählen Sie die Art der Updates für das Gerät aus. Für jedes dieser Updates können Sie auch Updates auswählen, für die kein Neustart erforderlich ist.
   - Betriebssystem-Aktualisierungen
   - Kritische Aktualisierungen
   - Konfigurationsdaten-Updates
   - Firmware-Update
   - Unkritische Updates

   > Der Administrator kann unkritische macOS-Updates verwalten (installieren/planen), indem er die Option **Unkritische Updates aktivieren** aktiviert. Diese Option ist für die vorhandenen Mieter standardmäßig deaktiviert und muss nach dem Upgrade bei Bedarf vom Administrator explizit aktiviert werden.

   > UnterBetriebssystem-Updateskönnen Administratoren das Gerät auf eine bestimmte macOS-Version aktualisieren.

   > Alle macOS-Updates können mit den folgenden Aktionen konfiguriert werden:

        - Standard
        - Nur benachrichtigen
        - Später installieren
        - Neustart nach Installation erzwingen
        - Nur herunterladen
        - So schnell wie möglich installieren
    -

Mögliche Werte sind "Niedrig" und "Hoch".

Standardeinstellung: Niedrig

Priorität

    - Max. Benutzerverzögerungen
      Der mögliche Wert ist eine Ganzzahl.
      Dies wird nur unterstützt, wenn die Option "Später installieren" gewählt wurde.

7. Wählen Sie die folgenden Zeitoptionen für die Updates aus:
    - [Start Time]
    - [End Time]
    - Zeitzone
8. Klicken Sie auf **Weiter**.
9. Wählen Sie die Option **Diese Konfiguration aktivieren**.
10. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
11. Klicken Sie auf **Fertig**.

Softwareupdates für Windows-Geräte konfigurieren

Verfahren

Aktualisieren Sie zur Konfiguration Ihrer Windows-Installation den Zeitplan:

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie auf **Software-Updates**.
4. Klicken Sie auf **Windows**, um das Konfigurations-Setup anzuzeigen.
5. Geben Sie je nach der Version Ihrer Windows-Geräte die folgenden Optionen ein.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Option **Diese Konfiguration aktivieren**.
8. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte

- Keine Geräte (Standard)
- Anpassbar

Klicken Sie auf **Fertig**.

Software-Updates Geräte mit Windows 10+

- Quellen aktualisieren – Wählen Sie eine der folgenden Quellen aus:
  - Enterprise WSUS
  - Microsoft Update und/oder Enterprise WSUS

Treiberupdatequelle

- Funktionsupdatequelle
- Sonstige Updatequelle
- Qualitätsupdatequelle
- URL für den Unternehmens-WSUS-Server
- Alternativer Microsoft-Update-Server für das Intranet
- Aktualisierungen von „vertrauenswürdigen Publishern“ zulassen – begrenzt die Quellen von Aktualisierungen auf vertrauenswürdige Publisher.
- Automatische Aktualisierungsstrategie – wählen Sie eine der Optionen aus dem Pulldown-Menü.
- Tag der geplanten Installation – definiert die Häufigkeit von Aktualisierungen.
- Zeit der geplanten Aktualisierung – definiert die Installationszeit für Aktualisierungen.
- Updates automatisch über kostenpflichtige Verbindungen herunterladen - Aktivieren oder deaktivieren Sie die Option.
- Keine Scans von Update-Verschiebungsrichtlinien für Windows Update zulassen - Aktivieren oder deaktivieren Sie die Option.
- Aktivierter Neustarttermin - Wählen Sie aus, nach wie vielen Tagen der Neustart erfolgen soll.
- Snooze-Neustarttermin aktivieren - Wählen Sie aus, nach wie vielen Tagen an den Neustart erinnert werden soll.
- Aktivierter Neustart des Übergangszeitplans - Wählen Sie aus, nach wie vielen Tagen der Übergangszeitplan neu gestartet werden soll.
- Leere Inhalts-URLs aktualisieren/füllen.
- Downloadlimit für MO-App - Wählen Sie eine der folgenden Optionen aus:
  - MO-Downloadlimit für Apps und deren Updates nicht ignorieren
  - Downloadlimit von MO für Apps und deren Updates ignorieren (unbegrenztes Herunterladen erlauben)
- Download-Limit für MO-Updates - Wählen Sie eine der folgenden Optionen aus:
  - MO-Downloadlimit für Betriebssystem-Updates nicht ignorieren
  - MO-Downloadlimit für Betriebssystem-Updates ignorieren (unbegrenztes Herunterladen erlauben)
- Vorschau-Builds verwalten - Wählen Sie eine der folgenden Optionen aus:
  - Vorschau-Builds deaktivieren
  - Vorschau-Builds deaktivieren, wenn das nächste Release öffentlich ist.
  - Vorschau-Builds aktivieren

- Zeitplan für automatischen Update-Warnhinweis - Wählen Sie aus, nach wie vielen Minuten der Warnhinweis automatisch neu gestartet werden soll.
- Erinnerung an Neustart definieren - Wählen Sie aus, nach wie vielen Stunden die Erinnerung an den Neustart angezeigt werden soll.
- Zeitplan für automatische Updates - Wählen Sie die Häufigkeit der automatischen Updates aus.
- Benachrichtigung für Updates automatisch neu starten - Aktivieren Sie die automatische Benachrichtigung für Updates.
- Produktversion – Geben Sie die Produktversion ein, die auf der Windows-Update-Versionsseite aufgeführt ist (URL: aka.ms/WindowsTargetVersioninfo), zum Beispiel "Windows 11" oder "11" oder "Windows 10".
- Release-Zielversion – Geben Sie die Release-Zielversion ein, die auf der Windows-Update-Versionsseite aufgeführt ist.
- Start aktive Stunden – Wenn diese Option aktiviert ist, wird der PC nach einem Update während der aktiven Stunden nicht automatisch neugestartet. Außerhalb der aktiven Stunden versucht der PC, einen Neustart durchzuführen.
- Ende aktive Stunden – Wenn diese Option aktiviert ist, wird der PC nach einem Update während der aktiven Stunden nicht automatisch neugestartet. Außerhalb der aktiven Stunden versucht der PC, einen Neustart durchzuführen.
- Aktive Stunden max. Bereich – Mit dieser Option geben Sie die maximale Anzahl der Stunden ab der Startzeit an, in denen Benutzer ihre aktiven Stunden festlegen können.
- Keine Updatebenachrichtigungen während der aktiven Stunden – Die Optionen für die Updatebenachrichtigungen sind nachstehend aufgeführt.
  - Standardbenachrichtigungen von Windows Update
  - Alle Benachrichtigungen mit Ausnahme von Neustartwarnungen deaktivieren
  - Alle Benachrichtigungen einschließlich Neustartwarnungen deaktivieren
- Updates für Treiber deaktivieren – Aktivieren Sie diese Option, um Treiber mit Windows-Qualitätsupdates auszuschließen. Wenn Sie diese Option deaktivieren oder nicht konfigurieren, schließt Windows Update Updates mit Treiberklassifizierung ein.
- Frist für Qualitätsupdates – Die Anzahl der Tage, nach deren Ablauf Qualitätsupdates automatisch und unabhängig von den aktiven Stunden auf den Geräten installiert werden.
- Toleranzfrist für Qualitätsupdates – Die Anzahl der Tage nach Installation des Updates, nach deren Ablauf frühestens automatische Neustarts für Qualitätsupdates durchgeführt werden.
- Frist für Funktionsupdates – Die Anzahl der Tage, nach deren Ablauf Funktionsupdates automatisch und unabhängig von den aktiven Stunden auf den Geräten bereitgestellt werden.
- Toleranzfrist für Funktionsupdates – Die Anzahl der Tage, nach deren Ablauf Funktionsupdates frühestens auf den Geräten bereitgestellt werden, unabhängig von den aktiven Stunden.
- Keine automatischen Neustarts vor Ablauf der Toleranzfrist – Wenn diese Option aktiviert ist, werden die Geräte erst dann automatisch außerhalb der aktiven Stunden neugestartet, wenn sowohl die Frist als auch die Toleranzfrist abgelaufen sind, selbst wenn ein Update zum Neustart ansteht. Ist die Option deaktiviert, wird mitunter ein automatischer Neustart außerhalb der aktiven Stunden versucht, wenn das Update vor Ablauf der Frist für den Neustart verfügbar ist.

Software-Updates für Geräte für Windows 10.0.14393

Die folgenden Einstellungen funktionieren nicht, wenn die Telemetriebeschränkung für ein Gerät deaktiviert ist:

- Aktualisierungen/Upgrades verschieben – Aktivieren Sie diese Option, um Änderungen auf ein späteres Datum zu verschieben.
- Updates aufschieben um – Stellen Sie eine Verzögerung von bis zu 4 Wochen ein.
- Upgrades aufschieben - Aktivieren Sie diese Option, um Upgrades aufzuschieben.

- Upgrades aufschieben um – Wählen Sie eine Verzögerung von bis zu 8 Monaten aus.

Software-Updates für Geräte mit Windows 10.0.14393+

- Zweigstelle zum Installieren von Updates – Hierüber kann der IT-Administrator festlegen, von welcher Zweigstelle ein Gerät seine Updates empfängt. Das Feld "Zweigstelle zum Installieren von Updates" enthält die folgenden Optionen:
  - Windows Insider Build – Schnell
  - Windows Insider Build - Langsam
  - Windows Insider Build freigeben
  - Halbjährlicher Kanal (gezielt)
  - Halbjährlicher Kanal
  - Nur Vorschau von Qualitätsupdates freigeben
  - Canary-Channel

Funktionsaktualisierungen (Upgrades): Wird nur auf Windows Professional, Windows Enterprise und Windows Education unterstützt.

  - Aktualisierungen aufschieben
  - Verschieben um – Wählen Sie eine Verzögerung von bis zu 180 Tagen aus.

Qualitätsaktualisierungen (Updates): Wird nur auf Windows Professional, Windows Enterprise und Windows Education unterstützt.

  - Aktualisierungen aufschieben
  - Verschieben um – wählen Sie eine Verzögerung von bis zu 30 Tagen aus.

Software-Updates für Geräte mit Windows 10.0.17083+

- Funktions-Updates:
  - Deinstallationszeitraum für Funktions-Updates - Wählen Sie aus, nach wie vielen Tagen, ein Funktions-Update deinstalliert werden soll.

Software-Updates für Geräte mit Windows 10.0.17763+

- Den Zugriff „Updates anhalten“ von Benutzern deaktivieren
- Den UXWU-Zugriff von Benutzern deaktivieren (Windows Update-Scan, Herunterladen und Installation)
- Benachrichtigungsebene aktualisieren - Wählen Sie eine der folgenden Optionen aus:
  - Standardbenachrichtigungen von Windows Update verwenden
  - Alle Benachrichtigungen mit Ausnahme von Neustartwarnungen deaktivieren
  - Alle Benachrichtigungen einschließlich Neustartwarnungen deaktivieren
- Funktions-Updates:
  - Frist bis zum automatischen Neustart für die Update-Installation - Wählen Sie aus, nach wie vielen Tagen wegen der Update-Installation automatisch neu gestartet werden soll.
  - Aktivierter Neustarttermin - Wählen Sie aus, nach wie vielen Tage neu gestartet werden soll.
  - Snooze-Neustarttermin aktivieren - Wählen Sie aus, nach wie vielen Tagen an den Neustart erinnert werden soll.
  - Aktivierter Neustart des Übergangszeitplans - Wählen Sie aus, nach wie vielen Tagen der Übergangszeitplan neu gestartet werden soll.

Erzwingen von Softwareupdates unter Verwendung von DDM

Der Administrator kann die Installation von Softwareupdates auf iOS-, macOS- und iPadOS-Geräten unter Verwendung von DDM erzwingen.

Unterstützt auf:

- iOS 17+
- iPadOS 17+
- macOS 14+

Verfahren

1. Erstellen Sie über den Abschnitt "Konfigurationen" eine Konfiguration vom Typ **Erzwingung von Softwareupdates**.
2. Führen Sie eine Aktion vom Typ "Check-in erzwingen" durch, um zu prüfen, ob die Konfiguration "Erzwingung von Softwareupdates" auf dem Gerät installiert ist.

Wenn Sie das Gerät öffnen, müsste normalerweise eine Benachrichtigung über erforderliche Softwareupdates angezeigt werden, aus der Details wie die Versionsnummer, das Zieldatum der Installation usw. hervorgehen.

> Wenn Sie das Softwareupdate nicht erzwingen möchten, setzen Sie die Option bei der Softwareverteilung auf **Keine**.

Verteilen von Prädikaten für eine Konfiguration vom Typ "Durchsetzung von Softwareupdates"

1. Erstellen Sie eine Konfiguration vom Typ "Durchsetzung von Softwareupdates".
2. Setzen Sie den Umschalter Aktivierung mit Prädikaten auf EIN und fügen Sie die Prädikate nach Bedarf über die Schaltfläche + hinzu.



Wechseln Sie zum Bearbeiten oder Löschen eines Prädikats zu **Admin** > **Apple** > **Prädikate**. Die Liste der verfügbaren Prädikate ist auf dieser Seite verfügbar. Klicken Sie auf **Bearbeiten**, um Änderungen an dem vorhandenen Prädikat vorzunehmen und zu speichern. Zum Löschen eines vorhandenen Prädikats wählen Sie es aus und klicken Sie auf **Löschen**.

> Sie können ein Prädikat nicht löschen, wenn es mit einer Konfiguration verknüpft ist.

10.10.4.59. Konfiguration "Einstellungen für Softwareupdate"

Ivanti Neurons for MDM ermöglicht die Konfiguration von Einstellungen für die Durchsetzung von Softwareupdates und definiert das Verhalten von Updates für den Endbenutzer in Bezug auf Kadenz und Verzögerungen.

Gilt für:

- iOS 18.0 überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- iOS 15.0 überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Einstellungen für Softwareupdate** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie die **Einstellungen für Softwareupdates** gemäß der folgenden Tabelle:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
iOS 18+ überwacht und **macOS15+** Beta-Registrierung	
Programmregistrierung (optional) **iOS 18+ überwacht** und **macOS15+ überwacht**	Wählen Sie eine der folgenden Optionen aus: • **Zulässig**: Der Benutzer kann sich bei beliebigen Beta-Programmen registrieren, die mit dem angemeldeten Apple-Konto verknüpft sind. • **Immer Ein**: Es werden die vom Unternehmen angegebenen Beta-Programme verwendet, und der Benutzer kann sich nicht über sein angemeldetes Apple-Konto bei einem Beta-Programm registrieren. **Programm anbieten** – Mit dieser Option können Sie ein erforderliches Programm erzwingen. Beim Erzwingen können Sie die erforderlichen Versionen für iOS- und macOS-Geräte festlegen. **Programm verlangen** – Das Gerät registriert sich automatisch bei diesem Beta-Programm. • **Immer Aus**: Das Gerät darf sich nicht bei Beta-Programmen registrieren. Das System entfernt das Gerät aus Beta-Programmen, falls es dort bereits registriert ist.
Benachrichtigungen	Markieren Sie die Kontrollkästchen **Benachrichtigungen** und **Alle Benachrichtigungen zur Durchsetzung von Softwareupdates anzeigen**, um alle Benachrichtigungen zur Durchsetzung von Softwareupdates auf dem Gerät des Benutzers anzuzeigen. Wenn Sie nur das Kontrollkästchen **Benachrichtigungen** aktivieren, zeigt das Gerät eine Stunde vor der Durchsetzungsfrist eine einzige Durchsetzungsbenachrichtigung an. Wenn Sie keines der Kontrollkästchen auswählen, zeigt das Gerät die ausgelösten Benachrichtigungen an, und es werden alle Durchsetzungsbenachrichtigungen zu Softwareupdates auf dem Gerät des Benutzers angezeigt.
Automatische Aktionen	
Herunterladen	Wählen Sie eine der folgenden Optionen aus: • **Zulässig**: Der Benutzer kann automatische Downloads auf "Ein" oder "Aus" setzen. • **Immer ein**: Automatische Downloads sind für den Benutzer immer auf "Ein" gesetzt. • **Immer aus**: Automatische Downloads sind für den Benutzer immer auf "Aus" gesetzt.
Betriebssystemupdates installieren	Wählen Sie eine der folgenden Optionen aus: • **Zulässig**: Der Benutzer kann die automatische Installation von Betriebssystemupdates auf "Ein" oder "Aus" setzen. • **Immer ein**: Die automatische Installation von Betriebssystemupdates steht für den Benutzer immer auf "Ein".

Einstellung	Beschreibung
	• **Immer aus**: Die automatische Installation von Betriebssystemupdates steht für den Benutzer immer auf "Aus".
Sicherheitsverbesserungen im Hintergrund	
Sicherheitsverbesserungen im Hintergrund	Aktivieren Sie das Kontrollkästchen **Sicherheitsverbesserungen im Hintergrund**, um die Installation und das Rollback von Updates zu steuern. Wählen Sie aus den folgenden Optionen: • **Aktivieren**: Wenn diese Option ausgewählt ist, wird dem Benutzer die Installation von **Sicherheitsverbesserungen im Hintergrund** angeboten. • **Rollback aktivieren**: Wenn diese Option ausgewählt ist, wird dem Benutzer das Rollback von **Sicherheitsverbesserungen im Hintergrund** angeboten.
iOS 18+ überwacht	
Empfohlene Kadenz	Wählen Sie eine der folgenden Optionen aus, um dem Benutzer Softwareupdates anzuzeigen, wenn mehrere Updates verfügbar sind: • **Alle**: Zeigt alle Versionen von Softwareupdates an. • **Älteste**: Dem Benutzer werden nur die ältesten Versionen von Softwareupdates angezeigt (mit niedrigerer Nummer). • **Neueste**: Dem Benutzer werden nur die neuesten Versionen von Softwareupdates angezeigt (mit höherer Nummer).
Verzögerungen	Für überwachte Geräte lassen sich die Softwareupdates verzögern. Sie können die **Sicherheitsverbesserungen im Hintergrund** nicht verschieben.
Kumulierter Zeitraum in Tagen	Legen Sie die Verschiebung in Tagen für ein Haupt- oder Neben-Systemupdate auf dem Gerät fest. Nach der Konfiguration wird das Haupt- oder Neben-Softwareupdate nach der angegebenen Anzahl von Tagen ab dem jeweiligen Release angezeigt. Sie können einen beliebigen Wert zwischen 1 und 90 Tagen festlegen.
macOS 10.15+ überwacht	
Betriebssystemupdates durch Standardbenutzer zulassen	Markieren Sie das Kontrollkästchen **Betriebssystemupdates durch Standardbenutzer zulassen**, um einem Standardbenutzer die Durchführung von Betriebssystemupdates zu erlauben. Markieren Sie das Kontrollkästchen **Standardbenutzern die Durchführung von Haupt- und Neben-Softwareupdates erlauben**, um Standardbenutzern die Durchführung von Haupt- und Neben-Softwareupdates zu erlauben. Wenn Sie das Kontrollkästchen nicht markieren, können nur Administratoren Haupt- und Neben-Softwareupdates durchführen.
Verzögerungen	
Zeitraum für Hauptupdate in Tagen	Legen Sie die Verschiebung in Tagen für ein Hauptupdate der Betriebssystemsoftware auf dem Gerät fest. Nach der Konfiguration wird das Haupt-Softwareupdate nach der angegebenen Anzahl von

Einstellung	Beschreibung
	Tagen ab Release angezeigt. Sie können einen beliebigen Wert zwischen 1 und 90 Tagen festlegen.
Zeitraum für Nebenupdate in Tagen	Legen Sie die Verschiebung in Tagen für ein Nebenupdate der Betriebssystemsoftware auf dem Gerät fest. Nach der Konfiguration wird das Haupt-Softwareupdate nach der angegebenen Anzahl von Tagen ab Release angezeigt. Sie können einen beliebigen Wert zwischen 1 und 90 Tagen festlegen.
Zeitraum für Systemupdate in Tagen	Legen Sie die Verschiebung in Tagen für ein Systemupdate des Betriebssystems auf dem Gerät fest. Nach der Konfiguration wird das Haupt-Softwareupdate nach der angegebenen Anzahl von Tagen ab Release angezeigt. Sie können einen beliebigen Wert zwischen 1 und 90 Tagen festlegen.
Automatische Aktionen	
Sicherheitsupdate installieren	Wählen Sie eine der folgenden Optionen aus: • **Zulässig**: Der Benutzer kann die Installation von Sicherheitsupdates auf "Ein" oder "Aus" setzen. • **Immer ein**: Die Installation von Sicherheitsupdates steht für den Benutzer immer auf "Ein". • **Immer aus**: Die Installation von Sicherheitsupdates steht für den Benutzer immer auf "Aus".

4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
5. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Einstellungen für Softwareupdate** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
6. Klicken Sie auf **Fertig**.

10.10.4.60. Konfiguration der Sicherheitspräferenzen

Administratoren können Benutzeränderungen an Firewall-Einstellungen, Sperrmeldungen und Passwortänderungen auf dem Gerät über die Konfiguration der Sicherheitseinstellungen verwalten und kontrollieren.

Gilt für: macOS 10.10+

Procedure

1. Gehen Sie zu Konfigurationen > +Hinzufügen.
2. Geben Sie Security in das Suchfeld ein, und klicken Sie dann auf die Konfiguration Sicherheitseinstellungen.
3. Geben Sie einen Namen und eine Beschreibung der Konfiguration ein.
4. Wählen Sie die gewünschten Konfigurationen aus:
    - Änderungen der Firewall-Einstellungen deaktivieren
    - Änderungen der Sperrmeldung deaktivieren
    - Änderungen des Passworts deaktivieren
5. Klicken Sie auf Weiter.
6. Wählen Sie die Option Diese Konfiguration aktivieren.
7. Wählen Sie eine der folgenden Kanaloptionen, um die Konfiguration zu übernehmen:
    - Gerätekanal (am häufigsten)
    - Benutzerkanal (aktuell registrierter Benutzer)
8. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
9. Klicken Sie auf Fertig.

10.10.4.61. Zeitserver

Gilt für: macOS 10.12.4 und unterstützte neuere Versionen.

Erstellen Sie eine Zeitserver-Konfiguration, damit Geräte eine Verbindung zu benutzerdefinierten Zeitservern herstellen können.

Zeitserver-Konfiguration erstellen

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie in dem Suchfeld **time** ein und klicken Sie dann auf die Konfiguration **Zeitserver**.
4. Geben Sie einen Namen ein und beschreiben Sie die Konfiguration.
5. Geben Sie den **NTP-Server** an.
6. Geben Sie die Zeichenfolge für die **Zeitzone** im Olson-Zeitzonen-ID-Format an (z. B. Pacific/Midway). Um das Olson-Zeitzonenformat zu erhalten, führen Sie den Befehl `"/usr/sbin/systemsetup -listtimezones` " auf dem MacOS-Gerät des Administrators aus.
7. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
8. Klicken Sie auf **Fertig**.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.4.62. Web-Content-Filter

Lizenz: Silver

Eine Konfiguration für einen Web-Content-Filter begrenzt den Webzugriff für iOS 7+-, macOS 10.15+- und visionOS 1.1+-Geräte.

Web-Content-Filter-Einstellungen

Einstellung	Aktion
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Zulässige Websites	**Limited Adult Content:** Wählen Sie diese Option aus, wenn Sie den Zugriff auf Websites entsprechend den automatischen Filtern von iOS beschränken wollen. Diese Filter versuchen hochgenau Websites mit unangemessenen Inhalten zu blockieren. **Nur bestimmte Websites:** Wählen Sie diese Option, wenn Sie die zugänglichen Websites manuell auflisten möchten. **Plugin (nur in iOS8 und macOS 10.15 überwacht):** Wählen Sie diese Option, wenn Sie ein Plugin eines Drittanbieters verwenden möchten.
Zulässige URLs	Diese Option ist nur verfügbar, wenn Sie „Nicht jugendfreie Inhalte beschränken“ ausgewählt haben. Geben Sie die zulässigen URLs ein. Jede URL muss entweder mit • http:// oder • https:// Wenn Sie für dieselbe Seite sowohl http:// als auch https:// zulassen möchten, geben Sie zwei separate URLs ein. Alle URLs, deren Anfangszeichen mit der angegebenen zulässigen URL übereinstimmen, sind zugänglich. Beispiel: http://www.someCompanySite.com gestattet den Zugriff auf folgende Seiten: • http://www.someCompanySite.com • http://www.someCompanySite.com/jobs Diese URLs sind auch dann verfügbar, wenn die automatischen iOS-Filter sie zulassen.
Verweigerungsliste für URLs verwenden	Diese Option ist nur verfügbar, wenn Sie „Nicht jugendfreie Inhalte beschränken“ ausgewählt haben. Geben Sie die Blacklist-URLs ein. Jede URL muss entweder mit • http:// oder • https:// Wenn Sie für dieselbe Seite sowohl http:// als auch https:// blockieren möchten, fügen Sie für jede URL eine Zeile ein. Alle URLs, deren Anfangszeichen mit der angegebenen URL auf der schwarzen Liste übereinstimmen, werden gesperrt. Beispiel: http://www.someCompanySite.com blockiert den Zugriff auf folgende Seiten: • http://www.someCompanySite.com • http://www.someCompanySite.com/jobs Diese URLs werden auch dann gesperrt, wenn die automatischen iOS-Filter sie zulassen.
Whitelist-Lesezeichen	Diese Option steht nur zur Verfügung, wenn Sie die Option "Nur spezifische Websites" ausgewählt haben. Optional können Sie den Ordner angeben, in dem das Safari-Lesezeichen hinzugefügt werden soll. Beispiel: /Sales/Products/ Wenn der Ordner fehlt, wird das Lesezeichen dem Standard-Lesezeichenverzeichnis hinzugefügt.

Einstellung	Aktion
Filtername	Diese Option steht nur zur Verfügung, wenn Sie "Plugin" ausgewählt haben. Geben Sie den Text ein, der zur Identifikation dieses Filters angezeigt werden soll.
Identifikator	Diese Option steht nur zur Verfügung, wenn Sie "Plugin" ausgewählt haben. Geben Sie die Bundle-ID des Plugins für den Filterdienst ein.
Dienstadresse	Diese Option steht nur zur Verfügung, wenn Sie "Plugin" ausgewählt haben. Optional: Geben Sie eine benötigte Serveradresse für das Plugin ein. Schlagen Sie in der Dokumentation des Plug-in nach, ob dieser Wert benötigt wird.
Organisation	Diese Option steht nur zur Verfügung, wenn Sie "Plugin" ausgewählt haben. Optional: Geben Sie den für das Plugin benötigten Organisationsstring ein. Schlagen Sie in der Dokumentation des Plug-in nach, ob dieser Wert benötigt wird.
Benutzername	Diese Option steht nur zur Verfügung, wenn Sie "Plugin" ausgewählt haben. Optional: Geben Sie einen für den Plugin-Dienst benötigten Benutzernamen ein. Schlagen Sie in der Dokumentation des Plug-in nach, ob dieser Wert benötigt wird.
Passwort	Diese Option steht nur zur Verfügung, wenn Sie "Plugin" ausgewählt haben. Optional: Geben Sie ein für den Plugin-Dienst benötigtes Passwort ein. Schlagen Sie in der Dokumentation des Plug-in nach, ob dieser Wert benötigt wird.
Zertifikat	Diese Option steht nur zur Verfügung, wenn Sie "Plugin" ausgewählt haben. Optional: Geben Sie ein für den Plugin-Dienst benötigtes Zertifikat zur Authentifizierung des Benutzers ein. Schlagen Sie in der Dokumentation des Plug-in nach, ob dieser Wert benötigt wird.
Webkit-Traffic filtern	Diese Option steht nur zur Verfügung, wenn Sie "Plugin" ausgewählt haben. Klicken Sie hier, um den Webkit-Traffic im Filter zu berücksichtigen.
Socket-Traffic filtern	Diese Option steht nur zur Verfügung, wenn Sie "Plugin" ausgewählt haben. Klicken Sie hier, um den Socket-Traffic im Filter zu berücksichtigen.
Benutzerdefinierte Daten	Diese Option steht nur zur Verfügung, wenn Sie "Plugin" ausgewählt haben. Optional: Geben Sie für den Plugin-Dienst benötigte Schlüssel/Wertpaare ein. Schlagen Sie in der Dokumentation des Plug-in nach, ob dieser Wert benötigt wird.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.4.63. Windows-Firewall

Mit der Konfiguration der Windows-Firewall können Sie die Profileinstellungen der Windows-Firewall sowie die gewünschten anpassbaren Regeln festlegen, die für das Gerät durchgesetzt werden sollen. Mit dieser Konfiguration können Sie Geräte verwalten, die nicht in der Domain angemeldet sind und die Gefahr von Netzwerksicherheitsbedrohungen für alle Systeme reduzieren, die eine Verbindung mit dem Firmennetzwerk haben.

Windows-Firewall konfigurieren

Verfahren

1. Gehen Sie zu Konfiguration > +Hinzufügen.
2. Wählen Sie die Konfiguration **Firewall** aus.
3. Klicken Sie auf das **Windows** -Symbol.
4. Geben Sie einen Namen für die Konfiguration ein.
5. Geben Sie eine Beschreibung für die Firewall-Konfiguration ein.
6. Definieren Sie im Abschnitt "Konfigurations-Setup" die übrigen Einstellungen gemäß der Beschreibung in der folgenden Tabelle.

Einstellung	So gehen Sie vor
Profile	
Aktivieren	Stellen Sie den Schalter auf EIN, um das Profil zu aktivieren.
Typ	Zeigt die Art des Profils an. Beispiel: Domäne.
Standard-Eingangsaktion	Wählen Sie eine Option für eine Standardoption, die bei eingehendem Traffic ausgeführt werden sollte. **Zulassen**: Traffic zulassen **Blockieren**: Traffic blockieren.
Standard-Ausgangsaktion	Wählen Sie die Standardoption, die bei abgehendem Traffic ausgeführt werden sollte. **Zulassen**: Traffic zulassen **Blockieren**: Traffic blockieren.

7. Um Regeln hinzuzufügen, klicken Sie auf **+Hinzufügen** und konfigurieren Sie die folgenden Einstellungen:

Einstellung	So gehen Sie vor
Regeln	
EIN	Verschieben Sie den Schalter, um das Profil zu aktivieren.
Regelbezeichnung	Geben Sie einen Namen ein, der diese Regel bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Regel erläutert.
Richtung	Wählen Sie aus, für welche Richtung des Traffics die Regel verwendet werden soll: • **In**: Für eingehenden Traffic • **Aus**: Für abgehenden Traffic • **Beide**: für beide Richtungen.
Aktion	Wählen Sie die auszuführende Aktion aus. • **Zulassen**: Traffic zulassen • **Blockieren**: Traffic blockieren.
Profil	Wählen Sie die Profile aus, für die die Regel gelten soll: • **Alle** • **Domäne** • **Privat** • **Öffentlich**
[App]	Geben Sie den Paket-Familiennamen (PFN) oder den kompletten Pfad zu der ausführbaren App an.
[Protocol]	Wählen Sie eines der folgenden Protokolle, für die die Regel gelten soll: • **TCP** • **UDP** • **ICMP**
Lokale Adressbereiche	Geben Sie die lokalen Ipv4/IPv6-Adressbereiche oder Subnet-Masken ein.
Lokale Portbereiche	Eine durch Komma getrennte Liste entfernter Ports oder Portbereiche. Beispiel: 20,50,100-120.
Remote Adressbereiche	Geben Sie die entfernten Ipv4/IPv6-Adressbereiche oder Subnet-Masken ein.
Remote Portbereiche	Eine durch Komma getrennte Liste entfernter Ports oder Portbereiche. Beispiel: 20,50,100-120.
Schnittstellentypen	Wählen Sie einen der folgenden Schnittstellentypen aus: • **Alle** • **Fernzugriff** • **Drahtlos** • **LAN**

Einstellung	So gehen Sie vor
	• **Mobiler Breitband-** Die Standardoption Alle wird verwendet, wenn Sie keinen Schnittstellentyp ausgewählt haben.

8. Klicken Sie auf **Weiter**.
9. Wählen Sie eine der folgenden Verteilungsoptionen aus:

- Alle Geräte
- Keine Geräte (Standard)
- Anpassbar

10. Klicken Sie auf **Fertig**.

10.10.4.64. Schutz von Windows-Informationen

Lizenz: Gold

Gilt für: Windows 10+

Die Konfiguration des Schutzes von Windows-Informationen (WIP) definiert die WIP-Einstellungen zum Schutz von Unternehmensdaten. Diese Konfiguration kann für verwaltete und registrierte Geräte übernommen werden. Sie können die WIP-Details für ein konfiguriertes Gerät auch auf der Übersichtsseite des Geräts einsehen.

Informationsschutz für Windows konfigurieren

Verfahren

1. Gehen Sie zu Konfiguration > +Hinzufügen.
2. Wählen Sie die Konfiguration **Schutz von Windows-Informationen** aus.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Definieren Sie in dem Abschnitt Konfigurations-Setup die übrigen Einstellungen aus der folgenden Tabelle.
6. Klicken Sie auf Weiter.
7. Wählen Sie eine Verteilungsebene für diese Konfiguration aus.

Kategorie	Einstellung	Aktion
	[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
	Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Unternehmensinformationen	**Alle Versionen (Windows 10+)**	
	Geschützte Domainnamen	Definieren Sie die Liste der Identitäten, für welche die Datenschutzrichtlinien konfiguriert sind. E-Mails und andere Daten im Zusammenhang mit diesen Identitäten werden als Unternehmensdaten betrachtet und geschützt. • Dies ist eine Liste der Domains, getrennt durch |, wobei die erste Domain in der Liste als primäre Identität für die Windows-Benutzeroberfläche gilt. • Beispiel: "domain1.com|domain2.co.uk"
	Netzwerkdomainnamen	Definieren Sie die Liste der Domains, die die Grenzen des Unternehmens darstellen. Daten aus einer dieser Domänen, die an ein Gerät gesendet werden, werden als Unternehmensdaten betrachtet und geschützt. • Diese Standorte gelten als sicherer Bestimmungsort für Unternehmensdaten, die geteilt werden sollen. • Es handelt sich um eine Domainliste mit Kommas als Trennzeichen. • Beispiel: „mail.domain3.com, domain4.com“
	Cloud-Ressourcen	Enthält eine Liste der Domains mit Unternehmensressourcen, die in der Cloud gehostet sind und geschützt werden müssen. Verbindungen zu diesen Ressourcen werden als Verbindungen mit Unternehmensdaten betrachtet. Definieren Sie mindestens einen Domänennamen mit optionalen Proxyadressen in Klammern. • Beispiel: „domainname1.com, domainname2 (10.0.0.1)“. • Wenn ein Proxy mit einer Cloud-Ressource gekoppelt ist, wird der Traffic zu der Cloud-Ressource über den definierten Proxy-Server auf Port 80 über das Unternehmensnetzwerk geleitet. • Alle in diesem Feld definierten Proxy-Adressen sollten auch in dem folgenden Feld des internen Proxy-Servers eingegeben werden.
	IP-Bereich	Definiert die Unternehmens-IP-Bereiche, die festlegen, welche Computer sich im Unternehmensnetzwerk befinden. Die Daten von diesen Computern werden als Teil des Unternehmens betrachtet und geschützt. Diese Standorte gelten als sicherer Bestimmungsort für Unternehmensdaten, die geteilt werden sollen. Es handelt sich um eine Liste der IPv4- und IPv6-Bereiche mit Komma als Trennzeichen.

Kategorie	Einstellung	Aktion
		• Es handelt sich um eine Liste der IPv4- und IPv6-Bereiche mit Komma als Trennzeichen. • Wählen Sie die Option **IP-Bereiche sind obligatorisch** aus, wenn der Client die konfigurierte Liste akzeptieren soll, ohne eine heuristische Analyse zur Suche anderer Teilnetze durchzuführen.
	Neutrale Ressourcen	definiert die Liste der Domainnamen, die für die Arbeit oder für private Zwecke verwendet werden dürfen.
	Proxy-Server	Definiert eine Liste der Proxy-Server mit Komma als Trennzeichen. Jeder Server in dieser Liste gilt als unternehmensfremder Server. • Beispiel: „157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59“. • Wählen Sie die Option **Proxy-Server sind verbindlich** aus, wenn der Client die konfigurierte Proxy-Liste akzeptieren und nicht versuchen soll, andere betriebliche Proxy-Server zu finden.
Datenschutz	Interne Proxy-Server **Alle Versionen (Windows 10+)**	Definiert die Liste mit den internen Proxy-Servern mit Komma als Trennzeichen. • Beispiel „157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59“. • Diese Proxy-Server wurden vom Administrator konfiguriert, um die Verbindung mit spezifischen Ressourcen im Internet herzustellen. Sie werden als Unternehmensnetzwerkstandorte betrachtet. Die Proxys werden nur bei der Konfiguration der EnterpriseCloudResources-Richtlinie verwendet, um über diese Proxys eine Traffic-Umleitung zu passenden Cloud-Ressourcen zu erzwingen.
	Durchsetzungsebene	Wählen Sie eine der folgenden Stufen für die zwangsweise Umleitung: • Aus – Kein Schutz (zuvor verschlüsselte Daten werden entschlüsselt). • Im Hintergrund – Die Daten und die Audit-Aktivitäten auf dem Gerät werden verschlüsselt, nachdem die Daten geschützt sind. Der Benutzer wird über negative Daten und App-Informationen informiert. • Überschreiben – Ähnlich wie die Option „Im Hintergrund“. Wenn eine App oder Daten falsch verwendet werden, wird der Benutzer außerdem aufgefordert, die aktuelle Operation des Benutzers fortzusetzen oder abzubrechen. • Sperren – Ähnlich dem Modus „im Hintergrund“. Wenn eine App oder Daten falsch verwendet werden, wird bei diesem Modus außerdem die Operation des aktuellen Benutzers gesperrt und der Benutzer gewarnt sowie der Grund für die Sperre genannt. Außer im Modus „Aus“ werden alle Apps oder Daten, die nicht als

Kategorie	Einstellung	Aktion
		Unternehmensdaten oder Unternehmensressourcen betrachtet wurden, auf dem Gerät protokolliert. Diese Daten können bei Verwendung eines anderen Konfigurationsdiensteanbieters (CSP) vom Gerät entfernt werden.
	Datenwiederherstellungszertifikat	Geben Sie ein Wiederherstellungszertifikat an, das für die Datenwiederherstellung verschlüsselter Dateien verwendet werden soll. • Dieses Zertifikat ist identisch mit dem Zertifikat des Datenwiederherstellungsagenten (DRA) zur Verschlüsselung des Dateisystems (EFS). Dieses Zertifikat wird jedoch über MDM und nicht über die Gruppenrichtlinie bereitgestellt. Sie können auch eine oder mehrere der folgenden Optionen auswählen: • Benutzerentschlüsselung zulassen • Bei Aufhebung der Registrierung zurückziehen • EDP-Symbole anzeigen • Schutz bei Sperre erforderlich (nur Windows 10 Mobile)
RMS	**Alle Versionen (Windows 10+)**	
	Azure RMS zulassen	Geben Sie an, ob die Verschlüsselung des Azure Rechtemanagements (Azure RMS) für WIP zulässig ist.
	RMS-Vorlagen-ID	Geben Sie an, ob die TemplateID GUID für die RMS-Verschlüsselung verwendet werden soll. Mit der RMS-Vorlage können Administratoren im Detail konfigurieren, wer wie lange Zugriff auf eine RMS-geschützte Datei hat.
App-Kontrolle	**Alle Versionen (Windows 10+)**	
	Definieren Sie eine App-Sammlung, die auf der Seite **Apps > App-Katalog** mit einem WIP-Wert erstellt wurde. Definieren Sie die Regeln für Apps mit folgendem Parametersatz:	
	App-Typ	Wählen Sie einen der folgenden App-Typen aus: • Publisher/PFN Equals gilt für Windows 10+, die PFN unterstützen. • EXE/Win32 Equals gilt nur für Windows Desktop.
	App-Identifikator	Wählen Sie aus den angezeigten Optionen die App aus, um sie zum App-Identifikator hinzuzufügen. Sie können auch auf die Option **Apps suchen** klicken.
	App-Beschreibung	Geben Sie eine Beschreibung für die App ein.

10.10.4.65. Windows-Einschränkungen

Von den Windows-Einschränkungen hängt ab, welche Funktionen auf Windows 10+-Geräten aktiviert sind.

Windows Einschränkungseinstellungen

Kategorie	Einstellung	Aktion
	[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
	Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Gerätefunktionen	**Alle Versionen (Windows 10+)**	
	WLAN-Offloading deaktivieren	Wählen Sie diese Option aus, um zu verhindern, dass das Gerät auf kompatible Netzwerke zugreift, um Daten zu übertragen, die nur für autorisierte WLANs vorgesehen sind.
	Internet Sharing deaktivieren	Wählen Sie diese Option aus, um zu verhindern, dass das Gerät auf das Internet über andere drahtlose Geräte zugreift.
	Standort deaktivieren	Wählen Sie diese Option aus, um die Standortdienste zu deaktivieren.
	Mobilfunk-Daten-Roaming deaktivieren	Wählen Sie diese Option aus, um Daten-Roaming zu deaktivieren, wenn das Gerät Daten über Mobilfunk übertragen will.
	Bluetooth deaktivieren	Wählen Sie diese Option aus, um zu verhindern, dass das Gerät Bluetooth-Verbindungen aufbaut.
	VPN beim Roaming oder in einem Mobilfunknetz deaktivieren	Wählen Sie diese Option aus, um zu verhindern, dass das Gerät VPN-Verbindungen aufbaut, wenn kein WLAN verfügbar ist.
	Manuelle WLAN-Konfiguration deaktivieren	Wählen Sie diese Option, wenn Sie nicht möchten, dass Benutzer die WLAN-Einstellungen manuell auf dem Gerät konfigurieren können.
	Wi-Fi deaktivieren	Wählen Sie diese Option, um die WLAN-Verbindung zuzulassen oder zu verweigern.
Telemetrie - Erlaubt dem Gerät das Senden von Diagnose- und Nutzungstelemetriedaten.	**Nur für Windows 10**	
	Telemetrieebene	Klicken Sie auf eine der folgenden Telemetrie-Optionen für Datenberichte. • **Sicherheit** – Informationen über das vernetzte Benutzererlebnis, die Telemetrie-Komponenteneinstellungen, das Tool zur Entfernung bösartiger Software und Windows Defender senden. • **Basic** - Basisgeräteinformationen senden, beispielsweise qualitätsrelevante Daten, App-Kompatibilität, App-Nutzungsdaten und Daten aus der Sicherheitsebene.

Kategorie	Einstellung	Aktion
		• **Erweitert** – Weitere Informationen senden, beispielsweise zur Nutzung und den Eigenschaften von Windows, Windows Server, des System Center und der Apps. Erfasst werden auch erweiterte Zuverlässigkeitsdaten sowie Daten der Basis- und der Sicherheitsebene. • **Vollständig (Standard)** - Alle Daten zur Identifikation und Beseitigung von Problemen sowie Daten der Stufen Sicherheit, Basic und Erweitert senden.
Schutz vor Datenverlust (DLP)	**Alle Versionen (Windows 10+)**	
	Kamera deaktivieren	Wählen Sie diese Option aus, um zu verhindern, dass der Endbenutzer die Kamera-App verwendet.
	Zugriff auf Speicherkarte (SD-Karte) deaktivieren	Wählen Sie diese Option aus, um zu verhindern, dass das Gerät auf eine Speicherkarte zugreift.
	Screenshots deaktivieren (nur Desktop)	Wählen Sie diese Option, um zu verhindern, dass mithilfe entsprechender Apps auf dem Gerät Screenshots erstellt werden können.
Datennutzung	USB-Massenspeicher deaktivieren (nur HoloLens)	Wählen Sie diese Option aus, um zu verhindern, dass HoloLens auf Massenspeichergeräte zugreift.
	Windows 10+	
	Kosten von 3G-Verbindungen	Wählen Sie eine der folgenden Optionen aus: • **Uneingeschränkt** - Die Verbindung ist unbegrenzt und nicht durch Nutzungsentgelte und Kapazitätsengpässe eingeschränkt. • **Fest** - Die Verbindung ist durch Nutzungsentgelte und Kapazitätsengpässe auf ein bestimmtes Datenlimit eingeschränkt. • **Variabel** - Die Verbindung wird pro Byte abgerechnet.
	Kosten von 4G-Verbindungen	
Defender	**Windows 10+**	
	Echtzeitüberwachung von Defender deaktivieren	Klicken Sie auf die Option, um die Echtzeit-Überwachungsfunktion von Windows Defender zu deaktivieren.
DeviceGuard	**Windows 10+**	
	Virtualisierungsbasierte Sicherheit (VBS) deaktivieren	Klicken Sie auf die Option, um zu verhindern, dass Sicherheitsdienste durch virtuelle Sicherheit unterstützt werden.

Kategorie	Einstellung	Aktion
	Credential Guard mit virtualisierungsbasierter Sicherheit	Wählen Sie eine der folgenden Optionen aus: • **Deaktiviert** - Deaktivieren Sie Credential Guard mit virtualisierungsbasierter Sicherheit. • **Mit UEFI-Sperre aktiviert** - Aktivieren Sie Credential Guard mit virtualisierungsbasierter Sicherheit mit der Sperre des Unified Extensible Firmware Interface (UEFI). • **Ohne Sperre** aktiviert - Aktivieren Sie Credential Guard mit virtualisierungsbasierter Sicherheit ohne UEFI)-Sperre.
	Plattform-Sicherheitsebene (Plattform-Sicherheitsfunktionen erforderlich)	Wählen Sie eine der folgenden Optionen aus: • **VBS mit sicherem Start** - Wählen Sie diese Option, um virtualisierungsbasierte Sicherheit mit sicherem Start zu aktivieren. • **VBS mit sicherem Start und direktem Speicherzugriff** - Wählen Sie diese Option, um virtualisierungsbasierte Sicherheit mit sicherem Start und direktem Speicherzugriff (DMA) zu aktivieren.
Datenschutz	**Windows 10+**	
	Werbe-ID deaktivieren	Wählen Sie die Option aus, um die Werbe-ID zu deaktivieren.
	Zur Veröffentlichung des Aktivitäts-Feeds durch die Apps/das Betriebssystem deaktivieren	Wählen Sie diese Option aus, um zu verhindern, dass Apps/Betriebssysteme in dem Aktivitäts-Feed posten.
Windows und Anwendung	**Alle Versionen (Windows 10+)**	
	Microsoft-Konten für andere Dienste außer E-Mail deaktivieren	Wählen Sie diese Option aus, um zu verhindern, dass der Endbenutzer andere Dienste außer E-Mail mit Microsoft-Konten authentifiziert.
	Nicht-Microsoft-Konten deaktivieren	Wählen Sie diese Option aus, um zu verhindern, dass der Endbenutzer E-Mail-Konten mit Nicht-Microsoft-Konten konfiguriert.
	Cortana Personal Assistant deaktivieren	Wählen Sie diese Option aus, um zu verhindern, dass der Endbenutzer auf den persönlichen Assistenten von Microsoft zugreift.
	Standortsuche deaktivieren	Wählen Sie diese Option aus, um zu verhindern, dass Suchen unter Verwendung des Gerätestandorts durchgeführt werden.
	Entwicklerfreischaltung deaktivieren	Wählen Sie diese Option aus, um zu verhindern, dass der Endbenutzer Anwendungen per Sideloading installiert. Der

Kategorie	Einstellung	Aktion
		Standardmodus, wenn ein Gerät in MDM registriert wird, ist "SideLoad aktiviert".
	Nur unterstützte 11+-Editionen	
	Konfiguration des Teams-Chat-Symbols in der Taskleiste **Nur unterstützte Windows 10+-Versionen**	Wählen Sie eine der folgenden Optionen aus: • **Anzeigen:** Das Chat-Symbol wird standardmäßig in der Taskleiste angezeigt. Die Benutzer können es über die Einstellungen anzeigen oder ausblenden. • **Ausblenden:** Das Chat-Symbol ist standardmäßig ausgeblendet. Die Benutzer können es über die Einstellungen anzeigen oder ausblenden. • **Deaktiviert:** Das Chat-Symbol wird nicht angezeigt und die Benutzer können es nicht über die Einstellungen anzeigen oder ausblenden. • **Nicht konfiguriert:** Das Verhalten des Chat-Symbols ergibt sich aus den Standardeinstellungen für Ihre Windows-Edition. Änderungen treten erst in Kraft, wenn das Windows-Gerät neu gestartet wird.
	Automatische Aktualisierung von Apps von Microsoft Store deaktivieren	Wählen Sie diese Option aus, um ein automatisches Update der Apps über den Microsoft Store zu verhindern.
	Start aller vorinstallierten oder heruntergeladenen Apps über den Microsoft Store deaktivieren.	Wählen Sie diese Option aus, um zu verhindern, dass Endbenutzer alle vorinstallierten oder heruntergeladenen Apps aus dem Microsoft Store starten. Unterstützt nur die Windows-Editionen Enterprise und Education.
	Apps im Hintergrund starten lassen	Wählen Sie eine der folgenden Optionen aus: • **Kontrolle durch Benutzer:** Der Benutzer kann die Ausführung von Apps im Hintergrund steuern. • **Immer zulassen:** Ermöglicht die Ausführung von Anwendungen im Hintergrund. • **Immer verweigern:** Verhindert die Ausführung von Apps im Hintergrund.
Andere Einschränkungen	**Alle Versionen (Windows 10+)**	
	Registrierung auf der UEM-Plattform und Arbeitsplatzkonto nicht löschen.	Wählen Sie diese Option aus, um zu verhindern, dass der Endbenutzer seine Registrierung auf der UEM-Plattform und das

Kategorie	Einstellung	Aktion
		Image des Firmenkontos löscht.
	Änderung des Verlängerungszeitraums für Gerätesperre durch den Benutzer deaktivieren (nur HoloLens) **Nur unterstützte Windows 10+-Versionen**	Wählen Sie diese Option aus, um zu verhindern, dass der Benutzer den Verlängerungszeitraum bis zur Gerätesperre selbst einstellt.
	Verhindern, dass der Benutzer das Gerät über die Systemsteuerung und eine Hardware-Tastenkombination auf die Werkseinstellungen zurücksetzen kann	Wählen Sie diese Option aus, um zu verhindern, dass der Endbenutzer die Frist bis zur Gerätesperre selbst einstellt.
	Verlangen, dass Benutzer sich bei der Einrichtung des Geräts mit dem Netzwerk verbinden (Autopilot-Profil erforderlich) **Nur unterstützte Windows 11+-Versionen**	Wählen Sie diese Option, um TenantLockdown zu aktivieren und damit alle Windows-Geräte zu sperren, die mit der Autopilot-Funktion registriert wurden.
	Verhindern, dass Benutzer über die Benutzeroberfläche Änderungen an der eSIM vornehmen können.	Wählen Sie diese Option, um zu verhindern, dass Benutzer Änderungen an den eSIM-Profilen vornehmen können.

10.10.4.66. Einschränkungen für Windows Desktop

Gilt für: Windows 10 Desktops

Dieser Abschnitt enthält die folgenden Themen:

- **Einschränkungen für Windows Desktop konfigurieren**
- **Whitelist für entnehmbare Datenträger erstellen**

Administratoren können auf verwalteten Desktops unter Windows 10 kontrollieren, welche Betriebssysteminformationen angezeigt werden, indem sie den Benutzerzugang auf folgende Bereiche des Geräts beschränken:

- Systemsteuerung
- Task Manager
- File Explorer
- Registry-Editor

Die oben erwähnten Funktionen ermöglichen es einem Benutzer, diverse Änderungen auf seinem Gerät vorzunehmen. Mit dieser Funktion können Administratoren den Zugang zu diesen Kontrollen auf Systemebene beschränken und damit den Zugang absichern.

Diese Funktion erfordert Bridge. Details finden Sie unter **Ivanti Bridge**.

Einschränkungen für Windows Desktop konfigurieren

Verfahren

1. Gehen Sie zu **Konfiguration > +Hinzufügen** .
2. Wählen Sie die Konfiguration **Windows Desktop Einschränkungen**.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Definieren Sie in dem Abschnitt Konfigurations-Setup die übrigen Einstellungen aus der folgenden Tabelle.

Einstellung	Aktion
Task Manager **Systemsteuerung** **Registry-Editor**	Klicken Sie in das Kontrollkästchen **Zugriff verweigern** für die Einstellung, zu der der Zugriff verweigert werden soll.
File Explorer	Klicken Sie in das Kontrollkästchen **Funktionen beschränken**, um die Funktionen des Dateiexplorers zu beschränken. Beispiel: Netzwerklaufwerk entfernen. Klicken Sie auf den angegebenen Link, um die Liste der eingeschränkten Funktionen anzuzeigen.
Entnehmbarer Datenträger	
Zugriffsmodus für entnehmbare Datenträger	• **Lesezugriff beschränken**: diese Option verhindert jeglichen Zugriff und ist die restriktivste Konfiguration. • **Schreibzugriff beschränken**: Diese Option erlaubt einen eingeschränkten Zugriff, verhindert aber die Entfernung von Daten durch Unbefugte bzw. ein Hochladen von Viren und anderer Schadsoftware. auf dem Gerät.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:

- Alle Geräte
- Keine Geräte (Standard)
- Anpassbar

8. Klicken Sie auf **Fertig**.

> Damit die Konfiguration voll wirksam wird, muss das Gerät nach Übernahme der Konfiguration neu gestartet werden.

Whitelist für entnehmbare Datenträger erstellen

Wenn Sie eine Whitelist der genehmigten Speichergeräte erstellen wollen, führen Sie zunächst die folgenden Schritte aus:

- Schließen Sie die USB-Speichergeräte an, die Sie auf einem PC zulassen wollen.
- Öffnen Sie den Gerätemanager und klicken Sie auf USB-Controller.
- Suchen Sie in den Einstellungen jedes Controllers die Geräteinformationen.
- Speichern Sie die verwendeten Geräteinformationen zur Erstellung Ihrer Whitelist.

Whitelist für Geräte mit entnehmbarem Datenträger erstellen:

Verfahren

1. Klicken Sie auf der Konfigurationsseite **Windows Desktop Einschränkungen** auf **+Hinzufügen** im Abschnitt **Entnehmbarer Datenträger in der Whitelist**.
2. Geben Sie im Fenster **Hardware-IDs hinzufügen** die Hardware-ID für mindestens ein Gerät ein, das Sie aus der Zulassungsliste entfernen und als Speichergerät blockieren möchten.

3. Klicken Sie auf **Hardware-IDs hinzufügen**. Die Liste der Hardware-IDs in der Whitelist wird im Abschnitt **Entnehmbarer Datenträger in der Whitelist** angezeigt.

> Wählen Sie zum Bearbeiten oder Löschen einer Hardware-ID in der Liste die Option „Bearbeiten“ oder „Löschen“ unter der Spalte Aktionen.
>
> Damit die Konfiguration voll wirksam wird, muss das Gerät nach Übernahme der Konfiguration neu gestartet werden.

10.10.4.67. Desktop-Einstellungen für Windows 10

Mit der Konfiguration der Desktop-Einstellungen für Windows 10 können Sie die Desktop-Einstellungen anpassen und per Push auf Geräte mit Windows 10 übertragen. Mit dieser Konfiguration können Sie folgende Desktop-Einstellungen festlegen:

- Desktop-Hintergrundbild
- Sperrbildschirm
- Benutzerdefinierten Bildschirmschoner hochladen
- Desktop-Tastenkürzel

> Diese Funktion erfordert Bridge. Details finden Sie unter **Ivanti Bridge**.

Verfahren

1. Klicken Sie unter **Konfiguration** auf **+Hinzufügen**.
2. Wählen Sie die Konfiguration Desktop-Einstellungen für Windows 10.Die Seite **Desktop-Einstellungen für Windows 10** wird angezeigt.
3. Geben Sie in dem Feld Name eine passende Bezeichnung der Einstellungen ein.
4. (Optional) Klicken Sie auf den Link +**Beschreibung hinzufügen**, um eine Beschreibung für die Konfiguration hinzuzufügen.
5. Konfigurieren Sie im Abschnitt Konfigurations-Setup folgende Einstellungen:

Einstellung	Beschreibung
Dateizustellung	Wählen Sie eine der folgenden Optionen der Dateizustellung für die Desktop-Einstellungen aus: • **Datei hochladen** – Lädt Einstellungen zu Ivanti Neurons for MDM hoch. • **URL überschreiben**: Ermöglicht ein Überschreiben von URLs mit der Einstellungsdatei, die heruntergeladen werden soll.
Desktop-Wallpapereinstellungen	Klicken Sie auf **Datei wählen**, um ein Hintergrundbild ausfindig zu machen und hochzuladen. Folgende Dateiformate werden unterstützt: BMP, JPG, JPEG und PNG.
Einstellungen für Sperrbildschirm-Wallpaper (Die Hintergrundeinstellung des Sperrbildschirms wird auf Windows 10 Pro-Geräten **NICHT** unterstützt).	Klicken Sie auf **Datei auswählen**, um ein Wallpaper-Bild zu suchen und hochzuladen. Die Dateiformate BMP, JPG, JPEG, PNG werden unterstützt.
Bildschirmschoner-Einstellungen	Klicken Sie auf **Datei auswählen**, um eine Datei für einen Bildschirmschoner zu suchen und hochzuladen. Nur Windows-kompatible .SCR-Dateien hochladen. Wählen Sie **Kennwortschutz für Bildschirmschoner** aus, wenn Sie ein Kennwort zum Beenden des Bildschirmschonermodus festlegen möchten. Wählen Sie eine **Zeitüberschreitung für den Bildschirmschoner** (in Minuten) aus.
Desktop-Tastenkürzel	Klicken Sie auf **Tastenkürzel hinzufügen**, um die Desktop-Tastenkürzel auf Desktops zu ergänzen. Das Fenster **Tastenkombination hinzufügen** wird angezeigt. Füllen Sie die Tabelle mit folgenden Optionen aus: • **Position**: Geben Sie ein, wo das Tastenkürzel auf dem Windows-Gerät angezeigt werden soll. • **Zielpfad** - Geben Sie den lokalen Pfad oder UNC-Pfad oder den Laufwerksbuchstaben ein, zu dem die Verknüpfung führen soll. Der Zielpfad kann auch eine URL sein. • **Argumente**: Geben Sie beliebige Argumente ein, die beim Öffnen der Zieldatei verwendet werden sollen. • **Arbeitsverzeichnis**: Geben Sie den Pfad zu dem Ordner ein, der die für das Ziel benötigten Dateien enthält. • **Symboldatei**: Zum Hochladen gültiger Windows.ico-Dateien. Klicken Sie nach Konfiguration der Optionen auf **Tastenkürzel hinzufügen**.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:
   - Alle Geräte
   - Keine Geräte (Standard)
   - Anpassbar
8. Klicken Sie auf **Fertig**.

10.10.4.68. Konfiguration von Windows Hello for Business

Diese Konfiguration ermöglicht es den Administratoren, Windows Hello auf den Geräten einzurichten. Die Einrichtung von Windows Hello erfordert die Einrichtung einer PIN zur Anmeldung am Gerät.

Gilt für: Windows 10

ProcedureVerfahren

1. Gehen Sie zu Konfigurationen > +Hinzufügen.
2. Geben Sie windows in das Suchfeld ein, und klicken Sie dann auf die Konfiguration Windows Hello for Business.
3. Geben Sie einen Namen und eine Beschreibung der Konfiguration ein.
4. Schalten Sie die Option Windows Hello for Business für Windows 10-Geräte aktivieren/deaktivieren auf Ein.

> Die Umschaltfunktion ist standardmäßig auf Ein eingestellt. Wenn Sie Windows Hello for Business deaktivieren, wird die PIN nicht von den Geräten entfernt.

5. Stellen Sie die PIN-Komplexität ein.
6. Wählen Sie die gewünschten Konfigurationen aus:
    - Erfordert ein Trusted Platform Module (TPM) für Windows Hello for Business
    - Windows Hello for Business-Zertifikate als Smartcard-Zertifikate verwenden
    - Verwendung von biometrischen Gesten, wie Gesicht und Fingerabdruck, als Alternative zur PIN-Eingabe für Windows Hello for Business
    - Erfordert eine verbesserte Anti-Spoofing-Funktion zur Erkennung von Gesichtsmerkmalen bei der Windows Hello-Gesichtsauthentifizierung
    - Dynamische Sperre
    - Ermöglicht es Benutzern, sich mit einem FIDO2-Sicherheitsschlüssel anzumelden.
7. Klicken Sie auf Weiter.
8. Wählen Sie die Option Diese Konfiguration aktivieren.
9. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
10. Klicken Sie auf Fertig.

10.10.4.69. Konfiguration "Windows KI-Verwaltung"

Ivanti Neurons for MDM ermöglicht Administratoren das Verwalten von Windows KI-Einstellungen und -Konfigurationen. Die Windows-KI-Verwaltung bietet einen leistungsstarken KI-Assistenten, der Kreativität und Produktivität verbessert. Verwenden Sie die Konfiguration **Windows-KI-Verwaltung**, um Windows KI-Funktionen auf registrierten Windows-Geräten zu verwalten. Mit dieser Konfiguration können Administratoren Microsoft Copilot-, Windows Recall- und Microsoft Paint AI-Funktionen über Windows AI Configuration Service Anbieter (CSP)-Richtlinien steuern.

Administratoren können ausgewählte KI-Funktionen deaktivieren, den Zugriff auf Copilot-Funktionen entfernen, das Windows Recall-Verhalten steuern und KI-gestützte Funktionen für die Bildgenerierung in Microsoft Paint verwalten.

Gilt für: Windows 10+

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Windows KI-Verwaltung** ausfindig und wählen Sie sie aus.
3. Geben Sie einen **Namen** und eine **Beschreibung** der Konfiguration ein.
4. Wählen Sie im Abschnitt **Konfigurations-Setup** eine der folgenden Optionen aus: ### Copilot-Einstellungen

Einstellung	Beschreibung
Windows-Copilot deaktivieren	Verhindert, dass Benutzer auf Windows Copilot zugreifen können.
Copilot-Hardwareschlüssel deaktivieren	Deaktiviert den dedizierten Copilot-Hardwareschlüssel auf unterstützten Geräten.
Microsoft Copilot App entfernen	Entfernt die Microsoft Copilot-Anwendung vom Gerät.

Rückrufeinstellungen

Einstellung	Beschreibung
KI-Datenanalyse deaktivieren	Deaktiviert die KI-basierte Datenanalyse, die von Windows Recall verwendet wird.
Maximalen Speicherplatz für Recall-Snapshots festlegen (GB)	Gibt die maximale Speichergröße an, die Windows Recall zum Speichern von Snapshots verwenden kann.

Paint AI-Einstellungen

Einstellung	Beschreibung
Image Creator deaktivieren	Deaktiviert die Image Creator-Funktion in Microsoft Paint.
Cocreator deaktivieren	Deaktiviert die Cocreator-Funktion in Microsoft Paint.
Generatives Füllen deaktivieren	Deaktiviert die Funktion für generatives Füllen in Microsoft Paint.

Microsoft hat die von dieser Konfiguration verwendete Richtlinie **TurnOffWindowsCopilot** aufgegeben. Infolgedessen hat diese Konfiguration keine Auswirkungen mehr auf die auf den Geräten vorhandene Copilot-App.

Wenn Sie das Kontrollkästchen **Windows Copilot deaktivieren** nicht markieren, übersteuert die Konfiguration die vorherige Konfigurationsauswahl auf dem Gerät, um die Windows KI-Verwaltung zu aktivieren.

5. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
6. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Windows KI-Verwaltung** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
7. Klicken Sie auf **Fertig**.

10.10.4.70. Play Integrity (ehemals SafetyNet-Bestätigung)

Mit Play Integrity (ehemals SafetyNet) können Sie die Sicherheit und Kompatbilität von Android-Geräten mit den Play Integrity-APIs von Google einfacher bewerten. Nach der Konfiguration können Sie auf diese Weise Geräte in regelmäßigen Zeitintervallen analysieren und prüfen, ob diese manipuliert wurden.

> Play Integrity wird jetzt auf allen Android-Versionen unterstützt.

Verfahren

1. Klicken Sie auf der Registerkarte **Konfiguration** auf **+Hinzufügen**.
2. Wählen Sie die Konfiguration **Play Integrity** aus. Die Seite **Play Integrity-Konfiguration** wird angezeigt.
3. Geben Sie in das Feld **Name** einen geeigneten Namen für die Play Integrity-Konfiguration ein.
4. Klicken Sie auf den Link +**Beschreibung hinzufügen**, um eine Beschreibung für die Konfiguration hinzuzufügen. Dieses Feld ist optional.
5. Geben Sie im Abschnitt **Konfigurations-Setup** das Mindestzeitintervall (in Stunden) für die Prüfung der Sicherheit und Kompatibilität von Geräten ein. Der Wert sollte zwischen 1 und 24 liegen.
6. Klicken Sie auf **Weiter** und wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar

Klicken Sie auf **Fertig**.

> Wenn Play Integrity- und SafetyNet-Einmalwerte an das Gerät gesendet werden, hat die Play Integrity Nonce Vorrang gegenüber der SafetyNet Nonce.

10.10.4.71. Erweiterter Android-Passcode und Sperrbildschirm

Couldn't convert your doc.

10.10.4.72. Microsoft Defender for Endpoint

Die Microsoft Defender for Endpoint (MDE)-Konfiguration (ehemals Windows Advanced Threat Protection) ermöglicht es Kunden, Geräte beim MDE-Dienst an- und abzumelden (Onboarding/Offboarding).

Verfahren

1. Gehen Sie zu **Konfiguration > +Hinzufügen** .
2. Wählen Sie die Konfiguration **Microsoft Defender for Endpoint** aus.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Definieren Sie in dem Abschnitt Konfigurations-Setup die übrigen Einstellungen aus der folgenden Tabelle.

Einstellung	Beschreibung
Onboarding oder Offboarding Blob	Fügen Sie die Onboarding oder Offboarding Blob über die Website von Microsoft Defender for Endpoint Security Center ein.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:

- Alle Geräte
- Keine Geräte (Standard)
- Anpassbar

8. Klicken Sie auf **Fertig**.

10.10.4.73. Zertifikat-basierte Authentifizierung

Ivanti Neurons for MDMunterstützt die Authentifizierung mit Zertifikat, die es Administratoren ermöglicht, sich mit digitalen Zertifikaten und einem vom Mandanten angegebenen Hostnamen (Vanity-Hostname) anzumelden. Bei entsprechender Aktivierung und Konfiguration können sich die Administratoren mit digitalen Zertifikaten statt der Basis-Authentifizierung (mit Benutzername und Passwort) anmelden.

> Diese Funktion ist standardmäßig deaktiviert. Administratoren sollten sich an den Support wenden, um diese Funktion bei ihren Mandanten zu aktivieren. Diese Funktion ist nur in NA3-Cluster-Umgebungen verfügbar, und nur, wenn sie vom Support aktiviert wurde. Stellen Sie sicher, dass Sie Ihren Super-Admin-Benutzernamen und Ihr Passwort getestet und bereit haben, denn sobald die Authentifizierung mit Zertifikaten aktiviert ist, sind diese Anmeldedaten die einzigen, die Sie zur Anmeldung verwenden können, bis Sie Ihre Vanity-Domain erfolgreich konfiguriert haben.

Verfahren

1. Wählen Sie in der Registerkarte Admin die Option Vanity Host-Konfiguration aus.
2. Konfigurieren Sie auf der Seite Vanity Host-Konfiguration folgende Optionen:
3. Klicken Sie auf **Speichern**.
   Es kann einige Minuten dauern, bis Ihr Vanity Host erreichbar ist.

Einstellung	So gehen Sie vor
Vanity Domain erstellen	Geben Sie den Namen der Vanity Domain ein. Dies ist der Domainname, der Ihrer Unternehmensidentität stark ähnelt und bei dem Sie sich mit digitalen Zertifikaten anmelden können.
Vertrauenswürdige Ausstellungs-CA-Zertifikate hochladen	Klicken Sie auf **Datei wählen**, um das CA-Zertifikat auszuwählen und hochzuladen, das Zertifikate für Ihre Administratoren ausstellt. Um die Zertifikatswiderrufsprüfung zu aktivieren, wählen Sie **Aktivieren Sie die Zertifikatsstatus-Validierungseinstellungen für dieses Zertifikat** (optional). Diese Option ist standardmäßig aktiviert. Deaktivieren Sie diese Option, um den Zertifikatwiderruf zu deaktivieren. Klicken Sie auf **Weitere hinzufügen**, um weitere Zertifikate hinzuzufügen. Stellen Sie sicher, dass das Zertifikat im Format .p7b, .pem, .der, .crt oder .cer vorliegt.
Zuordnung von Zertifikatsattributen	Die Zertifikatsattributzuordnung konfiguriert die Zuordnung der Zertifikatsidentitätselemente zu den Kontoattributen des Administrators. Wählen Sie im Feld **Von-Zertifikat** eines der folgenden Zertifikatselemente aus: • **NT-Principal-Name** • **RFC 822-Name** Wählen Sie im Feld **An-Variable** eines der folgenden Kontoattribute des Administrators aus: • **Benutzer-UPN** • **$UserEmailAddress** • **$EDIPI**

10.10.5. Konfigurationen für Benutzerressourcen

Dieser Abschnitt enthält die folgenden Themen:

- CalDAV-Konfiguration
- CardDAV-Konfiguration
- Google-Konfiguration
- E-Mail-Konfiguration
- Konfiguration von Exchange
- Schriftkonfiguration
- Konfiguration für abonnierte Kalender
- Erstellen einer Web-Clip-Konfiguration
- Installation von Office 365
- Windows GPO-Einstellungen
- Konfiguration der BitLocker-Verschlüsselung

10.10.5.1. CalDAV-Konfiguration

Eine CalDAV-Konfiguration definiert den Zugriff auf einen Web-Kalender mithilfe des Internetstandards CalDAV.

CalDAV-Einstellungen

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Hostname und Port	Geben Sie den Host-Namen und den Port für den Kalenderserver ein.
Haupt-URL	Geben Sie die URL für den Zugriff auf Kalenderdienste ein.
Benutzer	Geben Sie den für den Zugriff zu verwendenden Benutzernamen ein.
Passwort	Geben Sie das für den Zugriff zu verwendende Passwort ein.
SSL verwenden	Wählen Sie aus, dass für die Kommunikation zwischen Geräts und Server ausschließlich Secure Socket Layer genutzt wird.
Per-App VPN	**Voraussetzung**: Konfigurieren Sie die Tunnel- oder Per-App-VPN-Konfiguration, bevor Sie Per-App-VPN in der CalDAV-Konfiguration einrichten. Wählen Sie aus dem Dropdown-Menü die vorkonfigurierte Per-App-VPN-Konfiguration aus. **Gilt für**: iOS 14+

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.5.2. CardDAV-Konfiguration

Eine CardDAV-Konfiguration definiert den Zugriff auf ein Web-Adressbuch über den Internetstandard CardDAV.

CardDAV-Einstellungen

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Hostname und Port	Geben Sie den Host-Namen und den Port für den Adressbuchserver ein.
Haupt-URL	Geben Sie die URL für den Zugriff auf Adressbuchdienste ein.
Benutzername	Geben Sie den für den Zugriff zu verwendenden Benutzernamen ein.
Passwort	Geben Sie das für den Zugriff zu verwendende Passwort ein.
SSL verwenden	Wählen Sie aus, dass für die Kommunikation zwischen Geräts und Server ausschließlich Secure Socket Layer genutzt wird.
Per-App VPN	**Voraussetzung**: Konfigurieren Sie die Tunnel- oder Per-App-VPN-Konfiguration, bevor Sie Per-App-VPN in der CardDAV-Konfiguration einrichten. Wählen Sie aus dem Dropdown-Menü die vorkonfigurierte Per-App-VPN-Konfiguration aus. **Gilt für**: iOS 14+
iOS 10+	
Regeln für den Kommunikationsdienst	Wählen Sie eine Standard-Anwendung für Audiogespräche mit Kontakten in dem CardDAV-System aus.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.5.3. Google-Konfiguration

Die Google-Kontokonfiguration verbindet iOS 9.3.2- und visionOS 1.1- oder Android 6.0+-Geräte – oder unterstützte neuere Versionen – mit Google-Konten. Für Google-Konten ist Android Enterprise erforderlich. Bei der Konfiguration können mehrere Google-E-Mail-Adressen sowie weitere Google-Dienste konfiguriert werden, die der Benutzer nach der Authentifizierung aktiviert.

Verfahren

1. Gehen Sie zu **Konfiguration > +Hinzufügen** .
2. Wählen Sie die Konfiguration **Google-Konto** aus.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Definieren Sie in dem Abschnitt für das Konfigurations-Setup die übrigen Einstellungen aus der folgenden Tabelle:

Einstellung	Aktion
iOS 9.3.2+ , Android 6.0+	
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Kontobeschreibung	Geben Sie den Anzeigenamen des Kontos ein.
Kontoname	Geben Sie den vollständigen Namen des Benutzers für das Konto ein.
E-Mail-Adresse	Geben Sie die Google E-Mail-Adresse des Kontos ein.
Per-App VPN	**Voraussetzung**: Konfigurieren Sie die Tunnel- oder Per-App-VPN-Konfiguration, bevor Sie Per-App-VPN in der Google-Konto-Konfiguration einrichten. Wählen Sie aus dem Dropdown-Menü die vorkonfigurierte Per-App-VPN-Konfiguration aus. **Gilt für**: iOS 14+
iOS 10+	
Regeln für den Kommunikationsdienst	Wählen Sie eine Standard-App aus, damit Sie Audioanrufe bei Ansprechpartnern im Google-System tätigen können, indem Sie eine der folgenden Optionen auswählen: • **Aus App-Katalog & System-Apps**: Suchen Sie nach Apps, in denen Sie die ersten Buchstaben der App-Bezeichnung eingeben. • **Bundle-ID eingeben (nur für Apple-Systemanwendungen)**: Geben Sie die Bundle-ID der Systemanwendung ein. Die Bundle-ID muss mit „com.apple“ beginnen.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:
   - Alle Geräte
   - Keine Geräte (Standard)
   - Anpassbar
8. Klicken Sie auf **Fertig**.

Wenn eine Google-Kontokonfiguration für das Gerät übernommen wird, fordert der Go-Client den Benutzer auf, sich bei Google anzumelden.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.5.4. E-Mail-Konfiguration

Eine E-Mail-Konfiguration richtet auf Geräten POP- oder IMAP-E-Mail ein.

E-Mail-Einstellungen

Einstellung	Aktion
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Kontobeschreibung	Geben Sie den Text ein, den Sie zur Identifizierung dieses E-Mail-Kontos verwenden möchten.
Kontotyp	Wählen Sie IMAP oder POP. Wenn Sie IMAP auswählen, können Sie auch das Pfad-Präfix eingeben. Der Internetdienstanbieter kann Ihnen Informationen dazu geben, welcher Kontotyp verfügbar ist. Ein Präfix ist im Allgemeinen erforderlich, wenn alle IMAP-Ordner im Posteingang aufgeführt werden. Internetdienstanbieter, die Präfixe voraussetzen, geben normalerweise Informationen zu dem speziellen Präfix für die Konfiguration an.
Anzeigename des Benutzers	Geben Sie den Text ein, den Sie zur Identifizierung des Benutzers des E-Mail-Kontos verwenden möchten. Hinweis: Auch der Benutzer kann diesen Wert auf dem Geräts einstellen.
E-Mail-Adresse	Geben Sie eine Variable zur Bestimmung der E-Mail-Adresse für das Konto ein.
Verschieben zulassen	Wählen Sie diese Option, wenn Sie nicht verhindern möchten, dass E-Mails von diesem Konto verschoben werden.
S/MIME aktivieren	Wählen Sie diese Option aus, um die Unterstützung für Verschlüsselung mit S/MIME zu aktivieren. Sie können dann die Zertifikate für Signatur und Verschlüsselung auswählen. Erfordert die Zwischenspeicherung von Zertifikaten. Kontrollieren Sie, ob Caching bei der verwendeten Zertifizierungsstelle in der Konfiguration des Identitätszertifikats aktiviert ist. **iOS 10.3+:** Wählen Sie in den betreffenden Feldern eine der folgenden Optionen für die **S/MIME-Signatur** und die **S/MIME-Verschlüsselung** aus: • [Off] • [On] • Benutzer Auswahl **iOS 12.0+:** • Benutzer zum Überschreiben der S/MIME-Signatureinstellungen aktivieren • Benutzer zur Auswahl der S/MIME-Signaturidentität aktivieren • Benutzer zum Überschreiben der S/MIME-Verschlüsselungseinstellungen aktivieren • Benutzer zur Auswahl der S/MIME-Verschlüsselungsidentität aktivieren **Aktivieren Sie ggf. die S/MIME-Signatur und Verschlüsselung für jede Nachricht.**

Einstellung	Aktion
Postfach zulassen	Wählen Sie diese Option aus, um Mail Drop dieses Konto zuzulassen. Mit Mail Drop kann der Benutzer E-Mails mit großen Dateianhängen versenden, indem er den Dateianhang in der iCloud speichert und in der E-Mail nur einen entsprechenden Link einfügt. Weitere Informationen zu Mail Drop finden Sie unter **https://support.apple.com/**
Per-App VPN	Die Möglichkeit, mehrere verschiedene VPN-Profile pro App auf Mail-Domins zuzuordnen, wird von Apple unterstützt. IMAP- und POP3-E-Mail-Konfigurationen werden jetzt über Per-App-VPN unterstützt. **Voraussetzung**: Konfigurieren Sie die Tunnel- oder Per-App-VPN-Konfiguration, bevor Sie Per-App-VPN in der E-Mail-Konfiguration einrichten. Wählen Sie aus dem Dropdown-Menü die Option **Per-App VPN config**.

Eingehende E-Mail

Einstellung	Aktion
Server und Port für E-Mails	Diese Adresse kann Ihnen der Internetdienstanbieter geben.
Benutzername	Geben Sie den Benutzernamen ein, um auf den Server für eingehende E-Mails zuzugreifen. Dieser ist häufig identisch mit der E-Mail-Adresse. Ihr Internetdienstanbieter kann das Format vorgeben.
Authentifizierungstyp	Wählen Sie den vom Internetdienstanbieter festgelegten Authentifizierungstyp aus.
Passwort	Geben Sie das Passwort für den Server für eingehende E-Mails ein.
SSL verwenden	Wählen Sie aus, dass für die Kommunikation zwischen Geräts und Server ausschließlich Secure Socket Layer genutzt wird.

Ausgehende E-Mail

Einstellung	Aktion
Server und Port für E-Mails	Diese Adresse kann Ihnen der Internetdienstanbieter geben.
Benutzername Authentifizierungstyp Passwort	Geben Sie den Benutzernamen ein, um auf den Server für ausgehende E-Mails zuzugreifen. Dieser ist häufig identisch mit der E-Mail-Adresse. Ihr Internetdienstanbieter kann das Format vorgeben. Wählen Sie den vom Internetdienstanbieter festgelegten Authentifizierungstyp aus. Geben Sie das Passwort für den Server für ausgehende E-Mails ein.
Passwort für ausgehenden E-Mailserver identisch mit dem für eingehende E-Mails	Wählen Sie wenn die SMTP-Authentifizierung dasselbe Passwort wie POP/IMAP verwendet.
Nur in E-Mail verwenden SSL verwenden	Damit bestimmen Sie, dass diese Konfiguration nur vom E-Mail-Client genutzt werden soll. Weitere Apps, die E-Mails verschicken, einschließlich Apps, die Inhalte mit dem nativen E-Mail-Client verschicken, können diese Konfiguration nicht nutzen. Wählen Sie aus, dass für die Kommunikation zwischen Geräts und Server ausschließlich Secure Socket Layer genutzt wird.

10.10.5.5. Konfiguration von Exchange

In einer Exchange-Konfiguration wird die ActiveSync-basierte E-Mail auf Android-, iOS und visionOS-Geräten sowie die Exchange Web Services-basierte E-Mail (EWS) für macOS-Geräte definiert.

> Die Exchange-Konfiguration wird auf Android 9 von Samsung eingestellt. Bei Samsung-Geräten mit Android 9 und späteren Versionen wird die Exchange-Konfiguration im Geräte-Admin-Modus nicht unterstützt.

Exchange:Einstellungen

Einstellung	Aufgabe
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Exchange-Host	Wenn Sie **Sentry** zur Kontrolle von E-Mail-Zugriffen verwenden, geben Sie den Hostnamen des Sentry-Servers ein. Geben Sie ansonsten die Adresse des ActiveSync-Servers ein.*
Verschieben zulassen	**Für iOS und Android:** Wählen Sie diese Option, wenn Sie nicht verhindern wollen, dass E-Mails aus diesem Konto verschoben werden. **Für Windows 10:** Nicht zutreffend.
S/MIME aktivieren	Wählen Sie diese Option, um die Unterstützung von Verschlüsselung mit S/MIME zu aktivieren. Sie können dann die Zertifikate für Signatur und Verschlüsselung auswählen. Erfordert die Zwischenspeicherung von Zertifikaten. Kontrollieren Sie, ob Caching bei der verwendeten Zertifizierungsstelle in der Konfiguration des Identitätszertifikats aktiviert ist. **iOS 10.3+:** Wählen Sie in den betreffenden Feldern eine der folgenden Optionen für die **S/MIME-Signatur** und die **S/MIME-Verschlüsselung** aus: • [Off] • [On] • Benutzer Auswahl **iOS 12.0+:** • Benutzer zum Überschreiben der S/MIME-Signatureinstellungen aktivieren • Benutzer zur Auswahl der S/MIME-Signaturidentität aktivieren • Benutzer zum Überschreiben der S/MIME-Verschlüsselungseinstellungen aktivieren • Benutzer zur Auswahl der S/MIME-Verschlüsselungsidentität aktivieren **Aktivieren Sie ggf. die S/MIME-Signatur und Verschlüsselung für jede Nachricht.**
Zuletzt benutzte E-Mail-Adressen synchronisieren	Wählen Sie diese Option, um kürzlich kontaktierte E-Mail-Adressen zwischen dem Gerät und dem Server zu synchronisieren.
Nur in E-Mail verwenden	Wählen Sie, ob diese Konfiguration nur vom E-Mail-Client verwendet werden soll. Weitere Apps, die E-Mails verschicken, einschließlich Apps, die Inhalte mit dem nativen E-Mail-Client verschicken, können diese Konfiguration nicht nutzen.
SSL verwenden	Wählen Sie aus, dass für die Kommunikation zwischen Geräts und Server ausschließlich Secure Socket Layer genutzt wird.
OAuth für Exchange-Payload aktivieren	iOS 12.0+ und macOS 10.14+: Wählen Sie diese Option, um die Authentifizierung über OAuth zu aktivieren. Wenn diese Option aktiviert ist, sind die folgenden zusätzlichen Einstellungen für E-Mail-Apps verfügbar, die die Authentifizierung mit OAuth unterstützen: • OAuth-Anmelde-URL • OAuth-Token-Anforderungs-URL

Einstellung	Aufgabe
Domäne	Geben Sie die Domain für dieses E-Mail-Konto ein, es sei denn, Sie wünschen, dass der Benutzer zur Eingabe aufgefordert wird.
Benutzer	Geben Sie eine Variable für die E-Mail-Adresse für dieses Konto ein.
Konto-Passwort	Geben Sie das Passwort für dieses Konto ein, es sei denn, Sie wünschen, dass der Benutzer zur Eingabe aufgefordert wird.
E-Mail-Adresse	Geben Sie eine Variable für die E-Mail-Adresse für dieses Konto ein.
Tage seit letzter E-Mail-Synchronisierung	Wählen Sie die Anzahl der Tage, an denen E-Mails zwischen dem Gerät und dem Server synchronisiert werden sollen.
Per-App VPN	Voraussetzung: Konfigurieren Sie die Tunnel- oder Per-App-VPN-Konfiguration, bevor Sie Per-App-VPN in der Sync-Konfiguration einrichten. Wählen Sie aus dem Dropdown-Menü die vorkonfigurierte Per-App-VPN-Konfiguration aus. **Gilt für**: iOS 14+
Android und Windows	
Kalender synchronisieren	**Für Android und Windows 10:** Wählen Sie diese Option, um Kalendereinträge zwischen Gerät und Server zu synchronisieren. **Bei Samsung-Geräten:** Diese Einstellung wird nicht verwendet (sie ist standardmäßig aktiviert). **Für die App Android Email+:** Diese Einstellung wird verwendet.
Kontakte synchronisieren	**Für Android und Windows 10:** Wählen Sie diese Option, um Kontakte zwischen Gerät und Server zu synchronisieren. **Bei Samsung-Geräten:** Diese Einstellung wird nicht verwendet (sie ist standardmäßig aktiviert). **Für die App Android Email+:** Diese Einstellung wird verwendet.
E-Mail synchronisieren	**Für Android und Windows 10:** Wählen Sie diese Option, um E-Mails zwischen Gerät und Server zu synchronisieren. **Bei Samsung-Geräten:** Diese Einstellung wird nicht verwendet (sie ist standardmäßig aktiviert). **Für die App Android Email+:** Diese Einstellung wird nicht verwendet (sie ist standardmäßig AKTIVIERT).
Aufgaben synchronisieren	**Für Android und Windows 10:** Wählen Sie diese Option, um Aufgaben zwischen Gerät und Server zu synchronisieren. **Bei Samsung-Geräten:** Diese Einstellung wird nicht verwendet (sie ist standardmäßig aktiviert). Für die App Android Email+: Nicht zutreffend.
iOS 13.0+ • Kalender synchronisieren • Kontakte synchronisieren	Legen Sie die individuelle Synchronisation von Outlook Exchange-Elementen wie Kalender, Kontakte, E-Mail, Notizen und Erinnerungen fest. Setzen oder entfernen Sie für jedes Element die Optionen **Aktivieren** und **Überschreibung durch Benutzer zulassen**. Die Synchronisation muss für mindestens eines dieser Elemente aktiviert sein. Wenn Sie die

Einstellung	Aufgabe
• Mail synchronisieren • Notizen synchronisieren • Synchronisierungs-Erinnerungen	Synchronisation für eine Option deaktivieren, dem Benutzer aber erlauben, die Einstellung zu überschreiben, kann der Benutzer sie trotzdem aktivieren.
Identitätszertifikat	Wählen Sie ein Identitätszertifikat aus der Liste, wenn Sie wünschen, dass das Gerät auf dem Server mit einem Zertifikat authentifiziert wird. Die Zertifikate werden in dieser Liste nur dann angezeigt, wenn sie bereits mit einer Konfiguration für Identitätszertifikate konfiguriert wurden.
Android-	
Nur Authentifizierung mit Zertifikaten verwenden.	Benutzen Sie das ausgewählte Identitätszertifikat als einziges Mittel zur Authentifizierung gegenüber dem Exchange-Server.
Alle SSL-Zertifikate akzeptieren	Wählen Sie diese Option, um Benutzern zu gestatten, Android-Geräte so einzustellen, dass diese alle SSL-Zertifikate akzeptieren. Diese Einstellung gilt für Android Email+ und Samsung Knox Email. • Seien Sie beim Aktivieren dieser Einstellung vorsichtig, da Benutzer das Gerät unwissentlich Angriffen aussetzen könnten. • Diese Option muss aktiviert werden, wenn das Sentry-Zertifikat ein unbekanntes oder selbst signiertes Zertifikat ist.
App-Priorität ändern	Wählen Sie den E-Mail-Client aus, der standardmäßig auf Android-Geräten konfiguriert werden soll - Android Email+ und Samsung Email. Die App Email+ wird im App Catalog für alle Mandanten hinzugefügt, die die Priorität der Exchange-App aktiviert haben.
iOS 10+	
Regeln für den Kommunikationsdienst	Wählen Sie eine Standard-Anwendung für Audiogespräche mit Kontakten in dem CardDAV-System aus.
Nur Windows 10+	
Outlook konfigurieren	Wählen Sie diese Option aus, um Microsoft Outlook auf einem Gerät zu konfigurieren. Diese Option wird nur unterstützt, wenn Bridge aktiviert ist.

*Geben Sie „$“ ein, um eine Liste mit unterstützten **Variablen** anzuzeigen, sofern dies für dieses Feld verfügbar ist.

10.10.5.6. Schriftkonfiguration

Eine Schriftkonfiguration ermöglicht es Ihnen, iOS 7-Geräte mit zusätzlichen TrueType- oder OpenType-Schriftartdateien auszustatten. In der folgenden Tabelle sind die Schriftarteinstellungen beschrieben:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Schriftarten hochladen	Ziehen Sie die Schriftartdatei in das gepunktete Feld oder klicken Sie auf **Datei auswählen**, um sie aus Ihrem Dateisystem auszuwählen. Die Schriftartdateien müssen das Format .otf oder .ttf haben.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.5.7. Konfiguration für abonnierte Kalender

Eine Konfiguration für abonnierte Kalender bestimmt den Zugriff auf einen öffentlichen Web-Kalender.

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
[URL]	Geben Sie die URL für den Zugriff auf den Kalender ein.*
Benutzer	Geben Sie den für den Zugriff zu verwendenden Benutzernamen ein.*
Passwort	Geben Sie das für den Zugriff zu verwendende Passwort ein.
SSL verwenden	Wählen Sie aus, dass für die Kommunikation zwischen Geräts und Server ausschließlich Secure Socket Layer genutzt wird.

Variables.htm Geben Sie „$“ ein, um eine Liste mit unterstützten Variablen anzuzeigen, sofern diese für dieses Feld verfügbar ist.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.5.8. Erstellen einer Web-Clip-Konfiguration

Ein Web-Clip ist eine direkte Verknüpfung zu einer Website bzw. Internetseite auf einem iOS-Gerät. Eine Web-Clip-Konfiguration dient zum Erstellen von Standard-Web-Clips auf Geräten. Sie können ein Web-Clip-Symbol zu Ihrem iOS-Gerät hinzufügen und darüber eine bestimmte Website aufrufen. Mit Web-Clips können Sie Lesezeichen auf den Startbildschirmen Ihrer Geräte schnell ausfindig machen und verwenden. Auch einige der Parameter der Mobile Safari-Anzeige für die Website lassen sich darüber steuern.

> Für diese Konfiguration ist die Delegierung mit benutzerdefinierter Verteilung verfügbar. Weitere Informationen finden Sie unter *Verteilen der Konfiguration* unter **Arbeiten mit Konfigurationen**.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Klicken Sie auf **Konfigurationen**.
3. Klicken Sie auf +Hinzufügen.
4. Machen Sie die Web-Clip-Konfiguration ausfindig und wählen Sie sie aus.
5. Konfigurieren Sie die Einstellungen auf dieser Seite. Hinweise zu den Werten finden Sie in der Tabelle unter dem Thema **Einstellungen für Web-Clip-Konfiguration**.
6. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
7. Wählen Sie **Benutzerdefiniert** und dann **Geräte/Gerätegruppen** aus.
8. Klicken Sie auf **Fertig**.

Einstellungen für Web-Clip-Konfiguration

In der folgenden Tabelle sind die Einstellungen für die Web-Clip-Konfiguration aufgeführt:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Bezeichnung	Geben Sie den gewünschten Text ein, der auf dem Bildschirm des Gerät unter der Verknüpfung angezeigt werden soll.
[URL]	Geben Sie die URL ein, auf die der Web-Clip zugreifen wird.*
Entfernbar	Markieren Sie das Kontrollkästchen, um dem Benutzer des Geräts zu gestatten, den Web-Clip zu löschen.
Symbol	Ziehen Sie die Symboldatei in das gepunktete Feld oder klicken Sie auf **Datei auswählen**, um sie aus Ihrem Dateisystem auszuwählen.
Vorgefertigtes Symbol	Wählen Sie diese Option zum Deaktivieren der Spezialeffekte, die von aktuellen Safari-Versionen hinzugefügt werden.
Vollbild	Wählen Sie diese Option, um den Web-Clip statt als Browserinhalt im Vollbildmodus anzuzeigen.
Manifestbereich ignorieren	Wählen Sie diese Option aus, um die Navigation zu einer externen Website ohne Anzeigen des Safari-Browsers anzuzeigen. Diese Option ist nur wirksam, wenn der Vollbildmodus aktiviert ist.
Bundle-ID für Zielanwendung	Die Anwendungs-Bundle-ID gibt an, welche Anwendung die URL öffnet. **Beispiel**: com.google.chrome.ios

> Variables.htmGeben Sie „$“ ein, um eine Liste mit unterstützten Variablen anzuzeigen, sofern diese für dieses Feld verfügbar ist.

Verwandte Themen:

- Sichere Anmeldung für mehrere Benutzer in iOS
- Erstellen einer Konfiguration

10.10.5.9. Installation von Office 365

Lizenz: Silver

Gilt für: Windows 10+

Installation von Office 365 konfigurieren

Die Installation von Office 365 ist eine Konfigurationseinstellung, die für ausgewählte Geräte zur Installation oder Deinstallation von Office 365 übernommen werden kann. Sie können die Konfigurationseinstellungen im xml-Format mit dem Bereitstellungstool von Microsoft Office definieren und dann die Datei hochladen. Nach dem Hochladen der Dateien können Sie die Konfigurationsoptionen per Push auf die ausgewählten Geräte übertragen.

Verfahren

1. Klicken Sie auf der Registerkarte **Konfiguration** auf **+Hinzufügen**.
2. Wählen Sie die Option **Office 365 Installation**. Die Seite **Installation von Office 365** wird angezeigt.
3. Geben Sie in dem Feld **Name**die entsprechende Bezeichnung der Konfiguration ein.
4. Klicken Sie auf den Link + **Beschreibung hinzufügen** , um eine Beschreibung für die Konfiguration zu ergänzen. Dieses Feld ist optional.
5. Aktualisieren Sie in dem Abschnitt **Konfigurations-Setup** folgende Felder:

Feldname	Beschreibung
Konfigurationsdatei zur Installation von Office 365	Klicken Sie auf die Schaltfläche **Datei auswählen**, um die Konfigurationsdatei im XML-Format zu suchen und auszuwählen, die die definierten Einstellungen zur Installation von Office 365 enthält. Beispiel: <Configuration> <Add OfficeClientEdition="64" Channel="Current"> <Product ID="O365ProPlusRetail"> <Language ID="en-us"/> </Product> </Add> </Configuration> Achten Sie darauf, dass die Konfigurationsdatei im xml-Format gespeichert ist und das grüne Häkchen angezeigt wird, nachdem Sie die Konfigurationseinstellungsdatei ergänzt haben.
Konfigurationsdatei zur Deinstallation von Office 365	Klicken Sie auf die Schaltfläche **Datei auswählen**, um die Konfigurationsdatei im XML-Format zu suchen und auszuwählen, die die definierten Einstellungen für die Deinstallation von Office 365 enthält. Beispiel: <Configuration> <Remove All="TRUE"/><Display Level="None" AcceptEULA="TRUE" /> </Configuration> Achten Sie darauf, dass die Konfigurationsdatei im xml-Format gespeichert ist und das grüne Häkchen angezeigt wird, nachdem Sie die Konfigurationseinstellungsdatei ergänzt haben.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Optionen aus, um die Einstellungen auf die Geräte zu verteilen.

Option	Beschreibung
Diese Konfiguration aktivieren	Durch einen Klick in das Kontrollkästchen aktivieren Sie die Konfiguration für die ausgewählten Geräte. Durch Deaktivierung des Kontrollkästchens entfernen Sie die Konfiguration, die bereits für Geräte übernommen wurde.
Alle Geräte	Diese Option verteilt die Einstellungen auf alle Geräte.
Keine Geräte	Diese Option zieht die Einstellungen zurück, die auf die Geräte verteilt werden sollen.
Anpassbar	Diese Option verteilt die Einstellungen auf eine definierte Gerätegruppe. Klicken Sie in das Kontrollkästchen neben der Geräteart, für die Sie die Einstellung verteilen wollen. Sie können alternativ auch nach Gerätegruppen suchen, indem Sie den Namen der Gerätegruppe in dem Suchfeld **Gerätegruppen suchen** eingeben. Wenn Sie eine neue Gerätegruppe erstellen wollen, klicken Sie am unteren Rand der Seite auf den Link **Neue Gerätegruppe erstellen**. Weitere Informationen finden Sie unter **Gerätegruppen**. Wenn Sie die Gerätekategorie auswählen, sehen Sie die Details (Name, Telefonnummer und Geräteart) in der Liste der Gerätebenutzer für die ausgewählte Gerätekategorie im Abschnitt Verteilungsübersicht.

8. Klicken Sie auf **Fertig**, um die Einstellung per Push auf die ausgewählten Geräte zu übertragen.

10.10.5.10. Windows GPO-Einstellungen

Lizenz: Bridge

Für: Windows Desktop

Windows GPO Einstellungen konfigurieren

Ein Gruppen-Richtlinien-Objekt (GPO) ist eine Sammlung von Einstellungen, die festlegt, welche Berechtigungen die Geräte haben bzw. nicht haben. Zur Verwaltung der GPO-Einstellungen müssen Sie Bridge konfiguriert haben. Weitere Details finden Sie unter **Ivanti Bridge**.

Kontaktieren Sie den Standort-Administrator, wenn die GPO-Metadaten nicht in die Datenbank hochgeladen sind. Die GPO-Konfiguration wird über PowerShell-Scripts und Bridge für die Geräte bereitgestellt. Mit den GPO-Einstellungen können Sie spezifische Geräteeinstellungen konfigurieren und per Push übertragen.

Verfahren

1. Klicken Sie auf der Registerkarte **Konfiguration** auf **+Hinzufügen**.
2. Wählen Sie die Konfiguration **Windows GPO-Einstellungen**. Die Seite mit den **Windows GPO-Einstellungen** wird angezeigt.
3. Geben Sie in dem Feld **Name** eine passende Bezeichnung der Windows-GPO-Einstellungen ein.
4. Klicken Sie auf den Link **+Beschreibung hinzufügen**, um eine Beschreibung für die Konfiguration hinzuzufügen. Dieses Feld ist optional.
5. Klicken Sie in dem Abschnitt „Konfigurations-Setup“ auf **+Hinzufügen**. Das Fenster **Windows Gruppen-Richtlinien-Objekt (GPO) hinzufügen** wird angezeigt.
6. Suchen und wählen Sie eine GPO, indem Sie auf die betreffende Komponente in dem GPO-Hierarchiebaum auf der linken Seite klicken. Der GPO-Hierarchiebaum entspricht dem Pfad der Richtlinieneinstellungen. Sie können auch nach einer bestimmten GPO-Einstellung suchen, indem Sie den Namen der GPO-Einstellung in dem Suchfeld eingeben.
   Wenn Sie eine GPO-Einstellung ausgewählt haben, können Sie die Details der ausgewählten GPO-Einstellungen auf der rechten Seite anzeigen.
7. In dem Feld **Einstellungsstatus** sind folgende Einstelloptionen verfügbar:

Option	Beschreibung
Nicht konfiguriert	Entfernt vorhandene GPO-Einstellungen.
Aktiviert	Aktiviert die GPO-Einstellungen.
Deaktiviert	Deaktiviert die GPO-Einstellungen.

8. Geben Sie in dem Feld **Einstellungswert** einen geeigneten Namen für das GPO ein.
   Klicken Sie zum Hinzufügen weiterer Einstellungswerte auf das Symbol **+**. Manche GPO-Einstellungen erfordern keinen zusätzlichen Einstellwert. Manche Einstellungen erfordern zusätzliche Daten, die unter "Wert einstellen" in Form eines Textes angegeben werden müssen. Bei solchen Einstellungen wählen Sie einen beliebigen Wert aus dem Dropdownmenü aus.

> Dieses Feld lässt sich nur bearbeiten, wenn die Option Aktiviert unter Einstellungsstatus ausgewählt ist.

9. Klicken Sie auf **Speichern & Schließen**, um das GPO zu speichern und das Fenster zu schließen. Wenn Sie ein anderes GPO ergänzen wollen, klicken Sie auf **Speichern & andere hinzufügen**, um das GPO zu speichern und das GPO-Fenster offen zu lassen.
   Die hinzugefügte GPO-Einstellung erscheint in dem Abschnitt Konfigurations-Setup.

> Sie können eine GPO-Einstellung bearbeiten oder löschen, indem Sie auf die betreffenden Symbole in der Spalte Aktionen klicken.

OptionBeschreibungDiese Konfiguration aktivieren Durch einen Klick in das Kontrollkästchen aktivieren Sie die Konfiguration für die ausgewählten Geräte. Durch Deaktivierung des Kontrollkästchens entfernen Sie die Konfiguration, die bereits für Geräte übernommen wurde.**Alle Geräte**Diese Option verteilt die Einstellungen auf alle Geräte.**Keine Geräte**Diese Option zieht die Einstellungen zurück, die auf die Geräte verteilt werden sollen.**Anpassbar**Diese Option verteilt die Einstellungen auf eine definierte Gerätegruppe. Klicken Sie in das Kontrollkästchen neben der Geräteart, für die Sie die Einstellung verteilen wollen. Sie können alternativ auch nach Gerätegruppen suchen, indem Sie den Namen der Gerätegruppe in dem Suchfeld **Gerätegruppen suchen** eingeben. Wenn Sie eine neue Gerätegruppe erstellen wollen, klicken Sie am unteren Rand der Seite auf den Link **Neue Gerätegruppe erstellen**. Weitere Informationen finden Sie unter Gerätegruppen.

Wenn Sie die Gerätekategorie auswählen, sehen Sie die Details (Name, Telefonnummer und Geräteart) in der Liste der Gerätebenutzer für die ausgewählte Gerätekategorie im Abschnitt Verteilungsübersicht.

10. Klicken Sie auf **Fertig**, um die GPO-Einstellung für die ausgewählten Geräte per Push zu übertragen.

10.10.5.11. Konfiguration der BitLocker-Verschlüsselung

Lizenz: Bridge

Für: Windows Desktop

Dieser Abschnitt enthält die folgenden Themen:

- BitLocker-Verschlüsselung konfigurieren
- BitLocker-Einstellungen anzeigen

BitLocker-Verschlüsselung konfigurieren

Die BitLocker-Verschlüsselung ist eine Funktion, die zum Datenschutz eine Verschlüsselung von Festplatten und entnehmbaren Laufwerken der Geräte erzwingt. Voraussetzung dafür ist eine Bridge-Konfiguration für die Verwaltung der BitLocker-Verschlüsselung. Weitere Details finden Sie unter **Bridge**. In der BitLocker-Verschlüsselungskonfiguration können Sie die Verschlüsselungseinstellungen für die Geräte konfigurieren.

Verfahren

1. Klicken Sie auf der Registerkarte **Konfiguration** auf **+Hinzufügen**.
2. Klicken Sie auf **BitLocker-Verschlüsselungs**-Konfiguration. Die Seite **BitLocker-Verschlüsselung** wird angezeigt.
3. Geben Sie in dem Feld **Name** eine passende Bezeichnung für die BitLocker-Verschlüsselung ein.
4. Klicken Sie auf den Link **Beschreibung hinzufügen**, um eine Beschreibung für die Konfiguration hinzuzufügen. Dieses Feld ist optional.
5. Konfigurieren Sie im Abschnitt „Konfigurations-Setup“ folgende Einstellungen:

Einstellung	Beschreibung
Verschlüsselungsverfahren und Verschlüsselungsart	Wählen Sie die Art des Verschlüsselungsalgorithmus entsprechend der Schlüsselgröße für die Verschlüsselung aus. Folgende Optionen stehen zur Verfügung: • **AES-CBL 128 Bit** • **AES-CBL 256-Bit**
Alle Hardwarelaufwerke verschlüsseln	Klicken Sie auf die Umschalttaste, um **die Einstellung zur Verschlüsselung aller Hardware-Laufwerke** ein- **oder** abzuschalten. Wenn auf einem Gerät bereits ein Hardware-Laufwerk verschlüsselt ist, wird die bearbeitete Konfiguration nicht übernommen, da der Verschlüsselungsprozess durch Bearbeitung nicht umkehrbar ist.
Laufwerke auswählen	Wählen Sie das zu verschlüsselnde Laufwerk aus. Beispiel: **C:** Klicken Sie auf **+Hinzufügen**, um weitere Laufwerke hinzuzufügen. Dieses Feld wird nicht angezeigt, wenn Sie die Option **Alle Hardware-Laufwerke verschlüsseln** eingeschaltet haben.
Hardware-Verschlüsselung für Laufwerksarten Markieren Sie (optional) die folgenden Kontrollkästchen für die Konfiguration: • **Schreibzugriff auf Festplatten verweigern, die nicht mit BitLocker geschützt sind.** • **Schreibzugriff auf entnehmbare Datenträger verweigern, die nicht**	Das Trusted Platform Module (TPM) ist ein Chip auf der Hauptplatine des Computers, der eine manipulationssichere Verschlüsselung unterstützt. Wenn Sie die BitLocker-Verschlüsselung oder Geräteverschlüsselung auf einem Computer mit TPM einsetzen, wird ein Teil des Schlüssels in dem TPM gespeichert. Sie können folgende Einstelloptionen für die Hardware-Verschlüsselung aus der Dropdown-Liste auswählen. • **TPM beim Start anfordern** • **Start-PIN mit TPM anfordern** • **TPM nicht verwenden** Die TPM-Option steht nur für Laufwerke mit dem Betriebssystem und ab TPM-Version 1.2 zur Verfügung. Sobald Sie eine Hardware-Verschlüsselungseinstellung auf einem Gerät übernehmen, können Sie diese Einstellung auf dem Gerät nicht länger bearbeiten. Wenn für ein Gerät bereits eine BitLocker-Konfiguration eingestellt ist, können Sie nicht mit einer anderen TPM-Option eine zweite BitLocker-Konfiguration übertragen.

Einstellung	Beschreibung
mit BitLocker geschützt sind.	
Aktion vor der Geräteverschlüsselung	Legen Sie mit einer der folgenden Optionen fest, wie mit dem Laufwerk umgegangen werden soll, das noch nicht vollständig entschlüsselt ist oder bereits über einen Schlüsselschutz verfügt. • Verschlüsselung beenden - Stoppt die Verschlüsselung, wenn eines der ausgewählten Laufwerke bereits verschlüsselt ist. • Das ausgewählte Laufwerk entschlüsseln, das nicht über einen Wiederherstellungs-Kennwortspeicher in Ivanti Neurons for MDM verfügt – Wählen Sie diese Option aus, um nur Laufwerke auszuwählen, die kein Wiederherstellungskennwort in Ivanti Neurons for MDM besitzen.
Wiederherstellungsoptionen	Die Wiederherstellungsoption wird verwendet, wenn ein Benutzer das Passwort vergessen hat. Sie können sie auf der Seite mit den Gerätedetails abrufen. Sie können folgende Wiederherstellungsoptionen konfigurieren: • **Wiederherstellung deaktivieren** • **Passwort verwenden und in AD speichern** • **Passwort verwenden und in AD sowie MobileIron speichern**
Neustartintervall	Nachdem die Konfiguration auf das Gerät übertragen wurde, erhalten Sie die Aufforderung zum Neustart. Nach dem Neustart beginnt die Verschlüsselung. Um das Neustart-Intervall zu konfigurieren, wählen Sie in der Dropdown-Liste die Zeitdauer aus, die das Gerät bis zum Neustart warten soll. Das Neustart-Intervall beträgt mindestens 1 Minute und maximal 120 Minuten (2 Stunden).
Neustart-Mitteilung	Geben Sie die Neustart-Mitteilung ein, die auf dem Gerät angezeigt werden soll. Gegebenenfalls wird dem Benutzer das Start-Passwort bzw. die Start-PIN ebenfalls angezeigt. Der Benutzer kann das Passwort bzw. die PIN notieren und nach dem Neustart wieder eingeben.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Optionen aus, um die Einstellungen auf die Geräte zu verteilen.

Einstellung	Beschreibung
Diese Konfiguration aktivieren	Durch einen Klick in das Kontrollkästchen aktivieren Sie die Konfiguration für die ausgewählten Geräte. Durch Deaktivierung des Kontrollkästchens entfernen Sie die Konfiguration, die bereits für Geräte übernommen wurde.
Alle Geräte	Diese Option verteilt die Einstellungen auf alle Geräte.
Keine Geräte	Diese Option zieht die Einstellungen zurück, die auf die Geräte verteilt werden sollen.
Anpassbar	Diese Option verteilt die Einstellungen auf eine definierte Gerätegruppe. Klicken Sie in das Kontrollkästchen neben der Geräteart, für die Sie die Einstellung verteilen wollen. Sie können alternativ auch nach Gerätegruppen suchen, indem Sie den Namen der Gerätegruppe in dem Suchfeld **Gerätegruppen suchen** eingeben. Wenn Sie eine neue Gerätegruppe erstellen wollen, klicken Sie am unteren Rand der Seite auf den Link **Neue Gerätegruppe erstellen**. Weitere Informationen finden Sie unter Gerätegruppen. Wenn Sie die Gerätekategorie auswählen, sehen Sie die Details (Name, Telefonnummer und Geräteart) in der Liste der Gerätebenutzer für die ausgewählte Gerätekategorie im Abschnitt Verteilungsübersicht.

8. Klicken Sie auf **Fertig**, um die Einstellung per Push auf die ausgewählten Geräte zu übertragen.

BitLocker-Einstellungen anzeigen

Sie können die BitLocker-Einstellungen für ein Gerät auf der Seite mit den Geräte-Details unter (**Geräte > Geräte >[Gerätename]**) im Abschnitt **BitLocker-Einstellungen** anzeigen. Standardmäßig werden die Details nicht angezeigt.

Sie können die folgenden Details anzeigen, indem Sie neben jedem Feld auf das Anzeigesymbol (Auge) klicken:

Einstellung	Beschreibung
Wiederherstellungs-Passwort	Wenn diese Option ausgewählt ist, wird in Windows das Wiederherstellungs-Passwort erzeugt und nach der Push-Übertragung der BitLocker-Konfiguration in die Cloud übertragen. Wenn das Gerät in den Wiederherstellungsmodus wechselt, wird der Benutzer aufgefordert, dieses Passwort einzugeben. Wenn mehrere Laufwerke verschlüsselt sind, sollte das gleiche Wiederherstellungspasswort verwendet werden. Das Wiederherstellungs-Passwort wird nur veröffentlicht, wenn die Wiederherstellungsoption **Passwort verwenden und in AD und MobileIron speichern** ausgewählt ist.
PIN	Zeigt die 6-stellige Start-PIN an. Die PIN wird nur angezeigt, wenn Sie die Option **Start-PIN mit TPM erforderlich** in der BitLocker-Konfiguration ausgewählt haben.
Start-Passwort	Das Start-Passwort für das Gerät Das Startpasswort wird nur angezeigt, wenn Sie die Option **Kein TPM verwenden** in den BitLocker-Konfigurationseinstellungen ausgewählt haben.
TPM-version	Zeigt die konfigurierte TPM-Version an.

Je nach den Einstellungen in der BitLocker-Konfiguration wird bei einigen Feldern gegebenenfalls **N/A** angezeigt.

- Der Status der Verschlüsselung wird im Geräte-Verschlüsselungsstatus auf der Seite mit den Gerätedetails angezeigt.
- Es wird für alle Laufwerke eines Gerätes, für die BitLocker verwendet werden soll, das gleiche Start-Passwort bzw. die gleiche PIN verwendet.
- Wenn Sie eine Konfiguration zur Verschlüsselung eines zweiten Laufwerks auf einem Gerät erstellen, auf dem bereits ein verschlüsseltes Laufwerk existiert und ein Wiederherstellungs-Passwort gespeichert ist, wird das ältere Passwort überschrieben. Wir empfehlen daher, die Option zur Passwort-Wiederherstellung in einem Gerät nur für ein Laufwerk zu verwenden.

10.10.6. Konfiguration des Unternehmensnetzwerkzugangs

Dieser Abschnitt enthält die folgenden Themen:

- AirPlay-Konfiguration
- AirPrint-Konfiguration
- Always-on VPN – Konfiguration
- Standard-App-Runtime-Berechtigungen
- Bildung
- Globale Proxy-Konfiguration
- LDAP-Konfiguration
- Konfiguration des macOS Servers
- Netzwerkrelais-Konfiguration
- Tunnel
- AppTunnel konfigurieren
- Per-App VPN-Konfiguration
- Single Sign-On-Konfiguration
- Sichere Anmeldung für mehrere Benutzer in iOS
- Konfiguration der Android-APN-Einstellungen
- VPN-Konfiguration
- VPN-on-Demand
- WLAN-Konfiguration

10.10.6.1. AirPlay-Konfiguration

Lizenz: Silver

Eine Airplay-Konfiguration richtet den Zugriff auf Ersatzgeräte zum Anzeigen von Medien ein. In der folgenden Tabelle sind die AirPlay-Einstellungen aufgeführt:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Liste zulassen	Geben Sie die Geräte-ID von jedem zugelassenen AirPlay-Zielort ein. Wenn Sie keine ID angeben, werden AirPlay-Zielorte nicht beschränkt. **Gilt für**: iOS 7.0+ und macOS 10.10+ (überwachte Geräte).
Geräteeinstellungen	Geben Sie die Geräte-ID (macOS) oder den Gerätenamen (iOS) und das Passwort für jedes bekannte AirPlay-Ziel ein.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.6.2. AirPrint-Konfiguration

Lizenz: Silver

Eine AirPrint-Konfiguration ermöglicht die Einrichtung zum drahtlosen Drucken. In der folgenden Tabelle sind die AirPrint-Einstellungen aufgeführt:

Einstellungen	Aufgabe
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
AirPrint-Einstellungen	**IP-Adresse:** Geben Sie die IP-Adresse des AirPrint-Druckers ein. **Ressourcenpfad:** Geben Sie den mit dem AirPrint-Drucker verbundenen Ressourcenpfad ein. Dieser entspricht dem rp-Parameter des Bonjour-Protokolls _ipps.tcp. Beispiele: • printers/Canon_MG5300_series • printers/Xerox_Phaser_7600 • ipp/print • Epson_IPP_Printer. Beim Ressourcenpfad ist Groß- und Kleinschreibung zu beachten. **Port:** Geben Sie den Listening-Port für das AirPrint-Ziel ein. Wenn dies nicht angegeben wird, verwendet AirPrint den Standard-Port. Details zu den Standard-Ports von Apple finden Sie unter **https://support.apple.com/en-us/HT202944.** **TLS erzwingen**: Ermöglicht die Absicherung der Verbindung durch Transport Layer Security (TLS). Standardmäßig ist die Option deaktiviert.

Nach der Installation der **AirPrint**-Konfiguration auf dem macOS werden die Druckerdetails über die **AirPrint**-Konfiguration an das Gerät übertragen. Benutzer können die automatisch übernommenen Druckerdetails anzeigen, indem sie auf Systempräferenz > Drucker & Scanner > + klicken. Im Bildschirm **Hinzufügen** muss der Benutzer **Standard** wählen und dann das gewünschte Druckprofil auswählen. Damit wird der gewünschte Drucker zu **Drucker & Scanner** hinzugefügt.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.6.3. Always-on VPN – Konfiguration

Lizenz:

- **Gold für Android Enterprise**
- **Silver-Lizenz für iOS**

Mit der Konfiguration von Always-on VPN stellen Sie sicher, dass Benutzer automatisch und ohne weitere Schritte mit dem VPN verbunden werden (wenn verfügbar). Diese Funktion erfordert Android 7.0 + oder iOS 8+ sowie einen VPN-Provider, der das Protokoll IKEv2 unterstützt.

Always-on VPN – Einstellungen für Android

Die Konfiguration für Always-on VPN wird an Android Enterprise-Geräte mit Android ab Version 7.0 gesendet. Auf dem verwalteten Gerät mit Arbeitsprofil (Android 8.0+) wird die VPN-Konfiguration in das Arbeitsprofil übernommen.

> Wenn ein Gerät im Modus **COSU** mit **AMA** als Geräteregistrierungstyp bereitgestellt wird und wenn eine App mit der Konfiguration **Always-on** auf dem Gerät bereitgestellt wird, wird auch die **Always-on**-Konfiguration auf dem Gerät bereitgestellt.

Um diese Konfiguration zu aktivieren, wählen Sie eine App aus dem App-Katalog oder geben einen Paketnamen ein.

Always-on VPN – Einstellungen für iOS

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Benutzen Sie die gleiche Tunnelkonfiguration für Mobilfunk und WLAN	Klicken Sie hier, um ein Server-ID-Paar für VPN-Verbindungen zu definieren, unabhängig davon, ob die Verbindung über ein Funknetz oder ein WLAN hergestellt wird.
[Server]	Geben Sie den Hostnamen bzw. die IP-Adresse des VPN-Servers ein.
Lokaler Identifikator	ID des IKEv2-Clients in einem der folgenden Formate: • [FQDN] • UserFQDN • Adresse • ASN1DN
Remote-Identifikator	Remoter Identifikator in einem der folgenden Formate: • [FQDN] • UserFQDN • Adresse • ASN1DN
EAP aktivieren	Klicken Sie, um die erweiterte Authentifizierung zu aktivieren.
Maschinenauthentifizierung	Nur verfügbar, wenn die Option "EAP aktivieren" nicht ausgewählt ist. Klicken Sie auf eine der folgenden Optionen: • Zertifikat • Gruppenpasswort
EAP-Authentifizierung	Nur verfügbar, wenn die Option "EAP aktivieren" ausgewählt ist. Klicken Sie auf eine der folgenden Optionen: • Zertifikat • Benutzername/Passwort
Gruppenpasswort	Nur verfügbar, wenn das Gruppenpasswort für die Maschinenauthentifizierung ausgewählt wurde. Geben Sie das Gruppenpasswort für die Verbindung ein.
Anmeldeinformationen	Nur verfügbar, wenn das Zertifikat für die Maschinenauthentifizierung ausgewählt wurde. Wählen Sie das zu verwendende Zertifikat aus. Dieses Zertifikat wird zur IKE-Client-Authentifizierung versendet. Wenn eine erweiterte Authentifizierung verwendet wird, kann dieses Zertifikat für EAP-TLS verwendet werden.
Konto	Nur verfügbar, wenn für die EAP-Authentifizierung [Username/Password] ausgewählt ist. Geben Sie die Konto-ID für den VPN-Server ein.

Einstellung	So gehen Sie vor
Passwort	Nur verfügbar, wenn für die EAP-Authentifizierung [Username/Password] ausgewählt ist. Geben Sie das Passwort für den VPN-Server ein.
Dead Peer-Erkennungsintervall	Klicken Sie auf eine der folgenden Optionen: • Keine (Deaktivieren) • Niedrig (keepalive wird einmal stündlich versendet). • Mittel (keepalive wird alle 30 Minuten gesendet). • Hoch (keepalive wird alle 10 Minuten gesendet).
Verschlüsselungsalgorithmus	Klicken Sie auf eine der folgenden Optionen: • DES • 3DES • AES-128 • AES-256 • AES-128-GCM • AES-256-GCM • ChaCha20-Poly1305
Integritätsalgorithmus	Klicken Sie auf eine der folgenden Optionen: • SHA1-96 • SHA1-160 • SHA2-256 • SHA2-384 • SHA2-512
Diffie-Hellman-Gruppe	Klicken Sie auf die Option "D-H-Schlüsselaustauschgruppe".
Nutzungsdauer in Minuten	Geben Sie die SA-Gültigkeitsdauer (Intervall für Neuverschlüsselung) in Minuten ein. Gültige Werte sind 10 bis 1440.
Sprachnachricht	Wählen Sie "Traffic über Tunnel zulassen", um in Always-on VPN für Voicemail-Traffic eine Ausnahme zuzulassen. Wählen Sie „Traffic ablegen“, um keine Ausnahme zu machen.
Airprint	Wählen Sie "Traffic über Tunnel zulassen", um in Always-on VPN für Airprint-Traffic eine Ausnahme zuzulassen. Wählen Sie „Traffic ablegen“, um keine Ausnahme zu machen.
Mobilfunkdienste	Wählen Sie "Traffic über Tunnel zulassen", um in Always-on VPN für Traffic über Mobilfunkdienste eine Ausnahme zuzulassen. Wählen Sie „Traffic ablegen“, um keine Ausnahme zu machen.
Traffic über Gäste-Webseite außerhalb des VPN-Tunnels zulassen.	Klicken Sie hier, um Traffic von Gäste-Webseiten außerhalb des VPN-Tunnels zuzulassen.

Einstellung	So gehen Sie vor
Traffic von allen Netzwerkanwendungen für Gastzugang außerhalb des VPN-Tunnels zulassen.	Klicken Sie hier, um den Traffic aus allen Gästenetzwerk-Apps außerhalb des VPN-Tunnels zuzulassen und die Netzwerkverarbeitung für Gäste zu erlauben.
Netzwerk-Anwendungspaketidentifikatoren für Gastzugang	Listen Sie die Bundle-IDs für Gäste-Netzwerk-Apps auf, deren Traffic außerhalb des VPN-Tunnels übertragen wird, um eine Gäste-Netzwerkverarbeitung zu unterstützen. Netzwerk-Apps mit Gastzugang können zusätzliche Rechte benötigen, um in einer Umgebung mit Gastzugang zu funktionieren.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.6.4. Standard-App-Runtime-Berechtigungen

Gilt für: Apps für Android API 23+ und Android 6.0+ auf Geräten mit Android Enterprise.

Administratoren können die Runtime-Berechtigungen in der Konfiguration für Apps einstellen, die auf Geräten mit Android Enterprise bereitgestellt werden. Apps, die mit API 23 (oder höher) unter Android 6.0 oder höher arbeiten, können von den Benutzern Berechtigungen für dieses Runtime anfordern. Die Konfiguration mit Standard-App-Runtime-Berechtigungen definiert die Standardberechtigungen für diese App-Runtime. Ivanti Neurons for MDM erstellt diese Konfiguration standardmäßig. Sie können die Systemstandardkonfiguration bearbeiten oder eine neue Konfiguration entsprechend Ihren Anforderungen erstellen.

Die App-spezifischen Berechtigungen haben Vorrang vor der allgemeinen Rechtekonfiguration der App. Für interne Apps gelten die globalen Berechtigungen. Die Konfiguration der Berechtigungen pro App wird für eigene Apps nicht unterstützt.

Globale Runtime-Berechtigungen konfigurieren

Administratoren können die Standard-App-Runtime-Berechtigungen und die Verteilung dieser Konfiguration wie folgt bearbeiten:

ProcedureVerfahren

1. Gehen Sie zu **Konfigurationen**.
2. Führen Sie eine der folgenden Aktionen aus:
    - Um die Standard-Systemkonfiguration zu bearbeiten, klicken Sie auf **Standard-App-Runtime-Berechtigungen** und dann auf **Bearbeiten**.
    - Klicken Sie zum Hinzufügen einer neuen Konfiguration auf **Hinzufügen > Standard-App-Runtime-Berechtigungen**.

Geben Sie einen Namen für die Konfiguration ein.

4. Geben Sie eine Beschreibung ein.
5. Wählen Sie in dem Abschnitt für das Konfigurations-Setup eine der folgenden Standard-Runtime-Berechtigungen:
    - Benutzeraufforderung (Standardoption)
    - Automatisch erteilen
    - Automatisch verweigern (Vorsicht!)

Klicken Sie auf **Weiter**.

7. Wählen Sie die Option **Diese Konfiguration aktivieren**.

> Wenn Sie diese Option deaktivieren, wird die Konfiguration für kein Gerät übernommen. Sie wird bei allen Geräten entfernt, auf die sie zuvor angewendet wurde.

8. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar

Klicken Sie auf **Fertig**.

App-spezifische Runtime-Berechtigungen konfigurieren

Administratoren können die Standard-Runtime-Berechtigungen für eine einzelne Anwendung wie folgt konfigurieren:

Verfahren

1. Gehen Sie zu **Apps**.
2. Klicken Sie auf den Namen der App.
3. Klicken Sie auf **App-Konfigurationen > Android Enterprise**.
4. Klicken Sie auf Hinzufügen oder klicken Sie auf den Konfigurationsnamen, um eine vorhandene Konfiguration zu bearbeiten.
5. Definieren Sie Konfigurationsoptionen wie Name, Beschreibung und Einschränkungen.
6. Klicken Sie in dem Abschnitt „Runtime-Berechtigungen“ auf **Berechtigungen verwalten**.
7. Wählen Sie die Berechtigungen in dem angezeigten Fenster aus und klicken Sie auf **Auswählen**.
   Zur Auswahl aufgelistet werden nur die gefährlichen Berechtigungen für die spezifische Anwendung. **https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups**Die komplette Liste gefährlicher Berechtigungen (beispielsweise zum Auslesen Ihrer Kontakte, zur Suche von Konten auf dem Gerät, zur Erfassung eines Anrufprotokolls usw.) finden Sie unter **https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups**.
   - Die Berechtigungen werden nur übernommen, wenn die Anwendung Berechtigungen anfordert.
   - Die Berechtigungen werden nicht übernommen, wenn die Benutzer die Berechtigungen bereits akzeptiert oder verweigert haben.

Wählen Sie in dem Abschnitt für die Runtime-Berechtigungen eine der folgenden Standard-Runtime-Berechtigungen aus:

- Standard/Global (Standardoption)
- Automatisch erteilen
- Automatisch verweigern (Vorsicht!)

Wählen Sie in dem Abschnitt „Diese App-Konfiguration verteilen“ eine der folgenden Verteilungsoptionen aus:

- Jeder mit der App
- Keiner
- Anpassbar

Klicken Sie auf **Speichern**.

10.10.6.5. Bildung

Lizenz: Gold

Gilt für: überwachte Geräte mit iOS 9.3+.

Apple Education Payload sowie die ClassRoom-App für Lehrer und Schüler. In der folgenden Tabelle sind die Einstellungen für Education aufgeführt:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Konfigurationsart	Klicken Sie auf eine der folgenden Typen: • Leiter • Mitglied
Diese Konfiguration aktivieren	• Wählen Sie diese Option aus, um die Konfiguration für die ausgewählten Geräte zu übernehmen. • Deaktivieren Sie diese Option, um diese Konfiguration von allen Geräten zu entfernen, auf denen sie zuvor verwendet wurde.
Verteilen	Wählen Sie eine der folgenden Verteilungsoptionen aus: • Alle Geräte • Keine Geräte • Anpassbar

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.6.6. Globale Proxy-Konfiguration

Lizenz: Silver

Eine globale Proxy-Konfiguration veranlasst Geräte dazu, HTTP Traffic an einen Proxy-Server weiterzuleiten. In der folgenden Tabelle sind die globalen Proxy-Einstellungen aufgeführt:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Typ	Wählen Sie Manuell oder Automatisch. Wenn Sie **Manuell** wählen, benötigen Sie den Host-Namen und den Port des Proxy-Servers und optional einen Benutzernamen und ein Passwort für den Proxy-Server. Wenn Sie **Automatisch** auswählen, können Sie eine URL für die automatische Proxykonfiguration (Proxy Auto Configuration, PAC) eingeben.
Hostname und Port	Wenn Sie **Manuell** ausgewählt haben, geben Sie den Host-Namen und die Portnummer des Proxy-Servers ein.
Benutzer	(Optional) Benutzername für Zugriff auf den Proxyserver.*
Passwort	(Optional) Passwort für Zugriff auf den Proxy-Server
PAC-URL	(Optional) Wenn Sie Automatisch ausgewählt haben, können Sie die URL der PAC-Datei auswählen, die die Proxy-Konfiguration bestimmt. Wenn Sie diese Einstellung leer lassen, nutzt das Geräts das Web Proxy Autodiscovery Protocol (WPAD) zur Ermittlung von Proxys.
Direkte Verbindung zulassen, falls PAC nicht erreichbar ist	(iOS 7 und höher) Wählen Sie diese Option, um eine direkte Verbindung zuzulassen, wenn das Geräts aus irgendeinem Grund nicht auf die PAC-Datei zugreifen kann.
Umgehen des Proxy zulassen, um auf Captive-Netzwerke zuzugreifen	(iOS 7 und höher) Wählen Sie diese Option, um zuzulassen, dass der Proxy umgangen wird, um die Anmeldeseite für ein Captive-Netzwerk anzuzeigen.

> Variables.htmGeben Sie „$“ ein, um eine Liste mit unterstützten Variablen anzuzeigen, sofern diese für dieses Feld verfügbar ist.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.6.7. Globale Proxykonfiguration (Android)

Gilt nur für Android-Geräte im Gerätebesitzer- und im AOSP-Modus.

Eine globale Proxy-Konfiguration veranlasst Geräte dazu, HTTP Traffic an einen Proxy-Server weiterzuleiten.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Klicken Sie auf **Konfigurationen**.
3. Klicken Sie auf +Hinzufügen.
4. Geben Sie **Global** in das Suchfeld ein und klicken Sie dann auf **Global Proxy**:
   Die Detailseite "Globale Proxykonfiguration" wird angezeigt.
5. Geben Sie einen Namen für die Konfiguration in das Feld **Name** ein.
6. Optional können Sie eine Beschreibung der Konfiguration hinzufügen.
7. Wählen Sie in der Liste **Plattform** die Option **Android** aus. Der Abschnitt **Konfigurations-Setup** wird angezeigt.
8. Wählen Sie als Typ **Manuell** oder **Automatisch** aus.
   - **Manuell**
     - Geben Sie den **Hostnamen** (Domänenname/IP-Adresse) und die Angaben zum **Port** ein.
     - Unter **Ausschlüsse hinzufügen** können Sie mehrere Hostnamen (Domänennamen/Platzhalter) hinzufügen, die sich in der Ausschlussliste befinden müssen.
   - **Automatisch**
     - Geben Sie die PAC-URL ein.
9. Klicken Sie auf **Weiter**, um die Verteilungseinstellungen zu konfigurieren und dann auf **Fertig**.

10.10.6.8. LDAP-Konfiguration

Eine LDAP-Konfiguration richtet den Zugriff auf ein Unternehmensverzeichnis ein. In der folgenden Tabelle sind die LDAP-Einstellungen aufgeführt:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
[Hostname]	Geben Sie den Hostnamen für den LDAP-Server ein.*
Benutzer	Geben Sie das Kennwort für den Zugriff auf das LDAP-Konto ein.*
Passwort	Geben Sie das Passwort für den Zugriff auf das LDAP-Konto ein.
SSL verwenden	Wählen Sie diese Option, wenn Sie SSL für die Verbindung zum LDAP-Server nutzen möchten.
Sucheinstellungen	Geben Sie mindestens einen Eintrag für das Konto ein. Jeder Eintrag repräsentiert einen Knoten in dem LDAP-Baum, von welchem aus die Suche gestartet wird. Klicken Sie auf die Schaltfläche „+“, um einen neuen Eintrag hinzuzufügen und diesen anschließend zu bearbeiten. Ein Eintrag besteht aus den folgenden Werten: Beschreibung: erläutert den Zweck der Sucheinstellung. Bereich: **Wählen Sie „Basis“, „Teilbaum“** oder **Eine Ebene**, um den Suchbereich zu markieren. **„Basis“** markiert nur die Knotenebene, **Teilbaum** markiert den Knoten und alle Kinder, **Eine Ebene** markiert den Knoten und eine Ebene mit Kindern. Suchbasis: der Konzeptpfad zu dem genauen Hinweis (z. B. ou=people, o=mycorp).
Per-App VPN	**Voraussetzung**: Konfigurieren Sie die Tunnel- oder Per-App-VPN-Konfiguration, bevor Sie Per-App-VPN in der LDAP-Konfiguration einrichten. Wählen Sie aus dem Dropdown-Menü die vorkonfigurierte Per-App-VPN-Konfiguration aus. **Gilt für**: iOS 14+
iOS 10+	
Regeln für den Kommunikationsdienst	Wählen Sie eine Standard-App für Audiogespräche mit Kontakten in dem LDAP-System aus.

> Variables.htmGeben Sie „$“ ein, um eine Liste mit unterstützten Variablen anzuzeigen, sofern diese für dieses Feld verfügbar ist.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.6.9. Konfiguration des macOS Servers

Eine macOS-Server-Konfiguration definiert ein macOS-Server-Konto mit den konfigurierten Kontenarten und Einstellungen. Diese Konfiguration erlaubt dem Benutzer die Aktivierung der Dateifreigabe auf dem Server.

Gilt für:4298} iOS 10+

Konfiguration des macOS-Servers

Verfahren

1. Gehen Sie zu **Konfigurationen > +Hinzufügen.**
2. Wählen Sie die Konfiguration für **macOS Server** aus, um die Seite **macOS Server-Konfiguration erstellen** anzuzeigen.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Geben Sie den **Hostnamen** ein, um die Serveradresse zu definieren.
6. Geben Sie den **Benutzernamen** ein, um den Anmeldenamen des Benutzers zu definieren.
7. (Optional) Geben Sie für den Benutzer ein **Passwort** ein.
8. (Optional) Geben Sie für das Konto eine **Beschreibung** ein.
9. (Optional) Unter den konfigurierten Konten geben Sie im Feld Port die Nummer ein, die bei der Kontaktaufnahme mit dem Server für das Dokumente-Wörterbuchkonto verwendet werden soll. Wenn keine Portnummer definiert ist, wird die Standardportnummer verwendet.
10. Klicken Sie auf **Weiter**.
11. Wählen Sie eine Verteilungsebene für diese Konfiguration aus.

10.10.6.10. Tunnel

Ivanti Tunnel aktiviert die VPN-Funktion auf iOS-, Android- und Windows-Geräten. Ivanti Tunnel interagiert mit der Unified Endpoint Management (UEM)-Plattform, Standalone Sentry und Access, um den Zugriff auf Unternehmensressourcen von außerhalb des Unternehmensnetzwerks zu sichern. Die Unternehmensressourcen können sich intern oder in der Cloud befinden. Die UEM-Plattformen sind Ivanti EPMM und Ivanti Neurons for MDM.

> Die Per-App-Konfiguration ist auf Android Enterprise-Geräten veraltet. Verwenden Sie stattdessen die verwaltete Konfiguration für Ivanti Tunnel aus dem App-Katalog.

Wissenswertes über die Ivanti Tunnel-Konfiguration

Konfigurationen für Ivanti Tunnel werden auf einer Unified Endpoint Management (UEM)-Plattform erstellt. Ivanti Tunnel empfängt die Konfiguration vom UEM-Client. Der Client für Ivanti EPMM ist Mobile@Work und der Client für Ivanti Neurons for MDM ist Go.

Aktuelle Dokumentation

Die neuesten Tunnel-Anweisungen finden Sie in der jeweiligen Produktdokumentation:

- Tunnel for Android, siehe **Ivanti Tunnel for Android – Handbuch**
- Tunnel for iOS, siehe **Ivanti Tunnel for iOS – Handbuch**
- Tunnel for macOS, siehe **Ivanti Tunnel for macOS – Handbuch**
- Windows Tunnel, siehe **Ivanti Tunnel for Windows – Handbuch**

> Ivanti Tunnel for Windows ist veraltet und wird nicht mit Ivanti Neurons for MDM unterstützt.

10.10.6.11. AppTunnel konfigurieren

Der AppTunnel schützt die App-Daten durch Absicherung jeder Sitzung zwischen einem App-Container und dem Unternehmensnetzwerk.

Dieser Abschnitt enthält die folgenden Themen:

- Sentry für AppTunnel mit Zertifikaten konfigurieren
- Sentry-Zertifikate hochladen
- Apps zur Verwendung von AppTunnel konfigurieren
- Über AppTunnel-Dienstnamen

Sentry für AppTunnel mit Zertifikaten konfigurieren:

> Wenn Sie eigenständiges Sentry zum ersten Mal installieren, wird ein selbstsigniertes Zertifikat mit installiert. Ivanti empfiehlt dringend, das Standardzertifikat durch ein öffentliches, vertrauenswürdiges Drittanbieterzertifikat zu ersetzen.

Voraussetzungen

- AppTunnel erfordert die letzte unterstützte Version von Sentry. Schließen Sie die Sentry-Installation ab, bevor Sie mit den AppTunnel-Konfigurationsaufgaben beginnen.
- Wenn Sie eine SCEP-Identität verwenden wollen:
  - Ergänzen Sie eine lokale oder externe Zertifizierungsstelle. Es muss ein Konnektor installiert werden.
  - Ergänzen Sie eine App-Identitäts-Konfiguration. Dies ist die dynamische Verteilung, die Sie bei Konfiguration von AppTunnel verwenden.

Sie können ActiveSync und/oder App Tunnel mithilfe von X.509-Zertifikaten zur Authentifizierung konfigurieren, um Sentry-Server zu verwenden, die einem Profil zugewiesen sind.

Verfahren

1. Gehen Sie zu **Administration > Sentry**.
2. Klicken Sie auf **+ Sentry Profil hinzufügen**.
3. Klicken Sie auf **ActiveSync bzw. AppTunnel mit Zertifikaten**.
4. Klicken Sie auf **Weiter**.
5. Beachten Sie die Richtlinien in der folgenden Tabelle und vervollständigen Sie die Seite **Globale Einstellungen**.

Tabelle: Globale Einstellungen für Administration > Sentry	
Einstellung	**Aktion**
[Name]	Geben Sie einen Namen ein, der dieses Profil bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieses Profils erläutert.
Externer Hostname und Port	Geben Sie Host-Name und Port für das Sentry ein.
Geräte-Authentifizierungsmodus	
Einzelnes Zertifikat zur 2-Phasen-Authentifizierung verwenden	Wählen Sie aus, ob Sie ein einzelnes Zertifikat zur Authentifizierung verwenden wollen. Wenn Sie noch kein **Zertifikat hochgeladen** haben, können Sie dies in dem unter der ausgewählten Option angezeigten Bereich tun.
Zertifikat auswählen	Gruppenzertifikat für die Geräteauthentifizierung hochladen: 1. Klicken Sie auf **Hinzufügen**. Das Fenster **Zertifikat hinzufügen** wird angezeigt. 2. Geben Sie den Namen des Zertifikats in das Feld **Zertifikatsname** ein. 3. Geben Sie das Passwort zum Schutz der PKCS12-Datei ein. 4. Klicken Sie auf Datei auswählen, um das MDM-Zertifikat auszuwählen.Stellen Sie sicher, dass die Datei das Format .p7b, .p12, .pfx, .pem, .der, .crt oder .cer hat.
Zertifikatsperrliste (CRL) aktivieren	Wählen Sie diese Option, um die vom Gerät vorgelegten Zertifikate anhand der von der Zertifizierungsstelle veröffentlichten Zertifikatssperrliste (CRL) zu validieren.
Standardverhalten von nicht verwalteten Geräten	
Empfang von E-Mails und Daten durch nicht verwaltete Geräte zulassen.	Wählen Sie aus, ob Sie den Datenzugriff für Geräte blockieren möchten, die nicht durch Ivanti Neurons for MDM verwaltet werden.

6. Klicken Sie auf **Weiter**.
7. Konfigurieren Sie auf der Seite **Sentry-Server-Konfiguration** die folgenden Felder:
8. Klicken Sie auf **Weiter**.

Tabelle: Sentry-Server-Konfiguration für Admin > Sentry	
Einstellung	So gehen Sie vor
Listener-Protokoll	Wählen Sie eine der folgenden Protokolloptionen aus: • **Nur HTTPS** • **Nur HTTP** • **HTTPS und HTTP**
Https-Port	Geben Sie die Https-Portnummer ein. Dieses Feld wird nicht angezeigt, wenn für das Listener-Protokoll „Nur HTTP“ ausgewählt ist.
Http-Port	Geben Sie die Http-Portnummer ein. Dieses Feld wird nicht angezeigt, wenn als Listener-Protokoll „Nur HTTPS“ ausgewählt ist.
Sentry TLS Server-Zertifikat / Schlüssel	
Selbstsigniertes Sentry-Zertifikat verwenden	Durch Aktivierung dieser Option wird das vom Cloud-Dienst erstellte und an Sentry als Teil dieses Profils gesendete selbstsignierte Zertifikat verwendet. Dieses Zertifikat dient der Kommunikation zwischen den Sentry- und Mobilgeräten.
Hinzufügen	Eigenes Zertifikat hochladen, das zur Authentifizierung erforderlich ist: 1. Klicken Sie auf **Hinzufügen**. Das Fenster **Zertifikat hinzufügen** wird angezeigt. Sie können diese Option nur sehen, wenn Sie die Option Selbstsigniertes Sentry-Zertifikat verwenden abwählen. 2. Geben Sie den Namen des Zertifikats in das Feld **Zertifikatsname** ein. 3. Geben Sie das Passwort zum Schutz der PKCS12-Datei ein. 4. Klicken Sie auf Datei auswählen, um das Zertifikat hochzuladen.Stellen Sie sicher, dass die Datei im .p12-Format vorliegt. 5. Klicken Sie auf **[Add]**. Alle hochgeladenen TLS-Server-Zertifikate (einschließlich der von der Sentry-Hauptseite und aus anderen Profilen hochgeladenen Zertifikate) werden im Abschnitt „Sentry TLS-Server-Zertifikat/Schlüssel“ angezeigt. Um das zur Authentifizierung erforderliche TLS-Zertifikat auszuwählen, klicken Sie auf die Radioschaltfläche neben dem Zertifikat.
Zweites Zertifikat hinzufügen	Wählen Sie diese Option aus, um ein zweites Zertifikat zu aktivieren. Sobald das primäre Zertifikat abläuft, wechselt Sentry automatisch und ohne administrativen Eingriff zum Reservezertifikat.

Tabelle: Sentry-Server-Konfiguration für Admin > Sentry	
	Tunnel speichert bereits beide Zertifikate und kann diese so abgleichen, dass die Konnektivität nicht unterbrochen wird.
Protokolle	Wählen Sie die gewünschten ein- und ausgehenden Protokolle aus.
Verschlüsselungssammlung	Verschlüsselungen werden in der SSL-verschlüsselten Kommunikation mit dem Sentry verwendet. Starke Verschlüsselungen werden bevorzugt. Ältere Geräte erfordern möglicherweise schwache Verschlüsselungen. Standardmäßig sind starke Verschlüsselungsalgorithmen ausgewählt. Sie können weitere Verschlüsselungsalgorithmen auswählen, die Sie verwenden wollen. Sie müssen mindestens einen Verschlüsselungsalgorithmus auswählen.

9. Ergänzen Sie mindestens einen der angezeigten Dienste.
10. Klicken Sie auf **Speichern**.

Sobald ein Sentry registriert wurde, wird es auf der Sentry-Seite im Abschnitt „Nicht konfigurierte Sentry-Server“ angezeigt. Um ein Profil einem Sentry zuzuweisen, klicken Sie in der Spalte **Aktionen** auf **Zuweisen**.

Sentry-Zertifikate hochladen

Ivanti Neurons for MDM lädt TLS-Serverzertifikate und Gruppenzertifikate hoch, wenn ein Sentry-Profil erstellt wird. Sie können diese Zertifikate auch von der **Sentry**-Seite im Abschnitt **Sentry-Zertifikate** hochladen.

Ivanti Neurons validiert Sentry-Zertifikate nach dem Upload und gibt abhängig von den in den Zertifikaten gefundenen Bedingungen die folgenden Informationstypen aus:

Bedingung	Informationstyp
Das untergeordnete Zertifikat enthält keine Zertifizierungsstelle, oder in der hochgeladenen Datei ist keine Zertifizierungsstelle enthalten.	Fehler
Es ist keine Stammzertifizierungsstelle verfügbar.	Warnung
Die Stammzertifizierungsstelle hat die Zwischenzertifizierungsstelle für das untergeordnete Zertifikat nicht abgezeichnet.	Warnung

Ivanti Neurons for MDM validiert außerdem die Regeln in diesem Artikel.

Verfahren

1. Klicken Sie im Abschnitt TLS Server-Zertifikate auf Hinzufügen. Das Fenster **Zertifikat hinzufügen** wird angezeigt.
2. Geben Sie den Namen des Zertifikats in das Feld **Zertifikatsname** ein.
3. Geben Sie das Passwort zum Schutz der PKCS12-Datei ein.

4. Klicken Sie auf **Datei auswählen**, um das MDM-Zertifikat auszuwählen. Stellen Sie sicher, dass die Datei das Format .p7b, .p12, .pfx, .pem, .der, .crt oder .cer hat.
5. Klicken Sie auf **Hinzufügen**. Das hochgeladene Zertifikat wird in der Tabelle angezeigt.
6. Klicken Sie zum Löschen des TLS Server-Zertifikats auf das Symbol „Löschen“ in der Spalte **Aktionen**.

> Wenn das TLS-Serverzertifikat in einem Sentry-Profil verwendet wird, können Sie das Zertifikat nicht löschen. Es wird eine Fehlermeldung angezeigt, wenn die Löschaktion durchgeführt wird.

Gruppenzertifikate hinzufügen

Verfahren

1. Klicken Sie im Abschnitt Gruppenzertifikate auf Hinzufügen. Das Fenster **Zertifikat hinzufügen** wird angezeigt.
2. Geben Sie den Namen des Zertifikats in das Feld **Zertifikatsname** ein.
3. Geben Sie das Passwort zum Schutz der PKCS12-Datei ein.
4. Klicken Sie auf **Datei auswählen**, um das MDM-Zertifikat auszuwählen. Stellen Sie sicher, dass die Datei das Format .p7b, .p12, .pfx, .pem, .der, .crt oder .cer hat.
5. Klicken Sie auf **[Add]**.

Klicken Sie zum Löschen des hochgeladenen Gruppenzertifikats auf das Symbol „Löschen“ in der Spalte **Aktionen**.

Sentry-Stammzertifikat bearbeiten

Als Administrator haben Sie die Option, die Verteilung der Konfiguration für das Sentry-Stammzertifikat zu bearbeiten. Sie können auch dem Administrator des benutzerdefinierten Spaces Bearbeitungsberechtigungen einräumen, indem Sie die Konfiguration an andere Spaces delegieren.

1. Gehen Sie zu **Konfigurationen**.
2. Starten Sie eine Suche nach dem **Sentry-Stammzertifikat**.
3. Klicken Sie auf das Symbol für Bearbeiten.
4. Markieren Sie die Kontrollkästchen der Geräte oder Gerätegruppen, an die das Zertifikat verteilt werden soll. Heben Sie alternativ die Markierung der Kontrollkästchen für die Geräte oder Gerätegruppen auf.
5. Wählen Sie je nach Bedarf eine der folgenden Optionen im Abschnitt "Verteilungsübersicht" aus:
   - **Nicht auf andere Spaces anwenden**
   - **Auf Geräte in anderen Spaces anwenden**
6. Markieren Sie optional das Kontrollkästchen **Space-Administrator das Bearbeiten der Verteilung erlauben**.
7. Klicken Sie auf **Speichern**.
8. Eine Warnmeldung wird angezeigt. Klicken Sie zur Bestätigung auf **Ja**.

Apps zur Verwendung von AppTunnel konfigurieren

Die neueste Sentry-Anleitung finden Sie unter **Produktdokumentation**; klicken Sie dort auf Sentry. Wählen Sie das gewünschte Dokument entsprechend Ihrer Sentry-Produktversion aus.

Über AppTunnel-Dienstnamen

Ein AppTunnel-Dienst legt den Backend-Dienst fest, mit dem eine AppConnect-App einen Tunnel aufbaut.

https://help.ivanti.comhttps://help.ivanti.com/#116https://help.ivanti.com/#103 Die neuesten Anleitungen finden Sie unter Produktdokumentation; wählen Sie dort die für Ihre Versionen von Sentry und AppConnect passenden Dokumente aus.

10.10.6.12. Per-App VPN-Konfiguration

Lizenz: Silver

Gilt für: iOS-, watchOS-, visionOS- und tvOS-Geräte

Eine Per-App VPN-Konfiguration bestimmt die Einstellungen für den Zugriff auf ein Virtual Private Network (virtuelles privates Netzwerk, VPN) für die folgenden Apps:

- **Per-App VPN-Einstellungen**
- **Psec (Cisco)**
- **[Cisco AnyConnect]**
- **Juniper SSL**
- **NetMotion VPN**
- **[F5 SSL]**
- **SonicWALL Mobile Connect**
- **Aruba VIA**
- **Benutzerdefinierte SSL**
- **Palo Alto Networks GlobalProtect**

> Die Per-App VPN-Konfiguration ist abhängig von der App-Konfiguration. Die Per-App VPN-Konfiguration wird im Rahmen des App-Konfigurations-Setups erstellt. Wenn die Per-App VPN-Konfiguration gelöscht oder ihre Verteilung rückgängig gemacht wird, tritt eine Fehlfunktion der App-Konfiguration auf, wodurch die App vom Netzwerk getrennt wird.

Konfiguration verteilen

Ab Ivanti Neurons for MDM Release 91 können globale Administratoren Space-Administratoren zur Bearbeitung der Per-App VPN-Konfiguration für alle Geräte und für die Option zur benutzerdefinierten Verteilung delegieren. Für die Per-App VPN-Konfiguration können Sie bei Bedarf die Option "Diese Konfiguration in allen Spaces verfügbar machen" auswählen.

> Die Änderungen an der Verteilung gelten nur für den jeweiligen Space. Alle anderen Spaces übernehmen weiterhin die Verteilungseinstellungen des Standard-Space.

Tragen Sie die Konfigurationseinstellungen anhand der Informationen aus den folgenden Tabellen nach Bedarf in die Felder ein und verteilen Sie anschließend die Konfiguration:

Weitere Informationen finden Sie unter *Verteilen der Konfiguration* unter Arbeiten mit Konfigurationen.

Per-App VPN-Einstellungen

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Verbindungstyp VPN-on-Demand aktivieren	Wählen Sie den zu konfigurierenden VPN-Typ. Die übrigen Einstellungen hängen von dieser Wahl ab. Bestimmen Sie, diese Konfiguration für Domänen und Host-Namen zu verwenden, die ein VPN-on-Demand einrichten.
iOS-Regeln aktivieren (Gilt nur, wenn die Option "VPN nach Bedarf aktivieren" ausgewählt ist.)	Für iOS- und macOS-Systeme können Sie Folgendes konfigurieren: • Netzwerkregeln, die den Verbindungsaufbau mit Netzwerken erlauben oder verhindern bzw. diese ignorieren, wenn die Prüfung den Wert „Wahr“ ergibt. • Sie können mit Verbindungsregeln Verbindungen mit Netzwerken zulassen oder verweigern, die bei der Prüfung den Wert „Wahr“ ergeben. Für Netzwerkregeln können Sie folgende Parameterarten definieren: • DNS-Domänen-Abgleich • DNS-Serveradressen-Abgleich • SSID-Abgleich • URL-Zeichenfolgen-Test • Schnittstellentyp-Abgleich Für Verbindungsregeln können Sie folgende Parameterarten definieren: • DNS-Domänen-Abgleich • DNS-Serveradressen-Abgleich • SSID-Abgleich • URL-Zeichenfolgen-Test • Schnittstellentyp-Abgleich • Domänen • DNS-Server • URL-Test
On-Demand-Match-App aktiviert	Klicken Sie, um die VPN-Verbindung pro App nach Bedarf zu aktivieren.
5G Network Slicing aktivieren **Domänen**	Wählen Sie **DNN** (Datennetzwerkname des Netzwerkanbieters) für den Tunnel aus und legen Sie als Ziel das spezifische Mobilfunk-Slice-VPN fest. Wählen Sie **App-Kategorie** aus (wird vom Netzwerkanbieter bereitgestellt), um den Typ der Mobilfunk-Slice für den Tunnel zu identifizieren.
Safari-Domains (iOS)	Ein Array, dessen Einträge jeweils eine Domain angeben müssen, die die VPN-Verbindung in Safari aufbaut. Jeder Eintrag hat das Format www.apple.com.
iOS 14.0+ und macOS 11.0+	

Einstellung	So gehen Sie vor
Zugehörige Domains	Geben Sie mindestens eine zugehörige Domain an. Verbindungen zu Servern innerhalb einer dieser Domains sind dem App-spezifischen VPN zugeordnet.
Ausgeschlossene Domains	Geben Sie mindestens eine ausgeschlossene Domain an. Verbindungen zu Servern innerhalb einer dieser Domains sind vom App-spezifischen VPN ausgeschlossen.
iOS 13+ und macOS 10.15+	
Mail-Domains	Klicken Sie auf **+Hinzufügen**, um mindestens eine Domain einzutragen, die diese VPN-Verbindung in Mail auslösen soll. Jeder Eintrag hat das Format www.apple.com.
Kontakte-Domains	Klicken Sie auf **+Hinzufügen**, um mindestens eine Domain einzutragen, die diese VPN-Verbindung in den Kontakten auslösen soll. Jeder Eintrag hat das Format www.apple.com.
Kalender-Domains	Klicken Sie auf **+Hinzufügen**, um mindestens eine Domain einzutragen, die diese VPN-Verbindung im Kalender auslösen soll. Jeder Eintrag hat das Format www.apple.com.
iOS 9 und höher	
Providerart (iOS 9+)	Wählen Sie einen der folgenden Tunnel-Provider: • App-Proxy – Tunnel-Traffic auf App-Ebene. Eine Übersicht über den App Proxy Provider finden Sie in der **Apple-Dokumentation**. • Paket-Tunnel – Tunnel-Traffic auf der IP-Ebene. Eine Übersicht über Packet Tunnel Provider finden Sie in der **Apple-Dokumentation**.

IPsec (Cisco)

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Maschinenauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Benutzer-PIN einschließen	Wählen Sie diese Option, um den Benutzer zur Eingabe einer PIN aufzufordern.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. **Wenn Sie „Manuell" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. **Wenn Sie „Automatisch" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

[Cisco AnyConnect]

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Gruppe	Geben Sie die Gruppe ein, die zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie **„Manuell“** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie **„Automatisch“** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Juniper SSL

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
[Realm]	Geben Sie den Realm ein, der zur Authentifizierung der Verbindung verwendet werden soll.
Rolle	Geben Sie die Authentifizierungsrolle ein, die zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie **„Manuell“** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie **„Automatisch“** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

NetMotion VPN

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	**Zertifikat** ist die zu verwendende Benutzerauthentifizierungsmethode. Das folgende Feld ist verfügbar: **Berechtigungsnachweis**: Wählen Sie das zu verwendende Identitätszertifikat. Vom Benutzer bereitgestellte Zertifikate werden nur bei iOS-Geräten unterstützt.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein. Wählen Sie aus den folgenden Optionen: • VPN On Demand aktivieren - Domänen oder Hostnamen hinzufügen, die ein VPN On Demand einrichten. • iOS-Regeln aktivieren. • On-Demand-Match-App aktiviert.
Safari-Domänen	Klicken Sie auf **Hinzufügen**, um Safari-Domains hinzuzufügen.
Providerart (iOS 9.0+)	**packet-tunnel** ist standardmäßig als Tunnelanbietertyp ausgewählt. Eine Übersicht über Packet Tunnel Provider finden Sie in der Apple-Dokumentation.

[F5 SSL]

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie **„Manuell“** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie **„Automatisch“** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

SonicWALL Mobile Connect

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Anmeldegruppe oder Domäne	Geben Sie die Anmeldegruppe oder Domäne ein, die zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie **„Manuell“** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie **„Automatisch“** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Aruba VIA

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie **„Manuell“** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie **„Automatisch“** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Benutzerdefinierte SSL

Einstellung	So gehen Sie vor
Identifikator	Geben Sie den Identifikator für dieses benutzerdefinierte SSL VPN im umgekehrten DNS-Format ein (zum Beispiel: com.mycompany.myserver).
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerdefinierte Daten	Geben Sie die Schlüssel-Wert-Paare zur Bestimmung der benutzerdefinierten Daten für dieses VPN ein.
Benutzerauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie **„Manuell“** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie **„Automatisch“** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.
(iOS 9.0+) Providertyp in Haupt- und Unter-VPN-Wörterbuch einschließen	Wählen Sie, ob Sie den Providertyp bei der Erstellung einer Plist (vordefinierte Konfigurationsdatei) einschließen möchten.
Bundle-Kennung des Providers	Geben Sie die Bundle-Kennung für den VPN-Provider ein. Sie können mehrere App-Konfigurationen für eine App anhand der unterschiedlichen Bundle-Kennungen verwalten.

Palo Alto Networks GlobalProtect

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerdefinierte Daten	Geben Sie die Schlüssel-Wert-Paare zur Bestimmung der benutzerdefinierten Daten für dieses VPN ein.
Benutzerauthentifizierung	Das Benutzer-Authentifizierungsverfahren ist „Zertifikat". Wählen Sie ein Identitätszertifikat für das Feld **Berechtigungsnachweis** aus.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie **„Manuell"** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie **„Automatisch"** wählen, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Variables.htmGeben Sie „$" ein, um eine Liste mit unterstützten Variablen anzuzeigen, sofern diese für dieses Feld verfügbar ist.

Verwandte Themen:

Erstellen einer Konfiguration

10.10.6.13. Single Sign-On-Konfiguration

Ivanti Neurons for MDM ermöglicht erweiterbares Single Sign-On (SSO) mit den Konfigurationen erweiterbares SSO und erweiterbares SSO Kerberos. Die Implementierung erfordert vom Identitätsanbieter eine App-Erweiterung, z. B. Microsoft Authenticator. Bei einer erweiterbaren SSO-Implementierung müssen sich Benutzer beim Zugriff auf Unternehmensressourcen nur einmal authentifizieren. Benutzer werden bei nachfolgenden Anmeldungen nicht mehr zur Authentifizierung aufgefordert. Informationen zu den Einrichtungsdaten für den vorgesehenen Identitätsanbieter finden Sie unter **Identity Provider konfigurieren**.

Dieser Abschnitt enthält die folgenden Themen:

- **Single Sign-On-Einstellungen**
- **Erweiterbare Single Sign-On-Einstellungen**
- **Erweiterbare Single Sign-On-Einstellungen für Kerberos-Konten**

Single Sign-On-Einstellungen

Gilt für:

- iOS 7.0 bis zur zuletzt freigegebenen Version, die von Ivanti Neurons for MDM unterstützt wird.
- visionOS 1.1 bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird.

Verwenden Sie die folgenden Einstellungen, um Kerberos Enterprise SSO für jede verwaltete App und den Apple Safari Browser auf iOS-Geräten zu konfigurieren.

> Diese Konfiguration erfordert Tunnel und Sentry. Weitere Informationen finden Sie unter „Single Sign-On mit Kerberos einrichten“ im Tunnel for iOS Guide.

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Benutzername	Geben Sie den Kerberos-Prinzipalnamen ein.
Kerberos-Realm-Name	Geben Sie den Kerberos-Bereichsnamen ein.
Zertifikat	**Für iOS 8 mit Gold-Lizenz:** Wählen Sie das Zertifikat zur Verlängerung der Kerberos-Anmeldeinformationen.
URL-Präfix-Abgleich	Liste der URL-Präfixe, die aufeinander abgeglichen werden müssen, damit dieses Konto für die Kerberos-Authentifizierung über HTTP verwendet werden kann.
Whitelist-Anwendungen für SSO	Fügen Sie Apps aus dem App Catalog hinzu, um sie für SSO auf die Whitelist zu setzen. Geben Sie zum Beispiel „Safari“ ein, um Apple Safari hinzuzufügen. Wenn bei einer solchen Konfiguration keine Apps auf der Whitelist für SSO stehen, können alle Apps, die iOS SSO unterstützen, SSO nutzen, auch integrierte iOS-Apps.

Erweiterbare Single Sign-On-Einstellungen

Gilt für:

- Ivanti Neurons for MDMiOS 13.0 bis zur jüngsten freigegebenen Version, die von unterstützt wird.
- Ivanti Neurons for MDMmacOS 10.15 bis zur letzten aktuellen Version, die von unterstützt wird.
- visionOS 1.1 bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird.

Verwenden Sie die folgenden Einstellungen zur Konfiguration des SSO-Erweiterungsprofils mit dem generischen Erweiterungstyp, um SSO für native Apps und Websites mit verschiedenen Authentifizierungsmethoden zu aktivieren.

> Das erweiterbare SSO funktioniert nicht, wenn die Konfiguration per Push in den Benutzerkanal für macOS 10.15.x-Geräte übertragen wird.

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
SSO-Typ wählen	Wählen Sie eine der folgenden SSO-Arten: • **Anmeldeinformationen** ◦ Geben Sie einen oder mehrere **Host** Namen oder Domain-Namen ein, die durch die App-Erweiterung authentifiziert werden können. Host- oder Domainnamen werden ohne Unterscheidung zwischen Groß- und Kleinschreibung abgeglichen, und alle Host-/Domainnnamen aller installierten erweiterbaren SSO-Payloads müssen eindeutig sein. Hosts, die mit einem "." beginnen, sind Platzhalter-Suffixe und stimmen mit allen Subdomänen überein. Anderenfalls muss der Host ein exakter Treffer sein. ◦ Geben Sie den Namen **Realm** ein. Dieser Wert sollte ordnungsgemäß in Groß- und Kleinbuchstaben geschrieben werden. • **Umleiten** ◦ Geben Sie mindestens einen **URL** Präfix von Identitätsanbietern ein, bei denen die App-Erweiterung SSO durchführt. Die URLs müssen mit http:// oder https:// beginnen, Schema und Hostname werden ohne Unterscheidung von Groß- und Kleinschreibung abgeglichen, Abfrageparameter und URL-Fragmente sind nicht zulässig, und die URLs aller installierten Extensible SSO-Payloads müssen eindeutig sein.
Erweiterungs-Identifikator	Geben Sie den Bundle-Identifikator der App-Erweiterung ein, die SSO für die angegebenen URLs durchführt.
Teamidentifikator	Die Teamkennung der App-Erweiterung. Dieser Schlüssel ist für macOS erforderlich und wird an anderer Stelle ignoriert.
Benutzerdefinierte Daten	Geben Sie benutzerdefinierte Daten als Schlüssel-Wert-Paare ein.
Authentifizierungsmethode (gilt nur für macOS 13+)	• Passwort • Sicherer Enclave-fähiger Benutzerschlüssel
Registrierungstoken	Geben Sie den Token ein. Dieses Feld wird aktiviert, sobald Sie eine der Authentifizierungsmethoden ausgewählt haben.

Einstellung	Beschreibung
Verhalten bei gesperrtem Bildschirm (gilt für iOS 15.0+ und macOS 12.0+)	Wählen Sie eine der folgenden Optionen aus: • **Abbrechen**: Das System bricht Authentifizierungsanforderungen ab, wenn der Bildschirm gesperrt ist. • **Nicht handhaben**: Authentifizierungsanforderungen werden ohne SSO fortgesetzt, wenn der Bildschirm gesperrt ist.
Verweigerte Bundle-Kennungen (gilt für iOS 15.0+ und macOS 12.0+)	Fügen Sie mehrere Bundle-Kennungen von Apps hinzu, die nicht das von dieser Erweiterung bereitgestellte SSO verwenden. Beispiel: *com.firma.appname.www*.

Gilt für: macOS 14.0 bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird.

Einstellung	Beschreibung
Anzeigename des Kontos	Geben Sie einen Namen für das Konto ein, der in Benachrichtigungen und Authentifizierungsanfragen angezeigt werden soll.
Zusätzliche Gruppen	Geben Sie die Namen der Gruppen ein, die keinen Administratorzugriff haben werden.
Administratorgruppen	Geben Sie den Namen der Gruppe ein, die Administratorzugriff besitzt.
Authentifizierungsmethode	Wählen Sie eine Authentifizierungsmethode aus der Dropdownliste aus: • Passwort • Sicherer Enclave-fähiger Benutzerschlüssel • Smart Card
Autorisierungsgruppen	Geben Sie das Autorisierungsrecht für einen Gruppennamen ein.
Autorisierung aktivieren	Markieren Sie das Kontrollkästchen, um Autorisierungsaufforderungen für Administratorgruppen, Autorisierungsgruppen oder zusätzliche Gruppen zu aktivieren.
"Benutzer bei Anmeldung erstellen" aktivieren	Markieren Sie das Kontrollkästchen, um die Erstellung neuer Benutzer bei der Anmeldung unter Verwendung der Authentifizierungsmethode Smart Card oder Kennwort zu aktivieren.
Anmeldehäufigkeit	Die Dauer in Sekunden, nach deren Ablauf das System anstelle einer Aktualisierung eine vollständige Anmeldung verlangt. Der Standardwert ist 64.800 (18 Stunden). Der Mindestwert ist 3.600 (1 Stunde).
Neuer Benutzerautorisierungsmodus	Wählen Sie einen Authentifizierungsmodus für neue Benutzer aus der Dropdownliste aus: • Standard: Das Konto ist für einen Standardbenutzer vorgesehen. • Admin: Das System fügt das Konto zur Gruppe des lokalen Administrators hinzu. • Gruppen: Das System ordnet den neuen Benutzer automatisch der Administratorgruppe, Autorisierungsgruppe oder zusätzlichen Gruppe zu.
Benutzer-Token-Zuordnung	Geben Sie den Kontonamen und den vollständigen Namen der neuen Benutzer ein, um sie für Autorisierungszwecke zuzuordnen.
Benutzerautorisierungsmodus	Wählen Sie einen Authentifizierungsmodus für Benutzer aus der Dropdownliste aus: • Standard: Das Konto ist für einen Standardbenutzer vorgesehen. • Admin: Das System fügt das Konto zur Gruppe des lokalen Administrators hinzu. • Gruppen: Das System ordnet den neuen Benutzer automatisch der Administratorgruppe, Autorisierungsgruppe oder zusätzlichen Gruppe zu.
Gemeinsame Geräteschlüssel verwenden	Markieren Sie das Kontrollkästchen, um dieselben Anmelde- und Verschlüsselungsschlüssel für alle Benutzer zu aktivieren.

Gilt für: macOS 15.4 bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird.

Einstellung	Beschreibung
Geräte-Identifikator-Bescheinigung zulassen	Markieren Sie das Kontrollkästchen, um die UDID und die Seriennummer des Geräts in Plattform-SSO-Bescheinigungen aufzunehmen und somit das Verfolgen registrierter Geräte am Backend zuzulassen.

Gilt für: macOS 14.0 bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird.

Wählen Sie zum Anzeigen der erweiterbaren Einstellungen für ein Single Sign-On-Konto im Feld **Authentifizierungsmethode** die Dropdownoption **Kennwort** aus.

Einstellung	Beschreibung
FileVault-Richtlinie	Aktivieren Sie die Richtlinie, um folgende Einstellungen anzuzeigen: • Authentifizierungsversuch • [Require Authentication] Markieren Sie das Kontrollkästchen **Authentifizierung erforderlich**, um zusätzliche Konfigurationseinstellungen zu aktivieren. • Offline-Toleranzzeitraum zulassen • Toleranzzeitraum für Authentifizierung zulassen
Anmelderichtlinie	Aktivieren Sie die Richtlinie, um folgende Einstellungen anzuzeigen: • Authentifizierungsversuch • [Require Authentication] Markieren Sie das Kontrollkästchen **Authentifizierung erforderlich**, um zusätzliche Konfigurationseinstellungen zu aktivieren. • Offline-Toleranzzeitraum zulassen • Toleranzzeitraum für Authentifizierung zulassen
Entsperrungsrichtlinie	Aktivieren Sie die Richtlinie, um folgende Einstellungen anzuzeigen: • Authentifizierungsversuch • [Require Authentication] Markieren Sie das Kontrollkästchen **Authentifizierung erforderlich**, um zusätzliche Konfigurationseinstellungen zu aktivieren. • Offline-Toleranzzeitraum zulassen • Toleranzzeitraum für Authentifizierung zulassen • TouchID zulassen oder Entsperrung überwachen
Toleranzzeitraum für Authentifizierung	Geben Sie den Zeitraum ein, in dem nach dem Auswählen einer Richtlinie nicht registrierte lokale Konten verwendet werden können. Bei Auswahl des Kontrollkästchens **Toleranzzeitraum für Authentifizierung zulassen** in einer der Richtlinien wird das Feld als Pflichtfeld festgelegt.
Offline-Toleranzzeitraum	Geben Sie den Zeitraum ein, in dem nach Auswählen einer Richtlinie das Kennwort eines lokalen Offline-Kontos nach erfolgreicher SSO-Anmeldung an der Plattform verwendet werden kann. Bei Auswahl des Kontrollkästchens **Offline-Toleranzzeitraum zulassen** in einer der Richtlinien wird das Feld als Pflichtfeld festgelegt.
SSO-Konten außerhalb der Plattform	Wählen Sie **+ Hinzufügen** aus, um die Liste der Benutzernamen einzugeben, die nicht der FileVault-, Anmeldungs- oder Entsperrungsrichtlinie unterliegen.

Erweiterbare Single Sign-On-Einstellungen für Kerberos-Konten

Gilt für:

- Ivanti Neurons for MDMiOS 13.0 bis zur jüngsten freigegebenen Version, die von unterstützt wird.

- Ivanti Neurons for MDMmacOS 10.15 bis zur letzten aktuellen Version, die von unterstützt wird.
- visionOS 1.1 bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird.

Verwenden Sie die folgenden Einstellungen, um eine App-Erweiterung zu konfigurieren, die SSO mit der Kerberos-Erweiterung durchführt.

> Erweiterbares SSO Kerberos funktioniert nicht, wenn die Konfiguration per Push in den Benutzerkanal für macOS 10.15.x-Geräte übertragen wird.

Einstellung	Beschreibung
Grundeinstellungen	
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Benutzername	Geben Sie den Kerberos-Prinzipalnamen ein.
[Realm]	Geben Sie den Kerberos-Bereichsnamen ein.
Zertifikat	Wählen Sie das Zertifikat aus, das zur Verlängerung der Kerberos-Anmeldeinformationen verwendet werden soll.
URL-Präfixe	Liste der URL-Präfixe, die aufeinander abgeglichen werden müssen, damit dieses Konto für die Kerberos-Authentifizierung über HTTP verwendet werden kann.
Erweiterte Einstellungen	
Automatische Anmeldung erlauben	Wenn die Passwörter falsch sind, dürfen sie nicht in der Keychain gespeichert werden. Standardmäßig ist diese Option aktiviert.
Benutzer-Setup verzögern	Hat diese Option den Status „wahr“, wird der Benutzer erst aufgefordert, die Kerberos-Erweiterung einzurichten, wenn der Administrator sie mit dem Tool app-sso aktiviert oder eine Kerberos-Challenge eingeht. Diese Option gilt für macOS 11 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version.
Benutzerpräsenz erforderlich	Hat diese Option den Status „wahr“, muss der Benutzer eine Touch-ID, Gesichts-ID oder seinen Passcode angeben, um auf den Keychain-Eintrag zuzugreifen.
Anmeldeinformationen-Cache überwachen	Hat diese Option den Status „falsch“, werden die Anmeldeinformationen bei der nächsten passenden Kerberos-Challenge oder Änderung des Netzwerkstatus angefordert. Wenn der Anmeldeinformationen abgelaufen sind oder fehlen, werden neue erstellt. Diese Option gilt für macOS 11 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version. Standardmäßig ist diese Option aktiviert.
Cache-Name	Geben Sie den Namen des Generic Security Service (GSS) für den zu verwendenden Kerberos-Cache ein. Diese Option ist nun veraltet.
Domain-Realm-Mapping	Geben Sie den Realm-Namen als Schlüssel ein. Der Wert ist ein Array von DNS-Suffixen, die auf das Realm abgebildet werden. Klicken Sie auf **+ Hinzufügen**, um mindestens ein Schlüssel-Wert-Paar hinzuzufügen.
Standard-Realm	Diese Eigenschaft gibt den Standard-Realm an, wenn es mehr als eine Kerberos-Erweiterungskonfiguration gibt.
Automatische Site-Erkennung verwenden	Hat diese Option den Status „falsch“, verwendet die Kerberos-Erweiterung nicht automatisch LDAP und DNS, um ihren AD-Site-Namen zu ermitteln. Standardmäßig ist diese Option aktiviert.

Einstellung	Beschreibung
Standort-Code	Geben Sie den Namen der Active Directory-Site ein, den die Kerberos-Erweiterung verwenden soll.
Replikationszeit	Geben Sie die Zeit (in Sekunden) ein, die erforderlich ist, um Änderungen in der Active Directory-Domain zu replizieren. Die Kerberos-Erweiterung verwendet dies bei der Überprüfung des Passwortalters nach einer Änderung. Diese Option gilt für macOS 11 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version. Diese Option ist nun veraltet.
Anmeldeinformationen-Bundle-ID ACL	Klicken Sie auf **+ Hinzufügen**, um eine Liste von Bundle-IDs hinzuzufügen, die zur Authentifizierung auf das Ticket Granting Ticket (TGT) zugreifen dürfen.
Verwaltete Apps in Bundle-ID-ACL einschließen	Hat diese Option den Status „wahr“, erlaubt die Kerberos-Erweiterung nur verwalteten Apps den Zugriff und die Verwendung der Anmeldeinformationen. Bei entsprechender Spezifikation ist dies eine Ergänzung der Anmeldeinformationen-Bundle-ID ACL. Diese Option gilt für iOS 14 oder unterstützte neuere Versionen von Ivanti Neurons for MDM.
Kerberos-Apps in Bundle-ID-ACL einschließen	Falls "Wahr", ermöglicht die Kerberos-Erweiterung den Kerberos-Standarddienstprogrammen, einschließlich Ticket Viewer und klist, auf die Anmeldedaten zuzugreifen und sie zu verwenden. Verfügbar in MacOS 12 und höher.
Benutzerdefinierte Benutzernamen-Bezeichnung	Geben Sie die benutzerdefinierte Bezeichnung des Benutzernamens ein, die in der Kerberos-Erweiterung anstelle von "Benutzername" verwendet wird, z. B. "Firmen-ID". Diese Option gilt für macOS 11 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version.
Hilfetext	Geben Sie den Text ein, der dem Benutzer unten im Kerberos-Anmeldefenster angezeigt werden soll. Er kann verwendet werden, um Hilfeinformationen oder den Text des Haftungsausschlusses anzuzeigen. Diese Option gilt für iOS 14 und macOS 11 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version.
Modus zur Verwendung von Anmeldeinformationen	Diese Einstellung bestimmt, wie die Kerberos Extension-Anmeldeinformationen von anderen Prozessen verwendet werden. Verwenden Sie eine der folgenden Optionen: • Immer (Standard) - Die Extension-Anmeldeinformationen werden immer verwendet, wenn der Dienstprinzipalname (SPN) mit dem Array Kerberos Extension Hosts übereinstimmt. Die Anmeldeinformationen werden nicht verwendet, wenn die aufrufende App nicht in credentialBundleIDACL enthalten ist. • Wenn nicht angegeben - Die Anmeldeinformationen werden nur verwendet, wenn keine anderen Anmeldeinformationen von der aufrufenden App angegeben wurden und der SPN mit dem Array Kerberos Extensions Hosts übereinstimmt. Die Anmeldeinformationen werden nicht verwendet, wenn die aufrufende App nicht in credentialBundleIDACL enthalten ist. • Kerberos-Standard - Es wird der standardmäßige Kerberos-Prozess zur Auswahl von Anmeldeinformationen verwendet, der normalerweise die standardmäßigen Kerberos-Anmeldeinformationen verwendet. Dies ist identisch mit dem Ausschalten dieser Funktion. (Optional) Wählen Sie **TLS für LDAP erforderlich**.

Einstellung	Beschreibung
Bevorzugte Key Distribution Center	Fügen Sie bevorzugte Key Distribution Center hinzu. Klicken Sie auf **+Hinzufügen**, um ein bevorzugtes KDC hinzuzufügen. **Fallback für Plattform-SSO-Authentifizierung zulassen** – Wenn diese Option und "Plattform-SSO-TGT verwenden" auf "Wahr" gesetzt sind, kann sich der Benutzer manuell anmelden. verfügbar ab macOS 13
	Nur Kerberos ausführen – Wenn auf "Wahr" gesetzt, verarbeitet die Kerberos-Erweiterung nur Kerberos-Anfragen. Verfügbar ab macOS 13.
Wechsel in Kennwortmodus konfigurieren	**Plattform-SSO-TGT verwenden** – Falls auf "Wahr" gesetzt, verwendet diese Konfiguration einen TGT über das Plattform-SSO, statt einen neuen anzufordern. Verfügbar ab macOS 13. Falls wahr, kann der Benutzer die Benutzeroberfläche in den Kennwortmodus versetzen. Verfügbar ab macOS 15.
Wechsel in Smartcard-Modus konfigurieren	Falls wahr, kann der Benutzer die Benutzeroberfläche in den Smartcard-Modus versetzen. Verfügbar ab macOS 15.
Starten im Smartcard-Modus konfigurieren	Falls wahr, startet die Benutzeroberfläche im Smartcard-Modus. Verfügbar ab macOS 15.
Filter für automatische Auswahl des Identitätsherausgebers	Filtert die Liste der verfügbaren Smartcards. Verfügbar ab macOS 15.
Passworteinstellungen	
Passwort-Änderung erlauben	Hat diese Option den Status „falsch“, werden die Passwortänderungen deaktiviert. Diese Option gilt für macOS 10.15 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version. Standardmäßig ist diese Option aktiviert.
URL zur Änderung des Passworts	Geben Sie die URL ein, die im Standard-Webbrowser des Benutzers gestartet werden soll, wenn dieser eine Passwortänderung initiiert. Diese Option gilt für macOS 10.15 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version.
Passwort-Komplexität zulassen	Falls "Wahr" müssen die Kennwörter der Definition für "komplex" von Active Directory entsprechen. Diese Option gilt für macOS 10.15 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version.
Mindestlänge des Passworts	Geben Sie die Mindestlänge (in Zeichen) der Passwörter in der Domain ein. Diese Option gilt für macOS 10.15 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version.

Einstellung	Beschreibung
Benachrichtigung bei Ablauf des Passworts	Geben Sie ein, wie viele Tage vor Ablauf des Passworts eine Benachrichtigung über den Ablauf des Passworts an den Benutzer gesendet werden soll. Diese Option gilt für macOS 10.15 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version. Der Standardwert ist 15 Tage.
Passwortablauf überschreiben	Geben Sie ein, wie viele Tage die Passwörter in dieser Domain verwendet werden können. Für die meisten Domains kann dies automatisch berechnet werden. Diese Option gilt für macOS 10.15 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version. (Diese Option ist nun veraltet.)
Für das Passwort erforderlicher Text	Geben Sie die Textversion der Passwortanforderungen der Domain ein. Wird nur verwendet, wenn pwReqComplexity oder pwReqLength nicht angegeben sind. Diese Option gilt für macOS 10.15 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version.
Zahl der bisher verwendeten Passwörter	Geben Sie die Anzahl der früheren Passwörter ein, die in dieser Domain nicht wiederverwendet werden dürfen. Diese Option gilt für macOS 10.15 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version.
Passwort-Mindestalter	Geben Sie das Mindestalter (in Tagen) der Passwörter für eine Änderung in dieser Domain ein. Diese Option gilt für macOS 10.15 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version.
Synchronisierung des lokalen Passworts erlauben	Wenn diese Option den Status „falsch“ hat, wird die Passwortsynchronisation deaktiviert. Dies funktioniert nicht, wenn der Benutzer mit einem mobilen Konto eingeloggt ist. Diese Option gilt für macOS 10.15 bis zur neuesten von Ivanti Neurons for MDM unterstützten Version.
Kennwortanforderung RTF-Daten	Die als RTF-Datei formatierte Version der Anforderungen für das Domänenkennwort. Verfügbar ab macOS 15. Wird nur verwendet, wenn pwReqComplexity oder pwReqLength nicht angegeben sind.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.6.14. Netzwerkrelais-Konfiguration

Ivanti Neurons for MDM aktiviert die Netzwerkrelais-Konfiguration für die Payload, die Sie zum Konfigurieren der Relaiseinstellungen für ein Gerät oder eine Anwendung verwenden, ohne dass VPN oder Tunnels auf private Ressourcen zugreifen müssen.

Gilt für:

- iOS 17.0 bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird.
- macOS 14.0 bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird.
- visionOS 1.1 bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Netzwerkrelais** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie die Einstellungen für das **Netzwerkrelais** gemäß der folgenden Tabelle:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
HTTP/3-Relais-URL **HTTP/2-Relais-URL**	Geben Sie einen URL-Wert an, den Sie als Wert im HTTP-Feld für diese Konfiguration verwenden möchten. Schließen Sie die HTTP/2-Relais-URL und/oder HTTP/3-Relais-URL ein. Geben Sie einen URL-Wert an, den Sie als Wert im HTTP-Feld für diese Konfiguration verwenden möchten. Schließen Sie die HTTP/2-Relais-URL und/oder HTTP/3-Relais-URL ein.
Zusätzliche Felder für HTTP-Header	Geben Sie den HTTP-Header-Feldwert für den entsprechenden Header-Feldnamen an.
Zertifikat	Wählen Sie eines der von Ihnen erstellten Identitätszertifikate in der Dropdownliste aus.
Unformatierter öffentlicher Schlüssel **+ Hinzufügen** **Domänen abgleichen**	Geben Sie die öffentlichen unformatierten Schlüssel an, um den Server während einer Netzwerkverbindung zu authentifizieren. Wählen Sie **+ Hinzufügen** aus, um mehrere Netzwerkrelais-Konfigurationen hinzuzufügen. Geben Sie die Domänenliste an, um zu bestimmen, welche Verbindung über die Server in den Relais geleitet werden soll.
Domänen ausschließen	Geben Sie die Domänenliste an, um zu bestimmen, welche Verbindung über die Server in den Relais vermieden werden soll.
FQDNs abgleichen (unterstützt auf Geräten mit iOS 18.4+ und macOS 15.4+)	Geben Sie die Liste der vollständig qualifizierten Domänennamen (FQDNs) oder Hostnamen an, die über die in Relais enthaltenen Server weitergeleitet werden sollen. Alle Verbindungen, die genau diesem FQDN oder Hostnamen entsprechen, verwenden die Relais. Wenn keine FQDNs und keine 'MatchDomains' aufgeführt sind, wird der gesamte Datenverkehr an alle Domänen, mit Ausnahme der, die mit einer ausgeschlossenen Domäne oder einem ausgeschlossenen FQDN übereinstimmen, an die Relais-Server weitergeleitet.
FQDNs ausschließen (unterstützt auf Geräten mit iOS 18.4+ und macOS 15.4+)	Geben Sie die Liste der vollständig qualifizierten Domänennamen (FQDNs) oder Hostnamen an, die **NICHT** über die in Relais enthaltenen Server weitergeleitet werden sollen. Alle Verbindungen, die genau diesem FQDN oder Hostnamen entsprechen, verwenden nicht den Relais-Server. Wenn auch 'MatchDomains' angegeben sind, sollte jede in 'ExcludedFQDNs' aufgeführte FQDN eine Unterdomäne von mindestens einer MatchDomain sein. Anderenfalls hat die Konfiguration keine Wirkung.

4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
5. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Netzwerkrelais** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
6. Klicken Sie auf **Fertig**.

10.10.6.15. Sichere Anmeldung für mehrere Benutzer in iOS

Mit dem Multi-User-Webclip können sich Benutzer bei iOS-Geräten, die in der Cloud registriert sind, an- und abmelden. Wenn sich ein Benutzer zum ersten Mal anmeldet, werden die Profile, Apps und Konfigurationen, die diesem Benutzer zugeordnet sind, per Push auf das Gerät übertragen. Wenn diese ihre Arbeit beendet haben, können sie den Webclip öffnen und die Funktion „Abmelden“ wählen, die das Gerät dem Nobody-Benutzer zuweist und die dem ursprünglich angemeldeten Benutzer zugeordneten Profile, Apps und Konfigurationen entfernt, solange die Konfigurationen und Anwendungen nicht an den Nobody-Benutzer verteilt werden. Nach einer Abmeldung wird der Webclip zurückgesetzt, so dass sich der nächste Benutzer anmelden und seine benutzerdefinierten Konfigurationen, Anwendungen und Richtlinien erhalten kann. Für die Verwendung der sicheren Mehrbenutzer-Anmeldefunktion ist keine Geräteüberwachung erforderlich. In dem Support-Wissensdatenbank-Artikel **Cloud: Sichere Anmeldung für mehrere Benutzer für iOS** finden Sie weitere Informationen über die Anmeldefunktion für mehrere Benutzer.

Gilt für: iOS-Geräte (gilt nicht für benutzerregistrierte Geräte)

Dieser Abschnitt enthält die folgenden Themen:

- **Unterstützte Anmeldeinformationen**
- **Informationen zum „Nobody“-Benutzer**
- **Bei einem Gerät anmelden**
- **Von einem Gerät abmelden**

Unterstützte Anmeldeinformationen

Zur Anmeldung bei dem sicheren Mehrbenutzer-Webclip müssen Benutzername und Passwort verwendet werden. Die PIN-Registrierung wird durch den sicheren Mehrbenutzer-Webclip nicht unterstützt.

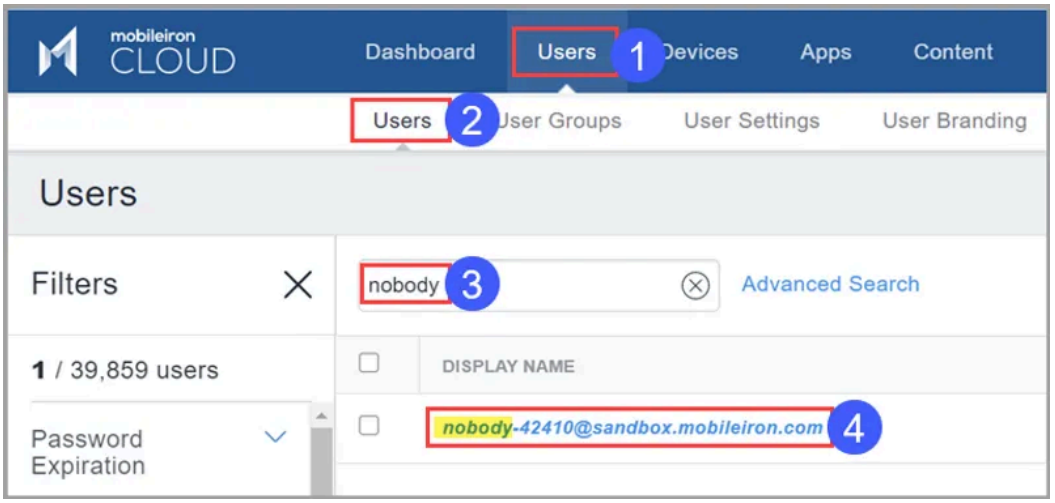
Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **Sichere Anmeldung für mehrere Benutzer in iOS**. Möglicherweise müssen Sie die Suchfunktion verwenden, wenn es mehrere Seiten mit Konfigurationen gibt. Auf diese Konfiguration kann nicht durch Auswahl von **+Hinzufügen**zugegriffen werden.
3. Klicken Sie auf **Verteilung bearbeiten** oder auf das zugehörige Symbol, um den Webclip an die entsprechende Gerätegruppe zu verteilen.
   
   Wenn Sie ihn an eine Benutzergruppe verteilen möchten, können Sie eine dynamische Gerätegruppe erstellen, die an eine Benutzergruppe gebunden ist.
4. Wählen Sie eine der folgenden Verteilungsoptionen und denken Sie daran, dass Sie den Webclip immer an den Nobody-Benutzer oder die mit dem Nobody-Benutzer verbundene Gerätegruppe verteilen müssen. Dies geschieht nicht standardmäßig, stellen Sie also sicher, dass Sie ihn an den Nobody-Benutzer verteilen.
   - Alle Geräte
   - Keine Geräte (Standard)
   - Anpassbar

Klicken Sie auf **Speichern**.

Informationen zum „*Nobody*"-Benutzer

Ivanti Neurons for MDMAuch wenn ein Gerät über den Webclip abgemeldet wurde, bleibt es bei MobileIron für einen speziellen Benutzer (den „Nobody User") angemeldet. Wenn Sie Apps und Konfigurationen von dem Gerät entfernen möchten, wenn sich ein Benutzer abmeldet, müssen Sie sicherstellen, dass diese Anwendungen und Konfigurationen nicht an den Nobody-Benutzer verteilt werden. Wenn Sie möchten, dass bestimmte Konfigurationen, wie WLAN, auf dem Gerät verbleiben, wenn sich ein Benutzer vom Secure Sign-In-Webclip abmeldet, müssen Sie sicherstellen, dass diese Konfigurationen auch an den Nobody-Benutzer verteilt werden.



Das bedeutet, dass Sie beachten müssen, auf welche Benutzergruppen und Gerätegruppen Sie Apps und Konfigurationen verteilen. Wenn Sie eine App an Jedermann verteilen und sie wieder entfernen möchten, wenn sich ein Benutzer von dem Gerät abmeldet, sollten Sie eine Benutzergruppe erstellen, die keinen Nobody-Benutzer enthält. Benutzerdefinierte Attribute machen es viel einfacher, eine Gruppe von Benutzern zu erstellen, die „Multi-User" sind, und eine weitere Benutzergruppe, die nur aus dem Nobody User besteht. Sie können unter Admin> System > Attribute ein Benutzerattribut mit der Bezeichnung „Mehrbenutzer-Eigentümer" erstellen und dann dem Nobody-Benutzer den Wert „Ja" oder „Wahr" zuweisen. Sie können dann Benutzergruppen und Gerätegruppen je nach dem Wert des Attributs erstellen.

Bei einem Gerät anmelden

Ein Benutzer kann sich bei einem iOS-Gerät anmelden und das Gerät seiner Person zuordnen. Nach der Anmeldung werden alle relevanten Anwendungen, Richtlinien, Konfigurationen und Zertifikate per Push auf das Gerät übertragen.

> Aus Sicherheitsgründen müssen sich iDP-Benutzer bei der Anmeldung erneut authentifizieren, selbst wenn sie bereits beim Gerät angemeldet sind.

Von einem Gerät abmelden

Ein Benutzer kann nach der Nutzung sein iOS-Gerät abmelden. Nach der Abmeldung werden die Anwendungen, Richtlinien, Konfigurationen und Zertifikate von dem Gerät entfernt und das Gerät bleibt in dem Status, in dem es sich vor der Benutzeranmeldung befand. Damit kann sich nun ein anderer Benutzer auf dem Gerät anmelden.

> Melden Sie sich von allen Microsoft-Apps ab, bevor Sie sich vom Web-Clip für mehrere Benutzer abmelden.

Multi_User_Sign-In_Branding.htmWeitere Informationen finden Sie unter Anmeldung für mehrere Benutzer - Branding

10.10.6.16. Konfiguration der Android-APN-Einstellungen

Mit den Android APN-Einstellungskonfigurationen können Sie die Einstellungen für den Access Point Name (APN) festlegen, die für Geräte in einem öffentlichen Netzwerk erforderlich sind. Diese Konfiguration gilt für verwaltete Android Enterprise Work-Geräte und verwaltete Geräte mit Arbeitsprofil auf firmeneigenem Gerät (mit Android Version 9.0 oder unterstützten neueren Versionen).

Verfahren

1. Gehen Sie zu **Konfiguration > +Hinzufügen**.
2. Wählen Sie die Konfiguration der **Android-APN-Einstellungen**.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Konfigurieren Sie im Abschnitt Konfigurations-Setup die folgenden Optionen:
6. Klicken Sie auf **Weiter**.

Einstellung	Beschreibung
Eintragname	Geben Sie den Namen der Zugangspunkt-Einstellungen ein.
Zugangspunktname	Geben Sie den Namen des Zugangspunkts ein.
Zugangspunktart	Wählen Sie die Art des Zugangspunktes aus folgenden Optionen aus: • **Standard** • **DUN** • **IMS** • **Notfall** • MMS • **HIPRI** • **CBS** • **MCX** • **SUPL** • **FOTA** • **IA**
MVNO-Typ	Wählen Sie die Art des mobilen virtuellen Netzwerkbetreibers aus folgenden Optionen aus: • **Keine** • **SPN** • **IMSI** • **GID** • **ICCID**
Bearer	Wählen Sie aus den folgenden Optionen die Art des für die Datenübertragung verwendeten Trägerdienstes aus: • **1xRTT** • **CDMA** • **EDGE** • **EHRPO** • **EVDO** • **EVDO A** • **EVDO B** • **GPRS** • **GSM** • **HSDPA** • **HASP** • **HSPAP** • **HSUPA**

Einstellung	Beschreibung
	• **IDEN** • **IWLAN** • **LTE** • **NR** • **TD_SCDMA** • **UMTS**
APN-Protokoll	Wählen Sie das für den APN erforderliche APN-Protokoll aus. Folgende Optionen sind verfügbar: • **Keine** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP** (Punkt-zu-Punkt-Protokoll) • **UNSTRUKTURIERT**
APN-Roaming-Protokoll	Wählen Sie das für den APN erforderliche APN-Roaming-Protokoll aus. Folgende Optionen sind verfügbar: • **Keine** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP** (Punkt-zu-Punkt-Protokoll) • **UNSTRUKTURIERT**
APN aktivieren/deaktivieren	Schalten Sie die APN-Konfiguration ein.
Träger-ID	Geben Sie den numerischen Wert der Provider-ID ein.
Authentifizierungstyp	Wählen Sie die Art des Authentifizierungsprotokolls aus folgenden Optionen aus: • **Keine** • **PAP** (Passwortauthentifizierungsprotokoll) • **CHAP** (Challenge-Handshake-Authentifizierungsprotokoll) • **PAP oder CHAP**
Benutzername	Geben Sie den Benutzernamen für die Anmeldung ein.
Passwort	Geben Sie das Anmeldepasswort ein.
Passwort bestätigen	Geben Sie das Passwort zur Bestätigung erneut ein.

Einstellung	Beschreibung
Port-Nummer	Geben Sie die Portnummer ein (numerischer Wert zwischen 1 und 65535).
Proxyadresse	Geben Sie die Proxy-Adresse ein.
Mobiltelefonie-Landescode	Geben Sie die Landesvorwahl für das Mobilfunknetz ein.
Mobiltelefonie-Netzwerkcode	Geben Sie die Vorwahl für das Mobilfunknetz ein.
MMS-Proxyadresse	Geben Sie die MMS-Proxy-Adresse ein.
MMS-Portnummer	Geben Sie die MMS-Portnummer ein (numerischer Wert zwischen 1 und 65535).
MMS-Server-Adresse (mmsc)	Geben Sie die MMS-Server-Adresse ein.

7. Wählen Sie eine der folgenden Verteilungsoptionen aus:
8. Klicken Sie auf **Fertig**.

- **Alle Geräte**
- Keine Geräte (Standard)
- **Anpassbar**

Sie können keine weitere APN-Konfiguration mit den gleichen Werten für die folgenden Felder hinzufügen, wenn bereits eine APN-Konfiguration mit diesen Werten für das Gerät vorhanden ist:

- Mobiltelefonie-Landescode
- Mobilnetzwerkcode
- Zugangspunktname
- Proxyadresse
- Port-Nummer
- MMS-Proxyadresse
- MMS-Portnummer
- MMS-Serveradresse
- APN aktivieren/deaktivieren
- MVNO-Typ
- APN-Protokoll
- APN-Roaming-Protokoll

Die Konfiguration der Android-APN-Einstellungen überschreibt die APN-Einstellungen, die bereits manuell oder durch den Netzbetreiber im Gerät konfiguriert wurden.

10.10.6.17. VPN-Konfiguration

Gilt für:

- Android (veraltet auf Android Enterprise-Geräten; verwenden Sie die verwaltete Konfiguration für spezifisches VPN aus dem App-Katalog)
- Windows
- iOS-
- macOS
- tvOS
- visionOS

Eine VPN-Konfiguration bestimmt die Einstellungen für den Zugriff auf ein Virtual Private Network (virtuelles privates Netzwerk).

> Für diese Konfiguration ist die Delegierung mit benutzerdefinierter Verteilung verfügbar. Weitere Informationen finden Sie unter *Verteilen der Konfiguration* unter **Arbeiten mit Konfigurationen**.

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Wählen Sie die **VPN**-Konfiguration aus.
3. Geben Sie einen **Namen** für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Konfigurieren Sie die VPN-Einstellungen gemäß den folgenden Beschreibungen.
6. (Nur iOS 9.0+) Klicken Sie im Abschnitt "Domains abgleichen" auf **+Hinzufügen**, um eine oder mehrere passende Domains hinzuzufügen (Beispiel: company.com). Die Proxyverbindung wird verwendet, wenn die Domain eine der angegebenen Domains ist.
7. Klicken Sie auf **Weiter**.
8. (Nur macOS) Wählen Sie auf der Seite „Verteilen“ eine der folgenden Verteilungsoptionen aus:
    - Gerätekanal - Die Konfiguration gilt für alle Benutzer eines Geräts. Dies ist die typische Option.
    - Benutzerkanal - Die Konfiguration gilt nur für den aktuell auf einem Gerät registrierten Benutzer.
9. Wählen Sie die verbleibenden Verteilungsoptionen für diese Konfiguration aus.
10. Klicken Sie auf **Fertig**.

VPN-Einstellungen

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Verbindungstyp	Wählen Sie den zu konfigurierenden VPN-Typ. Die übrigen Einstellungen hängen von dieser Wahl ab.

Die Protokolle und ihre Einstellungen sind im Folgenden aufgeführt:

- L2TP (wird nicht auf Ivanti Go unterstützt)
- PPTP (wird nicht auf Ivanti Go unterstützt)
- IPsec (Cisco) (wird nicht auf Ivanti Go unterstützt)
- Cisco AnyConnect (wird auf Ivanti Go unterstützt)
- Juniper SSL (wird nicht auf Ivanti Go unterstützt)
- NetMotion VPN (wird nicht auf Ivanti Go unterstützt)
- Pulse Secure (wird auf Ivanti Go unterstützt)
- F5 SSL (wird nicht auf Ivanti Go unterstützt)
- SonicWALL Mobile Connect (wird nicht auf Ivanti Go unterstützt)
- Aruba VIA (wird nicht auf Ivanti Go unterstützt)
- Benutzerdefiniertes SSL (wird nicht auf Ivanti Go unterstützt)
- Palo Alto Networks GlobalProtect (unterstützt auf Ivanti Go)
- KEv2 (nur Windows) (wird nicht auf Ivanti Go unterstützt)
- IKEv2 (wird nicht auf Ivanti Go unterstützt)

L2TP

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Wählen Sie die zu verwendende Authentifizierungsmethode: **Passwort** oder **RSA SecurID**.
Gruppenpasswort	Geben Sie das Gruppenpasswort ein, wenn der Verbindungsaufbau dies erfordert.
Kompletten Datenverkehr senden	Wählen Sie diese Option, um diese Verbindung für den gesamten Netzwerkverkehr zu nutzen. Diese verhindert, dass Daten kompromittiert werden, insbesondere in öffentlichen Netzwerken.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

PPTP

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Wählen Sie die zu verwendende Authentifizierungsmethode: **Passwort** oder **RSA SecurID**.
Verschlüsselungsstufe	Wählen Sie eine Stufe der Datenverschlüsselung für die Verbindung: **Keine, Automatisch** oder **Maximal (128 Bit)**.
Kompletten Datenverkehr senden	Wählen Sie diese Option, um diese Verbindung für den gesamten Netzwerkverkehr zu nutzen. Diese verhindert, dass Daten kompromittiert werden, insbesondere in öffentlichen Netzwerken.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

IPsec (Cisco)

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Maschinenauthentifizierung	Wählen Sie die zu verwendende Authentifizierungsmethode: **Gruppenpasswort/Gruppenname** oder **Zertifikat**.
Gruppenname	Authentifizierung per Gruppenpasswort/Gruppenname Geben Sie den Namen der zu verwendenden Gruppe ein. Wenn die hybride Authentifizierung verwendet wird, muss die Zeichenfolge mit „[hybrid]“ enden.
Gruppenpasswort	Authentifizierung per Gruppenpasswort/Gruppenname Geben Sie das Gruppenpasswort ein.
Hybride Authentifizierung verwenden	Authentifizierung per Gruppenpasswort/Gruppenname Wählen Sie diese Option, um die Hybride Authentifizierung zu spezifizieren, d. h., der Server stellt ein Zertifikat aus und der Client einen freigegebenen Schlüssel.
Passwortabfrage	Authentifizierung per Gruppenpasswort/Gruppenname Bestimmen Sie, ob der Benutzer beim Verbindungsaufbau zur Eingabe eines Passworts aufgefordert werden soll.
Anmeldeinformationen	*Authentifizierung per Zertifikat* Wählen Sie das zu verwendende Identitätszertifikat.
Benutzer-PIN einschließen	*Authentifizierung per Zertifikat* Wählen Sie diese Option, um den Benutzer zur Eingabe einer PIN aufzufordern.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie **Automatisch** wählen, sind die folgenden zusätzlichen Felder verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Cisco AnyConnect

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Gruppe	Geben Sie die Gruppe ein, die zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Wählen Sie die Methode für die Benutzerauthentifizierung: **Passwort** oder **Zertifikat**. Wenn Sie **Zertifikat** wählen, ist das folgende Feld verfügbar: **Berechtigungsnachweis**: Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Juniper SSL

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
[Realm]	Geben Sie den Realm ein, der zur Authentifizierung der Verbindung verwendet werden soll.
Rolle	Geben Sie die Authentifizierungsrolle ein, die zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Wählen Sie die Methode für die Benutzerauthentifizierung: **Passwort** oder **Zertifikat**. Wenn Sie **Zertifikat** wählen, ist das folgende Feld verfügbar: **Berechtigungsnachweis**: Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

NetMotion VPN

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Wählen Sie die Methode für die Benutzerauthentifizierung: **Passwort** oder **Zertifikat**. Wenn Sie **Zertifikat** wählen, ist das folgende Feld verfügbar: **Berechtigungsnachweis**: Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

F5 SSL

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Geben Sie die Methode für die Benutzerauthentifizierung ein: **Passwort** oder **Zertifikat**. Wenn Sie **Zertifikat** wählen, ist das folgende Feld verfügbar: **Berechtigungsnachweis**: Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie „Manuell“ oder „Automatisch“ zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

SonicWALL Mobile Connect

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Anmeldegruppe oder Domäne	Geben Sie die Anmeldegruppe oder Domäne ein, die zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Wählen Sie die Methode für die Benutzerauthentifizierung: **Passwort** oder **Zertifikat**. Wenn Sie „Zertifikat“ wählen, ist das folgende Feld verfügbar: **Berechtigungsnachweis**: Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Aruba VIA

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Wählen Sie die Methode für die Benutzerauthentifizierung: **Passwort** oder **Zertifikat**. Wenn Sie **Zertifikat** wählen, ist das folgende Feld verfügbar: **Berechtigungsnachweis**: Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie „Manuell“ oder „Automatisch“ zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Benutzerdefinierte SSL

Einstellung	So gehen Sie vor
Identifikator [Server] Konto Benutzerdefinierte Daten	Geben Sie den Identifikator für dieses benutzerdefinierte SSL VPN im umgekehrten DNS-Format ein (zum Beispiel: com.mycompany.myserver). Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein. Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll. Geben Sie die Schlüssel-Wert-Paare zur Bestimmung der benutzerdefinierten Daten für dieses VPN ein.
Benutzerauthentifizierung	Wählen Sie die Methode für die Benutzerauthentifizierung: **Passwort** oder **Zertifikat**. Wenn Sie „Zertifikat“ wählen, ist das folgende Feld verfügbar: **Berechtigungsnachweis**: Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Palo Alto Networks GlobalProtect

> Gilt nicht für Android-Geräte.

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerdefinierte Daten	Geben Sie die Schlüssel-Wert-Paare zur Bestimmung der benutzerdefinierten Daten für dieses VPN ein.
Benutzerauthentifizierung	Wählen Sie die Methode für die Benutzerauthentifizierung: **Passwort** oder **Zertifikat**. Wenn Sie „Zertifikat“ wählen, ist das folgende Feld verfügbar: **Berechtigungsnachweis**: Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

IKEv2 (nur Windows)

Einstellung	Aktion
[Server]	Geben Sie den Hostnamen bzw. die IP-Adresse des VPN-Servers ein.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

IKEv2

Einstellung	Aktion
[Server]	Geben Sie den Hostnamen bzw. die IP-Adresse des VPN-Servers ein.
Lokaler Identifikator	ID des IKEv2-Clients in einem der folgenden Formate: • FQDN • UserFQDN • Adresse • ASN1DN
Remote-Identifikator	Remoter Identifikator in einem der folgenden Formate: • FQDN • UserFQDN • Adresse • ASN1DN
Maschinenauthentifizierung	Nur verfügbar, wenn die Option **EAP aktivieren** nicht ausgewählt ist. Klicken Sie auf eine der folgenden Optionen: • Zertifikat • Gruppenpasswort
EAP-Authentifizierung	Nur verfügbar, wenn die Funktion **EAP aktivieren** ausgewählt ist. Klicken Sie auf eine der folgenden Optionen: • Zertifikat • Benutzername/Passwort
Gruppenpasswort	Nur verfügbar, wenn das Gruppenpasswort für die Maschinenauthentifizierung ausgewählt wurde. Geben Sie das Gruppenpasswort für die Verbindung ein.
Anmeldeinformationen	Nur verfügbar, wenn das Zertifikat für die Maschinenauthentifizierung ausgewählt wurde. Wählen Sie das zu verwendende Zertifikat aus. Dieses Zertifikat wird zur IKE-Client-Authentifizierung versendet. Wenn eine erweiterte Authentifizierung verwendet wird, kann dieses Zertifikat für EAP-TLS verwendet werden.
EAP aktivieren	Klicken Sie, um die erweiterte Authentifizierung zu aktivieren.
Konto	Nur verfügbar, wenn für die EAP-Authentifizierung [Username/Password] ausgewählt ist. Geben Sie die Konto-ID für den VPN-Server ein.
Passwort	Nur verfügbar, wenn für die EAP-Authentifizierung [Username/Password] ausgewählt ist. Geben Sie das Passwort für den VPN-Server ein.
Dead Peer-Erkennungsintervall	Wählen Sie eine der folgenden Optionen aus: • Keine (Deaktivieren) • Niedrig (keepalive wird einmal stündlich versendet). • Mittel (keepalive wird alle 30 Minuten gesendet). • Hoch (keepalive wird alle 10 Minuten gesendet).

Einstellung	Aktion
Trivialname des Server-Zertifikatausstellers	(Optional) – Allgemeiner Name eines Server-Zertifikatausstellers; veranlasst den IKE-Server, eine Zertifikatsanforderung des Zertifikatausstellers an den Server zu senden.
Trivialname des Server-Zertifikats	(Optional) – Allgemeiner Name eines Serverzertifikats zur Validierung des Zertifikats, das vom IKEv2-Server gesendet wurde.
IP4- und IP6-Subnetzattribute verwenden	(Optional) Wählen Sie diese Option aus, um IP4- und IP6-Subnetzattribute zu verwenden.
IKEv2 Mobilität und Multihoming-Protokoll (MOBIKE) aktivieren	(Optional) Die Standardeinstellung ist "0". MOBIKE (Die Möglichkeit, Mobilgeräte an mehreren Standorten zu unterstützen, wenn Verbindungen sowohl über WLAN als auch über Mobilfunk mit mehreren IP-Adressen aktiviert sind.) Diese Option ist standardmäßig aktiviert. Stellen Sie "1" ein, um MOBIKE zu deaktivieren.
Perfect Forward Secrecy (PFS) aktivieren	(Optional) Bei der Einstellung "1" wird PFS für IKEv2-Verbindungen aktiviert. Die Standardeinstellung ist "0".
IKEv2-Umleitung aktivieren	(Optional) Die Standardeinstellung ist "0". Die IKEv2-Verbindung wird umgeleitet, wenn eine Umleitanforderung vom Server empfangen wird. Diese Option ist standardmäßig aktiviert. Stellen Sie „1“ ein, um die IKEv2-Umleitung zu deaktivieren.
NAT keepalive aktivieren	Aktiviert die Netzwerkadressen-Übersetzung keepalive und verhindert, dass NAT-Einträge gelöscht werden, wenn kein Traffic vorhanden und die Netzwerkadress-Übersetzung zwischen IKE-Peers aktiviert ist.
NAT keepalive-Intervall	Wenn die Option "NAT keepalive" aktiviert ist, ist dies die Zeit in Sekunden, in der keepalive-Pakete für das Gerät gesendet werden.
PPK	Geben Sie den Post-quantum Pre-shared key (PPK) mit VPN-Servern ein, die RFC 8784 unterstützen. Wenn dieser Schlüssel vorhanden ist, muss auch die PKK-Kennung vorhanden sein.
PPK-Kennung	Geben Sie die PPK-Kennung ein.
PPK obligatorisch	Wählen Sie eine der folgenden Dropdownoptionen aus: • **Mandat**: Die VPN-Verbindung wird hergestellt, wenn der Server RFC 8784 unterstützt oder die bei "PKK-Kennung" angegebene PKK-Kennung akzeptiert. • **Kein Mandat**: Die VPN-Verbindung wird nicht hergestellt, wenn der Server RFC 8784 nicht unterstützt oder die bei "PKK-Kennung" angegebene PKK-Kennung nicht akzeptiert.
Verschlüsselungsalgorithmus	Wählen Sie eine der folgenden Optionen aus: • **DES** • **3DES** • **AES-128** • **AES-256** (Standard)

Einstellung	Aktion
	• **AES-128 GCM** • **AES-256 GCM**
Integritätsalgorithmus	Wählen Sie eine der folgenden Optionen aus: • **SHA2-256** (Standard) • **SHA2-384** • **SHA2-512**
Diffie-Hellman-Gruppe	Wählen Sie eine der folgenden Optionen aus: • **1** • **2** (Standard) • **5** • **14** • **15** • **16** • **17** • **18**
Nutzungsdauer in Minuten	Geben Sie die SA-Gültigkeitsdauer (Intervall für Neuverschlüsselung) in Minuten ein. Gültige Werte sind 10 bis 1440.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

*Geben Sie „$“ ein, um eine Liste mit unterstützten **Variablen** anzuzeigen, sofern dies für dieses Feld verfügbar ist.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.6.18. VPN-on-Demand

Gilt für iOS-Geräte

Eine VPN-on-Demand-Konfiguration bestimmt den Zugriff auf einen VPN-Server basierend auf Domänen, Host-Namen, usw.

VPN-on-Demand-Einstellungen

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Verbindungstyp	Wählen Sie den zu konfigurierenden VPN-Typ. Die übrigen Einstellungen hängen von dieser Wahl ab.
VPN-on-Demand aktivieren	Bestimmen Sie, diese Konfiguration für Domänen und Host-Namen zu verwenden, die ein VPN-on-Demand einrichten.
iOS-Regeln aktivieren (Gilt nur, wenn die Option "VPN nach Bedarf aktivieren" ausgewählt ist.)	Für iOS- und macOS-Systeme können Sie Folgendes konfigurieren: • Netzwerkregeln, die den Verbindungsaufbau mit Netzwerken erlauben oder verhindern bzw. diese ignorieren, wenn die Prüfung den Wert „Wahr“ ergibt. • Sie können mit Verbindungsregeln Verbindungen mit Netzwerken zulassen oder verweigern, die bei der Prüfung den Wert „Wahr“ ergeben. Für Netzwerkregeln können Sie folgende Parameterarten definieren: • DNS-Domänen-Abgleich • DNS-Serveradressen-Abgleich • SSID-Abgleich • URL-Zeichenfolgen-Test • Schnittstellentyp-Abgleich Für Verbindungsregeln können Sie folgende Parameterarten definieren: • DNS-Domänen-Abgleich • DNS-Serveradressen-Abgleich • SSID-Abgleich • URL-Zeichenfolgen-Test • Schnittstellentyp-Abgleich • Domänenname • DNS-Server • URL-Test
Providerart (iOS 9+)	Wählen Sie einen der folgenden Tunnel-Provider: • App-Proxy – Tunnel-Traffic auf App-Ebene. Eine Übersicht über den App Proxy Provider finden Sie in der **Apple-Dokumentation**. • Paket-Tunnel – Tunnel-Traffic auf der IP-Ebene. Eine Übersicht über Packet Tunnel Provider finden Sie in der **Apple-Dokumentation**.
EnforceRoutes	Falls aktiviert, übersteuern die nicht standardmäßigen Routen des VPN etwaige lokal definierte Routen. • Wenn IncludeAllNetworks aktiviert ist, ignoriert das System die Einstellung EnforceRoutes. • Verfügbar ab iOS 14.2 und höher.

Einstellung	So gehen Sie vor
ExcludeLocalNetworks	Wenn diese Option zusammen mit IncludeAllNetworks aktiviert ist, wird der gesamte lokale Datenverkehr außerhalb des VPN geleitet.
IncludeAllNetworks	Falls aktiviert, wird der gesamte Datenverkehr über das VPN geleitet.

Die Protokolle und ihre Einstellungen sind im Folgenden aufgeführt:

- **IPsec (Cisco)**
- **Cisco AnyConnect**
- **Juniper SSL**
- **NetMotion VPN**
- **F5 SSL**
- **SonicWALL Mobile Connect**
- **Aruba VIA**
- **Benutzerdefinierte SSL**
- **Palo Alto Networks GlobalProtect**

IPsec (Cisco)

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Maschinenauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Benutzer-PIN einschließen	Wählen Sie diese Option, um den Benutzer zur Eingabe einer PIN aufzufordern.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. **Wenn Sie „Manuell“ wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. **Wenn Sie „Automatisch“ wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Cisco AnyConnect

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Gruppe	Geben Sie die Gruppe ein, die zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. **Wenn Sie „Manuell" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. **Wenn Sie „Automatisch" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Juniper SSL

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
[Realm]	Geben Sie den Realm ein, der zur Authentifizierung der Verbindung verwendet werden soll.
Rolle	Geben Sie die Authentifizierungsrolle ein, die zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. **Wenn Sie „Manuell" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. **Wenn Sie „Automatisch" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

NetMotion VPN

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Das Benutzer-Authentifizierungsverfahren ist „Zertifikat". **Berechtigungsnachweis**: Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**" wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Wenn Sie „**Automatisch**" wählen, ist das folgende zusätzliche Feld verfügbar: **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

F5 SSL

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. **Wenn Sie „Manuell" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. **Wenn Sie „Automatisch" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

SonicWALL Mobile Connect

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Anmeldegruppe oder Domäne	Geben Sie die Anmeldegruppe oder Domäne ein, die zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. **Wenn Sie „Manuell" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. **Wenn Sie „Automatisch" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Aruba VIA

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. **Wenn Sie „Manuell" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. **Wenn Sie „Automatisch" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Benutzerdefinierte SSL

Einstellung	So gehen Sie vor
Identifikator	Geben Sie den Identifikator für dieses benutzerdefinierte SSL VPN im umgekehrten DNS-Format ein (zum Beispiel: com.mycompany.myserver).
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerdefinierte Daten	Geben Sie die Schlüssel-Wert-Paare zur Bestimmung der benutzerdefinierten Daten für dieses VPN ein.
Benutzerauthentifizierung	Nur die Authentifizierung per Zertifikat wird unterstützt.
Anmeldeinformationen	Wählen Sie das zu verwendende Identitätszertifikat.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. **Wenn Sie „Manuell" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. **Wenn Sie „Automatisch" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Palo Alto Networks GlobalProtect

Einstellung	So gehen Sie vor
[Server]	Geben Sie die IP-Adresse bzw. den Hostnamen für den VPN-Server ein.
Konto	Geben Sie das Benutzerkonto ein, das zur Authentifizierung der Verbindung verwendet werden soll.
Benutzerdefinierte Daten	Geben Sie die Schlüssel-Wert-Paare zur Bestimmung der benutzerdefinierten Daten für dieses VPN ein.
Benutzerauthentifizierung	Das Benutzer-Authentifizierungsverfahren ist „Zertifikat". Wählen Sie ein Identitätszertifikat für das Feld **Berechtigungsnachweis** aus.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. **Wenn Sie „Manuell" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. **Wenn Sie „Automatisch" wählen**, sind die folgenden zusätzlichen Felder verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.

Variables.htmGeben Sie „$" ein, um eine Liste mit unterstützten Variablen anzuzeigen, sofern diese für dieses Feld verfügbar ist.

Weitere Informationen finden Sie unter **Konfiguration erstellen**

10.10.6.19. WLAN-Konfiguration

Gilt für:

- Android
- Windows
- iOS-
- macOS
- watchOS
- visionOS
- tvOS

Dieser Abschnitt enthält die folgenden Themen:

WLAN-Einstellungen

- **WEP, WPA/WPA2/WPA3, beliebige (persönliche) Einstellungen**
- **WEP Enterprise, WPA/WPA2/WPA3 Enterprise, beliebige (persönliche) Einstellungen**
- **iOS, macOS und visionOS**

WLAN-Einstellungen

Eine WLAN-Konfiguration richtet den Zugriff auf ein Wireless-Netzwerk ein.

> Ein Benutzer kann einige WLAN-Einstellungen auf dem Gerät modifizieren. Der MDM-Server kann gegebenenfalls keine Informationen über die Änderungen empfangen, dies hängt vom Betriebssystem des Geräts ab. Die Konfigurationen werden daher nicht automatisch erneut per Push auf das Gerät übertragen, um die Konfiguration des Geräts mit der Konfiguration auf dem Server zu überschreiben.

> Für diese Konfiguration ist die Delegierung mit benutzerdefinierter Verteilung verfügbar. Weitere Informationen finden Sie unter *Verteilen der Konfiguration* unter **Arbeiten mit Konfigurationen**.

> Bei bestimmten Versionen von Android-Geräten müssen Administratoren möglicherweise Domänen- und weitere Informationen eingeben, um eine Verbindung zu TLS, TTLS, PEAP usw. herzustellen. (WPA2) Netzwerke. Es wird empfohlen, Änderungen an der WLAN-Konfiguration zunächst auf ausgewählten Geräten zu testen, bevor Sie sie auf eine größere Gruppe von Geräten anwenden.

> Bei Android 14.x-Geräten, die bei einer Ivanti Neurons for MDM-Version vor 94 registriert sind, wird der Konfigurationsstatus mit "Installation ausstehend" angezeigt. Wenn Sie ein Upgrade von Ivanti Neurons for MDM auf Version 94 durchführen, ohne die WLAN-Konfiguration zu bearbeiten, verbleibt der Konfigurationsstatus bei "Installation ausstehend". Sie müssen zuerst das Domänenfeld für EAP_PEAP aktivieren und die Domäne sowie die Zertifikate in der Konfiguration aktualisieren, damit der Status in "Installiert" wechselt.

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Wählen Sie die **WLAN**-Konfiguration.
3. Geben Sie einen **Namen** für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Konfigurieren Sie die WLAN-Einstellungen gemäß den folgenden Beschreibungen.
6. Klicken Sie auf **Weiter**.
7. (Nur macOS) Wählen Sie auf der Seite „Verteilen“ eine der folgenden Verteilungsoptionen aus:
    - Gerätekanal - Die Konfiguration gilt für alle Benutzer eines Geräts. Dies ist die typische Option.
    - Benutzerkanal - Die Konfiguration gilt nur für den aktuell auf einem Gerät registrierten Benutzer.
8. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
9. Klicken Sie auf **Fertig**.

In der folgenden Tabelle sind die WLAN-Einstellungen aufgeführt:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Service Set Identifier (SSID)	Geben Sie den Namen des Wireless-Netzwerks ein, auf das diese Einstellungen zutreffen. In diesem Feld ist Groß- und Kleinschreibung zu beachten.
Automatisch beitreten	Wählen Sie diese Option, wenn die Geräte automatisch an das entsprechende WLAN-Netzwerk angeschlossen werden. Wenn diese Option nicht ausgewählt ist, muss der Benutzer auf dem Geräts auf den Namen des Netzwerks tippen, damit das Geräts an das Netzwerk angeschlossen wird.
Verborgenes Netzwerk	Wählen Sie diese Option, wenn es sich bei dem Netzwerkzugriff nicht um Broadcast handelt.
Firmeneigene Netzwerkerkennung deaktivieren (iOS 10+)	Administratoren können den firmeneigenen Bypassmodus für WLANs aktivieren oder deaktivieren. Wenn Apple erkennt, dass ein firmeneigenes Portal vorhanden ist, öffnet es einen Anmeldebildschirm zur Abfrage der Zugangsdaten. Sie können die Erkennung firmeneigener Portale deaktivieren; in diesem Fall muss der Benutzer manuell einen Webbrowser starten, der die Portalanmeldung des firmeneigenen Netzwerks auslöst. Diese neue Einstellung ist zweckmäßig, wenn ein firmeneigenes ISE-Portal die Einblendung des Anmeldebildschirms verhindert, so dass die Benutzer irrtümlich der Ansicht sind, ihre nicht verbundenen Geräte seien mit dem Internet verbunden.
Proxy-Konfiguration	Wählen Sie **Manuell** oder **Automatisch** zur Konfiguration eines Proxy-Servers. Wenn Sie „**Manuell**“ wählen, sind die folgenden zusätzlichen Felder verfügbar: • **Server und Port**: Geben Sie die Netzwerkadresse und die Portnummer für den Proxy-Server ein.* • **Authentifizierung**: Geben Sie einen gültigen Benutzernamen ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert.* • **Passwort**: Geben Sie ein gültiges Passwort ein, wenn die Herstellung einer Verbindung mit dem Proxy-Server dies erfordert. Um den hinzugefügten Hostnamen zu entfernen, klicken Sie auf das „Minus“-Symbol. Wenn Sie „**Automatisch**“ wählen, ist das folgende zusätzliche Feld verfügbar: • **URL des Proxy-Servers**: Geben Sie die vollqualifizierte URL des Proxy-Servers ein.
Sicherheitstyp	Bestimmen Sie die für den Netzwerkzugriff erforderliche Sicherheitsmethode: • Beliebig (Freizeit) • Beliebig (Arbeit) • WEP • WEP für Unternehmen • WPA • WPA Enterprise

Einstellung	So gehen Sie vor
	• WPA2 • WPA2 Enterprise • WPA3 • WPA3 Enterprise WPA3/WPA3 Enterprise ist für iOS 13+ verfügbar. Windows unterstützt WPA, WPA Enterprise, WPA2 und WPA2 Enterprise.

WEP, WPA/WPA2/WPA3, beliebige (persönliche) Einstellungen

Einstellung	So gehen Sie vor
Passwort	(Optional) Geben Sie das Passwort für den Zugriff auf dieses Netzwerk ein. Ansonsten wird der Benutzer zur Eingabe eines Passworts für den Netzwerkzugriff aufgefordert.

WEP Enterprise, WPA/WPA2/WPA3 Enterprise, beliebige (persönliche) Einstellungen

Einstellung	So gehen Sie vor
Protokolle	
Akzeptierte EAP-Typen	Bestimmen Sie die EAP-Typen, die für den Zugriff auf dieses Netzwerk verwendet werden können: • TLS • TTLS - Wählen Sie im Feld „Innere Identität“ eines der Authentifizierungsprotokolle aus, z. B. OS Default, PAP, CHAP, MSCHAP, MSCHAPv2 und EAP. • PEAP • LEAP (wird nicht für Geräte unterstützt, die über AMAPI registriert wurden) • EAP-SIM • EAP-AKA • EAP-FAST (wird nicht für Geräte unterstützt, die über AMAPI registriert wurden)
EAP-FAST	Wählen Sie die Option „EAP-FAST“ zur Definition von Authentifizierungsverfahren: • **PAC verwenden:** Wählen Sie diese Option, um eine Proxy Auto-Config (PAC) zu verwenden. • **PAC zur Verfügung stellen:** Wählen Sie diese Option, um zuzulassen, dass eine PAC zur Verfügung gestellt wird. Ansonsten kann nur eine bereits auf dem Geräts zur Verfügung gestellte PAC verwendet werden. Diese Option ist nur verfügbar, wenn Sie „PAC verwenden“ ausgewählt haben. • **PAC anonym zur Verfügung stellen:** Wählen Sie diese Option, um zuzulassen, dass eine PAC ohne Authentifizierung des Servers zur Verfügung gestellt wird. Die Option ist nur verfügbar, wenn Sie „PAC zur Verfügung stellen“ ausgewählt haben
Authentifizierung	
Benutzername Für jede Verbindung ein Passwort verwenden	Bestimmen Sie den für den Netzwerkzugriff erforderlichen Benutzernamen. Wenn Sie dieses Feld leer lassen, wird der Benutzer aufgefordert, es auszufüllen. Wählen Sie diese Option, um den Benutzer des Geräts bei jeder Verbindung zur Eingabe eines Passworts aufzufordern. Wenn das Geräts wieder an dasselbe Netzwerk angeschlossen wird, wird der Benutzer zur erneuten Authentifizierung aufgefordert, um den Anschluss an das Netzwerk zu ermöglichen. Diese Option wird für AMAPI-registrierte Geräte nicht unterstützt.
Passwort Identitätszertifikat Authentifizierungszertifikat (nur für Windows-Geräte verfügbar)	(Optional) Geben Sie das Passwort für den Zugriff auf dieses Netzwerk ein. Ansonsten wird der Benutzer zur Eingabe eines Passworts für den Netzwerkzugriff aufgefordert. (Optional) Wählen Sie das Zertifikat, das als Identitätsnachweis verwendet werden soll. Die Identitätszertifikat-Konfiguration bestimmt jedes verfügbare Identitätszertifikat. Wählen Sie einen der folgenden drei Zertifizierungsspeicher aus, um ein Zertifikat auszuwählen und eine Verbindung zu einem WLAN-Netzwerk herzustellen: • Computer oder Benutzer: Wenn diese Option ausgewählt und der Benutzer nicht angemeldet ist, wird das Authentifizierungszertifikat aus dem Computerspeicher abgerufen. Wenn der Benutzer angemeldet ist, wird das jeweilige Zertifikat aus dem Benutzerspeicher abgerufen. • Computer: Wenn diese Option ausgewählt ist, wird das Authentifizierungszertifikat aus dem Computerspeicher abgerufen.

Einstellung	So gehen Sie vor
	• Benutzer: Wenn diese Option ausgewählt ist, wird das Authentifizierungszertifikat aus dem Benutzerspeicher abgerufen. Die Option "Benutzer" ist standardmäßig ausgewählt.
Äußere Identität	(Optional) TLS, TTLS, PEAP und EAP-FAST: Wählen Sie diese Option aus, um es Gerätebenutzern zu ermöglichen, ihre Identität zu verbergen. Der richtige Name des Benutzers wird nur in dem verschlüsselten Tunnel angezeigt. Diese Option kann die Sicherheit erhöhen, da ein Angreifer den Namen des authentifizierenden Benutzers nicht als Klartext erkennen kann.
Domäne	Wird unterstützt, wenn der EAP-Typ auf TLS oder TTLS lautet.
Vertrauensstatus	
Vertrauenswürdige Zertifikate (nicht für AMAPI-registrierte Geräte unterstützt)	Markieren Sie die jeweiligen Kontrollkästchen, um mehrere Zertifikate aus der Liste auszuwählen.
Vertrauenswürdige Serverzertifikatsnamen	Klicken Sie auf **+Hinzufügen**, um die Namen von einem oder mehreren vertrauenswürdigen Serverzertifikaten einzugeben. (Optional) Wählen Sie Vertrauensstatus - Ausnahmen zulassen, damit der Benutzer in einem Dialogfenster Entscheidungen zum Vertrauensstatus treffen kann.

iOS, macOS und visionOS

Einstellung	So gehen Sie vor
Alle Versionen	
Netzwerkart	Wählen Sie diese Option die Behandlung dieses Netzwerks als: • Standardnetzwerk • Legacy Hotspot-Netzwerk • Passpoint-Netzwerk
PAC-Fallback für Proxy zulässig	(Optional) Ermöglicht den direkten Anschluss des Geräts an den Zielort, falls die PAC-Datei nicht erreichbar ist.
Setup-Modi (optional)	Ein Array von Strings, mit dem Typ des Verbindungsmodus, der angehängt werden soll. • System: WLAN wird verbunden, bevor sich der Benutzer am Gerät anmeldet. • Anmeldefenster: Das WLAN ist verfügbar, sobald sich der Benutzer am Gerät angemeldet hat. Derzeit können Einrichtungsmodi nur verwendet werden, wenn die System- und Anmeldefenster-Modi aktiviert sind.
Passpoint-Einstellungen	Die Einstellungen in diesem Abschnitt werden angezeigt, wenn Sie als Netzwerkart "Passpoint" ausgewählt haben.
Domänenname	Geben Sie den Domainnamen ein, den Sie für die Passpoint-Freigabe verwenden wollen.
Mit Roaming-Partner Passpoint Networks verbinden	(Optional) Wählen Sie diese Option, um Verbindungen zu Roaming-Dienstanbietern zuzulassen.
Roaming Consortium Organization-IDs	(Optional) Geben Sie die Kennungen ein, die das IEEE den von diesem WLAN-Profil unterstützten Einheiten zugewiesen hat.
Netzwerkzugriffs-ID-Realm-Namen	(Optional:) Geben Sie die Netzwerkzugriffs-ID-Realm-Namen für die Passpoint-Freigabe ein.
MCC- und MNC-Paar	(Optional:) Geben Sie die Mobile Country Code (MCC)-/Mobile Network Code (MNC)-Paare für die Passpoint-Freigabe ein. Jede Zeichenfolge muss aus genau sechs Zeichen bestehen.
Angezeigter Bedienername	(Optional) Geben Sie den anzuzeigenden Namen des Netzbetreibers ein.
Cisco QoS	Die Einstellungen in diesem Abschnitt beziehen sich auf die Konfiguration der Cisco Fast Lane. Als Einstellungen werden beispielsweise die Aufnahme von Apps in die Whitelist mit einer L2- oder L3-Markierung

Einstellung	So gehen Sie vor
Fast Lane	angeboten, außerdem können Sie in der Whitelist den Audio- und Videotraffic integrierter Audio- und Videodienste wie FaceTime und WLAN Calling eintragen.
QoS-Markierung beschränken	Wenn Sie diese Option nicht aktivieren, nutzen alle Apps die L2- und L3-Markierung, wenn das Netzwerk Cisco QoS Fast Lane unterstützt. Wenn Sie diese Option aktivieren, fügen Sie mit den Einstellungen unter **App wählen** die Apps hinzu, für die Sie die L2- und L3-Markierung nutzen wollen. Alle nicht ausgewählten Apps nutzen die L2- und L3-Markierungen nicht.
QoS-Markierung aktivieren	Deaktiviert die L3-Markierung und verwendet nur die L2-Markierung für den im WLAN versendeten Traffic. Wenn diese Option nicht ausgewählt ist, geht das System davon aus, dass das WLAN nicht zum Cisco QoS Fast Lane Netzwerk gehört.
Audio-/Videoanrufe in der Apple Whitelist eintragen	Gibt an, ob der Audio- und Videotraffic integrierter Audio- und Videodienste in der Whitelist eingetragen werden soll, beispielsweise FaceTime und WLAN Calling.
Apps wählen **iOS 10+** **Cisco QoS Fast Lane**	Hiermit fügen Sie die Apps für eine L2- und L3-Markierung hinzu. Alle nicht ausgewählten Apps verwenden die L2- und L3-Markierung nicht. Die Einstellungen in diesem Abschnitt beziehen sich auf die Konfiguration der Cisco Fast Lane. Als Einstellungen werden beispielsweise die Aufnahme von Apps in die Whitelist mit einer L2- oder L3-Markierung angeboten, außerdem können Sie in der Whitelist den Audio- und Videotraffic integrierter Audio- und Videodienste wie FaceTime und WLAN Calling eintragen.
QoS-Markierung beschränken QoS-Markierung aktivieren	Wenn Sie diese Option nicht aktivieren, nutzen alle Apps die L2- und L3-Markierung, wenn das Netzwerk Cisco QoS Fast Lane unterstützt. Wenn Sie diese Option aktivieren, fügen Sie mit den Einstellungen unter **App wählen** die Apps hinzu, für die Sie die L2- und L3-Markierung nutzen wollen. Alle nicht ausgewählten Apps nutzen die L2- und L3-Markierungen nicht. Deaktiviert die L3-Markierung und verwendet nur die L2-Markierung für den im WLAN versendeten Traffic. Wenn diese Option nicht ausgewählt ist, geht das System davon aus, dass das WLAN nicht zum Cisco QoS Fast Lane Netzwerk gehört.
Audio-/Videoanrufe in der Apple Whitelist eintragen	Gibt an, ob der Audio- und Videotraffic integrierter Audio- und Videodienste in der Whitelist eingetragen werden soll, beispielsweise FaceTime und WLAN Calling.
Apps wählen **iOS 10.3+ überwacht**	Hiermit fügen Sie die Apps für eine L2- und L3-Markierung hinzu. Alle nicht ausgewählten Apps verwenden die L2- und L3-Markierung nicht.

Einstellung	So gehen Sie vor
WLAN-Whitelisting aktivieren **iOS 14.0+ und macOS 15.0+**	Legen Sie fest, mit welchen WLANs das Gerät eine Verbindung aufbauen darf. Wenn mehrere WLAN-Konfigurationen existieren, wird die strengste Konfiguration verwendet.
MAC-Adressen-Randomisierung deaktivieren	In iOS 14.0+ und macOS 15.0+ hat Apple das Standardverhalten für ein Gerät, das seine WLAN-MAC-Adresse meldet, so geändert, dass für neue Verbindungen statt der tatsächlichen WLAN-MAC-Adresse des Geräts eine zufällige Adresse gemeldet wird. Diese Funktion kann bei Unternehmen, die firmeneigene Portale verwenden oder die MAC-Adressen filtern, zu unerwartetem Verhalten führen. Administratoren können die **MAC-Adress-Randomisierung deaktivieren**, wenn sie für das betreffende WLAN die WLAN-Konfiguration bearbeiten und diese Option einschalten (standardmäßig "false"). Dies führt dazu, dass die WLAN-Konfiguration erneut an alle Geräte übertragen wird. Diese Option zeigt in den Geräteeinstellungen eine Datenschutzwarnung mit dem Hinweis, dass das Netzwerk den Datenschutz reduziert hat. Ein Gerätebenutzer kann diese Option immer noch manuell über die Einstellungen seines Geräts ein- oder ausschalten.
Android 11+	
MAC-Adressen-Randomisierung	• Deaktiviert: WLAN wird verbunden, bevor sich der Benutzer am Gerät anmeldet. • Aktiviert – Automatisch: WLAN ist verfügbar, sobald sich der Benutzer am Gerät angemeldet hat. • Aktiviert – Nicht persistent • Aktiviert – Persistent

Variables.htm Geben Sie „$“ ein, um eine Liste mit unterstützten Variablen anzuzeigen, sofern diese für dieses Feld verfügbar ist.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.7. Konfiguration des Mobilfunknetzes

Dieser Abschnitt enthält die folgenden Themen:

- APN-Konfiguration
- Mobilfunk
- Cellular Private Network Configuration.htmKonfiguration "Privates Mobilfunknetz"
- Konfiguration für iOS Telecom-Voreinstellungen
- eSIM-Konfiguration

10.10.7.1. APN-Konfiguration

Eine APN-Konfiguration richtet den Mobilfunk-Zugangspunktnamen für das Gerät ein. Für iOS 7 ist die **Mobilfunk-Konfiguration** zu verwenden.

APN-Einstellungen

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Zugangspunktname	Geben Sie den Namen für den entsprechenden Zugangspunkt ein. Im Allgemeinen wird der Name von dem Dienstanbieter bestimmt.
Benutzername für den Zugangspunkt	Geben Sie den Namen eines für diesen Zugriffspunkt autorisierten Benutzers ein.*
Passwort für Zugangspunkt	Geben Sie das entsprechende Passwort für den eingegebenen Benutzernamen ein.
Proxy-Server und Port	Geben Sie die IP-Adresse oder URL und die Portnummer des APN-Proxy ein.
XLAT464 aktivieren	Aktivieren Sie das Kontrollkästchen, um den Zugriffspunktnamen (APN) zu aktivieren. Diese Option stellt IPv4-Services auf einem Nur-IPv6-Netzwerk bereit.

Variables.htm Geben Sie „$“ ein, um eine Liste mit unterstützten Variablen anzuzeigen, sofern diese für dieses Feld verfügbar ist.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.7.2. Mobilfunk

Gilt für: iOS 7.0+ und watchOS 10.0+

Dieser Abschnitt enthält die folgenden Themen:

- **Mobilfunkeinstellungen für Standard-APN**
- **Mobilfunkeinstellungen für Daten-APNs**
- **Kontrolle des Mobilfunkzugriffs beim Roaming**
- **Mobilfunkzugriff kontrollieren**

Eine Mobilfunk-Konfiguration legt das Mobilfunkprofil für ein Gerät fest. Konfiguriert Mobilfunknetzeinstellungen auf Geräten ab iOS 7.0 oder ab watchOS 10.0. Manche Unternehmen haben Verträge mit ihren Mobilfunkbetreibern, die ihnen Zugang auf einen eindeutigen Zugriffspunktnamen (APN) für den Remote-Netzwerkzugriff oder für spezielle Abrechnungspläne gewähren. Konsultieren Sie für die Konfigurationsparameter Ihren Mobilfunkbetreiber.

- Es kann immer nur ein Mobilfunkprofil installiert werden.
- Ein Mobilfunkprofil kann nicht installiert werden, wenn bereits ein **APN-Profil** installiert ist.

Sie können die Mobilfunkeinstellungen für folgende APN-Typen in dem Dropdown-Feld **Konfigurierte APN-Typen** konfigurieren:

- Standard- und Daten-APNs
- Standard-APNs
- Daten-APNs

Geben Sie für alle Konfigurationen einen Namen ein, der die Konfiguration identifiziert, sowie ggf. eine Beschreibung.

Mobilfunkeinstellungen für Standard-APN

Standard-APN-Einstellungen	So gehen Sie vor
APN-Name	Geben Sie den Namen für den entsprechenden Zugangspunkt ein. Im Allgemeinen wird der Name von dem Dienstanbieter bestimmt.
APN-Authentifizierungsart	(Optional): Klicken Sie auf eine der folgenden Optionen: • CHAP (Challenge-Handshake-Authentifizierungsprotokoll) • PAP (Passwortauthentifizierungsprotokoll)
Benutzername	(Optional) Geben Sie einen zur Authentifizierung zu verwendenden Benutzernamen ein.
Passwort	(Optional) Geben Sie ein zur Authentifizierung zu verwendendes Passwort ein.

Mobilfunkeinstellungen für Daten-APNs

Daten-APN-Einstellungen	So gehen Sie vor
APN-Name	Geben Sie den Namen für den entsprechenden Zugangspunkt ein. Im Allgemeinen wird der Name von dem Dienstanbieter bestimmt.
APN-Authentifizierungsart	(Optional): Klicken Sie auf eine der folgenden Optionen: • CHAP (Challenge-Handshake-Authentifizierungsprotokoll) • PAP (Passwortauthentifizierungsprotokoll)
Benutzername	(Optional) Geben Sie einen zur Authentifizierung zu verwendenden Benutzernamen ein.
Passwort	(Optional) Geben Sie ein zur Authentifizierung zu verwendendes Passwort ein.
Proxy-Server	Definieren Sie den Proxyserver.
Proxy-Server-Port	Definieren Sie den Port des Proxyservers.
10.3+	
Zugelassene Protokollmaske	Wählen Sie IPv4, IPv6 oder beides.
Zugelassene Protokollmaske beim Inland-Roaming	Wählen Sie IPv4, IPv6 oder beides.
Zugelassene Protokollmaske beim Roaming	Wählen Sie IPv4, IPv6 oder beides.

Mobilfunkzugriff beim Roaming kontrollieren

Sie können den Zugriff auf Mobilfunkdaten für einige oder alle verwalteten Apps beschränken, wenn das Gerät sich im Roaming-Status befindet.

Verfahren

1. Wechseln Sie im Hauptnavigationsmenü von Ivanti Neurons for MDM zur Registerkarte **Konfigurationen**.
2. Klicken Sie auf **+Add**
3. Geben Sie **Netzwerk** in das Suchfeld ein und klicken Sie dann auf die Konfiguration **Netzwerknutzung**.
4. Klicken Sie in das Kontrollkästchen **Für alle verwalteten Anwendungen verweigern**, um zu verhindern, dass verwaltete Apps beim Roaming oder grundsätzlich auf Mobilfunkdaten zugreifen.
5. Lassen Sie das Kontrollkästchen deaktiviert, wenn Sie mit Name oder Bundle-ID festlegen wollen, welche verwalteten Apps keine Mobilfunkdaten empfangen dürfen.
6. Suchen Sie mit den Pulldown-Menüs in dem Feld „Apps“ nach Name oder Bundle-ID einer App zu suchen.

Mobilfunkzugriff kontrollieren

Sie können den Zugriff aller oder einiger verwalteter Apps auf Mobilfunkdaten zu jedem beliebigen Zeitpunkt beschränken. Die Apps können eingeschränkt trotzdem verwendet werden, haben aber keinen Zugriff auf Mobilfunkdaten.

Verfahren

1. Wechseln Sie im Hauptnavigationsmenü von Ivanti Neurons for MDM zur Registerkarte **Konfigurationen**.

2. Klicken Sie auf **+Add**
3. Geben Sie **Netzwerk** in das Suchfeld ein und klicken Sie dann auf die Konfiguration **Netzwerknutzung**.
4. Aktivieren Sie das Kontrollkästchen **Für alle verwalteten Apps verweigern**, um zu verhindern, dass verwaltete Apps zu einem beliebigen Zeitpunkt auf Mobilfunkdaten zugreifen.
5. Sie können das Kontrollkästchen deaktiviert lassen, wenn Sie festlegen wollen, welche verwalteten Apps keine Mobilfunkdaten empfangen dürfen.
6. Suchen Sie mit den Pulldown-Menüs in dem Feld „Apps“ nach Name oder Bundle-ID einer App zu suchen.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.7.3. Konfiguration "Privates Mobilfunknetz"

Ivanti Neurons for MDM ermöglicht der Payload "Privates Mobilfunknetz" das Bereitstellen von Geräteinformationen zu privaten Netzwerkbereitstellungen, darunter geografischer Standort, Präferenz gegenüber WLAN und Netzwerkbereitstellungstyp.

Gilt für:

iOS 17.0 bis zur zuletzt freigegebenen Version, die von Ivanti Neurons for MDM unterstützt wird.

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Privates Mobilfunknetz** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie die Einstellungen für das **private Mobilfunknetz** gemäß der folgenden Tabelle:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Mobile Daten bevorzugt	Markieren Sie das Kontrollkästchen, um anstelle von WLAN mobile Daten zu aktivieren und zu verwenden.
NR-Standalone	Markieren Sie das Kontrollkästchen, wenn das Mobilfunk-Datennetzwerk über NR-5G-Standalone verfügt.
Name des Datensets	Geben Sie den Namen des Datensets an, der mit dieser Konfiguration bezeichnet wird.
Versionsnummer	Geben Sie die Versionsnummer für das Datenset zum Verfolgen der Systemupdates an.
GeoFences	Geben Sie Breitengrad, Längengrad und Radius für jede Geo-ID an, um ein privates Netzwerk in einer geografischen Region bereitzustellen. Sie können eine Liste mit bis zu 1.000 Geofences für private Netzwerke erstellen.

4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
5. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Privates Mobilfunknetz** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
6. Klicken Sie auf **Fertig**.

10.10.7.4. Konfiguration für iOS Telecom-Voreinstellungen

Eine Konfiguration für iOS Telecom-Voreinstellungen bestimmt die Standardwerte für Roaming- und Hotspot-Einschränkungen.

iOS Telecom-Voreinstellungen

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Geräten die Verwendung von Sprachdiensten beim Roaming erlauben	Wählen Sie diese Option zur Aktivierung von Sprach-Roaming. Verfügbarkeit von Sprach-Roaming hängt vom Betreiber ab.
Geräten die Verwendung von Datendiensten beim Roaming erlauben	Wählen Sie diese Option zur Aktivierung von Daten-Roaming. Beachten Sie, dass durch die Aktivierung von Daten-Roaming auch Sprach-Roaming auf dem Gerät aktiviert wird.
Aktivierung eines persönlichen Hotspots für Benutzer zulassen	Wählen Sie diese Option zur Aktivierung eines persönlichen Hotspots. Die Verfügbarkeit dieser Funktion hängt vom Betreiber ab.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.7.5. Erweiterte 5G-Network-Slicing-Konfiguration

Ivanti Neurons for MDM bietet eine erweiterte 5G-Network-Slicing-Konfiguration zum Einrichten von 5G Network Slices für Android, mit der die Betreiber mobiler Netzwerke dedizierte 5G-Netzwerksegmente, so genannte Slices, zuteilen können. So lassen sich unterschiedliche Anwendungen mit ähnlichen Anforderungen, wie niedrige Latenz oder hohe Bandbreite, in einer Slice zusammenfassen und Netzwerkressourcen optimieren. Dadurch können MDM-Administratoren und Netzwerkanbieter die Slices für eine verbesserte App-Leistung direkt verwalten.

Wichtigste Funktionen

1. **Dediziertes Netzwerk**: Anstatt alle Anwendungen in einem einzigen Netzwerksegment unterzubringen, steht den Apps mit Network Slicing eine eigene Slice zur Verfügung, die auf ihre spezifischen Anforderungen zugeschnitten ist.

2. **Anpassung**: Administratoren können die Zuweisung der Apps zu bestimmten Netzwerksegmenten je nach Anforderung konfigurieren. So lassen sich beispielsweise eine geringe Latenz für Apps mit Echtzeitkommunikation oder eine hohe Bandbreite für Streamingdienste wie YouTube sicherstellen. Eine Slice für leistungsstarkes Gaming beispielsweise ist eher auf eine geringe Latenz ausgerichtet, während eine Slice für das Streamen von Medien für hohe Bandbreite optimiert ist.

3. **Partnerbeteiligung**: Diese Funktion erfordert oft die Zusammenarbeit mit Netzwerkanbietern. Diese definieren die Slices und stellen den MDM-Administratoren eine Liste der Slices mit der jeweiligen Bestimmung zur Verfügung.

Erstellen einer erweiterten 5G-Network-Slicing-Konfiguration

Verfahren

1. **Konfiguration hinzufügen**

- Wechseln Sie zu **Konfigurationen >> +Hinzufügen.** Die Seite **Konfiguration hinzufügen** wird angezeigt.
- Geben Sie in die Suchleiste den Begriff **Erweitertes Network Slicing** ein, um erweitertes Network Slicing zu konfigurieren. Die Seite **Erweiterte 5G-Network-Slicing-Konfiguration erstellen** wird angezeigt.
- Klicken Sie auf **+Beschreibung hinzufügen**, um eine Beschreibung für die Konfiguration einzugeben.

2. **Anwendung konfigurieren**

- Geben Sie unter **Konfigurations-Setup >> App-Katalog** den gewünschten Anwendungsnamen ein.
- Klicken Sie auf **Manuell hinzufügen**, falls die Anwendung nicht im Play Store oder App Store verfügbar ist.
- Geben Sie die **Paket-ID** ein und wählen Sie die gewünschte **Network Slice** aus dem Dropdownmenü aus.
- Wählen Sie die Slice aus dem Dropdownmenü **Slice auswählen** aus.
- Klicken Sie auf **Hinzufügen**. Die Anwendung wird jetzt bei **Network Slices konfigurieren** unter der ausgewählten Network Slice angezeigt.
- Klicken Sie zum Entfernen einer Anwendung im Abschnitt **Network Slice konfigurieren** auf **Entfernen**.

3. **Konfiguration verteilen**

- Klicken Sie auf **Weiter**, aktivieren oder deaktivieren Sie das Kontrollkästchen **Diese Konfiguration aktivieren** und wählen Sie eine Verteilungsoption (Alle Geräte, Keine Geräte oder Benutzerdefiniert).

- Klicken Sie auf **Fertig**, um die Konfiguration abzuschließen.

Erweiterte 5G-Network-Slicing-Konfiguration für Sperre & Kiosk

Mit einer erweiterten 5G-Network-Slicing-Konfiguration können Sie Geräte für einen eingeschränkten Betrieb konfigurieren und dadurch sicherstellen, dass Benutzer nur auf bestimmte Anwendungen und Einstellungen zugreifen können.

Unter den folgenden Sperren befindet sich das Kontrollkästchen **5G Network Slicing aktivieren**:

- **Arbeitsprofil** – Auf Mitarbeitergeräten mit einem Arbeitsprofil, das mithilfe von Android Enterprise Version 12.0 konfiguriert wurde, befindet sich das Kontrollkästchen "5G Network Slicing aktivieren" unter **Konfigurations-Setup > Arbeitsprofil-Sperreinstellungen**.
- **Verwaltetes Gerät mit Arbeitsprofil/Arbeitsprofil auf firmeneigenen Geräten** – Unter "Verwaltetes Gerät mit Arbeitsprofil/Arbeitsprofil auf firmeneigenen Geräten" befindet sich das Kontrollkästchen "5G Network Slicing aktivieren".

Dies ist eine Legacy-Einstellung, mit der Geräte die Funktion "5G Network Slicing" nutzen können. Sie ist wie folgt mit der neuen Konfiguration "Erweitertes 5G Network Slicing" korreliert:

Wird eine der obigen Sperren auf ein Gerät angewendet, während die Option *5G Network Slicing aktivieren* **nicht** ausgewählt ist, schlägt die Konfiguration *Erweitertes 5G Network Slicing* fehl und es wird einen Fehler ausgegeben.

Beispiele

- **Fall 1**: Wird die Gerätesperre nicht verteilt, während die erweiterte Network Slicing-Konfiguration verteilt wird, wird die erweiterte Konfiguration aktiviert.
- **Fall 2**: Wird die Gerätesperre verteilt, während das 5G-Kontrollkästchen deaktiviert (false) ist, gibt die erweiterte 5G-Netzwerkkonfiguration einen Fehler aus.
- **Fall 3**: Wird zuerst erweitertes Network Slicing und dann die Gerätesperre mit aktiviertem Kontrollkästchen verteilt, funktioniert die erweiterte Network Slicing-Konfiguration weiterhin, andernfalls schlägt sie fehl.

Konfigurationsdetails:

- Falls die Gerätesperre verteilt und die erweiterte Network Slicing-Konfiguration via Push übertragen/verteilt wird, müssen die Benutzer darauf achten, dass das Kontrollkästchen "5G Network Slicing aktivieren" markiert ist, um Fehler zu verhindern.
- Ist das Kontrollkästchen nicht aktiviert und die Konfiguration wird gesendet, wird auf dem Gerät ein Fehler ausgegeben.

10.10.7.6. eSIM-Konfiguration

Die eSIM-Konfiguration konfiguriert das Mobilfunknetz auf den Geräten mit dem Befehl RefreshCellularPlans. Administratoren müssen die URL des eSIM-Betreibers erhalten, bevor sie das Mobilfunknetz dem Gerät zuordnen.

Gilt für: Android 15+, iOS, iPadOS und Windows 11

Verfahren für Geräte mit Android 15+

1. Wechseln Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Geben Sie eSIM in das Suchfeld ein, und klicken Sie dann auf die Konfiguration **eSIM**.
3. Geben Sie einen Namen und eine Beschreibung der Konfiguration ein.
4. Wählen Sie in der Liste **Plattform** die Option **Android** aus.
5. Geben Sie im Abschnitt **Konfigurations-Setup** die **Provider-URL** ein.
6. **Automatisch aktivieren** – Wählen Sie diese Option aus, um das eSIM-Profil herunterzuladen und automatisch auf dem Gerät zu aktivieren. Wenn diese Option nicht ausgewählt ist, wird das eSIM-Profil heruntergeladen, jedoch nicht automatisch auf dem Gerät aktiviert.

> Diese Option ist für Geräte im Arbeitsprofilmodus NICHT verfügbar.

7. Wählen und verteilen Sie die Konfiguration unter Verwendung einer der folgenden Verteilungsoptionen:
   - Alle Geräte
   - Keine Geräte (Standard)
   - Anpassbar
8. Klicken Sie auf **Fertig**.

EID für Geräte mit Android 13+

Die Option **EID anfordern** ist jetzt bei den Gerätedetails und auf der Seite "Geräteliste" verfügbar. Diese Option wird nur für eSIM-kompatible Geräte in den Modi Arbeitsprofil, vom Unternehmen verwaltetes Gerät und Arbeitsprofil auf firmeneigenem Gerät unterstützt. Wenn ein Gerät registriert ist, wird die EID automatisch für das registrierte Gerät ausgewählt und auf der Seite "Gerätedetails" angezeigt. Anderenfalls wird dieses Feld aktiviert und Sie können die EID anfordern, indem Sie auf **EID anfordern** klicken. Sie können die EID auch über die Option **In CSV exportieren** der Listenseite "Geräte" exportieren.

> Auf der Seite **Gerätedetails** ist die Option **EID anfordern** für Geräte mit Android 13+ und mit Ivanti Go R122 oder einer neueren Version verfügbar.

eSIM-Datentarif beibehalten (gilt für iOS 11+ und Android 15.0+): Wenn Sie versuchen, ein Gerät, das mit einer eSIM-Konfiguration registriert wurde, vollständig zu löschen, bietet die Aktion **Komplettlöschung des Geräts durchführen** eine zusätzliche Option, um den Datenplan beizubehalten. Wenn Sie **eSIM-Datenplan beibehalten** auswählen (gilt für iOS 11+ und Android 15.0+) und auf **Komplettlöschung durchführen** klicken, wird der vorhandene eSIM-Datenplan beibehalten, während alle anderen Daten auf dem Gerät gelöscht werden. Sie können auf diese Option über die Seite **Gerätedetails** zugreifen oder indem Sie das Gerät auswählen, das Menü **Aktionen** öffnen und dann auf **Komplettlöschung durchführen** klicken.

Verfahren für iOS- und iPadOS-Geräte

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.

2. Geben Sie eSIM in das Suchfeld ein, und klicken Sie dann auf die Konfiguration eSIM.
3. Geben Sie einen Namen und eine Beschreibung der Konfiguration ein.
4. Wählen Sie **iOS/iPadOS** aus.
5. Geben Sie die URL des Anbieters ein.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Option Diese Konfiguration aktivieren.
8. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
9. Klicken Sie auf Fertig.

Verfahren für Windows 11-Geräte

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Geben Sie eSIM in das Suchfeld ein, und klicken Sie dann auf die Konfiguration eSIM.
3. Geben Sie einen Namen und eine Beschreibung der Konfiguration ein.
4. Klicken Sie im Abschnitt "Betriebssystem wählen" auf **Windows**.
5. Geben Sie im Abschnitt "Konfigurations-Setup" die Provider-URL (im FQDN-Format) in das Textfeld für den Servernamen ein.
    - Ist Ermittlungsserver – Aktivieren Sie diese Option, um den Server als ermittelbar festzulegen.
    - Automatisch aktivieren – Wählen Sie diese Option, um das Profil nach dem Herunterladen auf dem Gerät zu aktivieren.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Option Diese Konfiguration aktivieren.
8. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
9. Klicken Sie auf **Fertig**.

eSIM auf Werkseinstellungen zurücksetzen (nur für Windows 11-Geräte)

Diese Option ist bei allen Geräten im Abschnitt "Gerätedetails" verfügbar. Durch Klicken auf diese Option werden alle auf das Gerät heruntergeladenen eSIM-Profile gelöscht.

Wichtige Hinweise – Gilt nur für die eSIM-Konfiguration unter Windows

- Wenn ein Gerät registriert wird, zeigt der Abschnitt **Gerätedetails** unter **ESIM-fähig** nun an, ob das Gerät eSIM unterstützt. Bei eSIM-fähigen Geräten werden die jeweiligen eSIM-Bezeichnerdaten auch unter **ESIM-Bezeichner** angezeigt.
- Wenn ein mit Ivanti Neurons for MDM registriertes Gerät komplett gelöscht und neu registriert wird, sollte der alte Datensatz des Geräts (mit dem Status "Komplettlöschung durchgeführt") von der Seite "Geräte" gelöscht werden, um Bereitstellungsprobleme mit der eSIM-Konfiguration auf dem neu registrierten Gerät zu vermeiden.

- Das erneute Pushen derselben Konfiguration auf ein Gerät, das die Profile bereits heruntergeladen hat, bewirkt, dass die Profile nicht erneut heruntergeladen werden können. Wenn das Gerät die Profile von Neuem herunterladen soll, setzen Sie das eSIM-Modul zuerst auf die Werkseinstellungen zurück und pushen Sie die eSIM-Konfiguration anschließend erneut an das Gerät.
- Wenn eine eSIM-Konfiguration erfolgreich auf einem Gerät bereitgestellt wurde und geplant ist, das Gerät stillzulegen, sollte der Administrator zuerst eine eSIM-Komplettlöschung durchführen, um sicherzustellen, dass die eSIM-Profile vom Gerät gelöscht werden.
- Durch Entfernen der eSIM-Konfiguration wird lediglich die Konfiguration auf dem Gerät gelöscht. Sollten auf dem Gerät eSIM-Profile erkannt, heruntergeladen und aktiviert werden, würden diese solange aktiv bleiben, bis eine eSIM-Komplettlöschung durchgeführt wird.
- Durch eine eSIM-Komplettlöschung werden alle heruntergeladenen eSIM-Profile auf dem Gerät gelöscht. Diejenige eSIM-Konfiguration, die den Status "Installiert" aufweist, bleibt jedoch auf dem Gerät erhalten. Der Administrator muss die Verteilung der eSIM-Konfiguration aufheben, um die Konfiguration auf dem Gerät zu entfernen.

10.10.8. Andere Konfiguration

Dieser Abschnitt enthält die folgenden Themen:

- Konfiguration verknüpfter Domänen
- Konfiguration der Android-Dateiübertragung
- Apple TV-Konfiguration
- AirPlay-Konfiguration
- AirPlay Spiegelung
- Browser-Einstellungen
- Konfiguration des Single-App-Modus für iOS
- iOS-MDM-Profil definieren
- Konfigurieren eines iOS-MDM-Profils
- Content-Caching
- Erstellen einer Android-Tastenkombination
- Einstellungen für den Gerätenamen
- Ethernet-Konfiguration (macOS)
- EMA Server-Integrationskonfiguration
- Gerätehintergrundkonfiguration
- Sperrbildschirm-Nachricht - Konfiguration
- Erstellen der Konfiguration für den Bildschirmschoner
- Bildschirmschoner des Benutzers konfigurieren
- macOS Systemerweiterungskonfiguration
- MAM-Only
- Verwaltete Google Play-Konfiguration
- Einstellungen für den Migrationsassistenten
- Konfiguration "Benachrichtigungen"
- Druckereinstellungen
- Bloatware-Konfiguration entfernen
- Konfiguration der Samsung Mobiltelefon-Einschränkungen
- Single App Mode-Konfiguration
- Startmenü und Taskleiste
- Konfiguration der Systemaktualisierung
- Windows-Updatemanagement
- Zeitplanung von Windows Apps
- Windows BIOS-Konfiguration
- Windows BitLocker
- Windows Kiosk-Konfiguration

- Konfiguration der Windows-Lizenz
- Konfiguration der Empfehlungskadenz für Softwareupdates

10.10.8.1. Konfiguration verknüpfter Domänen

Lizenz: Gold

Die Konfiguration verknüpfter Domänen ist ein Wörterbuch, das Apps den zugehörigen Domänen zuordnet. Verknüpfte Domänen können mit Funktionen wie Extensible AppSSO, universelle Links und Kennwort-AutoFill verwendet werden.

Folgende Einstellungen stehen für verknüpfte Domänen zur Verfügung:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Anwendungsidentifikator	(Erforderlich) Die App-Kennung, mit der die Domänen verknüpft werden sollen.
Zugehörige Domains	(Erforderlich) Die Domänen, die mit der App verknüpft werden sollen. Jede Zeichenfolge weist das Format "dienst.domäne" auf. Bei Domänen sollte es sich um vollständig qualifizierte Hostnamen handeln wie www.beispiel.com.
Direktes Herunterladen aktivieren	Falls wahr, sollten die Daten für diese Domäne direkt und nicht über CDN heruntergeladen werden. Der Berechtigungswert für diese Domäne muss auf "service:domain?mode=managed" gesetzt sein, anderenfalls wird er ignoriert. Verfügbar in macOS 11 und höher. **Voreinstellung**: false

10.10.8.2. Konfiguration der Android-Dateiübertragung

Im Rahmen von Android 11 hat Google umfassende Änderungen am Speicherzugang auf einem Gerät über Apps eingeführt. Diese wirken sich auch darauf aus, wie Unternehmen Dateien an bestimmte Apps auf den betreffenden Geräten senden können. Infolgedessen stehen viele große Unternehmen vor Herausforderungen, wenn es darum geht, Dateien an Geräte und Apps zu verteilen, wenn die Geräte auf Android 11 oder höhere Versionen aktualisiert werden. Jeder Ansatz, der von bestimmten APIs von Hardwareanbietern abhängig ist, schränkt Unternehmen ein, da diese nicht denselben Ansatz für unterschiedliche Geräte unterschiedlicher Hersteller und mit unterschiedlichen Betriebssystemversionen verwenden können.

Ivanti hat eine Lösung für die Dateiübertragung entwickelt, die unabhängig von der Android-Version und dem Hardwareanbieter ist. Die Lösung beruht auf der Standardfunktion *Content-Provider* von Android. *Content-Provider* ermöglicht es der Go-App von Ivanti, einen eindeutigen Speicherort auf dem Gerät für jede über UEM gepushte Datei zu generieren.

Die Konfiguration der Dateiübertragung ist für Android-Geräte im vollständig verwalteten Gerätemodus verfügbar. Mithilfe dieser Konfiguration kann der Administrator eine Option bereitstellen, mit der Dateien auf dem Gerät übertragen werden können, damit sie von verschiedenen zulässigen auf dem Gerät vorhandenen Apps gemeinsam genutzt werden können. Andere Apps können die Dateien zu beliebigen Zwecken verwenden. Mögliche Anwendungsfälle wären etwa das Initiieren einer App-Konfiguration mithilfe von JavaScript oder das Anzeigen von Unternehmensinformationen anhand von PDFs oder Videos. Jede an die Dateiübertragungskonfigurationen von Ivanti hochgeladene Datei wird von Ivanti Go heruntergeladen, wenn sie die zugehörige Konfiguration und die zugeordnete Datei empfängt. Die Datei wird sicher innerhalb von Ivanti Go gespeichert.

Andere Apps können nicht beliebig auf diese Datei zugreifen.

Jede heruntergeladene Datei in der App Sandbox wird durch einen eindeutigen Speicherort referenziert. Dies ist die sogenannte *ContentURI* oder kurz *URI*. In benutzerdefinierten Attributen ist der ContentURI-Wert auf dem Server für jede Datei auf einem Gerät enthalten. Dadurch können Administratoren die Verfügbarkeit einer Datei auf dem Gerät einfacher bestimmen. Sie dienen außerdem der Bildung dynamischer Gerätegruppen und sind erforderlich, um die ContentURI mithilfe der Konfiguration für verwaltete Apps an die Ziel-App zu kommunizieren usw.

> In Bezug auf Apps, die nicht von Ivanti stammen, sollten Administratoren bei den jeweiligen App-Entwicklern prüfen, ob dieser Ansatz unterstützt wird. Dieser wird allgemein als "Verwenden der FileProvider-basierten ContentURI" bezeichnet.

Voraussetzungen:

- Fügen Sie ein neues gerätebasiertes benutzerdefiniertes Attribut hinzu, das für den Vorgang der Dateiübertragung verwendet werden soll. Für jede Dateiübertragungskonfiguration sollte ein eindeutiges benutzerdefiniertes Attribut erstellt werden. Jedes benutzerdefinierte Geräteattribut kann nur die ContentURI (Speicherort der Datei) des Geräts für eine Datei pro Konfiguration speichern.

Verfahren

1. Wechseln Sie zu **Konfigurationen** > **Konfiguration hinzufügen** > **Dateiübertragung**. Die Seite **Konfiguration für Dateiübertragung erstellen** wird geöffnet.
2. Geben Sie einen Namen für die Konfiguration im Kästchen **Name** ein.
3. Geben Sie eine **Beschreibung** für die Konfiguration ein.
4. **Konfigurations-Setup**
   Wählen Sie im Abschnitt **Datei für Übertragung** die zu übertragenden Dateien via Drag&Drop oder mithilfe der Option **Datei**

auswählen aus. Standardmäßig ist die maximale Dateigröße auf 50 MB begrenzt.

5. Wählen Sie (optional) eine oder mehrere der folgenden Optionen für das **Herunterladen auf das Gerät** aus:
   - **Download über ein getaktetes Netzwerk zulassen** – Wählen Sie diese Option aus, um die Datei auch in einem getakteten Netzwerk herunterzuladen.
   - **Aufladen erforderlich** – Wählen Sie diese Option aus, um sicherzustellen, dass das Gerät während des Dateiübertragungsprozesses aufgeladen wird.
   - **Gerät im Leerlauf erforderlich** – Wählen Sie diese Option aus, um das Gerät während des Dateiübertragungsprozesses im Leerlauf zu halten.
6. Verwenden Sie eine der folgenden zwei Optionen, um eine Datei mit anderen Apps zu teilen:
   - **Mithilfe der Android-Konfiguration für verwaltete Apps übertragen** – Verwenden Sie diese Option nur dann, wenn die Ziel-App die ContentURI unter Verwendung ihrer Konfiguration für verwaltete Apps nutzen kann.
   - **Mithilfe von Geräte-Intent übertragen** – Intents sind App-spezifisch. Um eine Datei mithilfe dieser Option freizugeben, konsultieren Sie Dokumentation der Ziel-App und stellen Sie im Intents-Abschnitt unten die jeweiligen Informationen bereit. Intents ermöglichen es der Ivanti Go-App, eine Nachricht auf dem Gerät zu senden, sobald die Datei für das Teilen mit anderen Apps zur Verfügung steht.

Mithilfe der Android-Konfiguration für verwaltete Apps übertragen

Verfahren

1. Geben Sie in das Feld **Vorhandenes gerätebasiertes, benutzerdefiniertes Attribut wählen, um diese Datei für andere Apps freizugeben** einen bereits vorhandenen Attributnamen ein, z. B. **Custom-Filename**. Weitere Informationen finden Sie unter Anpassbare Attribute für Geräte zuweisen.
2. Der Name des benutzerdefinierten Attributs muss neu und eindeutig sein und darf nur für diesen Vorgang der Dateiübertragung verwendet werden. Jedes benutzerdefinierte Geräteattribut kann nur die ContentURI (Speicherort der Datei) des Geräts für eine Datei pro Konfiguration speichern.
   Stellen Sie Zugriff auf folgende Apps und/oder Paketnamen bereit: Sie können App-Namen aus der entsprechenden Auswahlhilfe auswählen und Paketnamen hinzufügen.

> Dies sind die einzigen zulässigen Pakete, die berechtigt sind, auf die Datei zuzugreifen.

   - **App-Namen** – Über die Auswahlhilfe für App-Namen können Sie App-Namen auswählen.
   - **Paketnamen** – Hier können Sie die Bundle-IDs eingeben, z. B.Trennen Sie mehrere Paketnamen mit einem Strichpunkt (;).

```bash
com.mobileiron.filetransfer.android3.
```

Klicken Sie auf **Speichern**. Die neue Konfiguration für die Dateiübertragung wird auf der Seite "Konfigurationen" angezeigt.

Konfigurieren der Ziel-App

Verfahren

1. Wechseln Sie zu **Apps > App-Katalog**.
2. Wählen Sie die Ziel-App aus, die die Datei empfangen soll.

3. Navigieren Sie zu **App-Konfigurationen > Verwaltete Konfigurationen für Android**.
4. Erstellen Sie eine neue Konfiguration oder verwenden Sie eine bereits bestehende.
5. Eine App verfügt mitunter über eine Einstellung wie "Manifestinfos" oder andere Eigenschaften, in denen der Administrator die Ersetzungsvariable definieren und der Ziel-App den Speicherort der Datei mitteilen kann. Geben Sie etwa bei der Ivanti Velocity-App die Ersetzungsvariable im Dialogfeld für die App-Konfiguration unter **Konfigurationen abrufen** in das Feld **Manifestinfos** ein. Zum Beispiel: $Custom-File-Name$.
   Wählen Sie die Verteilung aus.
6. Klicken Sie auf **Speichern**.

Mithilfe von Geräte-Intent übertragen

Verfahren

1. Geben Sie in das Feld **Vorhandenes Geräteattribut wählen, um den Dateipfad in Intents-Extras zu übergeben** einen Namen für ein neues benutzerdefiniertes Attribut ein, z. B. deviceIntentURI.
2. In benutzerdefinierten Attributen ist der Speicherortwert (URI/ContentURI) für jedes Gerät auf dem Server enthalten. Dadurch können Administratoren die Verfügbarkeit einer Datei auf dem Gerät einfacher bestimmen. Weitere Informationen finden Sie unter Anpassbare Attribute für Geräte zuweisen.
   Geben Sie in das Feld **Zugriff für bestimmte App oder Paketnamen gewähren** den **App-Namen** oder den **Paketnamen** ein, z. B. Velocity.

> Dies sind die einzigen zulässigen Pakete, die berechtigt sind, auf die Datei zuzugreifen.

3. Geben Sie im Abschnitt "Intents-Standard" folgende Details an:
   - **Operationsart** – Wählen Sie über die Dropdownliste **Aktivität starten**/**Dienst starten** oder, je nach App, eine vergleichbare Option aus. Wählen Sie den richtigen Wert für dieses Feld gemäß den Anleitungen des Entwicklers der Ziel-App aus oder konsultieren Sie dazu die Dokumentation zur Ziel-App.
   - **Klassenname** (optional) – Wählen Sie den richtigen Wert für dieses Feld gemäß den Anleitungen des Entwicklers der Ziel-App aus oder konsultieren Sie dazu die Dokumentation zur Ziel-App.
   - **Aktion** – Setzen Sie die Aktion aufoder, je nach App, auf einen entsprechenden Wert.

     Bash

     ```
     com.wavelink.nameofapp.action.INSTALL_CONFIG
     ```

   - **Kategorie** – Trennen Sie mehrere Werte durch einen Strichpunkt (;).
   - **MIME-Typ** (optional) – Auf dem Hostserver des Administrators sollte für die Datei "custom.mobileconfig" der MIME-Typ "application/configuration" eingestellt werden, sodass das MDM-Profil für das Gerät heruntergeladen und auf dem Gerät installiert wird. Wählen Sie den richtigen Wert für dieses Feld gemäß den Anleitungen des Entwicklers der Ziel-App aus oder konsultieren Sie dazu die Dokumentation zur Ziel-App.
   - **Flags** (optional) – Wählen Sie die Anzahl der zu verwendenden Flags aus. Wählen Sie den richtigen Wert für dieses Feld gemäß den Anleitungen des Entwicklers der Ziel-App aus.

Geben Sie die **Intents-Extras**-Werte unter SCHLÜSSEL, TYP und WERT an (optional). Spezifischere Parameter sind der OEM-App-Dokumentation zu entnehmen. Wählen Sie den richtigen Wert für dieses Feld gemäß den Anleitungen des Entwicklers der Ziel-App

aus oder konsultieren Sie dazu die Dokumentation zur Ziel-App.

5. Klicken Sie auf **Speichern**.
6. Wählen Sie auf der Seite "Konfigurationen" die neue Konfiguration für Dateiübertragung und dann **Aktionen** > **Auf Beschriftung anwenden** aus. Das Dialogfeld **Auf Bechriftung anwenden** wird geöffnet.
7. Wählen Sie die gewünschte Beschriftung aus und klicken Sie anschließend auf **Anwenden**.
   Das Übertragen bzw. Teilen von Dateien an bzw. mit anderen Apps lässt sich nur überprüfen, indem Sie Protokolle von der Ziel-App oder vom Gerät abrufen.

Überprüfen des Download-Status

In benutzerdefinierten Attributen ist der Speicherortwert (ContentURI) für jedes Gerät auf dem Server enthalten. Dadurch können Administratoren die Verfügbarkeit einer Datei auf dem Gerät einfacher bestimmen.

Verfahren

1. Wechseln Sie zu **Geräte** > **Geräte**.
2. Wählen Sie ein bestimmtes Gerät aus, auf der die Dateiübertragungskonfiguration bereitgestellt wurde.
3. Wählen Sie auf der Seite "Gerätedetails" das Gerät und dann **Aktionen** > **Anmelden des Geräts erzwingen** aus.
4. Überprüfen Sie auf der Registerkarte "Konfigurationen", ob für die Dateiübertragungskonfiguration der Status **Angewendet** angezeigt wird.
5. Überprüfen Sie auf der Registerkarte "Benutzerdefinierte Attribute" ob der Name des neuen benutzerdefinierten Attributs (z. B. "Custom-File-Name$") mit dem zugehörigen Wert angezeigt wird. Dies liefert Ihnen die Informationen zum Speicherort der Datei auf dem Gerät und weist darauf hin, dass die Datei lokal auf das Gerät heruntergeladen wurde, das in der Ivanti Go-App-Sandbox verfügbar ist.
   Das Übertragen bzw. Teilen von Dateien an bzw. mit anderen Apps lässt sich nur überprüfen, indem Sie Protokolle von der Ziel-App oder vom Gerät abrufen.

10.10.8.3. Apple TV-Konfiguration

Lizenz: Silver

Eine Apple TV-Konfiguration bestimmt Sprache und Ort für Apple TV.

Die Apple TV-Einstellungen sind wie folgt:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Sprache	Geben Sie den zweistelligen Sprachcode ein, um die Sprache der Benutzeroberfläche zu bestimmen.
Region	Geben Sie das Landeskennzeichen ein, um das Land/die Sprache für die Benutzeroberfläche zu bestimmen.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.8.4. AirPlay Spiegelung

Lizenz: Gold

AirPlay Mirroring ist eine Funktion, mit der Sie den Bildschirm eines iOS-Geräts auf einem Monitor mit Apple TV anzeigen können. Apple TV und das iOS-Gerät müssen mit dem gleichen WLAN verbunden sein. Für diese Funktionalität werden die folgenden Geräte benötigt:

- Geräte mit iOS 7 und höher – überwachte Geräte
- Geräte mit macOS 10.10 und höher – überwachte Geräte
- Apple TV Version – überwacht
- AirPlay-

> Die Entscheidung, auch Nicht-iOS-Geräte zu verwalten, kann nicht rückgängig gemacht werden.

Dieser Abschnitt enthält die folgenden Themen:

- Konfiguration von Apple AirPlay
- Konfiguration von AirPlay auf dem Mobilgerät
- Konfiguration eines Monitors für Apple TV
- Verbindung Ihres iOS-Geräts mit Apple TV

Konfiguration von Apple AirPlay

Weitere Informationen zu den AirPlay-Konfigurationseinstellungen finden Sie unter AirPlay-Konfiguration.

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie auf **AirPlay**.
4. Geben Sie Name und Beschreibung der Konfiguration in den entsprechenden Feldern ein.
5. Geben Sie für alle unterstützten iOS-Versionen einen Gerätenamen und ein Passwort ein.
6. Klicken Sie auf **+Hinzufügen**, um gegebenenfalls ein anderes Gerät hinzuzufügen.
7. Sie können für überwachte Geräte mit iOS 7+ oder Geräte mit macOS 10.10+ auch Geräte-IDs in einer Zulassungsliste ergänzen.
8. Klicken Sie auf **Weiter**.
9. Wählen Sie eine Verteilungsebene.
10. Klicken Sie auf **Fertig**.

Konfiguration von AirPlay auf dem Mobilgerät

Verfahren

1. Apple Configurator verwenden
2. Gehen Sie zu **Geräte > Geräte**.

3. Klicken Sie auf den Namen eines iOS-Geräts, um die Seite mit den Details für dieses Gerät anzuzeigen.
4. Klicken Sie auf das ⋮-Symbol.
5. Wählen Sie **AirPlay Mirroring**, um den Dialog für AirPlay Mirroring anzuzeigen.
6. Wählen Sie ein Apple-TV-Gerät aus dem Pulldown-Menü.
7. Geben Sie eine Abtastzeit in Sekunden ein, um die Zeit für die Suche nach dem ausgewählten Gerät zu begrenzen.
8. Geben Sie das Passwort für das Apple-TV-Gerät ein.
9. Klicken Sie auf **Anfrage senden**.

Konfiguration eines Monitors für Apple TV

Verfahren

1. Gehen Sie auf einem mit Apple TV verbundenen Monitor zu **Einstellungen > Profil**.
2. Wählen Sie **Ivanti Neurons for MDM Apple-Konfigurator** aus.
3. Klicken Sie auf **Profil hinzufügen**.
4. Klicken Sie auf das ⋮-Symbol.
5. Wählen Sie **AirPlay Mirroring**, um den Dialog für AirPlay Mirroring anzuzeigen.
6. Wählen Sie ein Apple-TV-Gerät aus dem Pulldown-Menü.
7. Geben Sie eine Abtastzeit in Sekunden ein, um die Zeit für die Suche nach dem ausgewählten Gerät zu begrenzen.
8. Geben Sie das Passwort für das Apple-TV-Gerät ein.
9. Klicken Sie auf **Anfrage senden**.

Verbindung Ihres iOS-Geräts mit Apple TV

Verfahren

1. Verbinden Sie das Apple-TV-Gerät mit einem Monitor.
2. Gehen Sie in Apple TV remote auf **Einstellungen > Konten > Home Sharing**, um Home Sharing zu aktivieren.
3. **Verbinden Sie das iOS-Gerät** mit dem gleichen WLAN wie das **Apple-TV-Gerät**.
4. Öffnen Sie die Remote-App auf Ihrem **iOS**-Gerät.
5. Aktivieren Sie **Home Sharing** über den Bildschirm **Fernsteuerungseinstellungen**.

10.10.8.5. Browser-Einstellungen

Mit den Browser-Einstellungen können Sie Einstellungen und Einschränkungen für Google Chrome, Mozilla Firefox, Microsoft Edge und Internet Explorer auf Geräten mit Windows 10 konfigurieren.

Diese Funktion erfordert Bridge. Details finden Sie unter **Ivanti Bridge**.

> Stellen Sie sicher, dass die Browser auf dem Gerät installiert sind, bevor Sie die Browsereinstellungen übernehmen.

Browser-Einstellungen konfigurieren:

1. Gehen Sie zu **Konfiguration > +Hinzufügen** .
2. Wählen Sie die Konfiguration **Browser-Einstellungen**.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Definieren Sie in dem Abschnitt Konfigurations-Setup die übrigen Einstellungen aus der folgenden Tabelle.

Einstellung	Aktion
Browser	Wählen Sie die Browser-Art, für die die Einstellungen benötigt werden: • **Chrome** • **Firefox** • **Microsoft Edge** • **Internet Explorer**
Browser-Einstellungen	Konfigurieren Sie folgende Optionen: **Browser zulassen**: • Speichern von Passwörtern erlauben • Sicheren Browsermodus erlauben • Veraltete Plugins im Browser erlauben **Chrome und Firefox**: • **Löschen der Browser-History erlauben** **Chrome und Internet Explorer**: • **Drucken aus Browser erlauben** • **Neue Registerkarte „Seiten-URL“** **Nur Chrome**: • **Apps-Tastaturkürzel in der Lesezeichenzeile anzeigen** • **Home-Schaltfläche anzeigen** • **Synchronisierung von Daten mit Google erlauben** • **Apps weiter im Hintergrund laufen lassen, wenn Chrome geschlossen wird.** **Nur Firefox**: • **Installation von Erweiterungen erlauben** **Nur Internet Explorer**: • **Herunterladen von Daten von Websites erlauben**
Browser-Favoriten	Klicken Sie auf **+Hinzufügen**. Das Fenster **Browser-Favorit hinzufügen** wird angezeigt. Konfigurieren Sie die folgenden Felder: • **Anzeigename**: Geben Sie den Anzeigenamen für den Favoriten ein. • **URL**: Geben Sie die URL des Browser-Favoriten ein. Klicken Sie auf **[Add]**. Die Details des hinzugefügten Browser-Favoriten werden auf der Seite angezeigt. Klicken Sie in der Spalte **Aktionen** auf das Bearbeitungssymbol, um die Einstellung zu bearbeiten. Klicken Sie zum Löschen des Browser-Favoriten auf das Löschsymbol. **Browser-Favoriten - Ordnername**: Geben Sie den Namen des Ordnernamens für den Browser-Favoriten ein, wenn die Favoriten aufgelistet werden sollen. Sie können auch den Browser-Favoriten im CSV-Format hinzufügen. Im CSV-Format hochladen: 1. Klicken Sie auf CSV-Datei hochladen. Suchen Sie die CSV-Datei, die Sie hochladen wollen. 2. Klicken Sie auf **Hochladen**. Die Angaben in der CSV-Datei sollten in folgendem Format hinzugefügt werden:

10.10.8.6. Konfiguration des Single-App-Modus für iOS

Lizenz: Silver

Der Single-App-Modus beschränkt iOS- und tvOS-Geräte auf die Nutzung der angegebenen App. Sie könnten zum Beispiel Geräte einrichten, die nur eine von Ihrem Unternehmen entwickelte benutzerdefinierte App nutzen können.

Verfahren

1. Gehen Sie zu **Konfigurationen > Hinzufügen > Einzel-App-Modus**.
2. Definieren Sie mit den folgenden Richtlinien die App- und zugehörige Einstellungen.
3. Klicken Sie auf **Weiter**.

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
App wählen	Wählen Sie die zu verwendende Methode für das Auswählen der App aus: • Über App-Katalog und System-Apps: Durchsuchen Sie den -App-Katalog und die System-Apps (diese sind standardmäßig auf Apple-Geräten vorinstalliert). • Geben Sie den Namen der App ein und wählen Sie aus, wann diese in der App-Liste angezeigt wird. • Geben Sie die Bundle-ID an: Wählen Sie den eindeutigen Identifikator für die System-App aus, die Sie auswählen wollen.Nutzen Sie diese Option, wenn Sie die System-App mit der Option aus **App- Katalog & System-Apps** nicht finden können.
Touch deaktivieren	Wählen Sie diese Option, um den Touchscreen zu deaktivieren.
Geräterotation deaktivieren	Wählen Sie diese Option, um die Geräterotation zu deaktivieren.
Lautstärke-Tasten deaktivieren	Wählen Sie diese Option, um die Lautstärke-Tasten des Gerät zu deaktivieren.
Ringer Switch deaktivieren	Wählen Sie diese Option, um den Ruftonschalter des Gerät zu deaktivieren.
Schlaf/Wach-Taste deaktivieren	Wählen Sie diese Option, um die Schlaf/Wach-Taste des Gerät (am oberen rechten Rand des Gerät) zu deaktivieren.
Automatische Sperre deaktivieren	Wählen Sie diese Option, um zu verhindern, dass das Gerät nach einer Zeit im Leerlauf in den Ruhemodus wechselt.
Voice-Over aktivieren	Wählen Sie diese Option, um die Bildschirmlesetechnologie VoiceOver (Bedienungshilfe) zu aktivieren.
Zoom aktivieren	Wählen Sie diese Option, um die Zoomfunktion (Bedienungshilfe) zu aktivieren.
Farbumkehr aktivieren	Wählen Sie diese Option, um die Farbumkehr (Bedienungshilfe) zu aktivieren.
Assistive Touch aktivieren	Wählen Sie diese Option, um AssistiveTouch (Bedienungshilfe) zu aktivieren.
Sprachauswahl aktivieren	Wählen Sie diese Option, um die Funktion „Auswahl vorlesen“ (Bedienungshilfe) zu aktivieren.

Einstellung	So gehen Sie vor
Mono-Audio aktivieren	Wählen Sie diese Option, um von Stereo- zu Mono-Audio (Bedienungshilfe) zu wechseln.
Voice-Over-Einstellungen	Wählen Sie diese Option, um Benutzern zu gestatten, VoiceOver-Einstellungen vorzunehmen.
Zoom-Einstellungen	Wählen Sie diese Option, um Benutzern zu gestatten, Zoom-Einstellungen vorzunehmen.
Farbumkehr-Einstellungen	Wählen Sie diese Option, um Benutzern des Gerät das Umkehren von Farben zu gestatten.
Assistive Touch-Einstellungen	Wählen Sie diese Option, um Benutzern zu gestatten, AssistiveTouch-Einstellungen vorzunehmen.

4. Wählen Sie in dem Bildschirm **Verteilung** die Gerätegruppen aus, die diese Konfiguration erhalten sollen.
5. Klicken Sie auf **Fertig**.

Wenn Sie die Wählhilfe als die zu verwendende App definiert haben, funktioniert die Home-Taste, sobald das Gerät in den Einzel-App-Modus gewechselt ist.

10.10.8.7. iOS-MDM-Profil definieren

Die iOS-MDM-Konfiguration legt die Zugriffsgrenzen für Ivanti Neurons for MDM fest. Es gibt zwei Arten von iOS-MDM-Konfigurationen:

- **iOS MDM - Massenbereitstellung:** Für Geräte, die vom Unternehmen erworben und im Rahmen einer Masseninstallation bereitgestellt werden.
- **iOS MDM – Einzelbereitstellung:** Für einzeln bereitgestellte Geräte. Gilt nicht für überwachte und benutzerregistrierte Geräte.

Es wird immer nur eine der beiden Arten bereitgestellt und für alle Spaces aktiviert.

iOS-MDM-Konfiguration bearbeiten

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Gehen Sie zu **Konfigurationen**.
3. Wählen Sie die iOS-MDM-Konfiguration aus, die Sie bearbeiten wollen.
4. Klicken Sie auf das Stiftsymbol, um die Konfiguration zu bearbeiten.
5. Nehmen Sie Änderungen gemäß den folgenden Richtlinien vor:
6. Klicken Sie auf **Fertig**.

Einstellung	So gehen Sie vor
MDM-Zugriffsrechte	
Gerätesperre und Entfernen des Passcodes erlauben	Deaktivieren Sie die Option, um eine Konfiguration zu verhindern, bei der eine Passwort-Compliance erzwungen wird.
Gerätelöschung erlauben	Deaktivieren Sie die Option, um zu verhindern, dass eine Komplettlöschung des Geräts erzwungen wird.
Abfrage von Netzwerkinformationen erlauben (Mobiltelefon-/SIM-Nummern, MAC-Adressen)	Deaktivieren Sie die Option, um das Gerät aus den Netzwerkinformationsberichten auszuschließen. Wenn Sie diese Option deaktiviert haben, erscheint in der Gerätelistenansicht und Gerätedetailansicht für die Netzwerkinformationen „N/A“, die nicht länger gemeldet werden. Auch die Roaming-Richtlinie kann bei den betroffenen Geräten nicht mehr erzwungen werden.
Kennwort für Profilentfernung	
Kennwort zum Entfernen des Profils	Legen Sie ein Kennwort fest. Wenn der Benutzer ein Profil vom Gerät löschen möchte, wird er zur Eingabe eines Kennworts aufgefordert.
ADD erforderlich APP (iOS 15+)	
Durch Suche hinzufügen	Geben Sie den Namen der App ein, suchen Sie die App im App Store und wählen Sie die gewünschte App aus. Es kann jeweils nur eine App hinzugefügt werden. Wenn Sie eine App auswählen, werden die anderen Apps deaktiviert.
Manuell hinzufügen	Geben Sie die iTunes-ID der App ein.

Ihre Änderungen werden nur für diejenigen Geräte wirksam, die nach Vornahme der Änderungen bereitgestellt werden.

10.10.8.8. Konfigurieren eines iOS-MDM-Profils

Die macOS-MDM-Konfiguration legt Zugriffsgrenzen für Ivanti Neurons for MDM fest. Die macOS-MDM-Konfigurationen werden einzeln für die nacheinander bereitgestellten Geräte bereitgestellt.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Gehen Sie zu **Konfigurationen**.
3. Wählen Sie die macOS-MDM-Konfiguration aus, die Sie bearbeiten wollen.
4. Klicken Sie auf das Stiftsymbol, um die Konfiguration zu bearbeiten.
5. Nehmen Sie Änderungen gemäß den folgenden Richtlinien vor:
6. Klicken Sie auf **Fertig**.

Einstellung	So gehen Sie vor
Gerätesperre und Entfernen des Passcodes erlauben	Deaktivieren Sie die Option, um eine Konfiguration zu verhindern, bei der eine Passwort-Compliance erzwungen wird.
Gerätelöschung erlauben	Deaktivieren Sie die Option, um zu verhindern, dass eine Komplettlöschung des Geräts erzwungen wird.
Abfrage von Netzwerkinformationen erlauben (Mobiltelefon-/SIM-Nummern, MAC-Adressen)	Deaktivieren Sie die Option, um das Gerät aus den Netzwerkinformationsberichten auszuschließen. Wenn Sie diese Option deaktiviert haben, erscheint in der Gerätelistenansicht und Gerätedetailansicht für die Netzwerkinformationen „N/A“, die nicht länger gemeldet werden. Auch die Roaming-Richtlinie kann bei den betroffenen Geräten nicht mehr erzwungen werden.
Kennwort für Profilentfernung	
Kennwort zum Entfernen des Profils	Legen Sie ein Kennwort fest. Wenn der Benutzer ein Profil vom Gerät löschen möchte, wird er zur Eingabe eines Kennworts aufgefordert.

Ihre Änderungen werden nur für diejenigen Geräte wirksam, die nach Vornahme der Änderungen bereitgestellt werden.

10.10.8.9. Content-Caching

Lizenz: Gold

Gilt für: macOS 10.13.4 oder unterstützte neuere Versionen.

Konfigurieren Sie den Content-Caching-Dienst, um lokale App Store-Kopien der Software zu erlauben und verbundenen Clients schnellere Software- und Anwendungs-Downloads zu ermöglichen.

Content-Caching-Konfiguration

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie in dem Suchfeld **Caching** ein und klicken Sie dann auf die Konfiguration **Content-Caching**.
4. Geben Sie einen Namen ein und beschreiben Sie die Konfiguration.
5. Geben Sie die Konfigurationseinstellungen für **Content-Caching** ein.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Option **Diese Konfiguration aktivieren**.
8. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
9. Klicken Sie auf **Fertig**.

Konfigurationseinstellungen für Content-Caching

Verwenden Sie die Einstellungen in der folgenden Tabelle, um Content-Caching zu konfigurieren. Weitere Informationen zu diesen Einstellungen finden Sie in der **Apple-Dokumentation**.

Einstellung	Beschreibung
Erlauben Sie dem System, Inhalte automatisch aus dem Cache zu löschen. (Verfügbar in macOS 10.15 oder unterstützten neueren Versionen.	Erlauben Sie dem System, Inhalte automatisch aus dem Cache zu löschen, wenn es Festplattenspeicherplatz für andere Apps benötigt (d. h wenn der freie Festplattenspeicherplatz auf dem Computer knapp wird). Standardmäßig ist diese Option aktiviert.
Persönliches Caching zulassen	Zwischenspeichern der iCloud-Daten des Benutzers. Es kann einige Zeit (Stunden oder Tage) dauern, bis Clients auf Änderungen dieser Einstellung reagieren; sie hat keine sofortige Wirkung. Standardmäßig ist diese Option aktiviert.
Gemeinsames Caching zulassen	Zwischenspeichern von Nicht-iCloud-Inhalten wie Apps und Software-Updates. Es kann einige Zeit (Stunden, Tage) dauern, bis die Clients auf Änderungen dieser Einstellung reagieren; sie hat keine sofortige Wirkung. Standardmäßig ist diese Option aktiviert.
Automatische Aktivierung des Content-Cache zulassen	Aktiviert den Content-Cache automatisch, wenn möglich, und verhindert, dass er deaktiviert wird.
Automatische Aktivierung von Tethered Caching zulassen (Verfügbar in macOS 10.15.4 oder unterstützten neueren Versionen	Die gemeinsame Nutzung der Internetverbindung wenn möglich automatisch aktivieren und die Deaktivierung der gemeinsamen Nutzung der Internetverbindung verhindern.
Deaktiviert Tethered Caching	Deaktiviert Tethered Caching. Die Option Deaktiviert Tethered Caching setzt die Option „Automatische Aktivierung von Tethered Caching zulassen“ außer Kraft.
Cache-Begrenzung	Die maximale Anzahl Bytes des Festplattenspeichers, der für den Inhaltscache verwendet werden soll. Der Wert 0 bedeutet unbegrenzten Speicherplatz. Standardwert: 0
Datenpfad	Der Pfad zu dem Verzeichnis zum Speichern von zwischengespeicherten Inhalten. Wenn Sie diese Einstellung manuell ändern, wird der zwischengespeicherte Inhalt nicht automatisch vom alten zum neuen Speicherort verschoben. Verwenden Sie zum automatischen Verschieben von Inhalten den Bereich „Content Caching“ unter „Voreinstellungen teilen“. Der Wert muss /Library/Application Support/Apple/AssetCache/Data lauten oder damit enden.
Anzeige von Warnmeldungen	Content-Caching zeigt Ausnahmebedingungen (Alerts) als Systembenachrichtigungen in der oberen Ecke des Bildschirms an.

Einstellung	Beschreibung
zulassen (Verfügbar in macOS 10.15 oder unterstützten neueren Versionen.	
Gerät aktiv halten (Verfügbar in macOS 10.15 oder unterstützten neueren Versionen.	Verhindert, dass der Computer in den Ruhezustand versetzt wird, solange das Content-Caching eingeschaltet ist (Systemeinstellungen > Freigabe > Content-Caching eingeschaltet).
Abhörbereiche	Ein Array von Dictionaries mit einem Bereich von Client-IP-Adressen, die bedient werden sollen.
Erste IP-Adresse	Erste IP-Adresse der Clients in den Abhörbereichen.
Letzte IP-Adresse	Letzte IP-Adresse der Clients in den Abhörbereichen.
IP-Adressen-Typ	Wählen Sie eine der folgenden Optionen aus: • IPv4 (Standard) • IPv6
Nur Abhörbereiche zulassen	Der Content-Cache stellt nur den Clients in den Abhörbereichen Inhalte zur Verfügung.
Abhören von Peer- und Parent-Netzen zulassen	Der Content-Cache stellt den Clients im Verbund der Abhörbereiche, Peer-Abhörbereiche und Parents Inhalte zur Verfügung. Standardmäßig ist diese Option aktiviert.
Nur lokale Subnetze zulassen	Der Content-Cache bietet Inhalte nur für Clients im gleichen unmittelbaren lokalen Netzwerk an. Für Clients in anderen Netzwerken, die über den Content-Cache erreichbar sind, werden keine Inhalte angeboten. Wenn diese Option aktiviert ist, werden die Abhörbereiche ignoriert. Standardmäßig ist diese Option aktiviert.
Client-Identität protokollieren	Der Content-Cache protokolliert die IP-Adresse und Port-Nummer der Clients, die Inhalte anfordern.
Auswahl der Parent-Richtlinie	Wählen Sie eine der folgenden Richtlinienoptionen aus: • Zuerst verfügbar • URL-Pfad-Hash • Round-Robin (Standard) • Zufällig • Affin-Verfügbar
Parent	Ein Array mit den lokalen IP-Adressen anderer Inhalts-Caches, von denen dieser Cache Inhalte herunterladen oder auf die er Inhalte hochladen soll, statt diese direkt von Apple herunter- oder zu

Einstellung	Beschreibung
	Apple hochzuladen. Klicken Sie auf **+ Hinzufügen**, um eine oder mehrere IP-Adressen hinzuzufügen.
Nur lokale Peer-Subnetze zulassen	Der Content-Cache gleicht sich nur mit anderen Content-Caches im gleichen unmittelbaren lokalen Netzwerk ab und nicht mit Content-Caches, die die gleiche öffentliche IP-Adresse wie das Gerät verwenden. Standardmäßig ist diese Option aktiviert.
[Port]	Die TCP-Portnummer, auf welcher der Content-Cache Anfragen für Uploads oder Downloads annimmt. Setzen Sie den Port auf 0, wenn ein zufälliger, freier Port gewählt werden soll. Standardwert: 0
Öffentliche Bereiche	Ein Array von Dictionaries mit einem Bereich öffentlicher IP-Adressen, die die Cloud-Server für den Abgleich von Clients mit Inhalts-Caches verwenden sollen.
Erste IP-Adresse	Erste IP-Adresse der Server in den öffentlichen Bereichen.
Letzte IP-Adresse	Letzte IP-Adresse der Server in den öffentlichen Bereichen.
IP-Adressen-Typ	Wählen Sie eine der folgenden Optionen aus: • IPv4 (Standard) • IPv6

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.8.10. Erstellen einer Android-Tastenkombination

Shortcuts sind nur im Kiosk-Modus mit einem Browser aus der Whitelist verfügbar. Der Browser muss in der Sperr- und der Kiosk-Konfiguration. Die Verknüpfungen werden in der Ivanti Neurons for MDM-Kiosk-Startliste angezeigt.

Verfahren

1. Wechseln Sie zu **Konfigurationen > +Hinzufügen**
2. Klicken Sie auf **Android-Verknüpfung**, um die Seite **Konfiguration für Android-Verknüpfung erstellen** anzuzeigen.
3. Geben Sie einen Namen für die Konfiguration in das Feld **Name** ein.
4. Geben Sie eine Beschreibung der Konfiguration in das Feld **Beschreibung** ein.
5. Geben Sie eine eindeutige Bezeichnung für die Verknüpfung in das Feld **Bezeichnung** ein.
6. Geben Sie eine URL für das Ziel der Verknüpfung in das Feld **URL** ein.
7. Ziehen Sie optional eine Datei in das Symbolfeld oder klicken Sie auf **Datei wählen**, um zu der Datei zu navigieren und ein Symbol für die Verknüpfung auszuwählen.
8. Klicken Sie auf **Weiter**.

10.10.8.11. Erstellen von Konfigurationen für Einstellungen für Barrierefreiheit

Mit dieser Konfiguration können Unternehmen die Einstellungen für Barrierefreiheit auf Apple-Geräten einschränken, ändern oder konfigurieren.

Verfahren

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie auf **Konfigurationen für Einstellungen für Barrierefreiheit**.
4. Konfigurieren Sie die in der folgenden Tabelle angegebenen Einstellungen:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Wählen Sie eine der Einstellungen für Barrierefreiheit aus.	• **Einstellungen für Barrierefreiheit**: Hierüber konfigurieren Sie die Einstellungen für Barrierefreiheit auf macOS-Geräten. • **Einschränkungen für Einstellungen für Barrierefreiheit**: Hierüber konfigurieren Sie Einschränkungen für das Ändern von Einstellungen für Barrierefreiheit auf iOS-Geräten.
Einstellungen für Barrierefreiheit	**Konfigurations-Setup**
Nahansicht Fernpunkt	Die niedrigste Zoomstufe bei den Zoomeinstellungen
Nahansicht Nahpunkt	Die höchste Zoomstufe bei den Zoomeinstellungen
	"Scroll-Gesten verwenden" in Zoomoptionen aktivieren
	"Sanfte Bilder" in Zoomoptionen aktivieren
Kontrastwert	Wert angeben
	Markieren Sie das Kontrollkästchen "Bildschirmblinken in Audio-Optionen aktivieren".
Cursorgröße Anfangsverzögerung Maustreiber Maximale Geschwindigkeit Maustreiber "Anschlagverzögerung" in Tastaturoptionen aktivieren "Tastentöne" für langsame Tasten aktivieren	Markieren Sie das Kontrollkästchen "Maustasten in Maus- und Trackpad-Optionen aktivieren". Wert angeben Markieren Sie das Kontrollkästchen "Integriertes Trackpad ignorieren". Wert angeben Wert angeben Aktivieren Sie das Kontrollkästchen. Aktivieren Sie das Kontrollkästchen.
Verzögerung langsame Taste	Aktivieren Sie das Kontrollkästchen.
Geben Sie den Wert in Millisekunden an.	Aktivieren Sie das Kontrollkästchen.
Markieren Sie das Kontrollkästchen "Stereoton als Mono ausgeben". Einrastfunktion in Tastaturoptionen aktivieren	Aktivieren Sie das Kontrollkästchen. Aktivieren Sie das Kontrollkästchen.

Einstellung	So gehen Sie vor
Signalton aktivieren, wenn Änderungstaste für Einrastfunktion eingestellt ist	Aktivieren Sie das Kontrollkästchen.
"Gedrückte Tasten anzeigen" für Einrastfunktion aktivieren	Aktivieren Sie das Kontrollkästchen.
Voice-Over aktivieren	Aktivieren Sie das Kontrollkästchen.
"Farben umkehren" in Display-Anpassungen aktivieren	Aktivieren Sie das Kontrollkästchen.
Einschränkungen für Barrierefreiheit	**Konfigurations-Setup**
Fett dargestellten Text aktivieren	Aktivieren Sie das Kontrollkästchen.
"Kontrast erhöhen" aktivieren	Aktivieren Sie das Kontrollkästchen.
"Bewegung reduzieren" aktivieren	Aktivieren Sie das Kontrollkästchen.
"Transparenz reduzieren" aktivieren	Aktivieren Sie das Kontrollkästchen.
Apps für größeren Text, die die Verwendung von dynamischem Text unterstützen	Wählen Sie die Option aus der Dropdownliste aus.
Touch-Anpassungen aktivieren	Aktivieren Sie das Kontrollkästchen.
Voice-Over aktivieren	Aktivieren Sie das Kontrollkästchen.
Zoom aktivieren	Aktivieren Sie das Kontrollkästchen.

5. Wählen Sie die Option für die Verteilung aus und machen Sie die erforderlichen Angaben.
6. Klicken Sie auf **Fertig**.

10.10.8.12. Erstellen der Konfiguration für den Bildschirmschoner

Über die Konfiguration des Bildschirmschoners können Sie Optionen hinzufügen wie Kennwort, Leerlaufzeit, Modulpfad und Modulname.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Klicken Sie auf **Konfigurationen**.
3. Klicken Sie auf +Hinzufügen.
4. Geben Sie "Bildschirm" in das Suchfeld ein und klicken Sie dann auf **Bildschirmschoner**:
   Die Seite mit den Details für die Konfiguration des Startbildschirm-Layouts wird angezeigt.
5. Konfigurieren Sie die Einstellungen auf dieser Seite. Hinweise zu den Werten finden Sie in der Tabelle im Abschnitt Einstellungen der anpassbaren Konfiguration.
6. Klicken Sie auf **Weiter**, um die Verteilungseinstellungen zu konfigurieren und dann auf **Fertig**.

Konfigurationseinstellungen für den Bildschirmschoner

Einstellung	So gehen Sie vor
Name (obligatorisch)	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Kontrollkästchen "Kennwort abfragen"	Markieren Sie das Kontrollkästchen, damit der Gerätebenutzer ein Kennwort eingeben muss, wenn der Bildschirmschoner entsperrt oder gestoppt wird. Verfügbar in macOS 11 und höher.
Passwortabfrage	Geben Sie die Dauer der Verzögerung in Sekunden an.
Leerlaufzeit Anmeldefenster	Geben Sie die Leerlaufzeit in Sekunden an, nach deren Ablauf der Bildschirmschoner aktiviert werden soll.
Pfad zum Bildschirmschoner-Modul	Geben Sie den Pfad zum Bildschirmschoner-Modul an.
Name des Bildschirmschoner-Moduls (obligatorisch)	Geben Sie den Namen des Bildschirmschoners ein.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.8.13. Bildschirmschoner des Benutzers konfigurieren

Über die Konfiguration des Bildschirmschoners für den Benutzer können Sie Optionen wie Passwort, Leerlaufzeit, Modulpfad und Name hinzufügen.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Klicken Sie auf **Konfigurationen**.
3. Klicken Sie auf +Hinzufügen.
4. Geben Sie "Bildschirm" in das Suchfeld ein, und klicken Sie dann auf **Bildschirmschoner des Benutzers**:
   Die Detailseite "Konfiguration für den Bildschirmschoner des Benutzers erstellen" wird angezeigt.
5. Konfigurieren Sie die Einstellungen auf dieser Seite. In der Tabelle unter dem Thema **Konfigurationseinstellungen für den Bildschirmschoner des Benutzers** finden Sie Hilfestellungen zu den Werten.
6. Klicken Sie auf **Weiter**, um die Verteilungseinstellungen zu konfigurieren und dann auf **Fertig**.

Konfigurationseinstellungen für den Bildschirmschoner des Benutzers

Einstellung	So gehen Sie vor
Name (obligatorisch)	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Leerlaufzeit	Geben Sie die Leerlaufzeit in Sekunden an, nach deren Ablauf der Bildschirmschoner aktiviert werden soll.
Pfad zum Bildschirmschoner-Modul	Geben Sie den Pfad zum Bildschirmschoner-Modul an.
Name des Bildschirmschoner-Moduls (obligatorisch)	Geben Sie den Namen des Bildschirmschoners ein.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.8.14. Einstellungen für den Gerätenamen

Lizenz: Silver

Mithilfe einer Standardkonfiguration für den Gerätenamen können Sie eine neue Konfiguration erstellen, die bei oder nach der Registrierung via Push auf das Gerät übertragen wird und die Vergabe eines Namens ermöglicht. Der Administrator kann Standardgerätenamen nur für **überwachte iOS 8-Geräte** definieren. Zum Aufbau des Gerätenamens können Sie folgende Variablen verwenden:

- Geräteseriennummer
- Geräte-IMEI
- Gerätemodell
- Ivanti Neurons for MDM Benutzername (nur lokale Benutzer)
- LDAP-Organisationseinheit (OU)
- LDAP-Trivialname (CN)

Für Gerätenamen, die mit der Geräteseriennummer beginnen und mit der in LDAP definierten Benutzerorganisation enden, würden Sie beispielsweise $-$ eingeben.

Standardeinstellungen für den Gerätenamen (für iOS)

Einstellung	So gehen Sie vor
[Name] Beschreibung	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet. Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Gerätename Beschreibung	Geben Sie das Format für den Standardgerätenamen mit den verfügbaren Geräte- und LDAP-Attributen ein. Wenn der resultierende Gerätename mehr als 63 Zeichen umfasst, wird er gekürzt, so dass er auf dem Gerät korrekt angezeigt wird. Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.

> Variables.htmGeben Sie „$“ ein, um eine Liste mit unterstützten Variablen anzuzeigen, sofern diese für dieses Feld verfügbar ist.

Einstellungen für Gerätenamen (Android)

Der Android-Gerätename kann von Go app abgerufen werden. Beim Generieren des Berichts mit den Gerätedetails durch den Administrator wird anstelle des Gerätemodells oder Herstellernamens der tatsächliche Gerätename angezeigt. Falls der Benutzer den Gerätenamen ändert, wird der neue Name angezeigt, wenn der Bericht das nächste Mal generiert wird. Der jeweilige Gerätename wird unter **Geräte** > **Einstellungen** > **Gerätename** angezeigt.

10.10.8.15. Gerätehintergrundkonfiguration

Lizenz: Silver

Die Konfiguration des Gerätehintergrunds definiert ein Standardhintergrundbild für den Startbildschirm und den Sperrbildschirm von Geräten mit Android (verwaltete Geräte ab Version 7.0 mit Arbeitsprofil auf unternehmenseigenem Gerät) und iOS.

Android-Hintergrundeinstellungen

Standard-Hintergrundbild für Android-Geräte definieren:

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie auf **Gerätehintergründe**.
4. Klicken Sie auf das Android-Symbol, um den Abschnitt „Konfigurationseinrichtung“ für Android anzuzeigen und die folgenden Einstellungen zu konfigurieren.
5. Klicken Sie auf **Weiter**

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Android-Hintergrundbild hochladen Gleiches Bild für Startbildschirm und Sperrbildschirm verwenden. **Startbildschirm**	Wählen Sie diese Option, um ein einzelnes Bild für beide Bildschirme hochzuladen. Ziehen Sie die Bilddatei mit Drag&Drop in das Feld, oder klicken Sie auf **Datei wählen**, um die Bilddatei auszuwählen.
Sperrbildschirm	Ziehen Sie die Bilddatei mit Drag&Drop in das Feld, oder klicken Sie auf **Datei wählen**, um die Bilddatei auszuwählen.

6. Wählen Sie eine der folgenden Verteilungsoptionen aus:

- **Alle Geräte**
- **Keine Geräte** (Standard)
- **Anpassbar**

7. Klicken Sie auf **Fertig**.

Das hochgeladene Bild muss im Format .jpg oder .png vorliegen.

Einstellungen für iOS Wallpaper

Sie können ein Standard-Hintergrundbild für iOS-Geräte definieren.

Diese Einstellung gilt nur für überwachte Geräte.

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie auf **Gerätehintergründe**.
4. Klicken Sie auf das iOS-Symbol, um den Abschnitt „Konfigurationseinstellungen“ für iOS anzuzeigen und die folgenden Einstellungen zu konfigurieren.
5. Klicken Sie auf **Weiter**.

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
iPhone-Hintergrund hochladen	
Gleiches Bild für Startbildschirm und Sperrbildschirm verwenden.	Geben Sie an, dass Sie ein Einzelbild für das iPhone hochladen wollen.
Startbildschirm	Ziehen Sie die Bilddatei mit Drag&Drop in das Feld, oder klicken Sie auf **Datei wählen**, um die Bilddatei auszuwählen.
Sperrbildschirm	Ziehen Sie die Bilddatei mit Drag&Drop in das Feld, oder klicken Sie auf **Datei wählen**, um die Bilddatei auszuwählen.
iPad-Hintergrund hochladen	
Gleiches Bild für Startbildschirm und Sperrbildschirm verwenden.	Geben Sie an, dass Sie ein Einzelbild für das iPad hochladen wollen.
Startbildschirm	Ziehen Sie die Bilddatei mit Drag&Drop in das Feld, oder klicken Sie auf **Datei wählen**, um die Bilddatei auszuwählen.
Sperrbildschirm	Ziehen Sie die Bilddatei mit Drag&Drop in das Feld, oder klicken Sie auf **Datei wählen**, um die Bilddatei auszuwählen.

6. Wählen Sie eine der folgenden Optionen aus:

- **Alle Geräte**
- **Keine Geräte** (Standard)
- **Anpassbar**

7. Klicken Sie auf **Fertig**.

Die Bilder müssen 640 Pixel breit und 1136 Pixel hoch sein und im .jpg- oder .png-Format vorliegen.

macOS-Hintergrundbild-Einstellungen

Standard-Hintergrundbild für macOS-Geräte definieren:

1. Gehen Sie zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie auf **Gerätehintergründe**.
4. Klicken Sie auf das macOS-Symbol, um den Bereich „Konfigurationssetup“ für macOS anzuzeigen.
5. Geben Sie den Pfad zum Desktop-Bild ein.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Optionen aus:
    - **Alle Geräte**
    - **Keine Geräte** (Standard)
    - **Anpassbar**
8. Klicken Sie auf **Fertig**

> Sie können das Hintergrundbild je nach Einschränkung ändern. Wenn die macOS-Einschränkungskonfiguration **Ändern des Hintergrundbilds zulassen** aktiviert ist, können Sie das Hintergrundbild ändern.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.8.16. EMA Server-Integrationskonfiguration

Die EMA Server Integration-Konfiguration ermöglicht es Geräten mit Windows 10, sich mit dem konfigurierten Intel EMA-Server zu verbinden. Um Geräte mit dem konfigurierten Intel EMA-Server zu verbinden, sollten Sie das Installationsverzeichnis des ursprünglichen EMA-Agenten angeben und die .msh-Datei des EMA-Agent vom neuen EMA-Server hochladen.

Diese Funktion erfordert Bridge. Details finden Sie unter **Bridge**.

Verfahren

1. Gehen Sie zu **Konfiguration > +Hinzufügen** .
2. Wählen Sie die Konfiguration der **EMA Server Integration**.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Klicken Sie im Abschnitt für das Konfigurations-Setup auf **Datei auswählen**, um die .msh-Datei für den EMA-Agent auszuwählen.

> Die msh-Datei ist eine Agentenrichtliniendatei, die vom EMA-Server heruntergeladen werden kann.

5. Geben Sie im Feld **Original-EMA-Agent-Installationsverzeichnis** den Speicherort ein, an dem die Originaldatei EmaAgent.exe installiert ist.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
8. Klicken Sie auf **Fertig**.

10.10.8.17. Energiesparkonfiguration

Ivanti Neurons for MDM ermöglicht die Energiesparkonfiguration für die Payload, die Sie zum Konfigurieren der Energiespareinstellungen auf Windows- und macOS-Geräten verwenden.

Gilt für:

- Windows 10 bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird
- macOS 10.7 bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Energiesparen** ausfindig und wählen Sie sie aus.
3. Wählen Sie im Abschnitt "Betriebssystem wählen" die Option **Windows** oder **macOS** aus und klicken Sie auf **Weiter**.
4. Klicken Sie auf **+ Beschreibung hinzufügen**, um eine Kurzbeschreibung der Konfiguration einzugeben.
5. Konfigurieren Sie für Windows die folgenden Einstellungen zum **Energiesparen**:
   - **Gerät im Akkubetrieb**
   - **Gerät im Netzbetrieb**
6. Konfigurieren Sie die folgenden Einstellungen zum **Energiesparen**:
   - **Netzstrom-Energiespareinstellungen für Desktops**
   - **Zeitplan, nach dem der Computer startet oder herunterfährt**
   - **Netzstrom-Energiespareinstellungen für Laptops**
   - **Energiespareinstellungen für die Laptop-Batterie**
7. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
8. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Energiesparen** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
9. Klicken Sie auf **Fertig**.

Windows-Energiesparkonfiguration

Wenn eine neue Energiesparkonfiguration auf ein Gerät angewendet wird oder wenn vorhandene Konfigurationseinstellungen zum Energiesparen geändert werden, müssen die Benutzer zuerst ihre Geräte neustarten, damit die Änderungen wirksam werden.

Gerät im Akkubetrieb

Wenn das Gerät seine Energie über den Akku bezieht, wählen Sie aus den folgenden Energiespareinstellungen der Tabelle:

Einstellung	Beschreibung
Akkuschwellenwert für Aktivierung des Energiesparmodus	Wenn das Gerät seine Energie über den Akku bezieht, geben Sie den Akkuladezustand ein, ab dem das Gerät in den Energiesparmodus wechselt. Geben Sie dazu einen Wert zwischen 0 und 100 ein. Geben Sie einen Prozentwert ein, der dem Akkuladezustand entspricht. Beispiel: Wenn Sie 80 eingeben, wird der Energiesparmodus aktiviert, sobald die Ladung des Akkus 80 % oder weniger beträgt. Wenn Sie keinen Wert eingeben, ändert oder aktualisiert Ivanti Neurons for MDM diese Einstellung nicht. Bei Windows ist dieser Wert standardmäßig auf 70 % gesetzt.
Beim Schließen des Deckels	• **Keine Aktion durchführen**: Das Gerät bleibt eingeschaltet und nutzt weiterhin Akkuenergie. • **Standbymodus**: Das Gerät wechselt in den Standbymodus und bezieht nur wenig Akkuenergie. Der Computer bleibt eingeschaltet und Apps und Dateien werden im Arbeitsspeicher (Random Access Memory, RAM) gespeichert. • **Ruhezustand**: Das Gerät wechselt in den Ruhezustand. Geöffnete Apps und Dateien werden auf der Festplatte gespeichert und das Gerät wird ausgeschaltet. • **Herunterfahren**: Das Gerät fährt herunter. Geöffnete Apps und Dateien werden ohne Speichern geschlossen.
Bei Betätigung der Netztaste	• **Keine Aktion durchführen**: Das Gerät bleibt eingeschaltet und nutzt weiterhin Akkuenergie. • **Standbymodus**: Das Gerät wechselt in den Standbymodus und bezieht nur wenig Akkuenergie. Der Computer bleibt eingeschaltet und Apps und Dateien werden im Arbeitsspeicher (RAM) gespeichert. • **Ruhezustand**: Das Gerät wechselt in den Ruhezustand. Geöffnete Apps und Dateien werden auf der Festplatte gespeichert und das Gerät wird ausgeschaltet. • **Herunterfahren**: Das Gerät fährt herunter. Geöffnete Apps und Dateien werden ohne Speichern geschlossen.
Bei Betätigung der Standbytaste	• **Keine Aktion durchführen**: Das Gerät bleibt eingeschaltet und nutzt weiterhin Akkuenergie. • **Standbymodus**: Das Gerät wechselt in den Standbymodus und bezieht nur wenig Akkuenergie. Der Computer bleibt eingeschaltet und Apps und Dateien werden im Arbeitsspeicher (RAM) gespeichert. • **Ruhezustand**: Das Gerät wechselt in den Ruhezustand. Geöffnete Apps und Dateien werden auf der Festplatte gespeichert und das Gerät wird ausgeschaltet. • **Herunterfahren**: Das Gerät fährt herunter. Geöffnete Apps und Dateien werden ohne Speichern geschlossen.
Hybrid-Standbymodus aktivieren	• **Wahr**: Die Geräte können in den Hybrid-Standbymodus wechseln. Geöffnete Apps und Dateien werden im Arbeitsspeicher und auf der Festplatte gespeichert. Das Gerät nutzt nur geringfügig Akkuenergie. • **Falsch**: Verhindert, dass die Geräte in den Hybrid-Standbymodus wechseln können.

Gerät im Netzbetrieb

Wenn das Gerät seine Energie über eine externe Stromquelle bezieht, wählen Sie aus den folgenden Einstellungen der Tabelle:

Einstellung	Beschreibung
Akkuschwellenwert für Aktivierung des Energiesparmodus	Wenn das Gerät an die Netzstromversorgung angeschlossen ist, geben Sie den Akkuladezustand ein, ab dem das Gerät in den Energiesparmodus wechselt. Geben Sie dazu einen Wert zwischen 0 und 100 ein. Geben Sie einen Prozentwert ein, der dem Akkuladezustand entspricht. Beispiel: Wenn Sie 80 eingeben, wird der Energiesparmodus aktiviert, sobald die Ladung des Akkus 80 % oder weniger beträgt. Wenn Sie keinen Wert eingeben, ändert oder aktualisiert Ivanti Neurons for MDM diese Einstellung nicht. Bei Windows ist dieser Wert standardmäßig auf 70 % gesetzt.
Wenn der Deckel geschlossen wird	• **Keine Aktion durchführen**: Das Gerät bleibt eingeschaltet und nutzt weiterhin die externe Energiequelle. • **Standbymodus**: Das Gerät wechselt in den Standbymodus und verbraucht nur wenig Netzstrom. Der Computer bleibt eingeschaltet und Apps und Dateien werden im Arbeitsspeicher gespeichert. • **Ruhezustand**: Das Gerät wechselt in den Ruhezustand. Geöffnete Apps und Dateien werden auf der Festplatte gespeichert und das Gerät wird ausgeschaltet. • **Herunterfahren**: Das Gerät fährt herunter. Geöffnete Apps und Dateien werden ohne Speichern geschlossen.
Bei Betätigung der Netztaste	• **Keine Aktion durchführen**: Das Gerät bleibt eingeschaltet und nutzt weiterhin die externe Energiequelle. • **Standbymodus**: Das Gerät wechselt in den Standbymodus und verbraucht nur wenig Netzstrom. Der Computer bleibt eingeschaltet und Apps und Dateien werden im Arbeitsspeicher gespeichert. • **Ruhezustand**: Das Gerät wechselt in den Ruhezustand. Geöffnete Apps und Dateien werden auf der Festplatte gespeichert und das Gerät wird ausgeschaltet. • **Herunterfahren**: Das Gerät fährt herunter. Geöffnete Apps und Dateien werden ohne Speichern geschlossen.
Bei Betätigung der Standbytaste	• **Keine Aktion durchführen**: Das Gerät bleibt eingeschaltet und nutzt weiterhin die externe Energiequelle. • **Standbymodus**: Das Gerät wechselt in den Standbymodus und verbraucht nur wenig Netzstrom. Der Computer bleibt eingeschaltet und Apps und Dateien werden im Arbeitsspeicher (RAM) gespeichert. • **Ruhezustand**: Das Gerät wechselt in den Ruhezustand. Geöffnete Apps und Dateien werden auf der Festplatte gespeichert und das Gerät wird ausgeschaltet. • **Herunterfahren**: Das Gerät fährt herunter. Geöffnete Apps und Dateien werden ohne Speichern geschlossen.
Hybrid-Standbymodus aktivieren	• **Wahr**: Die Geräte können in den Hybrid-Standbymodus wechseln. Geöffnete Apps und Dateien werden im Arbeitsspeicher und auf der Festplatte gespeichert. Das Gerät verbraucht nur wenig Netzstrom. • **Falsch**: Verhindert, dass die Geräte in den Hybrid-Standbymodus wechseln können.

macOS-Energiesparkonfiguration

Netzstrom-Energiespareinstellungen für Desktops

Konfigurieren Sie die Netzstrom-Energiespareinstellungen für ein macOS-Desktop-Gerät, indem Sie die folgenden Einstellungen festlegen:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Nach Stromausfall automatisch starten	Legen Sie fest, dass das Gerät nach einem Stromausfall automatisch startet.
Festplatte in den Ruhemodus versetzen nach	Markieren Sie das Kontrollkästchen, um die Festplatte nach einem festen Intervall zwischen 1 und 180 Minuten in den Ruhemodus zu versetzen. Der Wert "0 Minuten" bewirkt, dass die Festplatte nie in den Ruhemodus versetzt wird.
Bildschirm ausschalten nach	Markieren Sie das Kontrollkästchen, um den Bildschirm nach einem festen Intervall zwischen 1 und 180 Minuten auszuschalten. Der Wert "0 Minuten" bewirkt, dass der Bildschirm nie ausgeschaltet wird.
Dynamischer Energieschritt	Markieren Sie das Kontrollkästchen, um den dynamischen Energieschritt zu aktivieren.
Prozessorgeschwindigkeit reduzieren	Markieren Sie das Kontrollkästchen, um die Prozessorgeschwindigkeit zu verringern.
Computer in den Ruhemodus versetzen nach	Markieren Sie das Kontrollkästchen, um den Computer nach einem festen Intervall zwischen 1 und 180 Minuten in den Ruhemodus zu versetzen. Der Wert "0 Minuten" bewirkt, dass der Computer nie in den Ruhemodus versetzt wird.
Für Netzwerkzugriff reaktivieren	Markieren Sie das Kontrollkästchen, um den Computer für Netzwerkzugriff zu reaktivieren.
Für Modemanruf reaktivieren	Markieren Sie das Kontrollkästchen, um den Computer für Modemanrufe zu reaktivieren.

Einstellungen für den Zeitplan, nach dem der Computer startet oder herunterfährt

Verwenden Sie die folgenden Einstellungen, um die macOS-Geräte für geplantes Starten oder Herunterfahren zu konfigurieren.

Deaktivieren der Geräteeinstellungen

Markieren Sie das Kontrollkästchen **Gerät ausschalten**, um die Geräte in bestimmten Intervallen herunterzufahren.

Einstellung	Beschreibung
Ereignistyp	Wählen Sie einen der Ereignistypen aus der Dropdownliste aus: • Ruhemodus • Neustart • Herunterfahren
Wann	Wählen Sie einen oder mehrere Wochentage aus, um einen Ereignistyp zu planen.
Um	Wählen Sie die Uhrzeit aus, um einen Ereignistyp zu planen.

Starten oder Reaktivieren der Geräteeinstellungen

Markieren Sie das Kontrollkästchen **Gerät starten oder reaktivieren**, um die Geräte in bestimmten Intervallen zu reaktivieren.

Einstellung	Beschreibung
Ereignistyp	Wählen Sie einen der Ereignistypen aus der Dropdownliste aus: • Reaktivieren • Starten/Reaktivieren
Wann	Wählen Sie einen oder mehrere Wochentage aus, um einen Ereignistyp zu planen.
Um	Wählen Sie die Uhrzeit aus, um einen Ereignistyp zu planen.

Netzstrom-Energiespareinstellungen für Laptops

Konfigurieren Sie die Netzstrom-Energiespareinstellungen für ein macOS-Laptop-Gerät, indem Sie die folgenden Einstellungen festlegen:

Einstellung	Beschreibung
Nach Stromausfall automatisch starten	Legen Sie fest, dass das Gerät nach einem Stromausfall automatisch startet.
Festplatte in den Ruhemodus versetzen nach	Markieren Sie das Kontrollkästchen, um die Festplatte nach einem festen Intervall zwischen 1 und 180 Minuten in den Ruhemodus zu versetzen. Der Wert "0 Minuten" bewirkt, dass die Festplatte nie in den Ruhemodus versetzt wird.
Bildschirm ausschalten nach	Markieren Sie das Kontrollkästchen, um den Bildschirm nach einem festen Intervall zwischen 1 und 180 Minuten auszuschalten. Der Wert "0 Minuten" bewirkt, dass der Bildschirm nie ausgeschaltet wird.
Dynamischer Energieschritt	Markieren Sie das Kontrollkästchen, um den dynamischen Energieschritt zu aktivieren.
Prozessorgeschwindigkeit reduzieren	Markieren Sie das Kontrollkästchen, um die Prozessorgeschwindigkeit zu verringern.
Laptop in Ruhezustand versetzen nach	Markieren Sie das Kontrollkästchen, um den Laptop nach einem festen Intervall zwischen 1 und 180 Minuten in den Ruhemodus zu versetzen. Der Wert "0 Minuten" bewirkt, dass der Laptop nie in den Ruhemodus versetzt wird.
Für Netzwerkzugriff reaktivieren	Markieren Sie das Kontrollkästchen, um den Laptop für Netzwerkzugriff zu reaktivieren.
Für Modemanruf reaktivieren	Markieren Sie das Kontrollkästchen, um den Laptop für Modemanrufe zu reaktivieren.

Energiespareinstellungen für die Laptop-Batterie

Konfigurieren Sie die Batterie-Energiespareinstellungen für ein macOS-Laptop-Gerät, indem Sie die folgenden Einstellungen festlegen:

Einstellung	Beschreibung
Nach Stromausfall automatisch starten	Legen Sie fest, dass das Gerät nach einem Stromausfall automatisch startet.
Festplatte in den Ruhemodus versetzen nach	Markieren Sie das Kontrollkästchen, um die Festplatte nach einem festen Intervall zwischen 1 und 180 Minuten in den Ruhemodus zu versetzen. Der Wert "0 Minuten" bewirkt, dass die Festplatte nie in den Ruhemodus versetzt wird.
Bildschirm ausschalten nach	Markieren Sie das Kontrollkästchen, um den Bildschirm nach einem festen Intervall zwischen 1 und 180 Minuten auszuschalten. Der Wert "0 Minuten" bewirkt, dass der Bildschirm nie ausgeschaltet wird.
Dynamischer Energieschritt	Markieren Sie das Kontrollkästchen, um den dynamischen Energieschritt zu aktivieren.
Prozessorgeschwindigkeit reduzieren	Markieren Sie das Kontrollkästchen, um die Prozessorgeschwindigkeit zu verringern.
Computer in den Ruhemodus versetzen nach	Markieren Sie das Kontrollkästchen, um die Laptop-Batterie nach einem festen Intervall zwischen 1 und 180 Minuten in den Ruhemodus zu versetzen. Der Wert "0 Minuten" bewirkt, dass die Laptop-Batterie nie in den Ruhemodus versetzt wird.
Für Netzwerkzugriff reaktivieren	Markieren Sie das Kontrollkästchen, um die Laptop-Batterie für Netzwerkzugriff zu reaktivieren.
Für Modemanruf reaktivieren	Markieren Sie das Kontrollkästchen, um die Laptop-Batterie für Modemanrufe zu reaktivieren.

10.10.8.18. Ethernet-Konfiguration (macOS)

Lizenz: Gold

Gilt für: macOS 10.13+ oder unterstützte neuere Versionen.

Der Administrator kann die Ethernet-Schnittstelle in verschiedenen Varianten konfigurieren. Für die Konfiguration des Ethernets stehen folgende Payloads zur Verfügung:

- Globales Ethernet
- Erstes aktives Ethernet
- Erstes Ethernet
- Zweites aktives Ethernet
- Zweites Ethernet
- Drittes aktives Ethernet
- Drittes Ethernet

> Die verschiedenen Payloads zur Konfiguration des Ethernets sind Allgemeiner Standard-Fallback sowie erste, erste aktive, zweite, zweite aktive, dritte und dritte aktive Ethernet-Schnittstelle. Apple hat ein bekanntes Problem mit der Installation der ersten, ersten aktiven, zweiten, zweiten aktiven, dritten und dritten aktiven Ethernet-Schnittstelle.

Ethernet-Konfiguration

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie **Ethernet** in das Suchfeld ein und wählen Sie dann **Ethernet**-Konfiguration aus.
4. Geben Sie einen Namen ein und beschreiben Sie die Konfiguration.
5. Wählen Sie das Konfigurations-Setup aus der Dropdownliste aus.
6. Geben Sie die Ethernet-Konfigurationseinstellungen ein.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie die Option **Diese Konfiguration aktivieren**.
9. Wählen Sie eine der folgenden Kanaloptionen, um die Konfiguration zu übernehmen:
    - Gerätekanal (am häufigsten)
    - Benutzerkanal (aktuell registrierter Benutzer)
10. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
11. Klicken Sie auf **Fertig**.

Ethernet-Konfigurationseinstellungen

Verwenden Sie die Einstellungen in der folgenden Tabelle, um Ethernet zu konfigurieren. Weitere Informationen zu diesen Einstellungen finden Sie in der **Apple-Dokumentation**.

Einstellung	Beschreibung
Protokolle	
Akzeptierte EAP-Typen	Bestimmen Sie die EAP-Typen, die für den Zugriff auf dieses Netzwerk verwendet werden können: • Transport Layer Security(TLS): TLS ist ein Protokoll, das eine verschlüsselte Sitzung zwischen zwei Computern im Internet aufbaut. Es verifiziert die Identität des Servers und verhindert, dass Hacker Daten abfangen können. • TTLS - Wählen Sie im Feld **Innere Identität** eines der Authentifizierungsprotokolle aus, z. B. OS Default, PAP, CHAP, MSCHAP, MSCHAPv2 und EAP. • PEAP • LEAP • EAP-SIM: Wählen Sie im Feld **EAP SIM-Nummer der RANDs** die Anzahl der RANDs aus der Dropdown-Liste. • EAP-AKA • EAP-FAST: Wählen Sie die Option EAP-FAST, die Authentifizierungsmethoden definiert: ◦ **PAC verwenden**:Wählen Sie diese Option, um eine Proxy-Autokonfiguration (PAC) zu verwenden. ◦ **PAC bereitstellen**: Wählen Sie diese Option, um die Bereitstellung eines PACs zu erlauben. Ansonsten kann nur eine bereits auf dem Geräts zur Verfügung gestellte PAC verwendet werden. Diese Option ist nur verfügbar, wenn Sie „PAC verwenden“ ausgewählt haben. ◦ **PAC anonym bereitstellen**: Wählen Sie diese Option, damit ein PAC ohne Authentifizierung des Servers bereitgestellt werden darf. Die Option ist nur verfügbar, wenn Sie „PAC zur Verfügung stellen“ ausgewählt haben
Authentifizierung	**Benutzername**: Geben Sie den für den Netzwerkzugriff erforderlichen Benutzernamen an. Wenn Sie dieses Feld leer lassen, wird der Benutzer aufgefordert, es auszufüllen. • Passwort pro Verbindung verwenden: Wählen Sie diese Option, um den Gerätebenutzer für jede Verbindung zur Eingabe eines Passworts aufzufordern. Wenn das Gerät demselben Netzwerk wieder beitritt, wird der Gerätebenutzer aufgefordert, sich erneut für das Netzwerk zu authentifizieren. Bei jedem Verbindungsaufbau wird das Passwort abgefragt. • Passwort bei Verbindung zum Netzwerk nur einmal abfragen: Das Passwort wird nur einmal abgefragt, wenn die Konfiguration auf das Gerät übertragen wird. Bei einem Verbindungsauf- und -abbau im Netzwerk wird kein Passwort abgefragt. **Passwort**: (Optional) Geben Sie das Passwort für den Zugriff auf dieses Netzwerk ein. Ansonsten wird der Benutzer zur Eingabe eines Passworts für den Netzwerkzugriff aufgefordert. **Äußere Identität**: (Optional) Wählen Sie für TTLS, PEAP und EAP-FAST aus, dass Gerätebenutzer ihre Identität verbergen können. Der richtige Name des Benutzers wird nur in dem verschlüsselten Tunnel angezeigt. Diese Option kann die Sicherheit erhöhen, da ein Angreifer den Namen des authentifizierenden Benutzers nicht als Klartext erkennen kann. **Systemmodus - Identität der Quelle der Anmeldeinformationen**: Zur Computerauthentifizierung wird der Systemmodus verwendet. Die Authentifizierung über den Systemmodus erfolgt, bevor sich ein Benutzer am Computer anmeldet. Der Systemmodus wird in der Regel so konfiguriert, dass eine Authentifizierung mit dem X.509-Zertifikat des Computers (EAP-TLS) erfolgt, das von einer lokalen Zertifizierungsstelle ausgestellt wurde.

Einstellung	Beschreibung
Vertrauensstatus	**Vertrauenswürdige Zertifikate:** Markieren Sie die jeweiligen Kontrollkästchen, um mehrere Zertifikate aus der Liste auszuwählen. **Vertrauenswürdige Serverzertifikatsnamen**: Fügen Sie den Namen des Zertifikats hinzu. • **Vertrauensausnahmen zulassen**: Lassen Sie Vertrauensentscheidungen (über Dialogfeld) durch den Benutzer zu. • **TLS-Zertifikat anfordern** **Maximal zulässige TLS-Version bei EAP-Authentifizierung** **Minimal zulässige TLS-Version bei EAP-Authentifizierung** **vertrauenswürdige TLS-Zertifikate: MobileIron Agent CA-Zertifikat**

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.8.19. Google BeyondCorp-Konfiguration

Ivanti Neurons for MDM kann für bedingten Zugriff in Google BeyondCorp integriert werden. Ivanti Neurons for MDM sendet ein Statussignal für die Geräte-Compliance an Google BeyondCorp. Dadurch wird sichergestellt, dass nur kompatible Geräte unter N-MDM auf Google-Workspace-Anwendungen zugreifen können.

Gilt für:

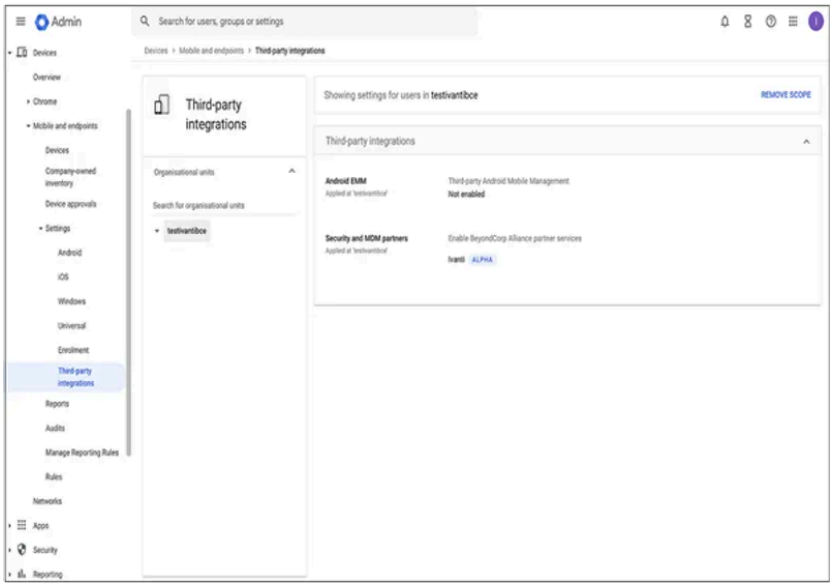
- iOS-
- Android
- Windows

Voraussetzungen

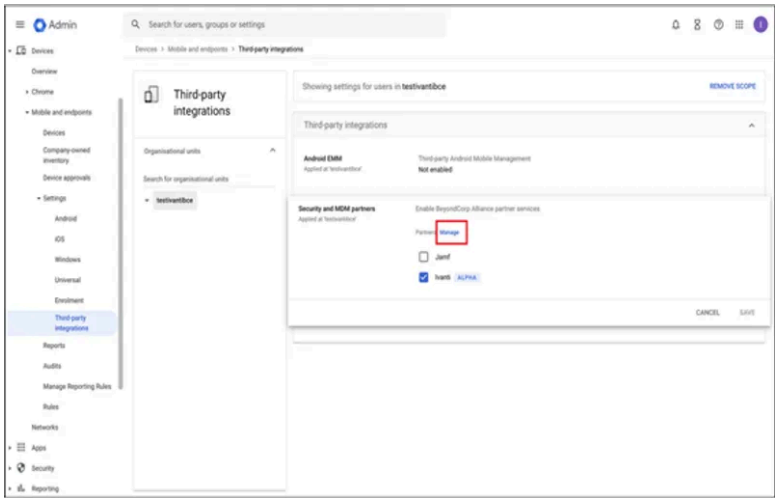
- Für Ivanti Neurons for MDM benötigen Sie eine Lizenz vom Typ Ivanti Professional Plus/Premium.
- Für Google benötigen Sie die Lizenz BeyondCorp Enterprise, Google Workspace Enterprise oder Cloud Identity Premium.
- Für Windows muss Folgendes auf dem Gerät installiert sein:
  - Ivanti Bridge
  - Google Chrome

Verfahren (Google)

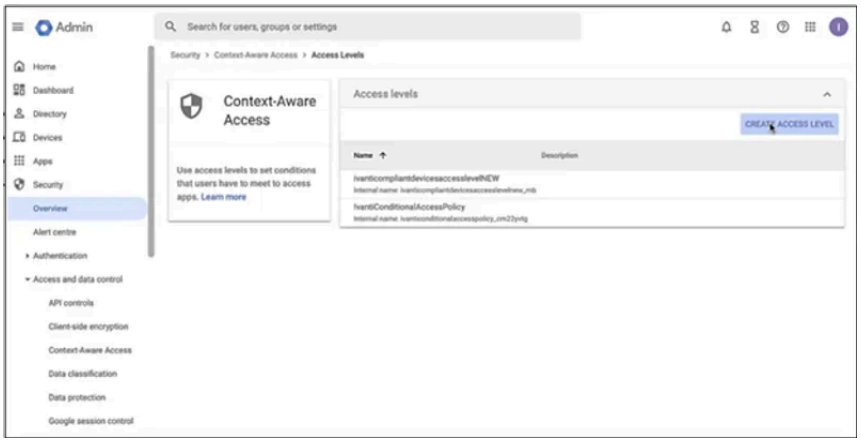
1. Melden Sie sich mit Administrator-Anmeldeinformationen bei der **Google Admin Console** an.
2. Wechseln Sie zu **Geräte** > **Mobilgeräte und Endpunkte** > **Einstellungen** > **Integrationen von Drittanbietern**.



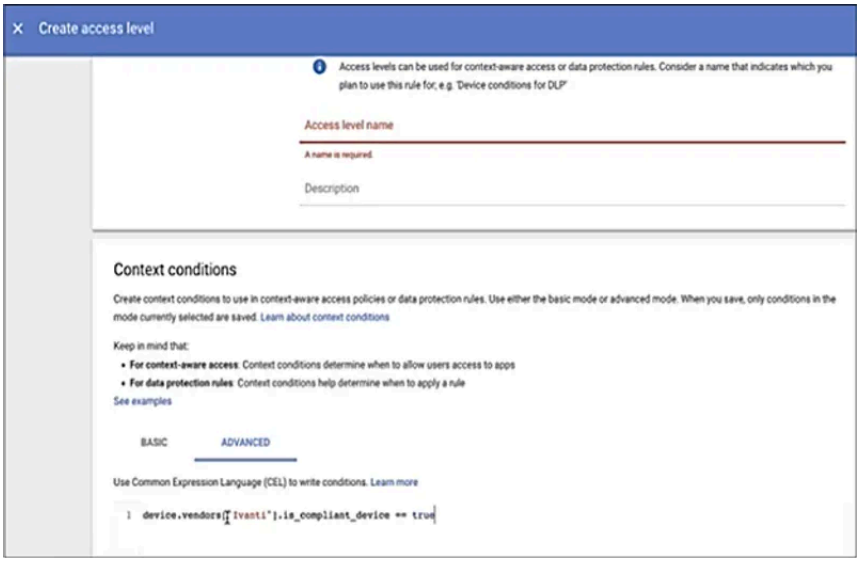
3. Klicken Sie auf **Partner für Sicherheit und Mobilgeräteverwaltung** > **Verwalten**.



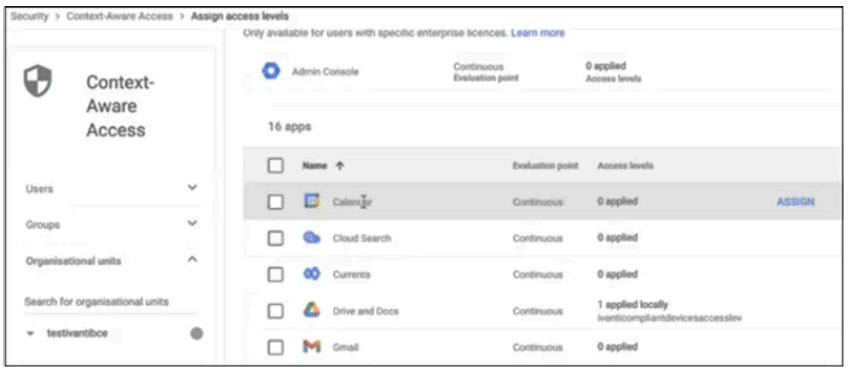
4. Wählen Sie im Fenster **Partnerverbindungen verwalten** den Eintrag **Ivanti** aus.
5. Klicken Sie auf **Verbindung öffnen**.
   Sie werden zurück zur Ivanti Neurons for MDM-Anmeldeseite geleitet. Geben Sie die Administrator-Anmeldeinformationen für den Mandanten ein. Nachdem Sie sich beim Mandanten angemeldet haben, werden Sie feststellen, dass **Google BeyondCorp** aktiviert und direkt mit Ihrem Google-Konto verknüpft wurde.
6. Wechseln Sie in der Google Admin Console zu **Sicherheit** > **Kontextsensitiver Zugriff** > **Zugriffsebenen**.



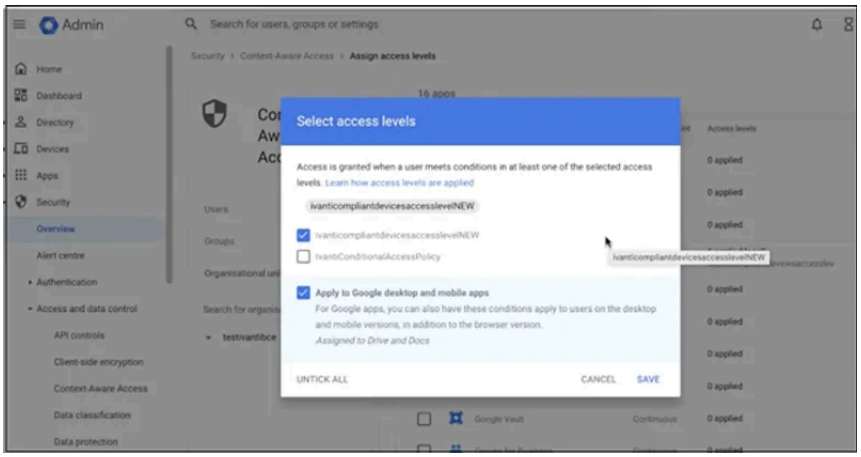
7. Klicken Sie auf **Zugriffsebene erstellen**.
   Klicken Sie im Fenster "Zugriffsebene erstellen" unter dem Abschnitt mit den Kontextbedingungen auf **ERWEITERT** und machen Sie die erforderlichen Angaben.



8. Wechseln Sie zu **Sicherheit** > **Kontextsensitiver Zugriff** > **Zugriffsebene** und wählen Sie die Anwendung aus, der Sie die Richtlinie zuweisen möchten.



9. Klicken Sie auf **Zuweisen**.
10. Wählen Sie im Fenster **Zugriffsebenen auswählen** die zuzuweisenden Richtlinien aus und klicken Sie auf **Speichern**.



Sobald die Einrichtung oben abgeschlossen ist, können Sie die Konfiguration für die Partnergeräte-Compliance mithilfe von **Google BeyondCorp** erstellen.

Verfahren (Ivanti Neurons for MDM**)**:

1. Wechseln Sie zu **Konfigurationen** > **Konfiguration hinzufügen**.
2. Wählen Sie die Konfiguration **Compliance von Partnergeräten** aus.
3. Die Konfigurationsseite "Compliance von Partnergeräten erstellen" wird angezeigt.
   Geben Sie einen Namen für die Konfiguration ein.
4. Wählen Sie in der Liste "Partner wählen" den Eintrag **Google BeyondCorp** aus.
5. Der Abschnitt "Einrichtung der Konfiguration" wird angezeigt. Stellen Sie sicher, dass die Option "Compliance-Status für iOS- und Android-Geräte melden" auf EIN steht.
   Klicken Sie auf **Weiter**.
6. Wählen Sie **Diese Konfiguration aktivieren** aus.
7. Wählen Sie **Benutzerdefiniert** als Verteilungsoption aus.
8. Wählen Sie bei **Benutzerdefinierte Verteilung** die Option **Benutzer/Benutzergruppen** aus.
9. Wählen Sie im Abschnitt **Wählen Sie unten die Optionen zur Verteilung dieser Konfiguration aus** die Benutzer/Benutzergruppen aus der Liste aus.
10. Klicken Sie auf **Fertig**.

Google BeyondCorp Server kann jedes Gerät über die von der App verwaltete P-Liste eindeutig identifizieren.



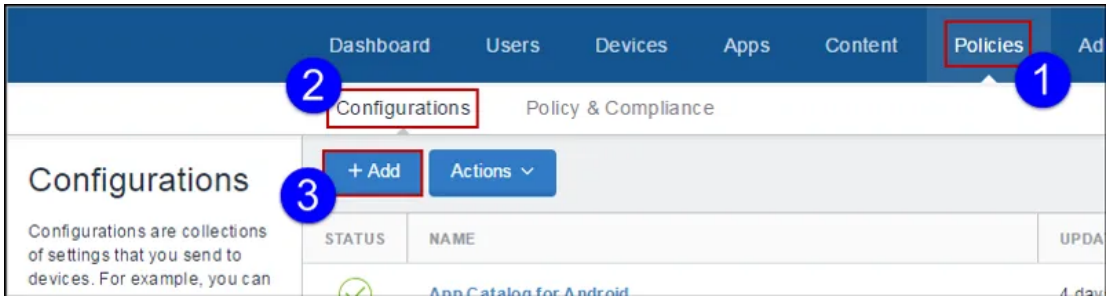
10.10.8.20. Sperrbildschirm-Nachricht - Konfiguration

Zeigt eine Meldung und Tag-Informationen des Geräts auf den Anmelde- und Sperrbildschirmen an. Dies gilt für überwachte Geräte mit iOS 9.3 oder unterstützten neueren Versionen.

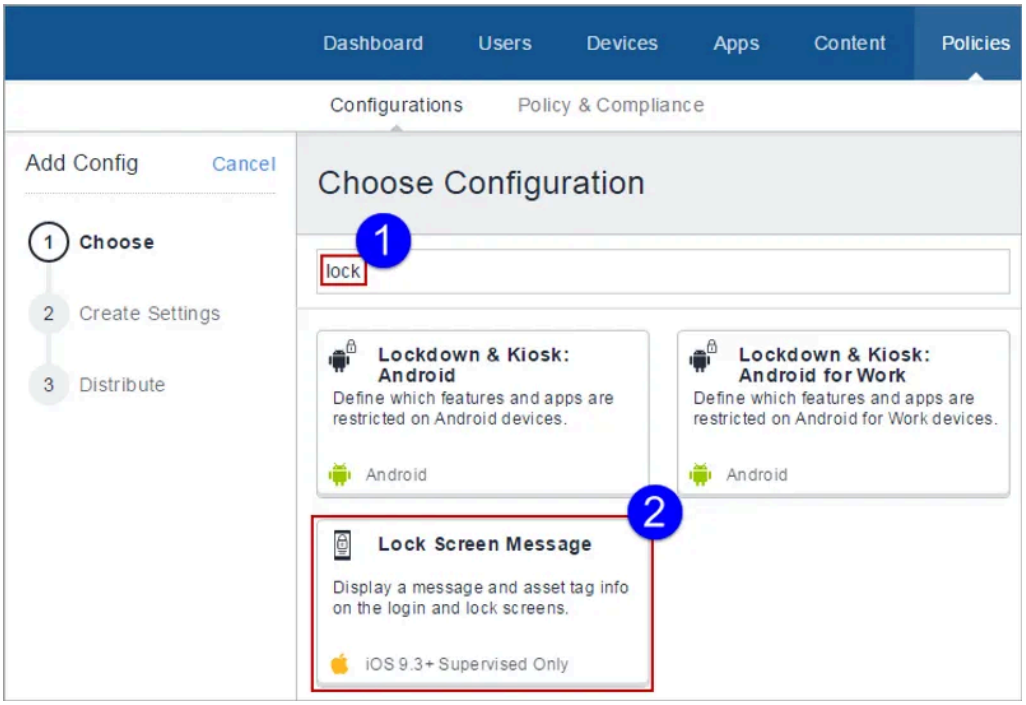
Erstellen einer Konfiguration der Sperrbildschirm-Nachricht

Verfahren

1. Klicken Sie auf **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.



Tippen Sie in dem Suchfeld**lock** ein und klicken Sie dann auf die Konfigurationsoption **Sperrbildschirm-Nachricht:**



Die Seite mit den Konfigurationsdetails der Sperrbildschirm-Nachricht wird angezeigt.
Konfigurieren Sie die Einstellungen auf dieser Seite. Hinweise zu den Werten finden Sie in der Tabelle im Abschnitt [Konfigurationseinstellungen für die Sperrbildschirm-Meldung](#).

5. Klicken Sie auf **Weiter**, um die Verteilungseinstellungen zu konfigurieren und dann auf **Fertig**.

Sperrbildschirm-Nachricht – Konfigurationseinstellungen

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Fußnote zum Sperrbildschirm	Dieser Text erscheint im Anmeldefenster und Sperrbildschirm.
Asset-Tag-Informationen	Dieser Text erscheint am unteren Rand des Anmeldefensters und Sperrbildschirms.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.8.21. Konfiguration des Anmeldefensters – macOS

Verfahren

1. Melden Sie sich bei Ivanti Neurons for MDM an.
2. Wechseln Sie zu **Konfigurationen** > **Konfiguration hinzufügen**.
3. Wählen Sie bzw. klicken Sie auf **Anmeldefenster**.
4. Geben Sie in das Feld **Name** einen Namen für die Konfiguration des Anmeldefensters ein.
5. Klicken Sie auf **+ Beschreibung hinzufügen**, um Details hinzuzufügen.
6. Füllen Sie im Abschnitt **Konfigurations-Setup** folgende Felder aus:
   - **Admin-Hostinfo**: Geben Sie den Hostnamen oder die IP-Adresse oder die Systemversion ein.
   - **Zulassungsliste**: Liste der Benutzer-GUIDs oder Benutzergruppen-GUIDs, deren Anmeldung das System zulässt. Ein Sternchen ('*') steht für alle Benutzer oder alle Gruppen.
   - **Kennwort für automatische Anmeldung**: Geben Sie das Kennwort für die automatische Anmeldung ein.
   - **Verweigerungsliste**: Liste der Benutzer-GUIDs oder Benutzergruppen-GUIDs, deren Anmeldung das System nicht zulässt. Diese Liste hat Vorrang gegenüber der Liste im Schlüssel 'AllowList'.
   - **Text für Anmeldefenster**: Geben Sie den Text für das Anmeldefenster ein.
   - Markieren Sie das Kontrollkästchen für zusätzliche Optionen wie:
     - **Konsolenzugriff deaktivieren**
     - **Automatische FDE-Anmeldung deaktivieren (FileVault-Festplattenverschlüsselung)**
     - **Funktionen für sofortige Bildschirmsperre deaktivieren**
     - **Administratoren beim Anzeigen von Benutzerlisten ausblenden**
     - **Nur Netzwerk- und Systembenutzer anzeigen**
     - **Mobile Konten ausblenden**
     - **Netzwerkbenutzer anzeigen**
     - **Menüpunkt "Abmeldung" deaktivieren**
     - **Ausschalten deaktivieren, wenn Benutzer angemeldet ist**
     - **Menüpunkt "Neustart" deaktivieren, wenn Benutzer angemeldet ist**
     - **Element "Neustart" deaktivieren**
     - **Dialogfeld für Name und Kennwort anzeigen**
     - **Andere Benutzer anzeigen – verwaltet**
     - **Eingabemenü anzeigen**
     - **Schaltfläche "Herunterfahren" deaktivieren**
     - **Schaltfläche "Energie sparen" deaktivieren**
     - **Schaltfläche "Herunterfahren" deaktivieren**
7. Klicken Sie auf **Fertig**.

10.10.8.22. macOS Systemerweiterungskonfiguration

Die Konfiguration der Systemerweiterung ermöglicht die Installation von Erweiterungstypen wie Treibererweiterung, Netzwerkerweiterung und Endpunktsicherheitserweiterung ohne Zugriff auf die Kernel-Ebene.

Verfahren

Gilt für: macOS 10.15+

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Geben Sie in dem Suchfeld **extension** ein und klicken Sie dann auf die Konfiguration **Systemerweiterungen**.
3. Geben Sie einen **Namen** und eine **Beschreibung** der Konfiguration ein.
4. Unter **Erlaubte Systemerweiterungen**, ergänzen Sie mit **+Hinzufügen Erlaubte Teamidentifikatoren** und **Erlaubte Systemerweiterungen**.
5. Unter **Zulässige Systemerweiterungsarten** ergänzen Sie mit **+Hinzufügen Erlaubte Teamidentifikatoren** und **Erlaubte Systemerweiterungen**.
6. Markieren Sie die Option **Benutzerüberschreibungen zulassen**.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie die Option **Diese Konfiguration aktivieren**.
9. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
10. Klicken Sie auf **Fertig**.

> Bei macOS 12 ermöglicht RemovableSystemExtensions der Anwendung, die Systemerweiterung zu deaktivieren, ohne dass bei der Deinstallation der Anwendung die Genehmigung des Administrators erforderlich ist.

10.10.8.23. MAM-Only

Ivanti Neurons for MDM bietet Ihnen die Möglichkeit, iOS- und Android-Geräte als reine MAM-Bereitstellung zu definieren und ihnen damit Mobile App Management (MAM) zur Verfügung zu stellen. Eine reine MAM-Bereitstellung ermöglicht es Ihnen, Apps zu verteilen und zu verwalten, ohne dass Sie das Gerät selbst verwalten müssen.

MAM-Only-Lösung – Alternative für Ivanti AppStation

Als alternative Lösung für Ivanti AppStation bietet Ivanti eine moderne und flexible MAM-Lösung (Mobile Application Management) an, die auf dem Ivanti Go-Client basiert und für iOS- und Android-Plattformen verfügbar ist.

Die neue MAM-Only-Lösung bietet einen integrierten App-Katalog mit Ivanti Neurons for MDM Web Clip-Funktionalität und erfüllt damit alle wesentlichen Anwendungsfälle, die bislang von AppStation abgedeckt wurden. Sie stellt sowohl Benutzern als auch Administratoren eine vereinfachte, sichere und einheitliche App-Verwaltung bereit.

Hauptmerkmale

- **Integrierter App-Katalog**: Hostet und verteilt genehmigte verwaltete Apps direkt innerhalb des Go-Clients.
- **App-Konfiguration und Updates**: Unterstützt Konfigurations- und Versionsupdates auf Anwendungsebene, die durch MAM-Richtlinien verstärkt wurden.
- Ivanti Neurons for MDM **Anforderung**: Ideal für BYOD- und Vertragspartnerszenarien, in denen eine Ivanti Neurons for MDM-Registrierung nicht möglich ist.

Verwendung von Web Clip für einfachen Zugriff

- **Direkter Zugriff auf den App-Katalog**: Bereitstellung von Web Clips via Ivanti Neurons for MDM zur Bereitstellung einer Verknüpfung zum App-Katalog oder bestimmten webbasierten Unternehmens-Apps.
- **Benutzerdefinierte App-Verknüpfungen**: Ermöglicht Benutzern das schnelle Aufrufen häufig genutzter Ressourcen über die Startseite.

Verbesserte Erfahrung für Administratoren und Benutzer

- **Einheitliche Oberfläche**: App-Katalog, Web Access und Compliance Messaging sind auf einer Schnittstelle zusammengefasst.
- **Vereinfachte Administration**: Macht separate Lösungen (hier AppStation) überflüssig und reduziert somit die Komplexität und das Risiko von Konfigurationsabweichungen.

Flexibilität und Anpassung

- **Anpassung der Katalogansichten**: Die Inhalte des App-Katalogs lassen sich nach Benutzerrolle, Region oder Organisationseinheit anpassen.
- **Nutzung der vorhandenen Infrastruktur**: Nutzt Ihre vorhandene Ivanti Neurons for MDM/MAM-Investition (keine separate Infrastruktur erforderlich).

Unterstützung für Benutzer mit Doppelrolle

Die Ivanti MAM-Only-Lösung ist darauf ausgelegt, moderne Arbeitsszenarien zu unterstützen, darunter auch Benutzer mit Doppelrolle:

- **Vollzeitbeschäftigter – Org. A**: Zugriff auf Unternehmens-Apps via Webclip (z. B. Apps@Work), bereitgestellt über Ivanti Neurons for MDM.
- **Vertragspartner – Org. B**: Verwendung von Ivanti Go Client im MAM-Only-Modus für sicheren Zugriff auf verwaltete Apps, ohne die Geräteregistrierung in Ivanti Neurons for MDM anzufordern.

Dies ermöglicht einen nahtlosen rollenbasierten Zugriff auf benötigte Apps, ohne Profilkonflikte oder Überlappung der Geräteverwaltung.

Migrationsanleitung

Ivanti empfiehlt Kunden von AppStation dringend, ihre Migration zur Go Client-basierten MAM-Only-Lösung zu planen und durchzuführen. Schrittweise Migrationsanleitungen finden Sie in den folgenden Ressourcen:

- Ivanti MAM-Only-Lösung
- **App-Katalog-Konfiguration in Go Client**
- **Erstellen einer Web-Clip-Konfiguration**

Wenn Sie Fragen zur Migration haben oder Unterstützung benötigen, wenden Sie sich bitte an den **Ivanti Support** oder Ihren Customer Success Manager.

10.10.8.24. Verwaltete Google Play-Konfiguration

Administratoren können die Einstellung für automatische Updates konfigurieren, die Google Play Store zum Aktualisieren von Apps auf dem Android Enterprise-Gerät verwendet.

Einstellungen für automatische Updates konfigurieren:

1. Gehen Sie zu **Konfiguration > +Hinzufügen**.
2. Wählen Sie die **Verwaltete Google Play**-Konfiguration.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Wählen Sie im Abschnitt Konfigurationseinstellungen eine Option zur Aktualisierung von Apps in Google Play.

Einstellung	Aktion
Benutzerdefiniert	Der Gerätebenutzer kann in dem Wartungsfenster für die automatische Aktualisierung von Anwendungen festlegen, wann die Anwendungen aktualisiert werden sollen. 1. Wählen Sie im Feld **Startzeit** aus, wann die Aktualisierung der Anwendung durchgeführt werden soll. 2. Wählen Sie im Feld **Dauer** den Zeitraum (in Stunden) aus, in dem die Aktualisierung durchgeführt werden soll. Der Zeitraum liegt zwischen 1 Stunde und 24 Stunden. Die Apps können nach der Startzeit jederzeit während der gewählten Frist aktualisiert werden. Wenn beispielsweise die 'Startzeit' auf 18 Uhr und die 'Dauer' auf 12 Stunden eingestellt ist, können die Apps jederzeit zwischen 18 Uhr und 6 Uhr aktualisiert werden.
Keine	Der Google Play Store aktualisiert Apps auf dem Gerät niemals automatisch.
Nur WLAN	Google Play Store aktualisiert Apps auf dem Gerät automatisch, jedoch nur über WLAN- und nicht über Mobilfunkverbindungen.
Immer	Der Google Play Store aktualisiert Apps auf dem Gerät automatisch über WLAN- oder Mobilfunkverbindungen.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:

- Alle Geräte
- Keine Geräte (Standard)
- Anpassbar

8. Klicken Sie auf **Fertig**.

10.10.8.25. Einstellungen für den Migrationsassistenten

Verwenden Sie **Einstellungen für Migrationsassistent**, um die Einstellungen des Migrationsassistenten auf überwachten Geräten zu konfigurieren. Diese Konfiguration hilft Administratoren, konsistente, richtlinienbasierte Kontrollen anzuwenden, die steuern, wie Benutzer Daten, Apps und Einstellungen während der Geräteeinrichtung oder Migration übertragen.

Gilt für:

- macOS 26.4+ überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Einstellungen für Migrationsassistent** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie die **Einstellungen für Migrationsassistent** gemäß der folgenden Tabelle:

Einstellung	Aktion
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Sollte verwaltete Migration durchführen	Aktivieren Sie das Kontrollkästchen, um die Migration von Geräten zu aktivieren und zu verwalten. Schalten Sie die Option **Via Push an das Gerät senden** um, um die Gerätemigration zu aktivieren.
Ausgeschlossene Konten	Geben Sie die Namen der Konten ein, die Sie von der Migration ausschließen möchten. Schalten Sie die Option **Via Push an das Gerät senden** um, um den Ausschluss von Konten zu aktivieren.
Ausgeschlossene Pfade	Geben Sie die Namen der Pfade ein, die Sie von der Migration ausschließen möchten. Schalten Sie die Option **Via Push an das Gerät senden** um, um den Ausschluss von Pfaden zu aktivieren.
Erforderliche Pfade	Geben Sie die Namen der Pfade ein, die Sie in die Migration einschließen möchten. Schalten Sie die Option **Via Push an das Gerät senden** um, um den Einschluss von Pfaden zu aktivieren.
Sollte Datenschutz-Sicherheitseinstellungen migrieren	Aktivieren Sie das Kontrollkästchen, um die Migration von Datenschutz-Sicherheitseinstellungen von Geräten zu aktivieren. Schalten Sie die Option **Via Push an das Gerät senden** um, um die Migration von Datenschutz-Sicherheitseinstellungen zu aktivieren.

4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
5. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Einstellungen für Migrationsassistent** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
6. Klicken Sie auf **Fertig**.

10.10.8.26. Konfiguration "Benachrichtigungen"

Mit der Konfiguration "Benachrichtigungen" können Administratoren stille und sichtbare Benachrichtigungen für iOS-Geräte planen. Die Konfiguration "Benachrichtigungen" kann auch geklont, exportiert oder gelöscht werden.

Verfahren

1. Gehen Sie zu **Konfiguration > +Hinzufügen**.
2. Wählen Sie die Konfiguration **Benachrichtigungen** aus.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Wählen Sie im Abschnitt "Konfiguration einrichten" eine oder beide Optionen für die **Benachrichtigungsplanung** aus:
    - Stille Benachrichtigungsplanung – Stille Benachrichtigungen werden verwendet, um Geräteverwaltungsvorgänge im Hintergrund zu unterstützen, die von Ivanti Neurons for MDM initiiert wurden. Sie ermöglichen automatisierte Aktionen wie Compliance-Prüfungen, Richtlinienaktualisierungen und App-Updates, ohne dass ein Benutzereingriff erforderlich ist. Ivanti Neurons for MDM sendet stille Benachrichtigungen an das Gerät auf der konfigurierten Ebene.
    - Sichtbare Benachrichtigungsplanung – Sichtbare Benachrichtigungen werden verwendet, wenn die Information an den Benutzer oder eine Aktion erforderlich ist, um die Compliance, Sicherheit oder Funktionalität des Geräts aufrechtzuerhalten. Sichtbare Benachrichtigungen werden erst nach dem angegebenen Intervall ausgelöst, auch wenn mehrere Aktionen oder Ereignisse während dieses Zeitraums auftreten. Eine sichtbare Benachrichtigung wird nur dann auf dem Gerät angezeigt, wenn während des sichtbaren Benachrichtigungsintervalls keine stille Benachrichtigung gesendet wurde.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
8. Klicken Sie auf **Fertig**.

Sichtbarer Benachrichtigungsinhalt für MTD-Geräte – Ihr Gerät ist möglicherweise anfällig für Bedrohungen. Starten Sie die Ivanti Go-Anwendung und überprüfen Sie den Threat Defense-Status.

Sichtbarer Benachrichtigungsinhalt für Nicht-MTD-Geräte – Um verbesserte Sicherheitsfunktionen zu erhalten und die neuesten Schutzmaßnahmen zu gewährleisten, starten Sie die App auf Ihrem Gerät.

10.10.8.27. Druckereinstellungen

In der Cloud können Sie Druckerprofile erstellen und zu Geräten hinzufügen. Diese Funktion erfordert Bridge. Details finden Sie unter **Bridge**.

> Wenn das Druckerprofil an das Gerät gesendet wird, muss der Drucker aktiv sein, sonst kann das Gerät ihn nicht erkennen.

Konfiguration der Druckereinstellungen für ein Windows-Gerät festlegen:

1. Gehen Sie zu Konfiguration > +Hinzufügen.
2. Wählen Sie die Konfiguration **Druckereinstellungen** aus.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Klicken Sie auf das Symbol **Windows**.
5. In dem Abschnitt **Konfigurations-Setup** konfigurieren Sie folgende Einstellungen:

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Windows-Druckereinstellungen	
Freigegebener Drucker	Wenn Sie die Option **Freigegebener Drucker** auswählen, wird der Drucker für andere Geräte freigegeben. Konfigurieren Sie die folgenden Felder: **Name**: Geben Sie den Namen für die Druckerkonfiguration ein. **Beschreibung**: Geben Sie eine Beschreibung des Druckers ein. **Druckerserver**: Geben Sie die IP-Adresse des Druckerservers ein. **Name des freigegebenen Druckers**: Geben Sie den Druckernamen ein.
Netzwerkdrucker	Wenn die Option **Netzwerkdrucker** ausgewählt ist, kann der Drucker nur von Geräten im gleichen Netzwerk erreicht werden. Konfigurieren Sie die folgenden Felder: **Name**: Geben Sie den Namen der Druckerkonfiguration ein. **Beschreibung**:Geben Sie eine Beschreibung des Druckers ein. **Druckername**: Geben Sie den Namen des Druckers im Netzwerk ein. **Drucker-Hostadresse**: Geben Sie die Host-IP-Addresse des Druckers ein. **Drucker-Portnummer**: Wählen Sie die Port-Nummer des Netzwerkdruckers. **Druckertreibername**: Geben Sie den Namen des Druckers ein. **Druckertreiber-URL**: Geben Sie die URL für den Druckertreiber ein. Laden Sie für den Druckertreiber ein ZIP-Archiv mit den erforderlichen Dateien hoch. Folgende Dateien müssen in diesem ZIP-Archiv enthalten sein: • .inf-Datei (Treiberinformationen) • .cat-Datei (Katalog/Signatur) • Zusätzliche Treiberbinärdateien, die in der INF referenziert werden INF (z. B. .dll, .sys usw.)

6. Klicken Sie auf Weiter.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:

- Alle Geräte
- Keine Geräte (Standard)
- Anpassbar

8. Klicken Sie auf **Fertig**.

Konfiguration der Druckereinstellungen für ein macOS-Gerät festlegen:

1. Gehen Sie zu **Konfiguration > +Hinzufügen** .
2. Wählen Sie die Konfiguration **Druckereinstellungen**.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Wählen Sie die entsprechende **macOS**- Option.
5. Nehmen Sie im Abschnitt **Druckerkonfiguration erstellen** die folgenden Einstellungen vor:

Einstellung	So gehen Sie vor
[Name] Beschreibung	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet. Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Konfigurations-Setup	Aktualisieren Sie die folgenden Felder, um den Drucker für macOS-Geräte zu konfigurieren: • Lokale Drucker zulassen • Standarddrucker-Anzeigename • Fußzeilen-Schriftart • Fußzeilen-Schriftgröße • Benutzer-Druckerliste • + Drucker hinzufügen

6. Klicken Sie auf Weiter
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:

- Alle Geräte
- Keine Geräte (Standard)
- Anpassbar

8. Klicken Sie auf **Fertig**.

10.10.8.28. Bloatware-Konfiguration entfernen

In der Konfiguration zur Entfernung von Bloatware können Sie die Liste der auf den Geräten installierten Anwendungen auswählen, die unbedingt entfernt werden müssen. Für diese Konfiguration benötigen Sie ein Setup für Bridge. Weitere Details finden Sie unter **Bridge**.

Apps starten oder deinstallieren:

1. Klicken Sie auf der Registerkarte **Konfiguration** auf **+Hinzufügen**.
2. Klicken Sie auf **Bloatware-Konfiguration entfernen**. Die Seite **Bloatware-Konfiguration entfernen** wird angezeigt.
3. Geben Sie in dem Feld **Name**die entsprechende Bezeichnung der Konfiguration ein.
4. Klicken Sie auf den Link + **Beschreibung hinzufügen** , um eine Beschreibung für die Konfiguration zu ergänzen. Dieses Feld ist optional.
5. Wählen Sie in dem Abschnitt mit dem **Konfigurations-Setup** die Apps aus, die entfernt oder deinstalliert werden sollen. Sie können nach einer App im Suchfeld auch mit dem App-Namen suchen, der in der Desktop-App-Liste angezeigt wird.

> Bevor Sie die Konfiguration Bloatware entfernen erstellen, sollten Sie Apps abrufen, indem Sie zu Apps>Desktop Apps>Apps holen gehen.Andernfalls stehen Ihnen beim Erstellen der Konfiguration für die Option Bloatware entfernen keine Anwendungen zur Verfügung, die Sie suchen oder auswählen können.

Die Dateien mit der Erweiterung .appx, .appxbundles, .xap und .msi können entfernt werden, nicht jedoch Dateien mit der Erweiterung .exe.

6. Konfigurieren Sie unter den erweiterten Optionen folgende Optionen:

Option	Beschreibung
Start dieser Konfiguration alle	Legen Sie fest, wie viele Minuten nach Ablauf des Intervalls die Konfiguration gestartet werden soll.
Start bei Anmeldung	Klicken Sie in das Kontrollkästchen, um die Konfiguration bei der Anmeldung zu starten.
Nach Deinstallation keinen Neustart erzwingen	Klicken Sie in das Kontrollkästchen, um einen Zwangsneustart nach Deinstallation der App zu verhindern.

10.10.8.29. Konfiguration "Safari-Erweiterung und -Einstellungen"

Safari-Erweiterung

Ivanti Neurons for MDM ermöglicht das Verwalten von Safari-Erweiterungen auf überwachten iOS- und macOS-Geräten. Administratoren können Safari-Erweiterungen für standardmäßiges und privates Browsing effektiv verwalten.

Gilt für:

- iOS 18.0 überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird.
- iOS 15.0 überwacht bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird.

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Einstellungen für Safari-Erweiterung** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie die Einstellungen für die **Safari-Erweiterung** gemäß der folgenden Tabelle:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Erweiterungs-ID	Geben Sie die zusammengesetzte Erweiterungskennung ein. Zum Beispiel "*Identifier (TeamIdentifier)*". Geben Sie "*" für alle Erweiterungen ein. Verwenden Sie zum Generieren dieser Zeichenfolge das Codezeichen *-dv <path_to_appex>*. Die Browser-Erweiterung befindet sich im Ordner mit den Plug-ins innerhalb des App-Bundles. Das erwartete Format lautet "*Identifier (TeamIdentifier)*". Für Erweiterungen, die nicht auf macOS verfügbar sind, sollte der App-Entwickler diese Informationen bereitstellen.
Status der Erweiterung	Wählen Sie eine der folgenden Optionen aus: • **Zulässig**: Der Benutzer kann die Erweiterung aktivieren oder deaktivieren. • **Immer ein**: Die Erweiterung steht für den Benutzer immer auf "Ein". • **Immer aus**: Die Erweiterung steht für den Benutzer immer auf "Aus".
Status von privatem Browsing	Wählen Sie eine der folgenden Optionen aus: • **Zulässig**: Der Benutzer kann die Erweiterung beim privaten Browsing aktivieren oder deaktivieren. • **Immer ein**: Die Erweiterung steht für den Benutzer immer auf "Ein", auch beim privaten Browsing. • **Immer aus**: Die Erweiterung steht nicht zur Verfügung.
Erlaubte Domänen	Geben Sie die Werte der Domäne oder Subdomäne ein, um der Safari-Erweiterung Zugriff zu gewähren. Sie können mehrere Werte für eine Domäne oder Subdomäne eingeben. Die Einstellungen für "Zulässige Domäne" gelten nicht für das Gerät, wenn Sie "*" in das Feld für die Erweiterungs-ID eingeben.
Verweigerte Domänen	Geben Sie die Werte der Domäne oder Subdomäne ein, um der Safari-Erweiterung den Zugriff zu verweigern. Sie können mehrere Werte für eine Domäne oder Subdomäne eingeben. Die Einstellungen für "Verweigerte Domäne" gelten nicht für das Gerät, wenn Sie "*" in das Feld für die Erweiterungs-ID eingeben.

4. Klicken Sie auf **+Hinzufügen**, um mehrere **Erweiterungen** hinzuzufügen.
5. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
6. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Einstellungen für Safari-Erweiterung** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
7. Klicken Sie auf **Fertig**.

Safari-Einstellungen

Ivanti Neurons for MDM ermöglicht das Verwalten von Safari-Einstellungen auf überwachten iOS- und macOS-Geräten. Administratoren können Safari-Erweiterungen für standardmäßiges und privates Browsing effektiv verwalten.

Gilt für:

- Betaversionen mit iOS 26.0+, iPad 26.0+, macOS 26.0+, visionOS 26.0+ bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Safari-Erweiterung und -Einstellungen** ausfindig und wählen Sie sie aus.
3. Klicken Sie auf **Safari-Einstellungen**.
4. Konfigurieren Sie die **Safari-Einstellungen** gemäß der folgenden Tabelle:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Konfigurationseinstellungen	Wählen Sie eine der folgenden Optionen, um den Typ der Startseite anzugeben: • **Start**: Zur Verwendung der Standardstartseite. Safari deaktiviert die vorhandene Startseite. • **Homepage**: Zur Verwendung der angegebenen Homepage-URL. Safari legt dies als Homepage fest. • **Erweiterung**: Zur Verwendung der von der Safari-Erweiterung angegebenen Seite mit der Kennung "ExtensionIdentifier". Safari deaktiviert die vorhandene Startseite.

5. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
6. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Safari-Einstellungen** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
7. Klicken Sie auf **Fertig**.

Safari-Datenschutzeinstellungen

Safari-Datenschutzeinstellungen ermöglichen es Administratoren, Standard-Kamera- und Mikrofonberechtigungen für bestimmte Websites in Safari mithilfe der deklarativen Geräteverwaltung (DDM) zu definieren. Diese Funktion hilft Unternehmen, die Datenschutzberechtigungen für Websites zentral zu verwalten und ein einheitlicheres Browsererlebnis auf verwalteten Apple-Geräten bereitzustellen.

Gilt für:

- iOS 27.0+ und macOS 27.0+ bis zur neuesten, von Ivanti Neurons for MDM unterstützten Version

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Safari-Erweiterung und -Einstellungen** ausfindig und wählen Sie sie aus.
3. Klicken Sie auf **Safari-Datenschutzeinstellungen**.
4. Konfigurieren Sie die **Safari-Datenschutzeinstellungen** gemäß der folgenden Tabelle:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.

Konfigurationseinstellungen	• **URL hinzufügen**: Geben Sie eine URL ein, um die Einstellung anzuwenden.
	• **+Standardeinstellungen hinzufügen**: Geben Sie die Standardwerte an, die Sie für diese Einstellung anwenden möchten.
	  ◦ Kamera zulassen/verweigern
	  ◦ Mikrofon zulassen/verweigern
	  ◦ Begründung Unternehmen (obligatorisch)

5. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.
6. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Safari-Einstellungen** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
7. Klicken Sie auf **Fertig**.

10.10.8.30. Konfiguration der Samsung Mobiltelefon-Einschränkungen

Konfigurationen

Mit der Konfiguration der Samsung Mobiltelefon-Einschränkungen können Sie Anrufeinschränkungen und Ausnahmen für Samsung-Geräte festlegen. Solche Einschränkungen llegen fest, welche Telefonnummern, die Benutzer wählen oder annehmen können.

Gilt für: Alle Samsung-Geräte mit Knox SDK 2.0+.

Konfiguration der Einschränkungen für Samsung-Mobiltelefone:

1. Klicken Sie auf der Registerkarte **Konfiguration** auf **+Hinzufügen**.
2. Klicken Sie auf die Konfiguration Samsung Mobiltelefon-Einschränkungen. Die Konfigurationsseite für die **Samsung Mobiltelefon-Einschränkungen** wird angezeigt.
3. Geben Sie in dem Feld **Name**die entsprechende Bezeichnung der Konfiguration ein.
4. Klicken Sie auf den Link + **Beschreibung hinzufügen** , um eine Beschreibung für die Konfiguration zu ergänzen. Dieses Feld ist optional.
5. Konfigurieren Sie in dem Abschnitt **Konfigurations-Setup** die folgenden Optionen:
   Option
   Beschreibung
   Eingehende Anrufe
   Gesperrte Nummern
   Klicken Sie auf das Hinzufügen-Symbol, um Rufnummern und reguläre Java-Ausdrücke zur Definition der Einschränkungen für eingehende Anrufe zu definieren.
   Whitelist-Nummern
   Klicken Sie auf das Hinzufügen-Symbol, um Rufnummern und reguläre Java-Ausdrücke zur Definition der zulässigen Rufnummern aus einem größeren Rufnummernblock für eingehende Anrufe zu definieren.
   Diese Option hat keinen Effekt, wenn keine gesperrten Rufnummern vorhanden sind.
   Ausgehende Anrufe
   Gesperrte Nummern
   Klicken Sie auf das Hinzufügen-Symbol, um Rufnummern und reguläre Java-Ausdrücke zur Definition der Einschränkungen bei abgehenden Anrufen zu definieren.
   Whitelist-Nummern
   Klicken Sie auf das Hinzufügen-Symbol, um Rufnummern und reguläre Java-Ausdrücke zur Definition der zulässigen Rufnummern aus einem größeren Rufnummernblock für eingehende Anrufe zu definieren.
   Diese Option hat keinen Effekt, wenn keine gesperrten Rufnummern vorhanden sind.
6. Klicken Sie auf **Fertig**, um die Einstellung per Push auf die ausgewählten Geräte zu übertragen.

> Wenn das Gerät außer Dienst gestellt wird, werden alle Anrufeinschränkungen von dem Gerät entfernt.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.8.31. Konfiguration "Standardbrowser" – iOS und visionOS

Mit dieser Konfiguration lassen sich die Einstellungen von Standardanwendungen auf iOS- und visionOS-Geräten ändern.

Voraussetzungen

- Gilt nur für die Versionen iOS (18.2+) und visionOS 2.2.
- Diese Apps werden auf iOS-Geräten unter **Einstellungen** – **Apps** – **Standard-Apps** eingestellt.

Verfahren

1. Registrieren Sie auf der Seite **Geräte** ein iOS-Gerät (18.2 +) oder ein visionOS 2.2-Gerät.
2. Navigieren Sie zu **Konfigurationen** > **Konfiguration hinzufügen** > **Einstellungen für Standardanwendung**, um den Standardbrowser auf iOS-Geräten festzulegen.
3. Klicken Sie auf **Konfigurationen** > **Einstellungen erstellen** > **Konfigurationseinstellungen für Standardanwendung erstellen**.
4. Geben Sie bei den Konfigurationsdetails einen **Namen** und eine **Beschreibung** ein.
5. Machen Sie unter "Konfigurationseinstellungen > App hinzufügen > Durch Suche hinzufügen" den gewünschten Browser ausfindig. Die Liste der Browser wird angezeigt.
6. Wählen Sie den gewünschten Browser aus der Liste aus.
7. Klicken Sie auf der Seite **Konfigurationseinstellungen für Standardanwendung erstellen** auf **Benutzerdefiniert**, um die Konfiguration an bestimmte Geräte oder Gerätegruppen oder an bestimmte Benutzer oder Benutzergruppen zu verteilen.
8. Wählen Sie unter **Wählen Sie eine der folgenden Optionen für die benutzerdefinierte Verteilung** die gewünschte Option aus, um die Verteilung der Konfiguration an Benutzer/Benutzergruppen bzw. Geräte/Gerätegruppen anzugeben.
9. Wählen Sie die gewünschte Option unter **Alle verfügbaren** aus, um die Konfiguration zu verteilen.
10. Klicken Sie auf **Fertig**.

10.10.8.32. Konfiguration "Hosteinstellungen für Bildschirmfreigabe"

Die Konfiguration **Hosteinstellungen für Bildschirmfreigabe** ermöglicht Administratoren das sichere Steuern von macOS-Bildschirmfreigabefunktionen für verwaltete Geräte unter Verwendung von Ivanti Neurons for MDM. Diese Funktion ermöglicht die Spezifizierung autorisierter Benutzer sowie von Authentifizierungsmethoden und Diensteinschränkungen, um einen konformen und sicheren Remotezugriff sicherzustellen.

Gilt für: macOS 14.0 bis zur zuletzt veröffentlichten Version, die von Ivanti Neurons for MDM unterstützt wird.

Vorbereitung: Für eine nahtlose Integration der Konfiguration **Hosteinstellungen für die Bildschirmfreigabe** muss der Benutzer die Option **Remoteverwaltung** auf seinem Gerät aktivieren. Wechseln Sie auf Ihrem Gerät zu **Einstellungen** > **Remoteverwaltung** > **Remoteverwaltung aktivieren**.

Verfahren

1. Gehen Sie zu **Konfigurationen** > **+Hinzufügen**.
2. Machen Sie die Konfiguration **Hosteinstellungen für die Bildschirmfreigabe** ausfindig und wählen Sie sie aus.
3. Konfigurieren Sie die **Hosteinstellungen für die Bildschirmfreigabe** gemäß der folgenden Tabelle:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
Portbasis	Geben Sie die anfängliche UDP-Portnummer für die Hostverbindung ein. Für die Bildschirmfreigabe sind mehrere Verbindungen erforderlich. Das System inkrementiert daher diesen Wert für jede zusätzliche Verbindung um 1. Dadurch ändert sich jedoch nicht die Portnummer, die das System anfangs zum Herstellen der Hostverbindung nutzt. Dieser Port ist immer TCP-Port 5900. **Mindestwert Portbasis**: 1024 **Höchstwert Portbasis**: 65.535
Maximale virtuelle Anzeigen	Sie können maximal zwei virtuelle Anzeigen verwenden.
Kopieren von Dateien vom Host verhindern	Markieren Sie das Kontrollkästchen, um zu verhindern, dass Benutzer Dateien vom bildschirmteilenden Host kopieren.
Kopieren von Dateien an den Host verhindern	Markieren Sie das Kontrollkästchen, um zu verhindern, dass Benutzer Dateien in den bildschirmteilenden Host kopieren.
Hochleistungsverbindungen verhindern	Markieren Sie dieses Kontrollkästchen, um zu verhindern, dass Benutzer Hochleistungsverbindungen zum Host herstellen können.

4. Klicken Sie auf **Weiter**, um die Verteilungseinstellung zu konfigurieren.

5. Wählen Sie eine der Verteilungsoptionen aus, um die Konfiguration **Hosteinstellungen für die Bildschirmfreigabe** einzurichten. Weitere Informationen zum Konfigurieren von Verteilungsoptionen finden Sie unter **Arbeiten mit Konfigurationen**.
6. Klicken Sie auf **Fertig**.

10.10.8.33. Single App Mode-Konfiguration

Konfigurationen

Lizenz: Silver

Eine Single App Mode-Konfiguration beschränkt Geräte auf die Nutzung einer bestimmten App. Sie können beispielsweise Geräte so konfigurieren, dass nur diese eine benutzerspezifische App verwenden können, die Ihr Unternehmen entwickelt hat.

Single App Mode-Konfiguration

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.
App wählen	Wählen Sie die zu verwendende Methode für das Auswählen der App aus: • Über App-Katalog und System-Apps: Durchsuchen Sie den -App-Katalog und die System-Apps (diese sind standardmäßig auf Apple-Geräten vorinstalliert). • Geben Sie den Namen der App ein und wählen Sie aus, wann diese in der App-Liste angezeigt wird. • Geben Sie die Bundle-ID an: Wählen Sie den eindeutigen Identifikator für die System-App aus, die Sie auswählen wollen.Nutzen Sie diese Option, wenn Sie die System-App mit der Option aus **App- Katalog & System-Apps** nicht finden können.
Touch deaktivieren	Wählen Sie diese Option, um den Touchscreen zu deaktivieren.
Geräterotation deaktivieren	Wählen Sie diese Option, um die Geräterotation zu deaktivieren.
Lautstärke-Tasten deaktivieren	Wählen Sie diese Option, um die Lautstärke-Tasten des Gerät zu deaktivieren.
Ringer Switch deaktivieren	Wählen Sie diese Option, um den Ruftonschalter des Gerät zu deaktivieren.
Schlaf/Wach-Taste deaktivieren	Wählen Sie diese Option, um die Schlaf/Wach-Taste des Gerät (am oberen rechten Rand des Gerät) zu deaktivieren.
Automatische Sperre deaktivieren	Wählen Sie diese Option, um zu verhindern, dass das Gerät nach einer Zeit im Leerlauf in den Ruhemodus wechselt.
Voice-Over aktivieren	Wählen Sie diese Option, um die Bildschirmlesetechnologie VoiceOver (Bedienungshilfe) zu aktivieren.
Zoom aktivieren	Wählen Sie diese Option, um die Zoomfunktion (Bedienungshilfe) zu aktivieren.
Farbumkehr aktivieren	Wählen Sie diese Option, um die Farbumkehr (Bedienungshilfe) zu aktivieren.
Assistive Touch aktivieren	Wählen Sie diese Option, um AssistiveTouch (Bedienungshilfe) zu aktivieren.
Sprachauswahl aktivieren	Wählen Sie diese Option, um die Funktion „Auswahl vorlesen“ (Bedienungshilfe) zu aktivieren.

Einstellung	So gehen Sie vor
Mono-Audio aktivieren	Wählen Sie diese Option, um von Stereo- zu Mono-Audio (Bedienungshilfe) zu wechseln.
Voice-Over-Einstellungen	Wählen Sie diese Option, um Benutzern zu gestatten, VoiceOver-Einstellungen vorzunehmen.
Zoom-Einstellungen	Wählen Sie diese Option, um Benutzern zu gestatten, Zoom-Einstellungen vorzunehmen.
Farbumkehr-Einstellungen	Wählen Sie diese Option, um Benutzern des Gerät das Umkehren von Farben zu gestatten.
Assistive Touch-Einstellungen	Wählen Sie diese Option, um Benutzern zu gestatten, AssistiveTouch-Einstellungen vorzunehmen.

Weitere Informationen finden Sie unter **Konfiguration erstellen**.

10.10.8.34. Konfiguration der Empfehlungskadenz für Softwareupdates

Für Administratoren ist eine Option verfügbar, mit denen sie Benutzern die Anzeige und Aktualisierung der Geräte auf das Release mit der höchsten Nummer (neuestes Release) und/oder mit der niedrigsten Nummer (ältestes Release) ermöglichen.

Gilt für: iOS und iPadOS14.5 bis 26.0 (überwacht)

Verfahren

1. Gehen Sie zu Konfigurationen > +Hinzufügen.
2. Geben SieEmpfehlung für Software-Updatesin das Suchfeld ein und klicken Sie dann auf die KonfigurationEmpfehlungskadenz für Software-Updates.
3. Geben Sie einen Namen und eine Beschreibung der Konfiguration ein.
4. Wählen Sie das gewünschte Konfigurations-Setup in der Dropdown-Liste aus:
    - Beide Software-Updateversionen zeigen
    - Dem Benutzer nur die Software-Updateversion mit der niedrigeren Nummer (ältere Version) zeigen
    - Nur die Software-Updateversion mit der höchsten Nummer (neueste Version) zeigen
5. Klicken Sie auf Weiter.
6. Wählen Sie die Option Diese Konfiguration aktivieren.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
8. Klicken Sie auf Fertig.

10.10.8.35. Startmenü und Taskleiste

Sie können das Layout des Startmenüs für Ihre Benutzer festlegen und bestimmen, welche Anwendungen in der Verwendung sicher sind, und nicht benötigte Anwendungen entfernen. Die Versionen Windows 10 und 11 unterstützen unterschiedliche Funktionen, da die Startmenülayouts anders aussehen.

So konfigurieren Sie Startmenü und Taskleiste:

1. Gehen Sie zu **Konfiguration > +Hinzufügen** .
2. Wählen Sie die Konfiguration für **Windows Startmenü & Taskleiste**.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Wählen Sie die jeweilige Windows-Version aus.
5. **Windows 10-Geräte**:
   In dem Abschnitt **Konfigurations-Setup** konfigurieren Sie folgende Einstellungen:
   Einstellung
   So gehen Sie vor
   [Name]
   Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
   Beschreibung
   Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.**Wählen Sie ein Standardgerät aus.**
   Wählen Sie ein Gerät mit Windows 10 aus, auf dem die gewünschten Apps im Startmenü und in der Taskleiste bereitgestellt sind.
6. Klicken Sie auf die Option Startmenü-Layout vom Gerät holen und konfigurieren Sie die folgenden Optionen.
7. **Einstellung**
   So gehen Sie vorStartmenü- und Taskleisten-Layout
   Wählen Sie eine der folgenden Optionen aus, um die Liste der Apps zu verbergen.
   - Kein/e
   - Liste aller Apps ausblenden
   - Blenden Sie die Liste aller Apps aus und deaktivieren Sie in der App „Einstellungen“ die Option „App-Liste im Startmenü anzeigen“
   - Blenden Sie die Liste aller Apps aus, entfernen Sie die Schaltfläche „Alle Apps“ und deaktivieren Sie die Option „App-Liste im Startmenü anzeigen“ in der App „Einstellungen“

StartmenülayoutStartmenü anpassen
Klicken Sie auf **Ja,** um das Startmenü und die Layoutparameter anzupassen.**TaskleisteTaskleiste anpassen**Klicken Sie auf **Ja,** um die Taskleiste anzupassen.**Vorhandene angeheftete Taskleistenverknüpfungen vor dem Hinzufügen benutzerdefinierter Verknüpfungen entfernen**Klicken Sie auf **Ja**, um eine vorhandene Verknüpfung von der Taskleiste zu entfernen, bevor Sie eine benutzerdefinierte Verknüpfung hinzufügen.**App-Typ**Definiert die Art der App.**[App]**Definiert die ID der App.**Wiederherstellen**
Klicken Sie auf den Link **Wiederherstellen**, um die Taskleiste entsprechend der Taskleiste des Originalstandardgeräts wiederherzustellen.
Klicken Sie auf das Pfeilsymbol in der Zeile und ziehen Sie daran, um die Position der jeweiligen Zeile nach oben oder unten zu verschieben.
Klicken Sie auf das Löschsymbol, um die Zeile zu löschen.
Klicken Sie auf die Schaltfläche **Neu hinzufügen**, um eine neue Zeile hinzuzufügen.

8. **Windows 11-Geräte**
   In dem Abschnitt **Konfigurations-Setup** konfigurieren Sie folgende Einstellungen:
   Einstellung
   So gehen Sie vor
   [Name]
   Geben Sie einen Namen ein, der diese Konfiguration bezeichnet.
   Beschreibung
   Geben Sie eine Beschreibung ein, die den Zweck dieser Konfiguration erläutert.**Wählen Sie ein Standardgerät aus.**
   Wählen Sie das Windows 11-Gerät aus, auf dem die Apps im Bereich ANGEHEFTET des Startmenüs konfiguriert sind.**Startmenü- und Taskleisten-LayoutStartmenü- und Taskleisten-Layout**
   Wählen Sie eine der folgenden Optionen, um die Suchoption in der Taskleiste anzuzeigen:
   - **Ausblenden**
   - **Suchsymbol**
   - **Suchsymbol und Beschriftung**
   - **Suchfeld (Standard)**

Markieren Sie das Kontrollkästchen **Aufgabenansicht ausblenden**, um die Aufgabenansicht auszublenden.**Am häufigsten verwendete Apps**
Wählen Sie eine der folgenden Optionen, um die Anzeige der am häufigsten verwendeten Apps im Startmenü zu konfigurieren:

- **Anzeige der Liste der am häufigsten verwendeten Apps auf der Startoberfläche nicht erzwingen**
- **Anzeige der Liste der am häufigsten verwendeten Apps auf Startoberfläche erzwingen**
- **Ausblenden der Liste der am häufigsten verwendeten Apps auf Startoberfläche erzwingen**

Das Kontrollkästchen **Anheften in Taskleiste zulassen** ist standardmäßig markiert.
Markieren Sie das Kontrollkästchen **Abschnitt "Empfohlen" ausblenden**, um alle Abschnitte vom Typ "Empfohlen" auszublenden.
Aufgrund eines Problems beim Anbieter hat das Kontrollkästchen **Abschnitt "Empfohlen" ausblenden** keine sichtbare Wirkung auf das Gerät, auch wenn sich der Benutzer abmeldet oder anmeldet. Derzeit lässt sich dieser Abschnitt nicht ausblenden.**TaskleisteApp-Typ**
Wählen Sie eine der folgenden Optionen, um den Typ der App anzugeben:

- **App-Benutzermodell-ID**
- **Link mit Pfad zur Desktop-Anwendung**

[App]Gibt die ID oder den Pfad der App an.**Wiederherstellen**
Klicken Sie auf den Link **Wiederherstellen**, um die Taskleiste entsprechend der Taskleiste des Originalstandardgeräts wiederherzustellen.
Klicken Sie auf das Pfeilsymbol in der Zeile und ziehen Sie daran, um die Position der jeweiligen Zeile nach oben oder unten zu verschieben.
Klicken Sie auf das Löschsymbol, um die Zeile zu löschen.
Klicken Sie auf die Schaltfläche **Neu hinzufügen**, um eine neue Zeile hinzuzufügen.

9. Klicken Sie auf **Startmenülayout vom Gerät brufen** aus.
10. Nachdem Einstellungen vom Standardgerät abgerufen wurden, werden die im Abschnitt ANGEHEFTET des Startmenüs konfigurierten Apps für den Administrator angezeigt, damit er diese überprüfen kann.
    Klicken Sie auf **Weiter** und verteilen Sie die Konfiguration an alle relevanten Geräte- und Benutzergruppen.

Aufgrund eines Anbieterfehlers bleiben die angehefteten Apps wie ursprünglich konfiguriert, wenn die Konfiguration nicht verteilt wird. Wird jedoch eine neue Konfiguration verteilt, wird das vorherige Layout überschrieben und das neue wird angewendet.

10.10.8.36. Konfiguration der Systemaktualisierung

Administratoren können die Verwaltung von Systemupdates durch Benutzer auf Geräten mit Android 6.0 (oder unterstützten neueren Versionen) einschränken. Diese Funktion gilt nur für Geräte mit Android Enterprise.

Gehen Sie zur Konfiguration wie folgt vor:

1. Gehen Sie zu **Konfiguration > +Hinzufügen**.
2. Wählen Sie die Konfiguration **Systemupdate**.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Konfigurieren Sie im Abschnitt Konfigurations-Setup die folgenden Optionen:

Einstellung	Beschreibung
Automatisch	Systemupdates werden im Hintergrund installiert, sobald neue Firmware verfügbar ist.
Verschieben In Fenstern (Ortszeit) **Manuelles Betriebssystemupdate (Android 10+)** Nicht anwendbar oder unterstützt auf Samsung- und Zebra-Geräten	Verschiebt die Installation von Systemaktualisierungen um 30 Tage. Nach Ablauf der 30-Tage-Frist fordert das System den Gerätebenutzer auf, das Update zu installieren. Es wird ein Zeitraum festgelegt, um das Systemupdate im Hintergrund zu installieren. Wählen Sie die **Startzeit** und **Endzeit**. Wählen Sie diese Option aus, um das Betriebssystemupdate manuell auf einer begrenzten Anzahl von Geräten durchzuführen, bevor Sie das Update auf alle Geräte ausrollen. **Firmwaredatei** – Wählen Sie **Benutzerdefiniertes Attribut** oder **HTTPS-URL** aus. Geben Sie folgende Details ein: • Firmwarespeicherort – Falls Sie die Option **Benutzerdefiniertes Attribut** für die Firmwaredatei gewählt haben, geben Sie das benutzerdefinierte Attribut an, das für die Dateiübertragung verwendet wurde. Die Firmwaredatei kann selbst gehostet oder unter Verwendung der Konfiguration "Dateiübertragung" zu Ivanti Neurons for MDM hochgeladen werden. Weitere Einzelheiten finden Sie unter **Konfiguration "Dateiübertragung"**. Zum Hochladen von Dateien mit einer Größe von über 50 MB zu Ivanti Neurons for MDM ist eine Add-On-Lizenz erforderlich. • Beschreibung (optional) • Fingerabdruck (obligatorisch) – Zur Validierung, dass tatsächlich die beabsichtigte Betriebssystemversion auf dem Gerät installiert wird. Der Fingerabdruck befindet sich in der OTA-Datei. Entpacken Sie dazu den OTA-Ordner und öffnen Sie die Datei "/META-INF/com/android/metadata". Machen Sie einen Eintrag ähnlich dem folgenden ausfindig: "post-build=google/xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxxxx:user/release-keys" Im obigen Eintrag entspricht **google/ xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxx:user/release-keys** dem Fingerabdruck, wobei TQ3A.230805.001.S1 die Build-ID darstellt (die Build-ID ist der 4. Wert von links der Blöcke, die im Fingerabdruck durch '/' getrennt sind). • Prüfsumme (optional) **Updateeinstellungen** → **Betriebssystemupdate-Anforderung** – Die Einstellungen in diesem Abschnitt sind mit denen der Zebra-Firmware-Konfiguration identisch. Siehe Abschnitt *Zebra Firmware-Konfiguration* in dieser Tabelle. Wenn Sie die Option **HTTPS-URL** für die Firmwaredatei gewählt haben, sind folgende Angaben erforderlich: • Firmwarespeicherort – Geben Sie den Pfad an, über den die Firmware ohne Anforderung einer Authentifizierung heruntergeladen werden kann. Beschreibung (optional) • Fingerabdruck (obligatorisch) – Zur Validierung, dass tatsächlich die beabsichtigte Betriebssystemversion auf dem Gerät installiert wird. • Prüfsumme (optional) Die Abschnitte **Download-Anforderung** und **Bedingungen während des Downloads** sind zusätzlich zum Abschnitt **Betriebssystemupdate-Anforderung** verfügbar. Die verfügbaren Optionen in den Abschnitten **Download-Anforderung initiieren** und **Bedingungen während des Downloads** sind mit denen im Abschnitt **Zebra Firmware-Konfiguration** identisch.

Einstellung	Beschreibung
	Wenn ein Systemupdate auf dem Gerät gestartet wurde und das Gerät während des Updates neugestartet wird, wird der Updatevorgang abgebrochen.
Freeze-Zeitraum	Das Systemupdate wird in einem bestimmten Zeitraum nicht installiert. Diese Option gilt für Geräte mit Android 9.0+. Klicken Sie auf **Freeze-Zeitraum hinzufügen**. Wählen Sie das **Anfangsdatum** und **Enddatum** für den Freeze-Zeitraum. Die Sperrfrist kann nicht mehr als 90 Tage betragen und Sie können mehrere Sperrfristen hinzufügen. Der nächste Freeze-Zeitraum kann erst 60 Tage nach dem letzten Enddatum ausgewählt werden. Um einen Freeze-Zeitraum zu löschen, klicken Sie auf das Symbol „Löschen“.
Zebra Firmware-Konfiguration	Wählen Sie **Zebra OTA konfigurieren**, um ein Upgrade oder Update der Betriebsfirmware der Zebra-Geräte (mit Android Version 8.0 oder unterstützten neueren Versionen) durchzuführen. Dies gilt nur für die Geräteeigentümermodi. Um Zebra OTA-Updates zu konfigurieren, müssen Sie den Cloud OTA-Service unter **Admin>Firmware Management>Zebra OTA** aktivieren und es müssen Zebra-Geräte in der Cloud vorhanden sein. Sie müssen Ihre Zebra-Zugangsdaten in das Popup-Fenster eingeben. Wenden Sie sich direkt an Zebra, um Ihre Zugangsdaten neu zu erstellen. Wenn diese Option ausgewählt ist, wird die Liste der registrierten Zebra-Geräte angezeigt. Firmware für das Gerätemodell auswählen und übernehmen: 1. Führen Sie in der Spalte **Aktion** für das Zebra-Gerät eine der folgenden Aktionen aus: ◦ **Keine**: Es wird keine Aktion für das Gerätemodell durchgeführt. ◦ **Vollständiges Upgrade**. Wählen Sie im Fenster **Zebra Firmware für Ziel auswählen** die Vollversion der Zebra-Firmware aus, die für das Gerätemodell übernommen werden soll . Während eines **vollständigen Upgrades** wird nur Port 443 benötigt. Sie können in das Feld **Suche** die Zeichen einer Build-ID eingeben, um nach Upgrades auf der Grundlage der Build-ID zu suchen. Die Build-IDs werden in absteigender Reihenfolge (letzte ganz oben) sortiert und angezeigt. Die Option **Patchupgrade** ist auf Geräten mit Android 11 oder späteren Versionen **NICHT** verfügbar. 2. Konfigurieren Sie nach Bedarf folgende Optionen: **Download-Anfrage initiieren** – Diese Bedingungen werden von Go app geprüft. ◦ **Mindestens erforderlicher Akkuzustand**: Legen Sie den mindestens erforderlichen Akkuzustand mithilfe des Schiebereglers aus dem verfügbaren Bereich aus. ◦ **Aufladen des Geräts verlangen**: Wählen Sie diese Option aus, damit das Gerät während des Prozesses im Lademodus bleibt. ◦ **Download-Zeitplan**: Mit dieser Option können Sie Zeitplan erstellen, um Download-Anfrage und Datei-Download zu initiieren. ◦ Die Parameter **Gerät im Leerlauf erforderlich**, **Aufladen erforderlich** und **Download über gebührenpflichtiges Netzwerk zulassen** werden an den Android Download Manager übergeben. Go app fügt die Anforderung zum Herunterladen in dem genannten Fenster mit den obigen Parametern zu Android Download Manager hinzu. **Zeitplan für Download verwenden** - Wählen Sie die **Wochentage** sowie die **Start-** und **Endzeit** aus, um den Download zu planen. Es können mehrere Tage ausgewählt werden, um den Download zu

Einstellung	Beschreibung
	planen. Wenn beispielsweise Samstag und Sonntag mit einer Start- und Endzeit zwischen 12:00 Uhr morgens und 23:00 Uhr abends ausgewählt ist, wird der Download in Zebra-Geräten nur während dieses Zeitraums an den ausgewählten Tagen durchgeführt. In Go app beginnt der Download wie geplant, wenn die Konfiguration auf das Gerät angewendet wird. Es gibt kein Zeitlimit für das Ende des Downloads und der Download kann auch nach der geplanten Endzeit abgeschlossen werden. ◦ Zeitplan für das Update übernehmen - Wählen Sie die **Wochentage** und die **Start-** und **Endzeit** aus, um die Installation des Firmware-Updates zu planen. Die Installation wird verschoben, wenn der Batteriestand des Geräts unter 32 liegt. Wenn kein Update-Zeitplan konfiguriert ist, beginnt die Installation unmittelbar nach Abschluss des Firmware-Downloads. 3. Konfigurieren Sie nach Bedarf folgende Optionen: **Bedingungen während des Downloads** – Diese Bedingungen werden von Download Manager geprüft. Sie können bei Ihrer Auswahl bestimmte Kriterien berücksichtigen. ◦ **Gerät im Leerlauf erforderlich** (standardmäßig ausgewählt): Ermöglicht Firmware-Updates auf dem Gerät, wenn das Gerät im Leerlauf ist. ◦ **Lademodus erforderlich** (standardmäßig ausgewählt): Ermöglicht Firmware-Updates auf dem Gerät, wenn es sich im Lademodus befindet. ◦ **Download über ein gebührenpflichtiges Netzwerk zulassen**: Wählen Sie diese Option aus, um den Download im WLAN-Modus zu erlauben. Diese Option ist standardmäßig deaktiviert. ◦ Die Parameter **Gerät im Leerlauf erforderlich**, **Aufladen erforderlich** und **Download über gebührenpflichtiges Netzwerk zulassen** werden an den Android Download Manager übergeben. Go app fügt die Anforderung zum Herunterladen in dem genannten Fenster mit den obigen Parametern zu Android Download Manager hinzu. **Fortsetzung des Downloads außerhalb des festgelegten Download-Zeitplans zulassen**: Wählen Sie diese Option aus, um zuzulassen, dass Downloads auch außerhalb des Download-Zeitplans durchgeführt werden. **Anforderung eines Betriebssystemupdates** ◦ **Mindestens erforderlicher Akkuzustand** – Über diese Option geben Sie den Akkuzustand an, der mindestens erreicht sein muss, damit ein Betriebssystemupdate angefordert wird. ◦ **Aufladen des Geräts verlangen** – Wählen Sie diese Option aus, damit das Gerät während des Prozesses im Lademodus verbleibt. ◦ **Zeitplan zum Starten des Betriebssystemupdates auf dem Gerät erstellen** – Wählen Sie diese Option, um einen Zeitplan festzulegen, auf dessen Basis das Betriebssystemupdate auf dem Gerät startet. In Go app beginnt der Download wie geplant, wenn die Konfiguration auf das Gerät angewendet wird. Es gibt kein Zeitlimit für das Ende des Downloads und der Download kann auch nach der geplanten Endzeit abgeschlossen werden. Klicken Sie auf [**Apply**.
Samsung e-FOTA	Wählen Sie **Samsung e-FOTA konfigurieren**, um ein Update oder Upgrade der Betriebs-Firmware der Samsung-Geräte (auf Knox Version 2.7.1 und höher) vorzunehmen. Dies gilt nur für die Modi „Verwaltetes Gerät

Einstellung	Beschreibung
Konfiguration	mit Arbeitsprofil“ und „Unternehmenseigenes Gerät“. Wenn keine Samsung e-FOTA-fähigen Geräte registriert sind, wird auf der Seite eine Meldung mit diesen Informationen angezeigt. Samsung_e-FOTA_License_Management.htmUm Samsung e-FOTA-Updates zu konfigurieren, müssen Sie die Samsung e-FOTA-Lizenz unter Admin>Firmware-Verwaltung>Samsung E-FOTA aktivieren. Wenn diese Option ausgewählt ist, wird die Liste der registrierten Samsung-Geräte angezeigt. Firmware für das Gerätemodell auswählen und übernehmen: 1. Führen Sie in der Spalte **Aktion** für das Samsung-Gerät eine der folgenden Aktionen aus: ◦ **Aktuell**: Die neueste Firmware-Version wird übernommen. Diese Option ist standardmäßig ausgewählt. ◦ **Erzwingen**: Wählen Sie im Fenster „Samsung-Zielfirmware auswählen“ die spezifische Firmware-Version aus, die (ohne Benutzereingriff) deren Übernahme auf das Gerätemodell erzwungen werden soll. Wenn diese Aktion ausgeführt wird, beginnt das Herunterladen der Firmware innerhalb von fünfzehn Minuten. ◦ **Ziel**: Wählen Sie im Fenster „Zebra Zielfirmware auswählen“ die spezifische Firmware-Version aus, die für das Gerätemodell übernommen werden soll . Wenn beim Ausführen der Aktionen „Erzwingen“ oder „Ziel“ keine Firmware für das Gerät aufgeführt ist, wird auf der Seite eine Meldung mit dieser Information angezeigt. 2. **Debug FW aktivieren** (Optional): Wenn die Option **Debug FW aktivieren** aktiv ist und die Konfiguration übernommen ist, wird das Gerät auf eine Dummy-Firmware aktualisiert. Mit der Dummy-Firmware der Samsung-Geräte-Firmware kann der Administrator das Konfigurationsverhalten der Systemaktualisierung auf den Geräten testen, ohne tatsächlich etwas am Gerät zu ändern. Um statt des Dummy-Firmware-Updates das echte Firmware-Update durchzuführen, muss der Admin sicherstellen, dass die Option debug FW aktivieren vor der Anwendung der Konfiguration deaktiviert ist. 3. Klicken Sie auf [**Apply**.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:

- Alle Geräte
- Keine Geräte (Standard)
- Anpassbar

8. Klicken Sie auf **Fertig**.

Samsung E-FOTA-Konfiguration (außer Betrieb)

Die Samsung E-FOTA-Konfiguration wird ab Juli 2022 nicht mehr unterstützt. Daher ist diese Konfiguration für neue Geräte nicht verfügbar. Nur Geräte mit der vorhandenen Konfiguration können diese Konfiguration deaktivieren.

10.10.8.37. Updateverwaltung unter Windows 10

Als Administrator können Sie die von Windows 10-Geräten gemeldeten Updates mithilfe der Updateverwaltung von Windows 10 anzeigen und genehmigen. Mit dieser Funktion können Sie verhindern, dass ungetestete oder unnötige Updates auf den Geräten installiert werden.

Um die Funktion zur Update-Verwaltung zu nutzen, müssen die Geräte für die Software-Update-Konfiguration mit der Option Update-Genehmigung anfordern aktiviert sein.Nur durch Übernahme dieser Konfiguration auf die Geräte melden die Geräte für die Installation verfügbare Updates und warten auf die Genehmigung.

Aktualisierungen verwalten

1. Wechseln Sie zum Abschnitt **Admin > Windows > Windows-Updates**. Die folgenden Details der Updates werden auf der Seite angezeigt.
   Erstellungsdatum: Das Datum, an dem das Update erstellt wurde.**Titel**: Beschreibt die Art des Updates, enthält die Artikelnummer aus der Knowledge Base.

> Wenn Sie auf das Update klicken, wird die Beschreibung angezeigt.

Klassifizierung: Ordnet den Updatetyp einer der folgenden Kategorien zu:

- Kritische Aktualisierungen
- Definitionsupdates
- Treiberupdates
- Sicherheitsupdates
- Updates
- Upgrade
- Updaterollups

Verteilung: Die Verteilung für das Update. Beispielsweise wird die Option **Alle** angezeigt, wenn das Update auf alle Geräte verteilt wird.

> Wenn das Update auf eine spezifische Anzahl von Gruppen verteilt wird, wird die Anzahl der Verteilungen angezeigt. Es wird beispielsweise Ziffer 3 angezeigt, wenn die Verteilung nur die Gruppen betrifft.

2. Zusätzlich können Sie anzeigen, ob eine Aktualisierung an die erforderlichen Geräte verteilt wurde oder nicht. Die folgenden Spalten verfügen über Zahlen, die angeben, wie viele Geräte in den verschiedenen Aktualisierungskategorien enthalten sind:
   - Geeignete Geräte
   - Installierte Geräte
   - Fehlgeschlagene Geräte
   - Geräte mit ausstehendem Neustart

Wenn Sie auf eine Zahl klicken, gelangen Sie zur gefilterten Ansicht der Geräteseite. Dort können Sie den Aktualisierungsstatus überprüfen und ggf. erforderliche Aktionen durchführen.
Prüfen Sie die Updates und klicken Sie auf das Update, das Sie auf die Geräte verteilen möchten, indem Sie das Kontrollkästchen für das Update aktivieren.

3. Klicken Sie unter **Aktionen** auf **Verteilung definieren**.
4. Wählen Sie in dem Fenster **Windows-Update verteilen** eine der folgenden Verteilungsoptionen:
   Alle Geräte: Verteilt die Aktualisierungen auf alle Geräte.
   Keine Geräte: Verschiebt die Verteilung der Updates auf die Geräte.**Anpassbar**: Verteilt die Updates für die definierten Gerätegruppen.
5. Klicken Sie auf **Speichern**.

Updates suchen und filtern

Sie können Updates nach folgenden Kriterien suchen und filtern:

- Artikel-ID der Knowledge Base
- Konfigurierte Verteilung

Nach Artikel-ID der Knowledge Base filtern:

1. Geben Sie auf der Seite **Windows 10-Updateverwaltung** die Wissensdatenbank-ID in das Schnellsuche-Feld ein (nur die Nummer bei "Suchen").
   Beispiel: Für KB4056892, geben Sie 4056892 ein. Das Update, das zu den Suchkriterien passt, wird auf der Seite angezeigt.

> Sie können außerdem nach weiteren Informationen zu dem Update suchen, indem Sie auf den Link **Support** und **Weitere Informationen** klicken. Der Link **Support** verlinkt zur Microsoft-Webseite mit den entsprechenden Produkt-Support-Informationen für das Update, der Link **Weitere Informationen** verlinkt zu der Microsoft-Webseite mit weiteren Informationen zum Update, beispielsweise zu dem Artikel in der Knowledge Base.

Nach konfigurierter Verteilung filtern:

Wählen Sie auf der Seite **Updateverwaltung unter Windows 10** eine der folgenden Filteroptionen für die konfigurierte Verteilung aus:

- **Alle**: Zeigt alle Aktualisierungen an.
- **Konfiguriert**: Zeigt die Liste der Aktualisierungen an, die auf Geräte verteilt werden.
- **Nicht konfiguriert**: Zeigt die Liste der Updates an, für die die Verteilung nicht definiert ist.

> Konfigurierte und nicht-konfigurierte Filter richten sich nach der durchgeführten Verteilung. Die Verteilung kann auch Keine sein.

Aktualisierungen für ein Gerät anzeigen

Detaillierte Update-Informationen speziell für ein Gerät anzeigen:

1. Gehen Sie zu **Geräte > Geräte**.
2. Klicken Sie auf einen Gerätenamen, um die Seite mit den Details aufzurufen.
3. Gehen Sie zur Registerkarte **Aktualisierungen**. Angezeigt werden die Updates für das Gerät, die noch ausstehen (Update vom Administrator genehmigt, aber noch nicht auf dem Gerät als installiert gemeldet), fehlgeschlagen und installiert sind.

Benachrichtigungen über neue Windows-Updates sehen Sie außerdem auf der Seite „Benachrichtigungen“ im Dashboard. Die Benachrichtigung erhält das Erstellungsdatum der Benachrichtigung, die Anzahl der verfügbaren Benachrichtigungen und den Zweck der Benachrichtigung. Die Benachrichtigung über das Windows-Update ist außerdem in der oberen rechten Ecke des Administrationsportals sichtbar.

10.10.8.38. Zeitplanung von Windows Apps

Apps für Windows Desktop können umfangreich sein und verursachen eine zusätzliche und längere Belastung der Netzwerke und Server während der Spitzenzeiten für das Unternehmen. Mit der Funktion zur Zeitplanung der Windows-App können Sie eine Zeit zur Installation von Apps, insbesondere großen Apps, auf Geräten einplanen.

App-Planung konfigurieren:

1. Gehen Sie zu **Apps > App-Katalog**.
2. Klicken Sie auf **Hinzufügen** und wählen Sie eine Windows-App aus. Fahren Sie anschließend mit den nächsten Schritten im Assistenten **App hinzufügen** fort.
3. Klicken Sie in Schritt 5 (Konfigurieren) auf **Anwendungskonfigurationseinstellungen installieren**, um die Seite **Konfigurations-Setup** anzuzeigen.
4. Aktivieren Sie das Kontrollkästchen **Installation planen**.

> Das Kontrollkästchen **Installation planen** wird nur angezeigt, wenn die Installation im Hintergrund aktiviert ist.

5. Wählen Sie eine **Startzeit** und eine **Endzeit**, um die Zeit für die Installation von Apps zu planen.
6. Wählen Sie ein **Startdatum** und ein **Enddatum** aus, um das Datum für die Installation von Apps zu planen.

> Sie können auch eine der beiden folgenden Aktionen auswählen, die ausgeführt werden, wenn das geplante Datum erfolglos verstreicht: **Beim nächsten Einchecken installieren** oder **Nicht installieren**.

7. Wählen Sie eine Option für die Verteilung der App-Konfiguration aus: **Jeder mit App**, **Keiner** oder **Benutzerdefiniert**.
8. Klicken Sie auf **Fertig**.

> Apps, die geplant werden müssen, sollten nicht in Apps@Work hinzugefügt werden.
> Die Zeitplanung der Apps gilt nicht für Store-Apps, da die Installation von Store-Apps im Hintergrund nicht unterstützt wird.

10.10.8.39. Windows BIOS-Konfiguration

Administratoren können auf Lenovo-Geräten Windows-BIOS-Einstellungen festlegen. Um diese Konfiguration einzustellen, muss mindestens ein Lenovo-Gerät, das BIOS-Einstellungen unterstützt, registriert sein.

Gehen Sie zur Konfiguration wie folgt vor:

1. Gehen Sie zu **Konfiguration > +Hinzufügen**.
2. Wählen Sie die **Windows BIOS**-Konfiguration aus.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Wählen Sie im Abschnitt „Gerätemodell auswählen“ das Gerätemodell aus der Dropdown-Liste aus.
6. Konfigurieren Sie im Abschnitt Konfigurations-Setup die folgenden Optionen:

> Die Liste der Einstellungen variiert je nach den verfügbaren Funktionen für das jeweilige registrierte Gerätemodell. Weitere Informationen erhalten Sie auf der Website zum jeweiligen Gerät.

Einstellung	Arbeitsschritte
AMT-Steuerung	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Adaptives Wärmemanagement AC	Wählen Sie eine der folgenden Optionen aus: • **Ausgewogen** • **Maximierte Leistung**
Adaptive Wärmemanagement der Batterie	Wählen Sie eine der folgenden Optionen aus: • **Ausgewogen** • **Maximierte Leistung**
Always-On-USB	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
BIOSPasswordAtBootDeviceList	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
BIOS-Passwort beim Neustart	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
BIOS-Passwort beim unbeaufsichtigten Booten	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
BIOS-Update durch Endbenutzer	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Bluetooth-Zugang	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Geräteneustart mit Funktionstaste F12	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**

Einstellung	Arbeitsschritte
Anzeigegerät neu starten	Wählen Sie eine der folgenden Optionen aus: • **DisplayPort** • **Dockanzeige** • **HDMI** • **LCD**
Neustartmodus	Wählen Sie eine der folgenden Optionen aus: • **Diagnostik** • **Schnell**
Startreihenfolge sperren	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
BootTimeExtension	Wählen Sie eine der folgenden Optionen aus: • **1** • **10** • **2** • **3** • **5** • **Deaktivieren**
Manipulation der unteren Abdeckung festgestellt	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
CPU-Energieverwaltung	Wählen Sie eine der folgenden Optionen aus: • **Automatisch** • **Deaktivieren**
Aktivierung des Computrace-Moduls	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Verhinderung der Datenausführung	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Ethernet LAN-Zugang	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Ethernet LAN Option ROM	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren**

Einstellung	Arbeitsschritte
	• **Aktivieren**
Authentifizierung mit Fingerabdruckpasswort	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Pre-Desktop-Authentifizierung per Fingerabdruck	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Zugriff auf Fingerabdruckleser	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Priorität des Fingerabdrucklesers	Wählen Sie eine der folgenden Optionen aus: • **Extern** • **Nur intern**
Fingerabdruck-Sicherheitsmodus	Wählen Sie eine der folgenden Optionen aus: • **Hoch** • **Normal**
Fn und Strg-Taste vertauschen	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
FnKeyAsPrimary	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
FnSticky	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
IPv4-Netzwerkstapel	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
IPv6-Netzwerkstapel	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Zugriff auf integrierte Kamera	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**

Einstellung	Arbeitsschritte
InternalStorageTamper	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Tastenton	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
BIOS-Einstellungen sperren	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Zugriff auf den Speicherkartensteckplatz	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Zugriff auf Mikrofon	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Mindestlänge des Passworts	Wählen Sie eine der folgenden Optionen aus: • 4 • 5 • 6 • 7 • 8 • 9 • 10 • 11 • 12 • **Deaktivieren**
NFFControl	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
NFC-Zugang	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Einschalten bei Anschluss des Netzkabels	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**

Einstellung	Arbeitsschritte
PasswordBeep	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Passwortanzahl überschritten - Fehler	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
TPM physisch vorhanden	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
TPM physisch vorhanden und bereitgestellt	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Schnellstart-Technologie	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Sicherer Neustart	Wählen Sie **Aktivieren**
Sichere Rollback-Verhinderung	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Sicherheitschip	Wählen Sie eine der folgenden Optionen aus: • **Aktiv** • **Deaktivieren** • **Aktivieren** • **Inaktiv**
Zugriff auf den Smart Card-Steckplatz	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
SpeedStep	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Startoptionstasten	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
TXT-Funktion	Wählen Sie eine der folgenden Optionen aus:

Einstellung	Arbeitsschritte
	• **Deaktivieren** • **Aktivieren**
Gesamter Grafikspeicher	Wählen Sie eine der folgenden Optionen aus: • **256 MB** • **512 MB**
TouchPad	Wählen Sie eine der folgenden Optionen aus: • **Automatisch** • **Deaktivieren**
TrackPoint	Wählen Sie eine der folgenden Optionen aus: • **Automatisch** • **Deaktivieren**
USB30-Modus	Wählen Sie eine der folgenden Optionen aus: • **Automatisch** • **Deaktivieren** • **Aktivieren**
USB BIOS-Unterstützung	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
USB-Anschlusszugriff	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Uefi Pxe Neustart-Priorität	Wählen Sie eine der folgenden Optionen aus: • **IPv4 zuerst** • **IPv6 zuerst**
VTd-Funktion	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Virtualisierungs-Technologie	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**

Einstellung	Arbeitsschritte
Wake on LAN	Wählen Sie eine der folgenden Optionen aus: • **Nur Netz** • **Netz und Batterie** • **Deaktivieren** • **Aktivieren**
WLAN-Zugang	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**
Drahtloser WAN-Zugang	Wählen Sie eine der folgenden Optionen aus: • **Deaktivieren** • **Aktivieren**

7. Klicken Sie auf **Weiter**.
8. Wählen Sie eine der folgenden Verteilungsoptionen aus:
   - Alle Geräte
   - Keine Geräte (Standard)
   - Anpassbar
9. Klicken Sie auf **Fertig**.

10.10.8.40. Windows BitLocker

Als Administrator können Sie den Wiederherstellungsschlüssel für einen Satz verschlüsselter Windows 10-Geräte massenweise aktualisieren, wenn Sie eine Excel-Datei mit der Geräte-GUID und dem Wiederherstellungspasswort hochladen.

Excel-Datei für die Massenaktualisierung des Wiederherstellungsschlüssels hochladen:

1. Gehen Sie zu Admin>Windows BitLocker.
2. Klicken Sie auf **Beispiel csv-Datei herunterladen**, um die Beispiel-CSV-Datei herunterzuladen und ein Beispiel für eine .csv-Datei anzuzeigen.
3. Erstellen Sie die Datensätze für die .csv-Datei der BitLocker-Wiederherstellungsschlüssel und fügen Sie sie hinzu.
4. Klicken Sie auf **Wiederherstellungspasswörter hochladen**.
5. Klicken Sie auf **Datei auswählen**, um die von Ihnen erstellte .csv-Datei hochzuladen.
6. Klicken Sie auf **Hochladen**. Beim Hochladen einer neuen Datei mit zuvor hochgeladenen Schlüsseln werden die alten Einträge überschrieben.

> In jedem Upload können maximal 1000 Datensätze übermittelt werden. Nach erfolgreichem Upload können Sie die einzelnen Schlüssel in den Gerätedetails des jeweiligen Geräts anzeigen.

10.10.8.41. Windows Kiosk-Konfiguration

Mit der Windows Kiosk-Konfiguration können Sie einen Kiosk mit einer oder mehreren Apps auf Geräten mit Windows 10 konfigurieren. Bei dieser Konfiguration können Kioskbenutzer nicht auf Funktionen außerhalb der Kiosk-Apps zugreifen. Für diese Konfiguration muss Windows Bridge aktiviert sein.

Es gibt 3 Modi, in denen die Konfiguration angewendet werden kann.

- Einzelne Anwendung
- Mehrere Anwendungen (Liste der Anwendungen vom Windows-Gerät abrufen)
- Mehrere Anwendungen (ein vorhandenes Layout aus der Startmenü-Konfiguration auswählen)

> Anwendungen, die für eine Windows Kiosk-Konfiguration verwendet werden, sollten bereits auf einem Gerät vorhanden sein, bevor Sie in einen konfigurierten Windows Kiosk-Modus wechseln.

So richten Sie die Windows Kiosk-Konfiguration ein:

1. Gehen Sie zu **Konfiguration > +Hinzufügen**.
2. Wählen Sie die **Windows Kiosk**-Konfiguration.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Definieren Sie in dem Abschnitt Konfigurations-Setup die übrigen Einstellungen aus der folgenden Tabelle.

Einstellung	Aktion
Wählen Sie den Kioskmodus: Wählen Sie eine der folgenden 3 Optionen.	
Einzelne Anwendung	Wählen Sie diese Option aus, um den Kioskmodus für eine einzelne Anwendungen für ein Gerät zu konfigurieren. 1. Wählen Sie im Abschnitt **Windows-Gerät auswählen (optional)** Windows 10-Gerät aus. Klicken Sie auf **Apps vom Gerät abrufen**, um die Liste der Apps von einem Gerät anzuzeigen. Das ausgewählte Gerät muss von Ihnen überwacht werden und erfordert eine Anmeldung, um App-Daten erfolgreich abzurufen. **Um diese Schritte zu überspringen, wählen Sie die Option Diesen Schritt überspringen.Sie können Ihre Meinung bei Bedarf später ändern**. 2. Klicken Sie auf **Aus abgerufener App-Liste hinzufügen**, um Apps aus der abgerufenen Liste hinzuzufügen. 3. Wählen Sie eine einzelne App aus, indem Sie auf das Optionsfeld in der App-Spalte **Name** klicken. Klicken Sie auf **Neue hinzufügen**, um eine neue App zur Liste hinzuzufügen. Klicken Sie zum Löschen einer App aus der Liste auf das Symbol „Löschen“.
Mehrere Anwendungen (Liste der Anwendungen vom Windows-Gerät abrufen)	Wählen Sie diese Option aus, um den Kioskmodus für mehrere Anwendungen für ein Gerät zu konfigurieren. 1. Wählen Sie im Abschnitt **Windows-Gerät auswählen (optional)** Windows 10-Gerät aus. Klicken Sie auf **Apps vom Gerät abrufen**, um die Liste der Apps von einem Gerät abzurufen. Das ausgewählte Gerät muss von Ihnen überwacht werden und erfordert eine Anmeldung, um App-Daten erfolgreich abzurufen. **Um diese Schritte zu überspringen, wählen Sie die Option Diesen Schritt überspringen.Sie können Ihre Meinung bei Bedarf später ändern**. 2. Klicken Sie unter **Kiosk-Apps und Startmenü-Layout** auf **Aus abgerufener App-Liste hinzufügen**. Das Fenster **Kiosk-App wählen** wird angezeigt. Wählen Sie die App(s) aus der abgerufenen Liste aus und klicken Sie auf **Ausgewählte App verwenden**. 3. Klicken Sie im Abschnitt „Zusätzliche zulässige Apps“ auf Aus abgerufener App-Liste hinzufügen.Das Fenster **Kiosk-App wählen** wird angezeigt. Wählen Sie die App(s) aus der abgerufenen Liste aus und klicken Sie auf **Ausgewählte App verwenden**. Zusätzliche erlaubte Apps sind die Apps, die als Abhängigkeiten für die ausgewählten Apps im Kiosk-Apps und Startmenü-Layoutbetrachtet werden. Ohne „erlaubte Apps“ verhindert das Betriebssystem den Start dieser Anwendung, selbst wenn das Anwendungssymbol im Startmenü angezeigt wird. 4. Klicken Sie auf **Neue hinzufügen**, um eine neue App zur Liste hinzuzufügen. Klicken Sie auf das Symbol „Löschen“, um eine App aus der Liste zu löschen. Sie können eine App an eine beliebige Position in der Liste ziehen und verschieben. 5. Wählen Sie in den **Weiteren Einstellungen für mehrere Apps** die gewünschten Optionen aus: ◦ **Ein-/Ausschalter ausblenden**

Einstellung	Aktion
	◦ **Benutzeranzeige ausblenden** ◦ **Taskleiste ausblenden** In Microsoft Windows 11 wird die Option **Taskleiste ausblenden** des Multi-App-Kiosk-Modus nicht unterstützt.
Mehrere Anwendungen (ein vorhandenes Layout aus der Startmenü-Konfiguration auswählen)	Wenn Sie eine Layoutkonfiguration für das Startmenü erstellt haben, können Sie die Konfiguration importieren und durch Auswahl dieser Option den Modus für mehrere Anwendungen konfigurieren. 1. Wählen Sie im Abschnitt **Layout auswählen** ein Layout aus, das zuvor als Startmenü konfiguriert wurde. Zuvor erstellte Konfigurationen mit anwendbaren Layout-Parametern werden in der Dropdown-Liste unten angezeigt. 2. Wählen Sie in den weiteren Einstellungen für mehrere Apps die erforderlichen Optionen aus: ◦ **Ein-/Ausschalter ausblenden** ◦ **Benutzeranzeige ausblenden** ◦ **Taskleiste ausblenden** In Microsoft Windows 11 wird die Option **Taskleiste ausblenden** des Multi-App-Kiosk-Modus nicht unterstützt.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:

- Alle Geräte
- Keine Geräte (Standard)
- Anpassbar

8. Klicken Sie auf **Fertig**.

> Damit die Konfiguration vollständig wirksam wird, muss das Gerät nach der Übernahme oder Aktualisierung einer Windows Kiosk-Konfiguration neu gestartet werden. Für manche Anwendungen einer Multi-App-Kioskkonfiguration ist ein zweiter Neustart des Geräts erforderlich. Bei der ersten Anmeldung werden einige Symbole möglicherweise nicht angezeigt, die fehlenden Symbole erscheinen jedoch nach dem zweiten Neustart.

Das Gerät muss neu gestartet werden, nachdem eine Kiosk-Konfiguration übernommen, gelöscht oder aktualisiert wurde. Dies kann mit dem Befehl „Gerät neu starten/herunterfahren“ im Aktionsmenü des Geräts erfolgen. Ohne Neustart:

- Das Gerät wird nach der Übernahme einer Kiosk-Konfiguration nicht automatisch in den Kiosk-Modus versetzt.
- Das Gerät beendet den Kiosk-Modus nicht automatisch, nachdem eine verwendete Kiosk-Konfiguration gelöscht wurde.
- Das Gerät ändert die laufende Kiosk-Konfiguration nicht.

Wenn ein Gerät mit einer Kiosk-Konfiguration eine aktualisierte Konfiguration erhält, entfernt das Windows-Betriebssystem auf dem Gerät einen vorhandenen Kioskbenutzer und erstellt einen neuen Kioskbenutzer mit einer neuen Kioskkonfiguration. Die Sitzung für den aktuellen Benutzer sollte explizit mit dem Neustart des Geräts beendet werden.

Vorzugsweise sollte die Konfiguration für eine Kiosk-Konfiguration für mehrere Anwendungen mit '.lnk' -Dateien und für eine Kiosk-Konfiguration mit einer Anwendung mit '.exe'-Dateien erfolgen. Eine importierte Startmenü-Konfiguration eines Geräts verwendet das

Format '.lnk'. Startmenüelemente, die manuell für '.exe'-Anwendungen erstellt wurden, werden möglicherweise je nach '.exe'-Anwendung nicht im Startmenü der Kiosk-Konfiguration für mehrere Anwendungen angezeigt.

Beispielsweise kann Windows Media Player mit einer der folgenden '.lnk'-Dateien zum Startmenü hinzugefügt werden:

- %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Media Player.lnk
- %ALLUSERSPROFILE%\Microsoft\\Windows\Start Menu\Programs\Windows Media Player.lnk

Wenn diese Anwendung direkt mit einer der folgenden '.exe'-Dateien hinzugefügt wird, erscheint kein entsprechendes Symbol, selbst wenn der erste '.exe'-Pfad intern in den oben genannten '.lnk'-Dateien verwendet wird:

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
- C:\Program Files\Windows Media Player\wmplayer.exe

Für die Kiosk-Konfiguration mit einer Anwendung können Sie Argumente zur exe-Datei hinzufügen. E.g. '%Programme%\Internet Explorer\iexplore.exe -k www.bing.com'. Das Symbol für die exe-Anwendung mit Argumenten wird jedoch bei einer Konfiguration mit mehreren Anwendungen nicht im Startmenü angezeigt. Wenn Sie eine exe-Anwendung mit Argumenten in der Kiosk-Konfiguration für mehrere Anwendungen benötigen, verwenden Sie die '.lnk'-Datei, die intern Argumente enthalten kann. '.lnk' funktioniert nicht bei einer Kiosk-Konfiguration mit einer einzelnen Anwendung.

Abhängigkeiten im Kiosk-Modus für mehrere Anwendungen

Bei Win32/64-Anwendungen kann es erforderlich sein, dass Abhängigkeiten im Abschnitt „Zusätzliche zulässige Apps“ im Kioskmodus für mehrere Anwendungen hinzugefügt werden. Für einen Kiosk-Modus mit einer einzigen Anwendung sind keine zusätzlichen zulässigen Apps erforderlich.

Beispiel 1: Für die Windows Media Player-App sind im Kioskmodus für mehrere Anwendungen die folgenden Abhängigkeiten erforderlich:

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\setup_wm.exe

Die erste Abhängigkeit sind die Binärprogramme der Anwendung, die von der entsprechenden „.lnk“ -Datei aufgerufen werden. Die zweite Abhängigkeit ist ein einmaliger Assistent, der aus der ersten Abhängigkeit aufgerufen wird.

Ohne „Zulässige Apps“ kann das Betriebssystem diese Anwendung nicht ausführen, auch wenn das Anwendungssymbol im Startmenü angezeigt wird.

Beispiel 2: Für Internet Explorer wird das Symbol im Startmenü angezeigt, wenn es mit einem Element aus der folgenden Liste konfiguriert ist:

- %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 erfordert die folgenden Abhängigkeiten:

- 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

Die erste Abhängigkeit sind App-Binärprogramme, die nur für das Element '.lnk' erforderlich sind, die anderen Abhängigkeiten sind für den einmaligen Assistenten. Ohne die erste Abhängigkeit blockiert das Betriebssystem die App mit dem Popup-Fenster. Ohne weitere Abhängigkeiten wird die Anwendung unmittelbar nach dem Start ohne weitere Benachrichtigungen vom Betriebssystem geschlossen.

10.10.8.42. Konfiguration der Windows-Lizenz

Die Konfiguration der Windows-Lizenz aktualisiert das Betriebssystem auf dem Gerät, beispielsweise von Windows 10 Pro auf Windows 10 Enterprise. Außerdem bietet diese Konfiguration die Möglichkeit, den Produktschlüssel von Desktops mit Windows 10 zu aktivieren oder zu ändern.

Windows-Lizenz aktualisieren:

1. Gehen Sie zu **Konfiguration > +Hinzufügen** .
2. Klicken Sie auf **Windows-Lizenz**-Konfiguration.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie in dem Abschnitt **Konfigurations-Setup** den **Produktschlüssel** ein.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie eine der folgenden Verteilungsoptionen aus:
    - Alle Geräte
    - Keine Geräte (Standard)
    - Anpassbar
7. Klicken Sie auf **Fertig**.

11. Richtlinien

Richtlinien bestimmen Voraussetzungen für Geräte und erläutern zudem, was passiert, wenn ein Gerät diese Voraussetzungen nicht erfüllt. Jede Richtlinie besteht aus einer Regel und einer Compliance-Aktion (die durchgeführt wird, wenn die Regel verletzt wird). Nutzen Sie die Seite Richtlinien zum Auswählen, Einrichten und Verteilen von Richtlinien.

> Für den automatisierten Geräte-Check-in beachten Sie bitte folgende Änderungen:

- Es werden nur die Geräte ausgewertet, die in den letzten 90 Tagen eingecheckt haben.
- Nur der Befehl "Check-in erzwingen" wird auch auf Geräten ausgelöst, die vor mehr als 90 Tagen und bis zu einem Jahr vorher zuletzt eingecheckt haben.
- Es wird keine Aktion auf Geräten ausgeführt, die im letzten Jahr gar nicht eingecheckt haben.

Dieser Abschnitt enthält die folgenden Themen:

- **Arbeiten mit Richtlinien**
- **Anpassbare Richtlinie**
- **Zulässige Apps überwachen und kontrollieren**
- **Prioritäten für Richtlinien**
- **Windows-Hardwarerichtlinie**

11.1. Arbeiten mit Richtlinien

Dieser Abschnitt enthält die folgenden Themen:

- Richtlinie implementieren
- Compliance-Aktionen
- Vorhandene Richtlinie suchen
- Richtlinie hinzufügen
- Richtlinie bearbeiten
- Richtlinie löschen

Richtlinie implementieren

Richtlinien bestimmen Voraussetzungen für Geräte und erläutern zudem, was passiert, wenn ein Gerät diese Voraussetzungen nicht erfüllt. Jede Richtlinie besteht aus einer Regel und einer Compliance-Aktion (die durchgeführt wird, wenn die Regel verletzt wird). Nutzen Sie die Seite Richtlinien zum Auswählen, Einrichten und Verteilen von Richtlinien.

Folgende Richtlinienarten stehen zur Verfügung:

Typ	Vorgesehene Funktion
Kompromittierte Geräte	Priorität (1 = höchste) Verstoß 1 Gefährdetes Plugin 2 Client manipuliert 3 Unbekannter Gerätehersteller: unbekannt 4 Verdächtiger Ordner erkannt: [Pfad] 5 Verdächtige Binärdatei gefunden: [Pfad] 6 Ordner /data ist durchsuchbar ODER Ordner /data/data ist durchsuchbar 7 Gefunden /system/app/Superuser.apk 8 Paketmanager gefährdet 9 Verdächtige App gefunden: [Paket] Markiert Geräte, die durch Jailbreaks (iOS) oder Roots (Android) gefährdet sind. Anzeige des Grundes für Schutzverletzungen, d. h. warum Android-Geräte bei Rooting als gefährdet eingestuft werden. 1. Klicken Sie auf die Registerkarte **Richtlinien** 2. Klicken Sie auf den Link **Gefährdete Geräte**. 3. Klicken Sie auf die Registerkarte **Aktive Verstöße**. 4. Klicken Sie auf den Grund für den Verstoß in der Verstoßspalte. Anzeige des Grundes für Schutzverletzungen, d. h. warum Android-Geräte bei Rooting als gefährdet eingestuft werden. 5. Klicken Sie auf die Registerkarte **Richtlinien**. 6. Klicken Sie auf den Link **Gefährdete Geräte**. 7. Klicken Sie auf die Registerkarte **Aktive Verstöße**. 8. Prüfen Sie den Grund für den Verstoß in der Spalte **Verstoß**. Folgende Gründe kommen in Frage:
Datenschutz/-verschlüsselung deaktiviert (nur macOS)	Markieren Sie die macOS-Geräte, bei denen kein Passcode bzw. keine Verschlüsselung aktiviert ist.
Internationales Roaming	Markiert Geräte, bei denen Gebühren für internationales Roaming entstehen könnten. Der Status wird aktualisiert, wenn das Gerät angemeldet wird. Bei iOS nutzt der Service Roaming-Markierung als von iOS eingestellt und gemeldet. Die Compliance-Aktion wird nur vom ersten Verstoß ausgelöst.
MDM-/Geräteadministration deaktiviert	Wenn das Gerät für MDM deaktiviert ist, wird es beim Anmelden nicht auf andere Richtlinien oder die Deltaverarbeitung von Konfigurationen oder Anwendungen geprüft.
Kein Kontakt	Markiert Geräte, die im angegebenen Zeitraum keinen Kontakt mit der Cloud hatten. Wählen Sie die auszuführenden Aktionen aus, wenn das Gerät sich für eine bestimmte Anzahl von Stunden (2 bis 3 bis 23 bis 24) oder für eine bestimmte Anzahl von Tagen nicht angemeldet hat.

Typ	Vorgesehene Funktion
Kein Kontakt mit MI-Client (nur iOS)	Ivanti Neurons for MDMMarkiert Clients, die im angegebenen Zeitraum keinen Kontakt mit der Cloud hatten. Wählen Sie die auszuführenden Aktionen aus, wenn der Client sich für eine bestimmte Anzahl von Stunden (2 bis 3 bis 23 bis 24) oder für eine bestimmte Anzahl von Tagen nicht angemeldet hat. Dies gilt auch für über iReg registrierte Geräte. Die Richtlinie kennzeichnet ein Gerät als nicht konform, wenn kein Client vorhanden ist oder der Client sich in einem definierten Zeitraum nicht angemeldet hat.
Zulässige Apps	Markiert Geräte, die Regeln für zulässige oder erforderliche Apps verletzen.
Anpassbare Richtlinie	Erstellen Sie eine anpassbare Richtlinie entsprechend den Bedingungen und Aktionen, die Sie festgelegt haben.

Compliance-Aktionen

Folgende Compliance-Aktionen stehen zur Verfügung:

Compliance-Aktion	Vorgesehene Funktion
Anzeigen	Markiert das Gerät auf der Geräteseite von Ivanti Neurons for MDM. Standardmäßig ist diese Option aktiviert.
Sperren	Weist Access und/oder Sentry an, ein Gerät zu sperren, wenn dieses versucht, über Sentry oder Access auf eine Ressource zuzugreifen, nachdem gemäß den Angaben der letzten Anmeldung gegen die Richtlinie verstoßen wurde.

Nachricht an Benutzer senden	• Markiert das Gerät auf der Geräteseite von Ivanti Neurons for MDM.
	• Sendet eine E-Mail an den Eigentümer des Geräts
	• Zusätzlich zu den vorhandenen Richtlinien ist der Umschalter **E-Mail-Vorlage für die Compliance-Richtlinie verwenden** nun auch für folgende Richtlinien verfügbar:
	  ◦ Data Protection/Datenverschlüsselung deaktiviert
	  ◦ Internationales Roaming
	  ◦ MDM-/Geräteadministration deaktiviert
	  ◦ Kein Kontakt
	  ◦ MI-Client ohne Kontakt
	  Sendet eine Push-Benachrichtigung an das Gerät

Quarantäne	• Entfernt die meisten Konfigurationen von dem Gerät. ◦ Ausnahmen: Passwortkonfigurationen, WLAN-Konfigurationen für Geräte, die nur über WLAN verfügen; Konfigurationen für Einschränkungen (iOS) • Entfernt alle von Ivanti Neurons for MDM installierten Apps. • Entfernt sämtlichen Content, der über die Cloud verteilt wurde, auch iBook- und ePub-Dateien. • Blockiert den Zugriff auf Ivanti Neurons for MDM-Kataloge. • Verhindert Aufforderungen zur Installation weiterer Apps • Sperrt den Zugriff auf AppConnect-fähige Apps. • Mit Unterstützung für AppConnect-fähige Apps. • Wenn diese Option aktiviert ist, werden private Apps auf der privaten Seite des unter Quarantäne gestellten Geräts zeitweilig deaktiviert, um anzuzeigen, dass der Gerätebenutzer die Compliance-Probleme auf dem Gerät beheben muss, um es wieder funktionsfähig zu machen. Wird auf Geräten mit Android 11+ unterstützt, die als Arbeitsprofil auf unternehmenseigenen Geräten bereitgestellt werden.
Zusätzliche Quarantäneaktionen (optional):	**Neue App-Downloads sperren** – Verhindert das Herunterladen neuer Apps auf das Gerät. **Verwaltete Anwendungen in Quarantäne verschieben** – Entfernt alle über Ivanti Neurons for MDM verwalteten Apps von dem Gerät und aktiviert die Option "Neue App-Downloads sperren", um zu verhindern, dass die Apps erneut auf dem Gerät installiert werden können. Wählen Sie eine der folgenden Optionen aus: • **Alle Anwendungen** • **Alle Apps entfernen, außer Folgende** – Entfernt alle Anwendungen mit Ausnahme derjenigen, die zur Anwendungsliste hinzugefügt wurden.

Compliance -Aktion	Vorgesehene Funktion
	• **Designierte Anwendungen** - Fügen Sie eine oder mehrere Anwendungen durch Suchen oder manuell (über die Bundle-ID oder den Paketnamen) hinzu. Klicken Sie auf die Registerkarte **Apps anzeigen** , um die Liste der hinzugefügten Apps zu überprüfen. Die Standard-Quarantänemaßnahme zum Blockieren des App Store-Zugriffs ist nicht mehr verfügbar. Auf bestimmten Geräten wird durch die Aktion "Quarantäne" die Anwendung aufgrund bestimmter Gerätebeschränkungen nicht vom Gerät entfernt. Diese Option ist standardmäßig ausgewählt (für: Alle Anwendungen, Alle Apps entfernen, außer Folgende und Zugewiesene Anwendungen) und kann nicht deaktiviert werden. Dadurch wird verhindert, dass die Apps auf dem Gerät neu installiert werden. **Konfigurationen entfernen** – Entfernt Ivanti Neurons for MDM-Konfigurationen vom Gerät. Wählen Sie eine der folgenden Optionen aus: • **Alle Konfigurationen** • **Designierte Konfigurationen** - Wählen Sie eine oder mehrere Konfigurationen aus der Liste aus oder suchen Sie nach ihnen. Klicken Sie auf die Registerkarte **Ausgewählte Konfigurationen**, um die Liste der ausgewählten Konfigurationen zu überprüfen. **Zugewiesene Konfigurationen per Push senden** – Verteilen Sie die zugewiesenen Konfigurationen im Rahmen der benutzerdefinierten Compliance. Diese Liste enthält Konfigurationen, die folgenden Kriterien erfüllen: • Aktivierte Konfiguration • Systemfremde Konfiguration • Quarantänefähige Konfiguration • Konfigurationen, die im aktuellen Space erstellt oder aus dem Standard-Space delegiert wurden. Die Liste der nicht quarantänefähigen Konfigurationen finden Sie unter Nicht quarantänefähige Konfigurationen. **Inhalt entfernen** – Entfernt den gesamten Inhalt und die Medien in Verbindung mit den Apps, die über Ivanti Neurons for MDM verteilt wurden, vom Gerät. **Private Apps suspendieren**Deaktivieren Sie Apps auf der privaten Seite des unter Quarantäne gestellten Geräts vorübergehend, um anzugeben, dass der Gerätebenutzer die Compliance-Probleme auf dem Gerät beheben muss, um es wieder funktionsfähig zu machen. Wird auf Geräten mit Android 11+ unterstützt, die als Arbeitsprofil auf unternehmenseigenen Geräten bereitgestellt werden.

Vorhandene Richtlinie suchen

Sie können mit Filtern und der Suchfunktion auf der Seite „Richtlinien“ eine oder mehrere bestehende Richtlinien finden.

Verfahren

1. Gehen Sie zu **Richtlinien**.
2. Um eine Liste nach Richtlinien mit bestimmten Kriterien zu filtern, klicken Sie auf **Filter**.
3. Wählen Sie mindestens ein Filterkriterium aus.
4. Um eine bestehende Richtlinie anhand ihres Namens zu suchen, geben Sie den Namen der Richtlinie in das Feld **Suche** ein.

Richtlinie hinzufügen

Verfahren

1. Gehen Sie zu **Richtlinien**.
2. Klicken Sie (oben rechts) auf +**Hinzufügen**.
3. Wählen Sie einen Richtlinientyp aus.
4. Ergänzen Sie die Einstellungen.
5. Wählen Sie die Gerätegruppen aus, die diese Richtlinie erhalten sollen.

> Sie können bis zu 100 Konfigurationsdateien auf einmal verteilen.

6. Klicken Sie auf **Fertig**.

Richtlinie bearbeiten

Verfahren

1. Gehen Sie zu **Richtlinien**.
2. Klicken Sie für die Suche nach der gewünschten Richtlinie auf das **Bearbeitungssymbol** (Bleistift) unter der Spalte „Aktionen“.
3. Nehmen Sie Ihre Änderungen vor.
4. Sichern Sie die Änderungen.

Richtlinie löschen

Verfahren

1. Gehen Sie zu **Richtlinien**.
2. Klicken Sie für die erforderliche Richtlinie auf das **Entfernungssymbol** in der Spalte „Aktionen“.
3. Klicken Sie zur Bestätigung auf **Ja**.

Wenn Sie die Seite „Richtlinien“ nicht sehen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie brauchen eine der folgenden **Rollen**:

- Geräteverwaltung
- Geräts schreibgeschützt

Weitere Informationen finden Sie unter **Richtlinien priorisieren**.

11.2. Anpassbare Richtlinie

Richtlinien

Lizenz: Platinum

Berechtigte Geräte: Android, iOS, Mac OS, Windows.

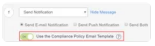
Sie können eine kundenspezifische Richtlinie für ein Gerät und die Benutzer-Attribute, Abschnittskriterien, Werte und Compliance-Aktionen erstellen, die Sie festlegen.

> Auch die Android-Sicherheitspatch-Einstellung kann zur Definition einer benutzerdefinierten Richtlinie verwendet werden.

Kundenspezifische Richtlinie hinzufügen

1. Gehen Sie zu **Richtlinien**.
2. Klicken Sie auf **+Hinzufügen**.
3. Wählen Sie die Option **Anpassbare Richtlinie**.
4. Geben Sie einen Namen für die anpassbare Richtlinie ein.
5. Klicken Sie gegebenenfalls auf **+ Beschreibung hinzufügen**, um weitere Details einzugeben.
6. Definieren Sie mit dem Rule Builder Bedingungen, die Aktionen auslösen, wenn die Bedingungen sich als wahr erweisen. Eine Anleitung zur Erstellung der Bedingungen finden Sie im Abschnitt **Einstellung der Bedingungen**. Der Ivanti Neurons for MDM-Administrator zeigt die Anzahl doppelter Benutzergruppen und die zugehörige Anzahl der GUIDs an, damit doppelte Gruppen identifiziert werden können, wenn das Attribut "Name der Benutzergruppe" im Regeleditor ausgewählt wird. Eine Tabelle unter dieser Regel zeigt außerdem die Liste der doppelten Benutzergruppen zusammen mit Details wie Name der Benutzergruppe, GUID, Quelle und Distinguished Name (DN).
7. Wählen Sie eine der Compliance-Maßnahmen (siehe Standardmaßnahmen unten), die ergriffen werden sollen, wenn die angegebenen Bedingungen erfüllt sind. Wird die Aktion „**Warten**“ zwischen anderen Aktionen eingefügt, haben die Gerätebenutzer Zeit, ihre Geräte zu aktualisieren und wieder die Compliance-Richtlinien zu erfüllen, bevor weitere Maßnahmen eingeleitet werden. Sie können beispielsweise eine Warnmitteilung senden und dann 24 Stunden warten, bevor Sie eine Quarantänemaßnahme einleiten.
8. Wählen Sie die Option **Benachrichtigung senden, wenn das Gerät wieder konform ist**, die standardmäßig deaktiviert ist.

- **E-Mail-Benachrichtigung senden** – Sendet eine E-Mail an die E-Mail-Adresse des Gerätebenutzers, wenn das Gerät wieder den Compliance-Anforderungen entspricht.
  - Aktivieren Sie die Option **E-Mail-Vorlage der Compliance-Richtlinien verwenden**, um die Nachricht, die Sie hier konfigurieren, in die E-Mail-Vorlage zur Richtlinienbenachrichtigung einzufügen. Konfigurieren Sie diese wie unter **E-Mail-Vorlage anpassen** in **Branding von E-Mail-Vorlagen** beschrieben. Einen Überblick finden Sie unter **Benachrichtigungs-E-Mails zur Einhaltung von Richtlinien konfigurieren und verwenden**

    
  - Sie können die Mitteilungen anpassen, indem Sie optionale Ersatzvariablen einfügen, um den Empfängern weitere Details über Richtlinienverletzungen und sonstige relevante Informationen mitzuteilen. Klicken Sie auf die folgenden Attributarten, um die komplette Variablenliste anzuzeigen:
    - Richtlinienattribute wie $, $ und $.
    - Benutzer-Attribute wie $, $ und $

    - Geräte-Attribute wie $, $ und $
    - Benutzerdefinierte Geräte-/Benutzer-/LDAP-Attribute, die über die Seite **Admin > Attribute** erstellt werden.

- **Push-Benachrichtigung senden:** Sendet eine Push-Benachrichtigung an das Gerät, wenn das Gerät wieder den Compliance-Anforderungen entspricht.
- **Beide senden** - Sendet sowohl eine Push-Benachrichtigung an das Gerät als auch eine E-Mail an die E-Mail-Adresse des Gerätebenutzers, wenn das Gerät wieder die Compliance-Anforderungen erfüllt. Sie können die Mitteilungen anpassen, indem Sie optionale Ersatzvariablen verwenden, die den Empfängern weitere Details übermitteln, wie bereits im Abschnitt „E-Mails versenden“ beschrieben.

9. Geben Sie die folgenden Optionen aus der Tabelle an, um Administratoren und Gerätebesitzer zu benachrichtigen, falls die Gerätebenutzer gegen die Regeln der Richtlinie verstoßen:

Option	Beschreibung
Betreff	Geben Sie den Text für den Betreff ein. Beispiel: "Sie haben gegen eine Richtlinie verstoßen!".
Textkörper	Geben Sie die gewünschte Nachricht ein. Beispiel: "Aktion erforderlich!".
E-Mail-Benachrichtigung nur an Administratoren senden	Wählen Sie diese Option aus, um E-Mail-Benachrichtigungen nur an Administratoren zu senden.
CC an Administratoren	Dieses Textfeld ist nicht verfügbar, wenn Sie die Option "E-Mail-Benachrichtigung nur an Administratoren senden" ausgewählt haben.
Geben Sie die E-Mail-Adressen der Administratoren ein.	Geben Sie die E-Mail-ID der Administratoren ein. Trennen Sie mehrere E-Mail-Adressen durch einen Strichpunkt (;).
Vorschau der E-Mail	Klicken Sie auf die Schaltfläche **Vorschau der E-Mail**, um die E-Mail-Adresse anzuzeigen.

10. Klicken Sie auf **Weiter**, um die Richtliniendetails zu speichern.

Standardaktionen:

1. Klicken Sie zur Bestätigung auf das Kontrollkästchen **Ja**, wenn eine Ergänzung der verknüpften Richtlinie eine bisherige Richtlinie und entsprechende Compliance-Aktionen, die bereits einmal auf dem Gerät ausgelöst wurden, zurücksetzen soll. Die neue, angepasste Richtlinie wird mit der nächsten Geräteanmeldung wirksam. Wenn Sie die Abschaltaktion ausgewählt haben, klicken Sie zur Bestätigung nochmals auf **Ja**, da diese Aktion nicht rückgängig gemacht werden kann.

- **Monitor** - Derzeit immer ausgewählt. Wenn Sie verknüpfte Compliance-Aktionen nutzen wollen, benötigen Sie Sentry Version 9.0.0 oder höher.
- **Nichts tun**
- **Benachrichtigung senden**
- **E-Mail senden** – Sendet eine E-Mail an die E-Mail-Adresse des Gerätebenutzers, wenn das Gerät nicht mehr den Compliance-Anforderungen entspricht.
    - Sie können die E-Mail-Vorlage für die Richtlinienbenachrichtigung wie oben beschrieben verwenden.
    - Sie können die Mitteilungen anpassen, indem Sie optionale Ersatzvariablen einfügen, um den Empfängern weitere Details über Richtlinienverletzungen und sonstige relevante Informationen mitzuteilen. Auf diese Weise erhalten die Benutzer mit

nicht der Compliance entsprechenden Geräten relevante Informationen über die Richtlinienverletzung, sodass sie entsprechende Gegenmaßnahmen ergreifen können. Klicken Sie auf die folgenden Attributarten, um die komplette Variablenliste anzuzeigen:

- Richtlinienattribute wie $, $ und $.
- Benutzer-Attribute wie $, $ und $
- Geräte-Attribute wie $, $ und $
- Benutzerdefinierte Geräte-/Benutzer-/LDAP-Attribute, die über die Seite **Admin > Attribute** erstellt werden.

- **Push-Benachrichtigung senden:** Sendet eine Push-Benachrichtigung an das Gerät, dass das Gerät nicht mehr die Compliance-Anforderungen erfüllt.
- **Beides senden -** Wählen Sie diese Option, um eine Push-Benachrichtigung an das Gerät und eine E-Mail an die E-Mail-Adresse des Gerätebenutzers zu senden, dass sein Gerät nicht mehr die Compliance-Anforderungen erfüllt. Sie können die Mitteilungen anpassen, indem Sie optionale Ersatzvariablen verwenden, die den Empfängern weitere Details übermitteln, wie bereits im Abschnitt „E-Mails versenden“ beschrieben.
- **Sperren:** Sperrt mit Sentry die verwalteten Geräte, damit sie nicht mehr auf E-Mails und AppConnect-fähige Apps zugreifen können. Für die Sperre wird Sentry in der Version 9.0.0 oder höher benötigt.
- **Außer Dienst:** Stellt das Gerät außer Dienst. Diese Aktion kann nicht rückgängig gemacht werden. Sie können beispielsweise eine Regel definieren, dass Geräte für alle deaktivierten Benutzer mit der Bedingung „Benutzer aktiviert“ abgeschaltet werden.
- **Warten:** Verzögert die Aktion für eine definierte Zeit (Stunden oder Tage), damit der Benutzer Gelegenheit hat, die Richtlinienverletzung zu beseitigen, bevor weitere Aktionen ergriffen werden, weil das Gerät nicht mehr den Compliance-Anforderungen entspricht.
- **Quarantäne:** Verhindert einen Zugriff auf Apps, Content und Server mit folgenden Maßnahmen:

(Optional) zusätzliche Quarantäne-Aktionen	Beschreibung
Verwaltete Anwendungen in Quarantäne stellen	Entfernt alle über die Cloud verwalteten Apps von dem Gerät und sperrt neue App-Downloads, so dass keine Apps neu auf dem Gerät installiert werden können. Wählen Sie eine der folgenden Optionen aus: • **Alle Anwendungen** • **Designierte Anwendungen** - Fügen Sie eine oder mehrere Anwendungen durch Suchen oder manuell (über die Bundle-ID oder den Paketnamen) hinzu. Klicken Sie auf die Registerkarte **Apps anzeigen** , um die Liste der hinzugefügten Apps zu überprüfen. Die Standard-Quarantänemaßnahme zum Blockieren des App Store-Zugriffs ist nicht mehr verfügbar. Auf bestimmten Geräten wird durch die Aktion "Quarantäne" die Anwendung aufgrund bestimmter Gerätebeschränkungen nicht vom Gerät entfernt.
Neue App Downloads sperren	Sperrt den Download neuer Apps für das Gerät. Wählen Sie eine der folgenden Optionen aus: • **Alle Anwendungen** • **Designierte Anwendungen** - Fügen Sie eine oder mehrere Anwendungen durch Suchen oder manuell (über die Bundle-ID oder den Paketnamen) hinzu. Klicken Sie auf die Registerkarte **Apps anzeigen** , um die Liste der hinzugefügten Apps zu überprüfen. Die Standard-Quarantänemaßnahme zum Blockieren des App Store-Zugriffs ist nicht mehr verfügbar. Standardmäßig ist diese Option ausgewählt (sowohl für alle Anwendungen als auch für bestimmte Anwendungen) und kann nicht deaktiviert werden. Dadurch wird verhindert, dass die Apps auf dem Gerät neu installiert werden.
Konfigurationen entfernen	Entfernt Ivanti Neurons for MDM-Konfigurationen vom Gerät. Wählen Sie eine der folgenden Optionen aus: • **Alle Konfigurationen** • **Designierte Konfigurationen** - Wählen Sie eine oder mehrere Konfigurationen aus der Liste aus oder suchen Sie nach ihnen. Klicken Sie auf die Registerkarte **Ausgewählte Konfigurationen**, um die Liste der ausgewählten Konfigurationen zu überprüfen.
Zugewiesene Konfigurationen per Push senden	Verteilen Sie die angegebenen Konfigurationen im Rahmen der benutzerdefinierten Compliance. Diese Liste enthält Konfigurationen, die folgenden Kriterien erfüllen: • Aktivierte Konfiguration • Systemfremde Konfiguration • Quarantänefähige Konfiguration • Konfigurationen, die im aktuellen Space erstellt oder aus dem Standard-Space delegiert wurden. Die Liste der nicht quarantänefähigen Konfigurationen finden Sie unter Nicht quarantänefähige Konfigurationen. Weitere Informationen finden Sie im Abschnitt **Angegebene Konfiguration per Push senden** im Anschluss an dieses Verfahren.
Inhalt entfernen	Entfernt den gesamten Content und die Medien, die mit Apps verbunden sind, welche über die Cloud von dem Gerät verteilt wurden.

(Optional) zusätzliche Quarantäne-Aktionen	Beschreibung
Private Apps suspendieren	Apps auf der privaten Seite des unter Quarantäne gestellten Geräts zeitweilig deaktivieren, damit der Gerätebenutzer die Compliance-Probleme auf dem Gerät behebt, um es wieder funktionsfähig zu machen. Wird auf Geräten mit Android 11+ unterstützt, die als Arbeitsprofil auf unternehmenseigenen Geräten bereitgestellt werden.
Standard-Quarantänemaßnahmen: Diese Aktionen werden immer durchgeführt.	
App-Speicherzugriff sperren	Verhindert, dass das Gerät über die Cloud auf App Stores zugreift.
Content Store-Zugriff sperren	Verhindert, dass das Gerät über die Cloud auf den Content Store zugreift.
AppConnect sperren	Verhindert, dass das Gerät die AppConnect-Funktionen verwendet.
AppTunnel sperren	Verhindert, dass Apps auf dem Gerät auf Content und Servers über AppTunnel zugreifen.
ActiveSync sperren	Verhindert, dass das Gerät über den ActiveSync-Server auf E-Mails zugreift.

2. Klicken Sie auf **Weiter**, um zu konfigurieren, für welche Geräte die Richtlinie und die Aktionen gelten sollen.
3. Klicken Sie auf **Fertig**.

Die folgende Tabelle zeigt das Quarantäne-Verhalten verschiedener Android-Geräten, wenn die Ivanti Neurons for MDM der Initiator der Quarantäneaktion ist:

Geräten	Quarantäne-Verhalten
Samsung-Geräte im Geräteverwaltungsmodus über die Go-Client-App	• Verwaltete öffentliche und interne Apps deinstallieren • Bestimmte Profile (außer MobileIron Threat Defense und andere) entfernen
Nicht-Samsung-Geräte im Geräteverwaltungsmodus über die Go-Client-App MAM über die AppStation-App	• Deinstallation oder Ausblenden von verwalteten öffentlichen und internen Apps nicht unterstützen • Bestimmte Profile (außer MobileIron Threat Defense und andere) entfernen
Android Enterprise über die Go-Client-App	• Verwaltete öffentliche und interne Apps verstecken • Bestimmte Profile (außer MobileIron Threat Defense und andere) entfernen

Angegebene Konfiguration per Push senden

Verteilen Sie die angegebenen Konfigurationen im Rahmen der benutzerdefinierten Compliance. Konfigurieren Sie die benutzerdefinierte Richtlinie zur Verteilung der Konfigurationen, wenn ein Gerät nicht mehr die Compliance-Anforderungen erfüllt. Zurücksetzen des Geräts in den vorherigen Zustand als Teil der Abhilfemaßnahme, wenn sich ein Gerätestatus von „nicht konform“ zu „konform“ ändert.

> Ein Fehler tritt dann auf, wenn ein Administrator versucht, eine benutzerdefinierte Richtlinie mit nicht delegierten Konfigurationen auf der Registerkarte „Angegebene Konfigurationen übertragen“ zu delegieren.

Im Folgenden wird das Verhalten beschrieben, wenn Konfigurationen unter bestimmten Bedingungen über benutzerdefinierte Richtlinien per Push übertragen werden:

Bedingungen	Verhalten
Es werden zwei Konfigurationen desselben Typs ausgewählt, die eine festgelegte Priorität haben.	Die Konfiguration mit der höheren Priorität wird per Push auf das Gerät übertragen.
Es sind zwei Konfigurationen des gleichen Typs ausgewählt, bei denen KEINE Priorität festgelegt ist.	Beide Konfigurationen werden auf das Gerät übertragen. Kann zu unerwartetem Verhalten führen.
Wenn das Gerät bereits über eine Konfiguration des gleichen Typs verfügt und die in der benutzerdefinierten Richtlinie definierte Priorität unterstützt. Wenn das Gerät bereits über eine Konfiguration des gleichen Typs verfügt und die in der benutzerdefinierten Richtlinie definierte Priorität NICHT unterstützt.	Die in der benutzerdefinierten Richtlinie definierte Konfiguration hat Vorrang und wird per Push auf das Gerät übertragen. Die auf dem Gerät vorhandene Richtlinie wird unabhängig von der Priorität entfernt (selbst wenn diese höher ist als die in der benutzerdefinierten Richtlinie definierte). Die in der benutzerdefinierten Richtlinie definierte Konfiguration wird per Push auf das Gerät übertragen. Beide Konfigurationen sind auf dem Gerät vorhanden. Kann zu unerwartetem Verhalten führen.
Wenn die Priorität einer Konfiguration geändert wird, nachdem die benutzerdefinierte Richtlinie erstellt wurde.	Bei der Anmeldung des Geräts wird die Konfiguration mit der höchsten Priorität per Push übertragen, wenn sie Teil der benutzerdefinierten Richtlinie ist.
Wenn beide Bedingungen erfüllt sind: • Bedingung A:Ein Gerät mit einem Verstoß hat eine Konfiguration als Teil einer benutzerdefinierten Richtlinie per Push übertragen (die Vorrang vor einer Konfiguration des gleichen Typs hatte, die bereits auf dem Gerät vorhanden war). • Bedingung B: Der Verstoß wurde behoben und das Gerät befindet sich nicht mehr in Quarantäne.	Die in der benutzerdefinierten Richtlinie definierte Konfiguration wird entfernt und die Konfiguration des gleichen Typs auf dem Gerät vor der Quarantäne durch die Verwendung bestehender Gerätegruppen per Push übertragen, so dass das Gerät wieder in seinen ursprünglichen Zustand versetzt wird.

Wenn Sie in der Aktion „Quarantäne“ neben „Angegebene Konfigurationen übertragen“ auch „Konfigurationen entfernen“ wählen, müssen Sie die folgenden Regeln beachten:

- Alle Konfigurationen entfernen + Angegebene Konfigurationen übertragen: In diesem Szenario werden alle Konfigurationen vom Gerät entfernt und die mit der Option „Angegebene Konfigurationen übertragen“ ausgewählten Konfigurationen auf das Gerät übertragen.

- Entfernen Sie designierte Konfigurationen (in einer benutzerdefinierten Richtlinie) + designierte Push-Konfigurationen (in einer anderen benutzerdefinierten Richtlinie) mit gemeinsamen Konfigurationen bei der Auswahl beider. Da die Konfigurationen in zwei unterschiedlichen Konformitätsrichtlinien ausgewählt werden, würde der restriktivste Ansatz gewählt werden, d. h. die Konfigurationen werden vom Gerät entfernt.

Sie können eine benutzerdefinierte Richtlinie aus dem Standard-**Space** an einen benutzerdefinierten Space delegieren. Damit eine benutzerdefinierte Richtlinie delegiert werden kann, müssen die in der benutzerdefinierten Richtlinie unter der Registerkarte „Designierte Konfigurationen per Push übertragen“ aufgeführten Konfigurationen an Spaces delegiert werden.

Auf der Seite **Geräte** können Sie auf den Namen eines Geräts klicken, um die Seite mit den Gerätedetails aufzurufen. Auf der Registerkarte „Konfigurationen“ zeigt die Spalte „Verteilungsmethode“ die Verteilungsmethode für eine per Push an das Gerät übertragene Konfiguration an. Die Verteilungsmethode kann entweder „Gerätegruppe“ oder „Compliance-Aktion“ sein.

Auf der Seite „Konfigurationen“ zeigt Ivanti Neurons for MDM für jede Konfiguration die Anzahl der Geräte an, die die Konfiguration über die Gerätegruppe und über die Compliance-Aktion erhalten haben.

Einstellung der Bedingungen

In der folgenden Tabelle werden einige Felder beschrieben, die zum Erstellen von Regeln verfügbar sind:

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
APNS-fähig	Dieses Feld gibt an, ob das Gerät APNS-fähig ist.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	iOS/macOS/Android
Nativer Anti-Phishing-Status	Dieses Feld zeigt den nativen Anti-Phishing-Status an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte • Nicht aktiviert • Nicht zutreffend • Aktiviert • Unbekannt	iOS, Android
Anti-Phishing-Status	Dieses Feld zeigt den Anti-Phishing-Status an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte: • Nicht aktiviert • Nicht zutreffend • Aktiviert • Unbekannt	iOS, Android
Anti-Phishing-VPN-Status	Dieses Feld zeigt den Anti-Phishing-VPN-Status an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte: • Nicht aktiviert • Nicht zutreffend • Aktiviert • Unbekannt	iOS, Android
Batterieinformationen	Dieses Feld besitzt folgende Attribute: • Akkustand – Zeigt den aktuellen, vom Android-Betriebssystem gemeldeten Ladezustand der Batterie an.	Informationen zu möglichen Werten finden Sie unter **Verwenden der erweiterten Suche**.	Android-

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
	• Batteriezustand – gemäß Meldung vom Android-Betriebssystem • Batterieladezustand – gemäß Meldung vom Android-Betriebssystem • Prozentualer Batteriezustand (OEM-spezifisch) – Prozentualer Batteriezustand für unterstützte Gerätehersteller wie Zebra-Geräte • Batterieherstellungsdatum (OEM) – Herstellungsdatum der Batterie für unterstützte Gerätehersteller wie Zebra-Geräte • Batterieladezyklen (OEM) – Anzahl der insgesamt durchgeführten Zyklen für unterstützte Gerätehersteller wie Zebra-Geräte		
Baseband-Systemzustand	Dieses Feld zeigt den Systemzustand des Basisbands des Geräts an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind "OK" und "Fehler".	iOS 27.0+ überwachte Geräte
Bootstrap-Token verfügbar	Dieses Feld gibt an, ob ein Bootstrap-Token für ein Gerät verfügbar ist.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	macOS
Autopilot registriert	Dieses Feld gibt an, ob das Gerät bei Autopilot registriert ist.	• Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	Windows
Letzter Check-in von Bridge	Dieses Feld gibt die Uhrzeit des letzten Check-ins von Bridge des Client an.	Mögliche Operatoren: • ist kleiner als • ist kleiner oder gleich • ist größer als • ist größer oder gleich • liegt innerhalb des Bereichs • liegt nicht innerhalb des Bereichs Geben Sie den numerischen Wert der letzten	Windows

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
		Check-in-Uhrzeit von Bridge ein. Wählen Sie für die Dauer eine der folgenden Optionen aus: • Stunden • Tage Beispiel: Der letzte Check-in von Bridge liegt weniger als 12 Stunden zurück.	
Kamera-Systemzustand	Dieses Feld zeigt den Systemzustand der Gerätekamera an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind: • OK • Fehler • Kein Original (wenn es sich nicht um eine echte Apple-Komponente handelt)	iOS 27.0+ überwachte Geräte
Letzter Check-in durch Client	Dieses Feld gibt die letzte Anmeldezeit des Kunden an.	Mögliche Operatoren: • ist kleiner als • ist größer als Geben Sie den numerischen Wert der letzten Anmeldezeit ein. Wählen Sie eine der folgenden Optionen für die Dauer: • Stunden • Tage Beispiel: Die letzte Anmeldung des Clients war vor weniger als 12 Stunden.	iOS/macOS/Android
Client registriert	Dieses Feld zeigt den Status des registrierten Clients an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	iOS/macOS/Android
Kompromittiert	Dieses Feld gibt an, ob das Gerät durch ein Rootkit oder in anderer Weise gefährdet ist.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind: • Durch Jailbreak oder Root gefährdet • Nicht gefährdet	iOS, Android

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
Aktueller Ländername	Dieses Feld gibt den Namen des aktuellen Landes entsprechend dem mobilen Ländercode (MCC) oder dem mobilen Netzwerkcode (MNC) an, den das Gerät als aktuell verbunden meldet.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Möglicher Wert ist ein Dropdown-Listenwert, der den Namen des Heimatlandes angibt.	iOS/macOS/Android
Aktueller MCC-Code	Dieses Feld gibt den aktuellen Ländercode für Mobiltelefone an.	Geben Sie den Wert des Attributes ein, das verifiziert werden soll. Mögliche Operatoren: • Ist gleich • ist nicht gleich	iOS/macOS/Android
Aktueller MNC-Code	Dieses Feld zeigt die aktuelle Mobilfunknetzvorwahl an.	Geben Sie den Wert des Attributes ein, das verifiziert werden soll. Mögliche Operatoren: • Ist gleich • ist nicht gleich	iOS/macOS/Android
Kundenspezifisches Geräteattribut	Mit diesem Feld können Sie ein vorhandenes kundenspezifisches Geräteattribut als Bedingung einer Regel hinzufügen, um diesen Wert zu verifizieren.	Geben Sie den Wert des Attributes ein, das verifiziert werden soll. Mögliche Operatoren: • Ist gleich • ist nicht gleich • enthält • enthält nicht Der Wert kann ein String aus ASCII-Zeichen sein (einschließlich Leerzeichen und Unicode-Zeichen).	iOS/macOS/Android/Windows
Benutzerdefiniertes LDAP-Attribut	Mit diesem Feld kann ein vorhandenes kundenspezifisches LDAP-Attribut als Bedingung einer Regel zur Überprüfung seines Wertes hinzugefügt werden.	Geben Sie den Wert des Attributes ein, das verifiziert werden soll. Mögliche Operatoren: • Ist gleich • ist nicht gleich • enthält • enthält nicht Der Wert kann ein String aus ASCII-Zeichen sein (einschließlich Leerzeichen und Unicode-Zeichen).	iOS/macOS/Android/Windows

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
Kundenspezifisches Benutzerattribut	Mit diesem Feld kann ein vorhandenes kundenspezifisches Attribut als Bedingung einer Regel zur Überprüfung seines Wertes hinzugefügt werden.	Geben Sie den Wert des Attributes ein, das verifiziert werden soll. Mögliche Operatoren: • Ist gleich • ist nicht gleich • enthält • enthält nicht Der Wert kann ein String aus ASCII-Zeichen sein (einschließlich Leerzeichen und Unicode-Zeichen).	iOS/macOS/Android/Windows
Daten-Roaming	Mit diesem Feld kann Daten-Roaming als Bedingung einer Regel zur Überprüfung seines Wertes verwendet werden.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein. Die Standardeinstellung ist „Nein“, wenn das unterstützte Gerät keine Informationen über dieses Feld anzeigt.	iOS, Android
Gerätetyp	Dieses Feld gibt das Gerätemodell an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • beginnt mit • endet mit Der mögliche Wert ist ein Textwert.	iOS/macOS/Android/Windows
Gerätetyp (Apple)	Dieses Feld gibt den Namen des Gerätemodells an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • beginnt mit • endet mit Der mögliche Wert ist ein Textwert.	iOS/macOS
Display-Systemzustand	Dieses Feld zeigt den Systemzustand des Gerätedisplays an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind: • OK • Fehler	iOS 27.0+ überwachte Geräte

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
		• Kein Original (wenn es sich nicht um eine echte Apple-Komponente handelt)	
Verschlüsselung aktiviert	Dieses Feld bestimmt, ob für das Gerät die Verschlüsselung und der Datenschutz aktiviert sind.	Ja – Auf dem Gerät sind Verschlüsselung und Datenschutz aktiviert. Nein – Auf dem Gerät sind Verschlüsselung und Datenschutz nicht aktiviert.	iOS/Android/Windows
GUID	Dieses Feld gibt die Geräte-GUID an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • beginnt mit • endet mit	iOS/macOS/Android/Windows
Face-ID-Systemzustand	Dieses Feld zeigt den Systemzustand der Face-ID des Geräts an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind "OK" und "Fehler".	iOS 27.0+ überwachte Geräte
Heimatlandname	Dieses Feld zeigt den Namen des aktuellen Landes an, das aus der Länderkennung (Mobile Country Code - MCC) bzw. der Mobilfunkanbieter-Kennung (Mobile Network Code - MNC) abgeleitet wird, das in die SIM oder eSIM des Geräts programmiert ist.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Möglicher Wert ist ein Dropdown-Listenwert, der den Namen des Heimatlandes angibt.	iOS/Android/Windows
Windows-Update fehlgeschlagen	Dieses Feld legt fest, ob das Gerät von den Regeln für das aktuelle Update abweicht.	Ja – das Gerät weicht von den Regeln für das aktuelle Update ab. Nein – das Gerät ist mit dem aktuellen Update konform.	Windows
Eigener MCC-Code	Dieses Feld zeigt die Landesvorwahl für das eigene Mobiltelefon an.	Geben Sie den Wert des Attributes ein, das verifiziert werden soll. Mögliche Operatoren: • Ist gleich • ist nicht gleich	iOS/macOS/Android
Eigener MNC-Code	Dieses Feld zeigt die Mobilfunknetzvorwahl für das eigene Mobiltelefon an.	Geben Sie den Wert des Attributes ein, das verifiziert werden soll. Mögliche Operatoren: • Ist gleich • ist nicht gleich	iOS/macOS/Android

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
IMEI	Dieses Feld gibt die IMEI-Nummer des ersten SIM-Steckplatzes an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • beginnt mit • endet mit	iOS/Android/Windows
IMEI2	Dieses Feld gibt die IMEI-Nummer des zweiten SIM-Steckplatzes an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • beginnt mit • endet mit	Android
IMSI	Dieses Feld gibt die IMSI-Nummer der SIM-Karte an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • beginnt mit • endet mit	Android/Windows
Institutioneller Wiederherstellungsschlüssel aktiviert	Dieses Feld zeigt an, ob der institutionelle Wiederherstellungsschlüssel auf dem Gerät aktiviert ist.	Mögliche Operatoren: • Ist gleich • ist nicht gleich	macOS
Letzte Anmeldung	In diesem Feld können Sie Bedingungen für die letzte Anmeldezeit des verwalteten Geräts über den MDM-Kanal festlegen.	Mögliche Operatoren: • ist kleiner als • ist größer als • ist leer Geben Sie den numerischen Wert der letzten Anmeldezeit ein. Wählen Sie eine der folgenden Optionen für die Dauer: • Stunden • Tage Beispiel: Die letzte Anmeldung des Clients war vor mehr als 12 Stunden.	iOS/macOS/Android/Windows

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
Letzte Hotfix-ID	Mit diesem Feld können Sie die Bedingungen für die letzte Hotfix-ID festlegen.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • ist kleiner als • ist kleiner oder gleich • ist größer als • ist größer oder gleich • enthält • enthält nicht • beginnt mit • beginnt nicht mit • endet mit • endet nicht mit	Windows
Letztes Hotfix installiert an	Mit diesem Feld können Sie Bedingungen für den Zeitpunkt der letzten Hotfix-Installation definieren.	Mögliche Operatoren: • ist kleiner als • ist größer als	Windows
Standortdienste aktiviert	Dieses Feld gibt an, dass das Gerät einen Gerätestandortdienst besitzt (beispielsweise Find My iPhone), der aktiviert ist.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	iOS-
Hersteller	Mit diesem Feld können Sie die Bedingungen für den Hersteller des Geräts definieren.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind: • Samsung • NOKIA • HTC • LGE • Apple Inc	iOS/macOS/Android/Windows
MTD-Aktivierungsstatus	Dieses Feld zeigt den MTD-Aktivierungsstatus an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte:	iOS, Android

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
		• Nicht zutreffend • Fehler • Ausstehend • Geschützt	
MDM-Verwaltung	Dieses Feld legt fest, ob für das Gerät MDM und ein Geräteadministrator aktiviert sind.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	iOS/macOS/Android
MDM-Registrierungstyp	Dieses Feld gibt den Registrierungstyp des Geräts an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind: • Benutzer • Gerät • Überwacht • Kein/e	iOS 27.0+, macOS 27.0+, tvOS 27.0+, visionOS 27.0+ und watchOS 27.0+
MDM-Wiederinbetriebnahme	Dieses Feld gibt den Gerätestatus für die MDM-Wiederinbetriebnahme unter App-Beibehaltung an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind "Wahr" und "Falsch".	iOS 27.0+ und VisionOS 27.0+
Mehrfach-Benutzer-Modus	Dieses Feld zeigt an, ob das Gerät (iPad) den Mehrbenutzermodus verwendet.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	iOS 27.0+
Nahfeld-Systemzustand	Dieses Feld zeigt den NFC-Systemzustand des Geräts an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind "OK" und "Fehler".	iOS 27.0+ überwachte Geräte
Betriebssystem	Dieses Feld entspricht der Betriebssystemversion des Geräts.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind: • macOS • Android	iOS/macOS/visionOS/Android/Windows

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
		• iOS- • Windows • visionOS	
Betriebssystem Build-Version	Dieses Feld enthält die Betriebssystemversion des Geräts.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • ist kleiner als • ist kleiner oder gleich • ist größer als • ist größer oder gleich • enthält • enthält nicht • beginnt mit • beginnt nicht mit • ist nicht leer • ist leer • endet mit • endet nicht mit	iOS/macOS/visionOS/Android/Windows
Betriebssystemversion	Dieses Feld entspricht der Betriebssystemversion des Geräts.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • ist kleiner als • ist kleiner oder gleich • ist größer als • ist größer oder gleich • liegt innerhalb des Bereichs • liegt nicht innerhalb des Bereichs Der mögliche Wert ist ein Text.	iOS/macOS/visionOS/Android/Windows
Betriebssystem mit Version	Dieses Feld entspricht dem Betriebssystem und der Betriebssystemversion des Geräts.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • ist kleiner als • ist kleiner oder gleich	iOS/macOS/visionOS/Android/Windows

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
		• ist größer als • ist größer oder gleich • liegt innerhalb des Bereichs • liegt nicht innerhalb des Bereichs Der mögliche Wert ist ein Text.	
Verantwortung	Dieses Feld gibt an, wer der Eigentümer des Geräts ist.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind: • Eigentum des Benutzers • nicht festgelegt • Eigentum des Unternehmens	iOS/macOS/Android/Windows
Persönlicher Wiederherstellungsschlüssel aktiviert	Dieses Feld zeigt an, ob der persönliche Wiederherstellungsschlüssel aktiviert ist.	Mögliche Operatoren: • Ist gleich • ist nicht gleich	macOS
Passcode konform mit Profilen	Dieses Feld gibt an, ob das Gerät die Passcode-Anforderungen der Profile erfüllt.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	iOS/macOS/Android
Persönlicher Hotspot aktiviert	Dieses Feld gibt an, ob die private Hotspot-Funktion auf dem Gerät aktiviert ist.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein. Die private Hotspot-Funktion wird nur von bestimmten Providern angeboten.	iOS-
Telefonnr.	Dieses Feld zeigt die Telefonnummer des Geräts an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • enthält • beginnt mit	iOS/Android/Windows

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
		• endet mit	
Öffentliche IP-Adresse	Dieses Feld gibt die öffentliche IP-Adresse an. Falls das Gerät eine VPN-Verbindung oder einen Proxyserver für die Verbindung mit Ivanti Neurons for MDM verwendet, wird die Proxy-WAN-IP-Adresse angezeigt.	Mögliche Operatoren: • liegt innerhalb des Bereichs • liegt nicht innerhalb des Bereichs • ist nicht leer • ist leer	Android/ChromeOS
Roaming	Dieses Feld gibt den Roaming-Status des Geräts an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	iOS/Android/Windows
Sicherheitssperrmodus	Dieses Feld gibt an, ob der Sperrmodus für ein Gerät aktiviert oder deaktiviert ist.	Mögliche Operatoren: • ist gleich • ist nicht gleich Mögliche Werte sind "Wahr" und "Falsch".	iOS 27.0+ und macOS 27.0+
Von Sentry blockiert	Gibt an, ob das Gerät von Sentry blockiert wird.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	iOS/macOS/Android/Windows
[Status]	Dieses Feld zeigt den Registrierungsstatus an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Der mögliche Standardwert ist „Aktiv“. In den benutzerdefinierten Richtlinien wird der Gerätestatus auf "Aktiv" beschränkt, indem alle anderen potenziellen Werte entfernt werden. Die Richtlinienprüfung erfolgt für die Status "Aktiv", "Stilllegung ausstehend" und "Komplettlöschung ausstehend" beim Geräte-Checkin und somit werden die Richtlinien dieser Geräte beim Einchecken geprüft.	iOS/macOS/Android
Seriennummer	Dieses Feld gibt die Seriennummer des Geräts an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • beginnt mit	iOS/macOS/Android/Windows

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
		• endet mit	
Überwacht	Dieses Feld gibt an, ob das Gerät überwacht wird.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	iOS/macOS
Zusätzliche Buildversion	Dieses Feld enthält die zusätzliche Buildversion des Geräts.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • ist kleiner als • ist kleiner oder gleich • ist größer als • ist größer oder gleich • enthält • enthält nicht • beginnt mit • beginnt nicht mit • endet mit • endet nicht mit • ist nicht leer • ist leer	iOS/macOS
Zusätzliches BS/Version Extra	Dieses Feld enthält die zusätzliche Betriebssystem-Buildversion des Geräts.	Mögliche Operatoren: • Ist gleich • ist nicht gleich • ist kleiner als • ist kleiner oder gleich • ist größer als • ist größer oder gleich • enthält • enthält nicht • beginnt mit • beginnt nicht mit • endet mit • endet nicht mit	iOS/macOS

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
		• ist nicht leer • ist leer	
Touch-ID-Systemzustand	Dieses Feld zeigt den Systemzustand der Touch-ID des Geräts an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind: • OK • Fehler • Nicht zutreffend (wenn es sich um ein iPhone handelt)	iOS 27.0+ überwachte Geräte
Benutzer aktiviert	Dieses Feld gibt an, ob der Benutzer aktiviert ist.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	iOS/macOS/Android/Windows
Benutzergruppe	Dieses Feld steht für die Benutzergruppe.	Mögliche Operatoren: • Ist gleich • ist nicht gleich	iOS/macOS/Android/Windows
Ultrabreitband-Systemzustand	Dieses Feld zeigt den Systemzustand des Ultrabreitbands des Geräts an.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind "OK" und "Fehler".	iOS 27.0+ überwachte Geräte
Sprach-Roaming	Dieses Feld gibt an, ob Voice Roaming für das Gerät aktiviert ist.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein. Die Voice-Roaming-Einstellung wird nur von bestimmten Providern angeboten. Bei Deaktivierung des Voice Roamings wird auch Daten-Roaming deaktiviert. Der Standardwert ist „ungleich", wenn das unterstützte Gerät keine Informationen über dieses Feld ausgibt.	iOS-
Von Access blockiert	Gibt an, ob das Gerät von Access blockiert wird.	Mögliche Operatoren: • Ist gleich	iOS/macOS/Android/Windows

UI-Feld	Beschreibung	Mögliche Werte	Unterstützte Plattformen
		• ist nicht gleich Mögliche Werte sind Ja und Nein.	
Compliance	Gibt an, ob das Gerät konform ist.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind "Konform" und "Nicht konform".	iOS/macOS/Android/Windows
Von Compliance-Aktion blockiert	Gibt an, ob das Gerät blockiert wird.	Mögliche Operatoren: • Ist gleich • ist nicht gleich Mögliche Werte sind Ja und Nein.	iOS/macOS/Android/Windows

Nicht quarantänefähige Konfigurationen

Die folgende Tabelle zeigt die Liste der Konfigurationen, die nicht quarantänefähig sind:

Betriebssystem	Nicht quarantänefähige Konfigurationen
Android	• App-Katalog für Android • Android-Verschlüsselung • Android Enterprise • App für Android Enterprise • Android Zebra • Anti-Phishing-Schutz • Android Work Challenge • Gerätepasswort • Datei herunterladen • Sperre & Kiosk: Android-Geräte Administratormodus • Sperre & Kiosk-Modus: Samsung Knox Standard • Nur MAM • Verwaltetes Gerät mit Arbeitsprofil/Arbeitsprofil auf firmeneigenem Gerät • Verwaltete Geräte (Geräteeigentümer) • Einschränkungen für Samsung Phone • SafetyNet-Attestierung • Arbeitsprofil auf einem unternehmenseigenen Gerät.
iOS und macOS	• Phishing-Schutz (iOS) • App-Benachrichtigungen (iOS) • AppStation-Sites (iOS) • Filevault-Wiederherstellungsschlüssel (macOS) • Filevault 2 (macOS) • Globaler Proxy (iOS und tvOS) • Startbildschirm-Layout (iOS und tvOS) • iOS-App-Kontrolle • iOS-Einschränkungen • iOS-Software-Aktualisierungen (iOS) • macOS-Firewall • macOS Software-Updates • Nur MAM (iOS) • MobileIron Client-Datenschutz (iOS/macOS) • Netzwerknutzung (iOS) • Konto für Office 365 erstellen (macOS) • Single-App-Modus (iOS und tvOS) • Systemrichtlinien-Steuerung (macOS)

Betriebssystem	Nicht quarantänefähige Konfigurationen
	• Verwaltete Systemrichtlinie (macOS) • Optionen für Systemrichtlinien-Regeln (macOS) • Zeitserver (macOS) • Web-Content-Filter (iOS)
Windows	• Windows App-Kontrolle • Windows-Einschränkungen DDF (Datendefinitionsdatei) • Windows-Firewall • Windows-Netzwerk-Proxy • Windows-Einschränkungen • Windows-Update
Alle	• Active Directory • Client-Dienste • Verwaltung mobiler Geräte (MDM) • Aktivierung der MobileIron-Bedrohungsabwehr • Lokale Aktionen von MobileIron Threat Defense • Passwort • Datenschutz • Datenschutzerklärung • ServiceConnect • Synchronisieren

Wenn Sie die Seite mit den Richtlinien nicht sehen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie brauchen eine der folgenden **Rollen**:

- Geräteverwaltung
- Geräts schreibgeschützt

11.3. Zulässige Apps überwachen und kontrollieren

Lizenz: Silver

Erstellen Sie eine Richtlinie für zulässige Anwendungen, um zu kontrollieren, welche Apps auf Geräten installiert werden. Diese Richtlinie unterstützt auch die internen MobileIron Packager (MIP) macOS-Apps. Die Richtlinie enthält folgende Informationen:

- App-Whitelist
- App-Blacklist
- {{Erforderliche Apps}}
- Compliance-Aktionen

Wenn eine App benötigt wird, aber in der Blacklist steht, hat die Bewertung der App in der Liste der erforderlichen Apps Vorrang. Wenn beispielsweise eine App A1 in der Liste der obligatorischen Apps, aber auch in der Blacklist steht, prüft die App-Richtlinie für dieses Gerät wie folgt:

- Das Gerät ist kompatibel, wenn A1 auf dem Gerät installiert ist.
- Das Gerät ist nicht kompatibel, wenn A1 nicht auf dem Gerät installiert ist.

Unterstützte Geräte

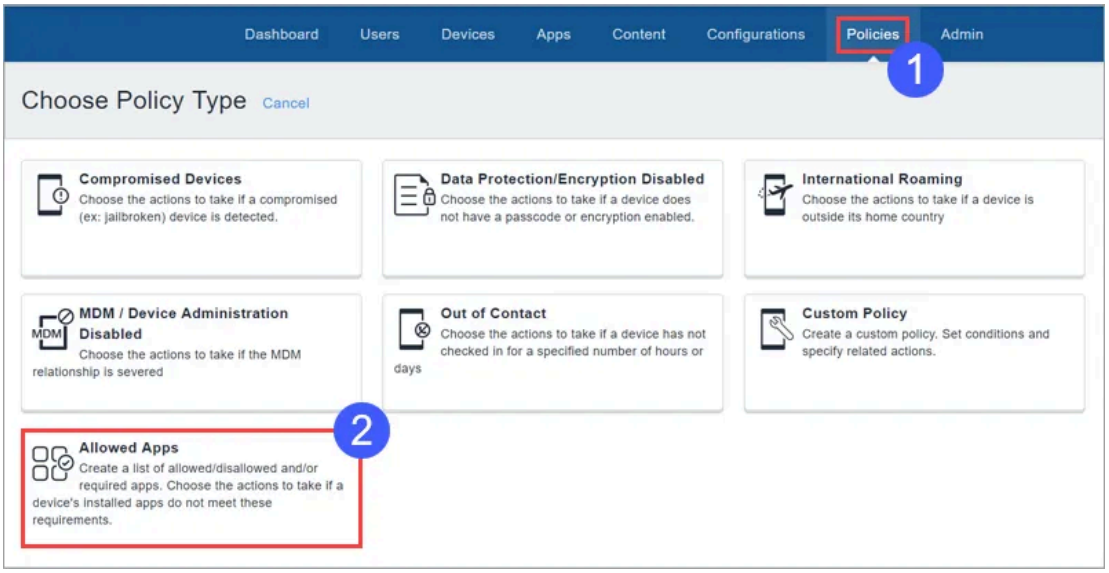
- Android 4.2 oder unterstützte neuere Versionen
- iOS 8.0 oder unterstützte neuere Versionen
- macOS 10.12 oder unterstützte neuere Versionen
- Windows 10 oder unterstützte neuere Versionen

Voraussetzungen

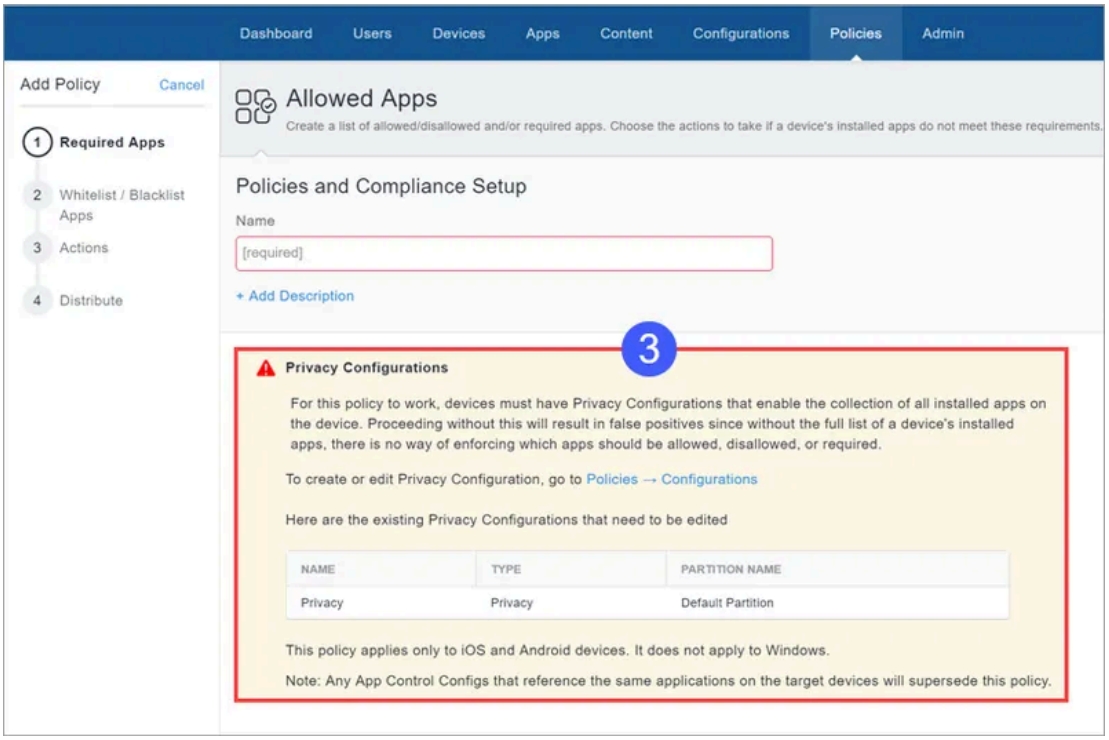
- Die zugewiesenen **Datenschutzeinstellungen** eines Geräts müssen die Erfassung der App-Informationen zulassen, damit die Richtlinie für zulässige Anwendungen korrekt funktioniert. Prüfen Sie die zugewiesenen Datenschutzkonfigurationen für die Geräte, für die Sie die Richtlinie für zulässige Apps verwenden wollen.

Wenn Sie sich nicht sicher sind, welche Konfigurationen betroffen sind:

1. Gehen Sie zu **Richtlinien**.



Klicken Sie auf **Zulässige Apps**.



3. Suchen Sie unter **Datenschutzkonfigurationen** die Konfigurationen, die Sie bearbeiten müssen.
4. Gehen Sie zu **Konfigurationen**.
5. Bei jeder Datenschutzkonfiguration müssen Sie auf Folgendes achten:
    1. Wählen Sie die Konfiguration aus.
    2. Klicken Sie auf **Bearbeiten**.
    3. Wählen Sie unter **App-Bestand erfassen** die Option **Für alle Apps auf dem Gerät**.
    4. Klicken Sie auf **Fertig**.

Richtlinie für zulässige Apps erstellen

Voraussetzungen

- Aktivieren Sie Android Enterprise, um auf den Google Play Store zuzugreifen und neue Anwendungen zur Richtlinie für zugelassene Anwendungen hinzuzufügen.

Verfahren

1. Gehen Sie zu **Richtlinien** und klicken Sie auf **+Hinzufügen**.

2. Klicken Sie auf **Zulässige Apps**.

3. Geben Sie in dem Feld **Name** einen Namen für diese Richtlinie ein.
4. Geben Sie in dem Feld **Beschreibung** einen optionalen Text ein, der den Zweck der Richtlinie erläutert.
5. Wählen Sie die Apps aus, die Sie in die Whitelist oder Blacklist stellen wollen, indem Sie auf eine oder beide der folgenden Registerkarten klicken:

- Klicken Sie auf die Option „Durch Suche hinzufügen“, um Apps im App Store oder App Catalog zu suchen und auszuwählen. Stellen Sie sicher, dass der Zugriff auf den Google Play Store für Android Enterprise aktiviert ist.

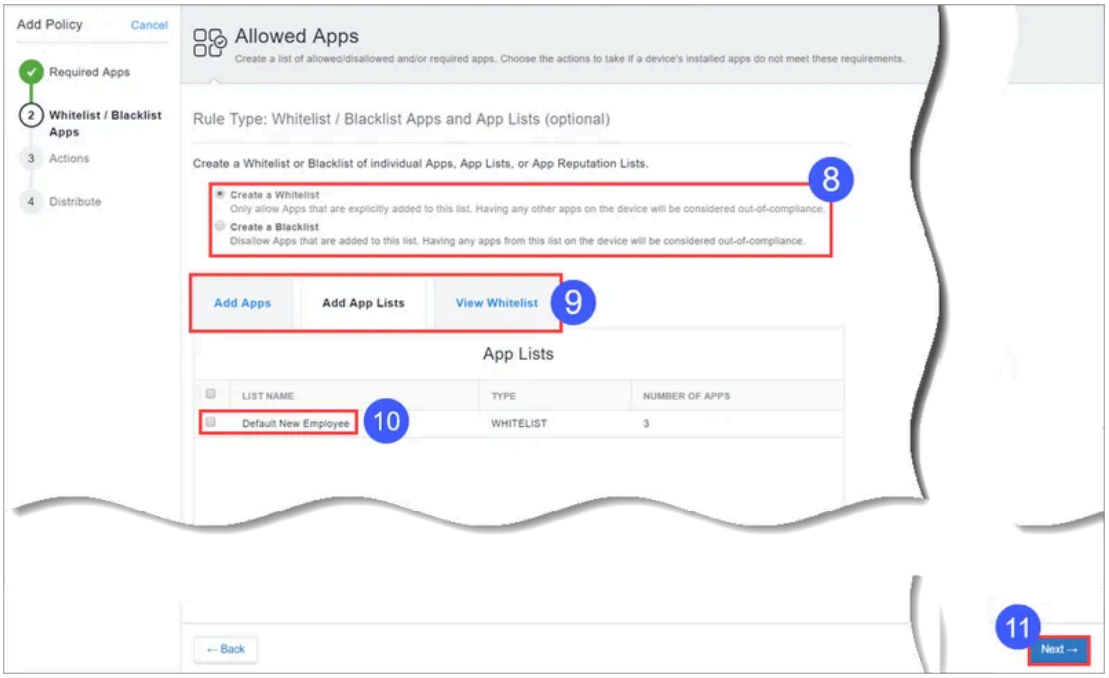
- Klicken Sie auf **Manuell hinzufügen**, um Apps durch Eingabe der Bundle-ID für Android-, Windows-, iOS- oder macOS-System-Apps auszuwählen.

Klicken Sie dann auf die Registerkarte **App-Listen hinzufügen** und wählen Sie die gewünschten App-Listen aus.

6. Wählen Sie die erforderlichen Apps oder App-Listen mit den entsprechenden Feldern aus.
7. Klicken Sie auf **Weiter**

> Klicken Sie für eine Liste von Apps, die Sie bisher ausgewählt haben, auf die Registerkarte **Erforderliche Liste anzeigen**.

8. Wählen Sie diese Option, um eine Whitelist oder Blacklist zu erstellen.



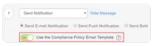
9. Wählen Sie in dem Abschnitt **Apps und App-Listen für die Whitelist/Blacklist** Apps und App-Listen aus.

> Sie können nicht gleichzeitig eine Whitelist und eine Blacklist für ein Gerät haben. Die Erstellung einer Whitelist bedeutet, dass alle anderen Apps auf der Blacklist stehen.

10. Wählen Sie die erforderlichen Apps oder App-Listen mit den entsprechenden Feldern aus.
    - Klicken Sie dann auf die Registerkarte **App-Listen hinzufügen** und wählen Sie die gewünschten App-Listen aus.
11. Klicken Sie auf **Weiter**.

> Klicken Sie auf die Registerkarte **Whitelist oder Blacklist anzeigen**, um eine Liste der bisher ausgewählten Anwendungen anzuzeigen.

12. Wählen Sie Aktionen für den Fall aus, dass ein Gerät die Compliance-Anforderungen nicht erfüllt:

Aktion	So gehen Sie vor
Überwachen	Ist zurzeit immer ausgewählt. Wenn Sie verknüpfte Compliance-Aktionen nutzen wollen, benötigen Sie Sentry Version 9.0.0 oder höher.
Nichts tun	Legen Sie fest, dass keine Aktion ausgeführt werden soll, wenn das Gerät nicht konform ist.
Benachrichtigung senden	
E-Mail senden	Wählen Sie die Option aus, um eine E-Mail an die E-Mail-Adresse des Gerätebenutzers zu senden, dass sein Gerät nicht mehr die Compliance-Anforderungen erfüllt. • Aktivieren Sie die Option **E-Mail-Vorlage der Compliance-Richtlinien verwenden**, um die Nachricht, die Sie hier konfigurieren, in die E-Mail-Vorlage zur Richtlinienbenachrichtigung einzufügen. Konfigurieren Sie diese wie unter **E-Mail-Vorlage anpassen** in **Branding von E-Mail-Vorlagen** beschrieben. Einen Überblick finden Sie unter **Benachrichtigungs-E-Mails zur Einhaltung von Richtlinien konfigurieren und verwenden**  • Sie können die Mitteilungen anpassen, indem Sie optionale Ersatzvariablen einfügen, um den Empfängern weitere Details über Richtlinienverletzungen und sonstige relevante Informationen mitzuteilen. Auf diese Weise erhalten die Benutzer mit nicht der Compliance entsprechenden Geräten relevante Informationen über die Richtlinienverletzung, sodass sie entsprechende Gegenmaßnahmen ergreifen können. Klicken Sie auf die folgenden Attributarten, um die komplette Variablenliste anzuzeigen: ◦ Richtlinienattribute wie $, $ und $. ◦ Benutzer-Attribute wie $, $ und $ ◦ Geräte-Attribute wie $, $ und $.
Push-Benachrichtigung senden	Klicken Sie auf die Option, um eine Push-Benachrichtigung an das Gerät zu senden, wenn das Gerät nicht mehr die Compliance-Anforderungen erfüllt.
Beide senden	Wählen Sie die Option aus, um eine Push-Benachrichtigung an das Gerät und eine E-Mail an die E-Mail-Adresse des Gerätebenutzers zu senden, dass sein Gerät nicht mehr die Compliance-Anforderungen erfüllt. Sie können die Mitteilungen anpassen, indem Sie optionale Ersatzvariablen verwenden, die den Empfängern weitere Details übermitteln, wie bereits im Abschnitt „E-Mails versenden" beschrieben.
Warten	Wählen Sie die Option, um eine Maßnahme für eine bestimmte Zeitdauer zu verzögern, damit der Benutzer Zeit hat, die Richtlinienverletzung zu beseitigen, bevor weitere Maßnahmen ergriffen werden, weil das Gerät die Compliance-Anforderungen immer noch nicht erfüllt.
Sperren	Blockiert mit Sentry verwaltete Geräte, damit diese nicht auf E-Mail und AppConnect-fähige Anwendungen zugreifen können.
Quarantäne	Wählen Sie die Option, um den Zugriff auf Apps, Content und Server mit den Maßnahmen in der folgenden Tabelle zu unterbinden. Die Entfernung aller Apps in einer Maßnahme ist nicht zulässig.
Benachrichtigung senden, wenn das	

Aktion	So gehen Sie vor
Gerät wieder konform ist	
E-Mail senden	Sendet eine E-Mail an die E-Mail-Adresse des Gerätebenutzers, sobald das Gerät wieder konform ist. • Sie können die E-Mail-Vorlage für die Richtlinienbenachrichtigung wie oben beschrieben verwenden. • Sie können die Mitteilungen anpassen, indem Sie optionale Ersatzvariablen einfügen, um den Empfängern weitere Details über Richtlinienverletzungen und sonstige relevante Informationen mitzuteilen. Klicken Sie auf die folgenden Attributarten, um die komplette Variablenliste anzuzeigen: ◦ Richtlinienattribute wie $, $ und $. ◦ Benutzer-Attribute wie $, $ und $ ◦ Geräte-Attribute wie $, $ und $. ◦ Benutzerdefinierte Geräte-/Benutzer-/LDAP-Attribute, die über die Seite **Admin > Attribute** erstellt werden.
Push-Benachrichtigung senden	Sendet eine Push-Benachrichtigung an das Gerät, wenn das Gerät wieder konform ist.
Beide senden	Sendet eine Push-Benachrichtigung an das Gerät und eine E-Mail an die E-Mail-Adresse des Gerätebenutzers, dass sein Gerät nicht mehr die Compliance-Anforderungen erfüllt. Sie können die Mitteilungen anpassen, indem Sie optionale Ersatzvariablen verwenden, die den Empfängern weitere Details übermitteln, wie bereits im Abschnitt „E-Mails versenden“ beschrieben.

Die Richtlinie „Erlaubte Apps“ unterstützt **abgestufte Compliance-Aktionen**, wenn Sie eine Platinum-Lizenz besitzen.

(Optional) zusätzliche Quarantäne-Aktionen	Beschreibung
Verwaltete Anwendungen in Quarantäne stellen	Entfernt alle über die Cloud verwalteten Apps von dem Gerät und sperrt neue App-Downloads, so dass keine Apps neu auf dem Gerät installiert werden können. Wählen Sie eine der folgenden Optionen aus: • **Alle Anwendungen** • **Designierte Anwendungen** - Fügen Sie eine oder mehrere Anwendungen durch Suchen oder manuell (über die Bundle-ID oder den Paketnamen) hinzu. Klicken Sie auf die Registerkarte **Apps anzeigen** , um die Liste der hinzugefügten Apps zu überprüfen. Die Standard-Quarantänemaßnahme zum Blockieren des App Store-Zugriffs ist nicht mehr verfügbar. Auf bestimmten Geräten wird durch die Aktion "Quarantäne" die Anwendung aufgrund bestimmter Gerätebeschränkungen nicht vom Gerät entfernt.
Neue App Downloads sperren	Sperrt den Download neuer Apps für das Gerät. Wählen Sie eine der folgenden Optionen aus: • **Alle Anwendungen** • **Designierte Anwendungen** - Fügen Sie eine oder mehrere Anwendungen durch Suchen oder manuell (über die Bundle-ID oder den Paketnamen) hinzu. Klicken Sie auf die Registerkarte **Apps anzeigen** , um die Liste der hinzugefügten Apps zu überprüfen. Die Standard-Quarantänemaßnahme zum Blockieren des App Store-Zugriffs ist nicht mehr verfügbar.
Konfigurationen entfernen	Entfernt Ivanti Neurons for MDM-Konfigurationen von dem Gerät. Wählen Sie eine der folgenden Optionen aus: • **Alle Konfigurationen** • **Designierte Konfigurationen** - Wählen Sie eine oder mehrere Konfigurationen aus der Liste aus oder suchen Sie nach ihnen. Klicken Sie auf die Registerkarte **Ausgewählte Konfigurationen**, um die Liste der ausgewählten Konfigurationen zu überprüfen.
Inhalt entfernen	Entfernt den gesamten Content und die Medien, die mit Apps verbunden sind, welche über die Cloud von dem Gerät verteilt wurden.
Private Apps suspendieren	Apps auf der privaten Seite des unter Quarantäne gestellten Geräts zeitweilig deaktivieren, damit der Gerätebenutzer die Compliance-Probleme auf dem Gerät behebt, um es wieder funktionsfähig zu machen. Wird auf Geräten mit Android 11+ unterstützt und als Arbeitsprofil auf unternehmenseigenen Geräten bereitgestellt.
Standard-Quarantänemaßnahmen: Diese Aktionen werden immer durchgeführt.	
App-Speicherzugriff sperren	Verhindert, dass das Gerät über die Cloud auf App Stores zugreift.
Content Store-Zugriff sperren	Verhindert, dass das Gerät über die Cloud auf den Content Store zugreift.

(Optional) zusätzliche Quarantäne-Aktionen	Beschreibung
AppConnect sperren	Verhindert, dass das Gerät die AppConnect-Funktionen verwendet.
AppTunnel sperren	Verhindert, dass Apps auf dem Gerät auf Content und Servers über AppTunnel zugreifen.
ActiveSync sperren	Verhindert, dass das Gerät über den ActiveSync-Server auf E-Mails zugreift.

Klicken Sie auf **Weiter**.

14. Konfigurieren Sie die Verteilung.
15. Klicken Sie auf **Fertig**.

Weitere Informationen zur Definition höherer oder niedrigerer Prioritäten für eine Richtlinie „Erlaubte Apps“ finden Sie unter **Richtlinien priorisieren**.

11.4. Prioritäten für Richtlinien

Die Richtlinie „Erlaubte Apps“ unterstützt eine Priorität, ähnlich wie bei Konfigurationen. Mit einer Priorität wird bestimmt, welche Richtlinie desselben Typs an mehrere Gerätegruppen verteilt wird und in welchem Fall dasselbe Gerät in diesen Gerätegruppen erscheint. Beispielsweise ist eine Richtlinienpriorität nützlich, um die Richtlinien-Verteilung in folgenden Fällen festzulegen:

- „Erforderliche App A“ muss an Gerätegruppe 1 verteilt werden,
- „Erforderliche App B“ muss an Gerätegruppe 2 verteilt werden, und
- Das Gerät des Benutzers ist Mitglied beider Gerätegruppen.

Sie können Richtlinien wie folgt priorisieren:

1. Gehen Sie zu **Richtlinien > Richtlinie & Compliance**.
2. Wählen Sie **Aktionen > Richtlinien priorisieren**. Wenn die Option **Aktion** nicht angezeigt wird, haben Sie maximal eine Richtlinie mit Prioritäten.
3. Listen Sie mit den Pfeiltasten die Prioritäten von der höchsten (oben) bis zur niedrigsten Priorität (unten) auf. Ein Schlosssymbol bedeutet, dass Sie die Priorität der Richtlinie nicht ändern können, ohne die Verteilungseinstellung für alle Geräte der Richtlinie zu bearbeiten.
4. Klicken Sie auf **Speichern**.

11.5. Windows-Hardwarerichtlinie

Couldn't convert your doc.

12. Administrator

Im Admin-Bereich können Sie Benutzer, Geräte und Konfigurationen über das Portal Ivanti Neurons for MDM verwalten. In den folgenden Abschnitten finden Sie eine Liste aller Aufgaben, die Sie als Administrator ausführen können:

- [System]
- Infrastruktur
- Einstellungen (Apple)
- Arbeiten mit Windows-Geräten
- Einrichtung mit Microsoft Azure
- Mit Google Apps verbinden
- Arbeiten mit ChromeOS-Geräten
- Firmware-Verwaltung
- Zeitweilige Sperre eines Mandanten
- Verwalten von Skripten und Dateien
- Branding
- Hinzufügen der Verwaltung von Nicht-iOS-Geräten

12.1. [System]

Dieser Abschnitt enthält die folgenden Themen:

- Attribute
- Einstellungen für die Gerätebereinigung
- DSGVO-Profile
- Benachrichtigungs-E-Mails
- Rollenverwaltung
- Räume
- Support-Administratoren
- Administrator > Benachrichtigung zur Systemnutzung

12.1.1. Attribute

Auf der Seite "Attribute" lassen sich folgende Aufgaben ausführen:

- Informationsarten verwalten, die Sie für Benutzer, Geräte und Apps erfassen können
- Standardinformationstypen anzeigen, die von Ivanti Neurons for MDM verfolgt werden

Benutzerdefinierte Benutzerattribute können bestimmte Informationen beinhalten, beispielsweise die Abteilung oder eine interne Kennung. Jedes Attribut besitzt eine entsprechende Variable, die Sie zum Erstellen von Gruppen oder Verteilen von Konfigurationen verwenden können.

> Wenn Sie Kriterien für eine Benutzergruppenregel erstellen und die benutzerdefinierten Attribute einen Zahlenwert beinhalten, beachten Sie, dass Ivanti Neurons for MDM keine Unterstützung für Ganzzahlenoperationen bietet.

Erstellen benutzerdefinierter Attribute

Benutzerdefinierte Attribute können Sie im Ivanti Neurons for MDM-Administrationsportal erstellen.

Verfahren

1. Melden Sie sich beim Administrationsportal an.
2. Wechseln Sie zu **Admin** > **System** > **Attribute**.
3. Klicken Sie unter **Kundenspezifische Attribute** auf **+Neu hinzufügen**
4. Geben Sie in dem Feld **Attributname** den Text für das Attribut ein.

> Beachten Sie, dass der von Ihnen eingegebene Text zur Erstellung der entsprechenden Variable in dem Feld **Nutzung** verwendet wird.

Wählen Sie einen beliebigen Attributtyp aus den folgenden Optionen **Attributtyp** aus.

   - **Benutzer**
   - **Gerät**
   - **[App]**
   - **IDP** (weitere Informationen siehe Benutzerbereitstellung mit SCIM oder Verbinden von Ivanti Neurons for MDM mit der Entra ID-Benutzerquelle)

Wählen Sie beim Attributtyp "Gerät" eine der folgenden Optionen für den **Datentyp** aus:

   - **Numerisch**
   - **Text**

7. **Attribut beibehalten** (optional): Diese Option kann nur verwendet werden, wenn der Attributtyp **Gerät** lautet. Wählen Sie diese Option aus, um das benutzerdefinierte Attribut auch dann beizubehalten, wenn eine Komplettlöschung oder Stilllegung auf einem Gerät durchgeführt wird.
8. Klicken Sie auf **[Add]**.
   Das erstellte benutzerdefinierte Benutzerattribut wird unter **Administrator hinzugefügt** auf der Seite „Attribute“ angezeigt.

> Die benutzerdefinierte Kombination $ + $ + $ + ${Static String} wird in beliebiger Reihenfolge unterstützt.

Benutzerspezifisches Attribut umbenennen

Die Umbenennung eines benutzerspezifischen Attributes führt zur Umbenennung aller Referenzen dieses benutzerspezifischen Attributes, die in folgenden Entitäten verwendet werden:

- Anpassbare Richtlinie
- Benutzergruppe
- Gerätegruppe
- App-Verteilungsfilter:
- Räume

> Bezugnahmen auf das benutzerspezifische Attribut in anderen Entitäten (beispielsweise in Konfigurationen, E-Mail-Vorlagen für Einladungen, E-Mail- und Push-Nachrichten in Aktionen zur Durchsetzung von Richtlinien usw.) werden nicht aktualisiert.

Verfahren

1. Klicken Sie unter **Benutzerspezifische Attribute** neben dem Attribut, das Sie umbenennen wollen, auf **+Bearbeiten**.
2. Geben Sie in dem Feld **Attributname** einen neuen Namen für das Attribut ein.

> Beachten Sie, dass der von Ihnen eingegebene Text zur Erstellung der entsprechenden Variable in dem Feld **Nutzung** verwendet wird.

Klicken Sie auf **Speichern**.

Benutzerspezifisches Attribut löschen

Beim Löschen eines kundenspezifischen Attributs werden dessen Werte bei allen zugeordneten Benutzern/Geräten entfernt. Diese Operation kann nicht rückgängig gemacht werden.

Benutzerspezifische Attribute können Sie nicht löschen, wenn das Attribut in einer der folgenden Entitäten verwendet wird:

- Anpassbare Richtlinie
- Benutzergruppe
- Gerätegruppe
- App-Verteilungsfilter:
- Räume

Entfernen Sie das benutzerdefinierte Attribut von den Entitäten, bevor Sie versuchen, es zu löschen.

Wenn das Attribut, das Sie löschen wollen, keine Bezugnahmen auf die oben erwähnten Entitäten hat, erscheint nach dem Klick auf die Option zum **Löschen** neben dem Attribut ein Popup-Fenster mit einer Bestätigungsrückfrage. Bestätigen Sie die Aktion und klicken Sie auf **Löschen**.

> Die Feldnamen der folgenden benutzerdefinierten Attribute werden in den jeweiligen Regeleditoren sortiert:

- Benutzerdefiniertes LDAP-Attribut
- Kundenspezifisches Benutzerattribut
- Kundenspezifisches Geräteattribut
- Benutzerdefiniertes IdP-Attribut
- Benutzerdefiniertes App-Attribut

System-Attribute anzeigen

System-Attribute sind vordefinierte Attribute, die Sie in Ihren Konfigurationen als Variablen verwenden können. Die vollständige Liste finden Sie im Abschnitt **Systemattribute** der Seite **Admin** > **System** > **Attribute**. System-Attribute sind u.a. folgende Attributarten:

- Benutzerattribute
- Geräteattribute
- E-Mail-Vorlagenattribute
- System-Attribute
- Zeitstempelattribute
- Benutzerdefinierte Entra ID-Benutzerattribute
- Richtlinienattribute

Benutzerattribute

Mithilfe von Benutzerattributen legen Sie Informationen zu Benutzern fest.

Schlüssel	Beschreibung
$	Abteilungsattribut (erfordert Entra ID)
$	Persönliche Kennung für den elektronischen Datenaustausch
$	Verwaltete Apple-ID des Benutzers
$	sAMAccountName-Attribut (erfordert Active Directory)
$	Common Name-Attribut (CN), extrahiert aus dem Distinguished Name (erfordert LDAP)
$	Anzeigename
$	Eindeutiger Name (erfordert LDAP)
$	Der Domänenteil der E-Mail-Adresse (nach dem '@')
$>	Der lokale Abschnitt der E-Mail-Adresse (der Teil vor '@')
$	E-Mail-Adresse
$	Vorname
$	Nachname
$	Region
$	Attribut "Organisationseinheit" (OU), extrahiert aus dem Distinguished Name (erfordert LDAP)
$	Kerberos-Bereichsinformationen (erfordert Active Directory)
$	Der Domänenteil der Anmelde-ID (nach dem '@')
$	Der lokale Teil der Anmelde-ID (vor dem '@')
$	Anmelde-ID (E-Mail-Adressformat)
$	Attribut "userPrincipalName" (erfordert Active Directory)

Geräteattribute

Mithilfe von Geräteattributen legen Sie Informationen zu einem Mobilgerät fest.

Schlüssel	Beschreibung
$	Datum der letzten Client-Anmeldung (aktuellere Anmeldung: entweder MDM oder Client)
$	Alternative Seriennummer
$	Von der Client-Anwendung verwendete Kennung
$	Global eindeutige Gerätekennung
$	ICCID
$	IMEI2
$	IMEI
$	IMSI
$	Datum der letzten Geräteanmeldung (aktuellere Anmeldung: entweder MDM oder Client)
$	Interne Gerätekennung
$	Für MDM verwendete Kennung
$	MEID
$	Modell
$	Gerätename
$	Telefonnummer des Geräts
$	Clustereigene Gerätekennung
$	SerialNumber
$	iOS UDID
$	WLAN-MAC-Adresse
	Telefonnummer 2
	ICCID 2

Wenn Sie ein benutzerdefiniertes Attribut erstellen und in einer verwalteten App-Konfiguration darauf verweisen und wenn der Attributwert dann aktualisiert wird, wird auch das in der verwalteten App-Konfiguration referenzierte Attribut aktualisiert. Die verwaltete App-Konfiguration wird anschließend erneut an das Gerät übertragen.

Wenn benutzerdefinierte Attribute oder Geräteattribute aktualisiert und die Konfiguration via Push auf ein Gerät übertragen wird, sollte die Android Kiosk-Brandingkonfiguration ebenfalls aktualisiert werden.

App-Attribute

Mithilfe von App-Attributen können Sie Informationen zu Anwendungen angeben und benutzerdefinierte Anwendungsgruppen erstellen.

Schlüssel	Beschreibung
$	Datum der Hinzufügung der Anwendung zum App-Katalog
$	Name der Anwendung
$	Betriebssystem der Anwendung
$	Anwendungs-Bundle oder Paket-ID
$	Quelle, aus der die Anwendung importiert wurde
$	Angabe, ob iOS- oder macOS-Anwendung VPP ist oder nicht

E-Mail-Vorlagenattribute

Schlüssel	Beschreibung
$	E-Mail-Textteil
$	E-Mail-Betreff

Zeitstempelattribute

Variablenschlüssel	Beschreibung
$	Aktueller Zeitstempel (Millisekunden seit Epoch)

Richtlinien-Vorlagenattribute

Schlüssel	Beschreibung
$	Name der verletzten Richtlinie
$	Nächste mehrstufige Compliance-Aktion (außer Warten und Stilllegen) nach dem Senden der Nachricht
$	Anzahl der Tage, an denen das Gerät nicht konform war.
$	Zeitstempel der ersten Auslösung der Richtlinienverletzung (Format UTC DD-MM-YYYY)
$	Regeldefinition (Abfrage-String, wie er jetzt angezeigt wird)

Verwandte Themen:

- Angepasste Attribute Benutzern zuweisen
- Anpassbare Attribute für Geräte zuweisen
- Anpassbare Attribute für Benutzer entfernen

- Anpassbare Attribute von Geräten entfernen
- Variablen

12.1.2. Einstellungen für die Gerätebereinigung

Die Gerätebereinigung automatisiert den Lebenszyklus nicht verwendeter Geräte. Sie können Geräte stilllegen, die seit einer bestimmten, konfigurierbaren Anzahl von Tagen nicht mehr kontaktiert wurden. Sie können Geräte löschen, die seit einer bestimmten, konfigurierbaren Anzahl von Tagen stillgelegt sind. Die Seite "Audit-Protokolle" erfasst die Einstellungen Gerät stilllegen, Gerät löschen, und Komplett gelöschte Geräte löschen.

Die folgende Tabelle enthält Informationen zu Android-Geräten, die Einstellungen für die Gerätebereinigung unterstützen:

Modus	Stilllegen, wenn nicht konform	Stillgelegte Geräte löschen	Stilllegen erzwingen oder Geräte mit ausstehender Stilllegung stilllegen	Komplett gelöschte Geräte löschen	Geräte mit ausstehender Komplettlöschung löschen
Android-Arbeitsprofil (Profilbesitzer)	**JA**	**JA**	**JA**	**NEIN**	**NEIN**
Geräteadmin/Arbeitsprofil auf unternehmenseigenem Gerät	**JA**	**JA**	**JA**	**JA**	**JA**
Vom Unternehmen verwaltetes Gerät/Von Android verwaltetes Gerät mit Arbeitsprofil	**NEIN**	**NEIN**	**NEIN**	**JA**	**JA**

Voraussetzungen

Damit Sie diese Einstellung nutzen können, müssen Sie über Berechtigungen für die Systemverwaltungsrolle verfügen.

Gerät stilllegen

Verfahren

1. **Wechseln Sie zu Admin > System > Gerätebereinigung. Die Seite "Gerätebereinigung" wird geöffnet.**
2. **Wählen Sie Gerät stilllegen aus.**
3. **Mithilfe der Tabelle Geräte stilllegen können Sie die Details angeben.**
4. **Klicken Sie auf Liste der Geräte anzeigen, die nicht eingecheckt haben. Daraufhin wird die Liste der Geräte angezeigt, die seit einer bestimmten Anzahl von Tagen nicht eingecheckt haben.**
5. **Klicken Sie alternativ auf Geräte jetzt stilllegen, um die Stilllegung der Geräte zu planen.**
6. **Das Ivanti Neurons for MDM-Administrationsportal legt die angegebenen Geräte still.**

	7.	Klicken Sie auf **Speichern**, um Ihre Einstellung zu speichern.

	8.	(Optional) Wenn Sie die Werte aktualisieren, können Sie die Einstellungen mit **Zurücksetzen** auf die ursprünglichen Werte zurücksetzen.

Gerät stilllegen

Feld	Beschreibung
Plattformen auswählen	Wählen Sie die Plattform aus, auf der die Einstellungen für die Gerätebereinigung angewendet werden sollen. Diese Option ist derzeit nur für die Einstellungen **Gerät stilllegen** und **Gerät mit ausstehender Stilllegung stilllegen** verfügbar.
Geräte stilllegen, die seit mehr als (Tagen) nicht mehr eingecheckt haben **Maximale Anzahl der stillzulegenden Geräte pro Sitzung**	Tage: Standardeinstellung ist 30 Tage, maximal sind 365 Tage erlaubt. Wählen Sie 100, 500 oder 1.000 aus (100 ist die Standardeinstellung).
Geräte automatisch nach Zeitplan stilllegen	Markieren Sie das Kontrollkästchen, um Geräte nach einem voreingestellten Zeitplan stillzulegen.
Konfiguration des Zeitplans für Stilllegungen	Wählen Sie eine der folgenden Optionen aus, um die Häufigkeit der Stilllegung festzulegen: • **Täglich** – Die Geräte werden täglich stillgelegt. • **Wöchentlich** – Geben Sie den Wochentag an, um die Stilllegung zu planen. • **Monatlich** – Die Geräte werden am ersten Tag eines Monats stillgelegt.

Stillgelegte Geräte löschen

Verfahren

1. Wechseln Sie zu **Admin** > **System** > **Gerätebereinigung**. Die Seite "Gerätebereinigung" wird geöffnet.
2. Wählen Sie **Stillgelegtes Gerät löschen** aus.
3. Mithilfe der Tabelle **Stillgelegte Geräte löschen** können Sie die Details angeben.
4. Klicken Sie auf **Liste der stillgelegten Geräte anzeigen**. Daraufhin wird die Liste der Geräte angezeigt, die seit einer bestimmten Anzahl von Tagen stillgelegt sind.
5. Klicken Sie alternativ auf **Stillgelegte Geräte jetzt löschen**, um die Löschung der Geräte zu planen.
6. Das Ivanti Neurons for MDM-Administrationsportal löscht die angegebenen Geräte.
7. Klicken Sie auf **Speichern**, um Ihre Einstellung zu speichern.
8. (Optional) Wenn Sie die Werte aktualisieren, können Sie die Einstellungen mit **Zurücksetzen** auf die ursprünglichen Werte zurücksetzen.

Stillgelegte Geräte löschen

Feld	Beschreibung
Geräte löschen, die seit mehr als (Tagen) stillgelegt sind	Tage: Standardeinstellung ist 30 Tage, maximal sind 365 Tage erlaubt.
Maximale Anzahl der zu löschenden stillgelegten Geräte pro Sitzung	Wählen Sie 100, 500 oder 1.000 aus (100 ist die Standardeinstellung).
Stillgelegte Geräte automatisch nach Zeitplan löschen	Markieren Sie das Kontrollkästchen, um Geräte nach einem voreingestellten Zeitplan stillzulegen.
Konfiguration des Zeitplans für Löschungen	Wählen Sie eine der folgenden Optionen aus, um die Häufigkeit der Löschung festzulegen: • **Täglich** – Die Geräte werden täglich gelöscht. • **Wöchentlich** – Geben Sie den Wochentag an, um die Löschung zu planen. • **Monatlich** – Die stillgelegten Geräte werden am ersten Tag eines Monats gelöscht.

Komplett gelöschte Geräte löschen

Verfahren

1. Wechseln Sie zu **Admin** > **System** > **Gerätebereinigung**. Die Seite "Gerätebereinigung" wird geöffnet.
2. Wählen Sie **Komplett gelöschtes Gerät löschen** aus.
3. Mithilfe der Tabelle **Komplett gelöschte Geräte löschen** können Sie die Details angeben.
4. Klicken Sie auf **Liste der komplett gelöschten Geräte anzeigen**. Daraufhin wird die Liste der Geräte angezeigt, die seit einer bestimmten Anzahl von Tagen stillgelegt sind.
5. Klicken Sie alternativ auf **Komplett gelöschte Geräte jetzt löschen**, um die Löschung von komplett gelöschten Geräten zu planen.
6. Das Ivanti Neurons for MDM-Administrationsportal löscht die angegebenen Geräte.
7. Klicken Sie auf **Speichern**, um Ihre Einstellung zu speichern.
8. (Optional) Wenn Sie die Werte aktualisieren, können Sie die Einstellungen mit **Zurücksetzen** auf die ursprünglichen Werte zurücksetzen.

Komplett gelöschte Geräte löschen

Feld	Beschreibung
Geräte löschen, die vor mehr als (Tagen) komplett gelöscht wurden	Tage: Standardeinstellung ist 30 Tage, maximal sind 365 Tage erlaubt.
Maximale Anzahl der komplett gelöschten und pro Sitzung zu löschenden Geräte	Wählen Sie 100, 500 oder 1.000 aus (100 ist die Standardeinstellung).
Komplett gelöschte Geräte automatisch nach Zeitplan löschen	Markieren Sie das Kontrollkästchen, um komplett gelöschte Geräte nach einem voreingestellten Zeitplan zu löschen.
Konfiguration des Zeitplans für die Löschung komplett gelöschter Geräte	Wählen Sie eine der folgenden Optionen aus, um die Häufigkeit der Löschung festzulegen: • **Täglich** – Komplett gelöschte Geräte werden täglich gelöscht. • **Wöchentlich** – Geben Sie den Wochentag an, um die Löschung zu planen. • **Monatlich** – Komplett gelöschte Geräte werden am ersten Tag eines Monats gelöscht.

Geräte mit ausstehender Komplettlöschung löschen

Verfahren

1. Wechseln Sie zu **Admin** > **System** > **Gerätebereinigung**. Die Seite "Gerätebereinigung" wird geöffnet.
2. Wählen Sie **Gerät mit ausstehender Komplettlöschung löschen** aus.
3. Mithilfe der Tabelle **Komplett gelöschte Geräte löschen** können Sie die Details angeben.
4. Klicken Sie auf **Liste der Geräte mit ausstehender Komplettlöschung anzeigen**. Daraufhin wird die Liste der Geräte angezeigt, die innerhalb einer bestimmten Anzahl von Tagen komplett gelöscht werden sollen.
5. Klicken Sie auf **Komplett gelöschte Geräte jetzt löschen**. Alternativ können Sie die Löschung der ausstehenden Geräte planen.
6. Das Ivanti Neurons for MDM-Administrationsportal löscht die angegebenen Geräte.
7. Klicken Sie auf **Speichern**, um Ihre Einstellung zu speichern.
8. (Optional) Wenn Sie die Werte aktualisieren, können Sie die Einstellungen mit **Zurücksetzen** auf die ursprünglichen Werte zurücksetzen.

Geräte mit ausstehender Komplettlöschung löschen

Feld	Beschreibung
Geräte löschen, deren Komplettlöschung seit mehr als (Tagen) aussteht	Tage: Standardeinstellung ist 30 Tage, maximal sind 365 Tage erlaubt.
Maximale Anzahl der Geräte mit ausstehender Komplettlöschung, die pro Sitzung gelöscht werden	Wählen Sie 100, 500 oder 1.000 aus (100 ist die Standardeinstellung).
Geräte mit ausstehender Komplettlöschung automatisch nach Zeitplan löschen	Markieren Sie das Kontrollkästchen, um komplett gelöschte Geräte nach einem voreingestellten Zeitplan zu löschen.
Konfiguration des Zeitplans für die Löschung von Geräten mit ausstehender Komplettlöschung	Wählen Sie eine der folgenden Optionen aus, um die Häufigkeit der Löschung festzulegen: • **Täglich** – Geräte mit ausstehender Komplettlöschung werden täglich gelöscht. • **Wöchentlich** – Geben Sie den Wochentag an, um die Löschung zu planen. • **Monatlich** – Geräte mit ausstehender Komplettlöschung werden am ersten Tag eines Monats gelöscht.

Geräte mit ausstehender Stilllegung stilllegen

Verfahren

1. Wechseln Sie zu **Admin** > **System** > **Gerätebereinigung**. Die Seite "Gerätebereinigung" wird geöffnet.
2. Wählen Sie **Gerät mit ausstehender Stilllegung stilllegen** aus.
3. Mithilfe der Tabelle **Geräte mit ausstehender Stilllegung stilllegen** können Sie die Details angeben.
4. Klicken Sie auf **Liste der Geräte mit ausstehender Stilllegung anzeigen**. Daraufhin wird die Liste der Geräte angezeigt, die innerhalb einer bestimmten Anzahl von Tagen stillgelegt werden sollen.
5. Klicken Sie auf **Stilllegung der Geräte mit ausstehender Stilllegung jetzt erzwingen**. Alternativ können Sie die Stilllegung der ausstehenden Geräte planen.
6. Das Ivanti Neurons for MDM-Administrationsportal legt die angegebenen Geräte still.
7. Klicken Sie auf **Speichern**, um Ihre Einstellung zu speichern.
8. (Optional) Wenn Sie die Werte aktualisieren, können Sie die Einstellungen mit **Zurücksetzen** auf die ursprünglichen Werte zurücksetzen.

Geräte mit ausstehender Stilllegung stilllegen

Feld	Beschreibung
Geräte mit ausstehender Stilllegung stilllegen, die seit mehr als (Tagen) nicht eingecheckt haben	Tage: Standardeinstellung ist 30 Tage, maximal sind 365 Tage erlaubt.
Maximale Anzahl der Geräte mit ausstehender Stilllegung, die pro Sitzung stillgelegt werden	Wählen Sie 100, 500 oder 1.000 aus (100 ist die Standardeinstellung).
Geräte mit ausstehender Stilllegung automatisch nach Zeitplan stilllegen	Markieren Sie das Kontrollkästchen, um die Geräte mit ausstehender Stilllegung nach einem voreingestellten Zeitplan stillzulegen.
Konfiguration des Zeitplans für die Stilllegung von Geräten mit ausstehender Stilllegung	Wählen Sie eine der folgenden Optionen aus, um die Häufigkeit der Löschung festzulegen: • **Täglich** – Die ausstehenden Geräte werden täglich stillgelegt. • **Wöchentlich** – Geben Sie den Wochentag an, um die Stilllegung der ausstehenden Geräte zu planen. • **Monatlich** – Die ausstehenden Geräte werden am ersten Tag eines Monats stillgelegt.

Wenn ein Gerät stillgelegt wird und der letzte Check-in lange zurückliegt, wird die letzte Check-in-Zeit nur für das Bestimmen der Gerätelöschung berücksichtigt. Beispiel: Wenn das Gerät zuletzt vor 30 Tagen eingecheckt hat und das Gerät heute stillgelegt wird (möglicherweise aufgrund der Option "Geräte, die seit mehr als (Tagen) nicht mehr eingecheckt haben") und wenn die Option "Geräte löschen, die vor mehr als (Tagen) stillgelegt wurden" auf 30 Tage festgelegt ist, wird das Gerät sofort gelöscht, sobald der Auftrag "Stillgelegtes Gerät löschen" ausgeführt wird.

12.1.3. DSGVO-Profile

Das Ivanti Neurons for MDM-Administrationsportal enthält jetzt die Seite "DSGVO-Profile", über die Sie Benutzergruppen DSGVO-Profile zuweisen können. Das DSGVO-Profil kann nur Benutzergruppen zugewiesen werden und nicht einzelnen Benutzern.

Beachten Sie Folgendes:

- Sie müssen das DSGVO-Profil zuerst aktivieren, bevor Sie es einer bestimmten Benutzergruppen zuweisen.
- Wenn Sie das DSGVO-Profil deaktivieren, werden alle Profileinschränkungen deaktiviert, die der Benutzergruppe bereits zugewiesen waren.
- Nachdem Sie das DSGVO-Profil aktiviert haben, wird die Bearbeitungsfunktion für einige Felder eingeschränkt oder deaktiviert.

Felder, die nach der Zuweisung des DSGVO-Profils ausgeblendet werden

Wenn für einen Benutzer ein DSGVO-Profil gilt, blendet Ivanti Neurons for MDM standardmäßig folgende Felder aus, wenn Informationen zum Benutzer angezeigt werden:

- **Benutzer-ID**
- **Name des Benutzers**
- **E-Mail-Adresse**
- **Seriennummer**
- **ICCID**
- **IMSI**
- **MEID**
- **IP-Adresse**
- **Telefonnummer**
- **IMEI**
- **eSIM-Kennung**
- **Standort**

> Falls der Standort zum DSGVO-Profil hinzugefügt wurde, werden die Gerätestandort-Felder "Zuletzt lokalisiert am", "Breitengrad" und "Längengrad" bei den Gerätedetails für diejenigen Benutzer maskiert, denen das DSGVO-Profil zugewiesen ist.

Aktivieren des DSGVO-Profils

Sie können ein DSGVO-Profil aktivieren und bestimmte Felder auswählen, die im Ivanti Neurons for MDM-Administrationsportal und auf den Geräten nicht sichtbar sein sollen.

ProcedureVerfahren

	1.	**Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.**
	2.	**Wechseln Sie zu Admin > System > DSGVO-Profile.**

	3.	Klicken Sie auf **Aktivieren**.
	4.	Klicken Sie auf das Bearbeitungssymbol (Stift).
	5.	Wählen Sie die auszublendenden Felder aus.
	6.	Klicken Sie auf **Speichern**. Die ausgewählten Felder werden maskiert und zeigen die Werte zu den jeweiligen Benutzern nicht an.

Zuweisen des DSGVO-Profils zu Benutzergruppen

Nachdem Sie das DSGVO-Profil aktiviert haben, können Sie es bestimmten Benutzergruppen zuweisen.

ProcedureVerfahren

	1.	Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
	2.	Gehen Sie zu **Benutzer** > **Benutzergruppen**.
	3.	Wählen Sie eine Benutzergruppe aus der Liste aus.
	4.	Klicken Sie auf die Dropdownliste **Aktionen** und wählen Sie **DSGVO-Profil zuweisen** aus. Das DSGVO-Profil wird allen Benutzern der jeweiligen Gruppe zugewiesen. Die ausgewählten Werte werden ausgeblendet, sodass sie im Administrationsportal und auf den Benutzergeräten nicht sichtbar sind. Da Sie als Administrator ebenfalls Mitglied der Gruppe "Alle Benutzer" sind, weisen Sie das DSGVO-Profil nicht der Gruppe "Alle Benutzer" zu.

12.1.4. Benachrichtigungs-E-Mails

Lizenz: Silver

Sie können die Liste mit den E-Mail-Adressen der Benutzer konfigurieren, die je nach Dringlichkeit der Benachrichtigung E-Mail-Benachrichtigungen erhalten sollen.

Die Funktion zur Benachrichtigung per E-Mail ist optimal. Sie können sie nach Bedarf ein- oder ausschalten. Voraussetzung ist, dass Sie Systemverwaltungsrechte zur Verwendung dieser Funktion erhalten haben.

1. Klicken Sie auf **Admin > System > Benachrichtigungs-E-Mails**. Die Seite für die **Benachrichtigungs-E-Mails** wird angezeigt.
2. Klicken Sie im Abschnitt mit den Benachrichtigungs-E-Mail-Einstellungen aufON, um die Benachrichtigungs-E-Mails zu aktivieren.
3. Klicken Sie auf **Empfänger hinzufügen**. Das Popup-Fenster Empfänger hinzufügen wird angezeigt.
4. Aktualisieren Sie in dem Popup-Fenster **Empfänger hinzufügen** folgende Felder:
    - Geben Sie die E-Mail-ID des Empfängers an, an den die Benachrichtigung gesendet werden soll.
    - Zu sendende Benachrichtigungsarten - Wählen Sie die Benachrichtigungsart aus, indem Sie das Kontrollkästchen aktivieren. Die folgenden Benachrichtigungsarten sind verfügbar: **Kritische Benachrichtigung, Warnmeldungen, Informationsbenachrichtigungen**.
5. Klicken Sie auf **OK**. Die Details der Einstellungen werden in einer Tabelle angezeigt.
6. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

12.1.5. Rollenverwaltung

Rollen sind gepackte Gruppen von Berechtigungen, mit denen Berechtigungsgruppen einem Administrator zugewiesen und deren Zugriff auf bestimmte spezifische Funktionsbereiche beschränkt wird. Cloud bietet einen Satz von Systemrollen, die zugewiesen (oder bearbeitet) werden können, sowie eine Möglichkeit, benutzerdefinierte Rollen zu erstellen. Sie können nach einer bestimmten Berechtigung basierend auf der Kategorie suchen, und alle Optionen, die mit der jeweiligen Rolle oder Berechtigung in der Benutzeroberfläche verbunden sind, werden angezeigt. Für Berechtigungen, die als abhängige Berechtigungen hinzugefügt werden, wird ein Tooltipp angezeigt.

> Die Seite "Rollenverwaltung" und die zugehörigen Optionen sind für konvergente Mandanten ausgeblendet, die sowohl Zugriff auf Ivanti Neurons for UEM als auch auf Ivanti Neurons for MDM haben.

Es gibt zwei Arten von Berechtigungen und damit auch zwei Arten von Rollen:

- Space-spezifische Rollen– Die Berechtigungen sind Space-spezifisch und gelten daher nur in einem bestimmten Space. Beispiele sind Gerätemanagement und App-Management in einem Space.
- Space-übergreifende Rollen– Die Berechtigungen gelten naturgemäß für alle Rollen. Beispiele sind Einstellungen auf Mandantenebene, MDM-Zertifikate und App-Katalogeinstellungen.

Kundenspezifische Rollen erstellen

Sie können eine benutzerspezifische, Space-übergreifende oder Space-spezifische Rolle erstellen. Wenn Sie Berechtigungen benötigen, werden die entsprechenden Berechtigungen automatisch ausgewählt. Dementsprechend kann ein Benutzer, dem eine benutzerdefinierte Rolle zugewiesen wurde, nur die spezifischen Aktionen (z. B. außer Dienst stellen, Löschen) ausführen, die verfügbar sind, wenn der Benutzer die Seite „Geräte“ oder die Seite „Gerätedetails“ besucht.

Wenn Sie die benutzerdefinierte Rolle "Benutzerregistrierungs-PIN anzeigen" anwenden, können Benutzer die PIN anderer Benutzer mit gleichen oder niedrigeren Zugriffsrechten anzeigen, sie können jedoch keine PINs für andere Benutzer erstellen.

> Die neu erstellte benutzerdefinierte Rolle kann nicht automatisch jedem zugewiesen werden. Der Superadmininstrator des Mandanten muss sie den erforderlichen Admin-Benutzern zuweisen, die sie später bei Bedarf anderen Benutzern zuweisen können.

Verfahren

1. Wechseln Sie zu **Admin** > **Rollenverwaltung**.
2. Klicken Sie auf **+Benutzerdefinierte Rolle hinzufügen**.
3. Geben Sie auf der Seite **Rolle erstellen** den **Namen** der neuen Rolle ein.
4. (Optional) Fügen Sie eine Beschreibung für die neue Rolle hinzu.
5. Wählen Sie als **Rollentyp** einen der folgenden Rollentypen aus:
    - **Space-übergreifende Rollen**
    - **Space-spezifische Rolle**
6. Wählen Sie unter **Berechtigungen** die erforderlichen granularen Berechtigungen aus.
7. Administrations- und Benutzerberechtigungen finden Sie in der folgenden Tabelle.
   Klicken Sie auf **Speichern**.

In der folgenden Tabelle werden die Berechtigungen, Rollen und Attribute aufgelistet, die Sie für die Erstellung einer benutzerdefinierten Rolle verwenden können:

Rollentyp	Berechtigungskategorie	Granulare Berechtigungen
Space-übergreifende Rollen		
Administrator		
	Benutzerdefinierte Attribute verwalten	• Benutzerattribut hinzufügen • Kundenspezifisches Attribut löschen • Benutzerdefiniertes Attribut bearbeiten • Benutzerdefiniertes Attribut anzeigen
	Support-Administratoren	• Support-Administratoren hinzufügen • Support-Administratoren löschen • Support-Administratoren deaktivieren • Support-Administratoren & bisherige Anmeldungen zeigen
	Zertifikatsautorität	• Zertifikatsautorität hinzufügen • Zertifikatsautorität löschen
	Connector	• Connector-Protokolle hinzufügen • Connector-Protokolle löschen • Connector anzeigen • Connector aktualisieren
	LDAP-Verwaltung	• Benutzer/Gruppe/OU hinzufügen • Server hinzufügen • Server durchsuchen • Server löschen • Server suchen • Sync-Server

Rollentyp	Berechtigungskategorie	Granulare Berechtigungen
		• Benutzer/Gruppe/OU entfernen • Server anzeigen Für alle LDAP-Berechtigungen in diesem Abschnitt ist die Berechtigung für View Connector erforderlich. Sie wird automatisch im Abschnitt „Konnektor“ ausgewählt, wenn Sie eine dieser LDAP-Berechtigungen auswählen.
	Lizenzverwaltung	Lizenzen anzeigen
	App-Verteilung verwalten	**App-Verteilung aktualisieren** Die Berechtigung **App-Verteilung aktualisieren** ist jetzt für benutzerdefinierte Rollen unter **App-Verteilung verwalten** verfügbar. Benutzer mit der Rolle Systemverwaltung erhalten diese Berechtigung standardmäßig automatisch. Die App-Verteilungsseite enthält jetzt das Kontrollkästchen **Space Admin erlauben, die Verteilung zu bearbeiten**, das standardmäßig für neue App-Versionen aktiviert ist. Benutzer, denen eine benutzerdefinierte Rolle mit dieser neuen Berechtigung zugewiesen wurde, sowie Benutzer mit der App Management-Rolle (ohne Systemmanagementzugriff) können diese Einstellung ändern. Für jede Anwendungsversion wird die Verfügbarkeit der Einstellung App-Verteilung sperren auf der Verteilungsseite angezeigt und alle Entschlüsselungsversuche werden jetzt im Audit Trail erfasst.
Benutzer		
	Benutzerverwaltungs-Aktionen	• Benutzer anzeigen • Benutzer aktualisieren • Nachricht an Benutzer senden • Rollen für Benutzer anhängen/zuweisen • Benutzer erstellen • Benutzer löschen • Benutzer einladen • Benutzerregistrierungs-PIN anzeigen
	Benutzerdefiniertes Benutzerattribut zuweisen	• Attribut löschen • Attribut anzeigen • Attribut hinzufügen/bearbeiten

Rollentyp	Berechtigungskategorie	Granulare Berechtigungen
	Benutzergruppen	• Benutzergruppe anzeigen • Benutzergruppe bearbeiten • Rollen an Benutzergruppe anhängen/zuweisen • Benutzergruppe erstellen • Benutzergruppe löschen
	Berichtsverwaltung	• Bericht erstellen • Bericht bearbeiten • Bericht ausführen • Berichtsdatensatz löschen • Bericht anzeigen • Bericht löschen • Berichtsdatensatz herunterladen
Geräten		
	Massenregistrierung	• Massenregistrierung erstellen • Massenregistrierung aktualisieren • Benutzer der Massenregistrierung zuweisen • Massenregistrierung anzeigen • Massenregistrierung löschen
Space-spezifische Rolle		
Geräten		
	Geräteaktionen	• Gerät einem Benutzer zuweisen • Geräteaktivierungssperre löschen • Gerät löschen • "Verloren-Modus" des Geräts deaktivieren • "Verloren-Modus" des Geräts aktivieren • Geräteanmeldung erzwingen

Rollentyp	Berechtigungskategorie	Granulare Berechtigungen
		• Gerät sperren • Gerät entsperren • Abmeldung des Geräts erzwingen • System-Apps des Geräts neu installieren • Gerät neu starten • iOS-Geräte-Updates planen • Übergabe des Geräteeigentums • Gerät außer Dienst stellen • Außerdienststellung des Geräts stornieren • Gerät herunterfahren • Gerät anzeigen • Wipe für Gerät durchführen • Löschung des Geräts stornieren • Betriebssystemversion des Geräts aktualisieren • Massenzuweisung über Upload • TeamViewer-Sitzung starten • Kiosk-Modus aufrufen • Kiosk-Modus beenden
	Kundenspezifische Geräteattribute zuweisen	• Benutzerdefiniertes Geräteattribut hinzufügen/bearbeiten • Benutzerdefiniertes Geräteattribut löschen • Benutzerdefiniertes Attribut des Geräts anzeigen Alle Berechtigungen zur Zuweisung von benutzerdefinierten Geräteattributen in diesem Abschnitt erfordern eine Leseberechtigung für die Geräte. Sie wird automatisch im Abschnitt „Geräteaktionen“ ausgewählt, wenn Sie eine der Berechtigungen für „Benutzerdefinierte Geräteattribute zuweisen“ auswählen.
	Gerätekonfigurationen	• Profil ausschließen • Push-Profil • Ausgeschlossenes Profil per Push übertragen • Installation bei Fehler wiederholen

Rollentyp	Berechtigungskategorie	Granulare Berechtigungen
	Gerätegruppen	• Gerätegruppe hinzufügen • Gerätegruppe löschen • Gerätegruppe bearbeiten • Gerätegruppe anzeigen
	Massenregistrierung	• Massenregistrierung erstellen • Massenregistrierung aktualisieren • Benutzer der Massenregistrierung zuweisen • Massenregistrierung anzeigen • Massenregistrierung löschen
Konfigurationen	App-Inventar	• App-Bestand anzeigen
	Konfigurationen	• Konfigurationen anzeigen/exportieren • Konfigurationen bearbeiten/priorisieren • Konfigurationen hinzufügen/klonen • Konfigurationen löschen
Richtlinien		
	Richtlinien	• Richtlinien anzeigen • Richtlinien bearbeiten/priorisieren • Richtlinien hinzufügen/klonen • Richtlinien löschen

Um eine Rolle zu bearbeiten, gehen Sie auf die Seite „Verwaltung, Rollenverwaltung“ und klicken auf das Bearbeitungssymbol unter **Aktionen** neben dem Namen der Rolle. Ein Benutzer kann eine Space-übergreifende Rolle nicht für eine Space-spezifische Rolle bearbeiten und umgekehrt.

Verwandte Themen:

- Weitere Informationen zum Zuweisen einer kundenspezifischen Rolle für einen Benutzer finden Sie unter **Rollen zuweisen**.
- Unter **Benutzerrollen** finden Sie eine Liste der Standardrollen.
- **Anpassbare Berichte verwenden**
- **Verwendung geplanter Berichte**

12.1.6. Räume

Dieser Abschnitt enthält die folgenden Themen:

- Räume
- Spaces verwalten
- Beispiele für Spaces
- Geräte delegieren
- Apps delegieren

12.1.6.1. Räume

Lizenz: Silver

Mit Spaces lässt sich ein UEM-System zur delegierten Administration in unabhängig voneinander verwaltete Einheiten aufteilen. Spaces können zur Abbildung einer Organisationshierarchie erstellt werden. Die Cloud unterstützt eine einstufige Delegation mit einer zentralen Verwaltungseinheit, dem so genannten Standard-Space, und einer Reihe untergeordneter Verwaltungseinheiten, die als delegierte Spaces bezeichnet werden. Jedes UEM-System wird mit einem Standard-Space erstellt.

> Die Seite "Spaces" und die zugehörigen Optionen sind für konvergente Mandanten ausgeblendet, die sowohl Zugriff auf Ivanti Neurons for UEM als auch auf Ivanti Neurons for MDM haben.

Ein Space ermöglicht die delegierte Verwaltung der folgenden Systemkomponenten. Benutzer und Benutzergruppen können nicht delegiert werden.

- Geräte
- Konfigurationen
- Richtlinien
- Gerätegruppen
- Anwendungen
- App-Katalog
- Ein Apple Apps and Books-Token

Wenn sich ein Administrator am Ivanti Neurons for MDM Admin Portal für einen Mandanten mit mindestens einem delegierten Space anmeldet, wird dem Administrator das Promo-Popup-Fenster für die Anmeldung beim Admin Portal angezeigt. Das Promo-Popup wird nach der Erstellung des delegierten Space und bei der Benutzeranmeldung nicht mehr angezeigt, wenn bereits ein delegierter Space erstellt wurde.

Rollen für globale und delegierte Space-Administratoren

Ein Administrator mit den entsprechenden Berechtigungen für den Zugriff auf den Standard-Space wird als "globaler Administrator" bezeichnet. Der Zugang zum Standard-Space kann entweder schreibgeschützt sein oder sowohl Schreib- als auch Leseoperationen erlauben. Ein globaler Administrator mit den entsprechenden Administrator-Rollen kann delegierte Spaces erstellen und delegierte Administratoren zu deren Verwaltung zuweisen. Einem delegierten Administrator kann die Verwaltung eines oder mehrerer delegierter Spaces übertragen werden.

Die Spaces, auf die ein bestimmter Administrator zugreifen kann, sind in dem Dropdown-Auswahlfeld für Spaces in der oberen linken Ecke der Registerkarten für Geräte und Apps aufgelistet. Wechseln Sie mit dem Dropdown-Feld zu dem gewünschten Space, um ihn anzuzeigen und zu verwalten.

Ein globaler Administrator hat die transparente Kontrolle über alle delegierten Spaces sowie den Standard-Space. Ein delegierter Administrator hat eine transparente Kontrolle nur für die Spaces, die ihm vom globalen Administrator übertragen wurden. Ein globaler Administrator behält die zentrale Kontrolle über die delegierten Spaces, wobei ein delegierter Administrator die ihm übertragenen Spaces selbstständig verwalten kann. Der Grad der Autonomie hängt davon ab, ob die Delegation vererbt oder aus dem Standard-Space kopiert wird.

Die folgenden Rollen sind unterschiedliche Benutzerrollen, die Benutzer können folgende Aufgaben ausführen:

Vererbte App in einem delegierten Space

- Zum Zeitpunkt der Delegation vorhandene Bewertungen oder Rezensionen werden vererbt und sind für die Benutzer in dem delegierten Space sichtbar, dies gilt auch für den Benutzernamen des Autors.
- Der delegierte Administrator kann Bewertungen und Bewertungen für eine vererbte App nicht löschen.
- Der delegierte Administrator kann Bewertungen und Bewertungen für eine vererbte App exportieren.
- Benutzer in delegierten Spaces können Bewertungen und Bewertungen für die vererbte App ergänzen.
- Für Benutzer in delegierten Spaces sind Bewertungen und Bewertungen von Benutzern in den delegierten Spaces sichtbar, dies gilt auch für den Benutzernamen des Autors.

App in einem delegierten Space (ergänzt, nicht vererbt)

- Nur der globale Administrator kann die Rezensionen unter **Apps > Katalogeinstellungen > Bewertungen und Rezensionen aktivieren oder deaktivieren**.
- Benutzer in dem delegierten Space können Bewertungen und Rezensionen ergänzen.
- Der delegierte Administrator kann von Benutzern im gleichen delegierten Space hinzugefügte Bewertungen löschen.
- Bewertungen oder Bewertungen, die Benutzer in anderen delegierten Spaces ergänzt haben, sind für Benutzer in anderen delegierten Spaces sowie im Standard-Space nicht sichtbar.
- Der delegierte Administrator kann von Benutzern hinzugefügte Bewertungen einschließlich der Benutzernamen exportieren.

Delegierte App in einem Standard-Space

- Der globale Administrator kann Bewertungen oder Bewertungen löschen, die ein Benutzer in einem delegierten Space ergänzt hat.
- Der globale Administrator kann alle Bewertungen oder Bewertungen einschließlich der von Benutzern im delegierten Space ergänzten Bewertungen und Bewertungen exportieren.
- Benutzer im Standard-Space können Bewertungen und Bewertungen sehen, die Benutzer in delegierten Spaces ergänzt haben. Dies gilt auch für den Benutzernamen.

Priorität eines delegierten Space

Der Standard-Space in einem UEM-System hat immer die niedrigste Priorität. Die Priorität eines delegierten Space gegenüber anderen Spaces wird vom globalen Administrator eingestellt und kann jederzeit geändert werden. Delegierte Spaces werden entsprechend ihrer Rangfolge aufgelistet; sie erscheinen in der Seite „Spaces“ in der Registerkarte „Administrator“ im Administrator-Portal, sortiert beginnend mit der höchsten Priorität.

Delegation durch Vererbung oder Kopieren

Ein wichtiges Konzept bei delegierter Administration ist die Vererbung bzw. Kopie einer Systemkomponente aus dem Standard-Space.

12.1.6.2. Spaces verwalten

Spaces ermöglichen Ihnen, Geräte zur Verwaltung verschiedenen Administratoren zuzuordnen (delegierte Administration). Der für eine Space zuständige Administrator kann die auf dem Gerät angewendeten Konfigurationen und Richtlinien in dem Space festlegen. Sobald Sie die Spaces erstellt haben, können Sie jeden Space dem jeweiligen relevanten oder geeigneten Administrator zuweisen.

Diese Seite zu Spaces beinhaltet Folgendes:

- Suchfunktionen zum schnellen Ermitteln von Spaces
- Paginierungssteuerungen zum Navigieren in einer großen Anzahl von Spaces
- Space-Priorisierungskontrollen zum Steuern der Reihenfolge delegierter Spaces
- Optionen zum Auswählen und Löschen mehrerer Spaces

> Der Standard-Space kann nicht gelöscht werden.

- Alphabetisches Sortieren von Spaces
- Liste der kürzlich angezeigten Spaces in der Space-Auswahl
- Dauerhafte Space-Auswahl auf den Seiten Geräte, Konfigurationen, Richtlinien und Inhalt, wodurch beim Navigieren zwischen den Seiten keine erneute Space-Auswahl erforderlich ist.

> Der Benutzer kann nur die zugewiesenen Spaces und nicht alle Spaces anzeigen. Bislang gilt diese Einstellung nur für die Module **Geräte**, **Gerätegruppen**, **Apps**, **App-Inventar**, **Inhalt**, **Konfigurationen**, **Richtlinien** und **Zertifikatverwaltung**. Spaces, die während dem Anzeigen eines dieser Module aus der Liste der Spaces ausgewählt werden, werden als vom Administrator bevorzugte Standardauswahl für das Modul gespeichert. Diese Einstellungen werden nicht nur für die derzeit angemeldete Sitzung, sondern auch für zukünftige Sitzungen gespeichert.

Die von Ihnen erstellten Spaces übernehmen alle Konfigurationen des Standard-Space. Daher können alle Konfigurationen, die Sie später in dem Standard-Space erstellen, auch für die anderen Spaces verwendet werden. Allerdings werden Änderungen an bestehenden Konfigurationen nicht übernommen.

Die von Ihnen erstellten Spaces erhalten nur Kopien von den Richtlinien, die zum Zeitpunkt der Erstellung im Standard-Space vorhanden sind. Richtlinien, die Sie später im Standard-Space erstellen, gelten nur für den Standard-Space.

Erstellen Sie die Richtlinien, die bestimmen, welche Geräte dem Space angehören. Sie können diese Regeln mit geeigneten Operatoren filtern, beispielsweise „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“ und „is not equal to. Die Regeln können miteinander mit den Optionen ANY (OR) oder ALL (AND) verschachtelt werden. Die Genauigkeit der Regeln lässt sich mit einem Text überprüfen, der am Ende der Regeln erscheint.

Das Ivanti Neurons for MDM-Administratorportal zeigt die Anzahl doppelter Benutzergruppen und die zugehörige Anzahl der GUIDs an, damit doppelte Gruppen identifiziert werden können, wenn das Attribut "Name der Benutzergruppe" im Regeleditor ausgewählt wird. Eine Tabelle unter dieser Regel zeigt außerdem die Liste der doppelten Benutzergruppen zusammen mit Details wie Name der Benutzergruppe, GUID, Quelle und Distinguished Name (DN).

Regeln können Geräte nach folgenden Merkmalen identifizieren:

- Bei Entra ID registriert
- APNS-fähig

- Alternative Seriennummer (nur für Android - für Samsung-Geräte im Geräteverwaltungs- oder Gerätebesitzermodus)
- 5G Network Slicing aktivieren (Android 12.0+)
- Android Work Managed-Gerät, nicht GMS-Modus (AOSP), aktiviert
- Dediziertes Android-Gerät
- Für Android Enterprise geeignet
- Verwaltetes Android-Gerät mit Arbeitsprofil
- Android-SafetyNet-Attestierungstyp
- Android Enterprise aktiviert
- Android Sicherheits-Patchlevel (für Android-Geräte)
- In Android Enterprise verwaltete Geräte aktiviert (Geräteeigentümer)
- Android Enterprise aktiviert
- Android-Arbeitsprofil auf unternehmenseigenen Geräten aktiviert
- Nativer Anti-Phishing-Status
- Anti-Phishing-Status
- Anti-Phishing-VPN-Status
- Automatische Geräteregistrierung eingereicht
- Automatische Geräteregistrierung aktiviert
- Autopilot registriert
- Azure Client-Status-Code
- Zeit des Compliance-Berichts für das Azure-Gerät
- Compliance-Status des Azure-Geräts
- ID des Azure-Geräts
- Von Sentry blockiert
- Von Access blockiert
- Bootstrap-Token verfügbar
- Massenbereitstellungstyp (Apple Configurator oder Keine)
- Mobilfunkanbieter
- Letzter Check-in durch Client
- Client registriert
- Compliance
- Von Compliance-Aktion blockiert
- Aktueller Ländername (wählen Sie den aktuellen Ländernamen aus der Auswahlliste)
- Aktueller MCC-Code
- Aktueller MNC-Code
- Kundenspezifisches Geräteattribut
- Benutzerdefiniertes LDAP-Attribut
- Kundenspezifisches Benutzerattribut

- Daten-Roaming
- Gerätequelle
- Gerätetyp
- Gerätetyp (Apple)
- Anzeigename
- Verschlüsselung aktiviert
- Name des Heimatlandes (wählen Sie den Namen des Heimatlandes aus der Auswahlliste)
- Eigener MCC-Code
- Eigener MNC-Code
- IMEI
- IMEI2 (nur auf Android-Geräten mit dualem SIM-Port und ab Version 8.0)
- Institutioneller Wiederherstellungsschlüssel aktiviert
- IP-Adresse
- Kiosk-Modus
- Letzte Anmeldung
- Modus "Verloren" aktiviert
- Nur MAM
- Hersteller
- MTD-Aktivierungsstatus
- Mehrfach-Benutzer-Modus
- Betriebssystem
- Betriebssystemversion
- Betriebssystem mit Version
- Verantwortung
- Persönlicher Wiederherstellungsschlüssel aktiviert
- Telefonnr.
- Isoliert
- Wiederherstellungssperre aktiviert
- Roaming
- Secure Apps Status
- Seriennummer
- [Status]
- Überwacht
- Zusätzliche Buildversion
- Zusätzliches BS/Version Extra
- Freischalt-Token verfügbar (iOS)
- User Enrollment Registriert

- Benutzergruppe
- Benutzername
- Sprach-Roaming
- Persönlicher Wiederherstellungsschlüssel für macOS hinterlegt
- macOS Wiederherstellungsschlüsseltyp

> Diese Regeln gelten nur für die Silver-Lizenz und höher.

Space erstellen

Verfahren

1. Wechseln Sie zu **Admin** > **System** > **Spaces**.
2. Klicken Sie auf **Space erstellen**.
3. Geben Sie einen Space-Namen ein.
4. Konfigurieren Sie die entsprechenden Regeln und Einstellungen für den Space.
5. Klicken Sie auf **Speichern**.

Prioritäten für Spaces definieren

Ivanti Neurons for MDM bewertet die Spaces in der Reihenfolge ihrer Auflistung.

Verfahren

1. Klicken Sie auf **Spaces priorisieren**.
2. Wählen Sie das Symbol für "nach oben" oder "nach unten" neben einem Space aus, um die Priorität anzupassen.
3. Klicken Sie auf **Speichern**.

Leerzeichen löschen

1. Wechseln Sie zu **Admin** > **System** > **Spaces**.
2. Wählen Sie ein oder mehrere Spaces aus, indem Sie die Kontrollkästchen aktivieren.
3. Klicken Sie auf **Löschen**. Bestätigen Sie den Löschvorgang, wenn Sie dazu aufgefordert werden.

Einen Administrator einem Space zuordnen

Verfahren

1. Gehen Sie zu **Benutzer**.
2. Suchen Sie den Benutzer, der der Administrator sein wird.
3. Klicken Sie auf den Link für den Benutzer, um Details anzuzeigen.
4. Wählen Sie **Aktionen** > **Rollen zuweisen** aus.
5. Wählen Sie **Geräteverwaltung**.
6. Wählen Sie unter **Geräteverwaltung** den Space für den Administrator aus.
7. Klicken Sie auf **Fertig**.

Wenn sich der Administrator anmeldet, werden nur die Geräte, Konfigurationen und Richtlinien in dem zugewiesenen Space angezeigt.

Konfiguration oder Richtlinie klonen

Sie können Sie eine Konfiguration oder Richtlinie klonen, wenn Sie diese mit einigen Abweichungen kopieren müssen. Sie können die geklonten Konfigurationen oder Richtlinien auch verschiedenen Gerätegruppen zuordnen. Alle Richtlinien können in einem Space geklont werden. Alle Konfigurationen, mit Ausnahme des vom Benutzer bereitgestellten Identitätszertifikats und Threat Defense, können innerhalb eines Space geklont werden. Die folgenden Konfigurationen können aus dem Standard-Space auch Space-übergreifend geklont werden:

- iOS-Einschränkungen
- Web-Clip
- Zertifikat
- Passwort
- SCEP (iOS und Windows)
- Identitätszertifikat (dynamisch generiert)

- Der Name einer Konfiguration oder Richtlinienart sollte in einem Space eindeutig sein. Alle anderen Eigenschaften einer Konfiguration oder Richtlinie können geklont werden.
- Die Konfigurationen werden für alle Spaces geklont, auf die Sie als Administrator Zugriff haben. Sie müssen kein globaler Administrator sein, um eine Konfiguration zu klonen.

Verfahren

1. Gehen Sie je nach der auszuführenden Aufgabe zu **Konfigurationen** oder **Richtlinien**.
2. Klicken Sie auf den Link für die Konfiguration oder Richtlinie, um die Details anzuzeigen.
3. Klicken Sie auf das Symbol **Klonen**.
4. Geben Sie in dem Pop-up-Fenster einen **Namen** und optional eine **Beschreibung** ein.
5. Klicken Sie auf **Weiter**.
6. Modifizieren Sie die Konfiguration oder Richtlinie entsprechend Ihren Anforderungen.
7. Klicken Sie auf **Weiter**.
8. Konfigurieren Sie die Verteilung.
9. Klicken Sie auf **Fertig**.

Weitere Informationen finden Sie unter Space-Beispiele.

12.1.6.3. Beispiele für Spaces

Dieses Thema enthält Beispiele, wie Spaces von Administratoren genutzt werden können.

Administrator pro Standort

ACME, Inc. verfügt über Niederlassungen in Nordamerika und Europa. Aufgrund von Problemen bezüglich Sprache und Zeitzonen, möchte ACME, dass ein Administrator in den USA die nordamerikanischen Geräte und ein Administrator in Deutschland die europäischen Geräten verwaltet.

Um diese Spaces einzurichten, hat ACME folgende Änderungen vorgenommen:

1. Erstellung einer Benutzergruppe in Ivanti Neurons for MDM für Benutzer aus Europa
2. Erstellung einer Benutzergruppe in der Cloud für Benutzer aus Nordamerika
3. Es wurde ein europäischer Space mit folgender Regel erstellt:
4. Benutzergruppe = Europa
   Erstellung eines nordamerikanischen Space mit folgender Regel:
5. Benutzergruppe = Nordamerika
   Die Geräteverwaltungsrolle für jeden Space wurde dem korrekten Administrator zugewiesen.

ACME verfügt nun über folgende Spaces:

- Europa
- Nordamerika
- Standard

Administrator pro Betriebssystem pro Standort

ACME hat beschlossen, dass Android-Geräte nur von Android-Experten verwaltet werden sollen. Den Organisationen in Nordamerika und Europa wurde jeweils ein Android-Experte hinzugefügt. Es werden also zwei neue Spaces benötigt.

Um diese Spaces hinzuzufügen, hat ACME folgende Änderungen vorgenommen:

1. Es wurde ein europäischer Android-Space mit folgenden Regeln erstellt:
2. Benutzergruppe = Europa
   Betriebssystem = Android
   Es wurde ein nordamerikanischer Android-Space mit folgenden Regeln erstellt:
3. Benutzergruppe = Nordamerika
   Betriebssystem = Android
   Die Geräteverwaltungsrolle für jeden Space wurde dem korrekten Administrator zugewiesen.

ACME verfügt nun über folgende Spaces:

- Europa-Android
- Nordamerika-Android
- Europa
- Nordamerika
- Standard

Administrator für Führungskräfte

Die Führungskräfte von ACME haben beschlossen, dass sie einen speziellen Service von einem speziellen Administrator möchten. Nur die wichtigsten Führungskräfte befinden sich auf dieser Liste.

Um diesen Space hinzuzufügen, hat ACME folgende Änderungen vorgenommen:

1. Es wurde ein Space für Führungskräfte mit folgenden Regeln erstellt:
2. Benutzername = jdoe@acme.com
   Benutzername = gkunz@acme.com
   Benutzername = prizzo@acme.com
   Benutzername = fvanhoff@acme.com
   Der Space wurde in der Liste der Seite **Space** nach oben verschoben.
3. Wäre dies nicht der Fall, hätten Führungskräfte mit Android-Geräten den falschen Administrator.
   Die Geräteverwaltungsrolle für den Space wurde dem speziellen Administrator zugewiesen.

ACME verfügt nun über folgende Spaces:

- Management-Team
- Europa-Android
- Nordamerika-Android
- Europa
- Nordamerika
- Standard

Administrator für alle anderen Geräte

Wenn ACME ein neues Büro in Japan eröffnet, werden die hinzugefügten Geräte dem Administrator des Standard-Space zugewiesen, bis ein Japan-Space erstellt wurde.

12.1.6.4. Geräte delegieren

Mit Spaces werden Ihre Geräte in unabhängig voneinander verwaltbare Einheiten getrennt. Die Mitgliedschaft für Spaces hängt von den Regeln ab, die Sie definieren. Mit der Geräte-Delegation kann ein globaler Administrator Geräte in einem UEM-System aufteilen und unabhängig voneinander verwalten. Wenn Geräte delegiert sind, kann der Zugriff auf diese Geräte einer Teilmenge delegierter Administratoren zugeordnet und die Zuständigkeit der Administratoren aufgeteilt werden.

Delegierte Geräte lassen sich in Gerätegruppen zusammenfassen, denen verschiedene kundenspezifische Konfigurationen zugeordnet werden, ohne dass dies sich auf Geräte im Standard-Space oder anderen delegierten Spaces auswirkt.

Regeln für delegierte Spaces erstellen

Mit den Richtlinien für einen Space bestimmen Sie, welche Geräte zu dem Space gehören. Ein Gerät kann nur einem Space angehören. Geräte, die nicht den Regeln für die von Ihnen erstellten Spaces entsprechen, gehören automatisch zum Standard-Space.

1. Wählen Sie **Beliebig**, wenn Sie möchten, dass Geräte in diese Definition eingeschlossen werden, wenn sie eine oder mehrere der Richtlinien erfüllen.
2. Wählen Sie **Alle**, wenn Sie möchten, dass Geräte in diese Definition eingeschlossen werden, wenn sie alle Richtlinien erfüllen.
3. Wählen Sie eine der folgenden Richtlinienarten aus der Dropdown-Liste aus:
    - **LDAP-Attribut:** Hier finden Sie die Regeln für LDAP-Attribute.
    - **Betriebssystem**: Für Richtlinien, die auf dem Betriebssystem des Geräts basieren.
    - **Benutzergruppe**: Richtlinien, die auf der Benutzergruppe des Geräts basieren (wie im Gerätemanagement beschrieben).
    - **Benutzername**: Für Richtlinien, die auf dem mit dem Gerät verbundenen Benutzernamen basieren.
4. Bestimmen Sie die Kriterien für die ausgewählte Richtlinienart:
    - **Anpassbares LDAP-Attribut:** Geben Sie den Namen des benutzerdefinierten LDAP-Attributs ein, das in den LDAP-Einstellungen konfiguriert wurde.
    - **OS**: Wählen Sie Android, iOS, macOSoder Windows.
    - Benutzer Gruppe: Wählen Sie eine der in der Dropdown-Liste angezeigten Benutzergruppen aus. Dies sind die unter **Benutzer > Benutzergruppen** definierten Benutzergruppen.
    - **Benutzername**: Geben Sie einen Benutzernamen ein.
5. Wenn Sie diesem Space eine weitere Regel hinzufügen möchten, klicken Sie auf das Pluszeichen + neben der vorangehenden Regel.
6. Klicken Sie auf **Vorschau**, um zu sehen, welche Geräte dem Space zugeordnet werden.
7. Klicken Sie auf **Speichern**, wenn Sie mit den Geräten in dem Space einverstanden sind.

Geräte, die die Regeln für einen Space nicht mehr erfüllen, werden automatisch in den nächsten passenden Space verschoben. Wenn das Gerät nicht den Richtlinien eines bestehenden Space entspricht, wird das Gerät in den Standard-Space verschoben. Zum Beispiel kann die Entfernung eines Benutzers aus einer Benutzergruppe dazu führen, dass die Geräte des Benutzers in einen anderen Space verschoben werden. Durch Verschieben in einen anderen Space können Veränderungen in den Richtlinien und Konfigurationen entstehen.

12.1.6.5. Apps delegieren

Durch die App-Delegation kann ein globaler Administrator die Cloud aufteilen und Apps unabhängig voneinander verwalten. Der globale Administrator kann öffentliche und hauseigene Apps zentral bereitstellen und verteilen sowie die Trennung und Kontrolle durch delegierte Spaces beibehalten.

Durch zentrale Verteilung einer App kann der globale Administrator das Verwaltungsverhalten der App über App-Konfigurationen sowie die Verteilungsregeln der App vordefinieren. Die App kann dann delegiert und im App-Katalog des delegierten Space angezeigt werden.

Die delegierte App wird dann an Benutzer mit Geräten in einem bestimmten delegierten Space verteilt. Wenn Geräte delegiert sind, kann der Zugriff auf diese Geräte einer Teilmenge delegierter Administratoren zugeordnet und die Zuständigkeit der Administratoren aufgeteilt werden.

Zur Delegation einer Anwendung muss zunächst zumindest ein delegierter Space definiert werden. Wenn eine Anwendung delegiert ist, wird sie allen Spaces zugeordnet. Der App-Delegierungs-Space wird wie folgt klassifiziert:

- Standard-Space
- Delegierte Spaces

App zu einem delegierten Space hinzufügen

Ein delegierter oder globaler Administrator kann eine App zu einem delegierten Space hinzufügen. Die App erscheint nur im App-Katalog des delegierten Space, dem sie hinzugefügt wurde. Wenn Sie eine bisher delegierte App aus dem Standard-Space in einem delegierten Space hinzufügen, tritt ein Fehler auf. In diesem Fall muss zuerst die Vererbung der App im Standard-Space deaktiviert werden, sodass sie einem delegierten Space hinzugefügt werden kann. Weitere Informationen finden Sie unter **Hinzufügen einer Konfiguration** unter **Arbeiten mit Konfigurationen**.

App-Verteilung in einem delegierten Space

Wenn eine App aus dem Standard-Space delegiert wird, werden ihre Verteilungsregeln vererbt. Diese App muss an alle Geräte verteilt werden, die dem delegierten Space zugeordnet sind, dessen Verteilungsregeln auf die App zutreffen.

Globale Administratoren können Space-Administratoren zur Bearbeitung des dynamisch generierten Identitätszertifikats für alle Geräte und für die Option zur benutzerdefinierten Verteilung delegieren.

> Die Änderungen an der Verteilung gelten nur für den jeweiligen Space. Alle anderen Spaces übernehmen weiterhin die Verteilungseinstellungen des Standard-Space.

> App-Genehmigungseinstellungen für Android-Apps: App-Genehmigungseinstellungen nach Space für Android-Apps werden nicht unterstützt. Apps, die im benutzerdefinierten Space genehmigt werden, sind in allen Spaces wirksam.

> Vorhandene Android-Katalog-Apps: Bei Mandanten, in denen öffentliche Android-Apps bereits zum Standard-Space hinzugefügt wurden, muss die Delegierung der Apps zuerst aufgehoben werden, damit eine öffentliche App zu einem anderen Space, der kein Standard-Spcae ist, hinzugefügt werden kann.

Android Enterprise-Apps können nur vom Tenant-Administrator und **nicht** vom Space-Administrator hinzugefügt werden. Verwaltetes Google Play wird auf Unternehmensebene konfiguriert, nicht pro delegiertem Space. Neue Android Enterprise-Apps können daher nur im Standardbereich genehmigt werden. Delegierte Administratoren können bereits genehmigte Apps innerhalb ihrer eigenen Bereiche zuweisen und verwalten, können jedoch keine neuen Android Enterprise-Apps innerhalb von delegierten Spaces genehmigen oder hinzufügen. Alle neuen Apps müssen zuerst im Standardbereich genehmigt werden und können erst dann den entsprechenden Gruppen zugewiesen werden.

Weitere Informationen finden Sie unter **Hinzufügen einer Konfiguration** unter **Arbeiten mit Konfigurationen**.

12.1.7. Support-Administratoren

User_Roles.htmDas Erstellen eines temporären Support-Administrators ermöglicht dem Service-Support-Team die Anmeldung mit Ihren Rollen und Berechtigungen. Dieses Benutzerkonto läuft automatisch nach sieben Tagen ab oder Sie können den Zugriff jederzeit beenden. Das Erstellen eines Support-Administrators erleichtert dem Support-Team die Behebung von Problemen.

Erstellen eines Support-Administrators

Verfahren

1. Klicken Sie auf der Seite Support-Administratoren auf Support-Benutzer hinzufügen.
2. Klicken Sie zur Bestätigung auf **Benutzer erstellen**.

Mit diesem Schritt wird eine E-Mail an das für die Geräteverwaltung zuständige Service-Support-Team gesendet.

> Beachten Sie, dass das Feld Anzeigename so lange „deaktiviert“ (disabled) anzeigt, bis ein Mitglied des Support-Teams das neue Benutzerkonto aktiviert.Der neue Anzeigename hat das folgende Format:

Support-[zufällige ID]-[Benutzername]@[Unternehmen].com

Sobald Sie einen Support-Administrator erstellt haben und Administration > Support-Administratoren auswählen, werden Sie direkt zur Liste mit den vorhandenen Support-Administratoren weitergeleitet. Wenn Sie weitere Support-Benutzer erstellen möchten, gehen Sie daher direkt zurück zu Schritt 2.

> Neu erstellte Support-Administrator-Konten sind standardmäßig schreibgeschützt. Benutzerdefinierte Rollen werden nicht automatisch zugewiesen, was dazu beiträgt, das Risiko unbeabsichtigter Konfigurationsänderungen zu reduzieren. Ein Administrator kann Rollen und Berechtigungen nach Bedarf später hinzufügen.

Benutzerverlauf anzeigen

Klicken Sie auf der Seite **Support-Administratoren** auf **Benutzerverlauf**, um die früheren Anmeldungen der Support-Administratoren anzuzeigen. Die Verfügbarkeit der Anmelde-Verlaufsdaten auf der Seite für Support-Administratoren ist auf die letzten 90 Tage beschränkt.

Sperre des Zugriffs für einen Support-Administrator

Verfahren

1. Klicken Sie auf der Seite Support-Administratoren auf den Link Löschen rechts neben dem Benutzerkonto, das Sie entfernen möchten.
2. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Benutzer entfernen**, um den Vorgang zu bestätigen.

Vorübergehende Sperre des Zugriffs für einen Support-Administrator

Klicken Sie auf der Seite Support-Administratoren auf den Link Deaktivieren rechts neben dem Benutzerkonto, das Sie entfernen möchten.

12.1.8. Administrator > Benachrichtigung zur Systemnutzung

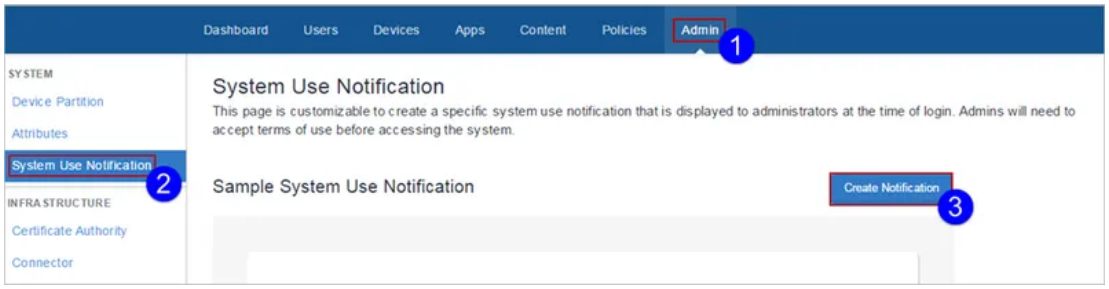
Lizenz: Silver

Erstellen Sie mit der Benachrichtigungsfunktion eine kundenspezifische Benachrichtigung zur Systemnutzung, die den Administratoren bei der Anmeldung angezeigt wird und von den Administratoren eine Bestätigung der Nutzungsbedingen fordert, bevor diese auf das System zugreifen dürfen.

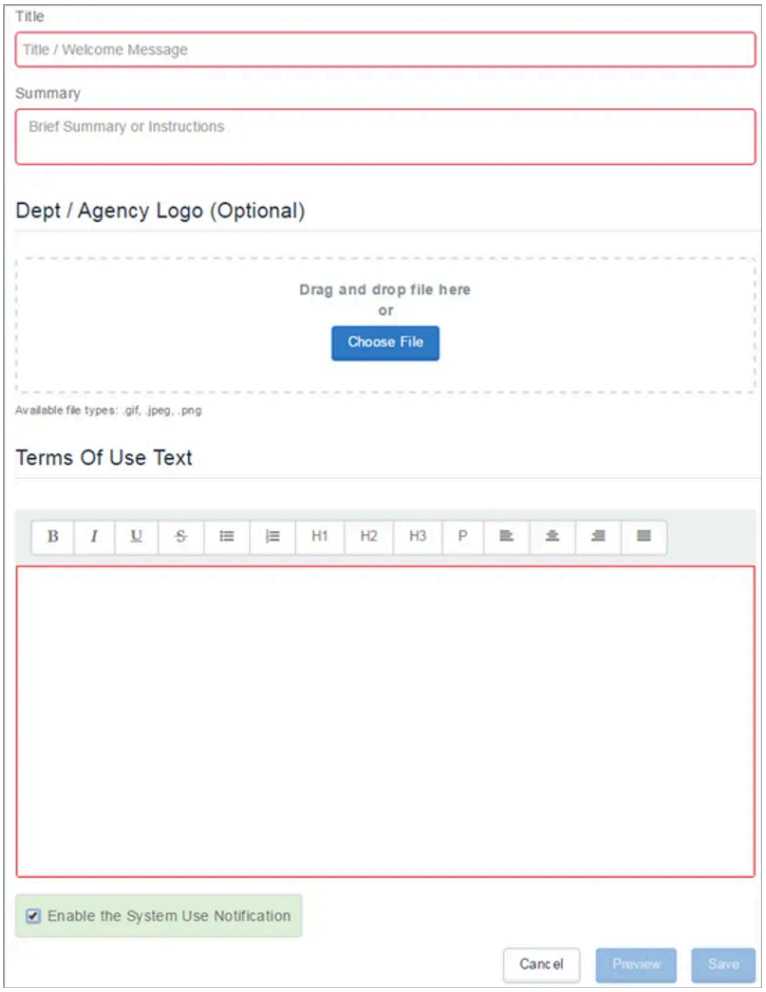
Erstellen einer System-Nutzungsbenachrichtigung

Verfahren

1. Wählen Sie **Administrator > Benachrichtigung zur Systemnutzung**.
2. Klicken Sie auf **Benachrichtigung erstellen**.



Die Seite mit den Details der Benachrichtigung zur Systemnutzung wird angezeigt.



Geben Sie einen Titel in dem Feld **Titel** ein.

4. Geben Sie eine Zusammenfassung oder Anweisungen in dem Feld **Zusammenfassung** ein.
5. Wählen Sie bei Bedarf ein Logo aus.
6. Geben Sie Nutzungsbedingungen als Text in dem Textfeld **Nutzungsbedingungen** ein. Diesen Text muss der Administrator bei der Anmeldung akzeptieren.
7. Klicken Sie in das Kontrollkästchen Benachrichtigung zur Systemnutzung aktivieren, um die Benachrichtigung zu aktivieren.
8. Klicken Sie auf **Vorschau,** um die Benachrichtigung zur Systemnutzung in der Vorschau anzuzeigen.
9. Klicken Sie auf **Speichern** wenn Sie mit der Benachrichtigung zur Systemnutzung zufrieden sind.

12.2. Infrastruktur

Dieser Abschnitt enthält die folgenden Themen:

- Zugriff
- App-Listen
- Audit-Protokolle exportieren
- Zertifikatsverwaltung
- SCEP-Konfiguration für externe Zertifizierungsstellen
- Anbieter abgeleiteter Anmeldeinformationen
- Connector
- Der Befehl httpproxy für den Connector
- Help@Work
- Infrastruktur-Identität
- Konfigurieren eines LDAP-Servers
- [Sentry]
- Aktivieren der Kerberos-Authentifizierung zwischen Ivanti Neurons for MDM und SCEP-Server

12.2.1. Zugriff

Gilt für: iOS und Android-Geräte.

MobileIron Access sichert die Unternehmensdaten und erlaubt zugleich ein problemloses produktives Benutzererlebnis auf beliebigen Geräten bzw. mit beliebigen Apps. Access definiert eine Datengrenze, die verhindert, dass Benutzer auf Unternehmens-Cloud-Dienste mit unsicheren Geräten, Apps oder Cloud-Diensten zugreifen.

Aktuelle Dokumentation

Besuchen Sie die **Produktdokumentation** und klicken Sie auf Access, um weitere Informationen über Access und die Einrichtung von Access zu erhalten. Wählen Sie das gewünschte Dokument entsprechend Ihrer Access-Version aus.

12.2.2. App-Listen

Lizenz: Silver

Sie können für die **Richtlinie zulässiger Apps** Listen mit benötigten, Whitelist- und Blacklist-Apps erstellen und mit diesen Listen Aktionen definieren, die ausgeführt werden, wenn die installierten Apps eines Geräts die Anforderungen in den App-Listen nicht erfüllen. Einmal erstellte App-Listen können Sie nicht mehr bearbeiten, weil die **Richtlinien zulässiger Apps** auf die App-Listen Bezug nehmen können. Sie können deshalb App-Listen auch nicht löschen, wenn eine Richtlinie für zulässige Apps darauf verweist.

Erstellen von App-Listen

Verfahren

1. Klicken Sie auf **Admin > Infrastruktur > App-Listen**.
2. Klicken Sie auf **Neue Liste erstellen**.
3. Geben Sie bei **App-Listenname** einen Namen für die Liste ein.
4. Wählen Sie die Art der Liste aus: **Whitelist**, **Blacklist** oder **Erforderlich**.
5. Wählen Sie im Abschnitt **Apps hinzufügen** den App-Typ aus: **App Store**, **OS X Store**, **Google Play** oder **App-Katalog**.
6. Geben Sie Suchkriterien ein, um die Auswahl einzuschränken.
7. Wählen Sie die Apps mit den Kontrollkästchen aus. Sie können mehrere Suchen durchführen und mehr als ein Kontrollkästchen aktivieren.
8. Klicken Sie auf die Registerkarte **Apps anzeigen**, um die bisher ausgewählten Apps in einer Liste anzuzeigen.
   Klicken Sie auf **Speichern**.

Sie können diese Liste dann verwenden, um die Richtlinie für **zulässige Apps** zu konfigurieren.

Wenn Sie die Seite **App-Listen** nicht sehen können, kann es sein, dass Sie nicht über die erforderlichen Berechtigungen verfügen. Sie brauchen eine der folgenden **Rollen**:

- Systemverwaltung
- System schreibgeschützt

12.2.3. Audit-Protokolle exportieren

Der Export von Audit-Protokollen ist eine Funktion, mit der Sie alle Audit-Protokoll-Informationen exportieren und auf einen bestimmten Server hochladen können. Der Server sollte über den Standard-Port zugänglich sein. Die Benutzer können die Einstellungen für den Audit-Protokoll-Export so konfigurieren, dass Archive mit Audit-Protokollen täglich automatisch auf einen bestimmten Server hochgeladen werden.

> Der Export von Audit-Protokollen wird auf Linux- und Windows-basierten SFTP-Servern unterstützt.

Konfiguration der Einstellungen zum Export der Audit-Protokolle:

1. Wählen Sie dazu **Administration > Audit-Protokoll**. Die Seite **Audit-Protokoll** wird angezeigt.
2. Klicken Sie auf der Seite **Audit-Protokolle** auf **ON**, um den Export der Audit-Protokolle zu aktivieren.
3. Aktualisieren Sie im Abschnitt **Exportieren** die folgenden Felder:

Funktion	Beschreibung
Exportformat	Wählen Sie eines der folgenden Formate für den Export der Audit-Protokolldaten aus: • **JSON** • **CEF** (Common Event Format) Die CEF-Protokollnachricht enthält folgende Standardwerte: ◦ Version : CEF-Formatversionsnummer v25 ist die aktuell unterstützte Version. ◦ Geräteanbieter: Ivanti Inc ◦ Geräteprodukt: Ivanti Neurons for MDM ◦ Geräteversion: Letzte Cloudversion zum Zeitpunkt der Entstehung des Ereignisses ◦ Klassen-ID des Geräteereignisses: Eine Entitäts-ID, die pro Protokoll eineindeutig ist. ◦ Name: Entitätsname und Entitätsaktion pro Protokoll. Beispiel: Konfigurationseinstellungen für eine Promotionsverteilung erstellen. ◦ Schweregrad: Definiert die Bedeutung des Ereignisses. Beispiel: Niedrig. Die CEF-Protokollnachricht enthält außerdem Erweiterungsfelder mit folgenden Schlüsselwertpaaren: ◦ CS1 & CS1Label: Audit-Protokoll-Metadaten wie CreatedAt, entityType, entityName und actionType. ◦ CS2 & CS2Label: Informationen über den Akteur. ◦ CS3 & CS3Label: vor dem Aktionsstatus. ◦ CS4 & CS4Label: nach dem Aktionsstatus. Wenn bei einem CEF-Export eines der Felder (beispielsweise die Schlüssel in CS3 oder CS4) die definierten Einschränkungen verletzen, wird der Istwert durch den Text "Value for this Key exceeds mapped dictionary key allowed length" ersetzt.
[Server]	Geben Sie den Namen des Servers für den Export des Audit-Protokolls ein.
Benutzer	Geben Sie den Benutzernamen für die Anwendung auf dem Server ein.
Passwort	Geben Sie das Anmeldepasswort für den Server ein.
Serverpfad	Geben Sie den Pfad zum Server ein und stellen Sie sicher, dass der angegebene Pfad auf dem Server existiert. Beispiel: /Users/Test/Export.
Schlüsselaustausch-Algorithmus	Wählen Sie die Liste der wichtigsten Schlüsselaustausch-Algorithmen für den Export des Audit-Protokolls für die ausgehende SFTP-Konfiguration. Die folgenden Schlüsselaustausch-Algorithmen sind standardmäßig ausgewählt: • **diffie-hellman-group-exchange-sha1** • **diffie-hellman-group14-sha1** • **curve25519-sha256** • **diffie-hellman-group-exchange-sha256** (standardmäßig ausgewählt)
Verschlüsselungsschlüssel	Wählen Sie die Liste der Verschlüsselungs-Chiffren für den Export des Audit-Protokolls für die ausgehende SFTP-Konfiguration. Die folgenden Verschlüsselungs-Chiffren sind standardmäßig ausgewählt: • **aes128-ctr**

Funktion	Beschreibung
	• **aes192-ctr** • **aes256-ctr** (standardmäßig ausgewählt)
HMAC	Wählen Sie die Liste der HMAC-Algorithmen für den Export des Audit-Protokolls für die ausgehende SFTP-Konfiguration. • **hmac-sha1 (standardmäßig ausgewählt)** • **hmac-sha2-256** • **hmac-sha2-512**

Die oben erwähnten Felder sind schreibgeschützt, wenn sie bereits konfiguriert sind. Zur Bearbeitung der konfigurierten Felder klicken Sie auf die Schaltfläche **Bearbeiten**. Wenn der Administrator den SFTP-Export bereits konfiguriert hatte, sind nach dem Upgrade alle Schlüsselalgorithmen ausgewählt.

Klicken Sie auf **Verbindung testen und speichern**, um die Serververbindung zu testen und die Exportkonfiguration für die Audit-Protokolle zu speichern.

Die archivierten Audit-Protokoll-Dateien stehen in einer ZIP-Datei im JSON-Format zur Verfügung.

Überprüfen Sie die Konfigurationseinstellungen in allen Feldern, bevor Sie die Einstellungen für den Export des Audit-Protokolls speichern. Wenn einer der eingegebenen Feldwerte ungültig ist, wird eine Fehlermeldung angezeigt.

Audit-Protokolle für die Vornahme und Aufhebung der Geräteregistrierung in Bereichen aktivieren

Wenn aktiviert, wird das Verschieben von Geräten zwischen Bereichen protokolliert, einschließlich der Ereignisse, die durch die Geräteregistrierung, Gerätelöschung und Bereichsaktualisierungen oder -löschungen ausgelöst werden. Space-Administratoren können betroffene Geräte identifizieren, Protokolle nach Space und Aktivitätstyp filtern und Auditdatensätze in CSV exportieren.

12.2.4. Zertifikatsverwaltung

Lizenz: Silver

Die Authentifizierung per Zertifikat ist eine effektive Methode zur Sicherung Ihrer Mobilgeräte. Zertifikate sind sicherer als Passwörter und ermöglichen Ihnen die Verwendung eines einzigen Berechtigungsnachweises, um VPNs, drahtlose Netzwerke, E-Mails usw. zu schützen. Wenn Ihr Unternehmen über Zugang zu einer externen Zertifikatsstelle verfügt, können Sie über einen Connector darauf zugreifen. Wenn Ihr Unternehmen keinen Zugriff auf eine Zertifizierungsstelle hat, können Sie die Ivanti Neurons for MDM als Zertifizierungsstelle verwenden. Das Produkt kann auch als ZwischenZertifikatsstelle für andere Zertifikatsautoritäten verwendet werden. Die von Ivanti Neurons for MDM ausgestellten Zertifikate werden als selbstsignierte Zertifikate bezeichnet.

- SHA-1-Zertifikate werden bei der Erstellung der Identitätszertifikate abgelehnt. Sie können andere Algorithmen auswählen. Bei der Aktualisierung der Zertifikate kann der gleiche SHA-1-Algorithmus verwendet werden, wenn die älteren Zertifikate SHA-1 verwenden. Wenn die älteren Zertifikate einen stärkeren Algorithmus als SHA-1 verwenden, ist eine Umschaltung auf SHA-1 nicht möglich.
- Wählen Sie bei der Konfiguration der lokalen bzw. externen Zertifizierungsstelle die Option **Cache-Identitäten in der** Ivanti Neurons for MDM, um die Zertifikate in der Ivanti Neurons for MDM zu speichern. Löschen Sie den Cache, um Zertifikate nach Bedarf zu generieren.
- Zertifikate werden implizit neu ausgestellt.
- Zur Verbesserung der Systemeffizienz werden die Zertifikate für die vom Administrator erstellten Konfigurationen offline mit einer First In First Out (FIFO)-Warteschlange erstellt. Während die Konfigurationen offline generiert werden, wird als Konfigurationsstatus **Zertifikat-Generierung läuft** in der Spalte **Status** der Registerkarte **Konfigurationen** auf der Seite **Gerätedetails** angezeigt. Sobald die Zertifikate generiert sind, erhalten die Konfigurationen den Status **Laufende Installation** und werden per Push zusammen mit den Zertifikaten automatisch durch eine erzwungene Anmeldung auf die Geräte übertragen.
- Alle Zertifikate der Zertifizierungsstelle, einschließlich der von der DigiCert PKI-Plattform oder den externen GlobalSign-Zertifizierungsstellen signierten Zertifikate, werden zurückgezogen, wenn ein Gerät außer Dienst gestellt oder gelöscht wird oder Zertifikate neu generiert werden.

Als Administrator können Sie Cloud-Zertifikate für die Smartcard-Anmeldung und benutzerdefinierte Objekt-IDs (OIDs) erstellen. Sie können Zertifikate für die folgenden Authentifizierungsoptionen erzeugen:

  - Client-Authentifizierung - standardmäßig aktiviert
  - IPSEC - optional, kann vom Administrator aktiviert werden
  - Smartcard-Anmeldung - optional, der Administrator kann diese aktivieren.
  - Benutzerdefinierte OIDs - optional, Administrator kann diese aktivieren.

Diese Funktion ist nur für die folgenden Zertifizierungsstellen verfügbar:

  - Lokale Zertifikatsautorität
  - Zwischengeschaltete Zertifizierungsstelle
  - Externe Zertifizierungsstelle - Konfiguration der Anwendungsrichtlinien der CA-Vorlage im NDES-Server zur Unterstützung von IPSEC, Smartcard-Anmeldung und benutzerdefinierten OIDs

> In den Modi Geräte-Admin, App-Station oder anderen Modi außerhalb von Android Enterprise wird die Zertifikatverwaltung auf Samsung-Gräten, die Samsung-APIs verwenden, nicht unterstützt. Es wird geraten, basierend auf der Empfehlung von Samsung, den Wechsel zu Android Keystore zu prüfen.

Weitere Informationen dazu finden Sie unter Zertifikatskonfiguration.

Verbinden mit einer On-Premise-SCEP-Zertifizierungsstelle

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Installieren und konfigurieren Sie einen Connector **(Admin > Connector)**. Weitere Informationen finden Sie unter Connector.
3. Wechseln Sie zu **Admin** > **Infrastruktur** > **Zertifikatsverwaltung**.
4. Klicken Sie unter dem Abschnitt **Zertifizierungsstelle** auf **Hinzufügen**.
5. Wählen Sie **On-Premise-SCEP-Zertifizierungsstelle hinzufügen** aus und klicken Sie auf **Fortfahren**.
6. Geben Sie einen beschreibenden Namen für die Konfiguration ein.
7. Wählen Sie eine der folgenden Zertifizierungsstellen-Arten aus:
   - Microsoft
   - EJBCA
   - Allgemeiner SCEP-Server
     Die Option „Allgemeiner SCEP-Server“ kann mit den meisten SCEP-Servern verwendet werden, die über ein statisches Challenge-Passwort verfügen.

Füllen Sie das angezeigte Formular aus.

9. Klicken Sie auf **Fertig**.

Externe Zertifizierungsstelle erstellen

Wählen Sie diese Option aus, wenn Sie die Zertifikatsstelle eines Drittanbieters verwenden wollen.

Verfahren

1. Klicken Sie auf der Seite **Zertifikatsverwaltung** unter dem Abschnitt **Zertifizierungsstelle** auf **Hinzufügen**.
2. Klicken Sie auf der Seite „Zertifizierungsstelle hinzufügen“ unter „Externe Zertifizierungsstelle erstellen“ auf **Fortfahren**.
3. Wählen Sie GlobalSign oder die DigiCert PKI-Plattform als externe Zertifizierungsstelle.
4. Füllen Sie die restlichen Felder in dem angezeigten Formular aus.
5. Klicken Sie auf **Fertig**.

Zertifikat der eigenständigen Zertifizierungsstelle anzeigen

Sie können die Details eines Zertifikats einsehen und das Zwischen-/alternative Root-Zertifikat für diese Zertifizierungsstelle hochladen, um die vorhandene gespeicherte Kopie zu ersetzen.

Verfahren

1. Klicken Sie unter der **Zertifizierungsstelle** auf der Seite **Zertifikatsverwaltung** neben der externen Zertifizierungsstelle auf **Aktionen** und dann auf **Zertifikat anzeigen**. Das Fenster **Zertifikat anzeigen** wird eingeblendet.
2. Klicken Sie im Fenster **Zertifikat anzeigen** auf **Zertifikat hochladen**. Das Fenster **Zertifikat hochladen: Externe CA** wird angezeigt.
3. Klicken Sie auf die Option **Datei auswählen**, um die Zertifikat-Datei auszuwählen, die Sie hochladen wollen.
4. Klicken Sie auf **Fertig**.

Eine Zwischenzertifizierungsstelle erstellen

- Wenn Sie ein Zertifikat benötigen, erstellen Sie eine Zertifikatsanforderung (CSR) und senden Sie diese an die Zeichnungsberechtigung. Wenn Sie das Zertifikat von der Zeichnungsberechtigung erhalten, laden Sie es hoch.
- Wenn Sie das erforderliche Zertifikat bereits besitzen, laden Sie es hoch.

CSR erstellen (Zertifikatsanforderung)

Verfahren

1. Klicken Sie unter dem Abschnitt **Zertifizierungsstelle** auf der Seite **Zertifikatsverwaltung** auf **Hinzufügen**
2. Klicken Sie auf der Seite „Zertifizierungsstelle hinzufügen“ unter „Zwischenzertifizierungsstelle erstellen“ auf die Option **CSR erstellen**.
3. Füllen Sie das angezeigte Formular aus.
4. Klicken Sie auf **Erstellen**.
5. Kopieren Sie den Inhalt zwischen BEGIN CERTIFICATE REQUEST und END CERTIFICATE REQUEST zu einer Textdatei.
6. Laden Sie die Textdatei in die Zertifizierungsstelle hoch.
7. Klicken Sie auf **Fertig**.

Hochladen des signierten Zertifikats

Wenn Sie das signierte Zertifikat von der Zertifizierungsstelle erhalten haben, laden Sie es hoch.

Verfahren

1. Unter dem Abschnitt **Z** auf der Seite **Zertifikatsverwaltung** finden Sie den Eintrag für den von Ihnen erstellten CSR.
2. Wählen Sie in dem Abschnitt **Aktionen > Neu signiertes Zertifikat hochladen**.
3. Klicken Sie auf **Datei auswählen**.
4. Wählen Sie das neue signierte Zertifikat.
5. Klicken Sie auf **Fertig**.

Hochladen eines bestehenden Zertifikats

In diesem Thema wird beschrieben, wie Sie ein signiertes Zertifikat hochladen.

Verfahren

1. Klicken Sie unter dem Abschnitt **Zertifizierungsstelle** auf der Seite **Zertifikatsverwaltung** auf **Hinzufügen**.
2. Klicken Sie auf der Seite „Zertifizierungsstelle hinzufügen“ unter „Zwischenzertifizierungsstelle erstellen“ auf die Option **Vorhandene Identität hochladen**.

3. Geben Sie im Feld **Name** einen Namen für das Zertifikat ein, der es von anderen Zertifikaten unterscheidet.
4. Klicken Sie auf **Hochladen**.
5. Wählen Sie das Zertifikat aus.
6. Geben Sie das Passwort für das Zertifikat ein.
7. Klicken Sie auf **Hochladen**.

Zertifikat der eigenständigen Zertifizierungsstelle anzeigen

Sie können die Details eines Zertifikats anzeigen sowie die CRL-URL (für die Zertifikat-Rücknahmeliste) der Zertifizierungsstelle laden.

Verfahren

1. Klicken Sie auf der Seite **Zertifizierungsstelle** neben der Zertifizierungsstelle auf **Aktionen** und dann auf **Zertifikat anzeigen**.
   Das Fenster **Zertifikat anzeigen** wird eingeblendet.
2. In dem Fenster **Zertifikat anzeigen** können Sie die URL in dem Feld **CRL URL** sehen.
3. Klicken Sie auf **Kopieren**, um die URL in die Zwischenablage zu kopieren und in eine andere Anwendung einzufügen. Mit dieser URL können Sie Office 365 so konfigurieren, dass von der Zertifizierungsstelle ausgestellte Zertifikate akzeptiert werden.

Eine eigenständige Zertifizierungstelle erstellen

Wählen Sie diese Option, wenn Sie eine neue komplett eigenständige (lokale und selbst signierte) Zertifizierungsstelle erstellen wollen.

Verfahren

1. Klicken Sie unter dem Abschnitt **Zertifizierungsstelle** auf der Seite **Zertifikatsverwaltung** auf **Hinzufügen**.
2. Klicken Sie auf der Seite „Zertifizierungsstelle hinzufügen“ unter „Eigenständige Zertifizierungsstelle erstellen“ auf **Weiter**.
3. Füllen Sie das angezeigte Formular aus.
4. Klicken Sie auf **Erstellen**.

Ablaufbenachrichtigung der eigenständigen Zertifizierungsstelle

Die Ablaufbenachrichtigung der eigenständigen (lokalen) Zertifizierungsstelle ist jetzt als Tooltip in der Spalte **ABLAUFDATUM** sichtbar, wenn weniger als 30 Tage bis zum Ablaufdatum des Zertifikats verbleiben.

Wenn das Ablaufdatum weniger als 365 Tage beträgt, kann diese Information zusätzlich zur gesendeten Benachrichtigung unter **Dashboards** > **Meldungen** angezeigt werden. Wählen Sie **Ablauf** als Filter aus.

Konfigurieren der Ablaufdauer des von der eigenständigen Zertifizierungsstelle ausgestellten Zertifikats

Sie können die Ablaufdauer der eigenständigen (lokalen) Zertifizierungsstelle konfigurieren.

Verfahren

1. Klicken Sie unter dem Abschnitt **Zertifizierungsstelle** auf der Seite **Zertifikatsverwaltung** neben der eigenständigen Zertifizierungsstelle auf **Aktionen**.
2. Klicken Sie auf **Bearbeiten**.
   Das Fenster **Zertifizierungsstelle bearbeiten** wird angezeigt.
3. Geben Sie in dem Abschnitt Client-Zertifikatvorlage in dem Feld **Zertifikatgültigkeit** die neue Ablaufdauer in Tagen ein.
4. Klicken Sie auf **Speichern**.

Sie können Benachrichtigungen und E-Mails (wenn optional aktiviert) erhalten, wenn die von einer lokalen Zertifizierungsstelle ausgestellten Zertifikate demnächst ablaufen oder bereits abgelaufen sind.

- Benachrichtigung an den Tagen des Zertifikatsablaufs - Benachrichtigungen werden in vordefinierten Intervallen während eines Zertifikatsablauf-Zeitfensters generiert. Die erste Benachrichtigung erfolgt 365 Tage vor Ablauf, gefolgt von weiteren Benachrichtigungen 180 Tage, 60 Tage, 45 Tage und 7 Tage vor Ablauf. Sie erhalten diese Benachrichtigung solange, bis Sie das Zertifikat ersetzen. Wechseln Sie dazu zu **Admin > Zertifikatsverwaltung > Aktionen > Neues signiertes Zertifikat hochladen**.
- Benachrichtigung über das abgelaufene Zertifikat - Sie erhalten eine Benachrichtigung, wenn das Zertifikat abläuft. Sie müssen das Zertifikat ersetzen, um den normalen Betrieb wieder aufzunehmen.
- Benachrichtigung, wenn ein neues gültiges Zertifikat hochgeladen wird - Die Benachrichtigung wird gesendet, sobald das neue signierte Zertifikat hochgeladen wird.

Anzeige eines Zertifikats der eigenständigen Zertifizierungsstelle

Sie können die Details eines Zertifikats anzeigen und die CRL-URL (für die Zertifikatsperrliste) der lokalen Zertifizierungsstelle abrufen.

Verfahren

1. Klicken Sie auf der Seite Zertifikatsverwaltung unter dem Abschnitt Zertifizierungsstelle neben der lokalen Zertifizierungsstelle auf Aktionen und dann auf Zertifikat anzeigen. Das Fenster **Zertifikat anzeigen** wird eingeblendet.
2. In dem Fenster **Zertifikat anzeigen** können Sie die URL in dem Feld **CRL URL** sehen.
3. Klicken Sie auf **Kopieren**, um die URL in die Zwischenablage zu kopieren und in eine andere Anwendung einzufügen. Mit dieser URL können Sie Office 365 so konfigurieren, dass durch die lokale Zertifizierungsstelle ausgestellte Zertifikate akzeptiert werden.

CRL-Nutzungsdauer einer Zertifizierungsstelle anzeigen

Sie können die Nutzungsdauer der CRL einer lokalen oder mittleren Zertifizierungsstelle anzeigen und bearbeiten.

Verfahren

1. Klicken Sie auf der Seite Zertifikatsverwaltung unter dem Abschnitt Zertifizierungsstelle neben der lokalen Zertifizierungsstelle auf Aktionen und dann auf Bearbeiten. Das Fenster **Zertifizierungsstelle bearbeiten** wird angezeigt.
2. Im Fenster **Zertifizierungsstelle bearbeiten** können Sie die CRL-Nutzungsdauer anzeigen. Der minimale Standardwert beträgt 24 Stunden. Der mögliche Höchstwert sind 10950 Stunden.
3. Bearbeiten Sie die CRL-Nutzungsdauer und klicken Sie auf **Speichern**.

Cloud-Zertifikatsstelle erstellen

Wählen Sie diese Option aus, wenn Sie die Zertifikatsstelle eines Drittanbieters verwenden wollen.

Verfahren

1. Wechseln Sie zu **Admin** > **Infrastruktur** > **Zertifikatsverwaltung**.
2. Klicken Sie auf der Seite **Zertifikatsverwaltung** im Abschnitt **Zertifizierungsstelle** auf **Hinzufügen**.
3. Klicken Sie auf der Seite **Zertifizierungsstelle hinzufügen** unter **Verbinden mit einer öffentlichen vertrauenswürdigen Cloud-Zertifizierungsstelle** auf **Weiter**.
4. Geben Sie einen Namen in das Feld **Name** ein.
5. Wählen Sie eine der folgenden Cloud-Zertifizierungsstellen aus:

- **Atos IDnomic CMS**
- **DigiCert One PKI-Plattform**
- **DigiCert PKI-Plattform**
- **Entrust**
- **GlobalSign**

6. Geben Sie die Basis-URL ein und laden Sie die Zertifikatsdaten hoch.
7. Klicken Sie auf **Fertig**.

Erweiterte Suche in Zertifikaten verwenden

Mit der Option „Erweiterte Suche“ können Sie mit Regeln nach ausgestellten Zertifikaten suchen, um Zertifikate nach bestimmten Kriterien zu identifizieren und anzuzeigen. Diese Regeln können unter Verwendung der anwendbaren Operatoren erstellt werden, beispielsweise mit den Operatoren „beginnt mit“, „endet mit“, „enthält“, „enthält nicht“, „beginnt nicht mit“, „endet nicht mit“, „ist kleiner als „,“ ist größer als „,“ liegt im Bereich „„, „ist gleich“ und „ist nicht gleich“. Die Regeln können miteinander mit den Optionen ANY (OR) oder ALL (AND) verschachtelt werden. Die ausgestellten Zertifikate, die den Regeln entsprechen, werden unterhalb des Abschnitts angezeigt. Ab Ivanti Neurons for MDM Release 76 besitzen die Operatoren für alle Vorlagen der Zertifikatsverwaltung Standardoperatoren. Die Operatoren der folgenden Vorlagen sind in diesem Release standardisiert:

- Admin > Zertifikatsverwaltung > Ausgestellte Zertifikate > Erweiterte Suche

Erweiterte Suche in ausgestellten Zertifikaten

Verfahren

1. Klicken Sie unter dem Abschnitt **Ausgestellte Zertifikate** auf der Seite **Zertifikatsverwaltung** auf den Link **Erweiterte Suche**.
2. Klicken Sie auf **Eine**, wenn die Benutzer mindestens eine der Regeln erfüllen müssen, oder auf **Alle**, wenn das Zertifikat allen Regeln erfüllen muss.
3. Erstellen Sie eine Regel mit Suchkriterien für die folgenden Attribute:
   - **CA**
   - **Name der Konfiguration**
   - **Ablauf**
   - **Ist privater Schlüssel**
   - **BETRIEBSSYSTEM**
   - **Seriennummer**
   - **[Status]**
   - **Art der Verwendung**
   - **Benutzer**
4. (Optional): Klicken Sie auf +, um weitere Richtlinien zu erstellen.
5. (Optional) Klicken Sie auf **Speichern**, um die Abfrage zu speichern.
6. Klicken Sie auf **Suchen**. Die Liste der Benutzer, die die Suchkriterien erfüllen, wird auf der Seite angezeigt.

Erweiterte Suche in von Benutzern bereitgestellten Zertifikaten

Verfahren

1. Klicken Sie unter dem Abschnitt **Von Benutzern bereitgestellte Zertifikate** auf der Seite **Zertifikatsverwaltung** auf den Link **Erweiterte Suche**.
2. Klicken Sie auf **Eine**, wenn die Benutzer mindestens eine der Regeln erfüllen müssen, oder auf **Alle**, wenn das Zertifikat allen Regeln erfüllen muss.
3. Erstellen Sie eine Regel mit Suchkriterien für die folgenden Attribute:
   - **Zertifikatsname**
   - **Ablaufdatum**
   - **Ausgegeben durch**
   - **Hochgeladen am**
4. (Optional): Klicken Sie auf +, um weitere Richtlinien zu erstellen.
5. (Optional) Klicken Sie auf **Speichern**, um die Abfrage zu speichern.
6. Klicken Sie auf **Suchen**. Die Liste der Benutzer, die die Suchkriterien erfüllen, wird auf der Seite angezeigt.

Suchabfragen für ausgestellte Zertifikate verwenden

So zeigen Sie die Liste der gespeicherten Suchanfragen an:

Verfahren

1. Klicken Sie unter dem Abschnitt **Ausgestellte Zertifikate** auf der Seite **Zertifikatsverwaltung** auf den Link **Erweiterte Suche**.
2. Klicken Sie auf das Symbol „Ordner“. Das Fenster **Erweiterte Suche** wird angezeigt. Die Liste der erstellten Suchanfragen wird im Abschnitt **Abfrage laden** angezeigt. Folgende Details werden in diesem Abschnitt angezeigt:
   - **Abfragename** - Der Name der geladenen Abfrage.
   - **Abfrageinhalt** - Zeigt den Inhalt der Regeln an, die die Suchabfrage definieren.
   - **Aktionen** - Wählen Sie die Aktion aus, die mit der Abfrage ausgeführt werden soll.
3. Klicken Sie in der Spalte **Aktionen** auf **Abfrage laden**, um die Liste der ausgestellten Zertifikate anzuzeigen, welche die in der geladenen Abfrage definierten Kriterien erfüllen.
   Um eine geladene Abfrage zu löschen, klicken Sie auf das Löschsymbol.

> Klicken Sie auf **In CSV exportieren**, um den Inhalt des Suchergebnisberichts in einer CSV-Datei zur späteren Bezugnahme oder Analyse herunterzuladen.

Ablauffrist der ausgestellten Zertifikate anzeigen

Im Abschnitt **Ausgestellte Zertifikate** können Sie in der Spalte **Ablauf (in Tagen)** die verbleibenden Tage bis zum Ablauf des Zertifikats anzeigen, wenn der Ablauf innerhalb der nächsten 30 Tage liegt. Wenn das Zertifikat bereits in den letzten 30 Tage abgelaufen war, wird in der Spalte **Läuft ab (in Tagen)** für das Zertifikat angezeigt, wie viele Tage seit dem Ablaufdatum vergangen sind.

Weitere Informationen finden Sie unter SCEP-Konfiguration für externe Zertifizierungsstellen.

Als CSV-Datei exportieren

Sie können die Zertifikate zur späteren Verwendung in eine CSV-Datei exportieren.

Verfahren

1. Wechseln Sie auf der Seite **Zertifikatsverwaltung** zu einer der folgenden Registerkarten:
    - **Zertifikatsautorität**
    - **Ausgestellte Zertifikate**
    - **Von Benutzern bereitgestellte Zertifikate**
2. Klicken Sie auf **Als CSV-Datei exportieren**.
3. Klicken Sie auf **Herunterladen**.
4. (Optional) Klicken Sie zum Löschen des Berichts auf **Löschen**.

12.2.5. SCEP-Konfiguration für externe Zertifizierungsstellen

Diese Funktion aktiviert die Unterstützung für die Konfiguration des Simple Certificate Enrollment Protocol (SCEP) externer Zertifizierungsstellen für Geräte mit Windows 10.

> Für diese Konfiguration ist die Delegierung mit benutzerdefinierter Verteilung verfügbar. Weitere Informationen finden Sie unter *Verteilen der Konfiguration* unter **Arbeiten mit Konfigurationen**.

Externe Zertifizierungsstelle hinzufügen

Sie müssen zunächst eine externe Zertifizierungsstelle konfigurieren. Sie können sofort zum nächsten Abschnitt wechseln, wenn Sie bereits über eine externe Zertifizierungsstelle verfügen.

1. Wechseln Sie zu **Admin > Infrastruktur > Zertifikatsverwaltung**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie einen Namen für die Zertifizierungsstelle ein.
4. Wählen Sie über das Pulldown-Menü Microsoft als **Zertifizierungsstellenart** aus.
5. Geben Sie die **SCEP-URL** ein.
6. Geben Sie den **Benutzernamen** und das **Passwort** ein.
7. Geben Sie die **Challenge-URL** ein.
8. Klicken Sie auf **Speichern**.

SCEP-Konfiguration

Sie können jetzt mit der SCEP-Konfiguration fortfahren.

1. Gehen Sie zu **Konfiguration > +Hinzufügen.**
2. Klicken Sie auf das Windows-Symbol.
3. Wählen Sie Identitätszertifikat aus, um zu der Seite Identitätszertifikatskonfiguration erstellen zu wechseln.
4. Geben Sie einen Namen für die Konfiguration ein.
5. Wählen Sie aus der Liste der SCEP-Konfigurationen im Pulldown-Menü **Verteilung von Zertifikaten** die Option **Windows-Konfiguration** aus.
6. Wählen Sie die Externe Zertifizierungsstelle.
7. Geben Sie die Details der Zertifikatsverteilung ein.
    - Geben Sie den Betreff ein. Beispiel: CN=$
    - Wählen Sie die Anzahl der Wiederholungen im Pulldown-Menü **Neu versuchen** aus.
    - Wählen Sie aus dem Pulldown-Menü **Wiederholungsverzögerung** aus, wie viele Sekunden vor jedem Eintrag gewartet werden soll.
    - Wählen Sie die Schlüsselgröße aus dem Pulldown-Menü Schlüssellänge aus.
    - Wählen Sie mindestens eine Zertifikatnutzungsoption aus.
    - Geben Sie die Zeitdauer in dem Feld **Gültigkeit** und im Pulldown-Menü ein.

- Geben Sie das Symbol für die Zertifizierungsstelle ein.
- Wechseln Sie zur SCEP-Challenge-URL, kopieren Sie den CA-Fingerabdruck und fügen Sie ihn hier ein oder klicken Sie auf **Von Zertifikat erstellen...**. um das Zertifikat hochzuladen, über das der CA-Fingerabdruck erstellt werden kann.
  Wählen Sie mindestens einen Hashing-Algorithmus unter **Hash-Algorithmus-Familie** aus.

8. Klicken Sie auf **Weiter**.

12.2.6. Anbieter abgeleiteter Anmeldeinformationen

Auf der Seite „Anbieter abgeleiteter Anmeldeinformationen“ können Sie die Liste der Anbieter abgeleiteter Anmeldeinformationen anzeigen, die für die Zertifikatsverteilung verwendet werden. Sie können angeben, welche Anbieter abgeleiteter Anmeldeinformationen als Standard festgelegt werden sollen und weitere benutzerdefinierte Anbieter abgeleiteter Anmeldeinformationen hinzufügen, die Sie verwenden.

Einen Anbieter abgeleiteter Anmeldeinformationen als Standard festlegen:

1. Gehen Sie zu **Admin > Anbieter abgeleiteter Anmeldeinformationen**. Folgende Anbieter abgeleiteter Anmeldeinformationen sind auf der Seite aufgeführt.
    - **Entrust**
    - **Intercede**
    - **Purebred**
2. Klicken Sie für den Anbieter, den Sie als Standard festlegen möchten, in der Spalte Aktionen auf Als Standard festlegen.Falls aktiviert, wird das Häkchensymbol unter der Spalte **Standardanbieter** für den Anbieter angezeigt, um darauf hinzuweisen, dass es sich um den Standardanbieter der Anmeldeinformationen handelt.

Einen benutzerdefinierten Anbieter abgeleiteter Anmeldeinformationen hinzufügen:

1. Gehen Sie zu **Administration > Anbieter abgeleiteter Anmeldeinformationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie den Namen des Anbieters abgeleiteter Anmeldeinformationen in das Textfeld unter der Spalte **Name** ein.
4. Klicken Sie auf **Speichern**.
   Sobald dieser benutzerdefinierte Anbieter abgeleiteter Berechtigungsnachweise hinzugefügt ist, ist er als Option unter dem Feld **Marke** verfügbar und kann ausgewählt werden, wenn die Verteilung abgeleiteter Anmeldeinformationen unter **Identitätszertifikat** konfiguriert wird.

Klicken Sie in der Spalte **Aktionen** auf **Löschen**, um einen Anbieter abgeleiteter Anmeldeinformationen zu löschen.

> Sie können den Anbieter abgeleiteter Anmeldeinformationen nicht löschen, wenn er als Standard eingestellt ist.

12.2.7. Connector

Lizenz: Silver

Über den Cloud Connector erhält Ihr Cloud-Dienst Zugang zu Unternehmensressourcen, beispielsweise den LDAP-Server oder eine Zertifizierungsstelle (CA). Konfigurieren Sie einen Connector für jede Ressource, auf die Sie zugreifen möchten.

Wenn Sie Microsoft Active Directory oder einen bei Amazon Web Services (AWS) gehosteten LDAP-Server verwenden, können Sie den Cloud Connector in AWS hosten. Ein LAN-Connector ist nicht erforderlich.

Der Connector aktualisiert sich automatisch auf die neueste Version der Software.

Das neueste Cloud Connector-Installationshandbuch finden Sie unter **https://help.ivanti.com/#106** unter dem Suchbegriff "Connector".

Connector-Hostingoptionen

Sie können den Cloud Connector in Ihrem Rechenzentrum im LAN oder bei Amazon Web Services (AWS) hosten:

- Hosten Sie den Connector im AWS, wenn Sie eine Microsoft AD oder eine selbstverwaltete AD in AWS hosten. In diesem Fall benötigen Sie keinen Connector im lokalen Netzwerk.
- Um auf die Ressourcen im lokalen Netzwerk zuzugreifen, beispielsweise auf einen LDAP-Server oder eine Zertifizierungsstelle, konfigurieren Sie den Connector für das LAN.

Connector auf AWS hosten

Kunden können den Connector in AWS für folgende Microsoft Active Directory-Optionen für AWS hosten:

- AWS-Verzeichnisdienst für Microsoft Active Directory
- Vom Kunden verwaltete Microsoft Active Directory in Amazon VPC

Weitere Informationen zum AWS Directory Service für Microsoft Active Directory finden Sie unter **https://aws.amazon.com/directoryservice**. Weitere Informationen zum Hosting von Microsoft Windows Server und Microsoft Active Directory in einem Amazon VPC finden Sie in der AWS-Dokumentation. Der Cloud Connector unterstützt Windows-Server 2012, 2012 R2, 2015.

Einrichten der Ivanti Neurons for MDM Connector-AMI in AWS

So richten der Ivanti Neurons for MDM Connector-AMI ein:

1. Melden Sie sich bei AWS mit Administrator-Anmeldeinformationen an.
2. Wählen Sie auf der Seite der AWS-Services **EC2** unter **Compute**.
3. Erweitern Sie Images und wählen Sie AMIs im linken Fensterbereich.
4. Wählen Sie Öffentliche Images aus der Dropdown-Liste im rechten Fensterbereich.
5. Machen Sie den Ivanti Neurons for MDM Connector ausfindig, indem Sie Stichwörter wie "mobileiron-kocab" eingeben.
6. Wählen Sie die neueste Version des Connectors aus der Liste aus und klicken Sie auf **Start**.
7. Folgen Sie den Anweisungen zum Installieren des Connectors im Abschnitt "Bereitstellen des MobileIron Connectors in AWS" im *Cloud Connector-Installationshandbuch* unter https://help.ivanti.com/mi/help/en_us/cld/*<version>*/inst/default.htm, wobei *version*

die Version des Cloud Connectors ist, die Sie installieren möchten. Für die Version 74 des Cloud Connectors finden Sie die Anleitung beispielsweise unter https://help.ivanti.com/mi/help/en_us/cld/**74**/inst/default.htm.

Connector im eigenen Unternehmen hosten

Um den Cloud Connector intern in Ihrem Rechenzentrum zu hosten, klicken Sie auf **Connector herunterladen** und richten Sie den Cloud Connector ein. Extrahieren Sie den Inhalt des heruntergeladenen Pakets und folgen Sie den Installationsanweisungen der im Paket enthaltenen Cloud Connector-Installationsanleitung.

Zugriff auf das Connector-Protokoll

Sie können die Connector-Protokolle über den Dienst kocab aufrufen, um mit dem Connector zusammenhängende Probleme zu beseitigen. Sie müssen dazu eine Rolle als Systemmanager oder System-Read-Only-Benutzer haben.

1. Gehen Sie zu **Administrator > Connector**, um die Seite „Connector“ anzuzeigen.
   Die Connectoren-Schnittstelle zeigt den Connector-Status (aktiviert oder deaktiviert), die Bezeichnung des Connectors, die Verbindung (verbunden oder nicht verbunden), die Versionsnummer, die Protokollebene und die Aktionen an (Connector deaktivieren oder entfernen).
2. Wählen Sie mit dem Pulldown-Menü **Protokollierungsebene** eine Ebene aus.
   Die verfügbaren Protokollebenen werden in dem Pulldown-Menü in aufsteigender Reihenfolge angezeigt:
   - Fehler
   - Warnung
   - [Info]
   - Debuggen
   - Rückverfolgen

Info-Niveau ist die Standardeinstellung für die Protokollebene. Wenn Sie eine andere Protokollierungsstufe wählen, erscheint ein rotierendes Synchronisationssymbol, das anzeigt, dass Informationen auf der von Ihnen gewählten Protokollierungsebene erhoben werden. Die Protokollebene wird nach einer Stunde wieder auf die Ebene "Info" zurückgesetzt. Die höchste Protokollebenen-Einstellung ist die Ebene "Rückverfolgen". Mit dieser Ebene erfassen Sie alle Mitteilungen aller anderen Ebenen. Das Synchronisationssymbol wird so lange angezeigt, wie die Anfrage läuft.

3. Fahren Sie bei Bedarf mit der Maus über das Synchronisationssymbol, um das Abbruchsymbol zu sehen. Klicken Sie auf das Abbruchsymbol, um die Protokollebenen-Änderung abzubrechen.
4. Bewegen Sie den Mauszeiger über dem Anforderungsymbol, um die Anforderungsinformationen anzuzeigen. Klicken Sie auf das Anforderungssymbol, um die Dateien aus dem aktuellen Protokollordner als ZIP-Datei anzufordern.
   Die Protokolldateien werden in diesem Fall zu einer ZIP-Datei zusammengefasst. Wenn eine neue Anforderung erfolgt, wird die ZIP-Datei der letzten Anforderung gelöscht.
5. Bewegen Sie bei Bedarf den Mauszeiger über das Symbol Request und es wird zum Abbruchsymbol . Klicken Sie auf das Abbruchsymbol, um die Anforderung zu stoppen.
   Wenn eine Anforderung vor dem Abschluss abgebrochen wird, wird das Download-Symbol nicht angezeigt, da die vorherige log.zip-Datei vom Server gelöscht wurde.Die Original-Protokolldateien des Connectors stehen immer noch für eine Anforderung zur Verfügung.
6. Klicken Sie auf das Download-Symbol, wenn die Anforderung abgeschlossen ist, um die Protokoll-ZIP-Datei mit den während der letzten Anforderung erfassten Protokolldateien herunterzuladen.
   Der Protokolldateiname hat das Format: kocab.log. Der Name der zip-Datei, die heruntergeladen wird, besteht aus dem Servernamen, der Verbindungsversion und einem Zeitstempel mit Tag, Monat, Jahr und Uhrzeit des Tages in folgendem Format:

<Connector_Hostname>_<Connector_Version>_<TimeStamp>.zip.Die archivierte ZIP-Datei hat folgendes Format: kocab.yyyy-mm-dd.0.log.gz.

7. Sie können optional auch über das Pull-Down-Menü **Aktionen** den Connector deaktivieren oder entfernen.

Wenn Sie die Seite **Connector** nicht sehen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie brauchen eine der folgenden **Rollen**:

- Systemverwaltung
- System schreibgeschützt

Weitere Informationen finden Sie unter **httproxy-Befehl für Connector verwenden**.

12.2.8. Der Befehl httpproxy für den Connector

Es wurde ein neuer klish shell-Befehl erstellt, damit Sie die Connector-Konfiguration für Ihre Installation in der Cloud leichter bearbeiten können. Ändern Sie mit diesem Befehl die Anmeldeinformationen und andere Parameter zur Konfiguration des Konnektors.

Der httpproxy-Befehl steht in diesem Release mit folgenden Anforderungen zur Verfügung:

- klish shell

So konfigurieren Sie den Konnektor:

1. Melden Sie sich bei der klish-shell an.
2. Geben Sie '?' ein, um eine Liste der verfügbaren KLISH-Befehle abzurufen.
3. Geben Sie **httpproxy** ein, um den aktuellen Wert der folgenden Parameter anzuzeigen:
    1. aktiviert
    2. Schema
    3. Server
    4. authtype
    5. [username]
    6. Passwort
4. Geben Sie **httpproxy ?** ein, um eine Liste der für httpproxy verfügbaren Befehle anzuzeigen.
    1. authtype – Setzt den Authentifizierungstyp des http-Proxy auf NONE, BASIC oder NTLM
    2. disable – deaktiviert den http-Proxy.
    3. enable – aktiviert den http-Proxy.
    4. host – definiert den Host des http-Proxy – dies muss ein FQDN oder eine IP mit dem Kürzel http bzw. https sein.
    5. password – definiert das Authentifizierungspasswort des http-Proxy-Servers.
    6. port – definiert den Port des Http-Proxy-Servers.
    7. scheme – definiert das Schema des Http-Proxy-Servers. Dieser muss entweder vom Typ http oder https sein.
    8. show - zeigt die aktuellen Einstellungen des Http-Proxy-Servers.
    9. username – definiert den Authentifizierungsbenutzernamen des Http-Proxy.
5. Verwenden Sie die oben aufgelisteten Befehle zur Konfiguration Ihrer Connector-Instanz.

12.2.9. Help@Work

Lizenz: Platinum

Unterstützt von: Android- und iOS-Geräte, die von Ivanti Neurons for MDM unterstützt werden.

Mit Help@Work for Android/iOS können Sie Benutzer von Android-Geräten und iOS-Geräten aus der Ferne unterstützen. Help@Work für Android/iOS basiert auf der TeamViewer QuickSupport App. Sie benötigen ein TeamViewer-Konto, um Help@Work for Android/iOS zu verwenden. Wenn Sie noch kein Konto haben, besuchen Sie bitte teamviewer.com und informieren sich dort über die Details.

Help@Work verändert die Benutzererfahrung mit dem Helpdesk für iOS 11.0+ und Android-Geräte. Die Benutzer können per Tastendruck Hilfe anfordern und den Bildschirm einem Helpdesk-Mitarbeiter teilen. Die Benutzer vergeuden somit keine wertvolle Zeit mit Versuchen, das Problem verbal zu beschreiben, und die IT-Mitarbeiter können Probleme effizienter beseitigen. Dies wird für reine MAM iOS-Geräte nicht unterstützt.

> TeamViewer wird auf Android-Geräten im Kiosk-Modus unterstützt.

> Die TeamViewer-Startbefehle werden gelöscht, sobald die App beendet oder das Gerät neu gestartet wird.

> Wenn auf Android-Geräten die Teamviewer QuickSupport-App nicht installiert ist, wird der Benutzer aufgefordert, die App herunterzuladen. Auf iOS-Geräten muss die App per Push über den App Catalog übertragen werden oder, wenn sie bereits auf dem Gerät installiert ist, in eine verwaltete App umgewandelt werden.

> Die Teamviewer QuickSupport App sollte im Vordergrund erscheinen, damit die Sitzung für die Anwendung übernommen werden kann. Für den unbeaufsichtigten Modus ist die TeamViewer-Host-App erforderlich.

> Die Version der Desktop-Anwendung, die der Administrator installiert, sollte mit der auf dem Client-Gerät installierten Quicksupport-Version kompatibel sein, um Remote-Sitzungen zu unterstützen.

Help@Work für Androidoder iOS einrichten

Nachfolgend finden Sie einmalige Einrichtungsschritte für das Branding und die Verteilung von Help@Work für Androidoder iOS:

1. Gehen Sie zur Registerkarte **Administrator**.
2. Klicken Sie unter Infrastruktur auf **Help@Work**.
3. Help@Work benötigt TeamViewer. Aktivieren Sie im Abschnitt "TeamViewer aktivieren" entweder die Option **TeamViewer - Beaufsichtigt** oder **TeamViewer - Unbeaufsichtigt (nur Android)**, indem Sie auf die Schaltfläche **Jetzt aktivieren** klicken.
4. Lesen Sie die TeamViewer-Lizenzvereinbarung und klicken Sie zum Fortfahren auf Zustimmen.Ihre Unternehmenslizenz ist jetzt aktiviert. Damit werden Kunden bei TeamViewer erkannt, sodass ein Zugriff eingeräumt wird.

> Die Option **Aktivierung entfernen** wird nach der Aktivierung von TeamViewer verfügbar. Wenn Sie im Abschnitt **TeamViewer aktivieren** auf **Aktivierung entfernen** klicken, wird das Fenster **Entfernen der Aktivierung bestätigen** auf dem Bildschirm angezeigt. Klicken Sie auf **Aktivierung entfernen**, um die TeamViewer-Aktivierung zu entfernen. Damit wird die Help@Work-Funktionalität von allen unterstützten Geräten entfernt. Sie können TeamViewer jedoch über ein vorhandenes Konto oder zu einem späteren Zeitpunkt über ein anderes Konto aktivieren.

> Wenn Sie das Konto **TeamViewer** im unbeaufsichtigten Modus löschen möchten, müssen Sie die Bereitstellung der zugehörigen Geräte aufheben, für die der Modus "Unbeaufsichtigt" aktiviert ist. Um die Bereitstellung der zugehörigen Geräte aufzuheben, müssen Sie die Verteilung der App **TeamViewer** auf den betreffenden Geräten rückgängig machen und das Einchecken erzwingen. Stellen Sie sicher, dass die TeamViewer-App tatsächlich von allen Geräten gelöscht wurde und löschen Sie dann die Bindung des Kontos über die Admin-Konsole.

Übertragen Sie die TeamViewer-App per Push an die Benutzer, die Fernsitzungen starten sollen. Verwenden Sie den Standard-Arbeitsablauf für die App-Verteilung. Dies gilt speziell für die Modi **Beaufsichtigt** und **Unbeaufsichtigt**. Möchte der Administrator das Gerät kontrollieren, muss das Universal Add-on oder das OEM-/modellspezifische Add-on von TeamViewer ebenfalls an das Gerät verteilt werden. Anweisungen finden Sie unter **App-Konfiguration**.

Fernsitzung mit Help@Work für Androidoder iOS starten

Eine typische Help@Work für Androidoder iOS-Sitzung beginnt mit einem Endbenutzer, der Hilfe benötigt.

Help@Work-Sitzung mit dem Gerät des Benutzers starten:

1. Wechseln Sie in Ivanti Neurons for MDM zu **Geräte**.
2. Klicken Sie auf der Seite mit der Geräteliste auf das Gerät, das Unterstützung benötigt.
3. Klicken Sie im Menü „Aktionen“ für Android-Geräte auf **TeamViewer Remote Control starten** oder auf für iOS-Geräte **Remote Display starten**. Es werden zwei Optionen angezeigt:
   - Beaufsichtigter Modus (Standardeinstellung) – Dazu muss die App **TeamViewer Quick Support** auf dem Zielgerät installiert und zur Positivliste hinzugefügt werden.
   - Unbeaufsichtigter Modus (nur auf Android verfügbar) – Dazu muss die App **TeamViewer Host** auf dem Zielgerät installiert und zur Positivliste hinzugefügt werden.

> Falls Sie die Hostnamen zur Whitelist hinzufügen oder die Sicherheitsrichtlinie für Inhalte überschreiben möchten, wenden Sie sich bitte an das Support-Team.

> Die Option für den unbeaufsichtigten Modus ist auch mit dem Kiosk-Modus kompatibel. Die Aktivierung sollte über die TeamViewer-Integrationsseite erfolgen. Für die unbeaufsichtigte Remotesteuerung sind die TeamViewer-Host-App auf dem Gerät, eine einmalige Aktivierung auf einem Gerät und eine MI-Add-on-Lizenz erforderlich. Bei der einmaligen Aktivierung wird die Eingabeaufforderung für die Berechtigung angezeigt, wenn die TeamViewer-Host-App installiert ist und zum ersten Mal gestartet wird. Der Administrator kann nach der Installation optional die TeamViewer-App automatisch starten (Einstellungen der Konfiguration für verwaltete Apps). Die Anzahl der Lizenzen wird basierend auf der Verteilung der TeamViewer-Host-App berechnet. Wird die TeamViewer-Host-App an ein Gerät verteilt, wird eine Lizenz für eine unbeaufsichtigte Remote-Hostsitzung verbraucht. Zusätzlich zur TeamViewer-Host-App werden möglicherweise andere Add-on-Apps benötigt, die im Kiosk-Modus oder im gemeinsam genutzten Kiosk-Modus zugänglich sein sollten. Je nach Gerätemodell und Hersteller können andere Add-ons erforderlich sein.

> Google Pixel-Geräte behalten diese Zustimmung nicht sitzungsübergreifend bei. Die Berechtigung muss für jede Sitzung neu erteilt werden.

Verfügt der Administrator über ein gültiges TeamViewer-Token, startet der Desktop-Client mit einer Support-Sitzung zum Gerät. Andernfalls muss sich der Administrator mit TeamViewer anmelden und Rechte erteilen.

Um eine Sitzung zur Entfernung von Apps schnell einzuleiten, können sich Administratoren zuvor bei der Desktop-Anwendung anmelden.

Installieren des TeamViewer

Installieren Sie TeamViewer auf dem Desktop, um aus der Ferne auf die Geräte Ihrer Benutzer zuzugreifen und diese zu unterstützen. So installieren Sie TeamViewer:

1. Laden Sie das Installationspaket für die Vollversion von TeamViewer für Mac, Windows oder Android hier herunter: **https://www.teamviewer.com/en/download/**
2. Starten Sie das TeamViewer-Installationsprogramm.
3. Wählen Sie Basisinstallation.
4. Wählen Sie Verwendung in Unternehmen/kommerzielle Nutzung.
5. Klicken Sie auf Akzeptieren – Fertigstellen.

Anfordern eines TeamViewer-Kontos

Sie müssen ein TeamViewer-Konto haben, um mit TeamViewer Support anzubieten. So erhalten Sie ein TeamViewer-Konto:

1. Gehen Sie zu **https://login.teamviewer.com/**.
2. Geben Sie Benutzername und Passwort ein.
3. Klicken Sie auf **Registrieren**.
4. Nutzen Sie das in Schritt 2 eingegebene E-Mail-Konto, um die Aktivierungs-E-Mail für Ihr TeamViewer-Konto zu erhalten.
5. Führen Sie die Anweisungen in der E-Mail aus, um Ihr TeamViewer-Konto zu aktivieren.

Bestätigung der TeamViewer-Sitzungs-ID.

TeamViewer erstellt eine Sitzungs-ID, wenn eine Verbindung zwischen dem Computer des Administrators und dem Mobilgerät des Benutzers hergestellt wird.

1. Wenn die Session-ID generiert ist, übergibt Ivanti Neurons for MDM sie über die verwaltete App-Konfiguration an die TeamViewer QuickSupport-App, die wiederum mit dieser Session-ID den TeamViewer-Client auf dem Gerät aufruft. Bei iOS läuft die Sitzungs-ID nach 30 Minuten ab.
2. Der Benutzer wird aufgefordert, die EULA des TeamViewers zu akzeptieren.

12.2.10. Infrastruktur-Identität

Dieser Abschnitt enthält die folgenden Themen:

12.2.10.1. Identity Provider konfigurieren

Lizenz: Silver

Konfigurieren Sie einen Identitätsanbieter (IdP) zur Authentifizierung von Benutzern, die Geräte in der Cloud registrieren bzw. das Administratorportal oder das Selbstbedienungsportal aufrufen wollen. Es ist ein internes, LDAP-kompatibles Benutzerverzeichnis erforderlich. Ivanti Neurons for MDM funktioniert mit jedem mit SAML 2.0 kompatiblen IdP. Mit Ivanti Neurons for MDM funktionieren nachweislich Microsoft Entra ID-Authentifizierung (Entra ID), Microsoft ADFS (Active Directory Federation Services), Okta, OneLogin, PingOne und PingFederate von Ping Identity.

Wenn Sie zuvor SAML auth/IdP eingerichtet haben, wird die SAML-Authentifizierung sowohl für die Geräteregistrierung als auch für die Portalauthentifizierung verwendet. Jetzt gibt es eine Umschalttaste zur Auswahl der verschiedene Authentifizierungsmethoden für den Zugang zum Admin-Portal und zur Geräteregistrierung. Die Bypassfunktion ist nur für die Registrierung von Geräten verwendbar.

Während der Geräteregistrierung kann der Administrator die Option "Identitätsanbieter" umgehen und dem Benutzer die Option zum Authentifizieren über eine PIN anstelle der Authentifizierung über die Seite des Identitätsanbieters zur Verfügung stellen.

Übersicht

- Wenn Sie Microsoft AD oder ein anderes LDAP-Verzeichnis im LAN verwenden, müssen Sie den Connector konfigurieren, um eine Verbindung mit der Cloud aufzubauen und Benutzer zu importieren. Konfigurieren Sie den Connector bzw. **LDAP**, sofern noch nicht geschehen.
- Wenn Sie einen Identitätsanbieter ergänzen, ändert sich die Benutzerauthentifizierung automatisch von LDAP auf IdP.
- Es ist immer nur ein IdP-Anbieter zulässig.
- Falls Ihr IdP-Eintritt nicht erreichbar sein sollte, können Sie mit dem Konto für den Cloud Tenant Admin (TA) auf dieses Verwaltungsportal zugreifen und die Fehler beheben. Der Mandanten-Administrator (TA) ist ein lokales Konto, für das keine externe Authentifizierung erforderlich ist. Das TA-Konto wird erstellt, sobald Ihre Cloud bereitgestellt ist und Informationen über den technischen Ansprechpartner Ihres Unternehmens usw. vorliegen. Wenn Sie die TA-Kontoinformationen nicht zur Hand haben, wenden Sie sich an Ihren Support-Ansprechpartner.
- Ivanti Neurons for MDM unterstützt Microsoft Entra ID (Entra ID) zum Authentifizieren von Benutzern bei der Registrierung von Windows 10-Geräten.

> Definieren Sie die Authentifizierungsart für Ihre LDAP-Benutzer mit den von Ihrem IdP-Anbieter zur Verfügung gestellten Tools. Das Authentifizierungsschema Ihres IdP hat Vorrang vor den Cloud-Einstellungen. Die Cloud-Authentifizierungseinstellungen finden Sie hier: **Benutzer > Benutzereinstellungen > Geräteregistrierungseinstellung > Geräteregistrierung Authentifizierungstyp**.

- Apple Device Enrollment und Geräteregistrierungen mit dem Konfigurator benötigen zur Benutzerauthentifizierung kein IdP.
- Zum Konfigurieren eines Identitätsanbieters für die Registrierung von Apple Business Manager iOS- und macOS-Geräten müssen Sie die Einstellung **Benutzerdefinierte Registrierung aktivieren** und die Einstellung für die zugehörige **von Ivanti gehostete Webseite** aktivieren. Diese befinden sich unter **Admin > Apple > Geräteregistrierung >** *Geräteregistrierungsprofil bearbeiten*. Weitere Informationen finden Sie unter **Geräteregistrierung**:



IdP-Einrichtungstypen

Die Seite Cloud-Identität führt Sie durch die Konfiguration folgender IdP-Provider:

- **Ivanti Neurons for MDM IdP-Einrichtung** - Unterstützte Ivanti Neurons for MDM-Identitätsanbieter sind Entra ID AD, OneLogin, Okta und PingOne.
- IDP-Setup für LAN – Unterstützte LAN-IDP-Anbieter sind ADFS 3.0, PingFederate 8.2.1 und PingFederate 8.1.3.
- Generisches IdP Setup – Dies ist ein generischer Konfigurationspfad, den Sie verwenden können, wenn Sie nicht mit Microsoft ADFS, Okta, OneLogin oder PingFederate arbeiten.

Konfigurieren eines Identitätsanbieters (IdP)

Verfahren

1. Gehen Sie zu **Admin** > **Identität** > **SAML-Authentifizierung**.
2. Klicken Sie auf einen Setup-Typ für einen Identitätsanbieter:
    - **Ivanti Neurons for MDM – IdP-Setup**
    - **IdP-Setup im lokalen Netzwerk**
    - **Generischer IdP – Setup**
3. Wählen Sie einen betreffenden IdP aus. Wenn Sie **Generischer IdP – Setup** in Schritt 3 ausgewählt haben, überspringen Sie diesen Schritt und fahren mit Schritt 5 fort.
4. Folgen Sie den Anweisungen auf dem Bildschirm, die für Ihren gewählten IdP angezeigt werden.
5. Klicken Sie auf **Fertig**.

> Administratoren dürfen bis zu 2 Stunden nach ihrer ersten Authentifizierung beim IdP ein Single Sign-On durchführen.

Einrichten von eventuell erforderlichen Aufgaben

Abhängig vom gewählten IdP werden Sie durch die folgenden verknüpften Seiten und Schritte geführt:

IdP	Verfahren
• Entra ID • Okta • OneLogin • PingOne	• Erzeugung eines Schlüssels, den Sie für Ihren IdP hochladen. • Anmeldung bei Ihrem IdP und Hochladen des erzeugen Schlüssels. • Meta-Datendatei von Ihrem IdP exportieren und in die Cloud importieren.
• ADSF 3.0 • PingFederate 8.2.1 • PingFederate 8.1.3	• Laden Sie die Metadatendatei von Ivanti Neurons for MDM herunter. • Konfiguration einer „vertrauenswürdigen Seite“ in ADFS oder einer „SP-Verbindung“ bei PingFederate und Import der Metadaten-Datei der Cloud. • Meta-Datendatei von Ihrem IdP exportieren und in die Cloud importieren
• Generischer IdP	1. Laden Sie die Metadatendatei von Ivanti Neurons for MDM herunter. 2. Folgen Sie den Anweisungen Ihres IdP-Anbieters, um Ihren IdP-Server/IdP-Dienst für die Kommunikation mit dem Cloud-Dienst als "Service-Anbieter" zu konfigurieren. Dies kann Folgendes beinhalten: 1. Metadatendatei aus Schritt 1 für den Identitätsanbieter hochladen. Diese Konfigurationsdatei enthält wichtige Informationen, mit denen die Cloud als SAML-2.0-Dienstanbieter mit Ihrem SAML-2.0 Identitätsanbieter kommunizieren kann. Die Standard-URLs für SAML 2.0, Zertifikate und Einstellungen sind in der Metadatendatei enthalten. Ivanti Neurons for MDM erwartet einen mit SAML 2.0 kompatiblen IdP, der in der Lage ist, eine XML-Metadatendatei zu importieren und zu verarbeiten, die von einem Dienstanbieter exportiert wurde. 2. Konfigurieren Sie Ihren IdP so, dass Sie RSA-SHA-1 zur Signierung von SAML-Authentifizierungsanfragen verwenden können. Informationen über das Signatur-Zertifikat zur Verifizierung der Authentifizierungsanfragen sind in der Metadatendatei enthalten, die Sie in Schritt 1 heruntergeladen haben. 3. Konfigurieren Sie Ihren IdP so, dass ein Benutzername in den SAML-Antworten enthalten ist, die an Ivanti Neurons for MDM gesendet werden. Geben Sie den Benutzernamen in dem Element [Name ID]der SAML-Antwort vom IdP an. Exportieren Sie eine Metadatendatei von Ihrem IdP und importieren Sie sie in Ivanti Neurons for MDM.

IdP	Verfahren
	3. (Optional) – Benutzernamen in die SAML-Authentifizierungsanfrage einfügen: Dient zum Einfügen des Benutzernamens des sich authentifizierenden Benutzers in die Authentifizierungsanfrage und zum Entfernen zusätzlicher Benutzereingaben bei der Authentifizierung mit einem IdP. Wenn Sie diese Option aktivieren, kann es zu Authentifizierungsfehlern kommen. Wenn Sie sich sicher in Bezug auf die IdP-Valdierung sind, wählen Sie die Option **Ich verstehe die Auswirkung dieser Änderung** aus und setzen Sie die Einstellung **Benutzernamen in die SAML-Authentifizierungsanfrage einfügen** auf **EIN**. Ivanti Access ist ein validierter IdP für diese Einstellung.

Zulassen, dass Benutzer die IdP-Authentifizierung umgehen

Wenn ein IdP oder eine Verbindung mit der Cloud ausfällt und eine Fehlerbehebung durch die Cloud erforderlich ist, benötigen manche Administratoren die Möglichkeit, sich in der Cloud ohne externe Systeme wie LDAP oder IdP zur Authentifizierung anzumelden. Nur lokale Benutzer mit Systemadministratorrollen können die IdP-Authentifizierung umgehen.

Erstellen Sie eine Liste mit lokalen Benutzern, um die IdP-Authentifizierung zu umgehen.

Verfahren

1. Klicken Sie auf **Admin > Identität**.
2. Klicken Sie im Abschnitt „Lokale Benutzer mit Umgehung der IdP-Authentifizierung“ auf **+Benutzer hinzufügen**.
3. Wählen Sie aus der Liste, die nur lokale Benutzer mit Systemadministratorrollen anzeigt, einige Benutzer aus.
4. Klicken Sie auf **Speichern**.

> Klicken Sie zur Entfernung eines Benutzers aus der Liste der lokalen Benutzer, die die IdP-Authentifizierung umgehen dürfen, auf das Lösch-Symbol neben dem Eintrag, den Sie löschen wollen.

Wenn Sie die Seite „Identität“ nicht sehen können, haben Sie möglicherweise nicht die erforderlichen Berechtigungen. Sie brauchen eine der folgenden **Rollen**:

- Systemverwaltung
- System schreibgeschützt

12.2.10.2. Benutzerbereitstellung mit SCIM

Dieser Abschnitt enthält die folgenden Themen:

- Benutzerbereitstellung
- Generieren eines Tokens über Ivanti Neurons for MDM
- Ändern des Tokenstatus
- Anzeigen des Tokenstatus über das Audit-Protokoll
- Konfigurieren von Attributen in der SCIM-Benutzerbereitstellung

Benutzerbereitstellung

Die Benutzerbereitstellung verwendet das SCIM-Protokoll, um einen Identitätsanbieter (IdP) mit Ivanti Neurons for MDM zu synchronisieren, und ermöglicht eine selektive Benutzer- und Gruppensynchronisierung. Die Benutzerbereitstellung verwendet das SCIM-Protokoll, um die vom IdP stammenden Benutzer- und Gruppenobjekte automatisch zu erstellen und mit Ivanti Neurons for MDM zu aktualisieren. Genau wie die aktuelle Integration in Entra ID und Okta, ist der Prozess zum Bereitstellen von Benutzern und Gruppen automatisiert. Falls Änderungen am Benutzer oder an der Gruppe im IdP vorgenommen werden, werden diese auch in Ivanti Neurons for MDM abgebildet.

> Der Benutzername eines über SCIM bereitgestellten Benutzers kann im Identitätsanbieter (IdP) umbenannt werden, wenn der Benutzername in Ivanti Neurons for MDM eindeutig ist.

> SCIM-Benutzer und -Gruppen können jetzt anhand ihrer jeweiligen externen IDs gesucht werden.

Generieren eines Tokens über Ivanti Neurons for MDM

Um mit der Benutzerbereitstellung für einen IdP zu starten, generieren Sie ein Token und die Ziel-URL über Ivanti Neurons for MDM.

> Speichern Sie den Token und die Ziel-URL.

> Es können maximal zwei Token gleichzeitig erzeugt werden.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Gehen Sie zu **Admin** > **Identität** > **Benutzerbereitstellung**.
3. Wählen Sie den Identitätsanbieter (IdP) aus der Dropdownliste aus.
4. Klicken Sie auf **Generieren**, um ein neues Token zu erstellen. Eine Benachrichtigungsmeldung wird angezeigt. Klicken Sie auf **Generieren**. Es wird eine neue Seite geöffnet, auf der die Details zum Token und die Ziel-SCIM-URL enthalten sind.
5. Klicken Sie auf **Kopieren** und kopieren Sie entweder das Token oder die SCIM-URL.
6. Aktualisieren Sie die Seite. Die Seite **Benutzerbereitstellung** zeigt die Tabelle "Tokenstatus" an.

Ändern des Tokenstatus

Sie können den Status eines vorhandenen Tokens ändern.

Verfahren

1. Klicken Sie auf das Dropdownmenü **Auswählen** der Seite **Entra ID-Benutzerbereitstellung**.
2. Klicken Sie auf **Auswählen**, und nehmen Sie die folgenden Änderungen am Token vor:
    - **Auf aktiv festgelegt**
    - **Auf inaktiv festgelegt**
    - **Verlängern**
    - **Entfernen**

Anzeigen des Tokenstatus über das Audit-Protokoll

Sie können die Protokolle zu den auf einem SCIM-Token erfolgten Aktionen oder Ereignissen über den Abschnitt "Audit-Protokolle" anzeigen. Der SCIM-Token kann einen der folgenden Status aufweisen:

- SCIM-Token erstellt – Ein SCIM-Token wurde erstellt.
- SCIM-Token aktiviert – Ein SCIM-Token wurde aktiviert.
- SCIM-Token deaktiviert – Ein SCIM-Token wurde deaktiviert.
- SCIM-Token verlängert – Ein SCIM-Token wurde verlängert.
- SCIM-Token gelöscht – Ein SCIM-Token wurde gelöscht.

Die Spalte DETAILS führt auch den Namen des SCIM-Anbieters (IDP) auf, z. B. Azure, Okta usw. Dies vereinfacht die Kommunikation mit Ivanti Neurons for MDM.

Konfigurieren von Attributen in der SCIM-Benutzerbereitstellung

In diesem Abschnitt wird beschrieben, wie Sie benutzerdefinierte Attribute und Unternehmensattribute für einen IdP während der Benutzerbereitstellung erstellen.

Zuordnen von Attributen

Nachdem die Verbindung hergestellt wurde, können Sie die Attribute zwischen dem IdP und Ivanti Neurons for MDM zuordnen. Ivanti Neurons for MDM unterstützt die folgenden Benutzerattribute:

Hauptattribute

- ID
- userName
- displayname
- Aktiv
- givenName
- familyName
- E-Mails

> Für Entra ID IdP wird ein externer IdP unterstützt.

Liste der Attribute mit zulässiger Aktualisierung

- userName
- Anzeigename
- E-Mails
- givenName
- familyName
- Aktiv
- urn:ietf:params:scim:schemas:extension:ivanti:2.0:User
- urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Benutzerdefinierte Attribute

Schema – urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<CustomAttribute123Name>

Unternehmensattribut

Derzeit wird nur das Abteilungsattribut unterstützt.

Schema – urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department

12.2.10.2.1. Benutzerbereitstellung für Entra ID IdP

Dieser Abschnitt enthält die folgenden Themen:

- Herstellen einer Verbindung mit Ivanti Neurons for MDM
- Zugewiesene Benutzer und Gruppen bereitstellen
- Alle Benutzer und Gruppen bereitstellen
- Überprüfen einer zugewiesenen Benutzerbereitstellung
- Benutzerbereitstellung für Entra ID IdP
- Einstellungen bearbeiten
- Konfigurieren von benutzerdefinierten Attributen und Unternehmensattributen
- Migrationsüberlegungen – Entra ID-Benutzerquelle zu Benutzerbereitstellung SCIM
- Migrationsüberlegungen – LDAP zu Benutzerbereitstellung SCIM
- Wichtige Hinweise – SCIM

Herstellen einer Verbindung mit Ivanti Neurons for MDM

Nachdem Sie die Benutzer und Gruppen in Ihrer Entra ID-Unternehmensanwendung erstellt haben, können Sie die Verbindung zwischen Entra ID und Ivanti Neurons for MDM herstellen.

Verfahren

1. Melden Sie sich beim Entra ID-Portal an.
2. Wechseln Sie zu **"Unternehmensanwendung"** und klicken Sie auf **"Eigene Anwendung erstellen"**. Das Fenster zum Erstellen einer eigenen Anwendung wird angezeigt.
3. Geben Sie den Namen der App an (**Standard: Non-gallery**) und klicken Sie auf **"Erstellen".** Zum Beistiel Ivanti Neurons for MDM-Benutzerbereitstellung.
4. Gehen Sie zu **Bereitstellung** > **Bereitstellung bearbeiten** > **Administratoranmeldedaten**.
5. Kopieren Sie die Ziel-SCIM-URL aus dem Ivanti Neurons for MDM-Administrationsportal und fügen Sie sie in das Feld **Mandanten-URL** im Entra ID-Portal ein.
6. Kopieren Sie das Token aus Ivanti Neurons for MDM und fügen Sie es in das Feld **Geheimes Token** im Entra ID-Portal ein.
7. Führen Sie eine der folgenden Schritte aus:
    - Wählen Sie **"Nur zugewiesene Benutzer und Gruppen synchronisieren"** aus. Weitere Informationen finden Sie unter "Bereitstellen zugewiesener Benutzer und Gruppen".
    - Wählen Sie **"Alle Benutzer und Gruppen synchronisieren"** aus. Weitere Informationen finden Sie unter "Bereitstellen aller Benutzer und Gruppen".

    > Wählen Sie zum Migrieren von Benutzern die Option "Alle Benutzer und Gruppen synchronisieren" aus.

Klicken Sie auf **Verbindung testen**. Ein Popup-Fenster mit einem grünen Häkchen bestätigt die Verbindung.

9. Klicken Sie auf **Speichern**.
10. Erweitern Sie den Eintrag **Zuordnungen** auf der Seite **Bereitstellung** im Entra ID-Portal.

11. Klicken Sie auf **Entra ID-Benutzer bereitstellen**. Die Seite "Attributzuordnung" wird geöffnet.
12. Klicken Sie auf **Löschen**, um die nicht unterstützten Attribute zu löschen.

Zugewiesene Benutzer und Gruppen bereitstellen

Nachdem die Verbindung zwischen Entra ID und Ivanti Neurons for MDM hergestellt wurde, können Sie Benutzer oder Gruppen bereitstellen.

> Beim Bereitstellen von Gruppen fügt Entra ID keine Mitglieder von verschachtelten Gruppen zur ausgewählten Gruppe hinzu. Entra ID fügt beim Synchronisieren nur unmittelbare Mitglieder und Gruppennamen zur Gruppe hinzu, und keine Mitglieder der Untergruppe.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Wechseln Sie in der Anwendung zu **"Benutzer und Gruppen"** und klicken Sie auf **"+Benutzer/Gruppe hinzufügen"**. Die Seite „Zuweisung hinzufügen" wird geöffnet.
3. Suchen Sie über das **Suchfeld** nach dem Benutzer oder der Gruppe. Klicken Sie auf **"Auswählen"** und dann auf **"Zuweisen"**. Die Seite „Benutzer und Gruppen" wird geöffnet.
4. Markieren Sie das jeweilige Kontrollkästchen für den Benutzer oder die Gruppe.
5. Klicken Sie auf **Bereitstellung** und dann auf **Bereitstellung starten**. Die Details zur erfolgreichen Konfiguration werden angezeigt.

Alle Benutzer und Gruppen bereitstellen

Nachdem die Verbindung zwischen Entra ID und Ivanti Neurons for MDM hergestellt wurde, können Sie Benutzer oder Gruppen bereitstellen.

Verfahren

- Klicken Sie auf **Bereitstellung** und dann auf **Bereitstellung starten**. Eine Seite mit den Details der erfolgreichen Bereitstellung wird geöffnet und der Benutzer wird in der Cloud bereitgestellt.

Überprüfen einer zugewiesenen Benutzerbereitstellung

Nachdem ein zugewiesener Benutzer auf dem Entra ID-Portal bereitgestellt wurde, überprüfen Sie die Bereitstellung auf dem Ivanti Neurons for MDM-Administrationsportal.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Gehen Sie zur Registerkarte **Benutzer** im Hauptmenü. Der bereitgestellte Benutzer wird in der Liste der Benutzer auf dieser Seite aufgeführt.

> Der Bereitstellungsvorgang kann bis zu einer Stunde dauern.

Überprüfen der Gruppenbereitstellung

Nach der Bereitstellung einer Gruppe im Entra ID-Portal sollten Sie die Bereitstellung in Ivanti Neurons for MDM überprüfen.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Wechseln Sie zur Registerkarte **Benutzer** > **Benutzergruppen**. Die bereitgestellte Gruppe wird in der Liste der Gruppen auf dieser Seite aufgeführt.

> Der Bereitstellungsvorgang kann bis zu einer Stunde dauern.

Einstellungen bearbeiten

Dieses Thema unterstützt Sie bei der Konfiguration der Entra ID-Einstellungen.

Verfahren

1. Wechseln Sie zu **Admin > Microsoft Azure > Entra ID-Benutzerbereitstellung**.
2. Klicken Sie auf **Token generieren** und kopieren Sie ihn.
3. Aktualisieren Sie die Seite. Die Seite "Entra ID-Einstellungen" wird angezeigt.
4. Klicken Sie auf **Einstellungen bearbeiten**.
5. Legen Sie **Aus Entra ID importierte Benutzer automatisch einladen** fest, um zu verwalten, ob aus Entra ID in Ivanti Neurons for MDM importierte Benutzer automatisch per E-Mail zur Registrierung eingeladen werden.
6. Stellen Sie **Verwaltete Apple-ID** ein. Diese Option ist standardmäßig deaktiviert. Klicken Sie auf den Umschalter, um die Option zu aktivieren. Die verwaltete Apple-ID kann während der Bereitstellung wie folgt eingerichtet werden:
   - **E-Mail-Adresse des Benutzers**
     - (Optional) Wählen Sie die Option "appleid-Subdomäne einschließen" aus, um Konflikte mit bestehenden Apple-IDs zu vermeiden.
   - Zuordnung zu **benutzerdefiniertem Attribut**

     > Das benutzerdefinierte Attribut sollte mit einer eindeutigen E-Mail-Adresse verbunden sein.
7. (Optional) Klicken Sie auf **Benutzerdefiniertes Attribut hinzufügen** - Definieren Sie für Ihren Verzeichnisdienst anpassbare Benutzerattribute für die Geräteverwaltung. Auf jedes Attribut kann dann mit $ in den Konfigurationsfeldern zugegriffen werden, die Variablen unterstützen. Für diese Option benötigen Sie eine konsistente Implementierung der benutzerdefinierten Attribute für alle Entra ID-Server. Wenn ein in Ihrer Implementierung enthaltener Entra ID-Server dieses Attribut nicht verwendet, funktionieren die von diesem Attribut abhängigen Optionen möglicherweise nicht wie erwartet. Die Spalte **Attributtyp** zeigt das Attribut **IDP** in der Tabelle **Benutzerdefinierte Attribute** des Abschnitts **Einstellungen bearbeiten** an.
8. Klicken Sie auf **Änderungen speichern**, nachdem Sie die Entra ID-Einstellungen geändert haben.

Konfigurieren von benutzerdefinierten Attributen und Unternehmensattributen

Verfahren

1. Wechseln Sie zu **Admin** > **Identität** > **Benutzerbereitstellung**.
2. Klicken Sie unter **Einstellungen bearbeiten** auf **+Benutzerdefiniertes Attribut hinzufügen**.
3. Geben Sie einen Namen in das Feld **Attributname** ein (z. B. custAttr1) und klicken Sie auf **Änderungen speichern**. Das Attribut wird auf der Seite **Admin** > **System** > **Attribut** aufgeführt und ist dort verfügbar. Das Attribut ist als IdP-Attribut definiert. Sie können lediglich die Löschaktion durchführen.

4. Melden Sie sich beim **Entra ID-Portal** an.
5. Wechseln Sie zu **Startseite** > **Unternehmensanwendung** und klicken Sie auf die SCIM-Anwendung.
6. Klicken Sie auf die Option **Entra ID-Benutzer bereitstellen** des Abschnitts **Zuordnungen**.
7. Markieren Sie das Kontrollkästchen **Erweiterte Optionen anzeigen**.
8. Klicken Sie auf **Attributliste für customappsso bearbeiten**.
9. Geben Sie einen neuen Eintrag für das benutzerdefinierte Attribut ein, das Sie auf der Benutzeroberfläche von Ivanti Neurons for MDM erstellt haben.
10. Fügen Sie das Schema für das benutzerdefinierte Attribut/Unternehmensattribut (Abteilung) wie folgt hinzu:
    Benutzerdefiniertes Attribut - **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<custAttr1> -** . Siehe Schritt 3.
    Unternehmensattribut – **urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department**
11. Klicken Sie auf **Änderungen speichern**.
12. Klicken Sie auf **Neue Zuordnung hinzufügen** und wählen Sie Quell- und Zielattribut aus dem Dropdownmenü aus.
13. Klicken Sie auf **OK** und dann auf **Zuordnung speichern**.
14. Wechseln Sie zu **Startseite** > **Unternehmensanwendung**. Klicken Sie auf die SCIM-Anwendung und dann auf **Benutzer und Gruppen**.
15. Klicken Sie auf den Benutzernamen. Die Seite "Profil" wird geöffnet.
16. Prüfen Sie, ob der mit dem Attribut verknüpfte Wert auf der Profilseite angezeigt wird.
17. (Optional) Klicken Sie auf die SCIM-Anwendung und dann auf Bereitstellung > Bedarfsbasierte Bereitstellung. Suchen Sie nach dem gewünschten Benutzer und klicken Sie auf Bereitstellung, um die in den vorherigen Schritten durchgeführten neuen Attributzuordnungen zu validieren.
18. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
19. Wechseln Sie zu **Benutzer** > **Benutzer** und wählen Sie den Benutzer aus.
20. Klicken Sie auf die Registerkarte **Attribute** und prüfen Sie den Attributwert. Das Attribut wird dem angegebenen Benutzer zugeordnet.

Migrationsüberlegungen – Entra ID-Benutzerquelle zu Benutzerbereitstellung SCIM

- Wenn Sie von Entra ID-Benutzerquelle zu Entra ID-Benutzerbereitstellung (SCIM) migrieren möchten, wählen Sie "Alle Benutzer und Gruppen synchronisieren" aus.
- Nachdem Benutzer und Gruppen mit einer SCIM Entra ID-Quelle aktualisiert wurden, kehren Sie zurück zur Seite "Azure-Bereitstellung" in Azure. Legen Sie mithilfe der Option "Nur zugewiesene Benutzer und Gruppen synchronisieren" die Benutzer und Gruppen fest, die von der Entra ID-Benutzerbereitstellung verwaltet werden sollen.
- Nach Abschluss der Synchronisierung können die nicht in Azure definierten Benutzer und Gruppen aus den Listen für die Ivanti Neurons for MDM-Benutzer und -Gruppen entfernt werden.
- Nach Beginn der Migration kann schreibgeschützt auf die Seite "Entra ID-Benutzerquelle" zugegriffen werden.

Migrationsüberlegungen – LDAP zu Benutzerbereitstellung SCIM

Voraussetzungen:

1. Die Option **Diesen LDAP-Server aktivieren** ist standardmäßig ausgewählt. Vor der Migration muss diese Option deaktiviert werden.

2. Erstellen Sie eine Enterprise-App in Entra ID und fügen Sie die synchronisierten LDAP-Benutzer/-Gruppen (dieselben LDAP-Benutzer/-Gruppen, die in Ivanti vorhanden sind) zur SCIM-App hinzu. Starten Sie die Bereitstellung.

Wichtige Überlegungen für die Migration von LDAP zu SCIM

- LDAP erfasst nicht alle Informationen zu synchronisierten Benutzern/Gruppen, während SCIM Benutzer-/Gruppenereignisse in Audit-Protokollen festhält.
- Für einen LDAP-Benutzer mit benutzerdefiniertem Attribut ist der Typ mit "ldap" festgelegt, während er bei SCIM "IdP" lautet. Wenn Benutzer mit benutzerdefiniertem Attribut von LDAP zu SCIM migriert werden, sollte das zugehörige benutzerdefinierte IdP-Attribut in der SCIM-App angelegt werden, damit die Benutzer migriert werden. Möchte der Benutzer das benutzerdefinierte ldap-Attribut später aktualisieren, wird der Attributwert ldap.custom nach der Migration nicht in MDM aktualisiert. Der IdP-Attributwert wird aktualisiert.
- Migrieren Sie LDAP-Benutzer, die einem oder mehreren benutzerdefinierten Attributen zugeordnet sind, speziell "ldap.custAttr1," und geben Sie dabei die Registrierung des LDAP-Geräts und der Konfiguration (Identitätszertifikat-Konfiguration) an, die via Push mit dem SAN-Typ an das Gerät übertragen wurde, der dem Wert des benutzerdefinierten LDAP-Attributs entspricht.
- Migration eines LDAP-Benutzers, dessen verwaltete Apple-ID mit einer E-Mail-Adresse verknüpft ist – Wenn der Benutzer vor der Migration von LDAP zu SCIM den Wert der verwalteten Apple-ID des LDAP-Benutzers behalten möchte, muss die Einstellung "Verwaltete Apple-ID in SCIM" aktiviert und die Einstellungen müssen gespeichert werden.
- Wenn der LDAP-Benutzer vom LDAP-Server entfernt wird, ist der Benutzer weiterhin aktiv, allerdings ist das Flag für "Keine Synchronisierung" für den betreffenden synchronisierten LDAP-Benutzer auf "wahr" gesetzt. Bei SCIM wird der Benutzerstatus deaktiviert, wenn ein bereitgestellter Benutzer gelöscht wurde.
- Sobald SAML für den Identitätsanbieter (IdP) für SCIM-Benutzer konfiguriert ist, werden alle Benutzer der verschiedenen Quellen wie "Lokal und LDAP" über SAML authentifiziert. Nur lokale Benutzer können zu einer Ausnahmeliste hinzugefügt werden, um den IdP-Authentifizierungsfluss zu umgehen. Diese Konfiguration kann auf der SAML-Seite unter **Admin** > **Identität** > **SAML** verwaltet werden.
- Nachdem SAML für die migrierten IDP (SCIM)-Benutzer konfiguriert wurde, lässt sich die Geräteregistrierung für Benutzer aus unterschiedlichen Quellen wie "Lokal und LDAP" umgehen (nicht über IDP). Dies wird unter **Benutzer** > **Benutzereinstellungen** verwaltet.
- In LDAP werden Benutzer, Gruppen und Org.-Einheiten unterstützt, während in SCIM, Benutzer und Gruppen, jedoch keine Org.-Einheiten unterstützt werden.
- Der Prozess der verschachtelten Gruppenbereitstellung wird in SCIM nicht unterstützt.

Wichtige Hinweise – SCIM

- Die E-Mail-Adresse ist ein Pflichtfeld für die Bereitstellung und Migration von Benutzern oder Mitgliedern.
- SCIM ermöglicht die einseitige Bereitstellung von Microsoft Entra ID zu Ivanti Neurons for MDM. Ivanti Neurons for MDM bietet keine Synchronisierungsoptionen. Wenn Sie eine über SCIM bereitgestellte Gruppe oder einen Benutzer aus Ivanti Neurons for MDM löschen, stellen Sie sicher, dass Sie die Gruppe bzw. den Benutzer auch aus Microsoft Entra ID entfernen.
- Sie können ein Attribut (Quelle oder Ziel) nur einmal im SCIM-Fenster für Anwendungszuordnung von Microsoft Entra ID verwenden. Ein und dieselbe Quelle kann nur einmal einem bestimmten Zielattribut zugeordnet werden.
- Inaktive Benutzer können nicht mithilfe von SCIM in Ivanti Neurons for MDM bereitgestellt oder dorthin migriert werden.
- Derzeit bietet Ivanti Neurons for MDM keine Unterstützung für die SCIM-Ereignisbenachrichtigung.
- Die Dauer der Migration oder Bereitstellung richtet sich nach der Anzahl der davon betroffenen Benutzer oder Gruppen.
- Microsoft Azure kontrolliert das Bereitstellungsintervall. Es beträgt etwa 40 Minuten.

- Bei der erneuten Bereitstellung wiederholt Microsoft Entra ID nur die fehlgeschlagenen Einträge. Sie können die Bereitstellungsprotokolle herunterladen, um zu prüfen, welche Benutzer erfolgreich über Microsoft Entra ID bereitgestellt werden konnten und welche nicht.
- Doppelte Gruppen aus unterschiedlichen Quellen sind in SCIM nicht zulässig.
- Wenn ein Benutzer via Hard-Delete aus Microsoft Entra ID gelöscht wird, wird er in Ivanti Neurons for MDM deaktiviert.
- Wenn eine bereitgestellte Benutzergruppe aus Microsoft Entra ID gelöscht wird, wird sie in Ivanti Neurons for MDM gelöscht. Alle unabhängigen Mitglieder der gelöschten Gruppe werden deaktiviert und der Gruppe "Alle Benutzer" zugeordnet.
- Wenn ein bereitgestelltes Mitglied einer bereitgestellten Gruppe via Hard-Delete aus Microsoft Entra ID gelöscht wird, wird das Mitglied in Ivanti Neurons for MDM deaktiviert, gehört jedoch weiterhin der Gruppe in Ivanti Neurons for MDM an.
- Wenn eine Attributzuordnung (Unternehmensattribut oder benutzerdefiniertes Attribut) aus einer App entfernt wird, wird der entfernte Attributwert weiterhin in Ivanti Neurons for MDM dargestellt.
- Wenn ein Benutzerattribut eines bereitgestellten Benutzers mit einem leeren Wert aktualisiert wird, wird der aktualisierte Attributwert nicht in Ivanti Neurons for MDM dargestellt.
- Wenn die Attribute FName und LName (name.formatted) während der Migration oder Aktualisierung von Microsoft Entra ID zu SCIM leer sind, schlägt die Migration bzw. die Aktualisierung fehl.
- Wenn Sie einen Benutzer in Entra ID löschen, löscht die zugehörige SCIM-API den Benutzer nicht dauerhaft. Stattdessen führt sie eine Löschung via Soft-Delete durch und ändert den Benutzerstatus von "Aktiv" zu "Inaktiv". Wenn Sie den Benutzer dauerhaft löschen möchten, melden Sie sich am Ivanti Neurons for MDM-Administrationsportal an und löschen Sie den inaktiven/deaktivierten Benutzer manuell.
- Wenn ein lokaler Benutzer bereits mit einer bestimmten Benutzer-ID in Ivanti Neurons for MDM vorhanden ist, wird ein entsprechender Benutzer mit derselben Benutzer-ID aus Entra ID in MDM bereitgestellt und die Benutzerquelle ändert sich von "Lokal" zu "SCIM Entra ID".
- Entra ID mit dem Abonnement "Entra ID Premium P1" ist mit dem Privileg ausgestattet, die erforderliche Gruppe zuzuweisen und bereitzustellen.

12.2.10.2.2. Benutzerbereitstellung für Okta IdP

Dieser Abschnitt enthält die folgenden Themen:

- Herstellen einer Verbindung mit Ivanti Neurons for MDM
- Bereitstellen von Benutzern und Gruppen
- Überprüfen einer zugewiesenen Benutzerbereitstellung
- Überprüfen der Gruppenbereitstellung
- Bearbeiten der Einstellungen
- Konfigurieren von benutzerdefinierten Attributen und Unternehmensattributen in der SCIM-Benutzerbereitstellung

Herstellen einer Verbindung mit Ivanti Neurons for MDM

Nachdem Sie die Benutzer und Gruppen in der **Okta**-Anwendung erstellt haben, können Sie die Verbindung zwischen **Okta** und Ivanti Neurons for MDM herstellen.

Verfahren

1. Melden Sie sich bei **Okta** an.
2. Wechseln Sie zu **Anwendungen** > **Anwendungen** > **App-Katalog durchsuchen**.
3. Suchen Sie nach dem Eintrag **SCIM 2.0-Test-App hinzufügen** (OAuth-Inhabertoken) und installieren Sie die App.
4. Klicken Sie auf die App und wechseln Sie zu **Bereitstellung** > **Integration**.
5. Klicken Sie auf **Bearbeiten** und geben Sie die Basis-URL an und fügen Sie dann den generierten Token ein.
6. Klicken Sie auf **Speichern**.
7. Wechseln Sie zu **Bereitstellung** und klicken Sie auf **Bearbeiten**.
8. Aktivieren Sie die benötigten Benutzeraktionen und klicken Sie auf **Speichern**.

Bereitstellen von Benutzern und Gruppen

Sobald die Verbindung zwischen **Okta** und Ivanti Neurons for MDM hergestellt wurde, können Sie Benutzer oder Gruppen bereitstellen.

Verfahren

1. Wechseln Sie zu **Zuweisungen** > **Zuweisen** > **Zu Personen zuweisen** oder **Zu Gruppe zuweisen**.
2. 2. Wählen Sie einen vorhanden Benutzer oder eine vorhandene Gruppe aus oder suchen Sie danach und klicken Sie auf **Zuweisen**.
3. Wiederholen Sie den Prozess, um weitere **Benutzer** oder **Gruppen** hinzuzufügen.
4. Klicken Sie auf **Fertig**.
5. Wählen Sie die Gruppe aus und klicken Sie auf **Gruppe nach Name pushen**, um die Gruppe zu speichern und zu synchronisieren.

Überprüfen einer zugewiesenen Benutzerbereitstellung

Nachdem ein zugewiesener Benutzer im Okta-Portal bereitgestellt wurde, überprüfen Sie die Bereitstellung im Ivanti Neurons for MDM -Administrationsportal.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Wechseln Sie im Hauptmenü zur Registerkarte **Benutzer**. Der bereitgestellte Benutzer wird in der Liste der Benutzer auf dieser Seite aufgeführt.

Überprüfen der Gruppenbereitstellung

Nach der Bereitstellung einer Gruppe im Okta-Portal müssen Sie die Bereitstellung in Ivanti Neurons for MDM überprüfen.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Wechseln Sie zur Registerkarte **Benutzer** und klicken Sie auf **Benutzergruppen**. Die bereitgestellte Gruppe wird in der Liste der Gruppen auf dieser Seite aufgeführt.

Bearbeiten der Einstellungen

Dieses Thema unterstützt Sie bei der Konfiguration der Okta-Einstellungen.

Verfahren

1. Gehen Sie zu **Admin** > **Identität** > **Okta-Benutzerbereitstellung**.
2. Klicken Sie auf **Einstellungen bearbeiten**.
3. Legen Sie **Aus Okta importierte Benutzer automatisch einladen** fest, um zu verwalten, ob aus Okta in Ivanti Neurons for MDM importierte Benutzer automatisch per E-Mail zur Registrierung eingeladen werden.
4. (Optional) Klicken Sie auf **Benutzerdefiniertes Attribut hinzufügen** - Definieren Sie für Ihren Verzeichnisdienst anpassbare Benutzerattribute für die Geräteverwaltung. Auf jedes Attribut kann dann über $ in den Konfigurationsfeldern referenziert werden, die Variablen unterstützen. Für diese Option benötigen Sie eine konsistente Implementierung der benutzerdefinierten Attribute für alle Okta-Server. Wenn ein in Ihrer Implementierung enthaltener Okta-Server das benutzerdefinierte Attribut nicht verwendet, funktionieren von dem benutzerdefinierten Attribut abhängige Optionen möglicherweise nicht wie erwartet. Die Spalte **Attributtyp** zeigt das Attribut **IDP** in der Tabelle **Benutzerdefinierte Attribute** des Abschnitts **Einstellungen bearbeiten** an.
5. Klicken Sie nach dem Ändern der Okta-Einstellungen auf **Änderungen speichern**.

Konfigurieren von benutzerdefinierten Attributen und Unternehmensattributen in der SCIM-Benutzerbereitstellung

Verfahren

1. Wechseln Sie zu **Admin** > **Identität** > **Benutzerbereitstellung**.
2. Klicken Sie auf **Einstellungen bearbeiten**.
3. Geben Sie das benutzerdefinierte Attribut ein (z. B. custAttr1) und klicken Sie auf **Änderungen speichern**.
4. Klicken Sie im Okta-Portal auf **Verzeichnis** > **Profileditor**.
5. Klicken Sie auf **SCIM 2.0-Test-App (OAuth-Inhabertoken)**.
6. Klicken Sie auf **Attribut hinzufügen**.
7. Fügen Sie die Werte für benutzerdefinierte Attribute hinzu, z. B.:
    - Anzeigename (entspricht dem benutzerdefinierten Attributwert in N-MDM, siehe Schritt 3).

- Variablenname : custAttr1
- Externer Name: custAttr1
- Externer Namespace : **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User**
- Benutzerberechtigung: (Lesen/Schreiben)

8. Klicken Sie auf **Attribut speichern**.
9. Klicken Sie auf **Profileditor** > **Zuordnungen**. Es werden zwei Abschnitte für Zuordnungen angezeigt (SCIM und Okta).
10. Ordnen Sie die in N-MDM erstellten benutzerdefinierten Attribute den in Okta definierten Attributen zu und speichern Sie die Zuordnungen.
11. Wechseln Sie zu **Benutzer** und klicken Sie auf den gewünschen Benutzer.
12. Klicken Sie auf **Profil** > **Bearbeiten**, um die Attribute zu bearbeiten.
13. Wechseln Sie zu **Anwendungen** > **SCIM 2.0-Test-App (OAuth-Inhabertoken)**.
14. Klicken Sie auf der Registerkarte **Zuweisungen** auf **Zuweisen** und wählen Sie **Zu Personen zuweisen** aus.
    Das Fenster **SCIM 2.0-Test-App (OAuth-Inhabertoken) zu Personen zuweisen** wird angezeigt.
15. Wählen Sie den gewünschten Benutzer aus und klicken Sie auf **Zuweisen**.
16. Klicken Sie auf **Fertig**.

So überprüfen Sie das benutzerdefinierte Attribut und seine Zuordnung in Ivanti Neurons for MDM:

- Wechseln Sie zu **Benutzer** > **Benutzer** (beliebiger Benutzer) > **Attribute**. Vergewissern Sie sich, dass das zugeordnete benutzerdefinierte Attribut für Okta im Bereich mit den Benutzerattributen angezeigt wird.

12.2.11. Konfigurieren eines LDAP-Servers

Lizenz: Silver

Die Konfiguration eines LDAP-Servers und eines Connector ermöglicht Ihnen das Importieren von Benutzern und Gruppen aus Ihrem Unternehmensverzeichnis. Nachdem Sie mindestens einen Connector installiert haben, können Sie einen oder mehrere LDAP-Server hinzufügen.

Beim Hinzufügen eines LDAP-Servers wird Folgendes konfiguriert:

- die *Verbindung* zum LDAP-Server
- die erforderlichen *Suchbegriffe* zur Anzeige der Daten im Zielverzeichnis
- der zu *importierende* Teil des Verzeichnisses
- ob Benutzer automatisch in den ausgewählten Teil des Verzeichnisses *eingeladen* werden sollen

Nachdem Sie einen LDAP-Server hinzugefügt haben, können Sie zu dieser Seite **zurückkehren, um die LDAP-Serverinformationen zu bearbeiten** oder **die ausgewählten LDAP-Benutzer zu ändern**.

> LDAP-Benutzer müssen nach Konfiguration eines LDAP-Benutzers importiert werden. Siehe dazu **LDAP-Benutzer importieren**. LDAP-Benutzernamen müssen, wie lokale Benutzernamen, eindeutig sein. Überprüfen Sie, ob diese Benutzer nicht bereits über ein lokales Benutzerkonto mit dem gleichen Benutzernamen verfügen oder ob der Benutzername bei Unternehmen mit mehr als einem Mandanten nicht bereits für einem anderen Mandanten zugeordnet wurde.

Zu einem LDAP-Server hinzufügen

Verfahren

1. Klicken Sie auf **Server hinzufügen**.
2. Geben Sie die folgenden Informationen an:
3. Klicken Sie auf die Option **Verbindung testen und fortfahren**.

Einstellung	So gehen Sie vor
[Name]	Geben Sie einen Namen ein, der diesen Server bezeichnet.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieses Servers erläutert.
Verzeichnis-URL	Geben Sie die URL für das Verzeichnis ein. Verwenden Sie eines der folgenden Formate: ldap://IP-Addresse oder ldap://IP-Addresse oder Beispiel: ldap://myserver1.mycompany.com:389
Benutzer-ID	Geben Sie die Benutzer-ID für ein Konto mit den folgenden Merkmalen ein: • vom LDAP-Server verwaltet • kann zur Anmeldung am LDAP-Server verwendet werden und Teilbäume nach Benutzer-, Gruppen- und Organisationseinheiten durchsuchen Dies ist in der Regel ein Konto mit Zugangsdaten für den Directory Administrator (DN oder Distinguished Name und Passwort)
Passwort	Geben Sie das Passwort für das Konto ein.
Passwort bestätigen	Geben Sie das Passwort für das Konto erneut ein.
Verzeichnistyp	Wählen Sie den Verzeichnistyp aus der Liste der unterstützten Verzeichnisse aus. • Microsoft Active Directory • OpenLDAP • Sonstige (mit Open LDAP kompatible) Verzeichnisse

4. Bei diesem Schritt werden die Informationen geprüft, die Sie bis jetzt angegeben haben.

- Wenn sich die Informationen als gültig erweisen, stellt der Dienst den LDAP-Namenskontext wieder her und nutzt diesen, um einige der Felder auf der nächsten Seite auszufüllen.
- Wenn eine Verbindung mit der LDAP-URL nicht aufgebaut werden kann, können Sie mit folgenden Schritten fortfahren. Dadurch kann jedoch die Funktionalität beschränkt sein, bis die Verbindung aufgelöst ist.

Vervollständigen Sie die übrigen Einstellungen:

5. Klicken Sie auf **Weiter**.

Einstellung	So gehen Sie vor
Failover-URL für Verzeichnis	Geben Sie die URL für das Sekundärverzeichnis ein. Verwenden Sie das Format: ldap://IP-Addresse oder Beispiel: ldap://myserver2.mycompany.com:389
Synchronisierungsintervall	Geben Sie die Zeit zwischen jeder versuchten Synchronisierung der LDAP-Daten von dem LDAP-Server an. Der Standardwert ist 15 Minuten. Ziehen Sie in Betracht, das Intervall zu verlängern, nachdem Sie erfolgreich alle LDAP-Zieldaten synchronisiert und bestätigt haben, dass Ihr LDAP-Setup Ihre Anforderungen erfüllt.
Synchronisationspause aktivieren	Auswählen, damit die LDAP-Sync-Daten automatisch verworfen werden, wenn der neu geladene Datensatz erheblich zurückgeht. Diese Option stellt sicher, dass ein Fehlverhalten seitens des LDAP-Systems nicht zu unnötigen, störenden Service-Updates und zur Entfernung der Konfigurationen von registrierten Geräten führt. Vergewissern Sie sich, dass diese Option deaktiviert ist, wenn Sie wesentliche Änderungen an Ihrem LDAP-Setup oder an dem LDAP-Server vornehmen möchten.
Diesen LDAP-Server aktivieren Laden Sie Benutzer automatisch ein, wenn sie importiert werden.	Wählen Sie diese Option, um diesen LDAP-Server mit Ihrem Dienst zu verwenden. Deaktivieren Sie diese Einstellung, wenn Sie diesen LDAP-Server außer Dienst stellen möchten. Auch wenn ein konfigurierter Failover auf einem zweiten LDAP-Server diesen Server automatisch ersetzen würde, können -Sie mit dieser Option vorausplanen und kurze Verbindungsstörungen während des Failover vermeiden. Wählen Sie die Optionen aus, um automatisch Einladungen an die Benutzer zu senden, sobald diese vom LDAP-Server importiert wurden.
CA-Zertifikat hochladen	Klicken Sie auf **Datei wählen**, um das TLS-Zertifikat hochzuladen, das von der auf diesem LDAP-Server installierten Zertifizierungsstelle ausgestellt wurde. Sie können mehrere CA-Zertifikate hochladen.
Referrals verfolgen	Das gilt nur, wenn Sie eine Domain mit mehreren Verzeichnisbäumen verwenden. Diese Option gibt an, ob Sie mehrere alternative Domain-Controller verwenden wollen, wenn der angesprochene Domain-Controller keine Kopie des angeforderten Projekts enthält. • Klicken Sie auf **Folgen**, wenn Sie Referrals verwenden wollen. • Klicken Sie auf **Ignorieren**, wenn Sie keine alternativen Domain-Controller verwenden wollen. • **Verwerfen** hat zurzeit den gleichen Effekt wie **Ignorieren**. Bei Auswahl von Folgen wird die LDAP-Authentifizierung verzögert.
Timeout für Suchergebnisse Suchergebnisse	Verlängern Sie dieses Timeout, wenn Sie auf Leistungsprobleme oder unvollständige Ergebnisse stoßen, während Sie die synchronisierten Daten vom LDAP-Server durchsuchen. Bestimmen Sie hier die Höchstzahl der Datensätze, die zu einem Zeitpunkt von dem LDAP-Server geliefert werden sollen. Es gibt Szenarien, bei denen diese Einstellung zur Verbesserung der Leistung geändert werden muss, zum Beispiel: • Der LDAP-Server liegt weit entfernt oder hinter einem Link mit langer Reaktionszeit. In diesem Fall dauert die Anzeige umfangreicher Suchergebnisse länger als die kleinerer Trefferzahlen, daher ermöglicht die Definition eines kleineren Satzes eine schnellere Anzeige von Teilmengen aktualisierter Daten.

Einstellung	So gehen Sie vor
	• Das LDAP-Verzeichnis ist riesig, und jede Suche ergibt eine enorme Menge an Ergebnissen. In diesem Fall könnten Sie – sofern keine Leistungsprobleme bestehen – aus einer größeren Ergebnismenge mit weniger Suchen alle Daten erhalten.

In einer Sandbox-Umgebung muss das LDAP-Synchronisierungsintervall auf mindestens 8 Stunden festgelegt werden.

6. Verwenden Sie die folgenden Richtlinien für die Konfiguration der Integration mit dem LDAP-Server:
7. Klicken Sie auf **Durchsuchen** oder **Suchen**.

Einstellung	So gehen Sie vor
Gruppenmitgliedsformat	Wählen Sie **DN** oder **UID**, um zu ermitteln, ob Sie den Distinguished Name oder die Benutzer-ID bei Ihrer Suche verwenden.
OU-Suchattribute	Bestimmen Sie Kriterien für die Suche auf der Organisationseinheitsebene.
Basis-DN	Geben Sie den Distinguished Name für die Ausgangsebene ein, in der Ihre Suche platziert werden bzw. beginnen soll. Ihre Auswahl bestimmt Standardwerte für verschiedene andere Felder, die Sie bei Bedarf verändern können.
Objekt-GUID	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen. Dieses Attribut ermöglicht unabhängig von Zeit und Namensänderungen die eindeutige Identifizierung einer Organisationseinheit.
Attributname	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Beschreibung	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Attribut DN	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Suchfilter	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Suchumfang	Wählen Sie den anzuvisierenden Teil der LDAP-Hierarchie: • **Basis** (nur die Ebene des Basis-Sucheintrags) • **Eine Ebene** (die Ebene unterhalb der Suchbasis) • **Teilbaum** (der Teilbaum in dem Verzeichnisbaum unterhalb des Suchbasis-DN)
Benutzer-Suchattribute	Bestimmen Sie die Kriterien für die Suche nach Benutzern in einer beliebigen Verzeichnisebene.
Basis-DN	Geben Sie den Distinguished Name für die Ausgangsebene ein, in der die Suche durchgeführt werden soll.
Attribut UID	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Objekt-GUID	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen. Dieses Attribut ermöglicht unabhängig von Zeit und Namensänderungen die eindeutige Identifizierung eines Benutzers.
Attribut DN	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Vorname	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Nachname	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Anzeigename	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.

Einstellung	So gehen Sie vor
E-Mail-Adresse	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Principal-Name	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Region	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Mitglied von	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Suchfilter	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Suchumfang	Wählen Sie den anzuvisierenden Teil der LDAP-Hierarchie: • **Basis** (nur die Ebene des Basis-Sucheintrags) • **Eine Ebene** (die Ebene unterhalb der Suchbasis) • **Teilbaum** (der Teilbaum in dem Verzeichnisbaum unterhalb des Suchbasis-DN)

Verwaltete Apple-ID	Wählen Sie, welche verwaltete Apple-ID für die LDAP-Benutzer synchronisiert werden soll.
	• **Keine**
	• **Muster**
	  ◦ **E-Mail-Adresse des Benutzers**
	  ◦ **userUPN**
	  Wählen Sie optional die **Option „appleid"-Subdomain einschließen**, um Konflikte mit bestehenden Apple-IDs zu vermeiden.

+Benutzerattribut hinzufügen	(Optional): Definieren Sie für Ihren Verzeichnisdienst bis zu 7 kundenspezifische Benutzerattribute für die Geräteverwaltung. Auf jedes Attribut kann dann mit $ in den Konfigurationsfeldern zugegriffen werden, die Variablen unterstützen. **Wichtig:** Für diese Option benötigen Sie eine konsistente Implementierung der kundenspezifischen Attribute für alle LDAP-Server. Wenn ein in Ihrer Implementierung enthaltener LDAP-Server dieses Attribut nicht verwendet, funktionieren von diesem Attribut abhängige Optionen möglicherweise nicht wie erwartet.
Gruppen-Suchattribute	
Basis-DN	Geben Sie den Distinguished Name für die Ausgangsebene ein, in der die Suche durchgeführt werden soll.
Objekt-GUID	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen. Dieses Attribut ermöglicht unabhängig von Zeit und Namensänderungen die eindeutige Identifizierung einer Gruppe.
Attribut DN	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Attributname	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.

Einstellung	So gehen Sie vor
Beschreibung	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Mitglied	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Suchfilter	Bei Bedarf können Sie den Standardwert an Ihre LDAP-Umgebung anpassen.
Suchumfang	Wählen Sie den anzuvisierenden Teil der LDAP-Hierarchie: • **Basis** (nur die Ebene des Basis-Sucheintrags) • **Eine Ebene** (die Ebene unterhalb der Suchbasis) • **Teilbaum** (der Teilbaum in dem Verzeichnisbaum unterhalb des Suchbasis-DN)

8. Bestätigen Sie, dass Ihre Konfiguration die gewünschten Daten liefert.
9. Sie können dies tun, indem Sie nach einem bekannten Objekt im Verzeichnis suchen.

Klicken Sie auf **Weiter**.

Benutzerdefiniertes LDAP-Attribut löschen

Sie können ein benutzerdefiniertes LDAP-Attribut löschen und dessen Werte von den zugeordneten Benutzern oder Geräten entfernen.

Verfahren

1. Gehen Sie zu **Administrator > Attribute**.
2. Klicken Sie in dem Abschnitt **Kundenspezifische Attribute** auf den Link **Löschen** neben dem LDAP-Attribut, das Sie löschen wollen. Ein Bestätigungsfenster wird angezeigt.
3. Klicken Sie auf **Löschen** , um den Löschvorgang zu bestätigen.

Beachten Sie, dass standardmäßig die Schaltfläche Löschen deaktiviert ist.Klicken Sie in das Kontrollkästchen **Ich weiß, dass ein gelöschtes kundenspezifisches Attribut nicht wiederhergestellt werden kann**, um die Schaltfläche **Löschen** zu aktivieren.

LDAP-Server-Informationen bearbeiten

Verfahren

1. Gehen Sie zu **Admin > LDAP**.
2. Wählen Sie im LDAP-Server-Eintrag das Symbol **Bearbeiten** in der Spalte **Aktionen**, um die Seite "LDAP-Server verbinden" anzuzeigen.
3. Nehmen Sie die nötigen Änderungen vor.
4. Klicken Sie auf die Option **Verbindung testen und fortfahren**.
   Wenn eine Verbindung mit der LDAP-URL fehlschlägt, können Sie mit den nächsten Schritten fortfahren. Dadurch kann jedoch die Funktionalität beschränkt sein, bis die Verbindung aufgelöst ist.
5. Klicken Sie auf **Durchsuchen** oder **Suchen**.

6. Bestätigen Sie, dass Ihre Konfiguration die gewünschten Daten liefert.
   Sie können dies tun, indem Sie nach einem bekannten Objekt im Verzeichnis suchen.
7. Klicken Sie auf **Fertig**.

LDAP-Benutzer importieren

Verfahren

1. Gehen Sie zu **Benutzer**.
2. Klicken Sie auf **+Hinzufügen > Benutzer aus LDAP einladen**.
3. Klicken Sie in dem LDAP-Server-Eintrag auf **Benutzer auswählen.**
4. Geben Sie auf der Seite „LDAP-Benutzer hinzufügen“ den Namen des Benutzers, der Gruppe oder der Organisationseinheit in dem Suchfeld ein.
5. Klicken Sie zum Hinzufügen neuer Benutzer oder Gruppen neben dem Eintrag, den Sie ergänzen wollen, auf **+ Hinzufügen**.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie aus, ob Sie die Einladung versenden wollen.
   - Niemanden einladen
     Um die Einladungen später zu versenden, gehen Sie zu Benutzer > Benutzer und klicken auf Aktionen > Einladung senden, um die Einladungen zu versenden.
   - Alle einladen

Klicken Sie auf **Fertig**.

Ausgewählte Benutzer, Gruppen oder Organisationseinheiten aktualisieren

Verfahren

1. Gehen Sie zu **Admin > LDAP**.
2. Wählen Sie im LDAP-Server-Eintrag das Symbol **Benutzer verwalten** in der Spalte **Aktionen** aus, um die Seite "LDAP-Benutzer hinzufügen" anzuzeigen.
3. Geben Sie den Namen des Benutzers bzw. der Gruppe im Suchfeld ein, den/die Sie hinzufügen wollen.
4. Klicken Sie neben dem Eintrag, den Sie ergänzen wollen, auf **+Hinzufügen** .
5. Klicken Sie neben dem Eintrag, den Sie entfernen wollen, auf das betreffende Symbol, um einen Benutzer, eine Gruppe oder Organisationseinheit zu entfernen.
6. Klicken Sie auf **Fertig**.

Benachrichtigung zum Abbruch der LDAP-Synchronisation aktivieren

Die Aktivierung der Benachrichtigung, ob eine LDAP-Synchronisation verworfen wurde, hilft dabei, Ausfälle durch unbeabsichtigte umfangreiche Änderungen der LDAP-Umgebung zu vermeiden.

Verfahren

1. Gehen Sie zu **Admin > LDAP**.
2. Wählen Sie im LDAP-Server-Eintrag das Symbol **Bearbeiten** in der Spalte **Aktionen**, um die Seite "LDAP-Server verbinden" anzuzeigen.

3. Aktivieren Sie das Kontrollkästchen **Sync verwerfen aktivieren**.
4. Geben Sie ein, bei wie viel Prozent der neu geladenen LDAP-Daten eine Synchronisationspause ausgelöst werden soll.
5. Klicken Sie auf die Option **Verbindung testen und fortfahren**.
   Wenn eine Verbindung mit der LDAP-URL nicht aufgebaut werden kann, können Sie mit folgenden Schritten fortfahren. Dies kann jedoch die Funktionalität einschränken, solange die Verbindung nicht wiederhergestellt ist.
6. Klicken Sie auf **Fertig**.
7. Klicken Sie im LDAP-Server-Eintrag auf das Symbol **Jetzt synchronisieren**.
   Wenn der Umfang der Änderungen, die zwischen LDAP und der Cloud synchronisiert werden sollen, über dem eingestellten Prozentsatz liegt, wird eine Warnnachricht erzeugt. Wenn die Änderungen nicht mehr die eingestellte Schwelle überschreiten, wird die Benachrichtigung gelöscht.

Auslöser	[Severity]	Benachrichtigungsart	Komponentenart	Komponente
LDAP-Synchronisationspause	Warnung	Datensynchronisation	LDAP,	LDAP-Servername
LDAP-Synchronisation wieder aufgenommen.	[Info]	Datensynchronisation	LDAP,	LDAP-Servername

Die Benachrichtigung „Teilweise Synchronisieren verwerfen“ wird erzeugt, wenn mindestens ein Benutzerdatensatz nicht mit LDAP synchronisiert wird. In diesem Fall ist als Anhang eine CSV-Datei mit einer Liste der Benutzer enthalten, die nicht synchronisiert werden konnten. Wenn ein Benutzer aufgrund fehlender Attribute verworfen wurde, ist die Liste der fehlenden Attribute ebenfalls in der exportierten CSV-Datei enthalten.

Änderungen mit dem LDAP-Server synchronisieren

Klicken Sie auf der LDAP-Seite im LDAP-Servereintrag auf **Jetzt synchronisieren**.

> Besteht der Anzeigename aus mehr als 128 Zeichen, ignoriert die LDAP-Synchronisierung den Benutzer und fährt mit der Synchronisierung anderer Benutzer oder Gruppen fort.

Behebung von Konnektivitätsfehlern des LDAPS-Servers

Wenn Sie Probleme beim Verbindungsaufbau mit dem LDAPS (LDAP over SSL)-Server feststellen, besteht möglicherweise ein Problem mit dem Zertifikat.

So beseitigen Sie das Problem:

- Überprüfen Sie, ob Sie nicht ein selbst signiertes Zertifikat auf dem LDAPS-Server verwenden.
- Überprüfen Sie, dass das LDAPS-Zertifikat nicht abgelaufen ist und nicht zurückgezogen wurde. Überprüfen Sie außerdem, ob der Hostname korrekt ist.

Warten Sie nach der Überprüfung auf die automatische LDAP-Synchronisation oder synchronisieren Sie manuell über das Symbol **Admin > LDAP > Jetzt synchronisieren** im LDAP-Server-Eintrag.

Wenn Sie die LDAP-Seite nicht sehen können, kann es sein, dass Sie nicht über die erforderlichen Berechtigungen verfügen. Sie brauchen eine der folgenden **Rollen**:

- Systemverwaltung
- System schreibgeschützt

12.2.12. [Sentry]

Sentry ist eine Komponente, die als Gateway zwischen Mobilgeräten und dem ActiveSync-fähigen E-Mail-System dient. Verwenden Sie Sentry, um zu kontrollieren, welche Geräte auf E-Mails zugreifen dürfen. Es kann als ISO-Datei heruntergeladen werden, die Sie auf einer virtuellen Maschine installieren können. Organisationen sollten einen Load Balancer verwenden, um mehrere (redundante) Sentrys zu pflegen.

Lizenz: Silver

Aktuelle Dokumentation

Die neueste Sentry-Anleitung finden Sie unter **Produktdokumentation**; klicken Sie dort auf Sentry.

Die aktuellen Installationsanweisungen für Sentry finden Sie in der *Installationsanleitung für eigenständiges Sentry im lokalen Netzwerk*.

Anweisungen zum Upgrade von Sentry finden Sie in der betreffenden Version der *Sentry-Anleitung*. Weitere Informationen dazu finden Sie in den folgenden Abschnitten der Anleitung für Sentry:

- Anweisungen zum Upgrade finden Sie in der Benutzeroberfläche für den Standalone Sentry System Manager unter "Standalone Sentry Software Updates" (Software-Updates für eigenständiges Sentry).
- Anweisungen zum Upgrade mit der Befehlszeilenschnittstelle (CLI) für ein eigenständiges Sentry finden Sie unter „Upgrades mit CLI durchführen“.

Lesen Sie die Informationen zum Sentry Release für die Version, auf die Sie upgraden wollen, bevor Sie mit dem eigentlichen Upgrade beginnen.

12.3. Apple-Einstellungen

Dieser Abschnitt enthält die folgenden Themen:

- Apple Configurator
- Geräteregistrierung
- Konfigurieren von Setup Assistant
- MDM-Zertifikat installieren
- Gemeinsam genutzte iPad-Geräte für Unternehmen
- School Manager
- Einstellungen (Apple)

12.3.1. Apple Configurator

Sie können mit dieser Seite den Apple Configurator auf die Konfiguration der Cloud-Geräteverwaltung auf iOS-Geräten vorbereiten. Mit dem Apple Configurator wird die Bereitstellung von iOS-Geräten in großer Zahl zum Kinderspiel. Darüber hinaus können Administratoren mit dem Configurator iOS-Geräte auf „Überwacht“ setzen, was die Konfigurations- und Verwaltungsmöglichkeiten erhöht. Weitere Informationen über Apple Configurator finden Sie im App Store.

Dies sind die wichtigsten Schritte:

1. Exportieren Sie das MDM-Profil Ihres Ivanti Neurons for MDM-Mandanten.
2. Importieren Sie das MDM-Profil in den Configurator.
3. Verwenden Sie den Configurator, um das MDM-Profil auf angebundene Geräte zu übertragen.

Standardbenutzer für Geräte definieren

Über den Apple Configurator konfigurierte Geräte werden dem Benutzer „Nobody“ in der Cloud zugeordnet, sofern Sie nicht einen anderen Benutzer auswählen:

1. Klicken Sie in der Option **Konfigurierte Geräte zuordnen** in das Feld.
2. Geben Sie den Benutzernamen des Cloud-Benutzers ein, den Sie auswählen wollen.
3. Wählen Sie den Benutzernamen aus, wenn er in der Dropdownliste angezeigt wird.
4. Klicken Sie auf **Speichern**.

Apps mit Apple Configurator installieren

Führen Sie vor der Nutzung des Apple Configurator zur Installation von Apps folgende Schritte aus:

- Der Zugriff auf den App Store von Apple wird durch die Gerätekonfiguration eingeschränkt.
- Die App-Installation wird durch die Gerätekonfiguration erlaubt.
- Der Apple Configurator muss auf dem Computer installiert werden, mit dem die Geräte konfiguriert werden.

So installieren Sie Apps mit dem Apple Configurator:

1. Wechseln Sie in Ivanti Neurons for MDM zu **Admin > Apple-Konfigurator**.
2. Aktivieren Sie die Option zur Registrierung von Geräten.
3. Klicken Sie auf eine der folgenden Optionen:
    - **Plist des Standardbenutzers**.
    - **Spezifische Benutzer-Plist** – Geben Sie den Benutzernamen bzw. die E-Mail-ID des betreffenden Benutzers ein.

Gehen Sie im Apple Configurator auf **Vorbereiten > Apps**.

5. Gehen Sie zu **Vorbereiten > Einstellung und Überwachung deaktivieren**.
6. Wählen Sie in dem Abschnitt iOS aktualisieren die Option **Gerät nie aktualisieren**.
7. Klicken Sie auf **Vorbereiten** (am unteren Rand des Apple Configurator).
   Die Apps werden auf dem Gerät nach der Geräteanmeldung in der Liste der installierten Apps angezeigt.

Apps mit UEM-Server installieren

Apps mit dem UEM-Server installieren:

1. Laden Sie eine App aus dem internen Store in die Registerkarte "Apps" hoch.
2. Wählen Sie die App aus.
3. Klicken Sie auf die Registerkarte **App-Konfigurationen**.
4. Optional können Sie **Auf Gerät installieren auswählen**.
   Vervollständigen Sie die Konfigurationseinstellungen.
5. Klicken Sie auf **Aktionen > Anmeldung erzwingen**.

Aufgaben des Endbenutzers

Apple erwartet, dass der Endbenutzer die Go mindestens einmal startet, sonst funktioniert die Cloud-Standortfunktion nicht einwandfrei. Auf diese Weise ist dem Endbenutzer bekannt, dass sein Standort erfasst wird.

Vorsicht: Wenn Geräte im Einzel-App-Modus mit dem Configurator bereitgestellt werden, ist dieses Konzept nicht möglich.

Wenn Sie die Seite **Apple Configurator installieren** nicht sehen können, kann es sein, dass Sie nicht über die erforderlichen Berechtigungen verfügen. Sie brauchen eine der folgenden **Rollen**:

- Systemverwaltung
- System schreibgeschützt

12.3.2. Kontogesteuerte Registrierung

Dieser Abschnitt gilt für die kontogesteuerte Benutzer- und Geräteregistrierung.

Unterstützte Geräte

- Geräte mit iOS 15+ (für die kontogesteuerte Benutzerregistrierung) und iOS17+ (für die kontogesteuerte Geräteregistrierung)
- Geräte mit macOS 14+
- Geräte mit visionOS 1.1+

Voraussetzungen:

Für die kontogesteuerte Benutzerregistrierung

- Benutzerkonto in Ivanti Neurons for MDM mit verwalteter Apple-ID (Benutzer in Apple Business Manager oder Apple School Manager)
- Wählen Sie im Abschnitt **Apple-Registrierung** in der Dropdownliste **Apple-Registrierungsart auswählen** die Option **Benutzerregistrierung** aus.
- Setzen Sie unter **Benutzer** → **Benutzereinstellungen** → die **Einstellungen für Gerätebesitzer** auf **EIN** > und wählen Sie die Option **Eigentum des Benutzers** aus.

Für die kontogesteuerte Geräteregistrierung

- Benutzerkonto in Ivanti Neurons for MDM mit verwalteter Apple-ID (Benutzer in Apple Business Manager oder Apple School Manager)
- Wählen Sie im Abschnitt **Apple-Registrierung** in der Dropdownliste **Apple-Registrierungsart auswählen** die Option **Geräteregistrierung** aus.
- Setzen Sie unter **Benutzer** → **Benutzereinstellungen** → die **Einstellungen für Gerätebesitzer** auf **EIN** > und wählen Sie die Option **Eigentum des Unternehmens** aus.

Die **kontogesteuerte Benutzerregistrierung** für Geräte mit iOS 15+, macOS 14+ und visionOS 1.1 ist eine Registrierungsoption für Unternehmen, die ein BYOD-Programm (Bring Your Own Device, jeder bringt sein eigenes Gerät mit) implementieren möchten. Die kontogesteuerte Benutzerregistrierung ist eine modifizierte Version des MDM-Protokolls und der Benutzerregistrierung mit dem Apple Business Manager mit einem deutlich stärkeren Datenschutz der Benutzer; implementiert wird ein Sicherheitsniveau, wie es Unternehmen benötigen.

Die **kontogesteuerte Geräteregistrierung** für Geräte mit iOS 17+, macOS 14+ und visionOS 1.1+ ist eine Registrierungsoption für Unternehmen, die firmeneigene Geräte/Unternehmensgeräte implementieren möchten. Die kontogesteuerte Geräteregistrierung nutzt das MDM-Protokoll und die Geräteregistrierung mit Apple Business Manager mit einem deutlich stärkeren Datenschutz der Benutzer. Sie implementiert ein Sicherheitsniveau, das den Anforderungen von Unternehmen gerecht wird. Endbenutzer können ihre Geräte unter Verwendung der Funktion "Arbeitskonto" bei den Einstellungen registrieren.

Discovery-Dienst einrichten

Wenn Ihr Unternehmen einen Firmendomänennamen besitzt (z. B. acme.com), gilt für Ihr Gerät die E-Mail-ID "gerätename@acme.com".

1. Der Benutzer meldet sich mit benutzername@acme.com bei seinem Arbeits- oder Schulkonto an, und das Gerät führt einen HTTP GET-Aufruf bei folgender URL durch: https://acme.com/.well-known/com.apple.remotemanagement?user-identifier=user@acme.com

Weitere Informationen finden Sie unter https://developer.apple.com/documentation/devicemanagement/discover_authentication_servers.

2. Konfigurieren Sie in der acme.com-Domäne eine Umleitungsregel für die URI - /. well-known/com.apple.remotemanagement, um sie auf folgende URL umzuleiten: https://<n-MDM cluster>/.well-known/com.apple.remotemanagement

Vereinfachte Dienstermittlung für kontogesteuerte Geräteregistrierung

> Gilt für Geräte mit iOS 18.2+, macOS 15.2+ und visionOS 2.2+.

Wenn ein Benutzer bei der kontogesteuerten Registrierung seine Unternehmens-E-Mail-Adresse eingibt, um sich bei seinem Arbeits- oder Schulkonto anzumelden, sucht das Gerät zuerst nach einer bekannten HTTP-Ressource in der Unternehmensdomäne, die einen Link zur MDM-Registrierungs-URL enthält.

Verfahren

1. Melden Sie sich beim Arbeits- oder Schulkonto an.
2. Überprüfen Sie die Domänen in **Apple Business Manager** und **Apple School Manager** – Gilt nur für Domänen, die innerhalb von Apple Business Manager oder Apple School Manager verifiziert wurden. Wenn die Domäne verifiziert wurde, kann das Gerät bei Apple Business Manager/Apple School Manager eine alternative MDM-Registrierungs-URL anfordern.
3. Legen Sie eine Standard-Ivanti Neurons for MDM-Zuweisung für die Plattformtypen **Mac**, **Apple Vision Pro**, **iPhone** und **iPad** fest. Gehen Sie zum Festlegen einer standardmäßigen Gerätezuweisung wie folgt vor:
    1. Melden Sie sich in **Apple Business Manager**/**Apple School Manager** mit einem Benutzer an, der die Rolle Administrator oder Device Enrollment Manager hat.
    2. Wählen Sie unten in der Seitenleiste Ihren Namen aus, wählen Sie Einstellungen und führen Sie dann einen der folgenden Schritte aus:
        - Wählen Sie "Zuweisung von Geräteverwaltungsdiensten" unter "Ihre Geräteverwaltungsdienste" aus und wählen Sie dann "Bearbeiten" neben "Zuweisung von Standard-Geräteverwaltungsdienst".
        - Wählen Sie einen vorhandenen Dienst bei den Geräteverwaltungsdiensten und anschließend "Ändern" unter "Standardgerätezuweisung" aus.
    3. Wenn Sie keine anderen konfigurierten Gerät haben, ändern Sie alle automatischen Gerätezuweisungen in den ausgewählten Dienst ab und wählen Sie **Speichern** aus.
4. Navigieren Sie in der Ivanti Neurons for MDM-Konsole zu **Admin** > **Apple** > **Geräteregistrierung**. Im Bildschirm **Geräteregistrierung** werden die Spalten **ADDE URL** und **ADDE URL SET TIME** hinzugefügt.

> **Erste Präferenz**: Das Gerät prüft die bekannte HTTP-Ressource in der Unternehmensdomäne.

Fallback-Option: Sollte die erste Methode fehlschlagen, kontaktiert das Gerät Apple ABM/ASM, um ein alternatives Ziel abzurufen, das von Ivanti Neurons for MDM angegeben wurde.

5. Wählen Sie bei den **Aktionen** die Option **ADDE-URL konfigurieren** aus.
6. Aktualisieren Sie die Seite.

Anweisungen für Gerätebenutzer

Dieses Thema beschreibt die Aktionen, die der Gerätebenutzer zum Registrieren über die kontogesteuerte Benutzer- oder Geräteregistrierung durchführen muss.

Verfahren

1. Wechseln Sie auf dem Gerät zu einer der folgenden Optionen:
   - Für ein **iOS**-Gerät: **Einstellungen** > **Allgemein** > **VPN-** und **Geräteverwaltung**.
   - Für ein **macOS**-Gerät: **Systemeinstellungen** > **Datenschutz und Sicherheit** > **Profile**.
   - Für **visionOS**-Gerät – **Einstellungen** > **Allgemein** > **VPN** & **Geräteverwaltung**.
2. Gehen Sie zu **Beim Arbeits- oder Schulkonto anmelden**.
3. Geben Sie die E-Mail-Adresse des Arbeits- oder Schulkontos ein. Die E-Mail-Adresse muss folgendes Format aufweisen: <enterprise domain name>Benutzername@<Domänenname des Unternehmens>, z. B. benutzername@firmaxy.com.
4. Die Anmeldeseite übernimmt automatisch die verwaltete Apple-ID und führt den Benutzer durch den iReg-Flow. Vergewissern Sie sich, dass Sie die Anmeldeinformationen für Ivanti Neurons for MDM eingeben.
5. Geben Sie die Anmeldedaten für das Arbeits- oder Schulkonto ein und klicken Sie auf **Weiter**.
6. Nach einer Zwei-Faktor-Authentifizierung wird die Geräteregistrierung abgeschlossen.

12.3.3. Geräteregistrierung

Mit dem Device Enrollment Program (DEP), das Teil von Apple Business Manager ist, können Kunden Geräte in großen Mengen kaufen und diese Geräte während der Aktivierung automatisch bei MDM anmelden. Ivanti Neurons for MDMWenn Sie sich beteiligen wollen, können Sie die Cloud als MDM-Server zur Verwaltung dieser Geräte verwenden. **https://business.apple.com/**Weitere Informationen finden Sie unter **https://business.apple.com/**.

Ivanti Neurons for MDMCloud mit der Geräteanmeldung verbinden

Ivanti Neurons for MDMIvanti Neurons for MDMUm die Cloud als MDM-Server für Device Enrollment zu verwenden, richten Sie das Apple Business Manager Server-Token unter ein.

Für jeden Apple Business Manager-Server sind die folgenden Aktionen in der Ivanti Neurons for MDM verfügbar:

- Verbindung testen
- Device Enrollment Profil hinzufügen
- Öffentlichen Schlüssel herunterladen
- Vollständige Synchronisation der Geräteregistrierung - Vollständige Synchronisation einleiten. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Sobald die Synchronisierung abgeschlossen ist, können Sie die Informationen in der Spalte „Letzte Synchronisierung“ anzeigen. Sie können die vollständige Synchronisierung nicht starten, wenn sie bereits läuft.

> Ivanti Neurons for MDM benachrichtigt Administratoren, wenn eine DEP-Serversynchronisierung fehlschlägt, was das Identifizieren von Problemen erleichtert. Wenn Sie einen DEP-Server löschen, löscht das System auch die zugehörigen Benachrichtigungen.

- Neuen Token hochladen
- Löschen

> Die Aktionen **Authentifizierung bearbeiten** und **Geräteattribut für Geräteregistrierung zuweisen** stehen jetzt für Geräteregistrierungsprofile statt für die Geräteregistrierung (MDM-Server) verfügbar.

Verfahren

1. Gehen Sie zuAdministration>Apple>Device Enrollment.
2. Klicken Sie auf **Schlüssel herunterladen**.
3. Speichern Sie Ihren Ivanti Neurons for MDM Schlüssel.
4. Klicken Sie auf **business.apple.com**.
5. Melden Sie sich mit Ihren Anmeldeinformationen für Apple Device Enrollment an.
6. Auf der Website Apple Device Enrollment:
7. Klicken Sie in Ivanti Neurons for MDM auf **Hochladen**.
8. Klicken Sie auf **Erste Schritte**.
9. Wählen Sie das vertrauenswürdige Telefon aus, das für die Authentifizierung der Services von Apple verwendet werden soll.
10. Geben Sie den Prüfcode ein, der an das ausgewählte Telefon gesendet wurde.
11. . Klicken Sie auf **MDM-Server hinzufügen**.

12. Geben Sie einen Namen ein, um den virtuellen MDM-Server für den Dienst zu identifizieren.
13. Klicken Sie auf **Weiter**.
14. Geben Sie den öffentlichen Schlüssel ein, den Sie zuvor heruntergeladen haben.
15. Klicken Sie auf **Weiter**
16. . Klicken Sie auf **Ihr Server Token**, um das Token herunterzuladen.
17. Klicken Sie auf **Fertig**.
18. Klicken Sie auf **Weiter**.
19. Auswählen einer Authentifizierungsoption:

- **Aufforderung des Benutzers zur Registrierung/Anmeldung**

> Geräte, die auf der visionOS-Plattform betrieben werden, werden nicht unterstützt. Verwenden Sie stattdessen die Option **Benutzeranmeldung überspringen**, um ein Gerät zu registrieren.

> Die Benutzer werden aufgefordert, einen Benutzernamen und ein Passwort einzugeben. Die Benutzer können in dem Passwortfeld entweder ein Passwort oder eine PIN eingeben. Bei Geräten mit macOS 15+ sind zusätzliche Optionen wie **Gesichts-ID**, **Touch-ID** oder **Sicherheitsschlüssel** für iDP-Benutzer verfügbar, wenn Identitätsanbieter mit Passkey-Unterstützung verwendet werden. User_Settings.htmDie bevorzugte PIN bzw. das bevorzugte Passwort können Sie unter Benutzer → Benutzereinstellungen für die Authentifizierung konfigurieren.

- **Benutzeranmeldung überspringen**

> Geräte, die dem Nobody-Benutzer („anonymous“) oder einem bestimmten Benutzer zugeordnet sind, können Sie später über die Seite **Geräte** immer noch bestimmten Benutzern neu zuordnen.

Wählen Sie eine der folgenden Optionen aus:

  - **Definieren Sie einen Benutzer, um alle Geräte zuzuordnen**
  - **Ordnen Sie alle Geräte einem anonymen Benutzer zu.**

10. User_Settings.htmDie ausgewählte Option überschreibt die Auswahl unterBenutzereinstellungen.

Klicken Sie auf **Hochladen**, um den in Schritt 3 erhaltenen Schlüssel zu installieren.

11. Füllen Sie das angezeigte Formular aus, um das Profil Ihrer Geräte für Device Enrollment zu definieren:
12. Legen Sie fest, welche Schritte vom Benutzer bei der Geräteaktivierung für folgende Setup-Optionen übersprungen werden dürfen:.

Einstellung	Aktion
[Name]	Geben Sie einen Namen ein, der dieses Device Enrollment Profil bezeichnet.
Beschreibung	Geben Sie eine Beschreibung für das Profil ein.
Abteilung	Geben Sie die Abteilung in Ihrer Organisation ein, die im Zusammenhang mit diesem Profil steht.
Überwachter Modus	Ermöglicht zusätzliche administrative Kontrolle über Konfigurationen und Einschränkungen. Für Geräte mit iOS 13+ und macOS 10.15+ ist diese Option standardmäßig aktiviert.
iOS 17+	**Betriebssystemversion für die Registrierung** • **Betriebssystem-Mindestversion für Registrierung anfordern**: Der Administrator kann eine mindestens erforderliche Betriebssystemversion für die Registrierung von Geräten festlegen. Wenn das Gerät die Kriterien bezüglich der Mindestversion des Betriebssystems nicht erfüllt, wird der Benutzer vom System aufgefordert, ein Upgrade auf die erforderliche Version durchzuführen. Lehnt der Benutzer das Upgrade ab, wird die Registrierung blockiert. **Neueste Version**: Der Administrator kann die neueste Betriebssystemversion für die Geräteregistrierung festlegen. Wenn das Gerät die Kriterien bezüglich der neuesten Version des Betriebssystems nicht erfüllt, wird der Benutzer vom System aufgefordert, ein Upgrade auf die erforderliche Version durchzuführen. Lehnt der Benutzer das Upgrade ab, wird die Registrierung blockiert. **Bestimmte Version**: Der Administrator kann eine mindestens erforderliche Betriebssystemversion für die Geräteregistrierung festlegen. Wenn das Gerät die Kriterien bezüglich der Mindestversion des Betriebssystems nicht erfüllt, wird der Benutzer vom System aufgefordert, ein Upgrade auf die erforderliche Version durchzuführen. Lehnt der Benutzer das Upgrade ab, wird die Registrierung blockiert. • **Mindest-iOS**: Wenn die angeforderte Build-Version nicht mit der im Schlüssel '**OSVersion**' angegebenen Betriebssystemversion übereinstimmt, hat die Betriebssystemversion Vorrang. • **Mindest-Build-Version**: Wenn die angeforderte Build-Version nicht mit der im Schlüssel '**OSVersion**' angegebenen Betriebssystemversion übereinstimmt, hat die Betriebssystemversion Vorrang. Dieses Feld ist optional, falls Sie die falsche Build-Nummer eingeben. • **Meldung**: Eine geeignete Beschreibung des Fehlers, die dem Benutzer angezeigt werden kann. Bei Bedarf ◦ kann der Client versuchen, die Meldung anzuzeigen, was jedoch ◦ aufgrund von lokalen Bedingungen eventuell nicht möglich ist. Es bewährt sich, die Meldung hinzuzufügen. • **Geräte zu Betaprogramm hinzufügen** **Beta-Programme für iOS**: Erzwingt während der automatischen Geräteregistrierung Beta-Softwareversionen auf iOS.
macOS 14+	**Betriebssystemversion für die Registrierung** • **Betriebssystem-Mindestversion für Registrierung anfordern**: Der Administrator kann eine mindestens erforderliche Betriebssystemversion für die Registrierung von Geräten festlegen. Wenn das Gerät die Kriterien bezüglich der Mindestversion des Betriebssystems nicht erfüllt, wird der Benutzer vom System aufgefordert, ein Upgrade auf die erforderliche Version durchzuführen. Lehnt der Benutzer das Upgrade ab, wird die Registrierung blockiert. **Neueste Version**: Der Administrator kann die neueste Betriebssystemversion für die Geräteregistrierung festlegen. Wenn das Gerät die Kriterien bezüglich der neuesten Version des Betriebssystems nicht erfüllt,

Einstellung	Aktion
	wird der Benutzer vom System aufgefordert, ein Upgrade auf die erforderliche Version durchzuführen. Lehnt der Benutzer das Upgrade ab, wird die Registrierung blockiert. **Bestimmte Version**: Der Administrator kann eine mindestens erforderliche Betriebssystemversion für die Geräteregistrierung festlegen. Wenn das Gerät die Kriterien bezüglich der Mindestversion des Betriebssystems nicht erfüllt, wird der Benutzer vom System aufgefordert, ein Upgrade auf die erforderliche Version durchzuführen. Lehnt der Benutzer das Upgrade ab, wird die Registrierung blockiert. • **Mindest-macOS**: Wenn die angeforderte Build-Version nicht mit der im Schlüssel '**OSVersion**' angegebenen Betriebssystemversion übereinstimmt, hat die Betriebssystemversion Vorrang. • **Mindest-Build-Version**: Wenn die angeforderte Build-Version nicht mit der im Schlüssel '**OSVersion**' angegebenen Betriebssystemversion übereinstimmt, hat die Betriebssystemversion Vorrang. Dieses Feld ist optional, falls Sie die falsche Build-Nummer eingeben. • **Meldung**: Eine geeignete Beschreibung des Fehlers, die dem Benutzer angezeigt werden kann. Bei Bedarf ◦ kann der Client versuchen, die Meldung anzuzeigen, was jedoch ◦ aufgrund von lokalen Bedingungen eventuell nicht möglich ist. Es bewährt sich, die Meldung hinzuzufügen. • **Geräte zu Betaprogramm hinzufügen** **Beta-Programme für macOS**: Erzwingt während der automatischen Geräteregistrierung Beta-Softwareversionen auf macOS.
iOS-Updates automatisch herunterladen und installieren	(nur iOS 9.0+) Wenn die Option zum automatischen Download auf dem Gerät unter **Einstellungen > iTunes & App Store** ausgewählt ist, werden die Betriebssystemupdates automatisch heruntergeladen, aber noch nicht installiert, auch wenn das Device Enrollment-Profil deaktiviert ist. Diese Einstellung wird bevorzugt, wenn für die überwachten Geräte, die für die Geräteregistrierung eingetragen sind, eine iOS-Software-Update-Konfiguration existiert. Jede Änderung dieser Einstellung gilt für das überwachte Gerät, das für die Geräteregistrierung eingetragen ist, auch ohne Reset des Geräts.
MDM entfernbar	Definiert, dass der Benutzer sich nicht mehr von MDM abmelden kann, wenn das Gerät registriert ist. Diese Einstellung gilt nicht für **gemeinsam genutzte iPads**.
MDM vorgeschrieben	Definiert, dass der Benutzer die Installation von MDM während der Aktivierung nicht überspringen kann. Für Geräte mit iOS 13+ und macOS 10.15+ ist diese Option standardmäßig aktiviert.
Profil aus Backup nicht verwenden	Wenn aktiviert, verwendet das Gerät dieses Profil nicht, wenn Sie das Gerät aus einer Sicherung wiederherstellen. Gilt nur für iOS 26+- und visionOS 26+-Geräte.
Kopplung zulassen	(Gilt nicht für iOS 13+ und macOS 10.15+) Ermöglicht Hostkopplungsfunktionen (Pairing), z. B. die iTunes-Synchronisierung. Die Kopplung wird für Hosts mit gültigem Kopplungszertifikat immer zugelassen.
Wiederinbetriebnahme	Setzen Sie **Wiederinbetriebnahme** auf **wahr**, um sicherzustellen, dass die Anwendung erhalten bleibt, wenn die Aktion **Wiederinbetriebnahme** ausgeführt wird. Dies ermöglicht dem Gerät das Erstellen einer Momentaufnahme der Anwendungen sowie das Bereitstellen einer schnelleren Wiederinbetriebnahme. Wenn

Einstellung	Aktion
	das deaktivierte Gerät weiterhin die Funktion "Wiederinbetriebnahme" ausführen kann, muss die Anwendung während des Neuregistrierungsprozesses erneut heruntergeladen werden. Zur Nutzung der Funktion **Apple Migration ABM** muss diese Funktion deaktiviert werden. Das Gerät kann nicht migriert werden, wenn **Wiederinbetriebnahme** aus **wahr** gesetzt ist. Gilt nur für iOS 26+- und visionOS 26+-Geräte.
Zertifikat	Klicken Sie auf **Hinzufügen**, um Zertifikate hochzuladen.
Support-Telefonnummer	Geben Sie eine Telefonnummer an, die Benutzer anrufen können, wenn sie Hilfe benötigen.
E-Mail-Adresse für den Support	Geben Sie eine E-Mail-Adresse an, an die sich Gerätebenutzer wenden können, wenn sie Hilfe benötigen.
Benutzerdefinierte Registrierung	(iOS 13.0+ und macOS 10.15+) Benutzerdefinierte Anmeldungs-Webseite(n) erstellen Geben Sie Ihre selbst angepasste Webseite (Webansicht) an, um Benutzer während der Geräteregistrierung zu authentifizieren. Verwenden Sie diese Seite, um benutzerdefinierte Informationen wie Authentifizierungsart, Branding, Zustimmungstext und Datenschutzrichtlinie anzuzeigen. Weitere Einzelheiten zu dieser Prozedur finden Sie im Abschnitt *Benutzerdefinierte Webseite zur Geräteregistrierung hinzufügen*. • Wählen Sie **Benutzerdefinierte Registrierung** aktivieren, um diese Funktion zu aktivieren. • Geben Sie die **URL**ein, z. B. https://mycustomweburl.com. Diese URL definiert den Wert der benutzerdefinierten URL, die dem Benutzer in einer Web-Ansicht angezeigt werden soll.
Mehrere Benutzer	(iOS 13.4+) Gemeinsam genutztes iPad für Unternehmen Bei gemeinsam genutzten iPads kann das Unternehmen Geräte für mehrere Mitarbeiter gemeinsam nutzen und trotzdem ein personalisiertes Erlebnis zu bieten. Wählen Sie den **Mehrbenutzermodus**, um einen gemeinsam genutzten iPad auf einem Gerät zu aktivieren. Shared iPad.htmWeitere Informationen finden Sie unter Gemeinsam genutztes iPad für Unternehmen. • Diese Einstellung gilt nicht für Apple Education. • Wählen Sie die Einstellung **Überwachter Modus**, um die Mehrbenutzereinstellung zu ändern.
Quotengröße	(iOS 13.4+) Gemeinsames iPad für Unternehmen Der Wert wird in Megabyte (MB) angegeben und bezeichnet den einem Benutzer zugeteilten Speicherplatz auf einem Gerät. Wenn der Wert zu klein ist, wird vom Gerät eine Standardkontingentgröße zugeteilt.
Residente Benutzer	(iOS 13.4+) Gemeinsam genutztes iPad für Unternehmen Der Wert gibt die Anzahl der Benutzer an, die auf dem Gerät genutzt oder gespeichert werden können. Wenn der Wert größer ist als die maximale Anzahl der Benutzer, die das Gerät unterstützt, verwendet der MDM-Server diesen Wert (maximale Anzahl der Benutzer) als Standard. Administratoren können entweder die Kontingentgröße oder den Wert für residierende Benutzer angeben. Wenn beide Werte angegeben werden, verwendet der MDM-Server die Kontingentgröße als Standard.

Einstellung	Aktion
Zeitüberschreitung der Benutzersitzung	(iOS 14.5+) Gemeinsames iPad für Unternehmen Zeigt die Zeitüberschreitung für eine Benutzersitzung in Sekunden an. Die Benutzersitzung wird nach der angegebenen Inaktivitätsdauer automatisch abgemeldet. Der Mindestwert beträgt 30 Sekunden. Wenn dieser Wert auf 0 gesetzt wird, wird die Zeitüberschreitung aufgehoben und die Standardzeitüberschreitung des Geräts verwendet. Werte von 1 bis 29 sind ungültig. Wenn diese Option gesetzt ist, wird das Gerät auf den Standard-Zeitüberschreitung eingestellt.
Temporäre Sitzungszeitüberschreitung	(iOS 14.5+) Gemeinsames iPad für Unternehmen Zeigt die Zeitüberschreitung in Sekunden für eine Gast- oder temporäre Sitzung an. Die temporäre Sitzung wird nach der angegebenen Inaktivitätsdauer automatisch abgemeldet. Der Mindestwert beträgt 30 Sekunden. Wenn Sie den Wert auf 0 setzen, wird die Zeitüberschreitung aufgehoben und auf die Standardzeitüberschreitung des Geräts gesetzt. Werte von 1 bis 29 sind ungültig. Wenn diese Option gesetzt ist, wird das Gerät auf den Standard-Zeitüberschreitung eingestellt.
Nur temporäre Sitzung	(iOS 14.5+) Gemeinsames iPad für Unternehmen Wenn dies der Fall ist, sieht der Benutzer nur den Willkommensbereich für Gäste und kann sich nur als Gastbenutzer anmelden. Wenn die Einstellung „false“ ist, kann sich der Benutzer mit einer verwalteten Apple-ID anmelden (Verhalten wie bisher). Voreinstellung: false
Verwaltete Standarddomänen für die Apple-ID	(ab iOS 16) Gemeinsames iPad für Unternehmen Geben Sie eine Liste von Domänen an. Benutzer können ihre Kontodomäne aus der Liste der Domänen auf der QuickType-Tastatur auswählen.
Toleranzperiode für die Onlineauthentifizierung	(ab iOS 16.0) Gemeinsames iPad für Unternehmen Geben Sie über die Anzahl der Tage an, wie häufig sich der Benutzer ohne Verbindung zum Netzwerk anmelden kann. Wenn Sie diesen Wert auf Null setzen, ist jedes Mal eine Online-Authentifizierung erforderlich. **Standard**: 0
Zeit bis zur automatischen Sperrung	(iOS 17.0+) Geben Sie die Zeit (in Sekunden) an, nach deren Ablauf das Gerät in den Energiesparmodus wechselt. Der Mindestwert beträgt 120 Sekunden.
Zeit bis zur Passcodesperre	Geben Sie die Zeit (in Sekunden) an, nach deren Ablauf der Benutzer den Gerätepasscode eingeben muss, um das Gerät zu entsperren. Der Mindestwert beträgt 0 Sekunden, der Höchstwert 14.400 Sekunden.
Zeitzone	Geben Sie die gewünschte Zeitzone für das Gerät an. **Beispiel**: Pacific/Midway

Setupoptionen

- Passcodeeingabe überspringen - Bei Auswahl dieser Option werden auch die Optionen „Apple Pay Setup überspringen“ und „Touch-ID überspringen“ automatisch aktiviert.
- Standortdienste überspringen
- „Aus Sicherung wiederherstellen“ überspringen
- Die Option „Verschieben nach iOS“ von Android überspringen
- Nutzungsbedingungen überspringen
- Signierung mit Apple-ID und iCloud überspringen – bei Auswahl dieser Option wird die Option "Apple Pay Setup überspringen" automatisch aktiviert.
- Touch-ID-Setup überspringen (nur iPhone 5s, 6, 6+, iPad Air 2, iPad Mini 3) – bei Auswahl dieser Option wird die Option "Apple Pay Setup" automatisch aktiviert.
- Apple Pay-Setup überspringen (nur iPhone 6, 6+, iPad Air 2, iPad Mini 3)
- Zoom-Setup überspringen
- Siri überspringen
- Intelligence überspringen (iOS 18+ und macOS 15+)
- Automatisches Senden von Diagnoseinformationen überspringen
- Cloud-Speicher überspringen (iOS 10.3 & macOS 10.13.4+)
- Anzeigeton-Setup überspringen (iOS 9 & macOS 10.14+)
- Empfindlichkeit der Home-Taste überspringen
- Tastaturauswahlbildschirm überspringen
- Onboarding-Infobildschirme überspringen - Diese Informationen sind für den Benutzer vorgesehen. Beispiel: Deckblatt, Multitasking und Systemsteuerung
- Bildschirm für die Apple Watch-Migration überspringen
- Auswahl des Look-Bildschirms (iOS 13.0+ & macOS 10.14+) überspringen
- Bildschirmzeit überspringen (iOS 12.0+ & macOS 10.15+)
- Privatsphäre überspringen (macOS 10.13.4 & tvOS 11.3+)
- "Sperrmodus aktivieren" überspringen (iOS 17.1+ und macOS 14.0+)
- Softwareupdate überspringen (iOS 12.0+ und macOS 15.4+)
- Anzeige „Mobilfunkktarif hinzufügen“ überspringen (iPhone Xs, iPhone Xs Max, iPhone XR)
- Zeigt kundenspezifischen Text auf der Anmeldeseite – wählen Sie diese Option, um eine kundenspezifische Textnachricht in dem Textfeld einzugeben. Diese Meldung wird bei der Einrichtung der Geräteregistrierung auf der Anmeldeseite des Geräts angezeigt, um den Endbenutzern zusätzliche Anweisungen zu geben, die sie durch den Prozess führen.
- Automatische Vorauswahl - Wählen Sie diese Option, um den Assistenten so einzurichten, dass er automatisch die Bildschirme zur Geräteeinrichtung aufruft. Der Standardwert ist auf „false“ gesetzt. Unterstützt unter tvOS und macOS 11 und höher. Die automatische Vorauswahl funktioniert nicht bei einer WLAN-Verbindung, das Gerät sollte über Ethernet angeschlossen sein.
- Adressbedingungen: Überspringt den Bereich "Adressbedingungen". (ab iOS 16)
- Liquid Glass-Bereich überspringen (iOS 27.0+ und macOS 27.0+)

Setupoptionen
iOS-
• Fenster „Erste Schritte überspringen“ (13.0+) • iMessage & FaceTime überspringen (12.0+) • Gesprochene Sprache überspringen (13.0+) • „Wiederherstellung überspringen“ abgeschlossen (14.0+) • „Update überspringen“ abgeschlossen (14.0+) • Sicherheit überspringen (16.0+) • Bereich "Aktionsschaltfläche einrichten" überspringen (17.0+) • Filterbereich für Webinhalte überspringen (18.2+) • "Sicherheit & Verarbeitung" überspringen (18.4+) • Bereich "Multitasking" überspringen (26.0+) • Bereich "Betriebssystemvorstellung" überspringen (26.0+) • Bereich für Barrierefreiheit-Erscheinungsbild überspringen (27.0+) **macOS** • iCloud Analytics-Bildschirm überspringen • True Tone Display-Bildschirm überspringen (10.13.6+) – (Optional) Wählen Sie diese Option, um das Fenster "True Tone Display" zu überspringen. • Barrierefreiheit überspringen (11.0+) • Entsperrung mit Watch überspringen (12.0+) • "Sperrmodus aktivieren" überspringen (14.0+) • Hintergrundauswahl überspringen (14.1+) • Bereich "Zusätzliche Datenschutzeinstellungen" überspringen (26.0+) • "Update abgeschlossen" überspringen (26.0+) **tvOS**
• Synchronisationsbildschirm für Apple TV-Begrüßungsbildschirm überspringen • Anbieter-Anmeldebildschirm für Apple TV überspringen • Option "Für Setup tippen" überspringen. • Aerial-Bildschirmschoner-Setup überspringen
Optionen des Setup-Assistenten für das macOS-Konto
• Erstellung des Administratorkontos überspringen • Erstellung des primären Setupkontos überspringen • Primäre Konten als regulärer Benutzer erstellen (als Administrator, falls nicht aktiviert)
Gerätekonfiguration während des Device Enrollment Setups abwarten

Setupoptionen
• Warten, bis Konfigurationen und Anwendungen mit hoher Priorität per Push an Geräte übertragen wurden - Wählen Sie diese Option, um die Konfigurationen sowie Anwendungen mit hoher Priorität an das Gerät zu übertragen, bevor Sie mit den restlichen Setup-Bildschirmen für die Geräteregistrierung fortfahren. Diese Einstellung bewirkt, dass der Endbenutzer das Gerät erst verwenden kann, nachdem die erforderlichen Konfigurationen und Anwendungen mit hoher Priorität per Push an das Gerät übertragen wurden. • Zeitlimit - Das Standardlimit beträgt 3 Minuten. Die maximale Zeit beträgt 10 Minuten. Wählen Sie zur Aktivierung dieser Funktion beim Bearbeiten des Geräteeintragungsprofils die Option **Überwachter Modus**.

Klicken Sie auf **Speichern**.

Die folgende Tabelle wird auf der Seite **Admin** > **Apple** > **Geräteregistrierung** ausgefüllt:

Einstellung	Aktion
[Name] (Klicken Sie auf die Spaltenüberschrift, um die Spalte alphanumerisch zu sortieren.) Über das Feld "Suchen" können Sie nach Elementen in dieser Spalte suchen.	MDM-Servername
Kontoname (Klicken Sie auf die Spaltenüberschrift, um die Spalte alphanumerisch zu sortieren.) Über das Feld "Suchen" können Sie nach Elementen in dieser Spalte suchen.	Verwaltete Apple-ID
Anzahl der Geräte	Anzahl zugewiesener Geräte
Registrierungsprofil(e)	Anzahl der Registrierungsprofile für zugewiesene Geräte
Letzte Synchronisierung (Klicken Sie auf die Spaltenüberschrift, um die Spalte alphanumerisch zu sortieren.)	Zuletzt kontaktiert um
Token abgelaufen (Klicken Sie auf die Spaltenüberschrift, um die Spalte alphanumerisch zu sortieren.)	Ablaufdatum des Tokens

- Ivanti Neurons for MDMWenn neue Geräte im Device Enrollment von Apple ergänzt werden, kann es bis zu 15 Minuten dauern, bis die Cloud diese neuen Geräte erkennt. Die neuen Geräte werden dann einem Registrierungsprofil zugeordnet. Wenn Sie keine neuen Geräte im Geräte-Registrierungsprogramm hinzufügen können, gehen Sie zu **Dashboard > Benachrichtigungen**, um die Benachrichtigungen von Apple für das Device Enrollment Program zu kontrollieren. Wenn EULA-Aktualisierungen verfügbar sind, informiert Sie eine E-Mail, mit welchen Schritten Sie die neue EULA akzeptieren können.
- Sie können alle kundenspezifischen Geräteattribute anzeigen, die bei Ihrem Mandanten existieren, und diese den Geräten bei der Registrierung über Apple Device Enrollment zuweisen.
- Auf gemeinsam genutzten macOS-Geräten wird über den Befehl ListUsers eine Liste aller lokalen Benutzer auf dem Gerät angezeigt und nur die letzten Check-in-Details des Benutzers, der das Gerät registriert hat.

Geräteeintragungsprofil bearbeiten

Verfahren

1. Gehen Sie zuAdministration>Apple>Device Enrollment.
2. Suchen Sie den Namen des Apple Business Manager-Servers (den Sie auf der Apple-Website erstellt haben) in der Spalte „Apple Account Name“.
3. Klicken Sie auf den Zahlenlink in der Spalte Enrollment Profile(s).
4. Wählen Sie für ein bestimmtes ProfilAktionen>Device Enrollment Profile bearbeiten.
5. Aktualisieren und speichern Sie das Profil.

- Wenn ein Device Enrollment Profile bearbeitet wird, wird der Gerätezähler für das geänderte Profil umgehend aktualisiert.
- Wenn Sie das Server-Token auf der Apple-Seite aktualisieren, wird das vorhandene Token ungültig. Allerdings bleiben die Anzeige auf der Geräteregistrierungsseite und das Ablaufdatum des Tokens bestehen, bis Sie das neue Token hochladen.
- Wenn ein Geräteregistrierungsprofil erstellt oder bearbeitet wurde, können die am Profil vorgenommenen Änderungen im Abschnitt "Audit-Protokolle" angezeigt werden. Durch Klicken auf den Link unter "Details" werden die Attribute und die daran vorgenommenen Änderungen in den Spalten "Vorher" und "Nachher" angezeigt. Sie können die folgenden Status der einzelnen Geräteregistrierungsprofile überprüfen: "Erstellt" (für ein neues Profil), "Aktualisiert" (für ein bearbeitetes Profil) oder "Gelöscht" (für ein gelöschtes Profil). Zum Filtern der Geräteregistrierungsprofile unter "Audit-Protokolle" müssen Sie die Kategorie "Admin-System" auswählen und als Typ "Automatische Geräteregistrierung" angeben.

Das Geräteregistrierungsprofil enthält folgende Angaben:

Einstellung	Aktion
Profil (Klicken Sie auf die Spaltenüberschrift, um die Spalte alphanumerisch zu sortieren.)	Geben Sie einen Namen ein, der dieses Device Enrollment Profil bezeichnet.
Beschreibung (Klicken Sie auf die Spaltenüberschrift, um die Spalte alphanumerisch zu sortieren.)	Geben Sie eine Beschreibung für das Profil ein.
Abteilung (Klicken Sie auf die Spaltenüberschrift, um die Spalte alphanumerisch zu sortieren.)	Geben Sie die Abteilung in Ihrer Organisation ein, die im Zusammenhang mit diesem Profil steht.
Support-Telefonnummer (Klicken Sie auf die Spaltenüberschrift, um die Spalte alphanumerisch zu sortieren.)	Geben Sie eine Telefonnummer an, die Benutzer anrufen können, wenn sie Hilfe benötigen.
Anzahl der Geräte	Zeigt die Anzahl der Geräte für das Profil an.
Aktionen	Profile verwalten

Mehrere Device Enrollment Profile verwalten

Sie können mehrere Device Enrollment Profiles für jeden Apple Business Manager-Server erstellen. Auf diese Weise können verschiedene Gerätesätze unterschiedliche Konfigurationen erhalten. Geräte können auch von einem Device Enrollment Profile in ein anderes verschoben werden.

Verfahren

1. Gehen Sie zuAdministration>Apple>Device Enrollment.
2. Suchen Sie den Namen des Apple Business Manager-Servers in der Spalte „Apple Account Name“.
3. Klicken Sie auf den Zahlenlink in der Spalte Enrollment Profile(s).
4. Um ein neues Device Enrollment Profile zu erstellen und mit dem ausgewählten Server zu verknüpfen, klicken Sie auf **Neues Profil erstellen**. Erstellen und speichern Sie das Profil.

5. Um jedes Profil zu verwalten, klicken Sie auf **Aktionen** und wählen Sie eine der folgenden Optionen:
    - Als Standardprofil festlegen – Legen Sie das Profil als Standardprofil innerhalb desselben virtuellen Servers fest. Neue Geräteregistrierungen erhalten dieses Standardprofil.
    - Profil bearbeiten – Vorhandenes Profil aktualisieren.
    - **Authentifizierung bearbeiten** - Bearbeitet die Authentifizierungseinstellung der Geräteregistrierung.
    - **Geräteattribut Geräteregistrierung zuweisen** - Administratoren verwenden benutzerdefinierte Attribute für Geräte, um diesen Objekten zusätzliche Eigenschaften zuzuordnen. Diese Eigenschaften können dann zur Definition von Gruppen oder zur Verteilung von Konfigurationen genutzt werden.
    - Löschen – Das Standardprofil kann nicht gelöscht werden. Wenn ein Nicht-Standardprofil gelöscht wird, werden alle zugehörigen Geräte wieder dem Standardprofil zugeordnet.
6. Um ein registriertes Gerät von einem Profil zu einem anderen Profil auf demselben virtuellen Server (und nicht zwischen verschiedenen Apple Business Manager-Servern) zu verschieben, klicken Sie auf den Zahlenlink unter der Spalte „Anzahl der Geräte“. Die Neuzuweisung von Profilen gilt für Geräte, die noch nicht registriert sind.
    1. Um ein einzelnes Gerät zu verschieben, klicken Sie für das spezifische Gerät auf **Registrierungsprofil zuweisen**, wählen das Profil aus der Dropdown-Liste und klicken auf **Zuweisen**.
    2. Um mehrere Geräte zu verschieben, wählen Sie die Geräte aus und klicken Sie auf Aktionen> Registrierungsprofil zuweisen, wählen das Profil aus der Dropdown-Liste und klicken Sie aufZuweisen.

- Wenn ein Device Enrollment Profile bearbeitet wird, wird die Geräteanzahl für das geänderte Profil umgehend aktualisiert.
- Wenn Sie das Server-Token auf der Apple-Seite aktualisieren, wird das vorhandene Token ungültig. Allerdings bleiben die Anzeige auf der Geräteregistrierungsseite und das Ablaufdatum des Tokens bestehen, bis Sie das neue Token hochladen.

Benutzerdefinierte Webseite zur Geräteregistrierung hinzufügen

Gilt für: iOS 13.0 und macOS 10.15 und unterstützte neuere Versionen

Im Abschnitt „Benutzerdefinierte Registrierung“ können Sie selbst eine benutzerdefinierte Webseite (Webansicht) angeben, um Benutzer während der Geräteregistrierung zu authentifizieren. Verwenden Sie diese Seite, um benutzerdefinierte Informationen wie Authentifizierungsart, Branding, Zustimmungstext und Datenschutzrichtlinie anzuzeigen.

Verfahren

1. Gehen Sie zuAdministration>Apple>Device Enrollment.
2. Suchen Sie nach dem Server-Namen, den Sie auf der Apple-Site erstellt haben.
3. Wählen SieAktionen>Geräteeintragungsprofil bearbeiten.
4. Wählen Sie im Abschnitt „Benutzerdefinierte Registrierung“ die Option **Benutzerdefinierte Registrierung aktivieren**.
5. Wählen Sie eine der folgenden Optionen aus:
    - Bei MobileIron gehostete Webseite– Wird an einen Identitätsprovider (IDP) umgeleitet, wenn die Registrierung über einen Identitätsprovider wie Microsoft Active Directory Federation Services (ADFS) oder Okta erfolgt. Sie kann für einen Ivanti Neurons for MDM Benutzer mit einer nicht-IDP-Authentifizierung auch auf das Selbstbedienungsportal umgeleitet werden.
    - **Benutzerdefinierte URL** - geben Sie eine URL wie https://mycustomweburl.com ein. Diese URL definiert den Wert der benutzerdefinierten URL, die dem Benutzer in einer Web-Ansicht präsentiert wird, die während der Ersteinrichtung eines

neuen Geräts oder eines gelöschten Gerätes für die Geräteregistrierung geladen wird. Verwenden Sie dieses Feld, um Ihre eigene Authentifizierungs-Benutzeroberfläche mit Authentifizierungsmethode zu definieren. Nachdem der Benutzer authentifiziert wurde, wird das MDM-Registrierungsprofil heruntergeladen.

Arbeitsablauf der benutzerdefinierten Webseite zur Geräteregistrierung

In diesem Abschnitt werden das Verhalten der benutzerdefinierten Geräteregistrierungs-Webseite und das Verfahren zur Erstellung der benutzerdefinierten Webseite (Webansicht) erläutert.

Wenn die im Feld **URL** angegebene benutzerdefinierte Webseite erstmals geladen wird:

- Hat die Konfigurations-Web-URL ein **https**-Schema und ist eine **GET**-Anforderung. Die Webseite sollte ein öffentliches, vertrauenswürdiges Zertifikat verwenden.
- Ein benutzerdefinierter Header **x-apple-aspen-deviceinfo** wird von dem Apple-Gerät, auf dem die Registrierung eingeleitet wird, an die GET-Anforderung angehängt. Er enthält eine Base64-Kodierung eines CMS-Envelope (Cryptographic Message Syntax Envelope), der wiederum eine plist mit Geräteattributen enthält. Es handelt sich dabei um dieselben Informationen in dem gleichen Format, das bei Geräteregistrierungen mit Token in der erstmaligen POST-Anforderung bereitgestellt wurde.

Wenn anschließend die benutzerdefinierte Webseite geladen wird:

- Der Gerätebenutzer interagiert mit der Webseite (Webansicht), bis der Host-Server des Administrators dem Client eine Datei custom.mobileconfig zur Verfügung stellt.Der Ivanti Neurons for MDM Server gibt den Bytecode des MDM-Profils zurück. Auf dem Host-Server des Administrators sollte für die Datei custom.mobileconfig ein MIME-Typ **application/x-apple-aspen-config** eingestellt werden, so dass das MDM-Profil für das Gerät heruntergeladen und auf dem Gerät installiert wird.
- Zur Authentifizierung mit der Ivanti Neurons for MDM sollte die Webseite den Authentifizierungs-Benutzernamen und das Passwort enthalten. Es sollte ein separater Benutzer in der Ivanti Neurons for MDM erstellt und dem Benutzer, der das MDM-Profil mit der Ivanti Neurons for MDMServer-URL abruft (z. B. https://micloudDomain.com/c/i/dep/custom.mobileconfig), die Rolle „Benutzerdefinierte Registrierung“ zugewiesen werden.
- Für die Geräteregistrierung und zum Abruf des MDM-Profils aus der Ivanti Neurons for MDM sollte der Host-Webserver des Administrators einen POST-Aufruf an die Ivanti Neurons for MDM Server-URL senden. Außerdem sollte er den Header „x-apple-aspen-deviceinfo“ mit dem Wert übergeben, den das Gerät liefert, wenn das Gerät die GET-URL findet, um die benutzerdefinierte Webseite zu laden. Wenn die Registrierungs-Benutzer-ID nicht angegeben ist, wird das Gerät auf den Benutzer „nobody“ registriert. Hier die zusätzlichen Details:
  - Wenn ein Gerät die benutzerdefinierte Web-URL findet, die im Geräteregistrierungsprofil konfiguriert ist, sollte der Host-Webserver des Administrators den vom Gerät angezeigten Header „x-apple-aspen-deviceinfo“ erfassen.
  - Um das MDM-Profil für dieses Gerät und den zugehörigen Benutzer zu erhalten, sollte der Host-Webserver des Administrators einen POST-Aufruf an die Ivanti Neurons for MDM Server-URL mit dem Header „x-apple-aspen-deviceinfo“ senden. Er sollte eine Basisauthentifizierung mit einer Ivanti Neurons for MDM Benutzer-ID als Anfrageparameter enthalten (z. B. https://miCloudDomain.com/c/i/dep/custom.mobileconfig?user=name@company.com). Dem Benutzer sollte die Rolle der benutzerdefinierten Registrierung zugewiesen werden.
  - Sobald der Host-Webserver des Administrators den Bytecode erhalten hat, sollte er den Bytecode auf das Gerät herunterladen, indem er die Antwort-Header Content-Disposition = attachment;filename=„profile.mobileconfig“ und Content-Type = application/x-apple-aspen-config setzt.
- Die Webansicht wird geschlossen und das Betriebssystem versucht, das Profil zu installieren; dazu muss es ein MDM-Anmeldeprofil sein.

> Ivanti Neurons for MDM authentifiziert nicht die Benutzer-ID, für die das MDM-Profil zurückgegeben wird. Daher sollten Administratoren die erforderliche Authentifizierung für die Benutzer-ID durchführen, bevor sie das MDM-Profil anfordern.

Für iOS wird dieser Workflow bei der Ersteinrichtung eines gelöschten Geräts unterstützt. Für macOS wird dieser Workflow sowohl im Setup-Assistenten als auch über die Einstellungskarte „Profile“ unterstützt, wenn die Geräteregistrierung im Setup-Assistenten übersprungen wurde.

Informationen für Entwickler zur Erstellung einer benutzerdefinierten Webseite finden Sie in den folgenden Verweisen der Apple-Dokumentation:

- **Web-Ansichten**
- **Authentifizierung durch Web-Ansichten**
- **Beispielcode zur Implementierung eines einfachen iPad-Webbrowsers, der entweder die Desktop- oder die mobile Version einer Website anzeigen kann.**

Authentifizierungseinstellung für die Geräteregistrierung bearbeiten

Verfahren

1. Gehen Sie zuAdministration>Apple>Device Enrollment.
2. Suchen Sie nach dem Server-Namen, den Sie auf der Apple-Site erstellt haben.
3. Wählen SieAktionen>Authentifizierung bearbeitenaus.

Bootstrap-Token-Verwaltung für mobile Konten

Gilt für:macOS 10.15-Geräte und unterstützte neuere Versionen, die über den Apple School Manager oder Apple Business Manager im MDM registriert sind.

Ivanti Neurons for MDM Cloud unterstützt die Bootstrap-Token-Verwaltung für mobile Konten. Mit Bootstrap-Token können sich mobile Konten bei MacOS-Geräten anmelden, die FileVault verwenden. Mit dieser Funktion erhalten alle mobilen Konten, die sich anmelden, automatisch ein SecureToken. Diese Funktion ist vorteilhaft, wenn sich mehrere Benutzer an einem verschlüsselten Rechner anmelden.

Wenn ein verwaltetes Administratorkonto versucht, sich bei einem Gerät anzumelden:

- Wird bei der ersten Anmeldung das Bootstrap-Token vom MDM-Server angefordert.
- Wenn der MDM-Server das Bootstrap-Token bereitstellt, erstellt das Gerät automatisch ein SecureToken für das Konto.
- Das Gerät aktiviert FileVault für den Benutzer.

„Bootstrap-Token verfügbar“ ist ein Feld auf der Seite „Gerätedetails“ und ein Filterattribut beim Erstellen einer neuen Gerätegruppe oder einer benutzerdefinierten Richtlinie.

Gehen Sie zur Fehlerbehebung und Überprüfung zur Seite mit den Gerätedetails eines Geräts. Verwenden Sie die Seite „Protokolle“, um die Geräteprotokolle mit Filtern für den Aktionsnamen auf „Bootstrap-Token setzen“ und „Bootstrap-Token holen“ einzugrenzen.

Verwaltetes MacOS-Verwaltungskonto mit Device Enrollment einrichten

Die Ivanti Neurons for MDM unterstützt die DEP-Registrierung bei Geräten, die auf die Werkeinstellungen zurückgesetzt wurden oder erstmalig aktiviert werden. Mit Device Enrollment kann ein Administratorkonto auf dem macOS-Gerät erstellt werden.

Ivanti Neurons for MDMIvanti Neurons for MDMDie Cloud unterstützt nur die optionale Registrierung für macOS; daher ignoriert die Cloud das Feld MDM vorgeschrieben im DEP-Profil, weil dieses nur iOS-Geräte betrifft.

Verfahren

1. Gehen Sie zu **Administration > Device Enrollment** .
2. Suchen Sie nach dem Server-Namen, den Sie auf der Apple-Site erstellt haben.
3. Wählen Sie **Aktionen > Geräteeintragungsprofil bearbeiten**.
4. Wählen Sie eine der folgenden Optionen aus den Optionen des macOS-Konto-Setup-Assistenten aus:
    - **Administrator-Kontoerstellung überspringen** - Wählen Sie diese Option, um die Erstellung eines sichtbaren oder unsichtbaren Administrator-Kontos zu verhindern. Deaktivieren Sie diese Option, wenn ein Administrator-Konto in dem Abschnitt **Verwaltetes macOS-Administrator-Konto definieren** möglich sein soll (siehe folgende Beschreibung).
    - **Primäre Setup-Kontoerstellung überspringen** - Wählen Sie diese Option, um die Konfiguration des Primärkontos auf dem macOS-Gerät zu überspringen. Außer dem Administratorkonto wird kein Benutzerkonto erstellt. Es wird ein weiterer Abschnitt **Verwaltetes macOS-Administratorkonto konfigurieren** angezeigt (Beschreibung weiter unten), um ein verwaltetes macOS-Administratorkonto zu erstellen. Das Konto kann bei den Benutzern & Gruppen auch ausgeblendet werden.
    - Primäre Konten für reguläre Benutzer erstellen (wenn diese Option nicht aktiviert ist, als Administrator) – Wählen Sie diese Option, um ein Nicht-Administrator-Standardkonto bei der Registrierung zu erstellen. Ein Administrator kann trotzdem ein Administratorkonto erstellen und per Push auf das Gerät übertragen. Es wird ein weiterer Abschnitt **Verwaltetes macOS-Administratorkonto konfigurieren** angezeigt (Beschreibung weiter unten), um ein verwaltetes macOS-Administratorkonto zu erstellen. Das Konto kann bei den Benutzern & Gruppen auch ausgeblendet werden.

Geben Sie nach Auswahl einer der oben erwähnten Optionen die folgenden Details in dem Abschnitt **Verwaltetes macOS-Administratorkonto konfigurieren** ein, wenn Sie ein verwaltetes macOS-Administratorkonto erstellen wollen:

- Vollständiger Name
- Kontoname
- Passwort
- Passwort bestätigen
- (Optional) Verwaltetes Administratorkonto in den Benutzern & Gruppen verbergen

Wenn Sie die Option **Erstellung des primären Einrichtungskontos überspringen** nicht auswählen, geben Sie die folgenden Details im Abschnitt **Primäres Konto einrichten** ein. Damit wird die Benutzer-Channel-Unterstützung für das verwaltete Administratorkonto hinzugefügt, indem der Kurzname des verwalteten lokalen Benutzers als Kurzname eines Administrators übernommen wird.

- **Vollständiger Name**
- **Kurzname**
- (Optional) **Änderung durch Endbenutzer verhindern** - Diese Einstellung wird überschrieben, wenn für „Vollständiger Name“ und/oder „Kurzname“ Substitutionsvariablen existieren, die bei Prüfung leer sind. Wenn Sie diese Option wählen, bestätigen Sie, dass die Einrichtung dieses primären Administratorkontos nur anwendbar ist, wenn eine der unten aufgeführten Optionen entsprechend eingestellt ist:
    1. Benutzerregistrierung/Anmeldung wird in der Ansicht Authentifizierungs-Setup ausgewählt.
    2. Die von MobileIron gehostete Webseite wird für die Anpassung der Registrierung ausgewählt.

7. Wählen Sie **Erstellung des primären Einrichtungskontos überspringen**, um den Benutzerkanal-Support für das verwaltete Administratorkonto zu aktivieren. Sie können als Kurznamen eines verwalteten lokalen Benutzers den Kurznamen eines

Administrators verwenden.
8. Klicken Sie auf **Speichern**.

Ändern des Kontopassworts für den lokalen macOS Administrator

Ein Administrator kann das lokale Passwort eines lokalen macOS-Administratorkontos ändern, das während der DEP-Registrierung vom Setup-Assistenten erstellt wurde.

Gilt für: macOS 10.11 oder unterstützte neuere Versionen.

Verfahren

1. Gehen Sie zu **Geräte**.
2. Klicken Sie auf den Benutzernamen, dem das Gerät zugeordnet ist, um die Gerätedetailseite anzuzeigen.
3. Klicken Sie im Menü „Aktionen“ aufmacOSAdmin-Passwort einstellen. Sie können diese Aktion auf der Gerätelisteseite oder durch Auswahl eines oder mehrerer Geräte ausführen.
4. Geben Sie das Passwort ein.
5. Klicken Sie auf **Speichern**.

Als CSV-Datei exportieren

Ivanti Neurons for MDM unterstützt Sie beim Exportieren der Geräte des Typs "Registriertes Gerät" in eine CSV-Datei.

Verfahren

1. Gehen Sie zu Administration > Device Enrollment .
2. Klicken Sie in der Spalte **Anzahl der Geräte** auf den jeweiligen Link zum Zählen der Geräte.
3. Klicken Sie auf die Option **Als CSV-Datei exportieren**, um die Geräteliste und die verknüpften Details in eine CSV-Datei zu exportieren. Sobald der Bericht bereitsteht, werden Sie mit einer Meldung aufgefordert, den Bericht herunterzuladen oder zu löschen. Der Administrator erhält außerdem eine E-Mail mit einem Link zum Herunterladen des Berichts.
4. Klicken Sie auf **Herunterladen**.
5. (Optional) Klicken Sie zum Löschen des Berichts auf **Löschen**.

12.3.4. Beta-Registrierung

Ivanti Neurons for MDM kann Geräte per Remotezugriff automatisch zu einem späteren Zeitpunkt registrieren, wenn das Gerät überwacht und darauf iOS 18, iPadOS 18, macOS 15 oder eine spätere Version ausgeführt wird. Bei Bedarf kann ein überwachtes Gerät aus einem Beta-Programm entfernt und die manuelle Registrierung durch einen Benutzer unterbunden werden. Dadurch muss der Benutzer keine manuellen Schritte durchführen und der Prozess wird für den gesamten Lebenszyklus des Beta-Tests optimiert.

Voraussetzungen

- Die Geräteregistrierung ist für die Beta-Registrierung verpflichtend. Weitere Informationen zur Geräteregistrierung finden Sie unter Geräteregistrierung.
- Um Beta-Versionen von AppleSeed for IT ohne Erfordernis eines Apple-Kontos anzubieten, muss sich ein Administrator in Apple Business Manager oder Apple School Manager am AppleSeed for IT-Portal anmelden und die Geschäftsbedingungen im Namen seines Unternehmens für die aktuelle Beta-Laufzeit akzeptieren.

Verbinden von Ivanti Neurons for MDM für die Beta-Registrierung

Um Ivanti Neurons for MDM als MDM-Server für die Beta-Registrierung zu verwenden, richten Sie das Apple Business Manager- oder Apple School Manager-Server-Token unter Ivanti Neurons for MDM ein.

Abschnitt "Beta-Registrierung"

[Name]	Beschreibung
Name des Unternehmens	Der Name des Unternehmens.
Letzte Synchronisierung	Datum und Uhrzeit der Synchronisierung.
[Status]	Der Status der Synchronisierung.
Synchronisierung Beta-Registrierungstoken	Klicken Sie auf **Synchronisieren**, um die neu verfügbaren Beta-Registrierungstokens für Beta-Updates zu synchronisieren.

12.3.5. Konfigurieren von Setup Assistant

Mit dem Konfigurations-Setup Assistant wählen Sie die Bildschirme aus, die beim Gerätesetup für iOS- und macOS-Geräte übersprungen werden sollen.

Verfahren

1. Melden Sie sich bei der Ivanti Neurons for MDM-Administrationskonsole an.
2. Gehen Sie zu **Konfigurationen**.
3. Wählen Sie **Setup Assistant** aus.
4. Klicken Sie zum Bearbeiten auf das Stiftsymbol.
5. Markieren Sie die Kontrollkästchen, um die jeweiligen Einrichtungsbildschirme auf dem Gerät zu überspringen.
6. Klicken Sie auf **Fertig**.
7. Wählen Sie **Gerätekanal** aus.
8. Wählen Sie **Alle Geräte** aus. Die Setup Assistant-Konfiguration wird via Push an die Geräte übertragen und auf der Registerkarte "Konfiguration" der Seite "Gerätedetails" wird der Status "Installiert" angezeigt.
9. Melden Sie sich beim Gerät an. Alle Bildschirme der Ersteinrichtung werden übersprungen.

12.3.6. MDM-Zertifikat installieren

Sie müssen ein Apple-MDM-Zertifikat zur Verwaltung von iOS-Geräten anfordern und installieren. Sie müssen außerdem dieses Zertifikat einmal im Jahr verlängern. (Das für die Erstellung des Zertifikats verwendete Apple-Konto erhält eine Benachrichtigung von Apple, wenn das Ablaufdatum ansteht.) Verwenden Sie die Seite "MDM-Zertifikat", um dieses Zertifikat hinzuzufügen oder zu verlängern.

MDM-Zertifikat holen und installieren

Verfahren

1. Mithilfe der Seite **MDM-Zertifikat** können Sie eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR) von Ihrem Cloud-Mandanten herunterladen.
2. Laden Sie die Zertifikatsignieraufforderung (CSR) bei Apple hoch, um ein neues Zertifikat zu erstellen.
3. Geben Sie auf der Apple Site eine Anmerkung ein, wofür das Zertifikat gedacht ist. Diese Anmerkung hilft Ihnen später bei der Verlängerung des Zertifikats.
   Speichern Sie das neue Zertifikat.
4. Installieren Sie das Zertifikat für Ihren Ivanti Neurons for MDM-Mandanten.

MDM-Zertifikat verlängern

Verfahren

1. Klicken Sie auf **Zertifikat verlängern** .
2. Laden Sie eine Zertifizierungssignieranforderung (CSR) von Ihrem Cloud-Mandanten herunter.
3. Laden Sie die CSR bei Apple hoch, um das entsprechende Zertifikat zu verlängern.
4. Prüfen Sie auf der Apple Site, ob Sie das richtige Zertifikat verlängern. Sobald ein anderes Zertifikat in die Cloud hochgeladen wird, werden alle registrierten iOS-Geräte automatisch außer Dienst gestellt.
   Installieren Sie das Zertifikat für Ihren Ivanti Neurons for MDM-Mandanten.

Sie erhalten eine Warnmitteilung, wenn Sie versuchen, das falsche Zertifikat hochzuladen.

Wenn Sie die Seite **MDM-Zertifikat installieren** nicht sehen können, kann es sein, dass Sie nicht über die erforderlichen Berechtigungen verfügen. Sie brauchen eine der folgenden **Rollen**:

- Systemverwaltung
- System schreibgeschützt

12.3.7. Gemeinsam genutzte iPad-Geräte für Unternehmen

Gemeinsam genutzte iPad-Geräte für Unternehmen ist für verwaltete Apple-IDs verfügbar, die in Apple Business Manager auf iOS 13.4 oder unterstützten höheren Versionen erstellt werden.

- Bei gemeinsam genutzten iPads kann das Unternehmen ein Gerät für mehrere Mitarbeiter gemeinsam bereitstellen und ihnen dennoch ein personalisiertes Erlebnis bieten.
- Mitarbeiter können sich mit einer verwalteten Apple-ID anmelden, um Daten wie E-Mail-Konten, Dateien, iCloud Photo Library, App-Daten usw. hochzuladen.
- Die Daten werden in iCloud gespeichert, sodass sich Mitarbeiter bei jedem gemeinsam genutzten iPad anmelden können, das dem Unternehmen gehört.

Gemeinsam genutzte iPad-Geräte können in Anwendungen in Gesundheitswesen, Einzelhandel und Industrie verwendet werden. Ärzte und Pflegepersonal beispielsweise können ein iPad-Gerät gemeinsam nutzen, da sie sicher auf das ihnen eindeutig zugewiesene Benutzerprofil zugreifen können. In Einzelhandelsgeschäften können die Mitarbeiter für Kunden Produktinformationen, Ressourcen und Fachwissen abrufen, um die Kunden zu begeistern und ihnen ein besseres Einkaufserlebnis zu bieten.

Funktionsweise

- Die iPad-Geräte werden zu Apple Business Manager hinzugefügt und mit einem automatischen Geräteregistrierungsprofil mit aktiviertem Freigabemodus registriert.
- Mitarbeiter melden sich mit einer vom Unternehmen bereitgestellten, verwalteten Apple-ID und einem zugehörigen Kennwort am gemeinsam genutzten iPad-Gerät an. Der Apple Business Manager-Administrator kann die Konten für die Benutzer manuell erstellen oder die Kontoerstellung einem Identitätsanbieter wie Entra ID übertragen.
- Jeder Benutzer kann ein eigenes Profil verwenden, wenn er am gemeinsam genutzten iPad-Gerät angemeldet ist. Administratoren können Apps basierend auf Benutzerrolle, Zuständigkeiten und Abteilung verteilen.
- Benutzer können sich als Gastbenutzer auf einem gemeinsam genutzten iPad-Gerät anmelden. Die Gastbenutzeranmeldung ist standardmäßig aktiviert. Ein Gastbenutzer muss sich nicht mit einer verwalteten Apple-ID und einem Kennwort anmelden. Die Gastbenutzeranmeldung kann deaktiviert werden, indem die Einstellung **Gastsitzung für gemeinsam genutzten iPad zulassen** in der Konfiguration **iOS-Einschränkungen** auf **Falsch** gesetzt wird.
- Wechseln Sie zu Ivanti Neurons for MDM **> Geräte**, klicken Sie auf den Namen eines gemeinsam genutzten iPad-Geräts und dann auf die Registerkarte **Benutzer**, um die Liste der Benutzer auf dem Gerät und ihre Details anzuzeigen (z. B. verwaltete Apple-ID, verfügbare Daten in Bytes, verwendete Daten in Bytes, besitzt Daten für Synchronisierung mit Cloud).
- Wechseln Sie zur Registerkarte **Protokolle** und wählen Sie bei den Filtern die Aktion **Bericht Benutzerliste** aus, um zusätzliche Benutzerdetails anzuzeigen.
- Die Anmeldung eines Gastbenutzers bei einem gemeinsam genutzten iPad-Gerät unterscheidet sich von der Gastbenutzerverwaltung durch Ivanti Neurons for MDM. Standardmäßig ist das Gastbenutzerkonto in Ivanti Neurons for MDM deaktiviert. Um einen Gastbenutzer auf einem gemeinsam genutzten iPad-Gerät zu verwalten, aktivieren Sie das Konto des Gastbenutzers.
- Auf gemeinsam genutzten iPad-Geräten ist die Bildschirmaufzeichnung über das Steuerungscenter verfügbar.
- Ivanti Neurons for MDM unterstützt eine Ersatzvariable für die Managed Apple ID, `${managedAppleID}`. Diese Systemvariable wird im Abschnitt „Systemattribute“ und im Abschnitt „Geräteattribute“ angezeigt.

- Ivanti Neurons for MDM verhindert, dass ein Administrator die verwaltete Apple-ID ansässiger Benutzer ändern kann, die in der Vergangenheit mit den derzeit angemeldeten Benutzern am gemeinsam genutzten iPad-Gerät angemeldet waren. Wenn Sie versuchen, die verwaltete Apple-ID zu ändern, weist eine Meldung darauf hin, dass die verwaltete Apple-ID des Benutzers nicht geändert werden kann, weil der Benutzer ein gemeinsam genutztes iPad-Gerät verwendet.
- Bei **Apple Apps and Books** werden Apps und Books auf gemeinsam genutzten iPad-Geräten basierend auf Gerätelizenzen installiert, unabhängig davon, ob die Option für Gerätelizenzen ausgewählt wurde.

Voraussetzungen

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Für ein gemeinsam genutztes iPad-Gerät ist eine verwaltete Apple-ID erforderlich. Administratoren können die Konten für die Benutzer manuell erstellen oder die Kontoerstellung einem Identitätsanbieter wie Entra ID übertragen.
- Die gemeinsam genutzten iPad-Geräte müssen iOS 13.4 oder eine unterstützte neuere Version davon enthalten.
- Die Geräte müssen mit Apple Business Manager-Konten verknüpft sein.
- Die Geräte müssen eine Speicherkapazität von mindestens 32 GB aufweisen.

Beachten Sie Folgendes:

- Ivanti Neurons for MDM unterbindet bestimmte Konfigurationen, wie Passcode, für gemeinsam genutzte iPad-Geräte, da Apple sie nicht unterstützt. Solche Konfigurationen werden nicht auf die Geräte übertragen (unter Geräte > Link mit dem Gerätenamen > Registerkarte Konfigurationen).
- Die **Passcode**-Konfiguration gilt nicht für gemeinsam genutzte iPad-Geräte, da diese verwaltete Apple-IDs erfordern, die mit Kennwörtern und nicht mit Passcodes verknüpft sind. Mit der Aktion "Entsperren" über das Ivanti Neurons for MDM-Administrationsportal wird nicht der Passcode auf einem gemeinsam genutzten iPad-Gerät gelöscht.
- Wählen Sie bei der Verteilung der **Konfiguration für iOS-Einschränkungen** an gemeinsam genutzte iPads den Gerätekanal oder den Benutzerkanal aus. Sie können separate Konfigurationen verteilen und Einschränkungen erzwingen, die nur für das Gerät oder den Benutzerkanal gelten.
- Ivanti Neurons for MDM überprüft die abgelaufenen Konten und legt die Geräte still, deren Benutzer abgelaufene Konten sind. Bei einem freigegebenen iPad-Gerät ist der Gerätebesitzer jedoch der zuletzt angemeldete Benutzer und möglicherweise nicht mit dem rechtlichen Eigentümer identisch. Wenn ein Besitzerkonto abgelaufen ist, schließt Ivanti Neurons for MDM die gemeinsam genutzten iPad-Geräte von der Stilllegung aus.
- Go für iOS-Client wird für gemeinsam genutzte iPad-Geräte nicht unterstützt.
- Auf gemeinsam genutzten iPad-Geräten können Benutzer keine Aktionen durchführen wie eine Stilllegung oder Komplettlöschung. Nur Administratoren können über das Ivanti Neurons for MDM-Administrationsportal Stilllegungen und endgültige Löschungen vornehmen.
- Administratoren können den Besitzer eines gemeinsam genutzten iPad-Geräts nicht über das Ivanti Neurons for MDM-Administrationsportal ändern.
- Zero-Sign-On wird für gemeinsam genutzte iPad-Geräte nicht unterstützt.
- Bei Aktivierung des Befehls ListUsers werden alle verwalteten Benutzer-IDs und ihre Check-in-Uhrzeit bei der Geräteregistrierung (Teil von Apple Business Manager) auf der Registerkarte **Admin** angezeigt.

Konfigurieren eines gemeinsam genutzten iPad-Geräts

Sie können ein gemeinsam genutztes iPad-Gerät einrichten und die Einstellungen konfigurieren.

Verfahren

1. Gehen Sie zu Administration > Device Enrollment .
2. Fügen Sie das Gerät zum Apple Business Manager hinzu, indem Sie das Gerät mit einem automatischen Geräteregistrierungsprofil registrieren. Informationen zu diesem Verfahren finden Sie unter **Device Enrollment**.
3. Aktivieren Sie in den Einstellungen für Device Enrollment:
   - **Überwachter Modus**.
   - **Mehrbenutzermodus** unter **Gemeinsam genutztes iPad-Gerät für Unternehmen**.
4. (Optional) Erstellen Sie ein lokales Benutzerkonto. Das Gerät wird auf diesen Benutzer registriert. Die Authentifizierung, da dieser Benutzer nur einmal während der Registrierung auftritt.
5. Setzen Sie das gemeinsam genutzte iPad zurück.

> Der Registrierungsprozess beginnt erst nach dem Zurücksetzen. Es dauert einige Minuten, bis das Gerät registriert und als gemeinsam genutztes iPad-Gerät konfiguriert ist.

6. Der rechtmäßige Eigentümer wird dem Benutzerkonto zugeordnet, unter dem das Gerät registriert wurde. Der Administrator kann den rechtmäßigen Eigentümer auf der Seite **Geräte** ändern.
7. Geben Sie im Anmeldebildschirm des Geräts die Anmeldedaten des Benutzers für die verwaltete Apple-ID ein.
   - Wie bei macOS-Geräten können Sie Konfigurationen auf gemeinsam genutzten iPad-Geräten via Push über den Gerätekanal oder den Benutzerkanal übertragen.
   - Die Benutzer-Ersetzungsvariablen werden nicht für Konfigurationen ersetzt (einschließlich der Konfiguration für verwaltete Apps), die via Push in den Gerätekanal übertragen werden.
   - Falls es sich bei einem an einem gemeinsam genutzten iPad-Gerät angemeldeten Benutzer nicht um einen verwalteten Benutzer handelt, gehört die verwaltete Apple-ID keinem Benutzer im Ivanti Neurons for MDM-Administrationsportal und das Gerät wird niemandem zugewiesen. Die Benutzer werden nicht verwaltet. Der Administrator kann keine Kanalkonfigurationen via Push über Ivanti Neurons for MDM übertragen.
   - Standardmäßig ist der von Ivanti Neurons for MDM erstellte Standard-Gastbenutzer deaktiviert. Wenn sich ein Gastbenutzer anmeldet, ist das Gerät keinem Benutzer zugewiesen und der Benutzer wird nicht verwaltet. Wenn der Gastbenutzer verwaltet werden muss, muss der von Ivanti Neurons for MDM erstellte Gastbenutzer aktiviert werden. Das Gerät wird dem Gastbenutzer zugewiesen, nachdem sich der Gastbenutzer angemeldet hat. Anschließend kann der Benutzer verwaltet werden.
   - Die Informationen zum Geräteeigentümer werden auf der Seite Ivanti Neurons for MDM > **Geräte** und in den Geräteprotokollen (Gerätedetails-Seite > **Protokolle**) angezeigt.

Rechtmäßige Eigentümer für gemeinsam genutzte iPads verwalten

Sie können nach den rechtlichen Eigentümern der gemeinsam genutzten iPad-Geräte suchen und sie anzeigen, indem Sie ihre E-Mail-IDs auf der Seite mit der Geräteliste verwenden. Sie können die rechtlichen Eigentümer der gemeinsam genutzten iPad-Geräte ändern, indem Sie die vorhandenen rechtmäßigen Eigentümer den neuen rechtmäßigen Eigentümern neu zuweisen. Wird der rechtliche Eigentümer eines nicht gemeinsam genutzten iPad-Geräts neu zugewiesen, ignoriert Ivanti Neurons for MDM die Zuweisung.

Verfahren

1. Gehen Sie zu **Geräte**.

2. Klicken Sie auf das Zahnradsymbol, um die Spalte **Rechtmäßiger Eigentümer** auszuwählen und zur Seite mit der Geräteliste hinzuzufügen.
3. Wählen Sie die gemeinsam genutzten iPad-Geräte aus.
4. Klicken Sie auf **Aktionen > Dem rechtmäßigen Eigentümer zuweisen**.

Senden einer E-Mail an den rechtlichen Eigentümer eines gemeinsam genutzten iPad-Geräts

Sie können dem rechtlichen Eigentümer eines gemeinsam genutzten iPad-Geräts E-Mails senden.

Verfahren

1. Gehen Sie zu **Geräte**.
2. Klicken Sie auf den Namen des gemeinsam genutzten iPad-Geräts.
3. Klicken Sie auf das **E-Mail**-Symbol.
4. Verfassen Sie die E-Mail.
5. Klicken Sie auf **Senden**.

Attribut „Mehrbenutzermodus“ verwenden

Sie können das Attribut "Mehrbenutzermodus" der gemeinsam genutzten iPad-Geräte in Ivanti Neurons for MDM verwenden.

Verfahren

1. Verwenden Sie auf der Seite **Geräte** das Attribut **Mehrbenutzermodus**.
2. Klicken Sie auf **Erweiterte Suche** und erstellen Sie eine Regel, um die Geräte über das Attribut **Mehrbenutzermodus** zu ermitteln.
3. Erstellen Sie auf der Seite **Geräte > Gerätegruppen** eine dynamische Gerätegruppe für die gemeinsam genutzten iPad-Geräte, indem Sie das Attribut **Mehrbenutzermodus** verwenden. Beispielsweise können Sie diese Gruppe als Verteilungsfilter verwenden, um Konfigurationen zu verteilen.
4. Erstellen Sie auf der Seite **Richtlinien** eine benutzerdefinierte Richtlinie für die gemeinsam genutzten iPad-Geräte, indem Sie das Attribut **Mehrbenutzermodus** verwenden.
5. Begrenzen Sie im **Filter Apps > Verteilung** mithilfe des Attributs **Mehrbenutzermodus** die Anzahl der zum Installieren verfügbaren Anwendungen.

- Ivanti Neurons for MDM unterstützt den Mehrbenutzermodus für Apple School Manager-Geräte nicht. Es wird nicht empfohlen, die Einstellung zu aktivieren und das Device Enrollment-Profil per Push auf Apple School Manager-Geräte zu übertragen.
- Die Konfiguration für sichere Mehrbenutzeranmeldung für iOS gilt nicht für gemeinsam genutzte iPad-Geräte.

Löschen von Benutzern von einem gemeinsam genutzten iPad-Gerät

Sie können ein oder mehrere Benutzerkonten von den gemeinsam genutzten iPad-Geräten löschen. Auf der Registerkarte mit der Benutzerliste wird für den derzeit angemeldeten Benutzer die Beschriftung **Aktiv** angezeigt. Die Option "Löschen" ist für den derzeit am gemeinsam genutzten iPad-Gerät angemeldeten Benutzer nicht verfügbar. Benutzer können über die Registerkarte **Geräte** oder **Benutzer** gelöscht werden.

Löschen von Benutzern aus der Registerkarte "Geräte"

Verfahren

1. Wechseln Sie zur Registerkarte **Geräte** und klicken Sie auf > **Gerätedetails**.
2. Wechseln Sie zur Registerkarte **Benutzer**. Die Liste der Benutzer wird angezeigt.
3. Klicken Sie auf **Alle Benutzer löschen**.
4. Klicken Sie auf das Minuszeichen (**-**), um bestimmte Benutzer zu löschen.
    - (Optional) Wählen Sie im Fenster **Benutzer löschen** die Option **Löschung des Benutzers erzwingen, auch wenn die Datensynchronisierung mit der Cloud ansteht** aus und klicken Sie auf **Ja**.

      > Durch Auswählen von **Löschung des Benutzers erzwingen, auch wenn die Datensynchronisierung mit der Cloud ansteht** wird die Löschung des Benutzers selbst dann erzwungen, wenn die Daten noch nicht mit dem Cloud-Administrationsportal synchronisiert sind.

Löschen von Benutzern aus der Registerkarte "Benutzer"

Verfahren

1. Wechseln Sie zur Registerkarte **Benutzer**.
2. Wählen Sie einen oder mehrere Benutzer aus, wechseln Sie in das Dropdownmenü **Aktionen** und klicken Sie auf **Löschen**. Eine Bestätigungsmeldung wird angezeigt. Nach dem Bestätigen wird der Befehl zum Löschen des Benutzers an die Geräte ausgegeben.
3. Wechseln Sie zu **Geräteprotokolle** bei den Gerätedetails und prüfen Sie, ob der Befehl zum Löschen des Benutzers an die ausgewählten Benutzer des gemeinsam genutzten iPad-Geräts gesendet wurde.

Abmelden von Benutzern von einem gemeinsam genutzten iPad-Gerät

Der Administrator kann Benutzer von einem freigegebenen iPad-Gerät abmelden.

Verfahren

1. Wählen Sie auf der Seite **Geräte** ein gemeinsam genutztes iPad-Gerät aus.
2. Wählen Sie **Abmeldung erzwingen** aus dem Menü **Aktionen**. Ein Popup-Fenster fordert zur Bestätigung der Abmeldung der Benutzer vom freigegebenen iPad-Gerät auf.
3. Klicken Sie auf **OK**, um die Zwangsabmeldung zu bestätigen.

12.3.8. School Manager

Lizenz: Gold

Gilt für: überwachte Geräte mit iOS 9.3+.

Apple School Manager ist ein Apple Cloud-Dienst für Bildungseinrichtungen, der beispielsweise den Kauf von Anwendungen in Apple Apps and Books, die Registrierung von iPads über die Apple-Geräteregistrierung und die Erstellung verwalteter Apple-IDs ermöglicht. Durch die vollständige Integration in Apple School Manager kann die Ivanti Neurons for MDM-UEM-Lösung die iPads der Lehrer und Schüler nahtlos und uneingeschränkt verwalten und das School Manager-Ökosystem sowie Apps wie ClassRoom umfassend nutzen.

> Apple Books wird nicht unterstützt.

Apple School Manager konfigurieren

1. Gehen Sie zu **Admin > School Manager**.
2. Klicken Sie auf die Option **Education konfigurieren**, wenn diese deaktiviert ist.
3. Wählen Sie eine der folgenden Optionen aus:
   - **Informationen über die Schule werden durch Synchronisation mit dem Apple School Manager-Konto importiert**:
     1. Gehen Sie zu **Administration > Device Enrollment** , um die Schlüsseldateien für Ihr Unternehmen herunterzuladen.
     2. Laden Sie die Schlüsseldateien in Ihr Apple School Manager-Konto, um die Verschlüsselungsschlüssel zu erzeugen.
     3. Laden Sie die Verschlüsselungsschlüssel aus dem Apple School Manager herunter und laden Sie diese dann in die Cloud hoch (unter **Administration > Apple > Device Enrollment**).

        > Bestehende Apple Device Enrollment-Konten können für Apple Education wiederverwendet werden. Apple räumt Ihnen die Möglichkeit ein, Ihr Device Enrollment-Konto mit den Education-Funktionen zu aktualisieren, wenn Sie auf den Apple School Manager zugreifen. Anweisungen für ein Upgrade finden Sie unter https://support.apple.com/en-in/HT206960.

     Wenn die Verschlüsselungsschlüssel akzeptiert wurden, wird die Schaltfläche **Jetzt synchronisieren** angezeigt.

     4. Klicken Sie auf die Option **Jetzt synchronisieren**, um die Datensynchronisation mit dem Apple School Manager zu beginnen.
   - **Daten aus CSV-Dateien importieren**:
     1. (Optional) Klicken Sie auf **CSV-Vorlagen-ZIP-Datei herunterladen**, um eine ZIP-Datei herunterzuladen, die Vorlagen für alle Datenarten enthält.
     2. Klicken Sie auf **Dateien auswählen**...
     3. Ergänzen Sie die folgenden sechs CSV-Dateien:
        - Schülerdatendatei (students.csv)
        - Dienstplandatendatei (roster.csv)
        - Mitarbeiterdatendatei (staff.csv)
        - Klassendatendatei (classes.csv)
        - Kursdatendatei (courses.csv)

- Standortdatendatei (locations.csv)

> Sie müssen die sechs CSV-Dateien jedes Mal gemeinsam auswählen, bevor Sie diese hochladen.

Klicken Sie auf **Hochladen**.

4. (Optional) Wenn die CSV-Dateien geändert werden müssen, archivieren Sie zuerst alle erforderlichen Daten in allen sechs Dateien, die zuvor hochgeladen wurden. Nehmen Sie die erforderlichen Änderungen vor und laden Sie die Dateien gemeinsam wieder hoch.

Suchen Sie auf den Registerkarten **Klassen** und **Einzelpersonen** nach Daten.

> Die Personen (Schüler und Mitarbeiter) werden auch auf der Seite **Benutzer** von Ivanti Neurons for MDM angezeigt.

5. Erstellen Sie wie folgt zwei Gerätegruppen für Geräte, die in Education durch die Schüler und Mitarbeiter verwendet werden:
   1. Gehen Sie zu **Administrator > anpassbare Attribute**.
   2. Erstellen Sie anpassbare Attribute für die Schüler und Mitarbeiter, mit denen dynamisch verwaltete Gerätegruppen erstellt werden können.
   3. Gehen Sie zu **Geräte > Gerätegruppen**.
   4. Klicken Sie auf **Hinzufügen+**.
   5. Erstellen Sie jeweils eine dynamisch verwaltete Gerätegruppe für die Schüler und Mitarbeiter, indem Sie die zuvor angelegten anpassbaren Attribute als Filter verwenden.
6. Weisen Sie die registrierten **Geräte** den Schülern und Mitarbeitern über die Seite Geräte und die Option **Aktionen > Benutzer zuweisen zu**.
7. Erstellen Sie eine Konfiguration für einen Leiter (Mitarbeiter) und eine Konfiguration für Mitglieder (Schüler), indem Sie die Payloads unter **Konfigurationen >** Education ergänzen.
8. Verteilen Sie die Konfigurationen für Leiter (Mitarbeiter) und Mitglieder (Schüler) an die Gerätegruppen der Schüler bzw. Mitarbeiter.
   Durch diese Verteilung werden die Konfigurationen per Push auf die betreffenden Geräte übertragen und die Zertifikate installiert.

> Wenn auf der Seite Administrator > School Manager kein Wert für den Klassennamen vorhanden ist, wird der Wert aus dem Klassensystem-Quell-Identifikator und dem Kurs-Identifikatorfeld abgeleitet.Diese Felder sind im Apple School Manager bzw. in der CSV-Datei optional. Wir empfehlen jedoch immer einen Wert einzugeben, da deren Kombination als Standard-Identifikator verwendet wird, wenn keine Klassenbezeichnung angegeben ist.

Classroom-App für die Lehrer per Push übertragen

Mit der Classroom-App können die Lehrer (Leiter) folgende Szenarien verwalten:

- Sie können mit der Classroom-Verwaltungsfunktion iPads und Apps aus der Ferne kontrollieren.
- Sie können eine Klassengruppe erstellen.
- Ein Lehrer kann die Schüler dieser Gruppe anzeigen.
- Ein Lehrer kann Content an die Schüler dieser Gruppe senden.
- Sie können Einschränkungen definieren, welche Apps und welchen Content die Schüler sehen können.

Sie können die Classroom-App per Push aus dem Apple App Store übertragen:

Verfahren

1. Gehen Sie zu der Seite **Apps > App-Katalog**.
2. Klicken Sie auf die Schaltfläche **+Hinzufügen**.
3. Suchen Sie die Classroom-App von Apple und wählen Sie diese aus.
4. Klicken Sie auf **Weiter**.
5. Geben Sie die Kategorie und Beschreibung ein.
6. Klicken Sie auf **Weiter**.
7. Verteilen Sie die App an die Lehrer-Gerätegruppe, die Sie gerade erstellt haben.
8. Konfigurieren Sie die App-Einstellungen auf der Seite "App-Konfigurationen".
9. Klicken Sie auf **Fertig**.

School Manager deaktivieren

Bei Deaktivierung des School Manager werden alle aktuellen Daten gelöscht. Deaktivieren Sie die Anwendung nur nach genauer Prüfung.

1. Gehen Sie zu **Admin > School Manager**.
2. Klicken Sie auf die Option **Education konfigurieren**, wenn diese noch nicht aktiviert ist.
3. Klicken Sie auf **[Yes]**.

12.3.9. Einstellungen (Apple)

Administratoren können verschiedene Einstellungen für Apple-Geräte konfigurieren, aktivieren und deaktivieren.

Stille Registrierung (nur für macOS)

Die Registrierung im Hintergrund für macOS-Geräte ist als „Aktiviert“ gesperrt. Dies gilt für alle neuen Geräteregistrierungen im Mandanten und wird von Mobile@Work 1.4 und unterstützten neueren Versionen unterstützt.

Allgemeine Einstellungen

Geräteabstimmung deaktivieren – Administratoren können jetzt die Geräteeinträge beibehalten, wenn sie dasselbe Gerät erneut registrieren möchten. Diese Option ist standardmäßig nicht aktiviert. Wählen Sie diese Option, um die inaktiven Gerätedetails beizubehalten.

> Wenn "Geräteabstimmung deaktivieren" nicht aktiviert ist und ein Gerät erneut mit demselben Benutzer registriert wird, wird ein neuer Eintrag erstellt. Andernfalls wird der Geräteeintrag mit neuen Informationen aktualisiert.

Profileinstellungen

Administratoren können den Versand von E-Mails an Endbenutzer und von Benachrichtigungen an macOS- und Go for iOS-Clients aktivieren oder deaktivieren, wenn das MDM-Profil nicht installiert ist. Die Benachrichtigungsfunktion für MDM-Profile ist standardmäßig aktiviert.

Verfahren

1. Gehen Sie zu Admin > Einstellungen.
2. Aktivieren oder deaktivieren Sie die Option **E-Mail an Benutzer senden und Benachrichtigung des Clients, wenn kein MDM-Profil installiert ist**.
3. Wählen Sie als maximale Anzahl der E-Mails/Benachrichtigungen 1 bis 4 aus.
4. Klicken Sie auf **Speichern**.

OS-Updates für die automatische Geräteregistrierung (nur iOS)

Administratoren können iOS-Betriebssystem-Updates für die automatische Geräteregistrierung aktivieren. Wenn diese Option aktiviert ist, verwenden die Geräte zur Geräteregistrierung die Konfiguration **Software-Aktualisierungen** anstelle der Einstellung für die geplante Betriebssystem-Aktualisierung im Geräteregistrierungsprofil.

Diese Option ist standardmäßig deaktiviert. In diesem Fall wird die Einstellung für die geplante Aktualisierung des Betriebssystems im Geräteregistrierungsprofil verwendet. Die Aktivierung dieser Einstellung ist dauerhaft und kann nicht zurückgenommen werden. Damit wird die Einstellung für die geplante Betriebssystem-Aktualisierung in allen verfügbaren Geräteeintragungsprofilen entfernt.

> Überwachte Geräte, die keine Geräteregistrierungsgeräte sind, verwenden die Konfiguration zur Software-Aktualisierung.

Verfahren

1. Gehen Sie zu Admin > Einstellungen.

2. Aktivieren oder deaktivieren Sie die Option **Software-Aktualisierungskonfiguration für die automatische Geräteregistrierung verwenden**.
3. Klicken Sie zur Bestätigung auf **Ja**.
4. Klicken Sie auf **Speichern**.

Sichere Anmeldung für mehrere Benutzer

Die Administratoren können das Gerätepasswort löschen, wenn sich der Benutzer aus dem Web-Clip „Sichere Anmeldung für mehrere Benutzer" auf freigegebenen iOS-Geräten abmeldet, indem er die Option „**Passcode nach Benutzerabmeldung löschen**" im Abschnitt „**Sichere Anmeldung für mehrere Benutzer**" unter Admin > Apple > Einstellungen auswählt.

Konfiguration der Prioritätseinstellungen für Einschränkungen

Der Administrator kann mehreren Konfigurationen mit iOS- und macOS-Beschränkungen Priorität einräumen, indem er die Optionen **Konfiguration der iOS-Beschränkungen** bzw. **Konfiguration der macOS-Beschränkungen** im Abschnitt **Prioritätseinstellungen für konfigurierte Beschränkungen** unter **Admin >Apple > Einstellungen** auswählt. Diese Option ist standardmäßig deaktiviert. Prioritätenvergabe für KonfigurationenWeitere Informationen zur Funktionsweise der Priorität finden Sie unter Konfigurationen priorisieren.

Verfahren

1. Gehen Sie zu **Admin > Apple > Einstellungen**.
2. Wählen Sie im Abschnitt **Prioritätseinstellungen für die Einschränkungskonfiguration** die Option **iOS-Einschränkungskonfiguration** oder **macOS-Einschränkungskonfiguration**.
3. Klicken Sie auf **Speichern**, um die Priorität zu aktivieren. Das Banner „**Prioritätseinstellungen für Beschränkungskonfiguration (iOS oder macOS) wurde aktiviert**" wird angezeigt. Bevor die Priorität **freigegeben** wird:
   - **Verteilungszusammenfassung bearbeiten (falls zutreffend)**: Wenn die Prioritätseinstellung aktiviert ist, wird die Verteilungszusammenfassung für die ausgewählte Beschränkungskonfiguration standardmäßig von „**Auf Geräte in anderen Spaces anwenden**" auf „**Auf alle Geräte in anderen Geräte-Spaces als höchste Priorität anwenden**" geändert.
   - **Standardpriorität wird in der Reihenfolge der Erstellung zugewiesen**: Bei einer ausgewählten Einschränkungstypkonfiguration wird eine vorhandene Standardpriorität in der Reihenfolge ihrer Erstellung zugewiesen.
   - **Verwaltung der Konfiguration aussetzen**: Die Verwaltung der ausgewählten Einschränkungskonfiguration (z. B. iOS-Einschränkungskonfiguration) wird ausgesetzt, bis Sie die Priorität genehmigen.

> Sobald die Priorität aktiviert ist, werden Änderungen an den Einschränkungen erst verarbeitet, wenn sie genehmigt wurden. Vor der Genehmigung kann der Administrator die Verteilung, die Verteilungszusammenfassung oder die Priorität für die Konfiguration der Einschränkungen im Abschnitt **Konfigurationen** bearbeiten.

4. Wählen Sie die Option **Freigeben**, um die Priorität in Kraft zu setzen.
5. Klicken Sie auf **Speichern**.

> Die Option **Genehmigung** ist nicht verfügbar, wenn eine iOS- oder macOS-Einschränkungskonfigurationsoption abgewählt wird; die Änderungen werden sofort übernommen.

Wenn die Prioritätseinstellung deaktiviert ist, ist keine Priorität mit den Konfigurationen verbunden. Alle Einschränkungskonfigurationen werden, falls zutreffend, bei der nächsten Gerätesynchronisierung per Push auf das Gerät übertragen.

- **Verteilungszusammenfassung (falls zutreffend): Wenn die Prioritätseinstellung für die Beschränkungskonfiguration deaktiviert ist, wird die Verteilungszusammenfassung von Als höchste Priorität auf alle Geräte in anderen Geräte-Spaces anwenden oder Als niedrigste Priorität auf alle Geräte in anderen Geräte-Spaces anwenden auf „Als höchste Priorität auf Geräte in anderen Spaces anwenden“ geändert.**
- **Keine Priorität zugewiesen**: Die zugewiesene Priorität wird für ausgewählte Beschränkungskonfiguration entfernt.

12.4. Arbeiten mit Windows-Geräten

Dieser Abschnitt enthält die folgenden Themen:

- Windows Autopilot-Profile konfigurieren
- Audit-Protokolle auf Windows Autopilot-Profilen
- TenantLockdown CSP
- ADMX (GPO) Browser
- App-Bestandsaufnahmeintervalle konfigurieren
- Hardware-Bestand

12.4.1. Windows Autopilot-Profile konfigurieren

Windows Autopilot ist eine Microsoft-Funktion, mit denen Administratoren neue Geräte einrichten und unternehmensfertig vorkonfigurieren können. Die Autopilot-Funktion ermöglicht die schnelle, zuverlässige und nahtlose Bereitstellung von Windows Desktop- oder HoloLens2-Geräten. Darüber hinaus erleichtert die Autopilot-Funktion die Ausführung der folgenden Aufgaben:

- Geräte automatisch in Entra ID (Entra ID) einbinden
- Geräte automatisch bei MDM-Diensten registrieren
- Geräte erstellen und automatisch zu Konfigurationsgruppen nach dem Profil des Geräts zuweisen
- Registrierungsabläufe anpassen
- AppConnect-Konfigurationen und Richtlinien anwenden
- Wichtige Anwendungen installieren

Voraussetzungen

Überprüfen Sie zum Verwenden der Seite "Windows-Autopilot" die Schritte für Ivanti Neurons for MDM-Partner und die Azure-Lizenzierungsanforderungen. Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind, damit die Autopilot-Funktion wie erwartet funktioniert:

- **Azure-Lizenzierung für Autopilot-Anforderungen**: Suchen Sie nach "Lizenzierungsanforderungen für Windows-Autopilot".
- **Azure Windows Autopilot-Geräteregistrierung**: Suchen Sie nach "Übersicht über die Windows Autopilot-Registrierung".
- **Händler, die Geräte zum Kundenkonto hinzufügen**: Suchen Sie nach "Verwenden von Windows Autopilot-Profilen zu neuen Geräten, um die Out-of-Box-Erfahrung eines Kunden anzupassen".

Weitere Anforderungen

1. Integrieren Sie Entra ID-Mandanten und Ivanti Neurons for MDM. Weitere Informationen finden Sie unter **Einrichtung mit Microsoft Azure**.
2. Stellen Sie sicher, dass Sie in Ivanti Neurons for MDM und in Entra ID über ein Administratorkonto verfügen.
3. Erstellen Sie zum Verwenden von Profilen mit eigenständiger Bereitstellung einen fiktiven Benutzer für die Registrierung benutzerloser Geräte mit eigenständiger Bereitstellung in Ivanti Neurons for MDM.
4. Erstellen und synchronisieren Sie den Dummy-Benutzer fooUser@Entra IDPrimaryDomain.com über die primäre Entra ID-Domäne.

> Zum Erstellen und Synchronisieren eines Dummy-Benutzers benötigen Sie keine Microsoft-Lizenzen.

5. Auf der Seite "Benutzerdefinierte Domänennamen" in Entra ID wird die primäre Domäne Ihrer Entra ID-Umgebung angezeigt.
6. Stellen Sie sicher, dass der Benutzer Geräte registrieren kann und dass er nicht deaktiviert ist. Beispiel: Wenn die primäre Domäne contoso.com lautet, lautet der Benutzer fooUser@contoso.com. Wenn die primäre Domäne contoso.onmicrosoft.com lautet, lautet der Benutzer fooUser@contoso.onmicrosoft.com.
7. Um den Benutzer mit SCIM in Ivanti Neurons for MDM bereitzustellen, bearbeiten Sie die Benutzerdetails in Entra ID und fügen Sie die E-Mail-Adresse hinzu. Im Allgemeinen entspricht die E-Mail-Adresse der in UPN.
8. Stellen Sie sicher, dass alle Benutzer, auch der fooUser, in Azure und Ivanti Neurons for MDM vorhanden sind.

9. Administratoren können Autopilot-Profile mithilfe von Microsoft Store for Business oder Ivanti Neurons for MDM erstellen. Zum Erstellen von Profilen mit Ivanti Neurons for MDM benötigen Administratoren Global Entra ID Admin- sowie Intune-Administrator-Berechtigungen.

> Administratoren benötigen Azure P1 oder P2 und es sind Lizenzen für Ivanti Neurons for MDM Secure UEM oder Secure UEM Premium erforderlich. Die Intune-Lizenz ist für Administratoren nicht erforderlich.

> In Neurons for MDM werden für die Erstellung von Autopilot-Profilen Microsoft Graph-APIs für Autopilot verwendet, die sich noch in der Betaversion befinden.

Autopilot-Registrierungsmodi

Wenn Sie Geräte einer bestimmten Benutzerprofilgruppe zugewiesen haben (Basis ist die Gerätenutzung), können Sie den Einstieg der Benutzer in die Arbeit mit dem Gerät mithilfe des Autopilot-Registrierungsmodus beschleunigen. Cloud bietet die folgenden Autopilot-Registrierungsmodi:

- Self-Deployment-Modus
- Benutzergesteuert (Modus "Vorab bereitgestellt")
- Benutzergesteuert

Autopilot-Modus mit eigenständiger Bereitstellung – Der Autopilot-Self-Deployment-Registrierungsmodus gewährleistet die nahtlose Bereitstellung eines Unternehmensgeräts für einen Benutzer. Die anfängliche Geräteeinrichtung wird umgangen und alle Konfigurationsdateien, die für den sicheren Start des Geräts erforderlich sind, werden auf das Gerät übertragen. Dieser Modus sichert die Hardware, schließt das Gerät an das Unternehmensnetzwerk an, registriert das Gerät bei Entra ID, beim MDM-Dienst und im Ivanti Neurons for MDM-Administrator-Portal anhand einer Dummy-Benutzer-ID und überträgt alle erforderlichen Konfigurationsdateien auf das Gerät, bevor sich der Benutzer anmeldet. Wenn die obligatorischen Konfigurationsdateien auf das Gerät übertragen wurden, startet das Gerät neu und zeigt den Anmeldebildschirm als Einstieg für den Unternehmensbenutzer an. Der Self-Deployment-Modus eignet sich für Geräte, die als Kiosk oder digital signiertes Gerät verwendet werden können.

Benutzergesteuerter Vorab-Bereitstellungsprofilmodus – Der Administrator erstellt ein benutzergesteuertes Vorab-Bereitstellungsprofil und weist das Profil einer Benutzergruppe zu. Die Gerätehardware-ID wird hochgeladen und der Entra ID-Gruppe zugewiesen. Das Gerät wird dem benutzergesteuerten vorab bereitgestellten Profil zugeordnet. Mit diesem Modus richtet ein Administrator ein Gerät ein, bevor es dem Unternehmensbenutzer ausgehändigt wird.

Verfahren

Führen Sie folgende Schritte für eine Bereitstellung mit Pre-Provisioning aus:

1. Schließen Sie das neue Hardwaregerät an das LAN an und drücken Sie fünfmal die Windows-Taste.
2. Das Gerät zeigt eine Abfrage an. Wählen Sie die Option „Windows Autopilot-Bereitstellung“ und klicken Sie auf „Weiter“. Entra ID erkennt den benutzergesteuerten Vorab-Bereitstellungsprofilmodus, und alle Basis-Konfigurationseinstellungen werden auf dem Gerät bereitgestellt. Der Bildschirm „Windows Autopilot-Konfiguration“ wird geöffnet.
3. Klicken Sie auf „Fortsetzen“. Das Gerät setzt den Vorgang fort und sichert die Hardware, schließt das Gerät an das Unternehmensnetzwerk an, registriert das Gerät bei Entra ID, beim MDM-Dienst und im Ivanti Neurons for MDM-Administrator-Portal anhand einer Dummy-Benutzer-ID und überträgt alle erforderlichen Konfigurationsdateien auf das Gerät. Anschließend wird eine Bestätigungsmeldung angezeigt.
4. Sie können das Gerät jetzt dem Benutzer aushändigen. Wenn sich der Benutzer beim Gerät anmeldet, wird die Benutzer-ID mit den Gerätedetails im Cloud-Administrator-Portal registriert.

Die folgenden Konfigurationen werden automatisch übertragen, bevor sich der Benutzer beim Gerät anmeldet:

Identitätszertifikat

WLAN

Windows Hello for Business

Windows-Einschränkungen

> Die übrigen Konfigurationen befinden sich im Status "Ausstehend" und werden bereitgestellt, sobald der Benutzer sich über eine E-Mail-Adresse bei dem Gerät angemeldet hat.

> Während des Autopilot-Registrierungsprozesses in den Modi "Selbstbereitstellung" und "Benutzergesteuert (Pre-Provisioning)" werden die zugewiesenen MSI- und EXE-Apps auf dem Gerät installiert, wodurch der Registrierungsprozess abgeschlossen wird. Wenn beim Installieren der MSI- und EXE-Apps während des Autopilot-Registrierungsprozesses die Apps eine Meldung generieren oder nicht generieren, wird der Autopilot-Prozess abgeschlossen und die Schaltfläche "Erneut versiegeln" wird aktiviert.

Windows Autopilot-Benutzerprofile erstellen

Wenn Sie die Entra ID-Benutzerquelle konfiguriert und die Benutzer und Entra ID-Benutzergruppen mit dem Ivanti Neurons for MDM-Mandanten synchronisiert haben, können Sie die Autopilot-Profile erstellen.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administratorportal an.
2. Wechseln Sie zu **Admin > Microsoft Azure > Windows-Geräteverwaltung**.

> Wenn keine Entra ID-Benutzerquelle konfiguriert wurde, ist die Schaltfläche **Hinzufügen** deaktiviert. Sie müssen die Benutzerquelle mithilfe der Option **Windows-Geräteverwaltung** im Abschnitt **Microsoft Azure** konfigurieren.

3. Klicken Sie auf **[Add]**.
   Die Seite **Windows Autopilot-Profil hinzufügen** wird auf dem Bildschirm angezeigt.
4. Geben Sie einen Profilnamen in das Feld **Name** ein.
5. Vervollständigen Sie die **Profileinstellungen** anhand der Tabelle unterhalb dieses Verfahrens.
6. Klicken Sie auf **Weiter**.
   Auf dem Bildschirm wird eine neue Seite mit allen Entra ID-Gerätegruppen angezeigt.
7. Wählen Sie mindestens eine Entra ID-Gerätegruppe aus, der das Autopilot-Profil zugewiesen werden muss.
8. Sie können außerdem eine Entra ID-Gerätegruppe erstellen und das Autopilot-Profil dieser neu erstellten Gruppe zuweisen.
   Weitere Informationen erhalten Sie unter .
   Wenn Sie das Autopilot-Profil allen Entra ID-Gruppen zuweisen möchten, wählen Sie die Option **Allen Entra ID-Gruppen zuweisen**.

> Aufgrund einer Beschränkung von Microsoft können Sie nicht mehr als ein Profil für „Alle Gruppen“ zuweisen.

9. Klicken Sie auf **Fertig**.

Einstellung	Beschreibung
Gerätetyp	Wählen Sie eine der folgenden beiden Optionen, je nach Gerät: • **Windows-PC** • **HoloLens** – Wenn diese Option ausgewählt ist, sollte der standardmäßige Bereitstellungsmodus auf den Modus **Self-Deployment** eingestellt werden. In seltenen Fällen kann die Registrierung von HoloLens-2-Geräten über Autopilot im Bildschirm „Gerät für die Arbeit einrichten“ hängen bleiben. In einem solchen seltenen Fall muss der Benutzer das Gerät über den Ein/Aus-Schalter ausschalten und wieder einschalten. Das Gerät zeigt dann den Anmeldebildschirm an, in den der Benutzer die Entra ID-Anmeldedaten eingibt, um die Registrierung abzuschließen.
Bereitstellungsmodus	• **Self-Deployment**: In diesem Modus wird das Gerät mit wenigen oder ganz ohne manuelle Schritte bereitgestellt. • **Benutzergesteuert**: Administratoren können mit dieser Option den Registrierungsmodus auswählen und damit ein neues Gerät für den Benutzer konfigurieren, bevor sie dem Benutzer das Gerät aushändigen.
Benutzerkontotyp	• **Administrator**: Wählen Sie diese Option, wenn der Benutzer nach der Bereitstellung des Geräts die volle Kontrolle benötigt. • **Standard**: Wählen Sie diese Option, wenn der Benutzer nach der Bereitstellung des Geräts die Autorisierung für die Basisfunktionen benötigt.
Sprache	Standardmäßig ist die Sprache betriebssystemspezifisch. Sie können zu einer anderen Sprache in der Liste wechseln.
Alle Zielgeräte zu Autopilot konvertieren	Mit dieser Option konvertieren Sie alle Geräte in der zugewiesenen Gruppe zu Autopilot.
Vorab-Bereitstellung erlauben	Mit dieser Option registrieren Sie Geräte für Autopilot über den normalen Registrierungsprozess. Diese Option ist nicht verfügbar, wenn die Option **Self-Deployment** ausgewählt ist.
Tastatur automatisch konfigurieren	Mit **Ja** überspringen Sie die Tastaturauswahl, wenn die Option **Sprache** nicht auf den Standardwert eingestellt ist, sondern auf einen anderen Wert.
Gerätenamensvorlage	Geben Sie einen Vorlagennamen ein, der während der Geräteregistrierung verwendet werden soll.
Microsoft Software-Lizenzbedingungen	Diese Option kann nur im benutzergesteuerten Bereitstellungsmodus ein- oder ausgeblendet werden.

Einstellung	Beschreibung
Datenschutzeinstellungen	Diese Option kann nur im benutzergesteuerten Bereitstellungsmodus ein- oder ausgeblendet werden.
Kontooptionen ändern	Diese Option kann nur im benutzergesteuerten Bereitstellungsmodus ein- oder ausgeblendet werden, wenn der Benutzerkontotyp „Standard“ aktiviert ist.

Windows-Geräteverwaltung

Der Administrator kann die Autopilot-Funktion für einen Mandanten über die neue Option "Windows-Geräteverwaltung" konfigurieren. Diese Option vereinfacht die Integration in Ivanti Neurons for MDM, falls der Benutzer über eine Entra ID-Umgebung verfügt.

Wechseln Sie zum Aufrufen dieser Option zu **Admin** > **Microsoft Azure** > **Windows-Geräteverwaltung**.

Diese Integration gewährt der Cloud Berechtigungen zum Verwalten von Geräten und Autopilot-Profilen, Überprüfen der Windows-Gerätecompliance und Validieren des Azure-Mandanten.

Verwandte Themen

- TenantLockdown CSP

Erstellen von Entra ID-Gerätegruppen

Der Administrator kann Entra ID-Gerätegruppen nach Bedarf über den Abschnitt "Entra ID-Gerätegruppen" erstellen. Die Entra ID-Mandantenvalidierung muss für die Erstellung von Entra ID-Gerätegruppen im Bereich "Geräte-Compliance" konfiguriert werden.

Verfahren

1. Wechseln Sie zu **Admin** > **Microsoft Azure** > **Entra ID-Gerätegruppen**.
2. Die Seite **Entra ID-Gruppeneinstellungen** wird auf dem Bildschirm angezeigt.
   Klicken Sie auf **ADD**.
3. Die Seite **Gruppeneinstellungen** wird auf dem Bildschirm angezeigt.
   Stellen Sie die folgenden Details bereit:
   - Gruppenname
   - Gruppenbeschreibung
   - Mitgliedschaftstyp
     - Statisches Gerät: Der Administrator kann die Liste der verfügbaren statischen Geräte über das Fenster **Mitglieder der Gruppe zuweisen** abrufen. Wählen Sie die erforderlichen Geräte aus, und klicken Sie auf **Speichern**.
     - Dynamisches Gerät: Der Administrator muss bestimmte Kriterien über das Fenster **Dynamische Anfrage** eingeben.

Die neue Entra ID-Gerätegruppe wird erstellt, und der Administrator kann Geräte zur neu erstellten Gruppe hinzufügen.

> Nach der Erstellung einer dynamischen Gruppe werden die Geräte nach einer gewissen Zeit auf der Registerkarte "Geräte" der jeweiligen Gerätegruppe angezeigt.

Autopilot-Geräte bearbeiten

Benutzer können die Autopilot-Geräte über das Ivanti Neurons for MDM-Administrationsportal bearbeiten.

Voraussetzungen

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Der IT-Administrator sollte über Azure Global Admin- und Intune Admin-Berechtigungen verfügen.
- Ein benutzerfreundlicher Name kann nur festgelegt werden, wenn der Benutzer festgelegt ist.
- Wenn ein Gerätename einmal festgelegt ist, kann er nicht mehr geändert werden.

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Gehen Sie zu **Admin** > **Windows** > **Autopilot**. Die Autopilot-Geräte werden auf der Registerkarte „Autopilot-Geräte“ aufgeführt.
3. Klicken Sie auf **Bearbeiten** (Bleistiftsymbol). Die Bearbeitungsseite wird angezeigt.
4. Bearbeiten Sie die folgenden Details:
    - **Benutzer**
    - **Benutzerfreundlicher Name**
    - **Gerätename**
    - **Gruppen-Tag**

Klicken Sie auf **Speichern**. Die Gerätedetails werden aktualisiert.

Autopilot-Geräte löschen

Benutzer können die Autopilot-Geräte über das Cloud-Administrationsportal löschen.

1. Melden Sie sich beim Ivanti Neurons for MDM-Administrationsportal an.
2. Gehen Sie zu **Admin** > **Windows** > **Autopilot**. Die Autopilot-Geräte werden auf der Registerkarte „Autopilot-Geräte“ aufgeführt.
3. Klicken Sie auf **Löschen**. Die Gerätedetails werden gelöscht.

12.4.2. Audit-Protokolle auf Windows Autopilot-Profilen

Mithilfe von Audit-Protokollen werden sämtliche Aktivitäten verfolgt, die auf allen Entitäten in der Cloud durchgeführt wurden. Diese Aktivitäten umfassen unter anderem das Hinzufügen, Löschen und Aktualisieren von neuen Geräten.

Weitere Informationen finden Sie unter **Audit-Protokolle**.

Der Administrator kann mithilfe von Audit-Protokollen die folgenden Aktivitäten auf allen Windows-Geräten durchführen, die im Autopilot-Modus registriert sind:

Autopilot-Profile

- Erstellen
- Bearbeiten
- Löschen
- Profil zu Gruppen zuweisen

Autopilot-Geräte

- CSV-Datei hochladen
- Bearbeiten
- Löschen

12.4.3. TenantLockdown CSP

Mit der TenantLockdown-CSP-Funktion kann der Administrator alle Windows-Geräte an Mandanten binden. Damit diese Funktion verwendet werden kann, müssen die Geräte mit der Autopilot-Option registriert werden. Diese Konfiguration kann auf Geräteebene erfolgen.

Beim Self-Deployment-Modus und beim benutzergesteuerten Modus in Autopilot kann der Administrator die Geräte direkt an die Mandanten binden. Dies ist für den Fall zweckmäßig, dass Geräte verloren gehen oder gestohlen werden. In diesen Fällen ist der Benutzer gezwungen, selbst dann eine Verbindung zum Mandanten herzustellen, wenn das Gerät zurückgesetzt wird, und die Erstellung eines lokalen Kontos im Self-Deployment-Modus wird nicht unterstützt. Falls die Kontoerstellung dagegen im benutzergesteuerten Modus verhindert werden muss, muss der Administrator bei der Konfiguration des Autopilot-Profils die Option **Ausblenden** für die Einstellung **Kontooptionen ändern** aktivieren.

Zum Aktivieren von TenantLockdown CSP kann der Administrator eine Windows-Einschränkungskonfiguration erstellen und die Option **Benutzer müssen sich bei der Einrichtung des Geräts mit dem Netzwerk verbinden (Autopilot-Profil erforderlich)** unter **Andere Einschränkungen** aktivieren.

Soll ein Gerät aus TenantLockdown CSP entfernt werden, muss der Administrator das Gerät manuell aus der Gruppe entfernen oder die Einschränkungen ändern.

12.4.4. ADMX (GPO) Browser

Mit dem ADMX (GPO) Browser können Sie die GPO-Einstellungen nach ADMX-Objekten des Mandanten sortiert anzeigen. Sie können die Standard-ADMX-Objekte suchen und anzeigen sowie spezifische ADMX-Dateien mit einer XML-Struktur zur Definition der Anzeige der GPO-Einstellungen ergänzen (hochladen).

Kundenspezifisches ADMX-Objekt hochladen:

1. Klicken Sie auf **Admin > ADMX (GPO) Browser**. Die Seite mit dem **ADMX (GPO) Browser** wird angezeigt.
2. Klicken Sie auf **Ergänzen**. Das Fenster **Kundenspezifische ADMX(GPO) Objekte ergänzen** wird angezeigt.
3. Klicken Sie auf die Option **Datei auswählen**, um die ADMX-Datei auszuwählen, die Sie hochladen wollen.

> Stellen Sie sicher, dass es sich bei der ADMX-Datei um eine komprimierte Datei handelt.

4. Klicken Sie auf **Ergänzen**. Bei erfolgreichem Hochladen wird eine Bestätigungsmeldung angezeigt.

> Stellen Sie sicher, dass der Stammordner nach dem Entpacken der komprimierten Datei die Datei mit der Erweiterung *.admx* enthält.

GPO-Einstellungen suchen

Im ADMX (GPO)-Browser können Sie ein GPO suchen und auswählen, indem Sie auf die betreffenden Komponente im GPO-Hierarchiebaum auf der linken Seite klicken. Der GPO-Hierarchiebaum entspricht dem Pfad der Richtlinieneinstellungen. Sie können alternativ nach einer spezifischen GPO-Einstellung suchen, indem Sie den GPO-Namen oder den ADMX-Dateinamen im Suchfeld eingeben. Die Details der ausgewählten GPO-Einstellung werden auf der rechten Seite angezeigt.

12.4.5. App-Bestandsaufnahmeintervalle konfigurieren

Sie können die Intervalle für die Bestandsaufnahme von Windows 10-Anwendungen für die Bestände mehrerer App-Quelltypen festlegen. Die Intervalle werden verwendet, wenn die Datenschutzkonfiguration so eingestellt ist, dass sie alle Apps des Geräts erfasst.

1. Navigieren Sie zu Admin>App-Bestandsaufnahmeintervalle.
2. Wählen Sie das Intervall (in Stunden) zur Erfassung des App-Bestands aus der Dropdown-Liste für die folgenden App-Quelltypen.
    - **Bestandsaufnahmeintervall für Apps, die nicht aus dem App Store stammen**
    - **App Store-Bestandsaufnahmeintervall**
    - **Intervall für die Systembestandsaufnahme**
    - **Bestandsaufnahmeintervall für Win32**
      Die Intervalloptionen für die Erfassung des Windows App-Inventars liegen zwischen **24** und **48** Stunden. Der Standardwert ist **24** Stunden.

12.4.6. Hardware-Bestand

Sie können die Erfassung von Hardwareinformationen von Windows 10-Geräten aktivieren . Hardware-Bestandsdetails werden mit Bridge abgerufen.

1. Navigieren Sie zu Admin> Hardwarebestand.
2. Aktivieren Sie die Option **Erfassung des Hardwarebestands aktivieren**.
3. Wählen Sie in dem **Lagerintervall** die Häufigkeit für die Erfassung des Hardwarebestands. Folgende Optionen stehen zur Verfügung:
    - **Einmal am Tag**(Standard)
    - **Wöchentlich**
    - **Alle 30 Tage**

Wenn die Option Hardwarebestand aktiviert ist, können Sie die Hardwaredetails des Geräts auf der Registerkarte **Hardware** auf der Seite mit den Gerätedetails anzeigen.

12.5. Einrichtung mit Microsoft Azure

Dieser Abschnitt enthält die folgenden Themen:

- Verwendung von Microsoft Azure
- Entra ID Windows 10 Unified Endpoint Management-Setup
- Zuweisen der Entra ID UEM-App
- Verbinden von Ivanti Neurons for MDM mit der Entra ID-Benutzerquelle
- Azure-Mandant
- Administration > Microsoft Azure > Office 365 App-Schutz

12.5.1. Verwendung von Microsoft Azure

Ivanti Neurons for MDM kann mit Microsoft Azure für die nahtlose Registrierung Ihrer Benutzer auf Windows Desktops und Tablets eingerichtet werden, auf denen Windows 10 ausgeführt wird. Führen Sie die folgenden Schritte aus, um Ihre Instanzen zu konfigurieren und zu verbinden.

Dieser Abschnitt enthält die folgenden Themen:

Einrichten des Entra ID-Kontos

So richten Sie ein Entra ID-Konto ein:

1. Gehen Sie zu **https://azure.microsoft.com/en-in/pricing/purchase-options/**, um Ihr Azure-Konto zu erwerben.
2. Verwenden Sie Ihre Hotmail- oder Outlook.com-Adresse oder erstellen Sie ein neues Konto und registrieren Sie sich als neuer Benutzer.
3. Erwerben Sie mit einer der Bezahloptionen ein Azure-Konto und folgen Sie den Schritten zur Verifizierung.
4. Bitten Sie Microsoft, den Ivanti Neurons for MDM-Mandanten in die Zulassungsliste aufzunehmen.
5. Verwenden Sie das gleiche Hotmail- oder Outlook.com-Konto, mit dem Sie sich in Schritt 2 bei Entra ID unter **https://manage.windowsazure.com/https://manage.windowsazure.com/** als Administrator angemeldet haben.
6. Gehen Sie zu der Registerkarte **Domain**.
   Standardmäßig ist die Domain TestMiBGLRoutlook.onmicrosoft.com, diese wird für Ihr Konto erstellt, und alle erstellten Benutzer gehören zu dieser Domain. Gegebenenfalls können Sie eine kundenspezifische Domain neu erstellen.

Erstellen von Benutzern in Entra ID

So erstellen Sie Benutzer in Entra ID:

1. Gehen Sie zu Active Directory - > **Standardverzeichnis →Benutzer.**
2. Auswahl der Option „Benutzer hinzufügen“ → Wählen Sie den neuen Benutzer in Ihrem Unternehmen aus.
3. Geben Sie den Benutzernamen ein. Klicken Sie auf "Weiter" **(→)**.
   Die Seite **Benutzerprofil** wird angezeigt.
4. Geben Sie die Benutzerinformationen ein, beispielsweise Vorname, Nachname und angezeigter Name.
5. Weisen Sie dem Benutzer über das Dropdown-Menü die entsprechende Rolle zu.
6. Erstellen Sie ein vorläufiges Passwort.
   Der Benutzer muss dieses Passwort bei der ersten Anmeldung ändern.

Verbinden von Entra ID mit UEM für Windows 10-Geräte

So verbinden Sie Entra ID mit UEM:

1. **Wechseln Sie zu Admin > Microsoft Azure > Windows-Registrierung und Compliance mit Entra ID.**
2. Führen Sie die im Abschnitt **Entra ID Windows 10 Unified Endpoint Management-Setup** beschriebenen UEM-Setup-Schritte durch.
3. Führen Sie das Setup **Zuweisen der Entra ID UEM-App** im Azure-Portal durch.
4. Geben Sie im Ivanti Neurons for MDM-Administrationsportal den Domänennamen Ihres Entra ID-Kontos ein, klicken Sie auf "Azure-Portal verbinden" und markieren Sie anschließend das Kontrollkästchen.

5. Akzeptieren Sie nach erfolgreicher Anmeldung die Zustimmung, damit MobileIron AD Tenant Validation APP überprüfen kann, ob Ihre Cloud UEM APP eingerichtet ist. Es erscheint eine Meldung über einen erfolgreichen Verbindungsaufbau.

Microsoft Passport for Work für Windows 10-Geräte

Microsoft Passport for Work wird durch Windows Hello for Business ersetzt. Weitere Informationen finden Sie unter **Konfiguration von Windows Hello for Business**.

Entra ID-Registrierung für Windows-Geräte

Voraussetzungen

Benutzer müssen bei Ivanti Neurons for MDM registriert sein.

Verbinden Sie Ihre Domäne, um Benutzer auf ihren Windows 10+-Geräten zu registrieren.

1. Klicken Sie auf **Entra ID beitreten**.
2. Geben Sie Benutzername und Passwort ein.
3. Klicken Sie auf **Anmelden**.
4. Akzeptieren Sie die EULA.
5. Klicken Sie auf **PIN erstellen**.
    - Wenn Sie den Microsoft Passport für die Work PIN-Komplexität aktiviert haben, werden Sie aufgefordert, eine komplexe PIN entsprechend der konfigurierten Richtlinie zu definieren.
    - Entra ID authentifiziert den Benutzer und lädt ein JWT (JSON Web Token) auf das Gerät herunter.
    - Damit ist das Gerät registriert.
    - Der Benutzer wird vom Gerät zur Verifizierung aufgefordert.
6. Geben Sie die PIN ein und bestätigen Sie diese.
7. Klicken Sie auf **OK**.

Unterstützung mehrerer Benutzer für Windows-Geräte

Ivanti Neurons for MDM unterstützt Funktionen für mehrere Benutzer für Windows 10-Geräte, die bei Entra ID registriert sind. Dazu gehört die Push-Übertragung bestimmter Profile wie VPN, WLAN, Standard-E-Mail-Client-Profile und Zertifikate für einen einzelnen Benutzer und nicht für ein Gerät. Unterstützt wird auch die Verteilung von internen und öffentlichen Anwendungen für den angemeldeten Benutzer. Jedes Mal, wenn sich ein neuer Entra ID-Benutzer bei einem Gerät anmeldet, prüft Ivanti Neurons for MDM das Gerät und den Benutzer. Wenn der Benutzer neu ist, aktualisiert Ivanti Neurons for MDM das Gerät für den Benutzer. Wenn es sich bei dem Benutzer um einen vorhandenen Benutzer auf dem Gerät handelt, wird geprüft, welche Änderungen am Gerät und an den Benutzereinstellungen seit der letzten Anmeldung aktualisiert werden müssen.

Die Details zu dem am Gerät angemeldeten Entra ID-Benutzer werden an das Ivanti Neurons for MDM-Administrationsportal gemeldet. Wenn sich der Benutzer von dem Gerät abmeldet und der zweite Benutzer bei dem Gerät anmeldet, werden die Details des zweiten Benutzers auf der Gerätedetailseite aktualisiert.

Microsoft Store for Business mit UEM konfigurieren

Microsoft Store for Business ist ein Portal, das von Microsoft als Teil von Azure bereitgestellt wird. Administratoren können sich bei diesem Portal anmelden, Apps kaufen und diese auf alle verwalteten Geräte verteilen. Ivanti Neurons for MDM kann mit Microsoft

Store for Business konfiguriert werden, um Anwendungen über das Ivanti Neurons for MDM-Administrationsportal zu verwalten. Dazu sind folgende Schritte erforderlich:

Schritt 1: Entra ID-Anwendung im Microsoft Azure Portal registrieren

1. Öffnen Sie den ersten Browser und melden Sie sich im Portal von Microsoft Azure an (https://portal.azure.com/https://portal.azure.com/).
2. Klicken Sie auf der linken Seite auf **App-Registrierungen**.
3. Klicken Sie auf **+Neue Anwendungsregistrierung**
4. Geben Sie die folgenden Informationen ein, um MobileIron als Azure-App zu registrieren:
   - **Name**: Geben Sie einen Namen für die MobileIron-App ein. (In diesem Feld müssen Sie mindestens 4 Zeichen eingeben.)
   - **Anwendungstyp**: Wählen Sie Web-App / API.
   - **Anmelde-URL**: Geben Sie die URL ein, auf die die Gerätebenutzer zugreifen, um sich bei MobileIron anzumelden (obligatorisch).
5. Klicken Sie auf **Erstellen**, um die App hinzuzufügen und zur Azure-Startseite zurückzukehren.
6. Gehen Sie zu Einstellungen und erstellen Sie einen neuen Schlüssel.

Schritt 2: Anwendung als Verwaltungstool hinzufügen

1. Klicken Sie in den Einstellungen von Microsoft Store for Business auf „Verwalten“.
2. Verteilungseinstellungen
3. Aktivieren Sie im Tool „Verwaltung hinzufügen“ die erstellte Anwendung.

Konto im Admin-Portal verbinden

1. Gehen Sie zu **Administration > Microsoft Azure > Microsoft Store für Unternehmen**.
2. Markieren Sie im Schritt 1 **Entra ID-Anwendung registrieren** das Kontrollkästchen **Ja, ich habe diesen Schritt abgeschlossen**.
3. Markieren Sie im Schritt 2 **Verwaltungstool hinzufügen** das Kontrollkästchen **Ja, ich habe diesen Schritt abgeschlossen.**
4. Aktualisieren Sie im Schritt 3 „Konto verbinden“ die folgenden Felder:
   - Entra ID-Domäne
   - Anwendungsidentifikator
   - Anwendungsschlüssel
   - Synchronisierungsintervall (Stunden)
5. Klicken Sie auf **Verbinden**. In einer Bestätigungsmeldung wird mitgeteilt, dass der MobileIron Store for Business erfolgreich eingerichtet wurde.
6. Klicken Sie auf **App synchronisieren**. Nach erfolgreicher Synchronisierung wird der Status **Anwendungen erfolgreich synchronisiert** angezeigt.

Wenn der Microsoft Store für die App auf das Gerät übertragen wird, sind die App-Details auf der Registerkarte **Installierte Apps** in den Gerätedetails verfügbar. Jede von einem Gerät gemeldete Microsoft Store for Business-App kann in der Spalte **Quelle** als **Microsoft Store for Business** identifiziert werden.

12.5.2. Entra ID Windows 10 Unified Endpoint Management-Setup

Windows 10 Unified Endpoint Management (UEM) einrichten:

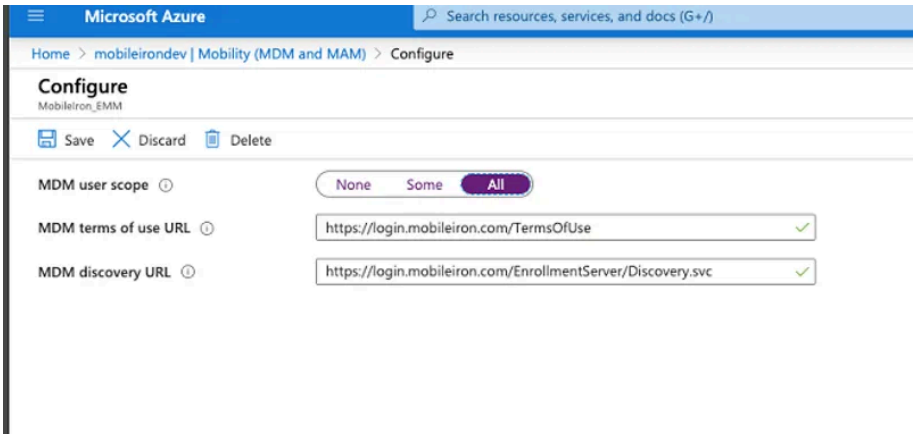
1. Melden Sie sich unter https://portal.azure.com/ als Admin-Benutzer an und wählen Sie Entra ID.
2. Wählen Sie in dem linken Fenster „Mobilität (MDM und MAM)“ und klicken Sie dann auf **Anwendung hinzufügen**.

3. Wählen Sie die App MobileIron_UEM aus der App-Galerie und klicken Sie auf **Hinzufügen**.


12.5.3. Zuweisen der Entra ID UEM-App

Einrichtung der Benutzerkonfiguration abschließen:

1. Klicken Sie auf die MobileIron UEM-App, die Sie in Schritt 2 unter **Entra ID Windows 10 Unified Endpoint Management-Setup** erstellt haben.
2. Weisen Sie ihn unter MDM-Benutzerbereich Ihren selbst definierten Benutzergruppen zu oder wählen Sie **Alle**.



12.5.4. Verbinden von Ivanti Neurons for MDM mit der Entra ID-Benutzerquelle

Um Entra ID verwenden zu können, müssen Sie Ivanti Neurons for MDM mit Details zu Ihrem Microsoft Entra ID-Konto konfigurieren. Sie benötigen ein vorhandenes und konfiguriertes Microsoft Entra ID-Konto. Diese Lösung erfordert weder einen Connector im LAN noch LDAP.

Dieser Abschnitt enthält die folgenden Themen:

- Anwendungsfälle
- Verwenden von Entra ID
- Entra ID-Einstellungen

Anwendungsfälle

In folgenden Anwendungsfällen können Sie Ivanti Neurons for MDM mit Entra ID verbinden:

- Sie arbeiten mit Microsoft Office 365.
- Sie konfigurieren Microsoft Entra ID, Microsoft ADFS oder einen anderen SAML-2.0-Identitätsanbieter (IdP) für die Benutzerauthentifizierung.
- Sie richten Microsoft Entra ID als Benutzerquelle ein.
- Sie synchronisieren Benutzer aus Microsoft Entra ID und starten. Alle Benutzer und Gruppen in Ihrer Entra ID-Domäne werden mit Ihrer Ivanti Neurons for MDM-Instanz synchronisiert.
  Wenn bei der Entra ID-Synchronisierung aus den unten genannten Gründen ein Fehler auftritt, wird eine Benachrichtigung auf der Seite **Benachrichtigungen** angezeigt.
  - Der Entra-Dienst ist nicht erreichbar.
  - Es werden keine Benutzerattribute mit Entra ID synchronisiert.
  - Einige Benutzerattribute werden nicht mit Entra ID synchronisiert.
- Umgebungen mit mehreren IdPs werden derzeit nicht unterstützt.
- Wenn Sie Microsoft Entra ID nicht als Benutzergruppe verwenden, können Sie lokale Konten oder Quellenbenutzer aus LDAP verwenden. Dazu muss ein Connector für den Zugriff auf die LDAP-Ressourcen im lokalen Netzwerk konfiguriert werden.
- Die Verwendung von Microsoft Entra ID allein für die Benutzer-Authentifizierung und die Verwendung von lokalem LDAP für das Benutzerverzeichnis werden derzeit nicht unterstützt.

Verwenden von Entra ID

Um Entra ID zu verwenden, richten Sie Ihren Identitätsanbieter mit einem der folgenden Verfahren für die Benutzerauthentifizierung ein:

- Um Microsoft Entra ID sowohl als Benutzerquelle als auch zur Benutzerauthentifizierung zu nutzen, konfigurieren Sie Entra ID als Ihren IdP. Wechseln Sie zu **Admin > Identität > Ivanti Neurons for MDM-Setup** und wählen Sie aus dem Menü **Entra ID** aus.
- Um Microsoft Entra ID als Benutzerquelle und ADFS zur Benutzerauthentifizierung zu verwenden, konfigurieren Sie ADFS als Ihren IdP. Wechseln Sie zu **Administrator > Identität > IdP-Setup im lokalen Netzwerk** und wählen Sie aus dem Menü "ADFS" aus.

- Wenn Sie einen anderen SAML 2.0-Identitätsanbieter als Entra ID und ADFS zur Benutzer-Authentifizierung verwenden möchten, wechseln Sie zu **Admin > Identität > Generisches IdP-Setup** und folgen Sie den Anweisungen auf der Seite.

Weitere Informationen finden Sie unter **Identity Provider konfigurieren**.

Entra ID-Einstellungen

Dieses Thema unterstützt Sie bei der Konfiguration der Entra ID-Einstellungen.

Verfahren

1. Wechseln Sie zu **Admin > Microsoft Azure > Entra ID-Benutzerquelle**.
2. Geben Sie die folgenden Details an:
    1. Den **Entra ID-Namen**
    2. **Synchronisierungsintervall** – Ändern Sie die Häufigkeit, mit der Ivanti Neurons for MDM die Benutzerdaten aus Ihrem Entra ID synchronisiert.
    3. **Dieses Entra ID aktivieren** – Verwenden Sie diese Option, um eine Entra ID-Instanz zu aktivieren oder zu deaktivieren.
    4. Wählen Sie **Aus Entra ID importierte Benutzer automatisch einladen** aus und legen Sie fest, ob aus Entra ID in Ivanti Neurons for MDM importierte Benutzer automatisch per E-Mail zur Registrierung eingeladen werden sollen.
    5. Wählen Sie **Verwaltete Apple-ID** aus und legen Sie fest, dass die verwaltete Apple-ID für Entra ID-Benutzer synchronisiert werden soll.
        - **Keine**
        - **Muster**
            - **E-Mail-Adresse des Benutzers**
            - **userUPN**
            - (Optional) Wählen Sie die Option "appleid-Subdomäne einschließen" aus, um Konflikte mit bestehenden Apple-IDs zu vermeiden.
    6. (Optional) Klicken Sie auf **Benutzerdefiniertes Attribut hinzufügen** - Definieren Sie für Ihren Verzeichnisdienst anpassbare Benutzerattribute für die Geräteverwaltung. Auf jedes Attribut kann dann mit $ in den Konfigurationsfeldern zugegriffen werden, die Variablen unterstützen. Für diese Option benötigen Sie eine konsistente Implementierung der benutzerdefinierten Attribute für alle Entra ID-Server. Wenn ein in Ihrer Implementierung enthaltener Entra ID-Server dieses Attribut nicht verwendet, funktionieren die von diesem Attribut abhängigen Optionen möglicherweise nicht wie erwartet.

Klicken Sie auf **Speichern**, nachdem Sie die Entra ID-Einstellungen geändert haben.

12.5.5. Azure-Mandant

Dieser Abschnitt enthält die folgenden Themen:

- Anforderungen
- Intune-Lizenz für Gerätebenutzer übernehmen.
- MobileIron als Compliance-Partner hinzufügen
- Richtlinie für bedingten Zugriff im Microsoft Endpoint Manager erstellen
- Verbinden von Microsoft Azure mit Ivanti Neurons for MDM
- Konformitätsrichtlinie für Partnergeräte erstellen
- Melden des Gerätestatus von Ivanti Neurons for MDM an Azure
- Bereitstellung des Azure-Mandanten aufheben

12.5.5.1. Azure Tenant Requirements

Dieser Abschnitt beschreibt die Einrichtung der Cloud mit Microsoft Azure Tenant.

Anforderungen

Microsoft

Cloud-Kunden müssen ein gültiges Abonnement für Microsoft Intune haben und den Gerätebenutzern eine Microsoft Intune-Lizenz zuweisen.

MobileIron

- Ivanti Neurons for MDM – Ivanti Neurons for MDM Version 75 bis zur neuesten von MobileIron unterstützten Version.
- Zusätzliche Lizenzierung - Azure Device Compliance ist ein Premium-Angebot und für **Secure UEM Premium** und Platinum-Kunden verfügbar. Für Bestandskunden reicht eine Platinum-Lizenz aus.
- Go for iOS (Client) oder Go for Android (Client) Version 75.0 bis zur neuesten Version, die von MobileIron unterstützt wird.

Unterstützung für mehrere Instanzen von Ivanti Neurons for MDM

Wenn Sie mehrere Clouds mit demselben Azure-Mandanten verbunden haben, trennen Sie die Verbindungen zu allen Clouds oder deaktivieren Sie die Konformitätsrichtlinie für die Entra ID-Compliance-Integration einer bestimmten (einzelnen) Cloud, damit sie keine Gerätedaten in Azure hochlädt.

> Stellen Sie sicher, dass Sie die Konformitätsrichtlinie vor der Trennung der Cloud deaktivieren.

Prozess für den Administrator von Ivanti Neurons for MDM

Der Prozess aus der Sicht des Cloud-Administrators:

1. Der Administrator übernimmt die Intune-Lizenzen für die Gerätebenutzer. Siehe dazu **Intune-Lizenz für Gerätebenutzer übernehmen.**.
2. Der Administrator meldet sich beim Azure-Portal an.
3. Der Administrator fügt MobileIron als Azure-Compliance-Partner hinzu. Siehe dazu **MobileIron als Compliance-Partner hinzufügen**.
4. Der Administrator erstellt die Richtlinie für den bedingten Zugriff für die Apps. Siehe dazu **Richtlinie für bedingten Zugriff im Microsoft Endpoint Manager erstellen**.
5. Der Administrator richtet die Verbindung zwischen MobileIron und Azure ein. Siehe **Verbinden von Microsoft Azure mit Ivanti Neurons for MDM**.
6. Der Administrator erstellt die Gerätekonformitäts-Richtlinie in der Cloud. Siehe dazu **Konformitätsrichtlinie für Partnergeräte erstellen**.
7. Die Richtlinie für bedingten Zugriff tritt in Kraft. Je nachdem, ob das Gerät konform ist oder nicht, wird der Zugriff auf die App(s) gewährt oder verweigert.

> Ivanti empfiehlt dem Administrator, für jede Microsoft-App Tests durchzuführen.

12.5.5.2. Intune-Lizenz für Gerätebenutzer übernehmen.

- Verwenden Sie diese Funktion nicht, wenn:
  - Sie Benutzer ändern oder Situationen verwalten, in denen wahrscheinlich die Benutzer wechseln.
  - das Gerät im Besitz von mehreren Benutzern ist
- Ivanti empfiehlt, die Option Benutzer zuweisen nicht auszuführen und die Gerätekonformitätskonfiguration nicht auf Geräte mit mehreren Benutzern zu verteilen, beispielsweise:
  - Geräte mit Secure Sign-In WebClip
  - gemeinsam genutzte iPads
  - Geräte im Android Kiosk-Modus

Ivanti Neurons for MDM -Lizenzanforderungen

Device Compliance ist ein Premium-Angebot und steht Secure UEM Premium- und Platinum-Kunden zur Verfügung. Für Bestandskunden ist eine Platinum-Lizenz ausreichend.

Massenlizenzen Gerätebenutzern zuweisen

Vorhandenen Gerätebenutzern massenhaft Lizenzen zuweisen:

Gruppenbasierte Zuweisung

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

PowerShell-basierte Zuweisung

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. MobileIron als Compliance-Partner hinzufügen

Voraussetzungen

- eine installierte Microsoft Intune-Lizenz Siehe dazu **Intune-Lizenz für Gerätebenutzer übernehmen.**.
- in Microsoft Azure angelegte Benutzer
- in Microsoft Azure erstellte Gruppen

Verfahren

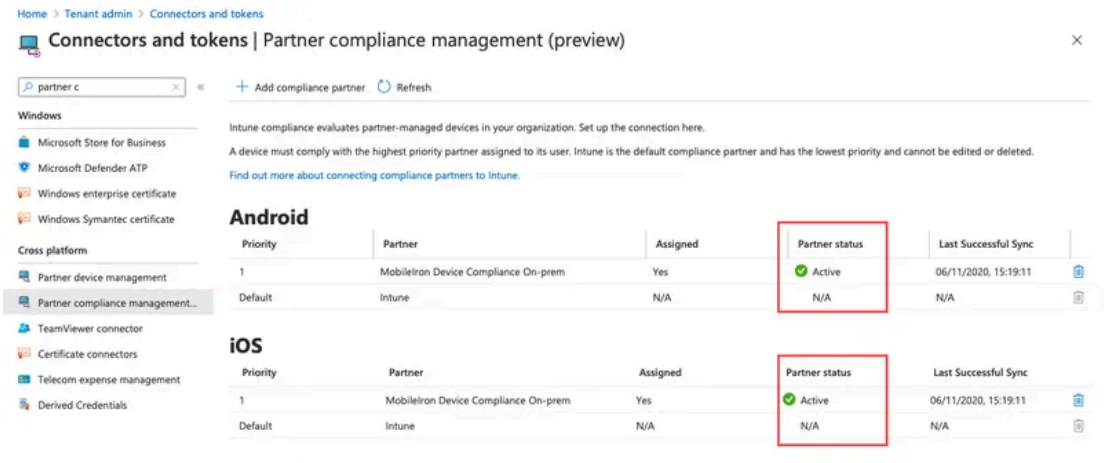
1. Melden Sie sich an unter: **https://endpoint.microsoft.com**.
2. Klicken Sie im linken Bereich der Seite des Microsoft Endpoint Manager Admin Center auf Mandanten-Administrator. Klicken Sie auf Connectors and Tokens > Partner-Konformitätsverwaltung.

3. Klicken Sie rechts neben dem Suchfeld auf + Compliance-Partner hinzufügen.

4. Wählen Sie auf der Registerkarte „Grundlagen“ MobileIron Device Compliance Cloud aus der Dropdown-Liste des Feldes Compliance-Partner.

5. Wählen Sie im Feld „Plattform“ die Option iOS oder Android und klicken Sie dann auf Weiter.
6. Klicken Sie auf die Registerkarte Zuweisungen. Wählen Sie in der Dropdown-Liste „Zuweisen“ den Benutzer/die Gruppe von Gerätebenutzern aus, für die der Konformitätsstatus gelten soll. Wählen Sie den Benutzer / die Gruppe aus, die Lizenzinhaber ist.

7. Wählen Sie Weiter.
8. Klicken Sie auf Erstellen. Der neue Compliance-Partner erscheint auf der Seite „Partner-Konformitätsverwaltung“.



12.5.5.4. Richtlinie für bedingten Zugriff im Microsoft Endpoint Manager erstellen

Verfahren

1. Melden Sie sich im Microsoft Endpoint Manager an (unter **https://endpoint.microsoft.com**).
2. Gehen Sie auf der Seite des Microsoft Endpoint Manager Admin Center zu Home > Endpunkt-Sicherheit > Bedingter Zugriff.
3. Klicken Sie auf „Richtlinien“ und dann auf + Neue Richtlinie.

4. Geben Sie den Namen der Richtlinie für den bedingten Zugriff ein.

5. Klicken Sie in „Zuweisungen“ auf „Richtlinie Benutzern und Gruppen zuweisen“.

6. Klicken Sie auf Cloud-Apps oder -Aktionen und dann auf Wählen. Suchen Sie die zu schützenden Apps und wählen Sie diese aus.

7. Klicken Sie auf „Bedingungen“ und dann auf Geräteplattform. Wählen Sie die entsprechenden Geräteplattformen aus.

8. Klicken Sie auf der Seite Neue bedingte Zugriffsrichtlinie > Zugriffskontrollen auf Gewähren und wählen Sie die Zugriffe und Sperren aus.

9. Um die neue Richtlinie zu aktivieren, klicken Sie auf Ein.

10. Klicken Sie auf Erstellen.

12.5.5.5. Verbinden von Microsoft Azure mit Ivanti Neurons for MDM

Verfahren

1. Ivanti Neurons for MDMMelden Sie sich bei an und wechseln Sie zu Admin > Microsoft Azure.
2. Klicken Sie im linken Navigationsbereich auf Microsoft Azure > Geräte-Konformität.
3. Geben Sie im Abschnitt "Konto verbinden" folgende Details an:
    - **Azure-Mandanten-ID** - Suchen Sie in Ihrer Microsoft Azure-Instanz.
    - **Registrierungs-URL (Optional)** – Wenn das Gerät nicht für MDM registriert ist, werden die Benutzer zur Registrierung auf diese URL verwiesen. Verwenden Sie zur Konfiguration das HTTPS-Format. Wenn Sie in Ihrem Unternehmen eine Seite hosten, die Ihre Gerätebenutzer zu den Registrierungsinformationen weiterleitet, fügen Sie diesen Link hier ein.
    - **Behebungs-URL (Optional)** – Wenn das Gerät nicht konform ist, werden die Gerätebenutzer zur Behebung auf diese URL verwiesen. Verwenden Sie zur Konfiguration das HTTPS-Format. Wenn Sie in Ihrer Organisation eine Seite hosten, die Ihre Gerätebenutzer zu Informationen zur Fehlerbehebung weiterleitet, fügen Sie diesen Link hier ein.
4. Klicken Sie auf **Konto verbinden**. Das Dialogfeld für die Azure-Mandantenvalidierung wird angezeigt.

> Mandanten, die bereits mit Azure verbunden sind und Geräte-Compliance für macOS-Geräte hinzufügen möchten, müssen die Kontoverbindung trennen und dann erneut herstellen.

5. Klicken Sie im Dialogfeld für die Azure-Mandantenvalidierung auf den **Link** in Schritt 1.
6. **Anmelden**.
7. Überprüfen Sie die Berechtigungen und klicken Sie dann auf **Akzeptieren**.

> Wenn Sie sich anmelden und aufgefordert werden, sich erneut anzumelden, schließen Sie die Browserregisterkarte/das Browserfenster.

8. Kehren Sie zurück zu Ivanti Neurons for MDM. Aktivieren Sie im Dialogfeld „Azure-Konto verbinden“ das Kontrollkästchen **Ich habe zugestimmt**. Klicken Sie auf **Bestätigen**.

- Um das Konto zu bearbeiten, klicken Sie auf **Konto bearbeiten**.
- Um die Verbindung zum Konto zu trennen, klicken Sie auf **Konto trennen**. Weitere Anweisungen finden Sie unter **Bereitstellung des Azure-Mandanten aufheben**.
- Alle Aktivitäten zum Hinzufügen, Bearbeiten und Deaktivieren eines Kontos werden in den Protokollen aufgezeichnet.

12.5.5.6. Konformitätsrichtlinie für Partnergeräte erstellen

Erstellen Sie eine Konformitätsrichtlinie für Partnergeräte in Ivanti Neurons for MDM und vergeben Sie die gewünschte Bezeichnung. Die Konformitätsrichtlinie für Partnergeräte meldet den Compliance-Status des Geräts für den bedingten Zugriff an Azure oder BeyondCorp.

Gilt für:

- iOS-
- Android
- Windows

Voraussetzungen

Sie müssen eine Azure-Mandanten-ID oder eine Google BeyondCorp-ID eingerichtet haben. Weitere Informationen zur Azure-Partnergerätekonformität finden Sie unter **Verbinden von Microsoft Azure mit Ivanti Neurons for MDM**.



Verfahren

1. Melden Sie sich bei Ivanti Neurons for MDM an und wechseln Sie zu **Konfigurationen**.
2. Klicken Sie auf **Hinzufügen** und machen Sie die Konfiguration **Partnergerätekonformität** ausfindig.
3. Geben Sie auf der Seite **Partnergerätekonformitäts-Konfiguration erstellen** folgende Details ein.

Objekt	Beschreibung
[Name]	Geben Sie einen Namen ein.
+ Beschreibung hinzufügen	Geben Sie eine Erläuterung ein.
Partner wählen	Wählen Sie **Microsoft Azure-Compliance** oder **Google BeyondCorp-Compliance – Beta** aus.
Konfigurations-Setup Azure den Compliance-Status für iOS-, macOS- und Android-Geräte melden	Standardmäßig EINgeschaltet. Wenn Sie dieses Feld nicht sehen, müssen Sie zuerst Ihre Azure-Mandanten-ID einrichten. Wenn die Option "Azure den Compliance-Status für iOS-, macOS- und Android-Geräte melden" aktiviert ist und die Konformitätsrichtlinie auf den Client angewendet wird, zeigt der Client in den Geräteeinstellungen "Microsoft 365 Access" an. Der Konformitätsstatus des Geräts wird gemeldet, wenn: • das Gerät nicht konform ist • das Gerät konform ist • das Gerät wieder konform ist • 24 Stunden abgelaufen sind. Wenn sich der Status nicht ändert, wird nur einmal pro Woche/alle sieben Tage ein Bericht gesendet.
Google BeyondCorp den Compliance-Status für iOS-, macOS- und Android- und Windows-Geräte melden	Standardmäßig EINgeschaltet. Der Konformitätsstatus des Geräts wird gemeldet, wenn: • das Gerät nicht konform ist • das Gerät konform ist • das Gerät wieder konform ist • 24 Stunden abgelaufen sind. Wenn sich der Status nicht ändert, wird alle 24 Stunden ein Bericht gesendet.

4. Klicken Sie auf **Weiter**.
5. **Diese Konfiguration aktivieren** ist standardmäßig ausgewählt.
6. Wählen Sie eine Verteilungsebene für die Konfiguration. Weitere Informationen zur Konfigurationsverteilung finden Sie unter Konfiguration hinzufügen.
7. Klicken Sie auf **Fertig**.

12.5.5.7. Melden des Gerätestatus von Ivanti Neurons for MDM an Azure

In den folgenden Fällen meldet die Cloud den Gerätebestand und den Konformitätsstatus.

- Änderung des Konformitätsstatus auf dem Gerät
- Bestandsänderung auf dem Gerät
- Einmal pro Woche meldet die Cloud den Konformitätsstatus und den Bestandsstatus.

Je nach der in der Konformitätsrichtlinie gewählten Aktion wird folgender Gerätestatus gesendet:

Aktion **(es gilt die restriktivste Variante)**	**Das sendet Ivanti Neurons for MDM:**
E-Mail blockieren, AppConnect Apps, Quarantäne	Gerät nicht konform
[Send Alert]	Konform mit Azure
Gerät löschen	Gerätedaten von der Azure-Plattform entfernt

Seite „Gerätedetails“

Um die Azure-Informationen über das Gerät anzuzeigen, wechseln Sie zur Seite „Gerätedetails“. Die Beschreibung der Felder und ihrer möglichen Werte:

Feld	Beschreibung
ID des Azure-Geräts	Die von Microsoft an das iOS- oder Android-Gerät gemeldete Geräte-ID. Beispiel: 007c8232-9489-4074-9b35-345b16f0a72d. Die Cloud erhält diese Geräte-ID, da sich die Gerätebenutzer bei der Microsoft Authenticator-Anwendung registrieren müssen, um diese Funktion zu nutzen. Wenn die Geräte-ID nicht abgerufen werden kann, bleibt dieses Feld leer.
Compliance-Status des Azure-Geräts	Listet den Konformitätsstatus des Geräts in Azure auf. Mögliche Werte: • Wird ausgeführt • Erfolgreich • Fehlgeschlagen
Azure Client-Status-Code	Zeigt an, ob das Gerät mit Azure verbunden ist. Mögliche Werte: • Success - Die Geräte-ID konnte abgerufen werden. • Internal_Error - Ein nicht behebbarer Fehler ist entweder innerhalb des Clients oder auf der Serverseite aufgetreten. • Workplace_Join_Required - Registrierung des Geräts erforderlich. Der Gerätebenutzer kann diesen Status abschwächen. • Interaction_Required - Eine interaktive Anmeldung ist erforderlich. Der Gerätebenutzer kann diesen Status abschwächen. • Server_Declined_Scopes - Für einige Bereiche wurde kein Zugriff gewährt. • Server_Protection_Policies_Required - Die angeforderte Ressource ist durch eine Intune-Richtlinie für bedingten Zugriff geschützt. • User_Canceled - Der Gerätebenutzer brach die Web-Auth-Sitzung ab, indem er im Webbrowser auf die Schaltfläche „Fertig“ oder „Abbrechen“ tippte. • Account_logged_out - Konto wurde abgemeldet.
Zeit des Compliance-Berichts für das Azure-Gerät	Die Zeit, zu der die Cloud den Konformitätsstatus des Geräts an Microsoft Intune meldete. Ein leeres Feld zeigt eine der folgenden Möglichkeiten an: • die Funktion ist deaktiviert • Die Cloud erhielt die Daten, muss aber noch die Microsoft-API aufrufen • es liegt ein Fehler vor, beispielsweise user_Cancelled oder Internal_Error

12.5.5.8. Bereitstellung des Azure-Mandanten aufheben

Wenn mehrere Instanzen von Ivanti Neurons for MDM für denselben Azure-Mandanten aktiviert sind, deaktivieren Sie die Bereitstellung in all diesen Instanzen. Wenn eine einzelne Cloud Azure nicht mehr nutzen darf, können Sie die Partner-Konformitätsrichtlinie für diese Cloud nur deaktivieren.

Wenn der Administrator die Verbindung zu Cloud trennt, meldet die Cloud den Gerätebestand und den Konformitätsstatus nicht mehr an Azure.

Voraussetzungen

- Stellen Sie sicher, dass alle Geräte nicht verwaltet sind.
- Stellen Sie sicher, dass alle Geräte als nicht konform eingestuft sind.

Verfahren

Microsoft

1. Melden Sie sich bei Microsoft Azure an.
2. Gehen Sie zu Intune > Bedingter Zugriff. Stellen Sie sicher, dass die Richtlinie für bedingten Zugriff deaktiviert ist.

Ivanti Neurons for MDM

1. Melden Sie sich bei Ivanti Neurons for MDM an und wechseln Sie zu Admin.
2. Klicken Sie im linken Navigationsbereich auf Microsoft Azure > Geräte-Konformität für iOS & Android.
3. Klicken Sie auf Kontoverbindung trennen.



4. Klicken Sie auf [Yes].

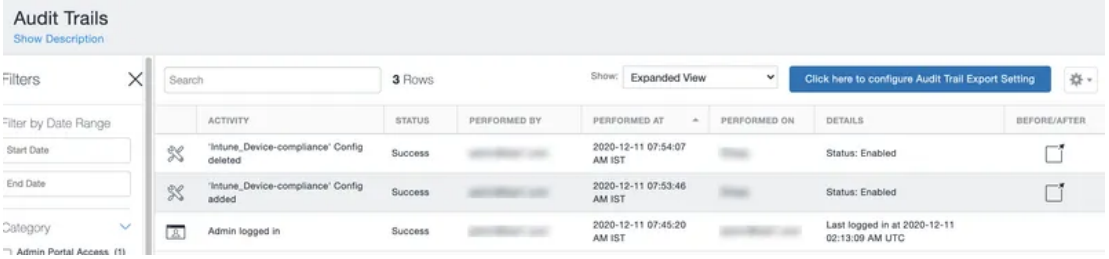
Gerät in Azure außer Dienst stellen

Wenn das Gerät außer Dienst gestellt wird, meldet die Cloud an Azure, dass das Gerät nicht mehr verwaltet wird und nicht mehr konform ist.

Azure löscht den Eintrag des außer Dienst gestellten Geräts nach 90 Tagen.

In den Protokollen aufgezeichnete Azure-Kontoaktivitäten

Alle Aktivitäten werden in den Protokollen aufgezeichnet.



12.5.6. Administration > Microsoft Azure > Office 365 App-Schutz

Lizenz: Gold

Sie können die Richtlinien zum Schutz der Apps in Office 365 konfigurieren, um Ihre Unternehmensdaten besser zu schützen. Die Richtlinien erzwingen Kontrollen zur Vermeidung von Datenverlust (DLP) für Apps in Microsoft Office 365 mit Microsoft Graph APIs. Mit einigen dieser Graph-APIs können Administratoren einen App-Schutz für native iOS- und Android-Apps erzwingen, die das Graph-SDK nutzen.

Mit dieser Funktion können Sie beispielsweise Richtlinien erzwingen, mit denen:

- Benutzer nicht aus Apps in Office 365 drucken können.
- Aus Apps in Office 365 keine Daten mit anderen Apps geteilt werden können.
- Für Apps in Office 365 die PIN-Eingabe erzwungen wird.
- Die Kontaktsynchronisation für Apps in Office 365 deaktiviert wird.

Voraussetzungen für den Schutz der Apps in Office 365

Bevor Sie den Schutz für die Apps in Office 365 verwenden können, müssen Sie über Folgendes verfügen:

- Eine gültige MobileIron-Lizenz.
- Office 365 App-Schutzfunktion in der Cloud aktiviert
- Ein gültiges Intune-Abo bzw. ein Microsoft EMS-Abo, das ein Intune-Abo enthält.
  - Für jede Nutzung der Richtlinie ist eine Lizenz erforderlich, für die Aktivierung und den Test der Integration jedoch nur eine einzige Lizenz.
- Ein gültiges Abo für Office Enterprise oder Business mit Zugriff auf die Apps von Office 365 auf einem Mobilgerät.
- Mindestens eine App von Office 365.
- Ihre Active Directory-Benutzer müssen mit Entra ID synchronisiert sein.
- Auf den Geräten muss ein Laufwerk für das Unternehmen installiert sein, um die Daten in Word, Excel und PowerPoint zu schützen. Letzteres ist nicht Pflicht.
- Rufen Sie das Microsoft Azure-Portal (**https://portal.azure.com/**) auf, um Richtlinien zum Schutz von Intune-Apps zu konfigurieren.
- Die App für das Intune-Firmenportal muss auf den Android-Geräten installiert sein.
  Die Gerätebenutzer müssen sich nicht anmelden, die App muss jedoch auf dem Gerät installiert sein, um die Daten auf dem Gerät zu schützen. Der Schutz gilt, wenn der Benutzer sich für die App anmeldet.

Registrierung von MobileIron als Azure-App

Dieses Thema beschreibt, wie Sie Ihren Azure-Mandanten registrieren, die Azure-Mandantenanmeldeinformationen in der Cloud speichern und Anwendungsschutzrichtlinien in der Microsoft Azure Cloud für Apps von Office 365 in Android und iOS aus der Ferne verwalten. Sie können (müssen aber nicht) zwei Browser öffnen, um die Schritte in den folgenden Prozeduren auszuführen. Benutzen Sie den ersten Browser, um sich im Microsoft Azure-Portal anzumelden. Benutzen Sie den zweiten Browser, um sich im Cloud-Administrator-Portal anzumelden.

Prozeduren für das Microsoft Azure-Portal

> Microsoft kann die Benutzeroberfläche des Azure-Portals von Zeit zu Zeit ändern. Diese Anleitung setzt voraus, dass Sie mit dem Microsoft Azure-Portal vertraut sind und notwendige Anpassungen vornehmen können, wenn Sie MobileIron als Azure-App registrieren.

1. Öffnen Sie den ersten Browser und melden Sie sich im Portal von Microsoft Azure an (**https://portal.azure.com/**).
2. Klicken Sie auf der linken Seite auf **App-Registrierungen**.
3. Klicken Sie auf **+Neue Anwendungsregistrierung**.
4. Geben Sie die folgenden Informationen ein, um MobileIron als Azure-App zu registrieren.
    - **Namen:** Geben Sie einen Namen für die MobileIron-App ein. (In diesem Feld müssen Sie mindestens 4 Zeichen eingeben.)
    - **Anwendungsart:** Wählen Sie Web-App / API aus.
    - **Anmelde-URL:** Geben Sie die URL ein, auf die die Gerätebenutzer zugreifen, um sich bei MobileIron anzumelden (obligatorisch).

Klicken Sie am unteren Rand der Seite auf **Erstellen**, um die App hinzuzufügen und zur Azure Homepage zurückzukehren.

6. Klicken Sie auf die neu erstellte MobileIron-App auf der Azure Homepage.
7. Kehren Sie zurück zur Azure-Homepage, um die Berechtigungen für die MobileIron-Azure-App zuzuordnen.
8. Um die erforderlichen API-Berechtigungen für die neu erstellte MobileIron-App festzulegen, klicken Sie unter „Anwendungsregistrierungen“ auf den App-Namen.
9. Klicken Sie auf **API-Berechtigungen** > **Berechtigung hinzufügen**.
10. Wählen Sie im Abschnitt Microsoft Graph > Delegierte Berechtigungen > DeviceManagementApps die Berechtigung DeviceManagementApps.Read.All und klicken Sie auf Speichern.Standardmäßig ist die Berechtigung user.read für die App aktiviert.
11. Um Zugang zu gewähren, klicken Sie auf **Zustimmung des Administrators für MobileIron gewähren**.
12. Führen Sie für das Verwaltungsportal Ivanti Neurons for MDM folgende Schritte durch.

Verfahren für das Ivanti Neurons for MDM-Administratorportal

1. Öffnen Sie den zweiten Browser und melden Sie sich im Cloud-Administratorportal an.
2. Gehen Sie zu **Administration > Microsoft Azure > Office 365 App-Schutz**.
3. Fügen Sie dazu die **App-ID** wie folgt in das Verwaltungsportal Ivanti Neurons for MDM ein:
4. **Verfahren**
    1. Gehen Sie zu dem Azure-Portal.
    2. Klicken Sie auf MobileIron App >**Eigenschaften**.
    3. Kopieren Sie die **Anwendungs-ID**.
    4. Kehren Sie zu **Admin > Microsoft Azure > Office 365 App-Schutz** im Admin-Portal zurück.
    5. Fügen Sie die Anwendungs-ID in dem Feld **Anwendungs-ID** ein.

Fügen Sie das **Anwendungs-Gruppenpasswort** (Client-Gruppenpasswort) im Ivanti Neurons for MDM Administrationsportal ein.

5. **Verfahren**
    1. Gehen Sie zu dem Azure-Portal.

2. Wählen Sie die MobileIron-App aus.
3. Klicken Sie auf **Schlüssel** und geben Sie einen Namen als **Schlüsselbeschreibung** ein; wählen Sie dann einen Verfallstermin unter **Dauer** aus.
4. Klicken Sie auf **Speichern** und kopieren Sie den **Schlüssel**-Wert.
5. Kehren Sie zu **Admin > Microsoft Azure > Office 365 App-Schutz** im Admin-Portal zurück.
6. Fügen Sie den Schlüsselwert in dem Kunden-Gruppenpasswortfeld **Anwendungs-Gruppenpasswort** ein.

Fügen Sie die **Mandanten-ID** im Ivanti Neurons for MDM Administrationsportal ein.

6. **Verfahren**
    1. Gehen Sie zu dem Azure-Portal.
    2. Klicken Sie auf der linken Seite auf "Entra ID" und dann auf "Eigenschaften".
    3. Kopieren Sie die Directory-ID.
    4. Kehren Sie zu **Admin > Microsoft Azure > Office 365 App-Schutz** im Admin-Portal zurück.
    5. Fügen Sie diese in dem Feld **Mandanten-ID** ein.

Geben Sie Ihren **Benutzernamen** als Intune-Administrator und das **Passwort** ein.

- Das Azure-Konto sollte entweder globale Admin-Rechte oder eingeschränkte Admin- + Verwaltungsrechte für den Intune-Dienst haben.
- Ivanti empfiehlt, ein lokales Azure-Konto nur mit den Administrationsrechten für den Intune-Dienst zu erstellen. Benutzerkonten, die mit einem Identitätsanbieter verbunden sind, werden von Microsoft zur Authentifizierung mit den Grafik-APIs nicht unterstützt.

Klicken Sie auf **Authentifizieren und speichern**.
Wenn das übergebene Datum falsch ist, wird eine Fehlermeldung angezeigt.

Richtlinien zum Schutz der App Office 365

Gehen Sie nach der Konfiguration der Anmeldeinformationen für Microsoft Graph zu **Apps > Schutz von Office 365**, um neue Richtlinien zum Schutz der Apps in Office 365 für iOS- oder Android-Geräte für verschiedene Benutzergruppen zu ergänzen.

Die Richtlinien finden Sie auf der Seite **Apps > App zum Schutz von Office 365** auf der Registerkarte **App-Richtlinien**. Diese Richtlinienliste enthält in einer Tabelle Details wie den aktualisierten Zeitstempel, die Plattform, die zugeordneten Apps und die bereitgestellten Benutzergruppen.

Richtlinie zum Schutz der Apps in Office 365 für iOS-Geräte hinzufügen

Verfahren

1. Gehen Sie zu **Apps > Schutz der App Office 365**.
2. Klicken Sie auf **App-Richtlinien > + Hinzufügen**.
3. Geben Sie einen **Namen** und optional eine **Beschreibung** für die Richtlinie ein.
4. Klicken Sie unter OS auswählen auf **iOS**.
5. Wählen Sie unter **Datenverlagerung** die folgenden Einstellungen und Optionen aus:
    - Datensicherung in iTunes und iCloud verhindern
    - Datentransfer aus der App an andere Apps zulassen – Alle Apps (Standard), Mit Richtlinien verwaltete Apps, Keine

- Empfang von Daten anderer Apps für die App-Zulassung – Alle Apps (Standard), Mit Richtlinien verwaltete Apps, Keine.
- „Speichern unter“ verhindern
- Ausschneiden, Kopieren und Einfügen mit anderen Apps beschränken – Jede App (Standard), Gesperrt, Mit Richtlinien verwaltete Apps, Durch Einfügen verwaltete Richtlinie
- Anzeige von Web-Content auf den verwalteten Browser beschränken
- App-Daten verschlüsseln – Wenn ein Gerät gesperrt ist (Standard), Wenn das Gerät gesperrt ist und offene Dateien vorhanden sind, Nach Geräteneustart, Geräteeinstellungen verwenden
- Synchronisation von Kontakten deaktivieren
- Drucken deaktivieren

6. Wählen Sie unter **Zugriff** die folgenden Einstellungen und Optionen aus:
   - Zugang mit PIN schützen
   - Anzahl der Anmeldeversuche, bevor die PIN zurückgesetzt wird (standardmäßig 5)
   - Einfache PIN zulassen
   - PIN-Länge (standardmäßig 4)
   - Fingerabdruck statt PIN zulassen (iOS 8+)
   - App-PIN deaktivieren, wenn Geräte-PIN verwaltet wird.
   - Unternehmens-Anmeldeinformationen für den Zugang anfordern
   - Verwaltete Apps auf Geräten mit Root oder Jailbreak sperren
   - Zugriffsanforderungen nach (Minuten) neu prüfen
     - Zeitüberlauf - Der Wert muss zwischen 1 und 65535 liegen (standardmäßig 30)
     - Offline-Nachfrist – Der Wert für die Nachfrist muss zwischen 1 und 65535 liegen (standardmäßig 720)
     - Offline-Intervall (in Tagen), bevor die App-Daten komplett gelöscht werden – dieser Wert muss zwischen 1 und 65535 liegen (standardmäßig 90).

   Mindestversion des iOS-Betriebssystems
   - Benötigte Mindestversion des iOS-Betriebssystems (Nur Warnung)
   - Mindest-App-Version
   - Benötigte Mindestversion der App (Nur Warnung)
   - Mindest-Schutzrichtlinie für die Intune-App erforderlich, SDK-Version

Klicken Sie auf **Weiter**.

8. Wählen Sie Apps aus und weisen Sie Apps zu, für die diese Richtlinie gilt.
9. Klicken Sie auf **Weiter**.
10. Wählen Sie die Benutzergruppen aus, für die diese Richtlinie gilt.
11. Klicken Sie auf **Fertig**.

Richtlinie zum Schutz der Apps in Office 365 für Android-Geräte hinzufügen

Verfahren

1. Gehen Sie zu **Apps > Schutz der App Office 365**.

2. Klicken Sie auf **App-Richtlinien > + Hinzufügen**.
3. Geben Sie einen **Namen** und optional eine **Beschreibung** für die Richtlinie ein.
4. Klicken Sie unter „OS wählen“ auf **Android**.
5. Wählen Sie unter **Datenverlagerung** die folgenden Einstellungen und Optionen aus:
    - Datensicherung in Android verhindern
    - Datentransfer aus der App an andere Apps zulassen – Alle Apps (Standard), Mit Richtlinien verwaltete Apps, Keine
    - Empfang von Daten anderer Apps für die App-Zulassung – Alle Apps (Standard), Mit Richtlinien verwaltete Apps, Keine.
    - „Speichern unter“ verhindern
    - Ausschneiden, Kopieren und Einfügen mit anderen Apps beschränken – Jede App (Standard), Gesperrt, Mit Richtlinien verwaltete Apps, Durch Einfügen verwaltete Richtlinie
    - Anzeige von Web-Content auf den verwalteten Browser beschränken
    - App-Daten verschlüsseln
    - App-Verschlüsselung deaktivieren, wenn die Geräteverschlüsselung aktiviert ist.
    - Synchronisation von Kontakten deaktivieren
    - Drucken deaktivieren
6. Wählen Sie unter **Zugriff** die folgenden Einstellungen und Optionen aus:
    - Zugang mit PIN schützen
    - Anzahl der Anmeldeversuche, bevor die PIN zurückgesetzt wird (standardmäßig 5)
    - Einfache PIN zulassen
    - PIN-Länge (standardmäßig 4)
    - Fingerabdruck statt PIN zulassen (Android 6+)
    - App-PIN deaktivieren, wenn Geräte-PIN verwaltet wird.
    - Unternehmens-Anmeldeinformationen für den Zugang anfordern
    - Verwaltete Apps auf Geräten mit Root oder Jailbreak sperren
    - Zugriffsanforderungen nach (Minuten) neu prüfen
        - Zeitüberlauf - Der Wert muss zwischen 1 und 65535 liegen (standardmäßig 30)
        - Offline-Nachfrist – Der Wert für die Nachfrist muss zwischen 1 und 65535 liegen (standardmäßig 720)
        - Offline-Intervall (in Tagen), bevor die App-Daten komplett gelöscht werden – dieser Wert muss zwischen 1 und 65535 liegen (standardmäßig 90).
    - Bildschirmfotos und Android-Assistent sperren
    - Mindestversion des Android-Betriebssystems
    - Benötigte Mindestversion des Android-Betriebssystems (Nur Warnung)
    - Mindest-App-Version
    - Benötigte Mindestversion der App (Nur Warnung)
    - Mindest-Schutzrichtlinie für die Intune-App erforderlich, SDK-Version
7. Klicken Sie auf **Weiter**.
8. Wählen Sie die Apps aus und weisen Sie die Apps zu, für die diese Richtlinie gilt.
9. Klicken Sie auf **Weiter**.

10. Wählen Sie die Benutzergruppen, auf die sich diese Richtlinie bezieht.
11. Klicken Sie auf **Fertig**.

Richtlinie zum Schutz der Apps in Office 365 ändern

Verfahren

1. Gehen Sie zu **Apps > Schutz der App Office 365**.
2. Klicken Sie auf **App-Richtlinien**.
3. Klicken Sie auf den Namen der Richtlinie, die Sie ändern wollen.
4. Klicken Sie auf der Seite mit den Richtliniendetails auf **Bearbeiten**.
5. Modifizieren Sie die Einstellungen der Richtlinienkonfiguration.
6. Klicken Sie auf **Weiter**.
7. Modifizieren Sie die Liste der Apps, auf die sich diese Richtlinie bezieht.
8. Klicken Sie auf **Weiter**.
9. Modifizieren Sie die Benutzergruppen, auf die sich diese Richtlinie bezieht.
10. Klicken Sie auf **Fertig**.

Richtlinie zum Schutz der Apps in Office 365 löschen

Verfahren

1. Gehen Sie zu **Apps > Schutz der App Office 365**.
2. Klicken Sie auf **App-Richtlinien**.
3. Klicken Sie unter der Spalte **Aktionen** auf das Symbol zum Entfernen der Richtlinie, die Sie löschen wollen.
4. Klicken Sie zur Bestätigung auf **Ja**.

Konfigurationen der App Office 365

Auf der Seite **Apps > App zum Schutz von Office 365** können Sie in der Registerkarte **App-Konfiguration** die Konfigurationen der App für Office 365 für verschiedene Benutzergruppen ergänzen, modifizieren oder löschen. In diesen App-Konfigurationen können Administratoren eine Liste von Schlüssel-Wertpaaren hinzufügen und die Konfigurationen einer oder mehreren Apps von Office 365 zuweisen. Die Registerkarte „App-Konfiguration“ enthält in einer Tabelle Details wie den aktualisierten Zeitstempel, die zugewiesenen Apps und den Bereitstellungsstatus.

Office 365 App-Konfiguration ergänzen

Verfahren

1. Gehen Sie zu **Apps > Schutz der App Office 365**.
2. Klicken Sie auf **App-Konfiguration > + Hinzufügen**.
3. Geben Sie einen **Namen** und optional eine **Beschreibung** für die Konfiguration ein.
4. Geben Sie die Schlüsselwertpaare ein.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie die Apps aus, für die diese Konfiguration gilt.

7. Klicken Sie auf **Weiter**.
8. Wählen Sie die Benutzergruppen aus, für die diese Konfiguration gilt.
9. Klicken Sie auf **Fertig**.

Office 365 App-Konfiguration modifizieren

Verfahren

1. Gehen Sie zu **Apps > Schutz der App Office 365**.
2. Klicken Sie auf **App-Konfiguration**.
3. Klicken Sie auf den Namen der Konfiguration, die Sie ändern wollen.
4. Klicken Sie auf der Seite mit den Konfigurationsdetails auf Bearbeiten.
5. Sie können auch auf die Registerkarten **App-Verteilung** bzw. **Benutzergruppenverteilung** klicken. Klicken Sie auf **Bearbeiten**, wenn Sie nur diese Einstellungen ändern wollen und anschließend auf **Speichern**.
6. Modifizieren Sie die Einstellungen der Konfiguration.
7. Klicken Sie auf **Weiter**.
8. Modifizieren Sie die Liste der Apps, auf die sich diese Konfiguration bezieht.
9. Klicken Sie auf **Weiter**.
10. Modifizieren Sie die Benutzergruppen, auf die sich diese Konfiguration bezieht.
11. Klicken Sie auf **Fertig**.

Office 365 App-Konfiguration löschen

Verfahren

1. Gehen Sie zu **Apps > Schutz der App Office 365**.
2. Klicken Sie auf **App-Konfiguration**.
3. Klicken Sie unter der Spalte **Aktionen** auf das Symbol zum Entfernen der Konfigurationsbezeichnung, die Sie löschen wollen.
4. Klicken Sie zur Bestätigung auf **Ja**.

Nicht konforme Benutzer mit Office 365-Apps

Administratoren können die Liste der Benutzer und deren Geräte auf Nicht-Compliance überprüfen. Mit dieser Seite löschen Sie Apps für Office 365 von solchen markierten Geräten.

Apps von Office 365 löschen

Verfahren

1. Gehen Sie zu **Apps > Schutz der App Office 365**.
2. Klicken Sie auf **Nicht konforme Benutzer**.
3. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Benutzer aus der Liste und klicken Sie auf **Apps von Office 365 löschen**.
   - Klicken Sie auf den Namen des Benutzers, um die Liste der Geräte anzuzeigen, deren Apps nicht mehr konform sind. Klicken Sie in der Spalte **Aktion** für ein bestimmtes Gerät auf das Symbol **Apps von Office 365 komplett löschen**.

- Klicken Sie auf den Namen des Benutzers, um die Liste der Geräte anzuzeigen, deren Apps nicht mehr konform sind. Klicken Sie auf den Namen des betreffenden Geräts, um die Apps, deren Bundle-IDs und Paketnamen sowie die markierten Gründe anzuzeigen. Klicken Sie auf **Apps von Office 365 löschen**.

4. Klicken Sie auf **Ja**, um die Aktion zu bestätigen.

Alternativ führen Sie die folgenden Schritte aus:

1. Gehen Sie zu **Benutzer**.
2. Klicken Sie auf den Namen des Benutzers, um die Seite mit den Benutzerdetails anzuzeigen.
3. Klicken Sie auf **Aktion > Apps von Office 365 löschen**.
4. Wählen Sie das Gerät aus, von dem die Apps von Office 365 gelöscht werden sollen.
5. Klicken Sie auf **OK**, um die Aktion zu bestätigen.

Löschanforderungen für Apps von Office 365 stornieren.

Verfahren

1. Gehen Sie zu **Benutzer**.
2. Klicken Sie auf den Namen des Benutzers, um die Seite mit den Benutzerdetails anzuzeigen.
3. Klicken Sie auf die Registerkarte **Schutz für Office 365** .
4. Wählen Sie in dem Dropdown-Feld **Berichtart auswählen** den Bericht **Löschanforderungen**, um die entsprechenden Informationen anzuzeigen.
5. Wählen Sie die Geräte aus, deren Löschanforderungen storniert werden sollen. Es können nur Geräte ausgewählt werden, deren Löschstatus „ausstehend“ ist.
6. Klicken Sie auf **Löschvorgang abbrechen**.
7. Klicken Sie auf **OK**, um die Aktion zu bestätigen.

App-Berichte für Benutzer mit der App zum Schutz von Office365

Administratoren können auf einen der folgenden Berichte klicken, um die Liste der Benutzer mit der App zum Schutz von Office 365 und die zugehörigen Informationen anzuzeigen:

- App-Richtlinienbericht
- App-Konfigurationsbericht
- Löschanforderungen

Informationen in den App-Berichten sind beispielsweise Bundle-ID/Paketname, Gerätename, Geräteart, Richtlinien oder Konfigurationen auf dem Gerät, Status (synchronisiert; synchronisiert, aber nicht aktuell, oder nicht synchronisiert) und die Zeit der letzten Anmeldung. Informationen aus den App-Berichten können in eine CSV-Datei exportiert und anschließend analysiert werden.

Informationen aus dem Löschanforderungsbericht enthalten beispielsweise den Anzeigenamen, den Benutzernamen, den Gerätenamen, den Gerätetyp und den Löschstatus (Wipe ausstehend oder Wipe abgeschlossen).

Führen Sie die folgenden Schritte aus, um einen der Berichte anzuzeigen:

1. Gehen Sie zu **Benutzer**.
2. Klicken Sie auf den Namen des Benutzers, um die Seite mit den Benutzerdetails anzuzeigen.
3. Klicken Sie auf die Registerkarte **Schutz für Office 365** .

4. Wählen Sie in dem Dropdown-Feld **Berichtart auswählen** einen Bericht aus, um die darin befindlichen Informationen anzuzeigen.
5. (Optional) Wählen Sie auf der Seite des Löschanforderungsberichts die Geräte aus, deren Löschanforderungen storniert werden sollen, und klicken Sie dann auf **Komplettlöschung abbrechen**. Es können nur Geräte ausgewählt werden, deren Löschstatus „ausstehend“ ist.
6. (Optional) Klicken Sie auf **In CSV exportieren**, um den Berichtinhalt als spätere Referenz oder zur Analyse als CSV-Datei herunterzuladen.

12.6. Mit Google Apps verbinden

Dieser Abschnitt enthält die folgenden Themen:

- Verwaltete Google Play-Konten (Android Enterprise-Konten)
- Android-Geräteregistrierung
- Android-Verwaltungs-API
- API für Google Apps
- Administration > Android Enterprise

12.6.1. Verwaltete Google Play-Konten (Android Enterprise-Konten)

Lizenz: Silver

Verwaltete Google Play-Konten sind erforderlich, um die Nutzung und Konfiguration von Android Enterprise-Geräten zu ermöglichen. Sie müssen zur Registrierung der Geräte nicht mehr Google Apps Directory Sync (GADS) oder Google-Konten verwenden.

Wichtig: Wenn Sie Android Enterprise bereits konfiguriert haben, müssen Sie zuerst diese Geräte außer Dienst stellen, damit Sie diese Funktion verwenden können.

Konfigurieren von Android Enterprise mit verwaltetem Google Play-Konto

Verfahren

1. Melden Sie sich beim Ivanti Neurons for MDM-Portal an.
2. Wechseln Sie zu **Admin > Google > Android Enterprise**.
3. Klicken Sie unter **Verwaltetes Google Play-Konto** auf **Google autorisieren**, um die Seite **Google Play for Work** anzuzeigen.
4. Geben Sie Ihre **Google Play-Konto-E-Mail-ID** ein.
5. Klicken Sie auf **Erste Schritte**.
6. Akzeptieren Sie die Android Enterprise-Vereinbarung.
7. Klicken Sie auf **Bestätigen**.
8. Klicken Sie auf **Registrierung abschließen.**
   Im Bereich **Android Enterprise wurde konfiguriert** werden die folgenden Informationen angezeigt:
   - **[Status]**
   - **Admin-E-Mail**
   - **Unternehmenstyp**
   - **Google Unternehmens-ID**

Wenn Android Enterprise mit verwalteten Google Play-Konten eingerichtet wird, gibt es eine Beschränkung für die Anzahl der Geräte, die pro Nutzer angemeldet werden können. Um diese Einschränkung zu umgehen, wählen Sie bei der Erstellung eines neuen Benutzers die Option **Android Enterprise-Gerätekonto**, damit mit diesem Konto verbundene, verwaltete Geräteregistrierungen mit Android Enterprise automatisch einem Google-Gerätekonto zugeordnet werden.

Gerätekonten sind für COSU-Bereitstellungen gedacht (d. h. für Einzweckgeräte im Kioskmodus). Benutzer mit Gerätekonten haben nur eingeschränkten Zugriff auf Google Play.

Gelegentlich läuft ein verwaltetes Google Play-Konto oder dessen Token aus verschiedenen Gründen ab, z. B. weil das Authentifizierungstoken abläuft oder das Konto oder Unternehmen gelöscht wird. In solchen Szenarien benachrichtigen die Google Play-Dienste den Client mit einer Broadcast-Aktion, die den Client dazu veranlasst, das Gerät neu bereitzustellen; dabei wird das vorhandene Konto entfernt und ein Konto mit einem neuen, vom UEM-Server erhaltenen Token hinzugefügt.

Falls die erneute Kontobereitstellung fehlschlägt, weil entweder das alte Konto nicht entfernt werden konnte oder weil viele Versuche unternommen wurden, es erneut bereitzustellen, wird der Benutzer aufgefordert, den Client zu löschen bzw. das Gerät auf die Werkeinstellungen zurückzusetzen, je nachdem, ob sich das Gerät im Arbeitsprofilmodus bzw. im Modus für verwaltete Geräte befindet.

Vorhandenes verwaltetes Google Play-Konto in verwaltetes Google Domain-Konto (BTE) migrieren

Diese Funktion ermöglicht die Migration von Android Enterprise-Konten und -Geräten von **Verwaltetes Google Play-Konto** zu **Verwaltetes Google Domain-Konto**.

Die Migration besteht aus folgenden Schritten:

- Konto aktualisieren
- Gerät migrieren

Voraussetzungen

- Die Geräte müssen entweder im Modus für firmenseitig verwaltete Geräte oder im Arbeitsprofilmodus registriert sein. Geräte, die im WPCOD-Modus (Work Profile on Company-Owned Device, Arbeitsprofil auf firmenseitig verwaltetem Gerät) registriert sind, müssen Android 12 oder höher ausführen.
- Den Geräten werden gültige Unternehmens- oder Geschäfts-E-Mail-IDs zugewiesen.

> Wenn das Gerät einer E-Mail-ID zugewiesen ist, die nicht dem Unternehmen zugeordnet ist, muss der Administrator eine gültige Unternehmens-E-Mail-ID neu zuweisen, damit das Gerät migriert werden kann.

Android Enterprise-Konto aktualisieren

Aktualisieren Sie das Android Enterprise-Konto von "Verwaltetes Google Play-Konto" auf "Verwaltetes Google Domain-Konto".

Verfahren

1. Wechseln Sie zu **Admin** > **Google** > **Android Enterprise**.
2. Klicken Sie auf **Konto aktualisieren**.
3. Melden Sie sich mit einer gültigen Unternehmens- oder Geschäfts-E-Mail-ID an.
4. Führen Sie den Upgrade-Prozess aus.
5. Aktualisieren Sie die Seite.

Konfiguration für Gerätemigration anwenden

Verfahren

1. Wechseln Sie zu "Konfigurationen".
2. Wählen Sie die Konfiguration **Android Enterprise: Gerätemigration von Verwaltetes Google Play-Konto zu Verwaltetes Google-Konto** und dann > **Bearbeiten** > **Weiter** > **Alle Geräte oder Benutzerdefiniert** > **Verteilung über langsamen Rollout** aus. Standardmäßig ist die Option **Manueller Rollout** ausgewählt. Wählen Sie aus der Dropdownliste **Benutzerdefinierter Anteil (%)der Geräte in der Auswahlübersicht (langsamer Rollout)** oder **Alle Geräte in der Auswahlübersicht** aus.
3. Klicken Sie auf **Fertig**.

Gerätemigration abschließen

Verfahren

1. Tippen Sie auf dem Gerät auf **Weiter**, wenn Sie aufgefordert werden, Ihr Arbeitskonto hinzuzufügen.
2. Überprüfen Sie die **Unternehmens-E-Mail-ID**.
3. Geben Sie das **Kennwort** ein.
4. Führen Sie die **Zwei-Faktor-Authentifizierung (2FA)** aus, falls verfügbar.
5. Führen Sie den Prozess der Kontoeinrichtung aus.

Migration überprüfen

Auf dem Gerät

1. Öffnen Sie **Google Play Store**.
2. Überprüfen Sie, ob sich der Kontotyp von einem Arbeitskonto in ein Unternehmensdomänenkonto geändert hat.

In der Admin-Konsole

- Um den Konfigurationsstatus **Android Enterprise: Gerätemigration von Verwaltetes Google Play-Konto zu Verwaltetes Google-Konto** anzuzeigen, navigieren Sie zu **Geräte** > **Geräte** > **Gerätedetails** > **Konfiguration** > **Android Enterprise: Gerätemigration von Verwaltetes Google Play-Konto zu Verwaltetes Google-Konto)**. Vergewissern Sie sich, dass der Konfigurationsstatus "Installiert" lautet.

Migrationsstatus überwachen

Administratoren können den Fortschritt der Migration (**migriert zu Verwaltetes Google-Konto**) wie folgt überwachen:

- **Gerätedetails** – Zeigen Sie den Migrationsstatus pro Gerät an.
- **Erweiterte Suche** – Filtern Sie nach migrierten und nicht migrierten Geräten.
- **Gerätegruppen** – Gruppieren Sie die Geräte in migrierte und nicht migrierte Geräte.

Diese Optionen helfen Ihnen dabei, Geräte zu identifizieren, für die weitere Aktionen erforderlich sind.

Neue Registrierung mit verwaltetem Google-Domänenkonto (BTE)

Android Enterprise kann unter Verwendung von **Verwaltetes Google-Domänenkonto** mit oder ohne Google-Authentifizierung konfiguriert werden.

Verfahren

1. Melden Sie sich beim Portal an.
2. Wechseln Sie zu **Admin** > **Google** > **Android Enterprise**.
3. Klicken Sie unter **Verwaltetes Google Play-Konto** auf **Autorisieren**.
4. Geben Sie Ihre **Unternehmens-** oder **Geschäfts-E-Mail-ID** ein und klicken Sie auf **Weiter**.
5. Wählen Sie **Neue Bindung erstellen mit** auf der Seite **Bindungsoption auswählen** aus.
6. Klicken Sie auf **Bestätigen**. Die Optionen **Überspringen** und **Aktivieren** werden angezeigt.

- **Überspringen** – So fahren Sie ohne Authentifizierung fort.
- **Aktivieren** – So fahren Sie mit Authentifizierung fort.

Im Bereich "Android Enterprise" werden die folgenden Informationen angezeigt:

- **Status**: Zeigt den Verbindungsstatus an.
- **Admin-E-Mail**: Zeigt die Unternehmens- oder Geschäfts-E-Mail-ID an.
- **Unternehmenstyp**: Zeigt den Unternehmenstyp an.
- **Google-Authentifizierungseinstellungen**: Zeigt, je nach Authentifizierungsanforderung, Nein/Ja an.
- **Google Unternehmens-ID**: Zeigt eine eindeutige Google Unternehmens-ID an.
- **Unternehmensname**: Zeigt den Namen des Unternehmens an.

12.6.2. Android-Geräteregistrierung

Bei einer Android-Geräteregistrierung können Sie diese Option konfigurieren, wenn Sie zum Abschluss der Registrierung Telefonberechtigungen von Benutzern benötigen, z.B. die Angabe der IMEI, die Telefonnummer und andere Telefonidentifikatoren. Nach der Konfiguration werden die Gerätebenutzer aufgefordert, dem GO-Client Zugriff auf die Geräteidentifikatoren zu erlauben.

> Diese Konfiguration gilt nur für Neuregistrierungen von Android-Geräten mit einer Android-Version ab 6.0.

1. Wählen Sie **Admin > Google > Registrierung**.
2. Wählen Sie **Android-Geräte-IDs während der Registrierung anfordern (Arbeitsprofil & Geräteadministrator)** aus.
3. Klicken Sie auf **Speichern**.

Weitere Informationen zum Verlustmodus finden Sie unter **Verwalten von Android-Geräten im Verloren-Modus**.

12.6.3. Android-Verwaltungs-API

Die Android Management API (AMAPI) ist die Cloud-Plattform-API von Google, die die Android UEM-Funktionen von Google in Ivanti Neurons for MDM integriert. Bei der Einrichtung von der Android Enterprise können Sie die Android Management API aktivieren, um Android Enterprise-Geräte zu verwalten, ohne dass auf den Geräten eine Client-Anwendung für die Geräteverwaltung installiert werden muss. Derzeit wird die Übertragung von Go app auf das Gerät zu anderen Funktionen (z. B. MTD) nicht unterstützt.

Wenn Sie beim Setup ein Konto für Android Enterprise konfiguriert haben, können Sie die Android Management API aktivieren und verwenden. Nach der Aktivierung können Sie:

- ein Registrierungsprofil hinzufügen, um den QR-Code für die Geräteregistrierung zu verwenden.
- Eine dedizierte Gerätekonfiguration (firmeneigenes Einzweckgerät oder COSU) für das registrierte Gerät für einen bestimmten Zweck erstellen.

Die Android Management API wird derzeit nur auf Geräten unterstützt, die unter Android Version 9 oder höher laufen und auf denen Google Play im dedizierten Modus installiert und bereitgestellt ist. Der Modus für unternehmenseigene dedizierte Geräte wird auch als COSU-Modus (unternehmenseigenes Einzweckgerät) bezeichnet und ist eine Abwandlung des Geräteeigentümermodus. Diese Funktion unterstützt auch die folgenden Geräteaktionen:

- Sperren
- [Reboot]
- Mit Server synchronisieren
- Wipe durchführen

Geräteanmeldungen werden in regelmäßigen Abständen (stündlich) veranlasst. Für eine sofortige Aktion nutzen Sie die Geräteaktion 'Mit Server synchronisieren' auf der Gerätedetailseite. AMAPI-Geräte senden keine obligatorischen Check-ins an Ivanti Neurons for MDM. Bestandsaktualisierungen werden durchgeführt, sobald eine Aktivität auf dem Gerät stattfindet.

Android-Verwaltungs-API aktivieren

Wechseln Sie zum Aktivieren der Android-Verwaltungs-API zu **Admin > Android Enterprise > Google autorisieren (erfordert gültige Google-Adresse) > Android Enterprise aktiviert**.

Der Status der Android Management API-Funktion (**Ja** für aktiviert und **Nein** für deaktiviert) wird außerdem auf der Seite mit den Gerätedetails angezeigt.

> GSuite-Konten werden derzeit nicht mit COSU unterstützt.

Enrollment Profile hinzufügen

Zur Registrierung eines Android-Geräts mit dem QR-Code-Scan oder der alphanumerischen Zeichenfolge des Tokens muss ein Enrollment Profile erstellt werden. Enrollment Profiles können nur erstellt werden, wenn die Android Management API aktiviert ist. Sie können auch benutzerdefinierte Geräteattribute erstellen, die mit dem Registrierungsprofil verknüpft werden.

1. Wählen Sie **Administration > Android Enterprise> Enrollment Profiles** .
2. Konfigurieren Sie die folgenden Einstellungen im Fenster **Enrollment Profile - Unternehmenseigenes dediziertes Gerät.**
3. Klicken Sie auf **Speichern**. Das Fenster **Profilübersicht** zeigt die folgenden Token-Details:

Einstellung	Beschreibung
[Name]	Geben Sie einen Namen für dieses Registrierungsprofil ein.
Beschreibung	Geben Sie eine Beschreibung ein, die den Zweck dieses Profils erläutert.
Benutzername	Geben Sie die ersten Buchstaben eines gültigen Benutzernamens ein und wählen Sie dann den Namen aus den angezeigten Übereinstimmungsergebnissen aus. Ein gültiger Benutzername könnte von einem lokalen Benutzer oder einem LDAP-Benutzer stammen. Registrierungsprofile kennzeichnen die mit dem QR-Code im Profil registrierten Geräte, damit diese als Geräte angezeigt zu werden, die dem Benutzer gehören, für den das Registrierungsprofil erstellt wurde.
Token-Gültigkeit	Geben Sie ein, wie viele Tage der QR-Code-Scan des Authentifizierungstokens gültig sein soll. Die eingegebene Zahl sollte zwischen 1 - 30 liegen. Das Gerät wird zurückgesetzt, wenn Sie das Token oder das Registrierungsprofil nach Ablauf der Gültigkeit verwenden.
Benutzerdefinierte Geräteattribute	Klicken Sie in der Spalte „Aktionen“ auf **+Neue hinzufügen**, um benutzerdefinierte Geräteattribute hinzuzufügen, die mit dem Registrierungsprofil verknüpft werden sollen. 1. Wählen Sie das benutzerdefinierte Geräteattribut aus der Dropdown-Liste in der Spalte **Attributname** aus. 2. Geben Sie in der Spalte **Wert** den Wert des benutzerdefinierten Attributs ein. 3. Klicken Sie auf **Speichern**. Das hinzugefügte benutzerdefinierte Geräteattribut wird in der Tabelle angezeigt. Klicken Sie zum Löschen auf die Option **Löschen** in der Spalte „Aktionen“. Die benutzerdefinierten Attribute können nur während der Profilerstellung zu einem Registrierungsprofil hinzugefügt werden. Die Attributfelder können nach der Profilerstellung nicht mehr bearbeitet werden.

- [Name]
- Beschreibung
- Benutzername
- Erstellungsdatum des Tokens
- Ablaufdatum des Tokens
- Token-Wert
- QR-Code
- Benutzerdefinierte Geräteattribute.

> Geräte werden zurückgesetzt, wenn die richtige Konfiguration für das Gerät nicht innerhalb des Zeitintervalls von 10 Minuten nach der Registrierung erworben wird. In solchen Fällen sollten Sie sich unter Verwendung des Registrierungs-Token/QR-Codes neu registrieren.

Wenn ein Registrierungsprofil erstellt ist, wird es auf der Seite **Registrierungsprofile** aufgelistet. Sie können folgende Aktionen in der Spalte **Aktionen** durchführen.

- Klicken Sie auf das Ansichtssymbol.um die Details des Registrierungsprofils im Fenster „Profilübersicht“ anzuzeigen. Der QR-Code wird ebenfalls in diesem Fenster angezeigt.
- Klicken Sie auf das Bearbeitungssymbol, .um die Details des Registrierungsprofils zu bearbeiten.

> Sie können nur die Gültigkeit des Tokens bearbeiten. Andere Attribute können nicht bearbeitet werden.

Klicken Sie auf das Löschsymbol, um das Registrierungsprofil zu löschen.

COSU-Konfiguration erstellen

Administratoren können mit Android Enterprise für einen bestimmten Zweck dedizierte Geräte konfigurieren, indem sie die dedizierten Geräte (unternehmenseigene Einzel- oder COSU-Konfiguration) verwenden. Die COSU-Konfiguration wird an die vom Unternehmen verwalteten Geräte verteilt (Geräteeigentümermodus) und stellt den Benutzern im Kioskmodus nur eine Anwendung zur Verfügung. Geräte im Arbeitsprofil für unternehmenseigene Geräte werden nicht unterstützt.

Mit dieser Konfiguration kann der Administrator die Geräte so konfigurieren, dass die App auf dem Bildschirm angeheftet wird, so dass der Benutzer im Kioskmodus diese App nicht vom Bildschirm entfernen und von der App zu anderen Bildschirmen des Geräts navigieren oder andere Apps auf dem Gerät verwenden kann.

> Andere Anwendungen können auch zwangsweise auf dem AMA-Gerät installiert werden, wenn Sie unter "Erweiterte Optionen & Anwendungskonfiguration" die Option "Auf Gerät installieren" auswählen. Sie können jedoch nicht mit ihnen interagieren, solange die Kiosk-Anwendung über die Konfiguration an den Bildschirm angeheftet ist. Für den Multi-App-Kiosk wird empfohlen, die Kiosk-Funktionalität des vom Unternehmen verwalteten Geräts (Geräteeigentümermodus) zu verwenden. Diese Vorgehensweise ermöglicht größere Kontrolle über die Apps und Geräteeinstellungen und kann auch zum Mehrbenutzermodus erweitert werden.

Admins können Konfigurationsänderungen vornehmen, z. B. die Systemnavigation und die Verwendung anderer, für den Endbenutzer per Push über Google DPC auf das Gerät übertragenen Apps erlauben, indem sie die verschiedenen Optionen je nach Bedarf prüfen.

COSU-Konfigurationen werden durch die ihnen zugeordnete Priorität bestimmt. Die Konfiguration mit der höchsten Priorität überträgt die Richtlinienkonfiguration per Push an Google. COSU-Konfigurationen werden für die Geräte innerhalb des definierten Space übernommen. Dieser kann an andere Spaces delegiert werden, wenn er im Standard-Space definiert ist.

Gehen Sie zur Konfiguration wie folgt vor:

1. Gehen Sie zu **Konfiguration > +Hinzufügen** .
2. In der Konfiguration **Sperre & Kiosk: Android Enterprise** klicken Sie auf **Dedizierte Geräte (unternehmenseigene Einzweckgeräte oder COSU)**.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Geben Sie eine Beschreibung ein.
5. Sie können folgende Einstellungen konfigurieren, indem Sie auf die entsprechenden Registerkarten klicken:

- **App-Einstellungen**
- **Allgemeine Sperren**
- **Kiosk-Anpassung**
- **System-Einstellungen**

Die folgende Tabelle enthält die Details der konfigurierbaren Felder:

Einstellung	Beschreibung
App-Einstellung	
App-Name **Allgemeine Sperren**	Wählen Sie die App aus, die auf dem Gerät platziert werden soll, indem Sie den Namen der App bzw. den Anfangsbuchstaben des Namens der App eingeben, damit die gewünschte App in der Dropdown-Liste erscheint. Wenn Sie die gewünschte App in der Dropdown-Liste nicht sehen, prüfen Sie, ob es sich bei der App, die Sie bereitstellen möchten, um eine öffentliche/private App handelt, die im Play Store verfügbar ist und dem App-Katalog hinzugefügt wurde. Dieses Feld muss ausgefüllt werden. Wenn Sie in diesem Feld keine App auswählen, die Sie hinzufügen wollen, können Sie die Konfiguration nicht erstellen. Sie können nur öffentliche und private Apps hinzufügen. Interne Apps und Web-Apps (private Apps) können nicht hinzugefügt werden .
Anzeige eingeschaltet lassen	Konfigurieren Sie die Batteriemodi, in denen das Gerät eingeschaltet bleibt. Wählen Sie eine der folgenden Optionen aus: • **AC** - Stromquelle ist ein Netzteil • **Drahtlos** • **USB** - Stromquelle ist ein USB-Anschluss • **Beliebig** - Die Stromquelle ist entweder ein Netzladegerät, ein USB-Anschluss oder ein drahtloses Ladegerät.
Kiosk-Anpassung **Statusleiste anpassen**	Wählen Sie eine der folgenden Optionen zum Anpassen der Statusleiste auf den Zielgeräten: • **Benachrichtigung und Systeminfo aktiviert** - Zeigt Systeminfo und Benachrichtigungen in der Statusleiste an. • **Nur Systeminfo aktiviert**- Um nur Systeminfo in der Statusleiste anzuzeigen.
Systemnavigation anpassen	Wählen Sie eine der folgenden Optionen, um den Zugriff auf die Navigationsfunktionen (Schaltflächen Home und Übersicht) im Kiosk-Modus festzulegen. • **Aktiviert** - Ermöglicht die Navigation über die Schaltflächen „Home“ und „Übersicht“. Benutzer können aus der angegebenen App heraus navigieren, wenn diese Option ausgewählt ist. • **Deaktiviert** - Deaktiviert die Navigation über die Schaltflächen Startseite und Übersicht. • **Nur Home-Button** - Aktiviert nur die Navigation über den Home-Button. Die Schaltfläche „Zurück“ ist bei all diesen Optionen verfügbar.
Globale Aktionen aktivieren	Wählen Sie diese Option, um globale Aktionen im Kiosk-Modus zu aktivieren. Die Neustart- und Abschaltfunktion in Verbindung mit den Netztasten wird über diese Option gesteuert.

Einstellung	Beschreibung
Systemfehler-Dialoge aktivieren	Aktivieren Sie dieses Kontrollkästchen, um Fehlerdialoge für abgestürzte oder nicht reagierende Apps im Kiosk-Modus zu aktivieren.
System-Einstellungen **Einstellungen für Systemaktualisierungen**	Konfigurieren Sie die folgenden Einstellungen zur Verwaltung von System-Updates: • **System Update** - Wählen Sie die Art des erforderlichen System-Updates aus. ◦ **Automatisch** - Automatisch installieren, sobald ein Update verfügbar ist. ◦ **Verschieben** - Verschiebt die automatische Installation bis zu einem Maximum von 30 Tagen. ◦ **Im Fenster** - Automatische Installation innerhalb eines täglichen Wartungsfensters. Legen Sie die Anfangs- und Endstunde für das Wartungsfenster fest. Die auf Geräten installierten Updates können je nach unterstütztem Funktionsumfang, Android-Version und der auf dem Gerät installierten Google DPC-Version abweichen. • **Sperrfrist** - Wenn ein Gerät in der Sperrfrist eingestellt wird, werden alle eingehenden Systemaktualisierungen blockiert und nicht installiert. Klicken Sie auf **Sperrfrist hinzufügen**, um das **Startdatum** und das **Enddatum** der Sperrfrist festzulegen. Außerhalb der Sperrzeit gilt für ein Gerät das normale Aktualisierungsverhalten. Liegt das Enddatum vor dem Startdatum, erstreckt sich die Sperrzeit zwischen dem aktuellen und dem darauf folgenden Jahr. Die Sperrfrist kann maximal auf 90 Tage festgelegt werden. Zwei aufeinander folgende Sperrfristen müssen mindestens 60 Tage auseinander liegen.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Verteilungsoptionen aus:

- **Alle Geräte**
- **Keine Geräte** (Standard)
- **Anpassbar**

8. Klicken Sie auf **Fertig**.

Anwendungen auf AMAPI-Geräten verwalten

Wenn die COSU-Konfiguration an Geräte verteilt wird, werden die Apps per Push auf den Bildschirm des AMA-Gerätes übertragen und dort angeheftet. Unabhängig von der COSU-Konfiguration, die auf das Gerät geschoben wird, können Apps, die auf dem AMA-Gerät installiert sind, weiterhin verwaltet werden. Im Folgenden finden Sie Einzelheiten zur App-Verwaltung auf folgenden Geräten:

- Es werden nur öffentliche, private Apps unterstützt; hausinterne Apps und Web-Clips werden nicht unterstützt.
- Apps werden nur per Push übertragen, wenn in den Installationseinstellungen die Option „Auf Gerät installieren“ oder „Installation im Hintergrund“ aktiviert ist. Anwendungen, die dem Benutzer/Gerät zugewiesen werden, ohne dass eine dieser Optionen aktiviert ist, werden weder auf dem Gerät noch im Play Store des Geräts für Benutzeraktionen angezeigt.

- Als Anwendungskonfigurationen unterstützt werden die Einstellungen für Managed Google Play und Work Managed Device (Android Enterprise). Verwaltete Konfigurationen für Apps werden unterstützt, einschließlich der verwalteten Konfiguration für OEMConfig-Apps.

Die Dauer des Installations- und Deinstallationsvorgangs für Konfigurationen kann variieren. Die Benachrichtigung durch Google (Messaging-Dienst) informiert darüber, ob die gewünschte Aktion durchgeführt wird.

- Go app wird nun im Rahmen der AMA-Geräteregistrierung standardmäßig installiert. Während der Registrierung wird die App an den Bildschirm angeheftet. Sobald die Einrichtung abgeschlossen ist, wird sie im Hintergrund ausgeführt.

Mit Richtlinien unterstützt wird nur die Durchsetzung der Geräte-Registrierungsanforderungen unter Berücksichtigung von Hersteller, Betriebssystemversion und Sicherheitspatch-Level. Es wird eine Geräte-Whitelist unterstützt, die es nur Geräten auf der Whitelist ermöglicht, sich bei Ivanti Neurons for MDM zu registrieren.

Verwalten der Unterstützung für App-Feedback auf AMAPI-Geräten

Die Unterstützung für App-Feedback kann auf AMAPI (COSU)-Geräten verwaltet werden. Wenn ein Gerät im AMAPI (COSU)-Modus registriert wird, überträgt Google die verwaltete App-Konfiguration direkt via Push an Ivanti Neurons for MDM und das ohne Intervention durch Go app. Die Informationen zum Feedback über die verwaltete App können auf Geräteebene unter **Gerätedetails > Installierte Apps > Feedback anzeigen** angezeigt werden. Auf App-Ebene lassen sie sich aufrufen, indem Sie auf der Registerkarte "App-Konfig. Feedback" zur jeweiligen Android-App im App-Katalog navigieren und dort den Gesamtbericht für alle Geräte prüfen. Informationen zu den Mechanismen des App-Feedbacks finden Sie unter **App-Feedback synchronisieren und abrufen**.

AMAPI-Einschränkungen

Derzeit gilt für AMAPI folgende Einschränkung:

- Es werden nur dedizierte Geräte (COSU-Modus) unterstützt.

Unterstützte Konfigurationen

Die folgenden Konfigurationen werden für AMAPI unterstützt:

- App-Verteilung (einzelne App oder mehrere Apps)
- Konfiguration von verwalteten Apps, die auf das Gerät übertragen werden
- WLAN-Konfiguration
- Für Sperre dedizierte Android Enterprise-COSU-Konfiguration
- Always-on-VPN-Konfiguration

12.6.4. API für Google Apps

Google-Kunden, die den Benutzerzugriff auf Google Apps mit SSO authentifizieren, können aufgrund der Einschränkungen des Protokolls Benutzer nicht über Exchange ActiveSync mit E-Mails, Kontakten und Kalender verbinden, weil das Protokoll SSO-gesteuerte Weiterleitungen auf externe Authentifizierungsdienste nicht unterstützt. Dieser Dienst berücksichtigt diese Situation durch Einrichtung und Verwaltung von Kontenpasswörtern für die ActiveSync-Verbindung.

Voraussetzungen

Zur Konfiguration der API-Funktion für Google Apps benötigen Sie:

- Administratorzugriff auf ein Konto unter https:// console.developers.google.com/.
- Administratorzugriff auf ein Konto unter https://admin.google.com.

Aktivierung der API-Funktion für Google Apps

Verfahren

1. Wählen Sie **Administration > Google > Google Apps API**.
2. Klicken Sie am unteren Rand des linken Rechtecks mit Ziffer 1 auf **Schritt 1: Google Dev** .
3. Die Seite Schritt 1: Google Dev wird angezeigt.
   Folgen Sie den Anweisungen auf der Seite Schritt 1: Google Dev und klicken Sie auf **Fertig**.
4. Klicken Sie am unteren Rand des mittleren Rechtecks mit Ziffer 2 auf **Schritt 2: Google Admin** .
5. Die Seite Schritt 2: Google Admin wird angezeigt.
   Folgen Sie den Anweisungen auf der Seite Schritt 2: Google Admin und klicken Sie auf **Fertig**.
6. Geben Sie in dem Rechteck mit Ziffer 3 den Google-Admin-Benutzernamen in dem Feld **Google Admin Benutzername eingeben** ein.
7. Klicken Sie in dem gleichen Rechteck auf **Datei auswählen**, um die JSON-Datei hochzuladen, die Sie in Schritt 1 heruntergeladen haben.
8. Klicken Sie auf **Speichern**.
9. Wenn Sie die Google Apps API Seite nicht sehen können, kann es sein, dass Sie nicht über die erforderlichen Berechtigungen verfügen. Sie brauchen eine der folgenden **Rollen**:
   - Systemverwaltung
   - System schreibgeschützt

12.6.5. Administration > Android Enterprise

Lizenz: Silver

- Android Enterprise-fähige Ivanti, Inc-Produktivitäts-Apps wie Email+, Docs@Work und Web@Work erfordern die Gold-Lizenz.
- Tunnel für Android Enterprise erfordert eine Platin-Lizenz.

Mit Android Enterprise können Android Enterprise-Apps verwendet und konfiguriert werden. Benutzer von Android Enterprise können Apps aus dem App-Katalog sowie dem Google Play Store anzeigen und installieren.

Wenn Sie ein neuer Kunde sind, erfolgt die App-Verteilung standardmäßig nach Gerät. Sie können diese Einstellung nicht ändern. Kunden, die ein Upgrade durchgeführt haben, können zwischen der App-Verteilung nach Benutzer bzw. nach Gerät wählen. Bei Kunden, die ein Upgrade durchgeführt haben, ist standardmäßig die App-Verteilung nach Benutzer ausgewählt. Viele Benutzer verfügen über mehrere Geräte. Wenn ein Benutzer über mehrere Geräte verfügt und die App-Verteilung nach Gerät festgelegt ist, können Sie auf jedem Gerät verschiedene Apps bereitstellen.

Dieser Abschnitt enthält die folgenden Themen:

- Android Enterprise konfigurieren
- Arbeitsprofil für Android Enterprise konfigurieren

Android Enterprise konfigurieren

1. Klicken Sie im Cloud-Portal auf **Admin > Google > Android Enterprise**.
2. Wählen Sie eine der folgenden Optionen aus:
    - **Verwaltetes Google Play-Konto:** Unternehmen, die G Suite nicht nutzen, können mit dieser Methode Benutzer für Android Enterprise registrieren lassen, ohne dass sie personenbezogene Informationen (E-Mail-Adressen an Google) versenden müssen. Die Cloud stellt die Benutzer automatisch mit Hilfe von Google bereit und verwaltet diese. Sie werden aufgefordert, Android Enterprise für ein Google-Administratorkonto zu autorisieren.
    - **Verwaltetes Google Konto:** Unternehmen, die G Suite nutzen, können mit dieser Methode die Benutzer für Android Enterprise mithilfe ihrer Google-Konten registrieren. Jeder Benutzer muss über ein Google-Konto verfügen, um sich bei Android Enterprise zu registrieren.

Folgen Sie den Anweisungen auf dem Bildschirm, um den Konfigurationsprozess abzuschließen:

4. Bei dem automatischen Verfahren gehören dazu folgende Schritte:
    - UEM-API aktivieren und Unternehmens-Anmeldeinformationen erstellen
    - Registrierung bei Google durch Autorisierung des Integrationsverantwortlichen. Dies sollte ein IT-Konto und kein privates Konto sein.
    - Erstellung Ihrer Anmeldedaten per Drag and Drop, indem Sie die JSON-Kunden-ID Ihres Dienstkontos in das betreffende Feld ziehen.

Bei dem alternativen Verfahren sind folgende Schritte erforderlich:

- Beziehen Sie sich auf die CLIENT-ID im folgenden Abschnitt und fügen Sie sie dem Google Admin hinzu.
- Suchen Sie Ihr MDM-Token im Google Admin- und Service-Konto in der Google Cloud-Konsole.
- Geben Sie in Cloud MDM-Token, Enterprise Google-Domäne und Enterprise-Admin-E-Mail-Adresse für das Google-Konto ein, um die Verbindung zum Google-Dienst herzustellen.

- Ziehen Sie die JSON-Client-ID Ihres Dienstkontos in das betreffende Feld von Cloud.
- Autorisieren Sie Ivanti Neurons for MDM zum Anzeigen und/oder Verwalten Ihrer Google-Benutzer, indem Sie in Ivanti Neurons for MDM auf **Autorisieren** klicken.

Die Benutzeroberfläche der Cloud führt Sie durch diese Schritte.

CLIENT-ID zum Binden von Ivanti Neurons for MDM an ein verwaltetes Google-Konto

Fügen Sie die Client-ID **140561810807-tiiglke17laibbrt5darupmvo4ae7cbj.apps.googleusercontent.com** in der Administratorkonsole hinzu, um den Cloud-Mandanten mit dem verwalteten Google-Konto zu verbinden.

Arbeitsprofil für Android Enterprise konfigurieren

1. Wechseln Sie im Ivanti Neurons for MDM-Portal zu **Konfigurationen**.
2. Klicken Sie auf **+Hinzufügen**.
3. Klicken Sie auf die Konfiguration **Sperre und Kiosk: Android Enterprise**.
4. Geben Sie einen Konfigurationsnamen und die Beschreibung ein.
5. Klicken Sie auf die **Sperrart für das Arbeitsprofil**.
   Klicken Sie auf die **Sperreinstellungen**, die Sie für die betreffenden Geräte übernehmen wollen.
   Wichtig: Wenn der Benutzer ein Google-Konto mit der Option „Konto hinzufügen“ unter „Einstellungen“ ergänzt, prüft der Google-Authentifizierungsserver, ob die Domain des Kontos als UEM-verwaltete Domain registriert ist. Überprüfen Sie, ob die Option **UEM-Richtlinien auf Android-Geräten erzwingen** aktiviert ist. In diesem Fall wird der GO-Client automatisch installiert oder aktualisiert (sofern er noch nicht auf dem Gerät installiert war) und gestartet. Sobald der Benutzer den Registrierungsprozess aufruft, wird er aufgefordert, ein Arbeitsprofil zu erstellen, und das Google-Konto wird automatisch auf das Arbeitsprofil übertragen.

12.7. Arbeiten mit ChromeOS-Geräten

Dieser Abschnitt enthält die folgenden Themen:

- ChromeOS und Ivanti Neurons for MDM
- Verteilen von Android-Apps an ChromeOS-Geräte
- ChromeOS Blueprint-Konfiguration
- Geräteaktionen
- Häufig gestellte Fragen
- Empfohlene Schritte für die Evaluierung

12.7.1. ChromeOS und Ivanti Neurons for MDM

ChromeOS ist ein Linux-basiertes Betriebssystem, das von Google entwickelt wurde und von Google verteilt wird.
Ivanti Neurons for MDM unterstützt Geräte, auf denen Android, Windows, iOS und macOS ausgeführt wird. Diese Unterstützung wurde nun auf ChromeOS-Geräte erweitert. Ivanti Neurons for MDM bietet eine einheitliche und einfache Lösung für die Mobilitätsverwaltung, mit der Sie Ihre ChromeOS-Geräte konfigurieren und verwalten können. Ivanti bietet eine einheitliche, einfache und funktionsreiche Lösung für ChromeOS-Geräte, die den Adminworkflows ähnelt, die für iOS, Android, Windows und Mac auf Ivanti Neurons for MDM verfügbar sind. Der Administrator kann Ivanti Neurons for MDM einfach mit seiner Google Cloud (auch als Google Admin-Konsole bezeichnet) verbinden, indem er eine simple Integration unter **Admin > Google > ChromeOS-Verwaltung** verwendet.

Voraussetzungen

1. Es ist ein verwaltetes Google Admin-Konto vorhanden.
2. Die LDAP-Benutzer und Org.Einheiten müssen in die Google Admin-Konsole importiert werden. Ivanti Neurons for MDM unterstützt nur Org.Einheiten, die aus einer LDAP-Quelle importiert wurden. Lokale Org.Einheiten werden nicht unterstützt.
3. Der Administrator hat die Organisationseinheiten (Benutzergruppen) mit Ivanti Neurons for MDM synchronisiert. Dazu kann er den LDAP-Server konfigurieren und dann die Organisationseinheiten hinzufügen.

Autorisieren von Google

Die in der Google Admin-Konsole verfügbaren ChromeOS-Geräte können nicht direkt bei Ivanti Neurons for MDM registriert werden. Stattdessen werden die Geräte bei Google registriert und die Informationen zu den Geräten werden zwischen Google und Ivanti Neurons for MDM synchronisiert. Der Administrator muss Google autorisieren, die Geräte zu importieren und andere Aktionen durchzuführen, wie Apps und Konfigurationen zuweisen und dergleichen.

Verfahren

1. Wechseln Sie zu **Admin → Google > ChromeOS-Verwaltung**.
2. Klicken Sie auf **Google autorisieren**.
3. Wählen Sie das zu autorisierende Google Admin-Konto aus.
4. Klicken Sie auf **Fortfahren**, um die Berechtigungen zum Bereitstellen der erforderlichen Dienste zu akzeptieren.
   Die Bestätigung **ChromeOS erfolgreich eingerichtet** wird angezeigt. Unter der Bestätigung befinden sich die Informationen zur Domäne.

Synchronisieren von ChromeOS-Geräten über Google

Der Administrator muss die ChromeOS-Geräte über die Google Admin-Konsole synchronisieren. Bei der ersten Verwendung der Google Admin-Konsole, um auf die ChromeOS-Geräte zuzugreifen, muss der Administrator die Geräte manuell synchronisieren, indem er die Option "Jetzt synchronisieren" der Seite "ChromeOS-Verwaltung" verwendet.

> Nachdem die Geräte beim ersten Mal manuell synchronisiert wurden, werden die nachfolgenden Synchronisierungen automatisch jede Stunde durchgeführt.

Löschen der Google Admin Console-Integration in Ivanti Neurons for MDM

Durch Löschen der Integration wird das OAuth-Token widerrufen, das wir von Google für den Zugriff auf Google-Ressourcen erhalten haben. Bei dem Vorgang werden die ChromeOS-Dienste, das mit der Blueprint- und App-Konfiguration verknüpfte Inventar und die Registrierungsmetadaten gelöscht. Die Blueprint-Konfiguration und hochgeladene Apps werden nicht gelöscht.

Falls die Mandantenregistrierung nicht gelöscht wird, können Sie ein Ticket erstellen, um das Problem prüfen zu lassen.

Verfahren

1. Wechseln Sie zu **Admin → Google > ChromeOS-Verwaltung**.
2. Klicken Sie im Abschnitt "ChromeOS Ivanti Neurons for MDM-Registrierung" auf **Löschen**.
   Es wird ein Popupfenster angezeigt, in dem Sie gefragt werden, ob Sie den Löschvorgang fortsetzen möchten. Wenn Sie bestätigen, werden alle mit der Integration verknüpften Geräte gelöscht. Wählen Sie **OK**.

12.7.2. Verteilen von Android-Apps an ChromeOS-Geräte

Der Administrator kann Android-Apps über den App-Katalog an ChromeOS-Geräte verteilen.

Voraussetzungen

1. Android Enterprise wurde konfiguriert. Weitere Informationen zum Einrichten von Android Enterprise finden Sie unter **Einrichten von Android Enterprise**.
2. Es sind Android-Apps im App-Katalog enthalten.
3. Der Benutzer des ChromeOS-Geräts (Chromebook) gehört einer Benutzergruppe (auch als Organisationseinheit bezeichnet) an, bevor Android-Apps und die ChromeOS Blueprint-Konfiguration verteilt werden.

Nachdem Sie die Android-App identifiziert haben, müssen Sie diese über einen Prozess verteilen, wie er auch für andere Apps üblich ist. Achten Sie beim Verteilen der Android-App darauf, dass Sie die gewünschten Benutzergruppen auswählen und dass die Installation auf dem Zielgerät im Hintergrund durchgeführt wird.

> Falls Ihre derzeitige Android-App-Bereitstellung für die Verteilung an Geräte/Gerätegruppen oder Benutzer konfiguriert ist, müssen Sie die Verteilung so ändern, dass sie auf Benutzergruppen basiert. Dies kann sich auf vorhandene Bereitstellungen auswirken, falls die App bereits verwendet wird. Es wird empfohlen, dies zuerst an einer komplett neuen App zu testen.

> Über die Installationseinstellungen können Administratoren die abschließende unbeaufsichtigte Installation steuern. Diese ist erforderlich, damit die App via Push auf die ChromeOS-Geräte übertragen werden kann. Die Benutzergruppen müssen hier ausgewählt werden.

12.7.3. Hinzufügen und Verteilen von Apps mit ChromeOS-Erweiterung

Der Administrator kann Apps mit ChromeOS-Erweiterung zum App-Katalog hinzufügen und die Apps an ChromeOS-Geräte verteilen.

Verfahren

1. Wechseln Sie zu **Apps** > **App-Katalog**.
2. Klicken Sie auf **+ Hinzufügen**.
3. Wählen Sie **ChromeOS** aus der Liste aus. Die Seite **ChromeOS-App hinzufügen – Details** wird angezeigt.
4. Geben Sie folgende Details an: **App-Name** – Der Name der App mit ChromeOS-Erweiterung, **Erweiterungs-ID** – Diese Information finden Sie im Chrome Web Store.
5. Klicken Sie auf **Weiter**. Die Seite **App-Konfigurationen** wird angezeigt. Sie können auswählen, ob die Aktualisierung sofort bei der nächsten Anmeldung des Geräts erfolgen soll oder ob die App automatisch aktualisiert werden soll, sobald neue Versionen verfügbar sind.
6. Wählen Sie eine der Optionen für die App-Verteilung aus und machen Sie die erforderlichen Angaben.

> Die ChromeOS-App-Verteilung wird nur für LDAP-Benutzergruppen unterstützt.

Nachdem Sie die App mit ChromeOS-Erweiterung identifiziert haben, müssen Sie diese über einen Prozess verteilen, wie er auch für andere Apps üblich ist. Achten Sie beim Verteilen der ChromeOS-App darauf, dass Sie die gewünschten Benutzergruppen auswählen und dass die Installation auf dem Zielgerät im Hintergrund durchgeführt wird.

> Über die Installationseinstellungen können Administratoren die abschließende unbeaufsichtigte Installation steuern. Diese ist erforderlich, damit die App via Push auf die ChromeOS-Geräte übertragen werden kann. Die Benutzergruppen müssen hier ausgewählt werden.

Sie können die Informationen zu einer App mit ChromeOS-Erweiterung bearbeiten oder eine App mit ChromeOS-Erweiterung aus dem App-Katalog löschen. Folgen Sie dabei dem Prozess, den Sie üblicherweise verwenden, um eine App zu bearbeiten oder aus dem App-Katalog zu löschen.

App mit ChromeOS-Erweiterung bearbeiten

1. Wechseln Sie zu **Apps > App-Katalog > Details**.
2. Klicken Sie auf **Bearbeiten**. Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **Speichern**.

Informationen zum Entfernen einer App finden Sie unter **Entfernen von Apps aus dem App-Katalog**.

12.7.4. ChromeOS Blueprint-Konfiguration

Für die ChromeOS Blueprint-Konfiguration sind folgende Einstellungen verfügbar:

- Geräteeinstellungen
- Benutzer- und Browsereinstellungen
- Einstellungen für verwaltete Gastsitzung

Sie können die ChromeOS-Konfiguration auf bestimmte Benutzergruppen anwenden (diese werden auch als Organisationseinheiten bezeichnet). Wenn Sie versuchen, die ChromeOS Blueprint-Konfiguration zu verteilen, ist nur der Abschnitt "Benutzergruppen" verfügbar. Alle LDAP-Benutzergruppen, die ebenfalls mit der autorisierten Google Admin-Konsole verknüpft sind, werden unter dem Abschnitt aufgeführt. Sie können eine oder mehrere der aufgeführten Gruppen auswählen und die Konfiguration darauf anwenden.

Verfahren

1. Wechseln Sie zu **Konfigurationen > Hinzufügen**.
2. Wählen Sie im Abschnitt mit den Betriebssystemen **Google ChromeOS** aus. Die Registerkarte **ChromeOS Blueprint-Konfiguration** wird angezeigt.
3. Klicken Sie auf **ChromeOS Blueprint**. Die Seite **ChromeOS Blueprint-Konfiguration erstellen** wird angezeigt.
4. Geben Sie einen Namen für die Konfiguration im Kästchen **Name** ein.
5. Beim Konfigurations-Setup können Sie die Geräteeinstellungen, die Benutzer- und Browsereinstellungen und die Einstellungen für verwaltete Gastsitzungen nach Bedarf bearbeiten. Aktivieren Sie anschließend den Umschalter "Via Push auf Gerät übertragen", um die modifizierten Einstellungen anzuwenden.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie **Benutzerdefiniert** aus, um die Verteilungsoptionen anzuzeigen.

> Nur die LDAP-Benutzergruppen stehen für die Verteilung der Konfiguration zur Verfügung.

> Wenn Sie die Konfiguration an alle verteilen möchten, funktioniert dies nur für die LDAP-Benutzergruppen, die in Ivanti Neurons for MDM und in der Google Admin-Konsole verfügbar sind.

Wählen Sie eine oder mehrere Gruppen aus und klicken Sie auf **Fertig**.

> Wird die Verteilung von Einstellungen rückgängig gemacht, werden die bereits angewendeten Einstellungen nicht aufgehoben.

> Sie können Dateien zur ChromeOS Blueprint-Konfiguration hochladen.

12.7.5. Geräteaktionen

Folgende Aktionen werden auf ChromeOS-Geräten unterstützt:

- **Komplett löschen** – Eine Komplettlöschung löscht alle Daten vom Gerät und setzt das Gerät auf die Werkseinstellungen zurück. Weitere Informationen finden Sie unter **Gerät „wipen“**.
- **Sperren** – Die Sperraktion verhindert, dass weitere Aktionen auf dem Gerät durchgeführt werden können. Weitere Informationen finden Sie unter **Gerät sperren**.
- **Entsperren** – Die Entsperraktion gibt das Gerät wieder für die Verwendung frei. Weitere Informationen finden Sie unter **Gerät entsperren**.

12.7.6. Häufig gestellte Fragen

In diesem Abschnitt finden Sie Antworten auf häufig gestellte Fragen zur Verwendung von ChromeOS-Geräten auf Ivanti Neurons for MDM.

- Wie unterscheidet sich ChromeOS von anderen Betriebssystemen?
- Bislang lässt Google nur die Konfigurationsverteilung auf Basis von LDAP-Benutzerguppen zu. Der Administrator sollte sich deshalb beim Arbeiten mit Konfigurationen oder Apps vergewissern, dass die Verteilung auf LDAP-Benutzergruppen basiert. Lokale Benutzergruppen oder Gerätegruppen werden für die ChromeOS-Geräteverwaltung nicht unterstützt.
  Welche Lizenzierung benötige ich von Ivanti zum Verwalten von ChromeOS-Geräten?
- Die ChromeOS-Geräte sollten über Lizenzen wie Chrome Enterprise Upgrade oder Chrome Education Upgrade verfügen. Diese können über den Handel im Rahmen von Hardware oder als eigenständige Lizenzen bezogen werden. Weitere Informationen finden Sie in der Dokumentation von Google. Für den Einstieg in die Chrome-Geräteverwaltung benötigen Sie von Ivanti eine Lizenz für Secure UEM (Unified Endpoint Management).
  Ist Mobile Threat Defense (MTD) oder eine vergleichbare Lösung für Bedrohungsschutz verfügbar? Benötige ich eine separate Lizenz für MTD?
- Dies ist derzeit nicht im Produkt verfügbar. Bitte lesen Sie den Abschnitt über derzeitige Einschränkungen. Weitere Informationen zu funktionalen Änderungen werden wir in späteren häufig gestellten Fragen und in Release-Ankündigungen bereitstellen.
  Warum enthalten die Registerkarten "Konfigurationen" und "Apps" keine Details wie bei anderen Geräten?
- Da Konfigurationen an Benutzergruppen verteilt und nicht basierend auf dem angemeldeten Benutzer angewendet werden, sind die Konfigurationen derzeit nicht bei den Gerätedetails sichtbar. Apps folgen derselben Verteilungslogik und unterliegen daher ebenfalls dieser Einschränkung. Weitere Informationen zu Änderungen an diesen Einschränkungen werden wir in späteren häufig gestellten Fragen und in Release-Ankündigungen bereitstellen.
  Wie viele Konfigurationen werden derzeit für ChromeOS unterstützt?
- Bei ChromeOS haben wir die Anzahl der verfügbaren Konfigurationskacheln und die Anzahl der mit der Konfiguration verbundenen Admin-Aufgaben reduziert. Wir bezeichnen diese Konfiguration als "ChromeOS Blueprint-Konfiguration". ChromeOS Blueprint unterstützt fast 700 Konfigurationen auf diesen Geräten. Informationen zu den Konfigurationsoptionen finden Sie in der Dokumentation von Google.
  Ist es einfach, eine Konfiguration für alle Geräte zu verwalten?
- Administratoren können einfach eine vorhandene Konfiguration klonen und sie bei Bedarf für ihre jeweiligen Benutzergruppen anpassen. Sie müssen nicht eine komplett neue Konfiguration erstellen.
  Wie lässt sich eine VPN-Konfiguration zu Chrome-Geräten hinzufügen?
- Dies lässt sich über die Android-Apps bewerkstelligen. Es wird kein natives VPN verwendet.
  Sind für solche Geräte Aktionen wie Stilllegung und Komplettlöschung verfügbar?
- Chromebooks in Enterprise werden immer von einem Unternehmen verwaltet und die Daten auf einem solchen Gerät gelten als reine Unternehmensdaten. Daher gilt:
  - Die Stilllegung wird blockiert.
  - Die Komplettlöschung ist erlaubt.
  - Die Sperrung ist erlaubt.
  - Die Entsperrung ist erlaubt.
  - Andere Aktionen werden nicht unterstützt.

Welche Chromebook-Hardware wird von Ivanti unterstützt?

- Geräte, die von Google Cloud-Geräteverwaltungslösungen unterstützt werden, sollten normalerweise auch von Ivanti unterstützt werden. Ivanti veröffentlicht derzeit keine Liste mit Hardware, die von der Ivanti Lösung unterstützt wird.
  Welche Version von ChromeOS wird unterstützt?
- Google Cloud unterstützt lediglich die neueste stabile Version von ChromeOS. Aufgrund der Beschaffenheit von Back-End-Integrationen folgt Ivanti dem von Google unterstützten Modell.
  Welche Einschränkungen gibt es für diese brandneue Funktionalität?

Die neue Unterstützung für ChromeOS ist ein wichtiger Schritt hin zur Bereitstellung von Funktionen, auf die unsere Kunden schon lange warten. Folgende Einschränkungen sollten von Administratoren berücksichtigt werden:

- ChromeOS-Erweiterungen (Browser-Apps) werden derzeit nicht als Apps für die Verteilung unterstützt.
- Die verwaltete App-Konfiguration wird für Android-Apps derzeit nicht unterstützt.
- Die WLAN-Konfigurations-API wurde vor Kurzem veröffentlicht und wird derzeit nicht unterstützt.
- Die Zertifikatverteilung wird derzeit nicht unterstützt.
- Die Verteilung der Android-App Ivanti Go (ehemals bekannt als MobileIron Go) wird derzeit nicht unterstützt.
- Die Ivanti Tunnel (VPN)-App wird derzeit nicht unterstützt.
- Spaces und Space-Delegierung werden derzeit nicht unterstützt.
- Die MTD-Lösung (Mobile Threat Defense) wird derzeit nicht unterstützt.
- Die Zero Sign-on-Lösung von Ivanti wird auf Geräten unterstützt, die als nicht verwaltete Geräte kategorisiert sind.
- Richtlinienaktionen werden nicht vollumfänglich unterstützt.

12.7.7. Empfohlene Schritte für die Evaluierung

Folgende Schritte werden für die Validierung einer Lösung empfohlen:

1. Erstellen Sie eine eigene Organisationseinheit (Benutzergruppe) mit einem Testbenutzer in Ihrer Verzeichnisquelle (z. B. Active Directory). Dadurch werden Beeinträchtigungen aktiver Organisationseinheiten vermieden.
2. Synchronisieren Sie die Benutzer zwischen Ivanti, Google und der Verzeichnisquelle (LDAP). Stellen Sie sicher, dass die "Test-Org.Einheit" in den Benutzergruppen verfügbar ist.
3. Integrieren Sie Ivanti Neurons for MDM in Google wie in den obigen Schritten erläutert.
4. Erstellen Sie die ChromeOS Blueprint-Konfiguration und verteilen Sie sie nur an die Benutzergruppe "Test-Org.Einheit".
5. Starten Sie ein Chromebook (vorgefertigt oder vorab registriert). Vergewissern Sie sich, dass es in der Geräteliste angezeigt wird.
6. Überprüfen Sie, ob die ChromeOS Blueprint-Einstellungen auf dem Gerät verfügbar sind.
7. Führen Sie die entsprechenden Schritte für die Android-App-Verteilung aus.

12.8. Firmware-Verwaltung

Dieser Abschnitt enthält die folgenden Themen:

- Für Zebra OTA-Service registrieren
- Samsung E-FOTA-Lizenzverwaltung (außer Betrieb)

12.8.1. Für Zebra OTA-Service registrieren

Wenn Sie sich beim Zebra OTA(Over The Air)-Dienst registriert haben, können Sie die Zebra OTA-Konfiguration aktivieren, um die Firmware-Details der in der Cloud registrierten Zebra-Geräte zu empfangen und zu aktualisieren.

Verfahren

1. Wechseln Sie zu **Admin > Infrastruktur > Zebra OTA**. Die Seite **Zebra OTA-Dienst** wird angezeigt.
2. Klicken Sie bei **Link zum OTA-Dienst von Zebra** auf **Starten**.
3. Geben Sie Ihre Zebra OTA-Zugangsdaten ein, um sich anzumelden, und folgen Sie den Schritten, um eine Genehmigung zur Nutzung der Zebra-Dienste anzufordern.
4. Klicken Sie auf **Verifizierung abschließen**, um die Bestätigung der Verbindung zum Zebra-Dienst zu erhalten. Wenn die Verbindung bestätigt wird, wird der Status der erfolgreichen Registrierung auf der Seite „Zebra OTA-Dienst“ angezeigt.

Um die Registrierung zu widerrufen, klicken Sie in der Spalte **Aktionen** auf **Widerrufen**. Die Aktion **Widerrufen** entfernt alle Zebra OTA-Konfigurationen aus den bestehenden Konfigurationen. Klicken Sie auf **Aktualisieren**, um sich erneut bei Zebra OTA anzumelden. Die Aktualisierungsaktion hat keine Auswirkungen auf die bestehenden Konfigurationen.

Nach der Registrierung können Sie die Zebra-Firmwarekonfiguration aktivieren, die der Go-Client empfängt und für Zebra-Geräte (mit Android Version 8.0 oder einer unterstützten neueren Version) im Geräteeigentümermodus übernimmt. Bei der Übernahme der Konfiguration wird die Firmware heruntergeladen und wie in der Konfiguration vorgesehen auf das Gerät installiert. Weitere Informationen zum Aktivieren der Zebra-Firmwarekonfiguration finden Sie unter **System-Update-Konfiguration**.

Nach Abschluss der Firmware-Aktualisierung können Sie den Status der Firmware-Aktualisierung auf dem Zebra-Gerät unter der Spalte **System-Update** auf der Seite „Geräte“ anzeigen. Im Folgenden finden Sie die möglichen Zustände:

- **Unbekannt** - Wird vom Client oder Betriebssystem nicht unterstützt
- **Aktuell** - Das Gerät verfügt über das aktuellste verfügbare Update
- **Ausstehend** - Die Konfiguration des System-Updates wird übernommen, aber das Update wurde noch nicht heruntergeladen oder angewendet.
- **Herunterladen** - Das System-Update wird auf den Client heruntergeladen.
- **Verfügbar** - System-Update ist derzeit für das Gerät verfügbar
- **Fehler** - Fehler beim Download oder der Installation.

Die Spalte **Zebra Patch Version** auf der Seite „Geräte“ zeigt die Zebra Patch-Informationen des Geräts an.

> Die **Zebra-Patchversion** wird für Geräte mit Android 11 oder einer späteren Version nicht unterstützt. Es wird nur das **vollständige Zebra-Upgrade** unterstützt.

12.8.2. Samsung E-FOTA-Lizenzverwaltung (außer Betrieb)

Der Samsung E-FOTA-Dienst wird ab Juli 2022 außer Betrieb gesetzt. Weitere Informationen finden Sie in den Ankündigungen von Samsung.

> Sie können den Samsung E-FOTA-Dienst ab sofort nicht mehr konfigurieren. Wenn Sie jedoch eine vorhandene E-FOTA-Konfiguration haben, können Sie die Konfiguration deaktivieren, indem Sie zu **Admin** > **Firmware-Verwaltung** > **Samsung E-FOTA** gehen und auf die Option **Deaktivieren** klicken.

12.9. Verwalten von Skripten und Dateien

Administratoren können Skripte und Dateien verwalten, die in Konfigurationen verwendet und per Push auf Geräte übertragen werden können.

Dieser Abschnitt enthält die folgenden Themen:

Alle Skripte

Dateien

12.9.1. Alle Skripte

Gilt für: macOS- und Windows-Geräte

Auf der Seite **Admin > Skripte und Dateien > Alle Skripte** ermöglicht es Ivanti Neurons for MDM Benutzern mit der Rolle "Systemverwaltung" Skripte zu erstellen oder hochzuladen und Skripte zu verwalten, die in Konfigurationen verwendet und an Geräte verteilt werden können. Sie können den Skripten benutzerdefinierte Attribute und die resultierenden Werte den konfigurierten Geräten zuweisen. Verwenden Sie Audit Trails, um Protokolle zu Skriptänderungen anzuzeigen, und die Seite "Gerätedetails", um die Ausführungsergebnisse anzuzeigen.

Sie können ein Skript schreiben, das beliebige Einstellungen auf Geräten konfiguriert. Beispielsweise können Sie Skripte ausführen, die:

- die Gerätebenutzer zwingen, ihre Passwörter monatlich zu ändern,
- den Bildschirm nach 5 Minuten ohne Eingabe sperren, oder
- ein sicheres WLAN konfigurieren.

Dieser Abschnitt enthält die folgenden Themen:

- Hinzufügen eines Skripts
- Skript ändern
- Verwenden von Skriptvariablen (gilt für Windows und macOS)
- Skript testen
- Ergebnisse der Skriptausführung überprüfen

Hinzufügen eines Skripts

Sie können ein Repository mit Bash-Skripten (für macOS) und ps1-Skripten (für Windows) erstellen oder hochladen. Dieses Repository kann in einer Konfiguration verwendet werden, um ein Skript auszuwählen und zu verteilen, das auf den Geräten gemäß dem in der Konfiguration angegebenen Zeitplan ausgeführt wird.

Sie können beispielsweise ein Shell-Skript für die Ausführung auf Geräten erstellen. Sie können bei Bedarf Wrapper verwenden. Die Ausführung von Binärdateien aus dem Shell-Skript heraus wird nicht unterstützt.

> Ivanti empfiehlt dringend, die Shell-Skripte zu testen, bevor Sie diese auf den Geräten ausführen, um deren Robustheit und Qualität sicherzustellen. Starten Sie Ihr Skript lokal und korrigieren Sie eventuelle Fehler.

Verfahren

1. Wechseln Sie zu **Admin > Alle Skripte**.
2. Klicken Sie auf **+Hinzufügen**.
3. Geben Sie einen Namen und eine Beschreibung für das Skript ein.
4. Wählen Sie als Plattformtyp macOS oder Windows aus.
5. Klicken Sie auf eine der folgenden Typen:
    - **bash**
    - **zsh**

- **python**
- **swift**
- **ps1**

6. Wählen Sie die Option **Als Root ausführen**, um das Skript als Root auf Geräten auszuführen. Standardmäßig ist diese Option aktiviert.
7. Im Skript-Editor können Sie ein Skript eingeben, per Drag&Drop ablegen oder kopieren und in das Textfeld einfügen.
8. Alternativ können Sie auch auf **Code aus einem Skript importieren** klicken, um eine vorhandene Skriptdatei per Drag & Drop zu verschieben, oder auf „Datei auswählen“, um die Skriptdatei zu suchen, die auf Ivanti Neurons for MDM hochgeladen werden soll. Dadurch wird ein vorhandenes Skript im Skript-Editor ersetzt. Diese Aktion kann nicht rückgängig gemacht werden. Klicken Sie auf **Importieren**. Der Code aus dem hochgeladenen Skript wird im Skript-Editor angezeigt.
9. (Optional) Wählen Sie im Abschnitt Benutzerdefinierte Attribute verfügbar ein oder mehrere der angezeigten benutzerdefinierten Geräteattribute aus, um sie mit dem Skript zu verknüpfen. Sie können damit die resultierenden Skriptausführungswerte den geräteeigenen Attributen der konfigurierten Geräte zuordnen. Klicken Sie auf **Beispielcode für benutzerdefinierte Attribute**, um einen Beispielcode mit benutzerdefinierten Attributen in einem Skript anzuzeigen.
10. Klicken Sie auf **Speichern**.

Die Bezeichnungen für benutzerdefinierte Attribute im Skript sollten in Kleinbuchstaben geschrieben werden. Wenn auf die benutzerdefinierten Attribute in einem Skript verwiesen wird, können die Attribute nicht entfernt werden. Wenn Sie ein benutzerdefiniertes Attribut (z.B. seinen Namen) ändern und es mit einem Skript verknüpft ist, sollten Sie die zugehörigen Skripte entsprechend ändern.

Skript ändern

Skript bearbeiten oder entfernen:

1. Wechseln Sie zu **Admin > Skripte > Alle Skripte**.
2. Klicken Sie in der Spalte **Aktionen** für das Skript auf das entsprechende Symbol, um die Aktion zu bearbeiten oder zu löschen.
3. Folgen Sie den Anweisungen auf dem Bildschirm, um die Aktion abzuschließen.

Wenn ein Skript (Inhalt, Name, Beschreibung) geändert wird, werden alle dem Skript zugeordneten Konfigurationen neu auf die Geräte verteilt.

Verwenden von Skriptvariablen (gilt für Windows und macOS)

Definieren und speichern Sie Skripteingaben wie Umgebungs- und Substitutionsvariablen im Skript-Repository. In der Mobile@Work for macOS-Skriptkonfiguration oder in der Ivanti Bridge für Windows-Skripte und -Aktionen-Konfiguration stehen, je nach verknüpftem Skript, die zugehörigen Skriptvariablen nach Bedarf zur Verfügung. Bei macOS erfordert diese Funktion **Mobile@Work for MacOS** 1.71.0 bzw. die letzte freigegebene Version, die von Ivanti Neurons for MDM unterstützt wird. Bei Windows ist für diese Funktion **Ivanti Bridge** erforderlich.

Verwenden Sie die Variablen, um ein Skript bei jeder Ausführung mit unterschiedlichen Werten auszuführen. Beispielsweise kann ein Administrator ein Skript mit der Umgebungsvariable $ als Skriptvariable erstellen und mit einer Skriptkonfiguration für Mobile@Work for macOS oder einer Windows-Konfiguration verknüpfen. Wenn die Konfiguration verteilt und auf jedem Benutzergerät installiert wird, sendet die Ivanti Neurons for MDM eine andere registrierte Benutzer-E-Mail-Adresse für jedes Gerät, um bestimmte Aktionen durchzuführen. Das Ivanti Neurons for MDM-Administrationsportal unterstützt benutzerdefinierte Variablen.

Skriptvariable hinzufügen:

1. Wechseln Sie zu **Admin > Skripte > Alle Skripte**.
2. Klicken Sie im Abschnitt „Skripteingabe“ auf **+ Hinzufügen**.
3. Geben Sie auf der Popup-Seite „Skripteingabe hinzufügen - Umgebungsvariable“ die folgenden Details ein:
    - Zu zeigende Beschriftung - Dieser Text wird als Beschriftung auf der Konfigurationsseite des Skripts Mobile@Work für macOS angezeigt. Zum Beispiel OS-Ordner eingeben, Apache-Nummer eingeben und so weiter.
    - Name der Umgebungsvariable - zum Beispiel JAVA_HOME, OS_VERSION und so weiter. Ivanti Neurons for MDM ersetzt Werte für die Skriptvariablen, wenn die Konfigurationsdetails an ein Zielgerät gesendet werden, da die Werte in der Datenbank enthalten sind.
    - Standardwert der Umgebungsvariable - z. B. 1024, bin/java, $, und so weiter. Die Eingabevariablen würden in dem von einem Administrator hochgeladenen oder bearbeiteten Skript verwendet. Siehe dazu auch die folgenden Hinweise.

Überprüfen Sie unter „Vorschau“, wie der Wert der Umgebungsvariablen als Skripteingabe auf der Konfigurationsseite angezeigt wird.

5. Klicken Sie auf **Speichern**.

Auf diese Weise stehen der Konfiguration nur das Label und der Standardwert zur Verfügung und nicht der Name der Umgebungsvariablen, was eine Abstraktionsebene darstellt.

- Als Wert der Umgebungsvariablen können alphanumerische Werte (z. B. 1024, bin/java, root@localhost) oder Systemattribute (z. B. $) verwendet werden.
- Der Wert der Umgebungsvariable kann bei der Bereitstellung auf der Konfigurationsseite geändert oder gelöscht werden.
- Wenn der Wert der Umgebungsvariablen nicht angegeben ist, stellen Sie sicher, dass bei der Skriptbereitstellung ein Wert angegeben wird. Andernfalls wird der leere Wert an das Skript übergeben.
- Nachdem eine Skriptkonfiguration verteilt und auf dem Gerät installiert wurde, hat die Bearbeitung von Umgebungsvariablen auf der Seite **Admin > Skripte und Dateien > Alle Skripte** keine Auswirkungen auf die vorhandenen Konfigurationen, die mit dem Skript verknüpft sind. Siehe auch **Mobile@Work für macOS-Skript-Konfiguration**. Für Windows siehe **Ivanti Bridge für Windows-Skripte und -Aktionen-Konfiguration**.

Skript-Variable bearbeiten

Um eine Skriptvariable zu ändern, klicken Sie auf das Bearbeitungssymbol (Bleistift) neben der Variable und speichern dann die Änderungen.

Wenn sich eine Skriptkonfiguration auf ein Skript mit Skriptvariablen bezieht, wird die Bearbeitung des Labels einer vorhandenen Skriptvariablen auch in der Skriptkonfiguration berücksichtigt. Aber:

- Eine Änderung des Standardwerts der Skriptvariable wird in bestehenden Konfigurationen nicht berücksichtigt.
- Eine Änderung des Standardwerts der Skriptvariable wird in allen neuen Konfigurationen berücksichtigt, die mit dem vorhergehenden Skript erstellt wurden.

Skript-Variable löschen

Um eine Skriptvariable zu löschen, klicken Sie auf das Löschsymbol (Minuszeichen) neben der Variable und bestätigen die Auswahl.

Eine neu erstellte Skriptvariable oder die Löschung einer vorhandenen Skriptvariable wird auch in einer bereits vorhandenen Konfiguration berücksichtigt.

Skript testen

Führen Sie ein Skript im Debug-Tool aus, ohne die Skripte speichern zu müssen, bevor Sie es auf einem Gerät testen.

Voraussetzungen

- Bei macOS erfordert diese Funktion **Mobile@Work for MacOS** 1.67 bzw. die letzte freigegebene Version, die von Ivanti Neurons for MDM unterstützt wird.
- Bei Windows erfordert diese Funktion die Konfiguration **Ivanti Bridge für Windows-Skripte und -Aktionen**.

Verfahren

1. Wechseln Sie zu **Admin > Skripte > Alle Skripte**.
2. Fügen Sie im Skript-Editor ein Skript hinzu oder importieren Sie es.
3. Wenn der Mandant mehrere Spaces hat, wählen Sie einen Space aus.
4. Wählen Sie im Abschnitt "Testskript" die Option **macOS** oder **Windows** als Plattform aus.
5. Suchen und wählen Sie im Textfeld **Geräte suchen** das Gerät, auf dem das Skript getestet werden kann. Das Gerät kann nach Seriennummer,Benutzername, Gerätename und OS -Version gesucht werden.
6. Klicken Sie auf **Jetzt testen**. Auf diese Weise können Sie eine Umgebungsvariable hinzufügen, bearbeiten und löschen und das Skript mit diesem Zustand testen (selbst ohne die vorgenommenen Änderungen zu speichern). Für **Windows** Script wird ein Popup-Fenster auf dem Bildschirm angezeigt, dass darauf hinweist, dass die Ausführung des Skripts gestartet wird. Sie können den Status nach einiger Zeit auf der Registerkarte "Gerätedetails – Protokolle" anzeigen.
7. Klicken Sie auf **Speichern**.
8. Warten Sie bei macOS, bis das Skript per Push auf das Gerät übertragen und ausgeführt wird.
9. Überprüfen Sie die veröffentlichten Testergebnisse in den Abschnitten „Skripteingabe“ (mit Angaben zu den Umgebungsvariablen), „Skriptausgabe“ und „Benutzerdefinierte Attribute“. Die Standardwerte der Umgebungsvariablen werden ebenfalls angezeigt.

Ergebnisse der Skriptausführung überprüfen

Protokolle der Ergebnisse der Skriptausführung anzeigen:

1. Gehen Sie zu Geräte.
2. Klicken Sie auf den Namen des Geräts.
3. Klicken Sie auf die Registerkarte **[Logs]**.
4. In einer Zeile, die die Aktion für die Skriptausführung anzeigt, können Sie folgende Informationen überprüfen:
    - Den Skriptnamen in der Spalte „Details“.
    - Den Status der Skriptausführung in der Spalte „Status“.
    - Datum und Uhrzeit der Skriptausführung in der Spalte „Datum“.
    - Die Skriptausführungsprotokolle (plist der Geräteprotokolle), indem Sie auf das Augensymbol unter der Spalte „Aktionen“ klicken.

Verwenden Sie Filter, um die Zeilen der **Skriptausführung** anzuzeigen. Protokolle aus diesen Zeilen enthalten die Ausgabe (plist) der Standardausgabe und den Standardfehler für die Skripte.

6. Verwenden Sie Filter, um die Zeilen der **Ergebnisverarbeitung der Skriptausführung** anzuzeigen. Protokolle aus diesen Zeilen enthalten Details (plist) über die Verarbeitung der Ergebnisse.

- Wenn einem Skript keine benutzerdefinierten Attribute zugeordnet sind, müssen keine Ergebnisse verarbeitet werden. Solche Skripte werden in der Liste der gefilterten Zeilen nicht angezeigt.
- Wenn einem Skript benutzerdefinierte Attribute zugeordnet waren und sie das erwartete Format besaßen, werden die benutzerdefinierten Attribute aus den Ergebnissen zugeordnet und der Status wird als Erfolg angezeigt. Sie können die zugeordneten benutzerdefinierten Attribute und deren Werte auf der Registerkarte **Attribute** überprüfen.
- Wenn einem Skript benutzerdefinierte Attribute zugeordnet waren und sie nicht das erwartete Format aufwiesen, werden die benutzerdefinierten Attribute aus den Ergebnissen nicht zugeordnet und der Status wird als Fehler angezeigt.
- Wenn das Ergebnisformat korrekt ist, aber nicht alle zugeordneten benutzerdefinierten Attribute in dem Ergebnis gesendet werden, wird als Status „Fehler“ angezeigt.
- Wenn eine Skript-Variable zusammen mit dem Skript gesendet wird, enthalten die Ergebnisprotokolle der die Skript-Ausführung Details (plist) für die Skript-Variable.

Verwandte Themen:

- **Script-Konfiguration für Mobile@Work für macOS**
- **Erstellen einer Konfiguration**
- **Ivanti Bridge für Windows-Skripte und -Aktionen-Konfiguration**

12.9.2. Dateien

Gilt für macOS-Geräte

Ivanti Neurons for MDM ermöglicht es Benutzern mit der Rolle "Systemverwaltung" Skripte zu erstellen oder hochzuladen und Skripte zu verwalten, die in Konfigurationen verwendet und an Geräte verteilt werden können.

Verfahren

1. Wechseln Sie zu **Admin** > **Skripte und Dateien** > **Dateien**.
2. Klicken Sie auf der Seite **Dateien** auf **+ Hinzufügen**.
3. Geben Sie im Fenster **Datei erstellen** folgende Details ein:
    1. Geben Sie in das Feld **Name** einen Namen zum Identifizieren der Datei ein.
    2. Geben Sie in das Feld **Beschreibung** eine Beschreibung ein, die den Zweck der Datei erläutert.
    3. Klicken Sie im Bereich **Datei hochladen** auf **Datei auswählen**, um die .zip-Datei hochzuladen. Alternativ können Sie eine Datei von Ihrem Gerät hierher ziehen.
4. Klicken Sie auf **Speichern**.
   Die neu hinzugefügte Datei wird auf der Seite **Dateien** angezeigt.

Bearbeiten einer Datei

1. Wechseln Sie zu **Admin** > **Skripte und Dateien** > **Dateien**.
2. Wählen Sie die zu bearbeitende Datei aus und klicken Sie auf **Bearbeiten**.
   Das Fenster **Datei bearbeiten** wird angezeigt.
3. Optional können Sie die Felder **Name** und **Beschreibung** bearbeiten.
4. Klicken Sie im Bereich **Datei hochladen** auf **Andere Datei auswählen**, um die .zip-Datei hochzuladen. Alternativ können Sie eine Datei von Ihrem Gerät hierher ziehen.
5. Klicken Sie auf **Aktualisieren**.

Löschen einer Datei

Um vorhandene **Dateien** zu löschen, wechseln Sie zu **Admin** > **Skripte und Dateien** > **Dateien**, wählen Sie die zu löschenden Dateien aus und klicken Sie auf **+ Löschen**.

Wenn die **Datei(en)** mit einer Konfiguration verknüpft ist/sind, zeigt Ivanti Neurons for MDM die folgende **Warnung** an: **"Die Datei kann nicht gelöscht werden, da sie von anderen Richtlinien verwendet wird."**

12.10. Branding

Dieser Abschnitt enthält die folgenden Themen:

- Administration > App-Katalog für Apple (Branding)
- Branding des Android App-Katalogs
- Admin > Android Kiosk-Branding
- Branding von E-Mail-Vorlagen
- Selbstbedienungsportal
- Branding für das Selbstbedienungsportal)
- Anmeldung mit Branding für mehrere Benutzer (Web-Clip)
- Organisation

12.10.1. Administration > App-Katalog für Apple (Branding)

Lizenz: Gold

Sie können den Apple App-Katalog mit einem Branding versehen, damit Ihre Endbenutzer auf iPhone-, iPad- und Mac-Geräten das Erscheinungsbild vertrauter ist. Sie können die folgenden Objekte im App-Katalog für Apple individuell anpassen:

- App-Symbol (PNG, 360px quadratisch)
- App-Name
- App-Banner-Bild (PNG, 360x64)
- Textfarbe

> Es gibt zwei Möglichkeiten, auf den Apple App Catalog zuzugreifen: Eigenständiger App Catalog und Integrierter App Catalog. Der eigenständige App Catalog ist für iPhone, iPad und Mac-Geräte verfügbar. Der integrierte App-Katalog ist nur für Mac-Geräte verfügbar.

Branding des Apple App-Katalogs

Die auf dieser Seite vorgenommenen Änderungen wirken sich auf den Startbildschirm, den Begrüßungsbildschirm und die Startseite der Anwendung aus. Die Schritte sind für den eigenständigen App Catalog und den integrierten App Catalog ähnlich.

Verfahren

1. Klicken Sie auf der Seite **Branding für den App-Katalog von Apple** auf **Anpassen** (oben rechts).
2. Ziehen Sie im Abschnitt **App-Symbol** die Logo-Datei in das gepunktete Feld oder klicken Sie auf **Datei auswählen**, um sie zu suchen und auszuwählen. Das App-Symbol wird auf dem iOS-Startbildschirm angezeigt.
3. Bearbeiten Sie im Abschnitt **App-Name** den Text **App-Katalog-Name**, um die Bezeichnung im Begrüßungsbildschirm zu ändern.
4. Der Name und das Symbol werden für das Banner des Startbildschirms übernommen. Deaktivieren Sie zur Änderung eines benutzerdefinierten Banner-Bildes die Option **Name und Symbol auf das Banner des Startbildschirms anwenden**. Daraufhin wird der Abschnitt **App-Banner-Bild** angezeigt.
5. Ziehen Sie zur Änderung des App-Bannerbildes die neue Banner-Bilddatei in das gepunktete Feld oder klicken Sie auf die Option **Datei auswählen**, um die Datei zu suchen und auszuwählen. Das App-Bannerbild erscheint in der oberen Leiste des App-Startbildschirms.
6. Klicken Sie im Abschnitt **Textfarbe** auf das Feld für den Hex-Farbcode, um eine Farbe auszuwählen, oder geben Sie den Hex-Farbcode ein, der dem Text und den Symbolen zugewiesen werden soll. Diese Einstellung gilt für den Text auf dem Begrüßungsbildschirm, den Namen der App, das Banner und die Aktionsschaltfläche.
7. Klicken Sie auf **Änderungen speichern**.

Der von Ihnen eingegebene Name des App Catalog gilt sowohl für Android als auch für macOS und iOS.

12.10.2. Branding des Android App-Katalogs

Lizenz: Gold

Sie können den Android {{App Catalog}} mit Ihrem eigenen Design versehen, damit er von Ihren Endbenutzern leichter wiedererkannt wird. Sie können die folgenden Objekte im App-Katalog für Android individuell gestalten:

- Logo für den Katalog (PNG, 360 x 64)
- Katalogname
- Farbe der Aktionsleiste
- Shortcut-Symbol
- Shortcut-Bezeichnung

Branding des Android App-Katalogs

Verfahren

1. Klicken Sie im Bildschirm **Branding für den App Catalog für Android** auf **Anpassen** (oben rechts).).
2. Ziehen Sie die Logo-Datei in das gepunktete Feld oder klicken Sie auf **Datei auswählen**, um sie aus Ihrem Dateisystem auszuwählen.
3. Klicken Sie auf die **Aktionsleiste**, um eine Farbpalette anzuzeigen, aus der Sie auswählen können, oder geben Sie die Hexadezimalzahl für die von Ihnen bevorzugte Farbe ein.
4. Bearbeiten Sie den **Namen des App-Katalogs**, um die Bezeichnung des Katalogs zu ändern.
5. Der von Ihnen eingegebene Name des App Catalog gilt sowohl für Android als auch für macOS und iOS.
   Um das Shortcut-Symbol zu ändern, ziehen Sie die Symboldatei in das gepunktete Feld. Sie können auch auf **Datei auswählen** klicken, um die Datei in ihrem Dateisystem auszuwählen.
6. Bearbeiten Sie die **Shortcut-Bezeichnung**, um die Beschriftung für das App-Shortcut zu ändern.
7. Klicken Sie auf **Änderungen speichern**.

12.10.3. Admin > Android Kiosk-Branding

Lizenz: Silver

Sie können die Seite in Android Kiosk mit Ihrem eigenen Design versehen, damit sie von Ihren Endbenutzern leichter wiedererkannt wird. Sie können folgende Einstellungen kundenspezifisch anpassen:

- Bannerlogo (PNG, 840x114 Pixel) oder Text
- Bannerrandfarbe
- Bannerhintergrundfarbe
- Bildschirmhintergrundfarbe
- Bildschirmhintergrundbild (1280x800 Pixel)
- Bildschirmhintergrundformat

Bildschirm Branding für Android Kiosk

Verfahren

1. Gehen Sie zu **Admin > Android Kiosk**.
2. Klicken Sie auf der Seite **Branding für den Kiosk-Modus** auf **Branding erstellen**.
3. Geben Sie im Feld **Name** den Namen für das Kiosk-Modus-Branding ein.
4. Wenn Sie das Banner ausschalten möchten, deaktivieren Sie das Kontrollkästchen **Oberes Banner aktivieren**.
5. Klicken Sie in das Feld **Banner-Hintergrundfarbe**, um eine Farbpalette anzuzeigen und die Hexadezimalzahl für die gewünschte Farbe auszuwählen oder einzugeben.
6. Klicken Sie in das Feld **Banner-Randfarbe**, um eine Farbpalette anzuzeigen und die Hexadezimalzahl für die gewünschte Farbe auszuwählen oder einzugeben.
7. Klicken Sie auf **Bild/Logo** oder **Text**, um den Bannerinhalt festzulegen.
8. Wenn Sie **Bild/Logo** ausgewählt haben, ziehen Sie die Bilddatei per Drag and Drop hinein, oder klicken Sie zur Auswahl einer Bilddatei auf **Datei wählen**.
9. Wenn Sie **Text** ausgewählt haben, geben Sie den gewünschten Text für die Anzeige im Banner ein.
10. Klicken Sie auf die Registerkarte **Hintergrund**.
11. Klicken Sie in das Feld **Hintergrundfarbe,** um eine Farbpalette anzuzeigen und die Hexadezimalzahl für die gewünschte Farbe auszuwählen oder einzugeben.
12. So ändern Sie das Hintergrundbild:
13. a. Löschen Sie das Standardbild.
    b. Ziehen Sie das gewünschte Bild per Drag&Drop in das Feld, oder wählen Sie das gewünschte Bild mit Datei wählen aus.
    c. Wählen Sie das bevorzugte Layout aus.
    Klicken Sie auf **Änderungen speichern**.
    Das erstellte Branding für den Kiosk-Modus wird auf der Seite **Branding für den Kiosk-Modus** angezeigt. Um das benutzerdefinierte Branding weiter zu bearbeiten, klicken Sie in der Spalte **Aktionen** auf das Symbol „Bearbeiten“. Klicken Sie auf das Löschsymbol, um das benutzerdefinierte Branding zu löschen. Beim Löschen des benutzerdefinierten Kiosk-Brandings wird die Konfiguration mit dem Branding auf das Standard-Branding zurückgesetzt.

12.10.4. Branding von E-Mail-Vorlagen

Sie können die E-Mail-Einladung für den Endbenutzer mit Ihrem eigenen Design versehen, damit sie von Ihren Endbenutzern leichter wiedererkannt wird. Klicken Sie auf die Option **Auf die Standardeinstellungen zurücksetzen**, um die Anpassungen zu löschen.

Sie können die folgenden E-Mail-Vorlagen in allen unterstützten Sprachen anpassen:

- **Endbenutzer-Einladung** – Laden Sie einen Benutzer ein, seine Geräte zu verbinden, um Zugriff auf Apps und Konfigurationen zu erhalten.
- **Benachrichtigung zum Zurücksetzen des Passworts** – Das System sendet Erinnerungs-E-Mails 7 Tage bzw. 24 Stunden vor Ablauf des Passworts lokaler Konten. Dies gilt nicht für LDAP-Konten.
- **Registrierungsbestätigung** – E-Mail, die gesendet wird, nachdem ein Benutzer die Registrierung abgeschlossen hat. Sie können diese Funktion nutzen, um den Benutzern für die Registrierung zu danken und ihnen weitere Lernressourcen vorzuschlagen.
- **Benachrichtigung zur Richtlinien-Compliance** – E-Mail, die gesendet wird, wenn Geräte nicht mehr konform sind.

Dieser Abschnitt enthält die folgenden Themen:

- E-Mail-Vorlage anzeigen und testen
- Anpassung der Header in der Mitteilung
- E-Mail-Vorlage anpassen
- Unterstützte E-Mail-Variablen

E-Mail-Vorlage anzeigen und testen

Sie können die E-Mail-Vorlagen in der Vorschau anzeigen und testen. Bei dem Test können Sie eine aus der Vorlage erstellte E-Mail an eine von Ihnen angegebene E-Mail-Adresse senden.

E-Mail-Vorlage anzeigen und testen:

1. Klicken Sie auf Administrator.
2. Klicken Sie unter „E-Mail-Vorlagen“ auf **Endbenutzer-Einladung**, **Benachrichtigung zum Zurücksetzen des Passworts**, **Registrierungsbestätigung** oder **Benachrichtigung zur Richtlinien-Compliance**.
3. Klicken Sie auf den Link **Vorschau und Test** für die E-Mail-Vorlage, die Sie anzeigen und testen wollen.
4. Zeigen Sie die erstellte Vorlage in dem Fenster für die erstellte Vorlage an..
5. Geben Sie eine Test-E-Mail-Adresse an, an die die Test-E-Mail gesendet werden soll.
   Wenn die von Ihnen angegebene E-Mail-Adresse einem aktuellen Benutzer gehört, ersetzt die Test-E-Mail die Werte für die meisten Variablen in der E-Mail-Vorlage, sodass Sie eine sehr genaue Vorstellung erhalten, wie der Benutzer die E-Mail sieht. Die Test-E-Mail ersetzt jedoch keine Werte für Variablen, welche die Cloud bei der Erstellung der eigentlichen E-Mail-Einladung generiert.
6. Klicken Sie auf **Test-E-Mail senden**.

Anpassung der Header in der Mitteilung

1. Klicken Sie auf Administrator.
2. Klicken Sie auf **E-Mail-Vorlagen**.

3. Klicken Sie auf das Symbol **Bearbeiten** (in der Spalte „Aktionen“, die mit der E-Mail-Vorlage verknüpft ist, die Sie bearbeiten wollen).
4. Geben Sie beliebige neue Einstellungen für den **E-Mail-Anzeigenamen**, die **Absender-E-Mail-Adresse**, die **Antwort-E-Mail-Adresse** und **SMTP-E-Mail-Konfiguration einrichten** ein.
5. Wenn Sie die Antwort- und die Senderadresse anpassen, sollten Sie den E-Mail-Relay-Service in die Whitelist aufnehmen, damit Ihre E-Mails nicht durch den SPAM-Filter blockiert werden. Weitere Informationen finden Sie in **diesem Dokument**.
   Klicken Sie auf **Speichern**.
6. Überprüfen Sie die Vorschau der E-Mail-Vorlage und klicken Sie auf **Speichern**.

Verwenden der SMTP-Konfiguration

Die hinzugefügte Option **SMTP-E-Mail-Konfiguration einrichten** ermöglicht es Administratoren, eine eigene E-Mail-Server-Integration für ausgehende Benachrichtigungen zu konfigurieren.

1. Wechseln Sie zu **Admin > Branding > E-Mail-Einstellungen** und aktivieren Sie die Option **SMTP-E-Mail-Konfiguration einrichten**.
2. Aktualisieren Sie die folgenden Felder:
   - SMTP-Server
   - SMTP-Serverport
   - [Protocol]
   - Benutzername
   - Passwort
3. Klicken Sie auf **Test**, um eine Test-E-Mail zu senden, Der Bildschirm **Test-E-Mail** wird angezeigt.
4. Geben Sie den **Empfänger** und den **Text** der Nachricht ein und klicken Sie auf **Speichern**.

> Wenn die Anmeldeinformationen falsch sind, wird eine Fehlermeldung angezeigt.

5. Klicken Sie auf **Speichern**.

Die folgende Tabelle enthält die Felder und Beschreibungen des Fensters "SMTP-Konfiguration":

Felder	Beschreibung
SMTP-Server	Geben Sie die IP-Adresse oder den vollständig qualifizierten Hostnamen des SMTP-Servers an, den der Ivanti Neurons for MDM Server verwenden soll.
SMTP-Serverport	Geben Sie den Port an, der für den SMTP-Server konfiguriert ist.
[Protocol]	Falls es sich bei dem zu konfigurierenden SMTP-Server um einen abgesicherten Server handelt, sprich, wenn er das SMTPS-Protokoll verwendet, wählen Sie die Schaltfläche "SMTPS". Anderenfalls übernehmen Sie die Einstellung "SMTP".
Benutzername	Geben Sie den Benutzernamen ein, der für die SMTP-Authentifizierung erforderlich ist.
Passwort	Geben Sie das Kennwort ein, das für die SMTP-Authentifizierung erforderlich ist.

E-Mail-Vorlage anpassen

1. Wählen Sie **Admin > Branding > E-Mail-Vorlagen**.
2. Wählen Sie die zu bearbeitende Vorlage **Endbenutzer-Einladung**, **Benachrichtigung zum Zurücksetzen des Passworts**, **Registrierungsbestätigung** oder **Benachrichtigung zur Richtlinien-Compliance**.
3. Klicken Sie auf das Stiftsymbol neben der E-Mail-Vorlage, die Sie anpassen wollen.

4. Bearbeiten Sie gegebenenfalls die Betreffzeile.
5. Bearbeiten Sie die E-Mail-Vorlage mit HTML-Elementen im Textbereich, um die Einladung für den Endbenutzer anzupassen.

Sie können die rechts neben dem E-Mail-Text angezeigten Variablen verwenden. Siehe dazu **Unterstützte E-Mail-Variablen**.

6. Klicken Sie auf die Option **Vorschau**, um die E-Mail-Vorlage anzuzeigen, und ändern Sie diese, bis Sie zufrieden sind.
7. Wenn Sie die Vorlage speichern wollen, klicken Sie auf **Vorschau**. Damit wird die Vorschau erstellt und eine Speicherfunktion angeboten.

8. Klicken Sie auf **Speichern**, wenn Sie mit der Vorschau zufrieden sind.

Whitelist- und Blacklist-Inhalte in kundenspezifischen Benutzereinladungen

Beim Anpassen der E-Mail-Vorlage für Benutzereinladungen in der **Endbenutzereinladung** gibt es eine Reihe von HTML-Tags und -Attributen der Whitelist, die erlaubt sind. Es gibt auch eine Liste von Zeichenketten in der Blacklist, die in der Benutzereinladung nicht zulässig sind, um eine Cross Site Scripting (XSS)-Sicherheitslücke zu verhindern.

Sie dürfen nur die in der Einladungs-E-Mail aufgeführten Tags und Attribute verwenden. Die folgende Tabelle listet die Whitelist-Tags und die entsprechenden zulässigen Attribute auf.

Einige in der Zulassungsliste enthaltene Tags (wie: <big>) sollten kein zugelassenes Attribut besitzen und werden daher leer angezeigt.

Whitelist-Tags	Whitelist-Attribute
<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"]

Whitelist-Tags	Whitelist-Attribute
	[]
	[]
<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"]

Im Folgenden finden Sie die Liste der Zeichenketten aus der Blacklist, die in der benutzerdefinierten Benutzereinladung nicht zulässig sind.

- Script, @import, ¼script¾, script>, <script, <script>, </script>, javascript, alert(, moz-binding, expression(, +ADw-SCRIPT+AD4-,+ADw-/SCRIPT+AD4-, xml:base
- Sonderzeichen und Suche nach Javascript oder Skripten
- Das Attribut meta content mit „url=“ unterscheidet nicht zwischen Groß- und Kleinschreibung.
- Das img src ohne .svg.
- Attributwert, der „\00“ enthält.

Wenn eine der oben genannten Zeichenketten aus der Blacklist im HTML-Content der Endbenutzereinladung verwendet wird, wird eine Fehlermeldung angezeigt, wenn Sie auf **Vorschau** klicken. Diese Fehlermeldung listet den HTML-Content auf, der in der Endbenutzereinladung nicht erlaubt ist. Bearbeiten und entfernen Sie den nicht zulässigen HTML-Inhalt und klicken Sie dann auf **Vorschau**, um fortzufahren.

> Sie können keine bearbeiteten Vorlagen speichern, wenn diese HTML-Content aus der Blacklist enthalten.

Unterstützte E-Mail-Variablen

Die Cloud bietet mehrere Variablen, mit denen Sie Ihre E-Mail-Vorlagen anpassen können.

Variablen zur Einladung des Endbenutzers

[Variable]	Beschreibung
$	Benutzeraktivierungs-URL – Dies ist der Hyperlink um den Text $.
$	URL für die Cluster-Registrierung – Diesen Eintrag finden Sie NICHT in der Standardvorlage, sondern nur als indirekte Referenz (über die Variable $\{email.idp.invitation.pg4\}).
$	Markenname des Produkts – dieser wird als <title> Tag im Header der Standardvorlage definiert.
$	URL mit Firmenlogo – Dies ist das einzige Bild in der Standardvorlage. Es zeigt auf ein Bild in der MobileIron-CDN. Durch Aktualisieren der **Benutzer-Branding**-Einstellungen ändert sich der Wert, auf den **$** verweist.
${message:$	Das Register für den Benutzergeräteeigentümer.
${message:$}	Titel der E-Mail-Einladung.
${message:$}	Überprüfung, ob der Benutzer sein Gerät zur Hand hat..
${message:$}	Textanweisung in der E-Mail-Einladung.
${message:$}	Anmelde- und Registrieranweisungen.
${message:$}	E-Mails und Apps, die per Push in die Gerätedaten übertragen werden..
${message:$}	Registrierinformationen, wenn der Benutzer sein Gerät nicht zur Hand hat; dazu gehört die URL für die Cluster-Registrierung..
${message:$}	Die Fußzeile der E-Mail-Einladung mit dem Website-Label des Unternehmens.
$	Website-Label des Unternehmens – diesen Eintrag finden Sie NICHT in der Standardvorlage, sondern NUR als indirekte Referenz (über die Variable $\.

Variablen für die Benachrichtigung zum Passwortablauf.

[Variable]	Beschreibung
$	URL zum Zurücksetzen des Passworts.
$	Markenname des Produkts – dieser wird als <title> Tag im Header der Standardvorlage definiert.
$	URL mit Firmenlogo – Dies ist das einzige Bild in der Standardvorlage. Es zeigt auf ein Bild in der MobileIron-CDN. Durch Aktualisieren der **Benutzer-Branding**-Einstellungen ändert sich der Wert, auf den **$** verweist.
${message:$}	Der Titel der Benachrichtigung zum Passwortablauf
${message:$}	Der Einführungsabsatz der Benachrichtigung zum Passwortablauf.
${message:$}	Der URL-Name zum Zurücksetzen des Passworts.
${message:$}	Die Fußzeile der E-Mail-Einladung mit dem Website-Label des Unternehmens.
$	Website-Label des Unternehmens – diesen Eintrag finden Sie NICHT in der Standardvorlage, sondern NUR als indirekte Referenz (über die Variable $\.

Variablen zur Bestätigung der Registrierung

[Variable]	Beschreibung
$	Markenname des Produkts – dieser wird als <title> Tag im Header der Standardvorlage definiert.
$	URL mit Firmenlogo – Dies ist das einzige Bild in der Standardvorlage. Es zeigt auf ein Bild in der MobileIron-CDN. Durch Aktualisieren der **Benutzer-Branding**-Einstellungen ändert sich der Wert, auf den **$** verweist.
${message:$}	Der Titel der Registrierbestätigung.
${message:$}	Einführungsabsatz der Registrierbestätigung.

Variablen zur Richtlinien-Compliance

[Variable]	Beschreibung
$	Diese Variable wird durch den Inhalt ersetzt, der in der Betreffzeile der E-Mail-Compliance-Aktion innerhalb der Richtlinie eingegeben wird.
$	Diese Variable wird durch den Inhalt ersetzt, der im Nachrichtenteil der E-Mail-Compliance-Aktion innerhalb der Richtlinie eingegeben wird.
$	Markenname des Produkts – dieser wird als <title> Tag im Header der Standardvorlage definiert.
$	URL mit Firmenlogo – Dies ist das einzige Bild in der Standardvorlage. Es zeigt auf ein Bild in der MobileIron-CDN. Durch Aktualisieren der **Benutzer-Branding**-Einstellungen ändert sich der Wert, auf den **$** verweist.
${message:$}	Die Fußzeile der E-Mail-Einladung mit dem Website-Label des Unternehmens.
$	Website-Label des Unternehmens – diesen Eintrag finden Sie NICHT in der Standardvorlage, sondern NUR als indirekte Referenz (über die Variable $\.

Kundenspezifische Benutzerattributvariablen

Ein Administrator kann unter folgenden Bedingungen **kundenspezifische Attribute** als E-Mail-Variablen in der angepassten E-Mail-Vorlage verwenden:

- Die kundenspezifischen Benutzerattribute müssen auf der Seite **Administrator > Attribute** vorhanden sein.
- Die kundenspezifischen Benutzerattribute müssen von **einem Administrator Benutzern zugeordnet sein**, und es müssen für jeden Benutzer die Werte für die kundenspezifischen Benutzerattribute angegeben sein.

12.10.5. Selbstbedienungsportal

Die Einladung zur Registrierung enthält einen Link zum Selbstbedienungsportal. Endbenutzer können das Portal für die folgenden Aufgaben nutzen:

- Sperren
- Sperre aufheben
- Standort anzeigen (sofern in den **Datenschutzeinstellungen** aktiviert)
- Wipe durchführen
- Gerät löschen
- Kontoinfo (Name, Passwort, E-Mail-Adresse) ändern
- Einchecken erzwingen
- Verschlüsselung und Signatur-Zertifikate hinzufügen

Zur Registrierung weiterer Geräte klicken Endbenutzer im Registrierungsportal auf den Link, der im Selbstbedienungsportal angezeigt wird.

Wenn Endbenutzer die URL für das Selbstbedienungsportal verlegen, schicken Sie diese an **https://mydevices.mobileiron.com/user/login.html**. Für iOS-Benutzer können Sie eine **Web Clip-Konfiguration** für das Selbstbedienungsportal erstellen.

Signatur- und Verschlüsselungszertifikate hochladen.

Sie können Ihren Endbenutzern erlauben, ihre E-Mail-Signatur- und Verschlüsselungszertifikate bei der Konfiguration der von den Benutzern bereitgestellten Zertifikate im Selbstbedienungsportal hochzuladen. Diese Einstellung können Sie mit der Konfiguration der „Vom Benutzer bereitgestellten Zertifikate“ konfigurieren. Nach der Konfiguration können die Endbenutzer ihre E-Mail-Signatur- und -Verschlüsselungszertifikate hochladen.

1. Klicken Sie auf der Registerkarte Meine Zertifikate auf Zertifikat hinzufügen. Das Fenster **Zertifikat hinzufügen** wird angezeigt.
2. Aktualisieren Sie die folgenden Felder:

Feldname	Beschreibung
Zertifikatsart	Wählen Sie die Art des Zertifikats aus, das Sie hochladen wollen. Die Optionen sind: • **Verschlüsselungszertifikat** • **Signaturzertifikat** Ivanti Neurons for MDMDiese Optionen werden über das Admin Portal erstellt.Weitere Informationen dazu finden Sie unter **Identitätszertifikats-Konfiguration**.
Hochzuladendes Zertifikat	Klicken Sie auf die Option **Datei auswählen**, um die Zertifikat-Datei auszuwählen, die Sie hochladen wollen. Stellen Sie sicher, dass die Datei im PKCS12-Format vorliegt.
Passwort	Geben Sie das Passwort für die Datei ein.

3. Klicken Sie auf **Hochladen**.

Nach dem Hochladen können Sie die Liste der Zertifikate in einer Tabelle mit folgenden Details anzeigen.

Feldname	Beschreibung
Zertifikatsname	Definiert die Art des Zertifikats, d. h. Verschlüsselungs- oderSignaturzertifikat.
Ausgegeben durch	Die Details des ausgestellten Zertifikats
Hochgeladen am	Das Datum, zu dem das Zertifikat hochgeladen wurde,
Ablaufdatum	Das Verfallsdatum des Zertifikats
Aktionen	Sie können folgende Aktionen ausführen: • **Zertifikat bearbeiten** – zur Bearbeitung der Zertifikatdetails. • **Privaten Schlüssel löschen** – löscht den privaten Schlüssel aus dem Zertifikatspaket PKCS#12). • **Zertifikat löschen** – löscht das Zertifikat vom Ivanti Neurons for MDM-Server.

Wenn der Benutzer eine Zertifikat-Konfiguration hochlädt, überträgt der Server die Konfiguration mit diesem Zertifikat per Push erneut.

> Wenn ein Benutzer die Optionen „Löschen“ bzw. „Privaten Schlüssel löschen“ verwendet, erfolgt keine erneute Push-Übertragung der Konfigurationen.

Weitere Informationen finden Sie unter **Selbstbedienungsportal - Branding**.

12.10.6. Branding für das Selbstbedienungsportal)

Lizenz: Silver

Sie können das **Selbstbedienungsportal** mit dem Logo Ihres Unternehmens individuell gestalten. Wenn Sie kein Logo hinzufügen, wird das Standardservicelogo des Selbstbedienungsportals angezeigt.

Branding des Selbstbedienungsportals

Verfahren

1. Klicken Sie in dem Bildschirm für das Branding des Selbstbedienungsportals auf **Anpassen** (oben rechts).
2. Ziehen Sie die Logo-Datei (PNG, 182 x 34) in das gepunktete Feld oder klicken Sie auf **Datei auswählen**, um sie aus Ihrem Dateisystem auszuwählen.
3. Klicken Sie auf **Änderungen speichern**.

12.10.7. Anmeldung mit Branding für mehrere Benutzer (Web-Clip)

Passen Sie Ihre sichere Anmeldung für mehrere Benutzer bei iOS benutzerspezifisch an, indem Sie einen neuen Titel und ein Webclip-Symbol ergänzen.

Verfahren

1. Gehen Sie zu **Administrator > Anmeldung für mehrere Benutzer (Web-Clip).**
2. In dem Bildschirm mit der Anmeldung für mehrere Benutzer (Webclip) klicken Sie auf **Anpassen**.
3. Ziehen Sie die Logo-Datei in das gepunktete Feld oder klicken Sie auf **Datei auswählen**, um sie aus Ihrem Dateisystem auszuwählen.
4. Bearbeiten Sie zur Änderung des Labels den Text für die **sichere Anmeldung**.
5. Ziehen Sie zur Änderung des Symbols für den Webclip per Drag&Drop die Webclip-Datei in das Feld mit den Punktlinien oder klicken Sie auf die Option **Datei auswählen**, um die Datei in Ihrem Dateisystem auszuwählen.
6. Rufen Sie die Vorschau der Updates auf und klicken Sie dann auf **Änderungen speichern**.

Erstellen Sie für iPhones und iPod-Touch-Geräte Symbole in der Größe 120 x 120 Pixel oder 60 x 60 Pixel (Standardauflösung).

Erstellen Sie für iPads Symbole von 152 x 152 Pixel bzw. 76 x 76 Pixel (Standardauflösung).

Weitere Informationen finden Sie unter **Sichere Anmeldung für mehrere Benutzer in iOS**.

12.10.8. Organisation

Sie können dem Unternehmen eine Branding-Bezeichnung hinzufügen oder die Betreffzeilen von Systemalarm-E-Mails personalisieren, indem Sie mandantenspezifische Kennzeichner (z. B. einen Kundennamen) in die Betreffzeile einfügen. Wenn Sie den Namen des Unternehmens nicht aktualisieren, zeigt der Unternehmensbildschirm den Standardwert an.

Branding für das Unternehmen

Verfahren

1. Geben Sie im Unternehmensbildschirm den gewünschten Namen in das Feld **Name** ein.
2. Klicken Sie zum Hinzufügen eines Präfixes auf **Bearbeiten** und aktivieren Sie die Option **In allen systemgenerierten E-Mails (z. B. Lizenzablauf) ein Präfix vor dem Namen des Unternehmens einfügen**.
3. Klicken Sie auf **Speichern**, um Ihre Änderungen zu übernehmen.

12.11. Hinzufügen der Verwaltung von Nicht-iOS-Geräten

Lizenz: Gold

Sie verwenden zurzeit eine Version der Cloud, die für iOS-Geräte optimiert ist. Dieser Abschnitt beschreibt, wie Sie die Verwaltung von Nicht-iOS-Geräten zulassen. Nach dem Umschalten können Sie außerdem folgende Geräte verwalten:

- Android 5.0 oder unterstützte neuere Versionen
- Windows 10+

Die Entscheidung, auch Nicht-iOS-Geräte zu verwalten, kann nicht rückgängig gemacht werden.

So aktivieren Sie die Verwaltung von Nicht-iOS-Geräten:

1. Klicken Sie auf **Administrator > Zulässige Plattformen.**.
2. Klicken Sie auf **Alle Plattformen zulassen**.
3. Klicken Sie in das Kontrollkästchen **Ich verstehe, dass diese Operation nicht rückgängig gemacht werden kann**, um zu bestätigen, dass Sie wissen und verstanden haben, dass die Operation irreversibel ist.
4. Klicken Sie auf **Alle Plattformen zulassen**.

13. Pakete

Dieser Abschnitt enthält die folgenden Themen:

- Upgrades durchführen
- Secure UEM- und Secure UEM Premium-Pakete
- Bronze-, Silver- und Gold-Legacy-Pakete
  - hinzufügen
  - hinzufügen
  - Platin
- Sandbox für Vorschau oder Tests

Secure UEM- und Secure UEM Premium-Pakete

Die Secure UEM- und Secure UEM Premium-Pakete bieten die folgenden Funktionen:

	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)		✓

Diese Pakete können sich möglicherweise ändern. Wenden Sie sich zur Bestätigung des aktuellen Schemas an **Ivanti Sales**.

Bronze-, Silver- und Gold-Legacy-Pakete

In diesem Abschnitt werden die Bronze-, Silver- und Gold-Legacy-Pakete beschrieben. Das Paket wurde für das Schema **Secure UEM und Secure UEM Premium** weiterentwickelt.

Bronze

Die grundlegenden Funktionen werden im Bronze-Paket bereitgestellt. Sie können das Bronze-Paket erweitern, indem Sie:

- Hinzufügen weiterer Geräte
- Silver hinzufügen
- Gold hinzufügen

- Platinum hinzufügen

Diese Zusatzoptionen erweitern Ihre mobile Lösung über die Basis-Gerätekonfiguration hinaus.

Administratoren können sich an den **Support** wenden, wenn sie eine oder mehrere, **nur bei Bedarf verfügbare**, standardmäßig deaktivierte Funktionen für ihre Mandanten aktivieren möchten.

hinzufügen

Beim Upgrade auf Silver erhalten Sie folgende Funktionen:

- **LDAP und Connector:** Unterstützung für zusätzliche Unternehmensverzeichnisse und Zertifizierungsstellen für die Cloud.
- **Sentry:** Unterstützung der E-Mail-Zugangskontrolle.
- **Spaces:** Unterstützt die Zuweisung von Geräten für die Verwaltung durch verschiedene Administratoren (delegierte Administration).
- **Überwachter Modus:** Unterstützung einer fein abgestimmten Konfiguration auf Geräteebene, inklusive Single-App-Modus
- **Branding für das Selbstbedienungsportal:** Fügen Sie im Selbstbedienungsportal Ihr Logo ein.
- **Zertifizierungsstellen:**Nutzen Sie die Cloud als Zertifizierungsstelle.
- **Installation/Deinstallation von Apps im Hintergrund:** Automatisches Anwenden und Entfernen von Apps auf einem Mobilgerät
- **App-Whitelist/Blacklist/erforderliche Apps:** Auf Geräten installierte Anwendungen anzeigen und kontrollieren.
- **Web-Content-Filter:** Übertragung der Whitelist-/Blacklist-Richtlinien der Website auf alle Browser
- **Apple-spezifische Funktionen:** AirPlay, AirDrop, iOS Wallpaper-Verteilung und Apple TV aktivieren/einschränken.
- **Open-In-Management:** Sie steuern, welche mobilen Apps welche Unternehmensinhalte öffnen können.
- **Apple Apps and Books:** Verteilen Sie Lizenzen für mobile Apps auf Geräte und weisen Sie diese Lizenzen nach Außerdienststellung eines Geräts wieder einem anderen Gerät zu.
- **Erweiterter Support für Android Enterprise**
- **Device Enrollment:** Das Geräteregistrierungsprogramm ermöglicht es Kunden, Apple-Geräte in großen Stückzahlen zu erwerben und während der Aktivierung automatisch für MDM zu registrieren.
- **Per-App Konfiguration:** Stellen Sie konfigurierte mobile Apps so bereit, dass der Endbenutzer kaum oder überhaupt nicht aktiv werden muss.
- **VPN für fremde Apps:** Die VPN-Sicherheit wird jetzt sofort im Hintergrund auf die jeweilige mobile App abgestimmt.
- **Richtlinienabhängige Maßnahmen**
- App-Verteilungsfilter
- **Audit-Protokolle**
- **Android Kiosk-Modus:** Unterstützung für die Konfiguration von Android-Geräten, die im Kiosk-Modus arbeiten sollen.
- **Android Kiosk-Branding: Ändern Sie Hintergrund und Banner des Kioskbildschirms, der angezeigt wird, wenn das Gerät im Kiosk-Modus arbeitet.**
- **Vermeidung von Datenverlust (DLP) für Office 365 mit Graph APIs**: Erzwingt DLP-Kontrollen für die Apps in Office 365 mit Graph APIs.

hinzufügen

Eine Aktualisierung auf Gold ergänzt auch die Funktionen der Silver sowie folgende Funktionen:

- **Single Sign-On:** Benutzer müssen sich nur einmal authentifizieren und werden automatisch bei anderen mobilen Apps des Unternehmens angemeldet.
- **Branding für den App-Katalog für iOS und Android:** Zeigen Sie Ihr Unternehmenslogo im App-Katalog an.
- **Höheres Content-Limit:** 50 Dateien zu je 25 MB
- **AppConnect für iOS:** AppConnect-fähige Apps sichern und konfigurieren.
- **AppTunnel für iOS:** Sichern Sie App-Zugriff auf Unternehmensressourcen.
- **Docs@Work für iOS:** Erlauben Sie Benutzern, Dokumente anzuzeigen, zu speichern und freizugeben.
- **Single-Sign-on mit iOS-8-Zertifikat**
- **iBook/ePub-Verwaltung in iOS 8**
- **Unterstützung für macOS**
- **Benutzer-Branding**
- **Mobiles Anwendungsmanagement (MAM) mit AppConnect**
- **Abgeleitete Anmeldeinformationen**
- Unterstützung für Windows 10 (einschließlich Bridge)

Platin

Eine Aktualisierung auf Platinum ergänzt auch die Funktionen für Gold sowie folgende Funktionen:

- **Tunnel:** Konfigurieren Sie den App-spezifischen Zugriff auf Unternehmensdaten.
- **Help@Work**
- **Überwachen**
- **ServiceConnect (ServiceNow, Splunk)**

Sandbox für Vorschau oder Tests

Kunden der Cloud besitzen einen Sandbox-Mandanten zur Vorschau und zum Test neuer Releases vor deren Übernahme in die Produktionsumgebung, wenn sie den **Premium Plus** Support erworben haben.

13.1. Upgrades durchführen

Dieser Abschnitt enthält die folgenden Themen:

- Upgrade einer Lizenz
- Upgrade anfordern
- Upgrade von einem früheren Release

Upgrade einer Lizenz

Die grundlegenden Funktionen werden im Bronze-Paket bereitgestellt. Sie können das Bronze-Paket erweitern, indem Sie:

- Hinzufügen weiterer Geräte
- Silver hinzufügen
- Gold hinzufügen
- Platinum hinzufügen

Diese Zusatzoptionen erweitern Ihre mobile Lösung über eine Basis-Gerätekonfiguration hinaus.

Upgrade anfordern

Verfahren

1. Wählen Sie den Menüpunkt **Upgrade-Optionen** im Dropdown-Menü „Administration“.
2. Klicken Sie auf **Upgrade anfordern / Geräte hinzufügen** (oben rechts).
3. Wählen Sie die Einheiten aus, die Sie hinzufügen möchten, und geben Sie Ihre Telefonnummer ein.

Ein Mitarbeiter wird sich innerhalb von 24 Stunden mit ausführlicheren Informationen bei Ihnen melden.

Upgrade von einem früheren Release

Beim Upgrade von einem früheren Release werden die Einstellungen auf der Seite **Device Enrollment Profil bearbeiten** nicht übernommen. Notieren Sie Ihre Optionseinstellungen, bevor Sie das Upgrade durchführen.

- Wenn die Option **Anmeldung bei AppleID und iCloud überspringen** aktiviert ist, bevor Sie mit dem Upgrade beginnen, wird nach dem Upgrade die Option **Apple Pay Setup überspringen** aktiviert.
- Wenn die Option **Passcodeeingabe überspringen** vor dem Upgrade aktiviert ist, werden nach dem Upgrade die Optionen **Touch ID überspringen** und **Apple Pay Setup überspringen** aktiviert.

Verfahren

1. Gehen Sie nach Abschluss des Upgrades auf die Seite **Device Enrollment Profil bearbeiten**, um das Device Enrollment Profil zu bearbeiten und die gewünschten Einstellungen wiederherzustellen.
2. Klicken Sie auf **Speichern**.

Nach einem Upgrade sind mehrere Konfigurationseinstellungen verändert.

- Die Werbeoptionen sind auf **Off** gesetzt.
  Die Installationseinstellungen sind auf **Nein** gesetzt.

Die Option **Nicht im App-Katalog anzeigen** ist nicht länger ausgewählt.

Die Option **Installation auf Android Samsung Knox im Hintergrund** ist auf „False“ gesetzt.

Die iOS-Verwaltungs-Flags sind wie folgt gesetzt:

- Datensicherung in der iCloud.
- Bei Deregistrierung entfernen.

Diese Flageinstellungen für die iOS-Verwaltung können für jede App einzeln ausgewählt werden.

App-Einstellungen:

- App-Einstellungen werden jetzt als "Konfigurationen" bezeichnet.
- Alle anderen App-Einstellungen bleiben auch nach dem Upgrade unverändert.

Weitere Informationen finden Sie unter **Pakete**.

14. Gerätelizenzen

Ivanti Neurons for MDM -Lizenzen auf Gerätebasis definieren die Anzahl der registrierbaren Geräte, die Größe des Inhalts, der zur Verteilung an Geräte konfiguriert werden kann, und welche Funktionen verfügbar sind. Wenn Sie die maximale Anzahl an Geräten erreicht haben, wird auf der Administrationsseite ein rotes Dreieck angezeigt. Wenn Sie die maximale Menge an Inhalten erreicht haben, hindert Sie der Dienst daran, mehr Inhalt hinzuzufügen und zeigt eine Nachricht an, die angibt, dass Sie die Grenze erreicht haben.

14.1. Zeitweilige Sperre eines Mandanten

Der Zugriff auf einen Mandanten mit einer Test- oder Produktionslizenz kann durch die Cloud vorübergehend gesperrt werden. Eine Testlizenz kann gesperrt werden, wenn der Testzeitraum abgelaufen ist oder der zulässige Nutzungsumfang überschritten wurde. Eine Produktionslizenz kann vorübergehend gesperrt werden, wenn der Abo-Zeitraum abgelaufen ist oder der zulässige Nutzungsumfang überschritten wurde. Die Cloud stellt einen vorübergehend gesperrten Mandanten wieder her, wenn die Lizenz verlängert wurde oder nach Überschreitung der Lizenzzahl weitere Lizenzen erworben wurden.

Bei zeitweiliger Sperrung eines Mandanten:

- funktionieren bereits registrierte Geräte normal weiter;
- können Administratoren sich nicht im Administrator-Portal anmelden;
- können keine neuen Geräte registriert werden;
- wird der API-Zugriff auf den Mandanten gesperrt.
- können Endbenutzer weiter auf das Selbstbedienungsportal zugreifen.

Maßnahmen bei einer zeitweiligen Sperrung des Mandanten und Fehlermeldungen

Maßnahme bei zeitweiliger Sperrung	Fehler	Angezeigte Fehlermeldung	Standort
Der Zugriff auf die API zur Integration von Endkunden ist gesperrt.	Der API-Aufruf schlägt fehl.	Zugriff verweigert Ihre Testlizenz ist abgelaufen. Bitte verlängern Sie Ihre Lizenz, um den API-Zugriff wieder zu aktivieren. Wenden Sie sich wegen Details an Ihren Systemadministrator.	API-Fehler 401.
Die Registrierung neuer Geräte wurde gesperrt.	Auf dem Registrierungsbildschirm wird eine Fehlermeldung angezeigt.	Ihr Gerät kann nicht registriert werden. Die Lizenz für Ihr System ist abgelaufen. Wenden Sie sich wegen Details an Ihren Systemadministrator. Bisher angemeldete Geräte funktionieren weiter normal.	Nach der Passwort-Verifizierung
Der Administrator kann sich nicht mehr im Administratorportal anmelden.	Auf dem Anmeldebildschirm wird eine Fehlermeldung angezeigt.	Anmeldung nicht möglich. Ihre Lizenz ist abgelaufen. Bitte verlängern Sie Ihre Lizenz, um wieder Zugang zum Administratorportal zu erhalten und neue Geräte zu registrieren. Geräte, die bereits zuvor registriert waren, funktionieren weiter normal. Wenden Sie sich an Ihren Vertriebsmitarbeiter, um Ihre Lizenzen zu verlängern. Beachten Sie, dass das Administratorpasswort nach einem Jahr (365 Tagen) verfällt.	Nach der Passwort-Verifizierung

15. Öffnen eines Support-Tickets

Besuchen Sie das **Ivanti Support-Portal**, um ein Support-Ticket zu öffnen.

16. Attribute von Drittanbietern

Ivanti Neurons for MDM beinhaltet Komponenten, die von Drittanbietern entwickelt wurden. Die Liste können Sie **hier** aufrufen.

17. Apps@Work

Ab Cloud Release 83 können Sie von der Go-Anwendung zum nativen Apps@Work wechseln. Für neu erstellte Mandanten wird die Apps@work Webclip-Konfiguration nicht standardmäßig für iOS-Geräte verteilt, die über iReg oder den Client installiert wurden. Der Administrator muss die Webclip-Konfiguration an die über iReg oder den Client registrierten Geräte manuell verteilen. Beachten Sie Folgendes:

Ivanti Neurons for MDM **Administrationsportal**:

- Standardmäßig erhalten nur neue Mandanten den App-Katalog für die native Clientkonfiguration, die an iOS-Geräte verteilt wurde.
- Für vorhandene Mandanten wird die native Anwendung Apps@Work nicht verteilt.
- Der Administrator muss den App-Katalog für die Konfiguration des nativen Clients via Push auf die Geräte übertragen, damit Apps@Work als native Appstore-Erfahrung verfügbar ist.

Client:

- Die Go-Anwendung zeigt jetzt eine Registerkarte für Apps@Work an.
- Die Konfiguration "App-Katalog für nativen Client" verfügt über die App-Katalog-Identität für das Native Client-Zertifikat und das App Station-Identitätszertifikat. Ivanti Neurons for MDM sendet Zertifikate mit dem App-Katalog via Push für die native Clientkonfiguration.

Apps@Work-Funktionen

Die Registerkarte "Apps@Work" bietet folgende Funktionen:

- **Aufrufen der Registerkarte "Apps@Work" über die Go-Anwendung**
- **Suchen**
- **Installieren einer App – Schaltfläche "Status"**
- **Empfohlene Anwendungen und Banner**
- **Update-Benachrichtigung für Anwendung**
- **Update-Benachrichtigung für Anwendung**

Aufrufen der Registerkarte "Apps@Work" über die Go-Anwendung

- Eine neue Registerkarte wird zu Go app for Apps@Work hinzugefügt.
- Zwei Standardregisterkarten sind in Apps@Work verfügbar: "Alle Apps" und "Kategorien".
- Auf der Registerkarte "Alle Apps" werden alle Apps in alphabetischer Reihenfolge aufgeführt.
- Auf der Registerkarte "Kategorien" werden nur die Kategorien angezeigt, die Anwendungen enthalten.
- Jede Kategorie zeigt die Anzahl der Anwendungen an, die in ihr enthalten sind.
- "Meine Apps" unter "Kategorien" ist eine Position, die alle installierten Anwendungen enthält. "Meine Apps" ist stets die erste Kategorie, alle anderen Kategorien sind alphabetisch darunter aufgeführt.
- Wenn keine Anwendungen installiert sind, wird in der Liste "Meine Apps" der Wert "Keine" angezeigt.
- Wenn Sie auf eine Kategorie klicken, werden alle in der Kategorie enthaltenen Anwendungen mit einer Installationsoption aufgelistet. Mit dem Assistenten können Sie jede Anwendung einzeln installieren, oder aber Sie klicken auf "Alle installieren", um

alle Anwendungen der Kategorie zu installieren. Sie werden aufgefordert, die Installation jeder einzelnen Anwendung zu erlauben.

Suchen

- Tippen Sie auf das Suchsymbol (Lupe), um nach Folgendem zu suchen:
  - Neue Releases – Eine Liste neu veröffentlichter Apps wird angezeigt, wenn kein Text in die Suchleiste eingegeben wurde.
  - Geben Sie beliebigen Text in das Suchfeld ein, um dynamisch Vorschläge übereinstimmender Anwendungen zu erhalten.
  - Die Anzahl der Suchergebnisse wird als Unterüberschrift angezeigt.
  - Durch Tippen auf die Schaltfläche "Installieren" können Sie eine Anwendung installieren, ohne auf die Seite mit den Details wechseln zu müssen.

Installieren einer App – Schaltfläche "Status"

- Da der Server für die App-Installation die Anforderung verarbeiten und die App via Push an das Gerät übertragen muss, zeigt die Installationsschaltfläche den Fortschritt nicht in Echtzeit an.
- Der Status der Schaltfläche "Installieren" wechselt von "Installieren" zu "Angefordert" zu "Installiert".
- Eine Alarmmeldung wird erstmals angezeigt, wenn eine Installation angefordert wurde.
- Der Alarm wird auch dann angezeigt, wenn Sie auf die Schaltfläche "Angefordert" tippen.
- Der Status "Installiert" ist keine Schaltfläche.

Empfohlene Anwendungen und Banner

- Die Registerkarte "Empfohlen" wird je nach Administratorkonfiguration angezeigt.
- Die Registerkarte "Empfohlen" ist die Standardlandinpage, wenn keine Updates verfügbar sind.
- Der empfohlene App-Banner zeigt eine Anwendung an.
- Unter "Empfohlene App" ist eine Liste aller empfohlenen Apps enthalten.

Update-Benachrichtigung für Anwendung

- Go sendet eine Benachrichtigung, sobald Updates für Anwendungen verfügbar sind. Die Benachrichtigung enthält jedoch nicht die Namen der betreffenden Anwendungen.
- Wenn Sie auf die Benachrichtigung hinsichtlich der Updates zu Anwendungen tippen, werden Sie zur Seite "Alle Apps" in Apps@Work weitergeleitet.
- In der Go-Anwendung zeigt das Symbol für die Registerkarte "Apps@Work" die Anzahl der Anwendungen an, für die Updates ausstehen.
- Auf der Registerkarte "Apps@Work" wird unter der Registerkarte "Alle Apps" im Unterabschnitt "Updates verfügbar" die Anzahl der Anwendungen angezeigt, für die ein Update verfügbar ist.
- Für jede Anwendung, die aktualisiert werden muss, wird ein Symbol mit einem roten Punkt angezeigt.

Einstellungen – Meine Geräte

- Die Registerkarte "Meine Geräte" ist jetzt bei den Einstellungen verfügbar.
- Wenn Sie auf die Benachrichtigung hinsichtlich der Updates zu Anwendungen tippen, werden Sie zur Seite "Alle Apps" in Apps@Work weitergeleitet.

- In der Go-Anwendung zeigt das Symbol für die Registerkarte "Apps@Work" die Anzahl der Anwendungen an, für die Updates ausstehen.
- Auf der Registerkarte "Apps@Work" wird unter der Registerkarte "Alle Apps" im Unterabschnitt "Updates verfügbar" die Anzahl der Anwendungen angezeigt, für die ein Update verfügbar ist.
- Für jede Anwendung, die aktualisiert werden muss, wird ein Symbol mit einem roten Punkt angezeigt.

18. Aktivieren der Kerberos-Authentifizierung zwischen Ivanti Neurons for MDM und SCEP-Server

Sie können die Kerberos-Authentifizierung für die Kommunikation zwischen Ivanti Neurons for MDM und SCEP verwenden. In den folgenden Abschnitten wird erläutert, wie Sie die Kerberos-Authentifizierung auf SCEP-Servern und Ivanti Neurons for MDM aktivieren.

> Diese Funktion ist mit der Version Ivanti Neurons for MDM Connector 93 verfügbar.

Schritte vor der Konfiguration

1. Prüfen Sie, welches Dienstkonto auf dem SCEP-Server für den SCEP-Dienst verwendet wird.
2. Stellen Sie auf dem SCEP-Server sicher, dass das Dienstkonto der lokalen Gruppe "IIS_USRS" angehört.
3. Stellen Sie in der bereitzustellenden CA-Serverzertifikatsvorlage sicher, dass das Dienstkonto über Registrierungsberechtigungen verfügt.

Konfigurieren von Windows-Servern

1. Führen Sie folgenden Befehl auf einem Domänencontroller aus:
   setspn -s http/<SCEP-SERVER-FQDN> <domain>\<service account>
2. Klicken Sie bei **Active Directory-Benutzer und -Computer** auf die Registerkarte **Delegierung** des Dienstkontos.
   1. Wählen Sie bei **Diesem Benutzer nur für die Delegierung an bestimmte Dienste vertrauen** die Option **Nur Kerberos verwenden** aus.
   2. Klicken Sie auf **Hinzufügen** und fügen Sie den Namen des SCEP-Servers hinzu.
   3. Wählen Sie den HTTP-Dienst aus.
   4. Klicken Sie auf **OK**.
3. Gehen Sie auf dem IIS-Server folgendermaßen vor, um sicherzustellen, dass zum Entschlüsseln von Kerberos-Tickets die Anmeldeinformationen für den Anwendungspool verwendet werden:
   1. Stellen Sie sicher, dass der SCEP-Anwendungspool unter dem vorhin von Ihnen überprüften Dienstkonto ausgeführt wird.
   2. Wählen Sie zum Aktivieren von useAppPoolCredentials auf der Microsoft SCEP-Admin (mscep_admin)- oder der Microsoft SCEP (mscep)-Webseite die Option **Konfigurationseditor > System.webServer > Sicherheit > Authentifizierung > Windows-Authentifizierung** aus und setzen Sie den Wert auf useAppPoolCredentials=True.
4. Deaktivieren Sie **Anonyme Authentifizierung** auf der Microsoft SCEP-Admin-Webseite (mscep_admin), indem Sie **Authentifizierung > Anonyme Authentifizierung** auswählen und auf **Deaktivieren** klicken.
5. Deaktivieren Sie die Kernel-Modus-Authentifizierung bei den erweiterten Einstellungen der Windows-Authentifizierung.

> Verwenden Sie als erste Option im Authentifizierungsdienst die Option **Aushandeln**.

6. Deaktivieren Sie die Kernel-Modus-Authentifizierung auf der Webseite mit den erweiterten Einstellungen der Windows-Authentifizierung.

7. Starten Sie den IIS-Dienst neu.

Konfigurieren von Kerberos

In diesem Abschnitt wird beschrieben, wie Sie Kerberos auf dem Ivanti Neurons for MDM-Server konfigurieren.

Konfigurieren der Kerberos-Einstellungen in Ivanti Neurons for MDM

Navigieren Sie zu **Admin > Infrastruktur > Kerberos** und geben Sie die folgenden Einstellungen wie in der Tabelle angegeben ein:

UI-Abschnitt	Auswahl
Kerberos-Bereich von Active Directory	IVANTI.COM
Entsprechender Key Distribution Center (KDC)-Server	kdc.ivanti.com
Anmeldeinformationen des Dienstbenutzers Domänen für die ausgehende Kommunikation mit Microsoft AD-Zertifikatdiensten (keine Unterscheidung zwischen Groß- und Kleinschreibung bei Hostnamen; müssen mit .ivanti.com oder .IVANTI.COM enden) SCEP- oder NDES-Server: Sie können auch Hostnamen wie ndes.ivanti.com oder scep.ivanti.com verwenden.	user@realm Beispiel: serviceuser@IVANTI.COM

Aktivieren der Kerberos-Authentifizierung in der Microsoft SCEP-Zertifikatregistrierungs-Konfiguration für eine vorhandene Zertifizierungsstelle

Führen Sie folgende Schritte aus, um die Kerberos-Authentifizierung für eine vorhandene Zertifizierungsstelle zu aktivieren:

1. Wechseln Sie in Ivanti Neurons for MDM zu **Admin > Infrastruktur > Zertifikatsverwaltung**.
2. Wählen Sie als Typ der Zertifizierungsstelle **Extern** aus.

> Diese externen Zertifizierungsstellentypen sollten mit Microsoft bezeichnet sein.

3. Wählen Sie im Dropdownfeld **Aktionen** die Option **Bearbeiten** aus.
4. Markieren Sie im Fenster **Externe Zertifizierungsstelle bearbeiten** das Kontrollkästchen **Kerberos-Authentifizierung bevorzugen** aus, um die Kerberos-Authentifizierung zu aktivieren.

Aktivieren der Kerberos-Authentifizierung in der Microsoft SCEP-Zertifikatregistrierungs-Konfiguration für eine neue Zertifizierungsstelle

Führen Sie folgende Schritte aus, um die Kerberos-Authentifizierung für eine neue Zertifizierungsstelle zu aktivieren:

1. Wechseln Sie in Ivanti Neurons for MDM zu **Admin > Infrastruktur > Zertifikatsverwaltung**.
2. Wählen Sie die Option **+Hinzufügen** aus.
3. Wählen Sie im Fenster **Zertifizierungsstelle hinzufügen** die Option **Mit einer On-Premise-SCEP-Zertifizierungsstelle verbinden** aus.

4. Klicken Sie auf Weiter.
5. Führen Sie im Fenster **Externe Zertifizierungsstelle hinzufügen** die folgenden Schritte aus:
    1. Wählen Sie die Option **Microsoft** in der Dropdownliste **Zertifizierungsstellentyp** aus.
    2. Markieren Sie das Kontrollkästchen **Kerberos-Authentifizierung bevorzugen** aus, um die Kerberos-Authentifizierung zu aktivieren.
    3. Füllen Sie alle Pflichtfelder aus.
    4. Klicken Sie auf **Fertig**.

19. Ivanti Neurons for MDM 127 – Administratorhandbuch

September 2026

Als moderner Ansatz für mobile Sicherheit bietet die Cloud Unified Endpoint Management (UEM)-Lösungen in einer hoch skalierbaren, sicheren und einfach zu aktualisierenden Infrastruktur, die Millionen von Geräten auf der ganzen Welt unterstützt.

{{Wenn Ihre Sprache nicht verfügbar ist}}

Zusammenfassung der neuen Funktionen

Als PDF anzeigen

Videos

20. Welcome

21. Welcome CSH

22. Windows-Updatemanagement

Als Administrator können Sie die von Windows-Geräten gemeldeten Updates mithilfe der Windows-Updateverwaltung anzeigen und genehmigen. Mit dieser Funktion können Sie verhindern, dass ungetestete oder unnötige Updates auf den Geräten installiert werden.

Um die Funktion zur Update-Verwaltung zu nutzen, müssen die Geräte für die Software-Update-Konfiguration mit der Option Update-Genehmigung anfordern aktiviert sein.Nur durch Übernahme dieser Konfiguration auf die Geräte melden die Geräte für die Installation verfügbare Updates und warten auf die Genehmigung.

Aktualisierungen verwalten

1. Gehen Sie zum Abschnitt Administrator > Windows-Updates. Die folgenden Details der Updates werden auf der Seite angezeigt. **Erstellungsdatum**: Das Datum, an dem das Update erstellt wurde.**Titel**: Beschreibt die Art des Updates, enthält die Artikelnummer aus der Knowledge Base.

> Wenn Sie auf das Update klicken, wird die Beschreibung angezeigt.

Klassifizierung: Ordnet den Updatetyp einer der folgenden Kategorien zu:

- Kritische Aktualisierungen
- Definitionsupdates
- Treiberupdates
- Sicherheitsupdates
- Updates
- Upgrade
- Updaterollups

Verteilung: Die Verteilung für das Update. Beispielsweise wird die Option **Alle** angezeigt, wenn das Update auf alle Geräte verteilt wird.

> Wenn das Update auf eine spezifische Anzahl von Gruppen verteilt wird, wird die Anzahl der Verteilungen angezeigt. Es wird beispielsweise Ziffer 3 angezeigt, wenn die Verteilung nur die Gruppen betrifft.

2. Zusätzlich können Sie anzeigen, ob eine Aktualisierung an die erforderlichen Geräte verteilt wurde oder nicht. Die folgenden Spalten verfügen über Zahlen, die angeben, wie viele Geräte in den verschiedenen Aktualisierungskategorien enthalten sind:
   - Geeignete Geräte
   - Installierte Geräte
   - Fehlgeschlagene Geräte
   - Geräte mit ausstehendem Neustart

Wenn Sie auf eine Zahl klicken, gelangen Sie zur gefilterten Ansicht der Geräteseite. Dort können Sie den Aktualisierungsstatus überprüfen und ggf. erforderliche Aktionen durchführen.
Prüfen Sie die Updates und klicken Sie auf das Update, das Sie auf die Geräte verteilen möchten, indem Sie das Kontrollkästchen für das Update aktivieren.

3. Klicken Sie unter **Aktionen** auf **Verteilung definieren**.

4. Wählen Sie in dem Fenster **Windows-Update verteilen** eine der folgenden Verteilungsoptionen:
   Alle Geräte: Verteilt die Aktualisierungen auf alle Geräte.
   Keine Geräte: Verschiebt die Verteilung der Updates auf die Geräte.**Anpassbar**: Verteilt die Updates für die definierten Gerätegruppen.
5. Klicken Sie auf **Speichern**.

Updates suchen und filtern

Sie können Updates nach folgenden Kriterien suchen und filtern:

- Artikel-ID der Knowledge Base
- Konfigurierte Verteilung

Nach Artikel-ID der Knowledge Base filtern:

1. Geben Sie auf der Seite **Windows-Updateverwaltung** die Wissensdatenbank-ID in das Schnellsuche-Feld ein (nur die Nummer bei "Suchen").
   Beispiel: Für KB4056892, geben Sie 4056892 ein. Das Update, das zu den Suchkriterien passt, wird auf der Seite angezeigt.

> Sie können außerdem nach weiteren Informationen zu dem Update suchen, indem Sie auf den Link **Support** und **Weitere Informationen** klicken. Der Link **Support** verlinkt zur Microsoft-Webseite mit den entsprechenden Produkt-Support-Informationen für das Update, der Link **Weitere Informationen** verlinkt zu der Microsoft-Webseite mit weiteren Informationen zum Update, beispielsweise zu dem Artikel in der Knowledge Base.

Nach konfigurierter Verteilung filtern:

Wählen Sie auf der Seite **Windows-Updateverwaltung** eine der folgenden Filteroptionen basierend auf der konfigurierten Verteilung aus:

- **Alle**: Zeigt alle Aktualisierungen an.
- **Konfiguriert**: Zeigt die Liste der Aktualisierungen an, die auf Geräte verteilt werden.
- **Nicht konfiguriert**: Zeigt die Liste der Updates an, für die die Verteilung nicht definiert ist.

> Konfigurierte und nicht-konfigurierte Filter richten sich nach der durchgeführten Verteilung. Die Verteilung kann auch Keine sein.

Aktualisierungen für ein Gerät anzeigen

Detaillierte Update-Informationen speziell für ein Gerät anzeigen:

1. Gehen Sie zu **Geräte > Geräte**.
2. Klicken Sie auf einen Gerätenamen, um die Seite mit den Details aufzurufen.
3. Gehen Sie zur Registerkarte **Aktualisierungen**. Angezeigt werden die Updates für das Gerät, die noch ausstehen (Update vom Administrator genehmigt, aber noch nicht auf dem Gerät als installiert gemeldet), fehlgeschlagen und installiert sind.

> Benachrichtigungen über neue Windows-Updates sehen Sie außerdem auf der Seite „Benachrichtigungen“ im Dashboard. Die Benachrichtigung erhält das Erstellungsdatum der Benachrichtigung, die Anzahl der verfügbaren Benachrichtigungen und den Zweck der Benachrichtigung. Die Benachrichtigung über das Windows-Update ist außerdem in der oberen rechten Ecke des Administrationsportals sichtbar.