ivanti

NMDM Admin Guide ZHCN

ivanti

CONTENTS

1. 关于 Ivanti Neurons for MDM 9
2. 新增功能摘要 10
3. 视频 13
4. 入门指南 16
   - 4.1. 配置 macOS 设备 23
   - 4.2. 配置和使用注册确认电子邮件 26
   - 4.3. 配置和使用策略合规通知电子邮件 27
   - 4.4. 按需功能 28
   - 4.5. 准备 Android Enterprise 设备支持 29
5. 仪表板 30
   - 5.1. 使用小组件 31
   - 5.2. 应用见解 36
   - 5.3. 使用计划的报告 40
   - 5.4. 使用自定义报告 46
6. 用户 53
   - 6.1. 添加用户 54
   - 6.2. 用户组 58
   - 6.3. 用户设置 62
   - 6.4. 用户加印品牌 71
   - 6.5. 使用 Apple 商务管理进行用户注册 72
   - 6.6. 用户许可证 80
   - 6.7. 管理用户 81
     - 6.7.1. 正在为 Cisco ISE 操作添加 API 用户 82
     - 6.7.2. 为用户分配角色 83
     - 6.7.3. 用户角色 85
     - 6.7.4. 查找并过滤用户 87
     - 6.7.5. 将用户分配到用户组 90
     - 6.7.6. 邀请用户 91
     - 6.7.7. 启用和禁用用户 92
     - 6.7.8. 管理多个管理员登录 94
     - 6.7.9. 更改密码 95
     - 6.7.10. 发送消息 97
     - 6.7.11. 将用户从用户组中移除 99
     - 6.7.12. 删除用户 100
     - 6.7.13. 导出用户 101
     - 6.7.14. 将自定义属性分配到用户 102
     - 6.7.15. 将自定义属性从用户中删除 103
     - 6.7.16. 更改用户区域设置 104
     - 6.7.17. 编辑用户名 105
     - 6.7.18. 选择退出位置数据收集 106
     - 6.7.19. 超时信息 107
     - 6.7.20. 选择退出系统使用情况分析 108
     - 6.7.21. 通过生成的 PIN 进行设备注册 109
7. 设备 110
   - 7.1. 开始使用设备 111
   - 7.2. 设备组 124
   - 7.3. 未托管设备 130
   - 7.4. 应用库存 131
   - 7.5. 管理设备 134
     - 7.5.1. 部署 Apple 设备 136
     - 7.5.2. 部署 Windows 设备 144
     - 7.5.3. 在 macOS 设备上设置 Apple 远程桌面 147
     - 7.5.4. 设备注册（iOS、macOS 和 Android） 148
     - 7.5.5. 设备注册（Windows 10+ PC 和 Microsoft Hololens 2） 151
     - 7.5.6. 本地管理员密码解决方案 (LAPS) 154
     - 7.5.7. 使用 PIN 配置软件包注册 156
     - 7.5.8. 使用针对 Windows 设备的批量注册 159
       - 7.5.8.1. Ivanti 批量注册 160
     - 7.5.9. 更改通行码设置 162

7.5.10. 更改设备名称 163
7.5.11. 查找并筛选设备 164
7.5.12. 使用设备所有者 166
7.5.13. 带有工作配置文件的托管设备 173
7.5.14. 使用 Android 的批量注册 174
7.5.15. 使用 CSV 文件上传进行批量注册 176
7.5.16. Device_to_User_BulkEnrollment 178
7.5.17. 使用 Samsung Knox 移动注册 179
7.5.18. 注册 Oculus 设备 180
7.5.19. 启用设备上的 Bluetooth 功能 182
7.5.20. 计划 iOS 更新 183
7.5.21. 重新安装 iOS 系统应用 184
7.5.22. 将设备分配到新用户 185
7.5.23. 重新分配 Android 设备 186
7.5.24. 强制设备进行签入 187
7.5.25. 定位设备 188
7.5.26. 锁定设备 189
7.5.27. 管理遗失模式下的 Apple 设备 190
7.5.28. 管理遗失模式下的 Android 设备 192
7.5.29. 请求调试日志 194
7.5.30. Apple_Enhanced_Logging 195
7.5.31. 停用设备 196
7.5.32. 放弃设备的所有权 197
7.5.33. 擦除设备 198
7.5.34. 删除设备 199
7.5.35. 解锁设备 200
7.5.36. 重新启动或关闭设备 202
7.5.37. 清除限制密码（仅 iOS） 204
7.5.38. 删除设备的 Sentry 关联 205
7.5.39. 将自定义属性分配到设备 206
7.5.40. 将自定义属性从设备中删除 207
7.5.41. 同步和获取应用反馈 208
7.5.42. 设置固件密码 209
7.5.43. 重新发布新个人恢复密钥 210
7.5.44. 设置或更改恢复锁定 211
7.5.45. Apple 访问管理 212
7.5.46. 组策略注册 213
8. 应用 214
8.1. 应用目录 215
8.2. 声明式设备管理 (DDM) 应用程序管理 231
8.2.1. DDM 应用程序管理设置 233
8.3. Apps@Work（iOS、Android、Windows 和 macOS） 236
8.4. iOS Apps@Work AppStore 功能 239
8.5. iOS Go 高级功能 241
8.6. 查看应用详细信息 246
8.7. 应用配置 249
8.8. 将自定义属性分配给应用程序 264
8.9. Android 的托管配置 265
8.10. 管理 Google Play 应用 269
8.11. 从 App Catalog 中删除应用 270
8.12. 升级内部应用 271
8.13. 查找 Android 应用程序的软件包名称 272
8.14. 类别 273
8.15. 分配过滤器 274
8.16. 排除或分发应用程序 277
8.17. 评论 278
8.18. AppleApp 和图书 280
8.19. 目录设置 288
8.20. 部署应用依赖性 291
8.21. 使用 Android Enterprise 部署 Divide Productivity 294
8.22. 设置配置器应用程序 296
8.23. 管理 Windows 应用程序 298

8.24. Ivanti Bridge 301
9. 内容 306
9.1. 管理内容 307
9.2. 类别 309
10. 配置 310
10.1. 使用配置 311
10.2. 创建用户自助服务门户配置 322
10.3. 自定义配置 323
10.4. 使用自定义配置向设备推送 SyncML 325
10.5. 主屏幕布局配置 326
10.6. 应用控制配置：控制每个设备上安装哪些应用 328
10.7. 应用通知配置 330
10.8. 导出配置 332
10.9. 确定配置的优先级 333
10.10. 管理配置 334
10.10.1. 配置类型 335
10.10.2. 变量 346
10.10.3. AppConnect 配置 351
10.10.3.1. AppConnect 概述 352
10.10.3.2. AppConnect 通行码 353
10.10.4. 安全配置 354
10.10.4.1. Android Enterprise 356
10.10.4.2. Apple 密钥认证 357
10.10.4.3. 应用程序隐私默认值 358
10.10.4.4. 编辑 Android Enterprise 默认配置 360
10.10.4.5. 设置 Android Enterprise 361
10.10.4.6. Android Enterprise：工作托管设备非 GMS 模式 (AOSP) 367
10.10.4.7. Android 工作认证 (Work Challenge) 368
10.10.4.8. 证书配置 373
10.10.4.9. 证书透明度 375
10.10.4.10. 证书吊销检查配置 376
10.10.4.11. 创建自主单应用程序模式配置 377
10.10.4.12. 创建 DNS 代理配置 378
10.10.4.13. 设备日志记录配置 379
10.10.4.14. 磁盘管理配置 381
10.10.4.15. Android 加密 382
10.10.4.16. 加密的 DNS 383
10.10.4.17. 外部智能设置 386
10.10.4.18. 威胁防御 387
10.10.4.19. FileVault 2 388
10.10.4.20. FileVault 恢复密钥 389
10.10.4.21. FileVault 选项配置 390
10.10.4.22. 身份证书 391
10.10.4.23. Apple 激活锁定配置 396
10.10.4.24. iOS 自定义配置 399
10.10.4.25. 智能设置 400
10.10.4.26. iOS 限制 403
10.10.4.27. 会议室显示 417
10.10.4.28. 键盘设置 418
10.10.4.29. 锁定和自助服务终端：Android 设备管理模式 420
10.10.4.30. 设置 Android 的自助服务终端模式 423
10.10.4.31. 设置 Android 共享设备自助服务终端 425
10.10.4.32. 锁定和自助服务终端：Android Enterprise 426
10.10.4.33. 锁定和自助服务终端：Samsung Knox Standard 445
10.10.4.34. 本地管理员密码解决方案配置 449
10.10.4.35. macOS 防火墙 450
10.10.4.36. macOS 限制 451
10.10.4.37. macOS AppStore 限制 457
10.10.4.38. macOS 磁盘刻录限制 458
10.10.4.39. 允许的媒体控制（已弃用） 459
10.10.4.40. macOS Finder 设置 462
10.10.4.41. macOS 内核扩展策略 463

10.10.4.42. Mobile@Work for macOS ... 464
10.10.4.43. macOS 软件更新规则配置 ... 469
10.10.4.44. 证书首选项 ... 470
10.10.4.45. Active Directory (macOS) ... 471
10.10.4.46. 身份首选项 ... 474
10.10.4.47. Office 365 自动帐户创建 (macOS) ... 475
10.10.4.48. 认证 ... 477
10.10.4.49. Apple 应用目录 ... 478
10.10.4.50. 托管域 ... 479
10.10.4.51. 通行码配置 ... 480
10.10.4.52. 隐私首选项 (macOS) ... 483
10.10.4.53. 隐私配置 ... 485
10.10.4.54. 客户端隐私声明信息 ... 488
10.10.4.55. Ivanti Go Client 设置 ... 489
10.10.4.56. Siri 设置 ... 491
10.10.4.57. 服务配置文件配置 ... 492
10.10.4.58. 软件更新 ... 493
10.10.4.59. 软件更新设置配置 ... 500
10.10.4.60. 安全首选项配置 ... 503
10.10.4.61. 时间服务器 ... 504
10.10.4.62. Web 内容筛选 ... 505
10.10.4.63. Windows 防火墙 ... 508
10.10.4.64. Windows 信息保护 ... 511
10.10.4.65. Windows 限制 ... 515
10.10.4.66. Windows 桌面限制 ... 520
10.10.4.67. Windows 10 的桌面设置 ... 522
10.10.4.68. Windows Hello for Business 配置 ... 524
10.10.4.69. Windows AI 管理配置 ... 525
10.10.4.70. Play Integrity（原 SafetyNet Attestation） ... 527
10.10.4.71. 高级 Android 密码和锁屏 ... 528
10.10.4.72. Microsoft Defender for Endpoint ... 529
10.10.4.73. 基于证书的身份验证 ... 530
10.10.5. 用户资源配置 ... 531
10.10.5.1. CalDAV 配置 ... 532
10.10.5.2. CardDAV 配置 ... 533
10.10.5.3. Google 配置 ... 534
10.10.5.4. 电子邮件配置 ... 535
10.10.5.5. Exchange 配置 ... 537
10.10.5.6. 字体配置 ... 541
10.10.5.7. 订阅日历配置 ... 542
10.10.5.8. 创建 Web 剪辑配置 ... 543
10.10.5.9. Office 365 安装 ... 545
10.10.5.10. Windows GPO 设置 ... 547
10.10.5.11. BitLocker 加密配置 ... 549
10.10.6. 企业网络访问配置 ... 553
10.10.6.1. AirPlay 配置 ... 554
10.10.6.2. AirPrint 配置 ... 555
10.10.6.3. Always-on VPN 配置 ... 556
10.10.6.4. 默认应用程序运行时权限 ... 559
10.10.6.5. 教育 ... 561
10.10.6.6. 全局代理配置 ... 562
10.10.6.7. 全局代理配置 (Android) ... 563
10.10.6.8. LDAP 配置 ... 564
10.10.6.9. macOS 服务器配置 ... 565
10.10.6.10. Tunnel ... 566
10.10.6.11. 设置 AppTunnel ... 567
10.10.6.12. Per-App VPN 配置 ... 572
10.10.6.13. 单点登录配置 ... 580
10.10.6.14. 网络中继配置 ... 587
10.10.6.15. iOS 的多用户安全登录 ... 589
10.10.6.16. Android APN 设置配置 ... 591
10.10.6.17. VPN 配置 ... 595

10.10.6.18. 按需 VPN ... 607
10.10.6.19. Wi-Fi 配置 ... 614
10.10.7. 手机网络配置 ... 622
10.10.7.1. APN 配置 ... 623
10.10.7.2. 移动电话 ... 624
10.10.7.3. 蜂窝专用网络配置 ... 627
10.10.7.4. iOS 电信预置配置 ... 628
10.10.7.5. 增强 5G 网络切片配置 ... 629
10.10.7.6. eSIM 配置 ... 631
10.10.8. 其他配置 ... 633
10.10.8.1. 关联域配置 ... 635
10.10.8.2. Android 文件传输配置 ... 636
10.10.8.3. Apple TV 配置 ... 639
10.10.8.4. AirPlay 镜像 ... 640
10.10.8.5. 浏览器设置 ... 642
10.10.8.6. 为 iOS 配置单一应用模式 ... 645
10.10.8.7. 配置 iOS MDM 配置文件 ... 647
10.10.8.8. 配置 macOS MDM 配置文件 ... 648
10.10.8.9. 内容缓存 ... 649
10.10.8.10. 创建 Android 快捷方式 ... 652
10.10.8.11. 创建辅助功能设置配置 ... 653
10.10.8.12. 创建屏幕保护程序配置 ... 656
10.10.8.13. 配置用户的屏幕保护程序 ... 657
10.10.8.14. 设备名称设置 ... 658
10.10.8.15. 设备壁纸配置 ... 659
10.10.8.16. EMA 服务器集成配置 ... 662
10.10.8.17. 节能配置 ... 663
10.10.8.18. 以太网配置 (macOS) ... 669
10.10.8.19. Google BeyondCorp 配置 ... 671
10.10.8.20. 锁定屏幕消息配置 ... 675
10.10.8.21. 登录窗口配置 - macOS ... 677
10.10.8.22. macOS 系统扩展配置 ... 678
10.10.8.23. 仅限 MAM ... 679
10.10.8.24. 托管的 Google Play 配置 ... 681
10.10.8.25. 迁移助手设置 ... 682
10.10.8.26. 通知配置 ... 683
10.10.8.27. 打印机设置 ... 684
10.10.8.28. 删除 Bloatware 配置 ... 686
10.10.8.29. Safari 扩展和设置配置 ... 687
10.10.8.30. Samsung 手机限制配置 ... 690
10.10.8.31. 默认浏览器配置 - iOS 和 visionOS ... 691
10.10.8.32. 屏幕共享主机设置配置 ... 692
10.10.8.33. 单应用模式配置 ... 693
10.10.8.34. 软件更新推荐节奏配置 ... 695
10.10.8.35. 开始菜单和任务栏 ... 696
10.10.8.36. 系统更新配置 ... 698
10.10.8.37. Windows 10 更新管理 ... 702
10.10.8.38. Windows 应用计划 ... 704
10.10.8.39. Windows BIOS 配置 ... 705
10.10.8.40. Windows BitLocker ... 713
10.10.8.41. Windows 自助服务终端配置 ... 714
10.10.8.42. Windows 许可证配置 ... 718
11. 策略 ... 719
11.1. 使用策略 ... 720
11.2. 自定义策略 ... 726
11.3. 监控和控制允许的应用程序 ... 746
11.4. 确定策略的优先级 ... 751
11.5. Windows 硬件策略 ... 752
12. 管理 ... 753
12.1. 系统 ... 754
12.1.1. 属性 ... 755
12.1.2. 设备清理设置 ... 760

12.1.3. GDPR 配置文件 764
12.1.4. 通知电子邮件 766
12.1.5. 角色管理 767
12.1.6. 空间 773
12.1.6.1. 空间 774
12.1.6.2. 管理空间 776
12.1.6.3. 空间示例 781
12.1.6.4. 授权设备 783
12.1.6.5. 授权应用程序 784
12.1.7. 支持管理员 785
12.1.8. 管理 > 系统使用通知 786
12.2. 基础设施 788
12.2.1. 访问 789
12.2.2. 应用程序列表 790
12.2.3. 导出审计跟踪 791
12.2.4. 证书管理 794
12.2.5. 适用于外部证书授权机构的 SCEP 配置 801
12.2.6. 派生凭据提供商 802
12.2.7. 连接器 803
12.2.8. 使用 Connector 的 httpproxy 命令 805
12.2.9. Help@Work 806
12.2.10. 基础设施身份 809
12.2.10.1. 配置标识提供者 810
12.2.10.2. 使用 SCIM 进行用户配置 814
12.2.10.2.1. Entra ID IdP 用户配置 817
12.2.10.2.2. Okta IdP 用户配置 822
12.2.11. 配置 LDAP 服务器 825
12.2.12. 卫士 833
12.3. Apple 设置 834
12.3.1. Apple Configurator 835
12.3.2. 账户驱动型注册 837
12.3.3. 设备注册 839
12.3.4. 测试版注册 852
12.3.5. 配置设置辅助 853
12.3.6. 安装 MDM 证书 854
12.3.7. 共享 iPad 设备企业版 855
12.3.8. 校园教务管理 859
12.3.9. 设置 (Apple) 862
12.4. 使用 Windows 设备工作 864
12.4.1. 配置 Windows Autopilot 配置文件 865
12.4.2. 针对 Windows Autopilot 配置文件的审计跟踪 871
12.4.3. TenantLockdown CSP 872
12.4.4. ADMX (GPO) 浏览器 873
12.4.5. 配置应用库存间隔 874
12.4.6. 硬件库 875
12.5. 使用 Microsoft Azure 设置 876
12.5.1. 使用 Microsoft Azure 877
12.5.2. Entra ID Windows 10 统一端点管理设置 880
12.5.3. 分配 Entra ID UEM 应用程序 881
12.5.4. 连接 Ivanti Neurons for MDM 与 Entra ID 用户源 882
12.5.5. Azure 租户 884
12.5.5.1. Azure Tenant Requirements 885
12.5.5.2. 将 Intune 许可证应用于设备用户 886
12.5.5.3. 将 MobileIron 添加为合规合作伙伴 887
12.5.5.4. 在 Microsoft Endpoint Manager 中创建条件访问策略 888
12.5.5.5. 将 Microsoft Azure 连接到 Ivanti Neurons for MDM 889
12.5.5.6. 创建合作伙伴设备合规性策略 890
12.5.5.7. 从 Ivanti Neurons for MDM 向 Azure 报告设备状态 892
12.5.5.8. 取消配置 Azure 租户 894
12.5.6. 管理员 > Microsoft Azure > Office 365 应用保护 895
12.6. 与 Google 应用连接 903
12.6.1. 受管 Google Play 帐户（Android Enterprise 帐户） 904

12.6.2. Android 设备注册 907
12.6.3. Android 管理 API 908
12.6.4. Google Apps API 914
12.6.5. 管理员 - Android Enterprise 915
12.7. 使用 ChromeOS 设备 917
12.7.1. ChromeOS 和 Ivanti Neurons for MDM 918
12.7.2. 向 ChromeOS 设备分发 Android 应用程序 919
12.7.3. 添加和分发 ChromeOS 扩展应用程序 920
12.7.4. ChromeOS 蓝图配置 921
12.7.5. 设备操作 922
12.7.6. 常见问题解答 923
12.7.7. 建议的评估步骤 925
12.8. 固件管理 926
12.8.1. 正在注册 Zebra OTA 服务 927
12.8.2. Samsung E-FOTA 许可证管理（已停用） 928
12.9. 管理脚本和文件 929
12.9.1. 所有脚本 930
12.9.2. 文件 934
12.10. 品牌 935
12.10.1. 管理员 > Apple 应用目录（品牌化） 936
12.10.2. 将 Android App Catalog 品牌化 937
12.10.3. 管理员 > Android 自助服务终端加印品牌 938
12.10.4. 品牌化电子邮件模板 939
12.10.5. 自助门户 947
12.10.6. 自助门户（品牌化） 949
12.10.7. 多用户登录 (Webclip) 品牌加印 950
12.10.8. 组织 951
12.11. 添加对非 iOS 设备的管理 952
13. 程序包 953
13.1. 升级 957
14. 设备许可证 959
14.1. 租户暂停 960
15. 打开支持票证 961
16. 第三方属性 962
17. Apps@Work 963
18. 在 Ivanti Neurons for MDM 和 SCEP 服务器之间启用 Kerberos 身份验证 965
19. Ivanti Neurons for MDM 127 管理员指南 967
20. Welcome 968
21. Welcome CSH 969
22. Windows 更新管理 970

1. 关于 Ivanti Neurons for MDM

作为现代的移动安全性方法，Ivanti Neurons for MDM 在高度可扩展和易于更新的安全基础设施中提供了统一端点管理 (UEM) 解决方案，该基础设施支持全球数百万台设备。

- 即时更新：在可用时，获取自动软件和安全更新，以及新增功能的访问权限。
- 按需扩展：随业务需求变化扩展部署，无需担心容量规划。
- 将硬件成本最小化：基于云的服务需要零占用情况进行管理，无需维护本地硬件。
- 高正常运行时间和高可用性。
- 将现有投资最大化：将 IT 资源从硬件维护重新分配到更具战略意义的任务，这将为企业创造价值。

您可以查看此版本推出的新增功能摘要的摘要。

2. 新增功能摘要

本部分概述了此版本提供的新增功能和功能增强。 此外，也提供了对描述这些功能和功能增强的文档的参考（可用时）。

常规功能和功能增强

Android 功能

iOS、macOS、watchOS、visionOS 和 tvOS 功能

Windows 功能

常规功能和功能增强

- **增强的 macOS 程序包 ID 处理**：通过在应用程序上传期间自动检测和填充正确的程序包 ID，并确保相同的程序包 ID 发送到设备，改进了 macOS 内部 PKG 应用程序部署。 这样可以提高应用程序识别的准确性，解决服务器设备安装状态不匹配问题，并改进安装状态报告。 在部署后锁定之前，可以在上传期间查看和编辑捆绑包 ID。
- **已安装应用程序的捆绑包 ID 可见性**：设备详细信息页面上的已安装应用程序部分现在包含捆绑 ID 列，可以从页面设置启用或隐藏该列。
- **失败 Android 应用程序安装的自动重试**：进入错误安装状态的 Android 应用程序安装现在将在设备注册后一小时开始自动重试。 安装命令每 30 分钟重新发送一次，最多可尝试五次，以提高应用程序部署成功率。
- **空间设备移动审计跟踪**：添加了启用空间中设备注册和取消注册的审计跟踪设置，以跟踪空间之间的设备移动。 有关更多信息，请查看导出审计跟踪。
- **设备清理设置的操作系统平台筛选器**：管理员现在可以在删除“已停用”和“待停用”设备时按操作系统平台筛选设备清理操作。 默认情况下，所有支持的平台保持选中状态，保留现有行为。 管理员可以根据需要修改选择并将清理操作限制在特定平台上。 有关详细信息，请参阅设备清理设置。
- **Office 365应用程序保护策略同步**：以前，管理员可以在创建或修改应用程序保护策略时直接在 Ivanti Neurons for MDM 中选择应用程序。 Microsoft 已弃用用于检索可用应用程序列表的 API，导致受保护应用程序列表在 Ivanti Neurons for MDM 中显示为空白。 Microsoft Office 365 应用程序保护策略管理已更新，以与 Microsoft Intune 中的更改保持一致。 Intune 中配置的应用程序现在会自动同步到 Ivanti Neurons for MDM，确保受保护应用程序的持续可见性。 虽然仍可从 Ivanti Neurons for MDM 中移除应用程序，但新的应用程序分配必须在 Microsoft Intune 中配置，并会自动同步到系统中。
- **空间设备移动审计日志记录**：管理员现在可以通过审计日志跟踪空间之间的设备移动。 启用后，每当设备从一个空间中删除并添加到另一个空间时，新的审计设置都会记录事件，从而提供对自动化和基于规则的空间分配的更大可见性。 有关详细信息，请参阅导出审计跟踪。
- **使用设备组的自动自定义属性分配**：管理员现在可以在设备组级别分配自定义属性。 属于设备组成员的设备会自动继承配置的属性值，从而减少手动配置，并帮助确保一致的设备分类。 有关详细信息，请参阅设备组。
- **OS 级设备注册限制**：按平台限制设备注册，仅允许批准的 **Apple**、**Android** 和 **Windows** 设备注册。 有关详细信息，请参阅用户设置。

Android 功能

- **在使用应用程序时阻止应用程序更新**：管理员现在可以防止托管 Android 应用程序在主动使用时被更新。 启用**在使用应用程序时不更新**后，应用程序更新将推迟，直到用户关闭应用程序或将其移动到后台，从而有助于最大限度地减少活动会话期间的中断。 有关详细信息，请参阅应用配置。
- **跨锁定策略更改维护自助服务终端模式**：增加了跨锁定策略更改维护 kiosk 模式的支持。 在锁定政策更新后，设备会自动返回到 kiosk 模式，从而减少手动干预并最大限度地减少专用设备的中断。 有关详细信息，请参阅锁定和自助服务终端：Android Enterprise。
- **启用未删减的通知**：新增了在设备所有者设备上配置锁屏通知可见性的支持。 管理员可以在锁屏上显示、隐藏或隐去通知内容，从而在保留通知功能的同时保护敏感信息。 有关详细信息，请参阅高级 Android 密码和锁屏。

- **在批量注册配置文件期间支持设备到用户映射**：增加了对批量注册配置文件中设备到用户映射的支持。 管理员可以通过批量注册 CSV 文件或在手动设备添加期间为每个设备分配特定用户，从而在注册期间启用自动用户分配并减少注册后管理任务。 管理员还可以在设备注册之前更新用户分配。 有关详细信息，请参阅批量注册配置文件中的设备到用户映射。

iOS、macOS、watchOS、visionOS 和 tvOS 功能

- **设备注册配置文件的新跳过密钥**：管理员现在可以在创建设备注册配置文件时使用以下跳过密钥：
  - **跳过 Liquid Glass 窗格**（iOS 27.0+ 和 macOS 27.0+）
  - **跳过无障碍功能状态窗格** (iOS 27.0+)
    这些跳过键允许管理员在设备注册期间隐藏特定的设置窗格，有助于简化注册体验。 有关详细信息，请参阅设备注册。
- **支持 DDM 设备系统健康状态**：Ivanti Neurons for MDM 现在支持**设备详细信息**页面上的 DDM 设备系统健康状态。 管理员可以在**设备组件健康状态**部分查看此状态，以监控受监控设备报告的系统健康状态。 有关详细信息，请参阅开始使用设备。
- **为 Apple 设备添加新的设备详细信息字段**：添加新的**设备详细信息**字段，以便更清楚地了解 Apple 设备管理状态。 管理员现在可以查看以下详细信息：
  - iOS 27.0+ 上运行的设备的**多用户模式**。 此字段指示 iPad 是否配置为共享设备。
  - 在 iOS 27.0+、macOS 27.0+、tvOS 27.0+、visionOS 27.0+ 和 watchOS 27.0+ 上运行的设备的 **MDM 注册类型**。
  - **MDM 返回服务**，为在 iOS 27.0+ 和 visionOS 27.0+ 上运行的设备保留应用程序。
    这些字段可帮助管理员直接从设备详情页面查看设备配置和注册信息。 有关详细信息，请参阅开始使用设备。
- **支持应用程序隐私默认值配置**：管理员现在可以使用 Apple 设备声明式管理 (DDM) 为一个或多个应用程序配置**应用程序隐私默认值**。 当应用程序首次启动时，用户会收到单个同意提示，以允许或推迟支持的隐私组件的推荐权限，例如相机、麦克风、位置、蓝牙和本地网络访问。 有关详细信息，请参阅应用程序隐私默认值。

> macOS 27.0+ 受监督设备现在支持应用程序隐私默认值配置。

- **添加新的 DDM 应用程序管理属性**：将 DDM 应用程序管理属性 **Apple DDM 应用程序已启用**字段添加到“高级搜索”和设备列表页面。 它显示哪些设备具有通过 DDM 分发的应用程序。 管理员可以通过用户设置将此项打开。 有关详细信息，请参阅开始使用设备。
- **增强的 macOS 可扩展 SSO 配置**：更新了 macOS 可扩展 SSO 配置，以正确映射 **preferred_username** 和 **name** 等令牌属性。 这样可以解决无效令牌到用户映射导致的配置错误，并允许将 SSO 配置文件成功部署到设备。
- **Apple 增强日志记录**：管理员可以使用 AppleCare 提供的令牌在支持的 Apple 设备上启动 Apple 增强日志收集。 设备详细信息显示会话状态、令牌和时间戳信息，如果需要，可以取消活动会话。 有关详细信息，请参阅 Apple 增强日志记录。
- **锁定模式状态**（iOS 27+、macOS 27+）：新增支持使用**设备详细信息**页面、**高级搜索**和设备组规则中的**安全锁定模式**字段，按锁定模式状态查看和筛选设备。 此字段指示设备是否启用锁定模式 (**true**) 或禁用锁定模式 (**false**)。 有关详细信息，请参阅开始使用设备、设备组和自定义策略。
- **macOS 软件更新设置支持更新**：macOS 27 及更高版本的设备不再支持 **macOS 软件更新设置**配置。 此配置现在仅适用于最高支持 macOS 26.x 的版本。 有关详细信息，请参阅 macOS 软件更新规则配置。
- **限制支持更新**（iOS 27+、macOS 27+）：更新了**允许后台安全改进安装** 以及**允许后台安全改进移除**限制，以表明 iOS 27 及更高版本以及 macOS 27 及更高版本设备不再支持这些限制。 有关详细信息，请参阅 iOS 限制和 macOS 限制。
- **Siri 设置配置更新**（iOS 27.0+、macOS 27.0+、tvOS 27.0+ 和 visionOS 27.0+）：在 Siri 设置配置中添加了对新限制设置的支持。 有关详细信息，请参阅 Siri 设置。
- **Intelligence 设置配置更新**（iOS 27.0+、macOS 27.0+ 和 visionOS 27.0+）：在 Intelligence 设置配置中添加了对新限制设置的支持。 有关详细信息，请参阅 智能设置。
- **Safari 隐私设置**（iOS 27.0+、macOS 27.0+）：在 Safari 扩展和设置配置中增加了对 Safari 隐私设置的支持，允许管理员使用 Apple 声明设备管理 (DDM) 配置特定网站的默认相机和麦克风权限。 有关详细信息，请参阅 Safari 扩展和设置配置

Windows 功能

- **Windows AI 管理配置**：Windows AI Management 现在支持其他 Windows AI CSP 策略，用于管理 Microsoft Copilot、Windows Recall 和 Microsoft Paint AI 功能。 管理员可以禁用 Copilot 硬件密钥、删除 Microsoft Copilot 应用程序、禁用 Recall 的 AI 数据分析、配置 Recall 快照存储限制，以及禁用 Paint 中的 Image Creator、Cocreator 和 Generative Fill 。 还增加了对用户范围策略和设备范围策略的支持，从而能够更精细地控制 Windows 设备上的 AI 功能。 有关详细信息，请参阅 **Windows AI 管理配置**。

移动威胁防御功能

移动威胁防御 (MTD) 可避免托管设备受到影响设备、网络和应用的移动威胁和漏洞的破坏。 有关适用于当前版本的 MTD 相关功能的信息，请查看适用于平台的移动威胁防御解决方案指南（请见 Ivanti 产品文档页面的移动威胁防御部分）。

> MTD 指南的每个版本包含目前经过完整测试，以及可在服务器和客户端环境中使用的所有移动威胁防御功能。 由于服务器与客户端版本之间存在差异，因此在功能完全可用时，该系列的最终版本将提供 MTD 指南的新版本。

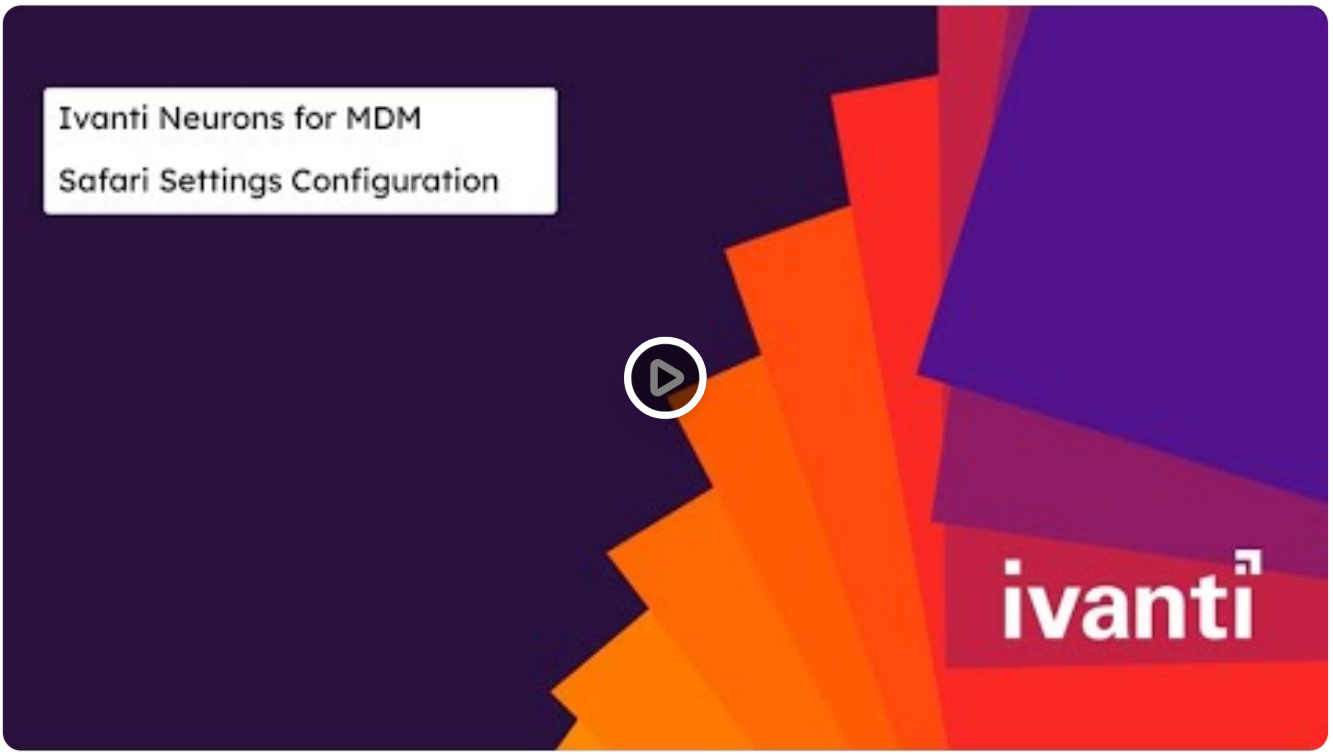
3. 视频

精选视频


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


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


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



正在寻找 Ivanti Neurons for MDM 中特定功能的视频？ 通过在本文档任何页面的“**这篇文章有用吗？**”部分中分享您的反馈，将您的看法告知我们。

4. 入门指南

本节提供需要在 Ivanti Neurons for MDM 门户之间交互的功能的设置和使用情况概览。 本部分包含以下主题：

- 解决方案概览
  - 关键功能
  - 架构关系图
  - Ivanti Neurons for MDM 应用
  - 角色
  - 入门指南
- 设置浏览器中的首选语言
- Ivanti Neurons for MDM 和 Access 的统一导航界面
- 用于管理 Android 设备的设备管理 (DA) 模式 - 已弃用

解决方案概览

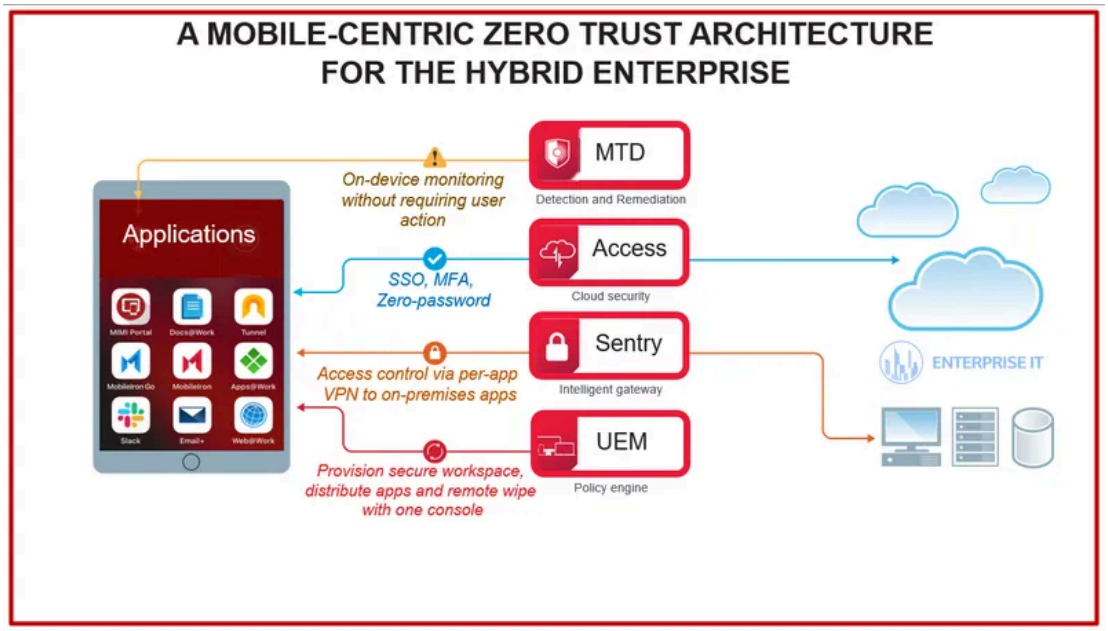
对于持续访问移动设备和企业网络外部其他端点中的业务数据，这需要特别留意安全性。 要满足当前安全需求，企业需要考虑如何：

- 配置端点，例如手机和笔记本电脑
- 根据一组命令性数据授予访问权限
- 保护静态和动态数据
- 根据需要，强制实施措施

针对此现代问题的 Ivanti 解决方案可以应对全部挑战。 您可以监控端点并触发自适应策略，修复威胁、隔离设备并维持合规性。 下列组件共同帮贵组织实现以移动为中心的零信任框架：

- Ivanti Neurons for MDM - 对于基于角色的用户，帮助您在任何设备上创建安全工作区，其中包含应用、配置和策略。 对于提高效率所需的资源，用户拥有轻松安全的访问权限
- **Sentry** - 这是一款嵌入智能网关，可帮您安全访问本地资源
- **Access**– 帮您验证用户、设备、应用、网络类型，以及是否存在威胁。 自适应访问控制检查是零信任模型的基础。 Access 在云段提供单点登录和安全性
- **移动威胁防御** - Ivanti Neurons for MDM 与移动威胁防御 (MTD) 的组合，使用最先进的加密和威胁监控，保护设备和网络中的数据，并检测设备、网络和应用级攻击

下图显示了解决方案概览：



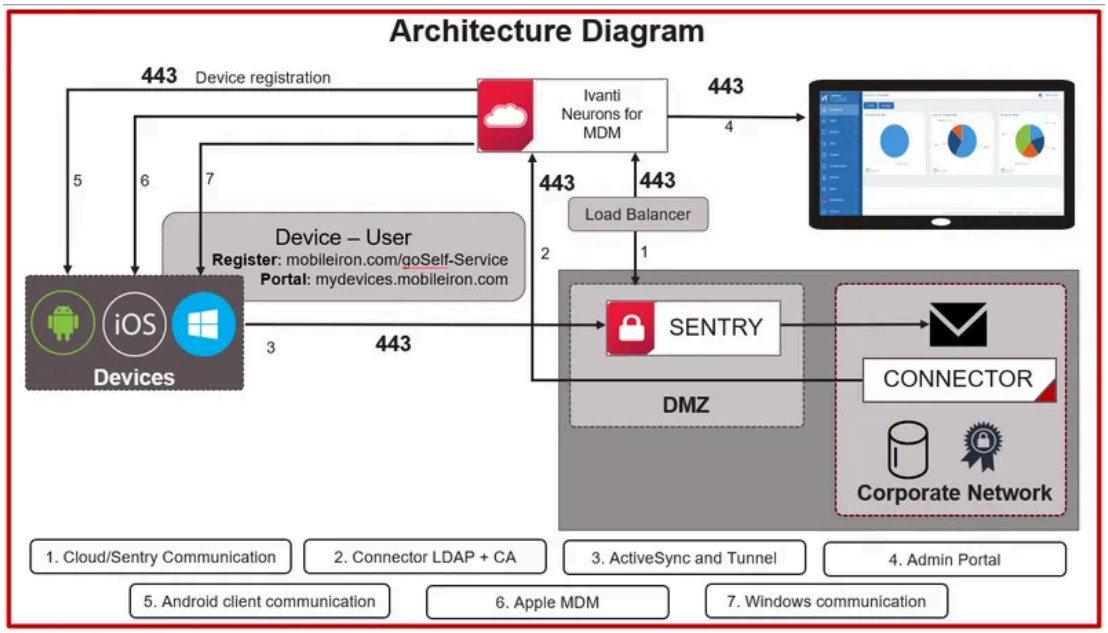
关键功能

Ivanti Neurons for MDM 平台提供基本可见性和 IT 控制，这些功能可以保护、管理和监控访问关键业务数据的任何企业或员工拥有的移动设备或台式电脑。 Ivanti Neurons for MDM 平台允许组织保护在组织中使用的各种员工设备，并管理设备的整个生命周期，其中包含：

- 策略配置管理和强制实施
- 应用分发和管理
- 适用于桌面设备的脚本管理和分发
- 设备操作
- 访问控制和多重身份验证
- 威胁检测和修复

架构关系图

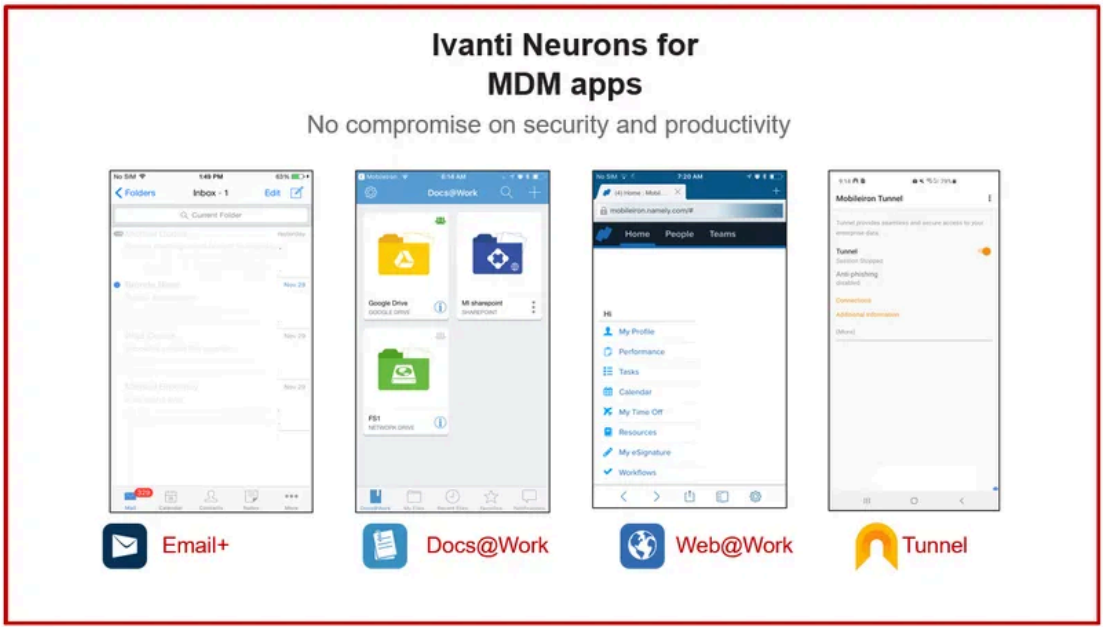
下图显示 Ivanti Neurons for MDM UEM 平台的架构概览：



Ivanti Neurons for MDM 应用

- **App Catalog** – App Catalog 是可自定义的企业应用店面。 IT 管理员可以直接将私人或内部应用发布到最终用户设备。 App Catalog 也可以与 Apple 批量采购计划一起使用，这有助于在 iOS 设备上安全分发移动应用。 而且，Ivanti 可以利用 iOS 托管应用和 Android Enterprise 的功能。 这允许在 Ivanti Neurons for MDM UEM 平台中轻松配置应用级设置，以及高级应用安全功能的安全策略。
- **Email+** - 这是保护适用于 iOS 和 Android 的 PIM 应用的跨平台。 通过与企业中的 ActiveSync 服务器进行通信，Email+ 可以在公司拥有和个人设备上保护电子邮件、日历、联系人和任务。
- **Docs@Work** - 允许用户从 Microsoft Share Point 等存储库以及 Box 和 Dropbox 等云服务安全地访问、创建、编辑、标记和共享内容。 此操作十分重要，因此用户可以随时随地最大限度地提高效率。
- **Web@Work** - 这是安全浏览器，并允许企业用户安全访问企业内部网中的 Web 内容。 使用 Web@Work，您可以将企业数据的访问权限限制为授权用户。 在 Web@Work 与 App Tunnel 一同部署时，您可以保护企业动态数据。 使用 Web@Work，用户可以轻松快速地访问内部网资源。

下图显示 Ivanti Neurons for MDM 应用：



角色

管理员 - 作为企业管理员，您对以下任务负责：

- 在工作区电子邮件、应用、配置及 Wi-Fi 和 VPN等连接方面，为企业用户提供无缝安全访问权限。
- 在员工设备上将个人数据与业务数据分开，这样业务数据不会泄漏到个人应用，IT 也不会无意访问个人数据。

用户 – 作为企业用户，您可以从现代安全移动设备、桌面和云服务无缝访问业务应用和个人数据。 如需详细了解您能够以用户身份执行的各种任务，请参阅用户 和角色管理。

入门指南

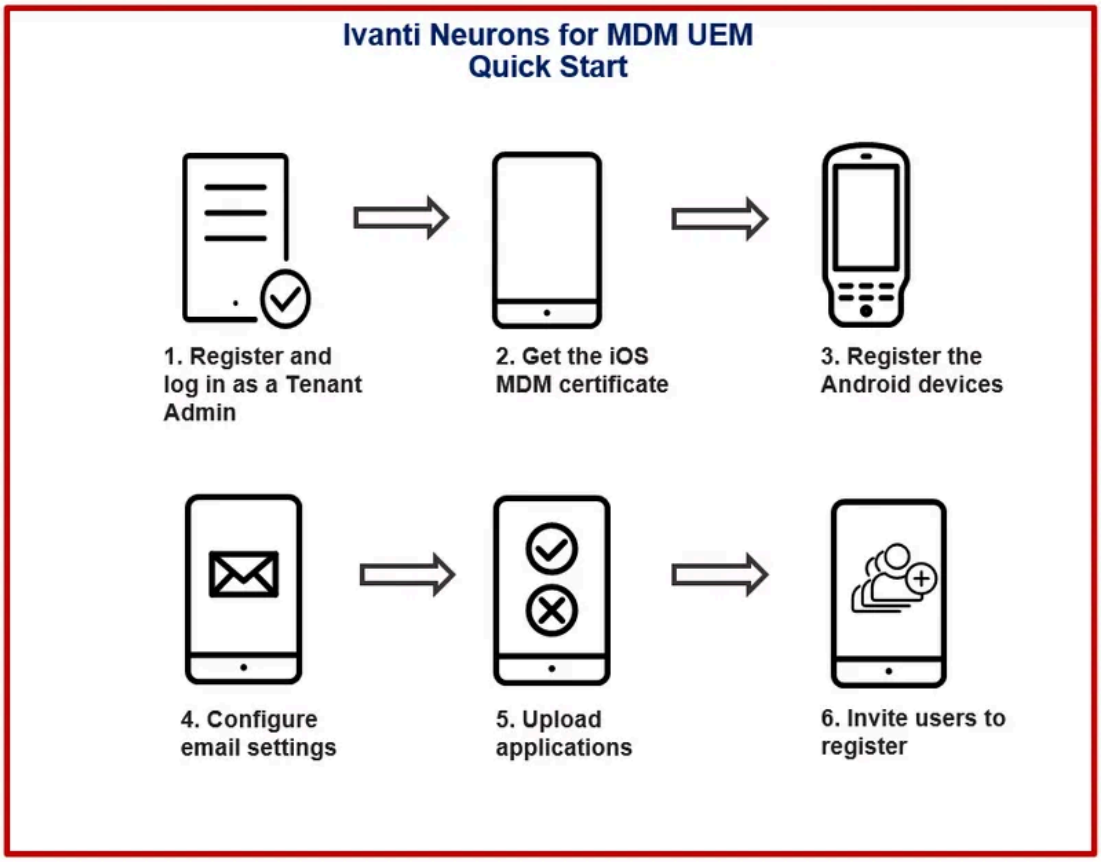
如果您是刚注册的新用户，请按照本节提供的步骤快速熟悉 Ivanti Neurons for MDM 服务。

在订阅 Ivanti Neurons for MDM 平台后，Ivanti 将为您创建 Ivanti Neurons for MDM 租户。 您会收到一封发送到注册电子邮件地址的电子邮件，其中包含 PDF 文件，以及为企业创建的租户的相关信息：

- 关于您购买的软件捆绑包的信息
- 租户的 URL 和超级管理员登录凭据
- 如何访问适用于 Ivanti Neurons for MDM 的支持社区和常见问题解答
- 在何处访问技术文档并下载软件

> Ivanti, Inc 未提供软件密钥。 通过使用超级管理员凭据登录 Ivanti Neurons for MDM 租户并接受服务条款，您可激活 Ivanti Neurons for MDM 产品。

下图介绍了开始使用 Ivanti Neurons for MDM 的步骤：



步骤

1. 单击租户注册电子邮件中提供的 URL。 将显示密码重置提示。
2. 更改密码。
3. 使用 ID 和密码，登录租户帐户。 将显示欢迎向导。
4. 请填写**欢迎**表单中的详细信息，接受条款与协议，并单击**继续**。
5. 要安装 iOS MDM 证书，请查看安装 MDM 证书。

> 如果需要在稍后某个时间点管理 iOS 设备，您可以跳过 iOS MDM 证书安装。 然后，向导将提示您注册企业的 Android 设备。 跳过 iOS MDM 证书安装意味着 iOS 设备将无法注册。 用户将看到一条消息，说明未启用 iOS 设备注册。

6. 要在 Android Enterprise (AE) 模式中注册 Android 设备，请查看受管 Google Play 帐户（Android Enterprise 帐户）。 然后，向导将提示您设置电子邮件帐户。

> 如果需要在稍后某个时间点管理 Android 设备，您可以跳过 Android 托管 Google Play 帐户注册。 跳过托管 Google Play 帐户注册，您将无法注册 Android Enterprise 设备。 Android 设备仍可以通过设备管理员注册，但受管 Google Play 和应用配置等关键功能将无法使用。

7. 要配置电子邮件设置和 ActiveSync，请查看 Exchange 配置和电子邮件配置。
8. 单击**继续**。 将提示通行码创建提示。
9. 选择通行码类型，并单击**继续**。
10. 选择要上传的应用，并单击**继续**。

11. 指定用户的电子邮件地址，然后点击**继续**。 用户将收到一封电子邮件，以便注册移动设备。 将显示配置的摘要。
12. 单击**已完成**。 将显示仪表板页面。
13. 要了解更多，请执行以下操作：
    - 转到**用户**。 将列出所有受邀用户。
    - 转至**应用** 。 将列出您上传的所有应用。
    - 转至**配置**。 将列出您在注册过程中推送的所有配置。

有关您可以管理员身份执行的各类任务的更多信息，请查看管理部分。

设置浏览器中的首选语言

如果用户将浏览器语言设置为不支持的语言，该用户可以将 en_US（英语，美国）设置为门户网站的默认语言。

要对在 macOS 10.15+ 设备上运行的 Safari 浏览器设置语言首选项，用户可以通过如下方式设置首选语言：

1. 在 macOS 设备上，转到**系统首选项**。
2. 转到**语言和区域 > 通用**。
3. 将 **en_US**（或任何其他语言选项）设置为**首选语言**。

Ivanti Neurons for MDM 和 Access 的统一导航界面

对于一些群集中的新客户，Access 可用作 Ivanti Neurons for MDM 的统一导航界面。 使用 Ivanti Neurons for MDM 管理员凭据登录。 Access 选项作为独立选项卡在左侧导航窗格中可用。 访问产品文档并单击 Access，以了解有关 Access 及如何设置 Access 的更多信息。

统一的导航界面包含以下功能：

- 适用于 Ivanti Neurons for MDM 和 Access 的统一登录。
- 左侧导航窗格中的产品选取器，用于在 Ivanti Neurons for MDM 与 Access 产品之间切换。
- 产品选择内存：在首次登录后，将显示 Ivanti Neurons for MDM 管理门户。 在后续登录时，将显示 Ivanti Neurons for MDM 或 Access，并映射在首次登录时选择的产品。
- 适用于 Ivanti Neurons for MDM 和 Access 的左侧导航窗格。
- 具有选项链接的统一帐户设置窗格，例如升级选项、文档、支持门户网站、更改密码和注销。

用于管理 Android 设备的设备管理 (DA) 模式 - 已弃用

管理 Android 设备的设备管理 (DA) 模式将从 Ivanti Neurons for MDM 78 开始分阶段弃用。

对于在 Ivanti Neurons for MDM 78 中创建新租户的任何新用户，他们无法在 DA 模式下注册任何设备（Android 6 及更高版本）。 对于需要为 Android 6 至 Android 9 启用 DA 注册的任何新租户，他们必须联系 Ivanti 支持。

- 我们将继续阻止 Android 10 和更高设备注册到 DA 模式。
- 对于现有用户（具有或没有现有 DA 部署），管理现有 DA 设备（Android 6 至 Android 11）没有任何变化。 但在升级到 Ivanti Neurons for MDM 78 时，对于在现有租户上运行 Android 10+ 的任何新注册设备，也不允许它们在 DA 模式下运行。 此现有租户仅可在 DA 模式中注册从 Android 6 至 Android 9 版本的设备。
- 如果任何用户计划将 DA 设备从 Core 实例迁移到 Ivanti Neurons for MDM R78，请确保在触发迁移前启用 Android Enterprise，并将至少一个系统配置分发到目标集：PO、DO 或 COPE。 此步骤非常重要，可防止设备在迁移后报废。

DA 注册类型	现有租户（已升级到 78）	新租户
搭载 OS >=10 设备的新 DA 注册	不允许	不允许
搭载 OS < 10 设备的新 DA 注册	已允许	不允许
搭载 OS >= 10 的现有 DA 设备	仍将保持活动状态	不适用
搭载 OS < 10 的现有 DA 设备	仍将保持活动状态	不适用
搭载 OS >= 10 的已迁移 DA 设备	将停用	将停用
搭载 OS < 10 的已迁移 DA 设备	仍将保持活动状态	将停用

4.1. 配置 macOS 设备

这是一个概述主题，并提供了与在 Ivanti Neurons for MDM 中配置 macOS 设备相关的常见过程和其他内容的列表。 可以访问 Ivanti Neurons for MDM*管理员指南*中的所有 macOS 主题。

内容

- 注册设备
- 配置用户邀请模板
- 设置 Zero Sign-On 功能
- 设置 Mobile@Work for macOS 客户端
- 设置 macOS Shell 脚本
- 设置 macOS 配置
- 设置 macOS 策略

注册设备

大多数用户在开始之前都必须先注册设备。 可使用以下任意方法开始注册流程：

- 向一名或多名最终用户发送邀请（iReg 注册）。 有关详细信息，请参阅**设备注册**小节中的 *macOS 设备注册*主题。
- **设备注册**和**带有 Apple 商务管理的用户注册**

有关详细信息，请参阅设备注册。

配置用户邀请模板

您可以对最终用户电子邮件邀请进行品牌化，以使最终用户更熟悉其外观。 有关更多信息，请查看**品牌化电子邮件模板**。

使用用户识别的名称和徽标，您可以自定义设备注册过程。 有关更多信息，请查看**用户品牌化**。

有关更多信息，请查看**配置和使用注册确认电子邮件**。

设置 Zero Sign-On 功能

有关 Zero Sign-On 相关文档，请查看 *Access 指南*中的“使用 Access 进行 Zero Sign-On”。

有关零接触自动注册，请查看用户设置主题，“为新设备注册配置设置”部分的第 13 步。

设置 Mobile@Work for macOS 客户端

Mobile@Work for macOS 应用提供了：

- macOS 设备中的脚本功能
- 适用于最终用户的 App Catalog
- 推送通知
- 用户入门（欢迎/状态）屏幕，并用于自动设备注册注册

在将 Mobile@Work 推送给最终用户之前，请确保已创建 **Mobile@Work for macOS Configuration.htmMobile@Work for macOS**并设置为分发至目标 macOS 设备。

在自动设备注册过程中，您可以为 macOS 设备启用用户入门。 在设备注册完成时，Mobile@Work for macOS 会立即推送到设备，以及配置文件、配置和应用。

设置 macOS Shell 脚本

Ivanti Neurons for MDM允许您自行创建 macOS Shell 脚本，您可将其上传到 Ivanti Neurons for MDM，并在受管 macOS 设备上运行。 您可以使用 Mobile@Work for macOS 脚本配置进行脚本配置。 Mobile@Work for macOS 会将脚本执行结果返回到 Ivanti Neurons for MDM，并将显示在设备日志中。 在**日志**选项卡中，您可以从 macOS 设备的设备详细信息页面查看设备日志。 有关创建、上传和管理脚本存储库的更多信息，请查看所有脚本。

在 macOS 设备上运行 Shell 脚本前，请确保用户在设备上运行 Mobile@Work for macOS 应用，并将 Mobile@Work for macOS 配置推送到设备。 脚本可以运行一次，或定期运行。 通过 Ivanti Neurons for MDM 中的脚本，管理员也可以从设备收集信息，并将其作为自定义属性存储到 Ivanti Neurons for MDM。 例如，如果您需要了解 macOS 设备中的 Java 版本，您可以收集此信息，并根据每个设备将其存储到自定义设备属性。 有关详细信息，请查看 **Mobile@Work for macOS** 中的*创建 Mobile@Work for macOS 脚本配置*。

设置 macOS 配置

配置是发送到设备的设置集合。 例如，您可以使用配置自动设置这些设备上的 VPN 设置和通行码要求。 使用**配置**页面，以选择、设置并分发配置。 有多种可用的配置类型。 在页面中，您可以查看可用 macOS 配置的列表，其中包含以下配置：

- **Wi-Fi**
- **通行码**
- **VPN**
- **加密的 DNS**
- **FileVault 2**
- **FileVault 恢复密钥**
- **macOS 防火墙**
- **macOS 限制**
- **macOS AppStore 限制**
- **macOS Finder 设置**
- **macOS 内核扩展策略**
- **Active Directory (macOS)**
- **Office 365 自动帐户创建 (macOS)**

您可以使用自定义配置，以导入和分发预定义的配置文件。

设置 macOS 策略

策略可以定义设备的要求，以及设备不符合要求时将产生的后果。 每种策略都由规则和合规性操作（违反规则将产生的后果）组成。 使用**策略**页面可对策略进行选择、设置和分配。 数据保护/加密已禁用，允许的应用是 macOS 相关策略。 您可以使用自定义策略，根据您指定的设备和用户属性、部分条件、值和合规性操作，创建自定义策略。

分发 macOS 应用

Ivanti Neurons for MDM 通过 Apple 的 MDM 协议并使用 Mobile@Work 应用支持 macOS 应用分发。 管理员可以选择使用以下其中一种或两种方法：

- Apple 的 MDM 协议 - 管理员仅可将特定 PKG 格式（分发格式）作为内部应用上传，并且也可以从 Mac App Store 分发应用（包含 Apple 的 Apps 和图书许可支持）。 但此方法不允许管理员分发 DMG 和其他 PKG 格式。
- Mobile@Work for macOS 应用程序 - 作为一种向用户分发应用程序的方式，管理员可以使用 MobileIron Packager (MIP) 应用程序，以将任何 PKG、DMG 或 .app 文件转换为 MIP 文件。 将 MIP 文件作为内部应用上传到 Ivanti Neurons for MDM。

> 从 MobileIron 软件下载中，您可以下载 Ivanti Neurons for MDM Mac Packager 实用程序。

管理员可以使用 Mobile@Work，以分发格式为 DMG、PKG 或 .app 的内部应用。 对于仅在 Mac App Store 中提供的应用，管理员可以继续使用 Apple 的本地 MDM 功能，其中包含 Apple App 和图书许可证功能。

4.2. 配置和使用注册确认电子邮件

管理员可以在用户完成注册后配置和触发向用户发送的电子邮件。 例如，此电子邮件包含用户在成功注册后所需的其他说明。 管理员可以启用在用户邀请期间发送此电子邮件。

流程：

- **配置功能：**
  - 配置电子邮件模板：默认情况下，英文电子邮件模板如下所示；但您可以按照**品牌化电子邮件模板**的**自定义电子邮件模板**中的说明进行修改，以更贴合您的目的：



  - 打开注册确认电子邮件。 请查看**用户设置**中的**配置用户注册确认电子邮件**。
- **使用功能：**
  - 如**邀请用户**所述，向用户发送注册邀请。 在用户成功注册时，Ivanti Neurons for MDM 将向该用户发送注册确认电子邮件。

4.3. 配置和使用策略合规通知电子邮件

管理员可以在“自定义和允许的应用策略”发送的电子邮件中封装策略合规通知电子邮件模板，以向设备不合规的用户发送电子邮件操作。 以下过程介绍了配置：

- **配置功能：**
  - **配置电子邮件模板**。
    默认情况下，英文电子邮件模板如下所示；但您可以按照品牌化电子邮件模板的自定义电子邮件模板中的说明进行修改，以更贴合您的目的：
    
  - **打开策略合规通知模板**。 对于您使用“自定义和允许的应用策略”发送电子邮件操作编写的消息，此模板应与其一起使用。 Ivanti Neurons for MDM 会将您在这些电子邮件操作中指定的信息插入策略合规性通知模板。 在您创建或编辑自定义或允许的应用策略时，您可以打开策略合规电子邮件模板。 有关为自定义策略或允许的应用策略启用策略合规通知模板的说明的更多信息，请分别查看添加自定义策略和创建允许的应用策略。
- **使用功能：**
  - 对于启用策略通知模板的设备，在不符合自定义或允许的应用策略时，Ivanti Neurons for MDM 会向设备所有者发送一封电子邮件，并先在策略通知模板中封装电子邮件。 您与该功能的交互旨在按照上文总结的方式对其进行配置，而 Ivanti Neurons for MDM 会使用该功能。

4.4. 按需功能

Ivanti Neurons for MDM 包含一些默认禁用的按需功能。 此类功能可能会对性能产生一些影响，也可能尚未完全准备好在生产中部署。

如果管理员有兴趣在租户设备上启用默认禁用的一个或多个按需功能，可以联系支持部门。

下表包含记录的按需功能的列表：

功能	描述	平台	许可证
Windows 10 功能	功能适用于 Windows 10 设备。	Windows 10	• 旧版：Gold • 当前：安全 EUM 请查看程序包，以了解有关旧版和当前产品的更多信息。
App Catalog URL 复制到剪贴板	为管理员提供将 App Catalog URL 复制到应用程序剪贴板的能力。 该 URL 可以通过电子邮件分发给用户。 如果用户点击已注册设备的链接，则具有该应用程序的 App Catalog 将在浏览器中打开，用户可以选择安装该应用程序。 管理员负责限制将此 URL 分发给目标用户。	• iOS • macOS	不适用（特定租户）
将 Web 剪辑设置为应用程序	在 App Catalog 中将 **Web 剪辑**设置为应用程序，以使 Web 应用程序在用户的 App Catalog 中可用。 Web 剪辑可以定义为配置，但配置只能由管理员推送。 用户可以选择在其设备上安装 Web 应用程序或退出，而用户无权选择退出 Web 剪辑配置。	iOS	不适用（特定租户）
打开已加入允许列表的设备的注册	允许基于“用户 > **用户设置** > 默认设备注册设置”中的已加入允许列表的序列号进行设备注册。	• iOS • macOS	不适用（特定租户）
基于证书的身份验证	通过**基于证书的身份验证**功能，管理员可以使用数字证书和租户指定的主机名或虚主机名登录。 使用**管理员**选项卡中的虚主机配置，配置此身份验证设置。	此功能并不特定于平台。	不适用（特定租户） 此功能仅在 NA3 群集环境中可用，并且仅在由支持启用时可用。
创建专用设备配置（公司拥有的单用途或 COSU）	通过 Android Enterprise 或专用设备（企业拥有的单用途或 COSU 配置），管理员可以配置可用于特定目的的专用设备。**COSU 配置**已分发到工作托管设备（设备所有者模式），以在 Kiosk 模式中仅向用户提供一个应用。	Android Enterprise	Silver
仪表板非活动期	默认情况下，仪表板非活动期设置为 15 天。 可根据租户需求更新此设置，最长为 30 天。 如果您需要更长的非活动期，请联系**支持**团队。	此功能并不特定于平台。	

4.5. 准备 Android Enterprise 设备支持

本节描述 Android Enterprise 设备的最低网络要求。 Android 设备通常不要求打开防火墙上的入站端口才能正常工作。 然而，在为 Android Enterprise 设备设置网络环境时，管理员需要注意一些出站连接。

下表中提供的网络更改列表并非详尽无遗，可能会有所变化。 它涵盖了企业管理 API 和 GMS 应用程序当前和过去版本的已知端点。

> 除了下表列出的端口之外，Android Enterprise 设备还需要访问 Ivanti Neurons for MDM。

有关 Android Enterprise 设备要求的信息，请参阅 Android Enterprise 帮助中的 **Android Enterprise 网络要求**。

Google 没有提供特定的 Ip，所以您应该允许防火墙接受所有 IP 地址的传出连接，这些地址包含在 Google 的 15169 的 ASN 中（在 **http://bgp.he.net/AS15169#_prefixes** 中列出）。

> AS15169 块未列出 Google 对等点和边缘节点的 IP。 请查看 **https://peering.google.com/**，以了解有关 Google Edge 网络的更多信息。

5. 仪表板

仪表板显示已注册设备和用户的重要统计数据。 仪表板上的各个部分称作小组件。 对于每个小组件，您可以定义：

- 显示数据的类别（如设备或用户）
- 如何对数据进行分组（如按操作系统内部版本或模型）
- 如何筛选数据（如仅显示 iOS 设备，或按操作系统内部版本显示）
- 如何显示数据（例如饼图或条形图）

验证报告和其他信息

仪表板显示了已注册设备和用户的重要统计数据。 仪表板上的各个部分称作小组件。

您可以验证其他信息，如下所示：

- **查看通知**：转到**仪表板 > 通知**页面（或单击钟形图标（右上角）），以查看通知并在必要时采取措施。
- **报告**：转到**仪表板 > 报告**页面，以访问统一端点管理 (UEM) 系统中的数据。
- **审计跟踪**：转到**仪表板 > 审计跟踪**页面，以访问记录时间序列，这些记录捕获了对 Ivanti Neurons for MDM 中所有实体所执行的活动。要启用此功能，请转到**管理员 > 基础设施 > 审计跟踪**页面，并点击**启用审计跟踪**。
- 应用见解：转到**仪表板 > 应用程序见解**页面，以查看和分析应用程序分发，以及其他应用程序详细信息。

此小节包含以下主题：

- 使用小组件
- 应用见解
- 使用计划的报告
- 使用自定义报告

5.1. 使用小组件

本部分包含以下主题：

- 添加小组件
- 安排小组件
- 编辑小组件
- 查看通知
- 报告
- 审计跟踪

仪表板显示已注册设备和用户的重要统计数据。 仪表板上的各个部分称作小组件。 对于每个小组件，您可以定义：

- 显示数据的类别（如设备或用户）
- 如何对数据进行分组（如按照操作系统版本或模型）
- 如何筛选数据（如仅显示 iOS 设备）
- 如何显示数据（例如饼图或条形图）

添加小组件

1. 单击**添加**（右上角）。
2. 为小组件分配名称。
3. 选择数据类别。
4. 完成它们显示的过滤选项。
5. 选择默认显示类型（如饼图、条形图、折线图）。
6. 单击**完成**。

安排小组件

小组件通常一行显示三个。 然而，您可更改小组件的显示顺序。

1. 点击**排列**（右上角）。
2. 按照小组件出现的顺序将框拖放到位。
3. 单击**确定**。

编辑小组件

1. 单击小组件的设置图标（右上角）。
2. 选择**编辑**。
3. 做出更改。
4. 单击**完成**。

查看通知

单击钟表图标（右上角）或转到**仪表板 > 通知**页面，以查看通知并根据以下条件采取必要措施：

- 组件类型
  - 应用程序
  - LDAP
  - Entra ID
  - 设备允许列表
  - App 和图书
  - iOS
  - Android
  - macOS
  - visionOS
  - watchOS
  - tvOS
  - 租户
  - CA
  - 连接器
  - 卫士
  - 设备注册服务器令牌

通知类型

  - 失效
  - 数据同步
  - 使用限制
  - 管理员操作
  - 服务器身份验证错误
  - 验证错误
  - 状态更改

严重等级

  - 已清空
  - 信息
  - 关键
  - 警告

管理员可以选择 APP 组件，以在“通知”页面上和钟表通知部分中快速查看所有特定于应用的通知。 如果 Google Play 应用接受的新权限，则管理员可在单击通知（而不是访问每个应用页面）时接受，以查看并接受权限。

> Ivanti Neurons for MDM 客户/租户将获取 Android Go 应用批准通知，即使 Android Go 应用没有导入应用程序目录。

查看用户密码到期和 ID 更改通知

管理员可以在**通知**页面中查看即将到来的密码过期。 他们还可以提前两周到一天得到密码到期通知，包括包含相应用户列表的 CSV 报告文件的链接。 在密码过期后，将不再生成通知。

管理员还可以查看列出用户的通知，此类用户的 ID (UID) 在最后一次 LDAP 同步期间检测到已经更改。

清除通知

您可以根据需要从**通知**页面手动清除任何严重性的这些通知。

1. 在**通知**页面中，针对您要删除的通知，单击与该通知对应的**操作**列中的图标。 将显示**确认清除通知**窗口。
2. 单击**清除通知**。 清除后，**状态**列中的通知状态更改为**已清除**。

> **通知**页面将显示已清除的通知总数。

报告

在**仪表板 > 报告**页面中，您可以访问 Unified Endpoint Management (UEM) 系统中的数据。 例如，在创建设备和屏蔽的设备报告时，管理员可以使用相应的筛选选项，将设备空间名称和设备自定义属性等信息添加到报告。 相应地，这些报告分别具有设备空间名称和设备自定义属性的列。 在创建报告时，自定义设备属性在筛选选项中可用。 管理员可以从用于设备的自定义设备属性密钥列表中选择，并选择可用运算符。

从 Ivanti Neurons for MDM 76 版本开始，所有报告模板的运算符均含标准运算符。 在此版本中，以下模板的运算符将标准化：

- 仪表板 > 报告 > 创建报告

以下是报告的工作流程：

1. 选择 - 从预定义的报告模板中进行选择。
2. 定义范围 - 设置报告数据的时间段。
3. 设置详细信息 - 命名并自定义您的报告。
4. 运行或计划 - 立即运行报告或创建计划。
5. 共享 - 指定报告接收者。

相关主题：

- 仪表板 > 报告（已计划）
- 仪表板 > 报告（自定义）

快速搜索：导航到报告选项卡。 快速搜索字段支持您从以下列搜索，即使包含空格或特殊字符，也可以搜索：

- 名称
- 说明
- 模板名称

审计跟踪

审计跟踪提供在 Ivanti Neurons for MDM 中执行的活动的时间顺序记录。 这些记录包括管理员、最终用户和系统组件执行的操作。

管理员使用**审计跟踪**来审查更改、验证操作、排除问题和支持合规性检查。 **审计跟踪**跟踪添加、更新和删除托管实体等操作，包括设备。 有关详细信息，请参阅设备注册（iOS、macOS 和 Android）。

启用审计跟踪

您需要启用**审计跟踪**选项，以捕获在 Ivanti Neurons for MDM 中执行的活动。

步骤

1. 转到**管理员** > **基础设施** > **审计跟踪**。
   随即显示**审计跟踪**窗格。
2. 选择**审计跟踪导出**切换按钮并将其设置为开。

> 启用后，您将无法禁用审计跟踪选项。 要禁用，请联系 Ivanti 支持。

查看审计跟踪

按照步骤查看有关**审计跟踪**的更多详细信息：

步骤

1. 转到**仪表板** > **审计跟踪**。

随即显示**审计跟踪**窗格。

2. 下表列出了显示在**审计跟踪**窗格中的详细信息：

设置	说明
图标	显示审计事件的活动图标。
活动	显示发生的操作，例如设备签入或管理员登录。
状态	显示活动是成功还是失败。 如果报告失败，您可以从**报告历史记录**中重试报告作业。 使用此选项可在不创建新报告计划的情况下重新运行失败的作业。
执行者	显示执行活动的管理员或用户。
执行时间	显示活动发生的日期和时间。
执行于	显示受活动影响的设备、账户或对象。
详细信息	显示有关活动的其他信息。
类型	显示活动类型，例如设备操作或账户。
类别	显示与活动相关的功能区域，例如设备管理或管理员门户访问。

3. 单击**操作**按钮可执行以下选项：

- **配置审计跟踪设置**：选择此选项，它会在**管理员** > **基础设施** > **审计跟踪**中显示**审计跟踪**配置。
- **导出到 CSV**：选择此选项可导出和下载**审计跟踪**。

4. （可选）您可以使用**筛选器**查看特定的**审计跟踪**。

活动详细信息视图

更改 - 之前和之后图标显示在**仪表板** > **审计跟踪** > **详细信息**列中。 它可帮助管理员比较审计操作前后的属性值。 通过此比较可以更轻松地识别更改的内容、验证用户或系统活动，以及排除配置更新的故障。

单击该图标，在**审计跟踪更改 - 之前和之后**窗格中查看审计跟踪比较详细信息，并显示以下详细信息：

设置	说明
属性	显示修改后属性的名称。 例如，`createdAt`。
之前	显示执行操作前的属性值。 以红色突出显示。
之后	显示执行操作后的属性值。 以绿色突出显示。

审计跟踪的高级搜索

使用高级搜索选项根据规则搜索审计跟踪。 定义特定标准，以识别和查看活动。 您可以使用以下属性来执行高级搜索：

- **活动**
- **类别**
- **创建时间**
- **执行者**
- **执行于**
- **空间名称**
- **状态**
- **类型**

创建审计跟踪报告

您可以计划每 12 小时或 24 小时运行**审计跟踪**报告，或生成自定义报告。 此外，您可以按需运行**审计跟踪**报告。 未计划按需报告，并包括过去 24 小时的**审计跟踪**数据。

您可以生成以下格式之一的审计跟踪报告：

- CSV
- JSON
- CEF

此外，在为**审计跟踪** > **报告分发**创建报告时，您可以选择 **SFTP 导出**选项将所有审计跟踪信息导出和上传到特定服务器位置。 审计跟踪导出使用安全外壳文件传输协议 (SFTP)。 服务器必须通过默认端口访问。 您可以配置**审计跟踪导出**设置，以便每天自动将审计跟踪存档上传到特定位置。 有关更多信息，请查看导出审计跟踪。

有关创建报告的详细信息，请参阅使用计划的报告和使用自定义报告。

5.2. 应用见解

本部分包含以下主题：

- 查看应用分发
- 查看应用详细信息
- 添加单个应用分发图表
- 添加未托管的 iOS 应用图表
- 添加前 10 个已安装的受管应用
- 添加评分排名前 5 位的内部应用

应用见解是一项仪表板功能，可帮您查看并分析以下应用分发：

- 内部应用分发需要安装
- 公共应用分发需要安装
- 未托管的 iOS 应用
- 前 10 个安装的受管应用程序
- 评分排名前 5 的内部应用

分析前 5 个应用需要安装：已将内部或公共应用分发到大量用户，但安装率相应地较低。 未托管的 iOS 应用图表提供了设备上非托管应用的信息。 您将能够查看未托管应用的列表、安装在哪些设备上，并采取措施将应用转换为托管应用。 这些是需要管理员注意或采取行动来改进分发的应用分发。 这些图表表示已安装应用的设备。 圆环图提供公共和内部应用的高级别概览，这不仅有助于分析需要应用安装的设备数量，而且也允许您通过单击图表特定区域进一步深入了解，以获取更加具体的应用信息。 此外，您也可以添加一个分发图表，以表示单个应用的版本特定分发情况。

> 仪表板仅显示过去 15 天内签入设备的相关信息。

查看应用分发

在**应用**页面中，您可在**仪表板**中查看以下图表：

- 内部应用分发需要安装
- 公共应用分发需要安装
- 未托管的 iOS 应用

默认情况下，显示 5 个内部应用、5 个公共和未托管的 iOS 应用的图表。 图表从左到右排序，并从卸载率最高的应用开始。

圆环图显示 2 个颜色，以表示安装状态。 蓝色表示已安装应用的设备数量。 红色表示需要安装的设备数量。 如果您将鼠标悬停在每个颜色区域上方，将显示设备计数。

通过单击图表右上角的删除选项，您可以删除图表。

查看应用详细信息

圆环图的中心也会显示需要安装的设备数量。 示例：750/1000 表示 1000 个设备中共有 750 个设备需要安装。

圆环图显示 3 种颜色，以表示应用的分发情况。

- 蓝色表示已安装应用的设备数量。 单击图表中的蓝色区域会导航到**设备**页面。 在**设备**页面中，**应用版本**列会显示已安装应用的版本和应用的安装日期。

> 也可以从左侧面板的**版本**部分中选择选项，从而根据已安装应用版本查看设备。

- 红色表示需要应用安装的设备数量。 单击图表中的红色区域会导航到**设备**页面。 在**设备**页面中，您可以查看需要安装应用的设备。

图表中心将显示应用图标。 在单击图标时，将导航到**应用 > 应用目录**中的应用详细信息页面。

在此页面中，单击**已安装应用的设备**选项卡，以查看选定应用的设备列表。

单击**未安装应用的设备**选项卡，以查看没有为选定应用安装的设备列表。

添加单个应用分发图表

您可在“应用”页面中为特定应用版本添加单个分发圆环图。 红色表示应安装应用的合格设备列表。 这些图表形象地表示以下应用分发的详细信息：

- 安装应用特定版本的设备
- 安装其他应用版本的设备
- 未安装应用的设备

步骤

1. 单击**应用**页面中的 **+ 添加**。 将显示**添加应用图表**窗口。
2. 在**图表类型**下拉列表中，选择**单个应用分发**。
3. 选择您想要查看单个应用分发图表的应用列表复选框。

> 或者，通过在搜索应用字段中键入应用名称，您可以搜索特定应用。

4. 单击**添加图表**。 单一应用分发图表将显示在“应用”页面中。

> 您可以从列表中最多选择 9 个应用。

图表中心将显示已安装特定应用版本的设备数量。

示例：5/10 表示 10 个设备中的 5 个设备已安装特定应用版本。

圆环图显示 3 种颜色，以表示应用的分发情况。

- 绿色表示已安装应用特定版本的设备数量。 单击图表中的绿色区域会导航到**设备**页面；该页面将显示已安装应用特定版本的设备列表。 通过从左侧 **AppVersion** 部分中选择选项，您也可以根据其他已安装应用版本查看设备。
- 淡绿色表示已安装其他应用版本的设备数量。 单击图表中的淡绿色区域会导航到**设备**页面；该页面显示已安装应用其他版本的设备列表。 通过从左侧 **AppVersion** 部分中选择版本选项，您也可以根据其他已安装应用版本查看设备。
- 红色表示未安装应用的设备数量。 如果您将鼠标悬停在每个颜色区域上方，将显示设备计数。 单击图表中的红色区域会导航到**设备**页面，您可在其中查看未安装应用的设备。 左侧面板也会显示应用在应用目录中可用时的日期。

图表中心将显示应用图标。 在单击图标时，将导航到**应用 > 应用目录**中的应用详细信息页面。 在此页面中，单击**已安装应用的设备**选项卡，以查看选定应用的设备列表。 单击**未安装应用的设备**选项卡，以查看没有为选定应用安装的设备列表。

通过单击图表右上角的删除选项，您可以删除图表。

添加未托管的 iOS 应用图表

通过将未托管的 iOS 应用图表添加到“应用”页面，您可以识别并查看未托管应用列表。 此图表在管理员将未托管 iOS 应用添加到目录时自动显示。 管理员可以根据需要删除或添加此图表。

步骤

1. 单击**应用**页面中的 **+ 添加**。 将显示**添加应用图表**窗口。
2. 在**图表类型**下拉列表中，选择**未托管的 iOS 应用**。
3. 单击**添加图表**。 **应用**页面将显示未托管的 iOS 应用图表。

该图表显示 App Catalog 中未托管的应用数量。 图表底部显示 3 列，提供以下详细信息:

- **具有未托管 iOS 应用的设备** - 指示未托管 iOS 应用的数量。 单击链接，在“具有未托管 iOS 应用的设备”窗口中查看具有未托管应用的设备的列表。
- **App Catalog 中的应用总数** - 显示 App Catalog 中可用的应用总数。
- **未托管 iOS 应用 (%)** - 以百分比表示未托管 iOS 应用。

如果某个应用已经从 iTune App Store 安装，您可以将该应用及其数据转换为托管应用。要将此类应用转换为托管应用:

1. 单击**具有未托管 iOS 应用的设备列**中的数字链接。 将显示**未托管的 iOS 应用**窗口。
2. 从列表中选择一个或多个未托管应用，然后单击未托管的 iOS 应用下方的数字链接。 选定的应用将转换为托管应用，并且状态将在下次设备签入时更新。

> 可以通过点击**导出到 CSV** 链接，将非托管应用上的数据导出为 CSV 格式。

添加前 10 个已安装的受管应用

通过使用“应用”页面中的前 10 个已安装的托管应用，您可以标识并查看前 10 个已安装的托管应用。 管理员可以根据需要删除或添加此图表。

默认情况下，前 10 个已安装的托管应用图表在**应用**页面中可用。 如果删除图表，管理员可从**应用**页面添加。

步骤

1. 单击**应用**页面中的 **+ 添加**。 将显示**添加应用图表**窗口。
2. 在**图表类型**下拉列表中，选择**前 10 个已安装的托管应用**。
3. 单击**添加图表**。 **应用**页面将显示前 10 个已安装的托管应用图表。

根据在**显示**下拉列表中选择类别，您可以查看前 10 个已安装的托管应用。 可用类别分别是：

- **所有应用**（默认选择）
- **内部应用**
- **公共应用**

在图表中显示的每个条形图代表每个特定应用，也显示应用名称。 将鼠标悬停在每个条形图上，以查看平台（Android、iOS 或 Windows）和安装应用的设备数量。

单击特定应用的条形图会导航到**设备**页面，并显示安装应用的设备详细信息。 设备页面的左侧面板表示安装应用的设备数量。 单击左侧面板中的 X 按钮会导航回仪表板中的**应用**页面。

通过单击图表右上角的删除选项，您可以删除图表。

添加评分排名前 5 位的内部应用

通过使用“应用”页面上评分前 5 位的内部应用图表，您可以标识并查看评分排名前 5 位的内部应用列表。 管理员可以根据需要删除或添加此图表。

默认情况下，评分排名前 5 位的内部应用图表在**应用**页面中可用。 如果删除图表，管理员可从**应用**页面添加。

步骤

1. 单击**应用**页面中的 **+ 添加**。 将显示**添加应用图表**窗口。
2. 在**图表类型**下拉列表中，选择**评分排名前 5 位的内部应用**。
3. 单击**添加图表**。 **应用**页面将显示评分排名前 5 位的内部应用图表。

通过应用的徽标及其星级评分，此图表代表数据。 星级评分由星形图像及整数表示（最高评分为 5 颗星）。 此外，也将显示评分应用的用户数量。

> 应用的评分数量不仅局限于管理员和空间的设备，而且也取决于应用的所有用户提供的评分。 评分是在注册设备上从 Apps@Work 查看应用的不同用户对应用全部评分的平均数。

单击特定应用会导航到显示应用特定详细信息的**应用详细信息**页面。

通过单击图表右上角的删除选项，您可以删除图表。

5.3. 使用计划的报告

许可证：Silver

该计划报告功能可让您使用预封装模板，根据多种指标计划并生成报告。 您必须具有系统管理员或系统只读角色，才能访问此功能。 目前最多可以创建 40 份报告。

> 如果设备为其创建多个 Tunnel 实例，策略违反报告可能包含相同设备的多个记录。 这适用于标准报告与自定义报告。

生成报告

可以计划和生成报告。

步骤

1. 前往**仪表板** > **报告**。
2. 单击**创建报告**，以显示“选择报告模板”页面。
3. 从您配置的选项中，为您的报告选择模板。
   - **受阻设备**：目前访问受到 Sentry 阻止的设备报告。
   - **设备**：报告所有系统分区中的设备。
   - **策略违反**：系统中的违反策略报告。
   - **用户**：系统中的用户报告。
   - **用户密码到期状态**：系统中用户密码到期状态报告。
   - **安装最多的应用程序**：报告系统中的所有应用，并根据每个应用的安装次数进行排序。
   - **未托管的应用**：报告系统内未托管的应用程序。
   - **所有应用程序**：报告您管理的设备中的所有应用程序。
   - **审计跟踪**：Ivanti Neurons for MDM 中所有实体上执行的所有活动的报告。
4. 单击**下一步**。
   随即显示**报告详细信息**页面。
   - 输入**报告名称**。
   - （可选）为报告输入**描述**。

从以下选项中选择**事件范围**：
对于现有报告：

- **所有事件**
- **前一天**
- **上一周**
- **上一月**
- **前一范围** - 显示使用范围滑块从以前的 Ivanti Neurons for MDM 管理门户版本中创建的报告。 如果管理员针对报告选择并保存上述任一选项，则将不显示“前一范围”选项。 范围值可以在“报告摘要”页面中查看。

对于新报告：

- **所有事件**

- **前一天**
- **上一周**
- **上一月**

单击**下一步**。 随即显示“报告数据”页面。

6. 点击**自定义列**可添加、删除或重新排序**报告列**部分的列。 而点击列名称可删除添加的列。
7. （可选）使用**选择所有列**复选框，选择列表中显示的所有列。
8. 单击**恢复默认设置**，以还原为此前生成的列。 要还原为没有任何自定义的列，您可以从**选择报告模板**页面中选择其中一个模板。
9. 基于**高级筛选器**部分中的特定规则创建筛选器。

> 并非所有筛选器选项都适用于所有报告。 有关可用筛选器列表的详细信息，请参阅此步骤下的筛选器主题。

> 在创建报告时，以下新的硬件属性可用于 Windows 设备 - BitLocker 加密、操作系统版本、系统版本、主板制造商、主板产品、主板状态、BIOS 制造商、BIOS 版本、硬盘分区、光驱类型、CPU 名称和 CPU 状态。

10. （可选）点击 **+** 图标添加另一个规则或点击**添加组**图标添加另一组规则。
11. 单击**下一步**。 随即显示“报告计划”页面。
12. 选择以下其中一*种*格式来下载报告：
    - CSV
    - PDF
    - **CSV 和 PDF**
      对于 PDF 报告文件，最多允许 10 列。 “报告图表”部分会显示 PDF 报告中将包含的两种图表类型。
      所有应用报告仅支持 CSV 格式。

点击**自动计划**，设置为按周期自动运行报告。 或者，点击**手动**运行一次报告，随后报告将通过电子邮件发送。

- 选择一个**定期报告**选项：
  - **每天**
  - **每周**
  - **每月**
  - **前一计划** - 对于现有报告
- 选择**开始日期**和**结束日期**（可选）。

14. 单击**下一步**。 随即显示“报告分发”页面。 选择报告的收件人。
15. （可选）点击**添加外部电子邮件**链接添加外部电子邮件 ID。
16. 单击**完成**。 随即显示**报告分发摘要**。
17. （可选）点击**编辑**可修改报告。
18. 单击**保存**。
19. 点击“下载”图标可选择报告的格式。 系统将向报告的接收者发送包含**下载报告**按钮（用于下载报告）的电子邮件。

筛选器

规则选项	说明
激活锁定已启用	基于已启用激活锁定的规则为**是**或**否**。 规则示例：“激活锁定已启用等于是”。
应用程序隧道状态	应用程序隧道状态的规则为**阻止**或**允许**。 规则示例：“应用程序隧道状态等于阻止”。
电池电量	设备的电池电量值。 规则示例：“电池电量等于 1080” 为电池电量输入的值应以秒为单位。
客户端上次签入	基于日期范围中客户端上次签入的规则。 规则示例：“客户端上次签入的范围 04/02/2019 06:00:00,04/05/2019 17:00:00”。
合规状态	基于合规状态的规则为**是**或**否**。 规则示例：“合规状态等于是”。
当前国家/地区名称	输入当前国家/地区名称。 规则示例：“合规状态等于法国”。
当前 MCC	基于当前移动设备国家/地区代码的规则。 规则示例：“当前 MCC 等于 410”。
当前 MNC	基于当前移动网络代码的规则。 规则示例：“当前 MNC 等于 06”。
已启用设备注册	基于设备注册的规则启用为**是**或**否**。 规则示例：“已启用设备注册等于是”
防网络钓鱼本机状态	选择以下任意防网络钓鱼本机状态选项： • 等于 • 不等于 可能的值： • 未启用 • 不适用 • 已启用 • 未知
防网络钓鱼 VPN 状态	选择以下任意防网络钓鱼 VPN 状态选项： • 等于 • 不等于 可能的值： • 未启用 • 不适用 • 已启用 • 未知

规则选项	说明
注册设备注册	基于注册设备注册的规则启用为**是**或**否**。 规则示例：“注册设备注册等于是”
数据保护	指示是否在设备上启用数据保护。 可能的值是**是**或**否**。 规则示例：“数据保护等于是”
数据漫游已启用	基于已启用数据漫游状态的规则为**是**或**否**。 规则示例：“数据漫游已启用等于是”
设备块状态	基于设备块状态的规则。 规则示例：“设备块状态等于阻止”。
设备 ID	适用于特定设备 ID 或设备 ID 范围内的规则。 规则示例：“设备 ID 大于 45”。 x
家用 MCC	基于家用移动设备国家/地区代码的规则。 规则示例：“家用 MCC 等于 310”。
家用 MNC	基于家用移动网络代码的规则。 规则示例：“家用 MNC 等于 510”。
IMEI	适用于特定 IMEI 值的规则。 规则示例：“IMEI 以 9900 开头”
邀请状态	选择以下任意邀请状态选项： • 无 • 挂起 • 已过期 • **已完成** 规则示例：“合规状态等于待定”。
定位器服务已启用	基于已启用定位器服务的规则为**是**或**否**。 规则示例：“定位器服务已启用等于是”
MTD 激活状态	选择以下任意 MTD 激活状态选项： • 等于 • 不等于 可能的值是： • 不适用 • 错误 • 挂起 • 受保护
隔离状态	基于已启用定位器服务的规则为**是**或**否**。 规则示例：“隔离状态等于是”

规则选项	说明
注册时间	用于选择设备注册时的日期和时间范围的规则。 规则示例：“注册时间范围 10/03/2017 09：00：00,10 / 20/2017 17:00:00”。
漫游	基于漫游状态的规则为**是**或**否**。 规则示例：“漫游等于是”
状态	选择以下任意邀请状态选项： • 活动 • 停用挂起 • 停用已发送 • 已停用 • 停用已取消 • 擦除挂起 • 擦除已发送 • 已擦除 • 擦除已取消 规则示例：“状态等于停用待处理”。
语音漫游已启用	基于已启用语音漫游状态的规则为**是**或**否**。 规则示例：“语音漫游已启用等于是”
WIFI MAC 地址	输入特定的 Mac 地址值。 规则示例：“Wifi Mac 地址不等于 00-14-22-01-23-45”。
iCloud 备份已启用	基于已启用 iCloud 备份的规则为**是**或**否**。 规则示例：“iCloud 备份已启用等于是”
iTunes Store 账户激活状态	基于 iTunes Store 账户激活状态的规则为**是**或**否**。 规则示例：“iTunes Store 账户激活状态不等于否”。
平台类型	适用于所有应用程序报告。
来源	适用于所有应用程序报告。
自定义属性	适用于所有应用程序报告。
托管	适用于“所有应用程序”和“最常使用的应用程序”报告。
应用标识符	默认适用于“所有应用程序”报告。
Meid	适用于“非托管应用程序”报告。

在“计划报告”页面中对报告执行操作。

可在“计划报告”页面中执行各种操作。

步骤

1. 前往**仪表板** > **报告**。
2. 在**我的计划报告**页面中，点击**操作**下拉菜单，然后选择下列选项之一：

操作选项	执行的操作
查看	允许您查看报告。
编辑	允许您编辑报告。 您还可以使用报告查看上一版本中选择的范围，即“前一范围”。
立即运行	运行报告。
下载 CSV	以 CSV 格式下载报告。
下载 PDF	下载 PDF 格式的报告。
删除	删除报告。

查看报告详细信息

可以查看报告详细信息，并对创建的报告执行一些操作。

步骤

1. 前往**仪表板** > **报告**。
2. 在**我的计划报告**页面中，点击报告名称可查看报告详细信息。 随即将打开报告页面。
3. 可以在此页面上查看报告摘要和报告历史记录。

相关主题：

- 要为用户分配自定义角色，请参阅**分配角色**。
- 有关默认角色的列表，请查看**用户角色**。
- **角色管理**
- **使用自定义报告**

5.4. 使用自定义报告

许可证：Gold

该自定义报告功能可让您通过准备使用的模板，根据多种指标自定义并生成报告。 您必须具有系统管理员或系统只读角色，才能访问此功能。 目前最多可以创建 40 份报告。

本部分包含以下主题：

生成报告

对报告执行操作

查看报告详细信息

生成报告

可以从 Ivanti Neurons for MDM 管理门户计划和生成报告。

步骤

1. 前往**仪表板** > **报告**。
2. 单击**创建报告**，以显示“选择报告模板”页面。
3. 从配置的选项中，选择报告模板。
   - **受阻设备**：目前访问受到 Sentry 阻止的设备报告。
   - **设备**：报告所有系统分区中的设备。
   - **策略违反**：系统中的违反策略报告。
   - **用户**：系统中的用户报告。
   - **用户密码到期状态**：系统中用户密码到期状态报告。
   - **安装最多的应用程序**：报告系统中的所有应用，并根据每个应用的安装次数进行排序。
   - **未托管的应用**：报告系统内未托管的应用程序。
   - **所有应用程序**：报告您管理的设备中的所有应用程序。
   - **审计跟踪**：Ivanti Neurons for MDM 中所有实体上执行的所有活动的报告。
4. 单击**下一步**。 随即显示“报告详细信息”页面。
5. 输入**报告名称**。
6. （可选）为报告输入**描述**。
7. 从以下选项中选择**事件范围**：
   对于现有报告：
   - **所有事件**
   - **前一天**
   - **上一周**
   - **上一月**
   - **前一范围** - 显示使用范围滑块从以前的 Ivanti Neurons for MDM 管理门户版本中创建的报告。 如果管理员针对报告选择并保存上述任一选项，则将不显示“前一范围”选项。 范围值可以在“报告摘要”页面中查看。

对于新报告：

- **所有事件**
- **前一天**
- **上一周**
- **上一月**

单击**下一步**。 随即显示“报告数据”页面。

9. 单击**自定义**，以生成自定义报告：

> 在**仪表板 > 报告**页面中，“模板名称”列将显示括在括号中的“自定义”，表明该报告为自定义报告。

10. 点击**自定义列**可添加、删除或重新排序**报告列**部分的列。 而点击列名称可删除添加的列。
11. （可选）使用**选择所有列**复选框，选择列表中显示的所有列。
12. 单击**恢复默认设置**，以还原为此前生成的列。 要将列恢复到自定义之前的状态，可以从**选择报告模板**页面中选择模板。 默认列带有锁状图标。
13. 基于**高级筛选器**部分中的特定规则创建筛选器。

> 并非所有筛选器选项都适用于所有报告。 有关可用筛选器列表的详细信息，请参阅此步骤下的筛选器主题。

> 在创建报告时，以下新的硬件属性可用于 Windows 设备 - BitLocker 加密、操作系统版本、系统版本、主板制造商、主板产品、主板状态、BIOS 制造商、BIOS 版本、硬盘分区、光驱类型、CPU 名称和 CPU 状态。

14. （可选）点击 **+** 图标添加另一个规则或点击**添加组**图标添加另一组规则。
15. 单击**下一步**。 随即显示“报告计划”页面。
16. 选择以下其中一*种*格式来下载报告：
    - **CSV**
    - **PDF**
    - **CSV 和 PDF**
      对于 PDF 报告文件，最多允许 10 列。 在“报告图表”部分中，显示将包含在 PDF 报告中的两种类型的图表。
      所有应用报告仅支持 CSV 格式。

点击**自动计划**，设置为按周期自动运行报告。 或者，点击**手动**运行一次报告，随后报告将通过电子邮件发送。

- 选择一个**定期报告**选项：
  - **每天**
  - **每周**
  - **每月**
  - **前一计划** - 对于现有报告
- 选择**开始日期**和**结束日期**（可选）。

> “立即运行”选项将生成一次性报告。 您可以使用相同模板，以生成计划报告。 在**仪表板 > 报告**页面中，频率和下次计划列将显示这些报告的“取消计划”状态。

18. 单击**下一步**。 随即显示“报告分发”页面。 选择报告的收件人。
19. （可选）点击**添加外部电子邮件**链接添加外部电子邮件 ID。
20. 单击**完成**。 随即显示**报告分发摘要**。
21. （可选）点击**编辑**可修改报告。
22. 单击**保存**。
23. 点击“下载”图标可选择报告的格式。 系统将向报告的接收者发送包含**下载报告**按钮（用于下载报告）的电子邮件。

筛选器

规则选项	说明
激活锁定已启用	基于已启用激活锁定的规则为**是**或**否**。 规则示例：“激活锁定已启用等于是”。
应用程序隧道状态	应用程序隧道状态的规则为**阻止**或**允许**。 规则示例：“应用程序隧道状态等于阻止”。
电池电量	设备的电池电量值。 规则示例：“电池电量等于 1080” 为电池电量输入的值应以秒为单位。
客户端上次签入	基于日期范围中客户端上次签入的规则。 规则示例：“客户端上次签入的范围 04/02/2019 06:00:00,04/05/2019 17:00:00”。
合规状态	基于合规状态的规则为**是**或**否**。 规则示例：“合规状态等于是”。
当前国家/地区名称	输入当前国家/地区名称。 规则示例：“合规状态等于法国”。
当前 MCC	基于当前移动设备国家/地区代码的规则。 规则示例：“当前 MCC 等于 410”。
当前 MNC	基于当前移动网络代码的规则。 规则示例：“当前 MNC 等于 06”。
已启用设备注册	基于设备注册的规则启用为**是**或**否**。 规则示例：“已启用设备注册等于是”
防网络钓鱼本机状态	选择以下任意防网络钓鱼本机状态选项： • 等于 • 不等于 可能的值： • 未启用 • 不适用 • 已启用 • 未知
防网络钓鱼 VPN 状态	选择以下任意防网络钓鱼 VPN 状态选项： • 等于 • 不等于 可能的值： • 未启用 • 不适用 • 已启用 • 未知

规则选项	说明
注册设备注册	基于注册设备注册的规则启用为**是**或**否**。 规则示例：“注册设备注册等于是”
数据保护	指示是否在设备上启用数据保护。 可能的值是**是**或**否**。 规则示例：“数据保护等于是”
数据漫游已启用	基于已启用数据漫游状态的规则为**是**或**否**。 规则示例：“数据漫游已启用等于是”
设备块状态	基于设备块状态的规则。 规则示例：“设备块状态等于阻止”。
设备 ID	适用于特定设备 ID 或设备 ID 范围内的规则。 规则示例：“设备 ID 大于 45”。 x
家用 MCC	基于家用移动设备国家/地区代码的规则。 规则示例：Home MCC 等于 310。
家用 MNC	基于家用移动网络代码的规则。 规则示例：“家用 MNC 等于 510”。
IMEI	适用于特定 IMEI 值的规则。 规则示例：“IMEI 以 9900 开头”
邀请状态	选择以下任意邀请状态选项： • 无 • 挂起 • 已过期 • **已完成** 规则示例：“合规状态等于待定”。
定位器服务已启用	基于已启用定位器服务的规则为**是**或**否**。 规则示例：“定位器服务已启用等于是”
MTD 激活状态	选择以下任意 MTD 激活状态选项： • 等于 • 不等于 可能的值是： • 不适用 • 错误 • 挂起 • 受保护
隔离状态	基于已启用定位器服务的规则为**是**或**否**。 规则示例：“隔离状态等于是”

规则选项	说明
注册时间	用于选择设备注册时的日期和时间范围的规则。 规则示例：“注册时间范围 10/03/2017 09：00：00,10 / 20/2017 17:00:00”。
漫游	基于漫游状态的规则为**是**或**否**。 规则示例：“漫游等于是”
状态	选择以下任意邀请状态选项： • 活动 • 停用挂起 • 停用已发送 • 已停用 • 停用已取消 • 擦除挂起 • 擦除已发送 • 已擦除 • 擦除已取消 规则示例：“状态等于停用待处理”。
语音漫游已启用	基于已启用语音漫游状态的规则为**是**或**否**。 规则示例：“语音漫游已启用等于是”
WIFI MAC 地址	输入特定的 Mac 地址值。 规则示例：“Wifi Mac 地址不等于 00-14-22-01-23-45”。
iCloud 备份已启用	基于已启用 iCloud 备份的规则为**是**或**否**。 规则示例：“iCloud 备份已启用等于是”
iTunes Store 账户激活状态	基于 iTunes Store 账户激活状态的规则为**是**或**否**。 规则示例：“iTunes Store 账户激活状态不等于否”。
平台类型	适用于所有应用程序报告。
来源	适用于所有应用程序报告。
自定义属性	适用于所有应用程序报告。
托管	适用于“所有应用程序”和“最常使用的应用程序”报告。
应用标识符	默认适用于“所有应用程序”报告。
Meid	适用于“非托管应用程序”报告。

对报告执行操作

可在“计划报告”页面中执行各种操作。

步骤

1. 前往**仪表板** > **报告**。
2. 在**我的计划报告**页面中，点击**操作**下拉菜单，然后选择下列选项之一：

操作选项	执行的操作
查看	允许您查看报告。
编辑	允许您编辑报告。
立即运行	运行报告。
下载 CSV	以 CSV 格式下载报告。
下载 PDF	下载 PDF 格式的报告。
删除	删除报告。

查看报告详细信息

可以查看报告详细信息，并对创建的报告执行一些操作。

步骤

1. 前往**仪表板** > **报告**。
2. 在**我的计划报告**页面中，点击报告名称可查看报告详细信息。 随即将打开报告页面。
3. 选择下列选项之一

操作选项	执行的操作
切换	允许您启用或禁用报告。
立即运行	运行报告。
查看	允许您查看报告详细信息。 使用“操作”下拉菜单可执行下列任何任务： • **禁用** • **下载最新的 CSV/PDF**（根据所选择的报告类型，如 CSV、PDF 或 CSV 和 PDF，将显示“下载”选项） • **历史记录** • **删除**
删除	删除报告。

相关主题：

- 要为用户分配自定义角色，请参阅分配角色。
- 有关默认角色的列表，请查看用户角色。
- 角色管理
- 使用计划的报告

6. 用户

邀请其他人注册移动设备之前，您需要为此人创建一个用户条目。 对于将使用 Ivanti Neurons for MDM 帮助管理设备或发布内容的任何人，您也需要为其创建管理员用户。

本部分包含以下主题：

- 用户组
- 用户设置
- 用户加印品牌
- 使用 Apple 商务管理进行用户注册
- 帐户驱动的用户注册
- 用户许可证
- 管理用户

6.1. 添加用户

本部分包含以下主题：

- 添加用户
- 添加多个用户
- 通过上传文件添加多个用户
- 添加管理员
- 无人用户
- 查看设备注册 PIN 信息

您可同时添加一个或多个用户。 一旦您添加多个用户，您可能需要筛选显示内容以仅显示您感兴趣的内容。

在该页面，您可以和用户一起执行的其他操作包括：

- 分配至用户组/从用户组移除用户
- 发送消息
- 邀请注册
- 分配角色
- 更改密码
- 删除
- 生成 PIN

所有设备所有者配置文件都分配了设备账户。 设备账户对分配给它的设备数量没有任何限制。 工作配置文件（员工拥有）被分配用户账户。

添加用户

步骤

1. 转到**用户**。
2. 单击 **+ 添加**（右上角）。
3. 选择**单个用户**。
4. 使用用户信息填写表单：
    - 电子邮件地址（必填）
    - 名字
    - 姓氏

> “用户名”字段显示您输入的电子邮件地址。 多数情况下，不可编辑默认值。 有关更多信息，请查看何时编辑用户名

    - 显示名称

> 如果您想更改用户的显示名称，编辑**显示姓名**字段的默认文本。

5. 如果您要分配密码，请在**密码**和**确认密码**字段中输入。
    - 如果您分配密码，您需要将密码告知用户以进行设备注册。

- 如果您未分配密码，用户将需要在设备注册过程中创建密码。

6. 从下拉列表中，选择**区域设置**。
7. 输入**受管 Apple ID**。 您可以将“appleid”包含为受管 Apple ID 的子域，以避免与现有 Apple ID 产生任何冲突。 例如，user@appleid.yourdomain.com。 子域必须是 Apple 商务管理中有效的已验证子域。

> 如果存在具有当前帐户受管 Apple ID 的活动用户注册的设备，无法使用不同受管 Apple ID 更新帐户。

（可选）分配一个或多个用户组。 当状态为“活动”和“待停用”的设备存在时，无法更新受管 Apple ID。

10. 如果您希望在邀请用户前设置其他功能，取消选中**立即发送该邀请**选项。 否则，在您单击**完成**时将会发送邀请邮件。
11. 单击**完成**添加用户。

对于 Android 设备，设备帐户专为单次使用的受管设备设计，其中一个本地服务帐户可用于注册大量设备。 在创建新用户时，必须启用**管理员 > Google > Android Enterprise** 下可用的 Android Enterprise 设备账户。 默认情况下，为设备所有者管理的 Google Play 账户注册启用设备账户（而不是用户账户）。

选中 **Android Enterprise 设备账户**复选框，向与此账户相关联的 Android Enterprise 工作托管设备注册自动分配 Google 设备账户。

编辑 Android 设备的本地或 LDAP 用户后，系统将在下次设备签入时，向与该用户关联的 Android Enterprise 设备所有者管理的 Google Play 账户设备分配设备账户，前提是满足以下条件：

- 通过选中 **Android 企业版设备帐户**复选框启用此功能。
- Android 设备上的 Go 应用版本为 47 及以上版本。

添加多个用户

步骤：

1. 转到**用户**。
2. 单击 **+ 添加**（右上角）。
3. 选择**多个用户**。
4. 默认情况下，您可以**手动**输入电子邮件地址。 输入或粘贴用户的电子邮件地址，以逗号分隔。
5. 示例：jdoe@mycompany.com, jsmith@mycompany.com, tjones@mycompany.com
   如果您希望在邀请用户前设置其他功能，取消选中**立即发送该邀请**选项。
6. 否则，在您单击**完成**时将会发送邀请邮件。
   单击**完成**添加用户。

通过上传文件添加多个用户

过程：

1. 转到**用户**。
2. 单击 **+ 添加**（右上角）。
3. 选择**多个用户**。
4. 选择**上传 CSV**。
5. 单击**下载 CSV 模版**。
6. 使用每个用户的以下信息编辑模版：

- 用户 ID（必填）
- 电子邮件地址（必填）
- 密码
- 名字
- 姓氏
- 显示名称
- 用户组
- 自定义属性

7. 此信息与添加单个用户时使用的信息相同。 请勿在文件中输入超过 10,000 个条目。
   保存文件。
8. 将其拖至上传区域或选择**上传 CSV** 以选择文件。
9. 显示上传的用户信息后，根据需要进行编辑。
10. 单击**下一步**（右下方）。
11. 如果不希望立即发送邀请，请选择**不发送邀请**。
12. 单击**完成**。

添加管理员

步骤：

1. 单击**添加**（右上角）。
2. 选择**单个用户**。
3. 使用用户信息填写表单：
   - 电子邮件地址
   - 名字
   - 姓氏
4. **用户名**字段显示您输入的电子邮件地址。
   如果您想更改用户的显示名称，编辑**显示姓名**字段的默认文本。
5. 在**密码**字段中分配密码。
6. 在**确认密码**字段再次输入密码。
7. 单击**完成**添加用户。
8. 将该密码告知帮助管理设备的人员。

无人用户

Nobody 用户是一个无法删除的默认用户。 该服务将用户用于没有关联用户的设备，如停用设备。

查看设备注册 PIN 信息

在添加新设备时，如果设备注册身份验证类型设置为仅限 PIN，则向管理员显示生成的注册 PIN 信息。 此信息可在帮助用户注册设备时非常有用。

- 对于一个用户，PIN 会通过**用户 > 邀请用户注册**部分显示，也会显示在“用户详细信息”页面的 PIN 信息部分中。

- 对于多个用户，除了 PIN 状态（有效或过期）、PIN 已发布和 PIN 过期列外，PIN 会作为列显示在“用户列表”页面中。

如果您无法在**用户**页面上执行任务，这可能是您没有所需权限。 您需要以下**角色之一**：

- 系统管理
- 用户管理

6.2. 用户组

本部分包含以下主题：

- 创建动态管理的用户组
- 创建手动管理的用户组
- 从其中一个重复用户组创建用户组
- 通过上传 CSV 文件创建用户组

创建一个用户组，以对多个用户分配应用和角色。 例如，如果您希望所有部门经理都是应用和内容的管理员，可以创建一个“经理”组。

您可以通过以下方法之一创建要管理的用户组：

- **动态管理（最常见）：**基于某些规则和/或属性，动态地将本地和 LDAP 用户添加到组/从组中删除。
- **手动管理（有限目的）：**手动将用户添加到组/从组中删除。 手动管理组仅推荐用于需要较少权限的测试目的。

您可以在**搜索**字段中输入文本，以显示名称以输入的文本开头的所有用户组的列表。

- 在输入文本时，搜索结果将实时显示为可能匹配项的列表。
- 从可能匹配项的列表中，选择所需的用户组名称，以便执行后续操作。
- 搜索匹配项区分大小写。

创建动态管理的用户组

> 以下程序不适用于动态用户组。

步骤

1. 点击 **+ 添加**。
2. 在**名称**字段中输入用户组名称。
3. （可选）单击**添加描述**，以便为用户组添加描述。
4. 单击**动态管理（最常见）**选项。
5. 按要求设置规则和/或属性。 以下是可用的规则选项：
    - 自定义 LDAP 属性
        - msExchPoliciesIncluded
        - msExchMailboxGrid
        - mailNickname

    默认 LDAP 属性

        - samAccountName
        - userPrincipalName

    默认用户属性

        - email_address
        - distinguished_name

- last_name
- display_name
- first_name
- 用户组
- 自定义用户属性

用户组 DN

- 用户组 GUID
- 用户组名称

6. 对于每个规则，在本地和 LDAP 用户之间进行选择。 您可以使用**用户组**筛选条件来包括或排除子组。
7. 通过单击加号图标添加更多规则。
   可以为添加的规则设置**任何**或**所有**条件筛选器。
8. 通过单击加号旁边的分层图标创建一组规则。
9. 在规则选择选项下的文本查询中查看用户组规则和属性。
10. 在**结果**部分，查看与配置的标准匹配的用户详细信息。 添加或修改规则或属性时，可以观察到匹配的用户是否显示（如果存在）。
11. 单击**保存**，保存已配置的用户组。

创建手动管理的用户组

1. 点击 **+ 添加**。
2. 输入组名。
3. （可选）单击**添加描述**，以添加描述。
4. 选择**手动管理（有限目的）**选项。
5. 在**搜索用户**字段中，输入要纳入组中的每位用户的电子邮件地址。
   在您输入时，系统会找到并显示匹配的用户（如果存在）。
6. 选择要添加到组中的用户。 您可以根据需要搜索并添加更多用户。
7. 单击**保存**。

> 您可以创建手动管理的用户组，然后将该组添加到动态管理的用户组。 在这种情况下，编辑手动管理的用户组不会破坏动态管理的用户组规则。 如果手动管理的用户组已添加到动态管理的用户组，则无法将其删除。

从其中一个重复用户组创建用户组

从 Neurons for MDM 127 开始，在规则生成器中选择“用户组名称”属性后，管理员门户会显示重复用户组的数量和相应的 GUID 数量，以便标识重复组。 此外，此规则下方的表会显示重复用户组的列表及其详细信息，例如用户组名称、GUID、来源和可分辨名称 (DN)。

步骤

1. 登录 Ivanti Neurons for MDM 管理员门户。
2. 转到**用户**，**用户组**。
3. 单击 **+ 添加**。 将打开创建用户组向导。
   1. 在**名称**字段中，指定名称。

2. 从规则生成器中选择**用户组名称**，选择**等于**，选择*其中一个*重复组名称。
3. 单击 **+** 加号图标，添加更多规则。
4. 选择**用户组 GUID**，**等于**。
5. 对于显示重复用户组名称和 GUID 列表的表，从中复制并粘贴 GUID。 结果将显示添加到新组的关联用户。
6. 单击**保存**。 现在，列出的用户已添加到创建的新用户组。

如果您无法在**用户组**页面上执行任务，这可能是您没有所需权限。 您需要以下[角色]之一：

- 系统管理
- 用户管理

通过上传 CSV 文件创建用户组

新添加的功能允许管理员使用 CSV 文件创建用户组并将用户添加到创建的组中。

步骤

1. 登录 Ivanti Neurons for MDM 管理员门户。
2. 转到**用户**，**用户组**。
3. 单击 **+ 添加**。
4. 选择**从 CSV 导入用户组**。 “导入用户组”向导随即打开。
    1. 在“下载 CSV”部分，点击**下载 CSV 模板**来下载 CSV 模板。 通过使用模板，可以编辑文件来创建用户组并将用户添加到新的/现有的用户组。
    2. 编辑并保存 CSV 文件后，点击**选择文件**来上传 CSV 文件。
    3. 单击**上传**。 上传成功后将显示确认消息。

属性	说明
CSV 文件大小限制	导入的 CSV 文件的上限为 2MB。
CSV 文件格式要求	CSV 文件应正好包含 2 列：accountUid 和 groupName。 • accountUid 和 groupName 的值均必填。 • 不符合这些标准的记录将在导入过程中删除。 管理员可以从导入部分下载示例 CSV 文件以供参考。
导入期间的错误处理	如果出现 CSV 导入错误或失败，则会生成错误文件。 • 管理员可以下载此错误文件来查看导入失败的 CSV 行并了解失败的原因。 • 错误文件包含导入失败的特定 CSV 行及原因说明。
导入成功的条件	仅在用户组是手动管理的本地用户组时，将用户导入用户组的操作才会成功。 • 用户必须在系统中才能成功导入。

创建用户组和添加用户的条件（含示例 CSV 文件）

示例 CSV 文件详细信息 -

accountUid：test_user_1@org.com

groupName：test_group_1

条件	说明
现有组	如果组 test_group_1 已存在，则用户 test_user_1@org.com 将与该组关联。
非现有组	如果组 test_group_1 不存在，则系统会创建一个名为 test_group_1 的新组，并将用户 test_user_1@org.com 与该组关联。
非本地组	如果组 test_group_1 已存在但不是本地组，则此记录将纳入错误 CSV 文件，错误原因为“不是本地组”。
非手动管理组	如果组 test_group_1 已存在但不是手动管理的组，则此记录将纳入错误 CSV 文件，错误原因为“不是手动管理的组”。
非现有用户	如果用户 test_user_1@org.com 不存在，则此记录将纳入错误 CSV 文件，错误原因为“找不到用户”。
非现有用户和组	如果用户 test_user_1@org.com 和组 test_group_1 都不存在，则系统会创建一个名为 test_group_1 的新组，同时，此记录将纳入错误 CSV 文件，错误原因为“找不到用户”。

6.3. 用户设置

本部分包含以下主题：

- 编辑默认设置
- 添加自定义设置
- 删除自定义设置
- 为新设备注册配置设置
- 配置每个用户的设备限制
- 配置设备擦除限制
- 用户设置
- 配置自助门户身份验证
- 设置密码复杂度
- 定义服务条款
- 配置用户邀请提醒电子邮件
- 配置用户注册确认电子邮件
- 配置用户工作计划设置
- 配置管理门户身份验证设置

用户设置定义了设备注册选项。 有以下几种类型：

- **设备注册设置**：设置通过密码、PIN 或两者进行身份验证；Apple 注册类型和设备所有权。
  - 此前，如果您设置 SAML 身份验证/IdP，SAML 身份验证将用于设备注册和门户身份验证。
  - **平台设备注册设置** - 管理员现在可以通过限制特定的 Apple、Android 和 Windows 平台向系统注册来控制操作系统级别的设备注册。 此新的操作系统级别限制设置将用作父注册控制，当为平台启用时，该平台的相关注册限制将自动禁用。 这有助于组织执行注册策略，并防止不受支持的设备平台被注册。

设备限制设置：设置每位用户可以注册的设备数量。

- **擦除限制设置**：设置一次可以擦除的最大设备数量限制。
- **自助门户身份验证设置：**设置自助门户的密码身份验证类型。
- **密码复杂性设置**：设置用于设备注册的本地帐户的密码复杂性和策略参数，以及管理员门户和自助服务门户的访问权限。
- **服务条款设置**：设置每次设备注册时向用户显示的服务条款。
- **用户邀请提醒设置：**设置发送用户邀请提醒电子邮件的日期和频率。
- **用户注册确认设置：** 控制发送用户注册确认电子邮件的功能。 有关解决方案的概述，请查看配置和使用注册确认电子邮件；有关特定用户设置说明，请查看下方配置用户注册确认电子邮件。
- **用户工作计划设置：**控制配置用户工作计划的功能；这将阻止在规定的非工作时间内从 Sentry 到托管设备的所有通信。 对施行离线权法律的区域有用。
- **管理门户身份验证设置：**控制 Ivanti Neurons for MDM 是提示管理员仅输入密码，还是提示管理员同时输入密码和 PIN。

您可为**所有用户**组编辑默认设置，或添加自定义设置并将其分配至其他用户组。

编辑默认设置

单击具有锁定图标的设置的**编辑**链接。 您无法删除默认设置。

添加自定义设置

单击**为特定用户组添加设置**链接。

删除自定义设置

单击 X 图标。

为新设备注册配置设置

您可以为新设备注册配置最低操作系统版本、身份验证类型和设备所有权。 Ivanti Neurons for MDM 早期版本生成的设备注册 URL 将不再适用于当前版本。 管理员将需要重新生成设备注册 URL。

允许列表设备注册

将设备注册加入允许列表的选项仅在默认用户设置中可用，不适用于自定义用户设置。 您可以使用包含序列号和自定义设备属性的模板上传 CSV 文件，这些属性用于将一些设备加入允许列表。 您可以包含一个或多个现有自定义设备属性，创建允许列表。 这将使您能够在注册后将属性分配给设备组或空间。

要创建自定义属性，请转到**管理 > 属性**。 如果启用允许列表功能，并且 CSV 文件未提及设备序列号，iOS 和 macOS 设备不允许通过 iReg 注册。 如果 CSV 文件包含重复的序列号，则 CSV 文件中的最后一个条目将被考虑，并且与该条目相关联的自定义设备属性将被考虑用于注册期间的设备分配。

如果**设备允许列表**选项已启用，则仅允许已加入允许列表的设备向 Ivanti Neurons for MDM 注册。 此功能仅适用于通过基于 Web 的注册流程进行注册的设备。 这不会影响已经注册 Ivanti Neurons for MDM 的设备。 注册后，如果设备序列号从 CSV 文件中删除，设备将不会停用。 CSV 文件中提到的用户是可选项，只有当 CSV 文件中提到该用户并且该用户是有效用户时，才可以分配该用户。

如果要上传新的 CSV 文件，可以删除现有 CSV 文件并上传新文件。 仅 iReg 支持允许列表；如果需要 Go 客户端，选择零接触注册。 为了使 AppConnect 和威胁防御等功能发挥作用，应在系统上安装 Go 客户端。 因为我们不支持应用内注册，所以用户可以首先通过 iReg 注册设备，然后，Go 应用可以从 App Catalog 推送到设备。 当用户接受安装应用程序时，设备将成为托管设备，并且所有功能将在注册后继续使用。 对于 AppConnect 处于活动或非活动状态的设备，无法在其中使用零接触配置。 仅可在 AppConnect 状态为无时使用。 在通过 iReg 注册后，AppConnect 状态在设备上启动 Go 客户端之前仍为无。

步骤

1. 登录 Ivanti Neurons for MDM。
2. 转到**用户 > 用户设置**。
3. 在**设备注册设置**下，点击 **+ 添加用于特定用户组的设置**。
4. 编辑默认**设备注册身份验证类型**设置，或添加新设置。
5. 在**名称**字段中输入名称。
6. （可选）输入设置描述。
7. 在 **OS 设置**部分中，定义 iOS、macOS 或 Windows 的最低 OS 版本：
8. 选择**启用最低版本**切换按钮，然后从下拉列表中选择操作系统版本。

> “启用最低版本”设置不适用于 DEP 设备注册。

对于 **Android**：

- 启用**最低安全修补程序**选项（仅限 Android），并通过从以下下拉列表选项中选择持续时间类型指定时期：
  - **天**
  - **月**
  - **年**

  启用**制造商允许列表/阻止列表**选项，并选择以下任何选项：
  - **创建允许列表** - 仅允许这些制造商的设备进行注册。
  - **创建阻止列表** - 仅阻止这些制造商的设备进行注册。
    添加制造商：
    1. 单击**添加制造商**。
    2. 在**制造商名称**字段中，键入制造商名称。
    3. 单击**保存**。 添加的制造商名称显示在表格中。

    > 制造商名称区分大小写。 要编辑或删除添加的制造商名称，单击制造商的**编辑**或**删除**选项。

在 Apple 注册部分中，选择 Apple 注册类型：

- **设备注册**
- **用户注册** - 默认情况下，用户注册适用于 iOS 和 iPadOS 设备。
- （可选）**包含 macOS 设备 (macOS 10.15+)** - 选择此选项，以使用户注册也适用于 macOS 设备。

在**注册邀请方法（仅限 iOS 和 Android）**部分中，启用 **MAM Only 注册**。

> 此选项应针对 MAM-Only 设备注册启用；在启用时，用户将重定向到公共 App Store，以下载 AppStation 客户端应用。

11. 在**设备注册身份验证类型**部分中，从**选择注册类型**下拉菜单中选择以下注册类型选项之一。 如果使用“设备注册”，请确保您的“设备注册”配置与选择相符。
    - **仅密码**
    - **仅 PIN** 选择此选项后，将锁定“绕过 IdP 设备注册身份验证”切换按钮。
    - **密码和 PIN**

      > 用户仍可以收到 PIN，以完成帐户激活。

> 此设置会影响正常注册和设备注册注册。

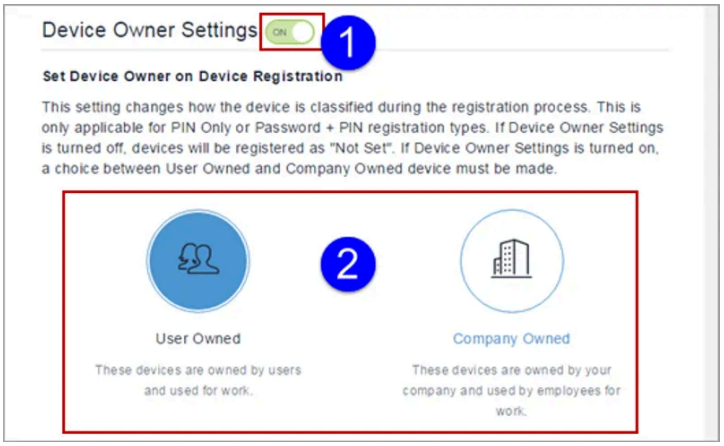
对于 PIN，请指定以下信息。 在设备注册期间，用户可以单击**重新发送 PIN**（如果需要）。

- **PIN 有效期限**：PIN 保持有效的时间（1-30 天）。
- **PIN 长度**：字符数 (4-12)。
- **允许用户请求新 PIN**（忘记或过期时）。

您还可以选择打开**设备所有者设置**，单击**用户所有**或**公司所有**。 此设置会更改如何在注册过程中分类设备。

- 如果**设备所有者设置**开启，并且管理员已将设备标记为“用户所有”，则会在用户登录期间（也会从自助门户）向用户显示将设备标记为“用户拥有”或“公司拥有”的选项。 对于“用户注册”注册的设备，无论管理员做出何种选择，默认设备所有者设置都将是“用户所

有”。
- 对于监管的设备，设备所有者设置将是“公司所有”。



对于您希望向其分配设置的用户组，至少为一个用户组单击**+添加**。

15. （仅适用于 iOS 和 macOS 设备的按需功能）或者，打开**设备允许列表**选项，允许基于允许列表中的序列号进行设备注册。
16. 单击**下一步**。 系统将打开“用户设置分发”页面。
17. 选择用户组分发。
18. 单击**完成**。
19. 向用户发送邀请。 有关详细信息，请参阅邀请用户。

注意以下几点：

> 如果用户设备是使用“仅 PIN”选项注册的，用户会收到一封带 PIN 的注册确认电子邮件，用于身份验证。

- PIN 会发送到用户的电子邮件 ID。
- 用户在设备注册页面上输入 PIN。
- 如果 PIN 正确，用户会被重定向以完成注册过程。

对于使用基于 SAML 的身份提供程序 (IdP) 配置的用户，Ivanti Neurons for MDM 支持在设备注册时进行基于 PIN 的身份验证。 设备注册身份验证类型应是 PIN 或 PIN 和密码。 “PIN 和密码”功能用于双重身份验证，以提高安全性。 在此情况下，在此用户尝试注册设备时：

- PIN 会发送到用户的电子邮件 ID。
- 用户在设备注册页面上输入 PIN。
- 如果 PIN 正确，用户会重定向到 IdP 的登录页面，用户在其中输入 IdP 用户名和密码。
- 如果 IdP 凭据正确，用户会重定向到设备，以完成注册过程。

配置每个用户的设备限制

步骤

1. 编辑默认**设备限制**设置或添加一个限制。
2. （可选）单击 **+ 添加用于特定用户组的设置**为特定用户组配置设备限制。
3. 编辑或分配一个名称以识别设置。
4. 输入设置的可选描述。

5. 在**最大活动设备数**下拉列表中，选择活动 Apple 设备限制。
6. 在**与 iPhone 配对的 Apple watchOS 设备最大数量**下拉列表中，选择要与 iPhone 配对的活动 Apple watchOS 设备限制。
7. （可选）如果选择了 **+ 添加用于特定用户组的设置**，请单击**下一步**并为此设置的分发选择至少一个用户组。
8. 单击**完成**。

配置设备擦除限制

步骤

1. 编辑默认**设备擦除限制**设置。
2. 开启**为所有用户启用擦除限制（包含默认角色）**选项。
3. 在**用户一次可以擦除的最大设备数量**字段中，键入一次可以擦除的最大设备数量。 默认值为 1。 您可以将最大值 200 设置为设备擦除限制。
4. 单击**完成**。

配置自助门户身份验证

步骤

1. 通过单击 **+ 为特定用户组添加设置**，编辑默认**自助门户身份验证**设置或添加新设置。
2. 编辑或分配一个名称以识别设置。
3. 输入设置的可选描述。
4. 从下拉列表中，选择**自助门户身份验证类型**。 这可以是以下其中一个原因：
   - 密码
   - 证书
5. 单击**下一步**。
6. 选择将分发此配置的一个或多个用户组。
7. 单击**完成**。

设置密码复杂度

您可以设置用于设备注册的本地帐户的密码复杂性和策略参数，以及管理门户和自助服务门户的访问权限。

> 密码长度、字符及下方设置的策略定义了密码的安全性。

这也会定义与用户选择有效密码关联的难度。 如果您使用最终用户的本地帐户，并需要访问管理员门户的安全密码，请考虑定义设备注册的 PIN，以确保密码复杂性不会妨碍设备注册。 在**用户设置 > 设备注册设置**中，使用“设备注册身份验证”类型设置，以为设备注册选择身份验证模式。

步骤

1. 编辑默认**密码复杂性**设置。
2. 定义以下密码复杂性设置：

设置	采取何种措施
最低密码长度	移动滑块指定密码的最小长度，以防止用户创建简单不安全的密码。 数字范围介于 8 至 32。
必需特性	指定在您选择密码时应满足的密码特性数量。 特定的最少数量应设置为 3（对于联邦客户，设置为 4）。
必需特殊字符（符号）	指定密码应包含的非字母字符数量。
需要大写字母字符	指定密码应包含的大写字母字符数量。
必需小写字母	指定密码应包含的小写字母字符数量。
必需数字字符	指定密码应包含的数字字符数量。
密码验证	
允许的数字序列	选择序列中重复数字的数量。 示例：123。
允许的重复字符	选择重复字母字符的数量。 示例：bbc。

3. 设置以下密码策略设置，以自定义行为。

设置	采取何种措施
保留密码历史	移动滑块，以在使用旧密码之前选择必须与用户帐号关联的新密码数量。 数量范围介于 3 - 36 之间。
密码有效期	移动滑块，以选择密码过期持续时间（天数）。 数字范围介于 30 - 365 天之间。
不活动超时	移动滑块，以指定用户在管理员门户或自助服务门户会话时间前处于非活动状态的时间。 数量范围介于 5 - 60（分钟）之间。
登录失败阈值	移动滑块，以选择在 5 分钟帐号锁定生效前失败登录尝试次数。 数量范围介于 2 - 5 之间。 当失败尝试次数在阈值限制范围内，将在锁定时向用户显示消息，并稍后尝试登录。 当失败尝试次数超过阈值限制时，将在锁定时向用户显示消息，并在指定时间后（分钟）尝试登录。

4. 单击**完成**。 如果您更改密码复杂性默认设置，现有本地帐号的早期密码仍保持不变。 在过期时，将提示用户更新密码。 对于尝试登录管理员门户的管理员，可以联系在重置密码方面提供指导帮助的帮助台。

> 在设备注册中，建议使用仅 PIN 注册模式。

定义服务条款

步骤

1. 创建新**服务条款**设置。

2. 分配一个名称以识别设置。
3. 输入设置的可选描述。
4. 选择**提示用户**... 选项。
5. 输入要显示的标题和文本。
6. 对于您希望向其分配设置的用户组，至少为一个用户组单击**+添加**。
7. 单击**保存**。

> 在接受后，无法删除该服务条款。 但是，可以通过清除**提示用户**关闭新注册提示... 选项。

配置用户邀请提醒电子邮件

管理员可以通过使用此设置发送用户邀请提醒电子邮件来驱动设备注册。

步骤

1. 编辑现有**用户邀请提醒设置**或添加新设置。
2. 编辑或分配一个名称以识别设置。
3. 输入设置的可选描述。
4. 确保开启**用户邀请提醒**选项。
5. 在"定义开始和结束日期"区域中，选择何时启动和停止发送电子邮件提醒。

> 最多可以发送 30 封电子邮件。 要重置此限制，管理员应重新发送邀请。

6. 在"定义频率"区域中，选择要发送电子邮件提醒的频率。
7. 单击**下一步**。
8. 选择此配置的分配水平。
9. 单击**完成**。

配置用户注册确认电子邮件

管理员可以向完成注册的新用户发送电子邮件。

步骤

1. 编辑现有**用户注册确认设置**，或添加新设置。
2. 编辑或分配一个名称以识别设置。
3. 输入设置的可选描述。
4. 请确保打开**在用户注册成功后发送确认电子邮件**选项。
5. 单击**下一步**。
6. 选择此配置的分配水平。
7. 单击**完成**。

配置用户工作计划设置

管理员可以为用户配置用户工作计划，这会阻止在规定的非工作时间内从 Sentry 到托管设备的所有通信。 这对施行离线权法律区域的用户有用。

步骤

1. 选择**用户**。
2. 选择**用户设置**。
3. 在**用户工作计划设置**部分中，选择 **+ 为特定用户组添加设置**。
4. 请为设置提供名称。
5. 打开设置。
6. 选择时区。
7. 配置 Ivanti Neurons for MDM 阻止 Exchange ActiveSync 协议、启用 AppConnect 的应用和受管应用的小时数。
8. 单击**下一步**。
9. 配置分发，然后单击**完成**。

> 应用的更改可能需要 1 小时 15 分钟，才可以在设备上生效。

配置管理门户身份验证设置

管理员可以设置身份验证类型，以验证用户登录。 此设置会控制是否提示用户仅需密码或密码和 PIN。

步骤

1. 编辑现有**管理员门户身份验证设置**，或添加新设置。
2. 编辑或分配一个名称以识别设置。
3. 输入设置的可选描述。
4. 在**管理员门户身份验证类型**中，选择以下任一选项：

选项	描述
密码	选择此选项仅使用密码验证登录。 用户仍可以收到 PIN，以完成帐户激活。
密码和 PIN	选择此选项使用密码和 PIN 验证登录。 选择此选项后，将显示以下附加字段： • **PIN 寿命**：从下拉列表中选择 PIN 生命周期的分钟持续时间。 分钟应在 1 到 15 的范围内。 • **PIN 长度**：从下拉列表中选择 PIN 字符的长度。 PIN 长度范围应介于 4 到 12 之间。 此选项仅适用于本地帐户，不适用于 LDAP 管理员帐户。
允许用户请求一个新 PIN	选择此选项可允许用户请求新的 PIN。

5. 单击**下一步**。
6. 选择此配置的分配水平。
7. 单击**完成**。

对于使用基于 SAML 的身份提供程序 (IdP) 的用户，Ivanti Neurons for MDM 支持对管理门户进行基于 PIN 的身份验证。 管理员门户身份验证类型应是 PIN 和密码。 此功能会用作双重身份验证，以提高安全性。 在此情况下，在此用户尝试登录门户时：

- PIN 会发送到用户的电子邮件 ID。
- 用户在管理门户登录页面上输入 PIN。
- 如果 PIN 正确，用户会重定向到 IdP 的登录页面，用户在其中输入 IdP 用户名和密码。
- 如果 IdP 凭据正确，用户会重定向到管理员门户。

在登录管理员门户时，用户可以单击**忘记密码**，以重置密码。 在下一个屏幕中，用户可以输入发送到用户电子邮件地址的新密码和 PIN（根据之前用户身份验证模式设置提示）。 如果需要，请点击**重新发送 PIN**。 用户在两次"忘记密码"请求之间必须等待 15 分钟。

> 在此配置分发到设备时，用户使用密码或 PIN 连续不成功的登录尝试（默认值：5 次尝试）将导致帐户锁定，并在锁定时向用户显示一条消息。

6.4. 用户加印品牌

通过用户加印品牌，您可以使用用户认出的名称和徽标自定义设备注册流程。 您可以通过以下方式自定义面向用户的品牌加印：

- 为注册 URL 设置自定义主机名。
- 在注册邮件和注册屏幕内显示您的徽标
- 在注册活动中显示自定义网站图标

> 更新上述设置会更改 **$** 引用的值。

许可证：Gold

先决条件：

- 决定您在自定义 URL 中要使用的主机名。 其必须满足以下要求：
  - 无空格
  - 无特殊字符

获得满足以下要求的徽标文件：

  - PNG 格式
  - 580 x 80 像素

获得满足以下要求的网站图标文件：

  - PNG 格式
  - 64 x 64 像素

过程：

1. 转至**用户 > 用户品牌加印**。
2. 单击**自定义**（右上角）。
3. 在**主机名**字段中，键入用作 URL 中主机名的简短名称。
4. 单击**检查可用性**，以便确认您输入的主机名尚未被其他人使用。
5. 如果主机名不可用，请输入其他名称。
6. 请注意 **URL 预览**下生成的注册 URL。
7. 单击**下一步**。
8. 在**徽标**下，单击**选择文件**，将注册电子邮件和注册屏幕中要使用的徽标上传。
9. 单击**下一步**。
10. 在**网站图标**下，点击**选择文件**，然后上传要在注册活动期间在 Ivanti Neurons for MDM 网站图标处显示的网站图标。
11. 单击**完成**。

6.5. 使用 Apple 商务管理进行用户注册

本部分包含以下主题：

- 启用用户注册的要求
- 注册优先级
- 标准 MDM 注册与用户注册之间的差异
- 用户注册与设备注册之间的差异
- 连接 Ivanti Neurons for MDM 与 Apple 商务管理

适用于：

- Ivanti Neurons for MDM 支持的 iOS 13.0 至最新版本的未监管设备。
- 搭载 macOS 10.15 或支持较新版本 Ivanti Neurons for MDM 的设备。

Apple 商务管理是一款适用于 IT 团队的工具，并用于自动化设备部署、购买和分发内容，并管理组织中的角色。 Apple 商务管理实施用户注册，即专为实施 BYOD（自带设备）的公司而设计的注册选项。 用户注册是 MDM 协议的修改版本；该版本更注重用户隐私，并以企业所需的安全级别进行实施。

用户注册允许管理员执行以下操作：

- 安装和移除受管应用
- 安装和移除网络配置
- 安装扩展到受管应用和帐户的部分 VPN
- 需要使用密码

启用用户注册的要求

以下是启用用户注册的要求。 如果未满足其中任意要求，注册类型将是设备注册。

- 搭载 iOS 13.0 至 Ivanti Neurons for MDM 支持的最新版本的非受监管的设备，或搭载 macOS 10.15 或支持的较新版本 Ivanti Neurons for MDM 的设备。
- Apple 注册类型的用户设置字段应设置为“用户注册”。
- Apple 商务管理帐户。
    - Apple 应用许可证帐户需要是相同 Apple 商务管理帐户的一部分。
    - 在 Apple 商务管理中，如果您的帐户列在“位置”中，您需要将 App 和图书匹配到同一个位置。 您可能需要添加一个新位置（例如，西海岸）。

受管 Apple ID - 与每个注册设备关联的受管 Apple ID。

- 对于 MDM 管理和应用许可，此受管 Apple ID 会提供身份验证。
- 在 MDM 推送应用和媒体时，必要 Apple 许可证将分配到与设备关联的受管 Apple ID。
- 作为 GDPR 合规性的一部分，受管 Apple ID 会在用户列表和用户详细信息页面中进行屏蔽，并将 Apple ID 视为用户数据。
- 受管 Apple ID 最初由 Apple 校园教务管理使用，现在由 Apple 商务管理使用以进行用户注册。

> 该设备的受管 Apple ID 与 App 和图书位置令牌应来自相同 Apple 商务管理帐户的组织。

如果不同，在应用的许可证分配失败时，将在 Ivanti Neurons for MDM 管理员门户中显示通知。

为联合身份验证配置的 Microsoft Entra ID，或者在 Apple 商务管理中使用验证域手动创建的 Apple ID。

- 如需使用联合身份验证的说明，请查看 Apple 网站上的 **Apple 商务管理用户指南**。 需要登录。

对于同步到 LDAP 的设备用户，将分配到设备管理角色，并与受管 Apple ID 关联。

在**用户**列表页面和**设备**列表页面中，您可以添加要为所有用户显示的受管 Apple ID 列。 在**设备**列表页面中，您可以添加用户注册已注册列，以显示用户注册设备的状态。 此外，用户和设备导出在 CSV 文件中包含这些列。

注册优先级

- 支持通过 Go for iOS 客户端和 iReg 进行用户注册。 Apple 不再支持通过 Ivanti Go for iOS 和 iReg 进行用户注册。 **账户驱动型用户注册**仅在设备的工作或教务账户中可用。
- 自动化设备注册和 Apple 配置器注册将始终是设备注册。
- 如果 MAM 配置应用于设备，MAM 注册优先于用户注册。
- 如果同时满足仅身份验证和用户注册要求，用户注册将优先。
- 如果您从 Go for iOS 客户端重新注册设备，注册类型将与设备注册期间的类型相同，无论 Ivanti Neurons for MDM 中的注册类型如何更改。 例如，如果设备是用户注册，并在 Ivanti Neurons for MDM 中将类型更改为设备注册，从 Go 客户端重新注册设备，该设备仍是用户注册，而非设备注册。

标准 MDM 注册与用户注册之间的差异

本部分解决了标准 MDM 注册与具有 Apple 商务管理的用户注册之间的差异。

标准 MDM 注册

以下列表指出 Ivanti Neurons for MDM 服务器可在标准 MDM 注册中执行什么操作，但在用户注册模式中无法执行什么操作。

MDM 服务器：

- 无法擦除设备。
- 未看到设备用户在设备上安装的个人应用。
- 无法将用户安装的应用转换为 MDM 受管应用。
- 无法清除设备通行码（如 解锁设备）。
- 无法设置长且复杂的设备密码要求。
- 无法配置设备范围的 VPN 或 Wi-Fi 代理，也无法对蜂窝功能实施任何管理。
- 无法查看设备标识符，例如 UDID、序列号或 IMEI。
- 无法应用多个设备范围的限制（例如限制应用内容分级），屏蔽 iCloud，并应用任何受监管的限制。

具有 Apple 商务管理的用户注册

在用户注册中，MDM 服务器仍可以执行管理企业应用、帐户和数据所需的一切操作。

用户注册可以：

- 安装内部应用，或通过基于用户的 (Apple) App 和图书许可证安装应用。
  - 许可证采用先到先得的方式应用，并由受管 Apple ID 使用。

- 对于在用户注册设备上安装的应用使用的许可证，将与在设备注册设备上安装的相同应用所用的许可证不同。
- 通过“许可证使用”选项卡，在用户详细信息页面中检查 Apple App 和图书应用的许可证类型 - 注册类型显示为“用户注册”或“设备注册”。

强制执行密码有效负载设置。 例如：

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

查询与企业管理的应用、证书和配置文件相关的数据。

- 对于由 MDM 安装的应用、邮件、联系人和日历，配置 Per-App VPN。
- 强制执行一些限制，例如受管打开方式、受管联系人、锁定屏幕上的受管数据及其他一些限制。

企业数据会存储到单独 Apple 文件系统 (APFS) 卷；该系统卷将在注册时创建，并与设备用户数据单独加密。 此卷包含受管应用存储的数据；企业备注；企业 iCloud Drive 文档；企业钥匙串条目；受管邮件附件和正文；日历附件。 从 MDM 取消注册会破坏音量和按键。

通过 Ivanti Neurons for MDM，所有第三方应用只能是个人应用或受管应用。 MDM 服务无法开始管理设备用户已安装的应用。 在此情况下，在通过 MDM 安装应用前，管理员将需要请求设备用户删除个人应用。 MDM 服务无法开始管理用户已安装的应用。 但备注和文件等一些系统应用程序将支持工作和个人帐户。

macOS 设备的用户注册

搭载 macOS 10.15 或支持的较新版本 Ivanti Neurons for MDM 的设备支持用户注册。

- macOS 用户注册已注册的设备不支持 Mobile@Work for macOS。
  - 即使应用分发到 macOS 用户注册已注册的设备，该应用也不会从 MDM 推送到该设备。
  - 因此，macOS 用户注册已注册设备不支持 Mobile@Work 功能，例如适用于 Packager (MIP) 应用的脚本管理和应用管理。

macOS 用户注册已注册的设备中的应用依赖关系和行为变化。

- 在 macOS 用户注册已注册的设备中，应用依赖关系将尽量发挥作用，因为在分配主应用前，MDM 不知道（不能确认）必备应用的安装状态。
- 应用和配置可以分发到属于 macOS 用户注册已注册设备的用户和用户组。 但应用始终会显示**安装**按钮，而不是“已安装”，因为 MDM 无法显示 macOS 用户注册已注册设备中应用的安装状态。
- 已安装的应用在**设备 > 应用清单**页面中显示为已请求的应用，因为 macOS 用户注册已注册的设备不会在清单报告中通知 Ivanti Neurons for MDM 服务器应用是否已安装。

在应用的分配筛选器中，用户注册已注册和自动设备注册已注册属性可根据需要用于自定义分发。

- 基于用户的许可证支持使用受管 Apple ID 安装 Apple App 和图书应用。 不允许基于设备的许可证。 App Catalog 仅显示 Apple App 和图书应用。
- 并非允许所有配置、策略和操作。 请参阅按照此过程列出的配置和策略的完整列表。
  - 如果不支持的配置分发到 macOS 用户注册已注册设备，将不会分发或应用于该设备，并可能显示一则消息，例如“限制 - 这不是有效的请求类型。”
  - 同样，不支持的管理设备操作将在 Ivanti Neurons for MDM UI 中通知。
  - Ivanti Neurons for MDM 不会发送不支持的报告。

以下是不支持分配到 macOS 用户注册已注册设备的配置和策略：

- 通行码
- 隧道
- Tunnel（按需）
- VPN 配置
- Office 365 自动帐户创建
- macOS 内核扩展策略
- 隐私首选项
- macOS 限制
- 软件更新
- AirPrint
- MI 客户端隐私
- FileVault 2
- FileVault 恢复密钥
- 防火墙
- 系统策略规则
- 证书首选项
- 系统策略控制
- 系统策略已托管
- macOS AppStore 限制
- macOS 磁盘刻录限制
- macOS Finder 设置
- Mobile@Work for macOS
- Mobile@Work for macOS 脚本
- 允许的媒体控制
- 时间服务器
- 允许的应用策略

用户注册与设备注册之间的差异

本部分介绍了用户注册与设备注册之间的不同。

用户注册适用于搭载 iOS 13.0 和 macOS 10.15 至支持的最新版本的设备。 无论设备用户是否启用用户注册，iOS 13.0 和 macOS 10.15 早期版本的设备将视为“设备注册”。

> 适用于 Apple 商务管理的用户注册不允许擦除或解锁。 但用户门户仍将包含可用选项，即使无法正常工作。

用户注册与设备注册			
功能	用户注册	MAM	设备注册
擦除设备，并查看用户的个人应用	✗	✗	✓
将受管转换为未受管，或反之亦然	✗	✗	✓
清除设备密码，配置设备范围的 VPN 或 Wi-Fi 代理，或管理手机功能	✗	✗	✓
查看设备标识符，例如序列号、IMEI	✗	✗	✓
应用受管限制	✗	✗	✓（仅受监控设备）
可安装并配置应用和帐户	✓	✓	✓
可以为已由 MDM 安装的应用、邮件、联系人和日历配置每个应用的 VPN	✓	✗	✓
可强制执行一些限制，例如受管打开方式、受管联系人、锁定屏幕上的受管数据及其他一些限制	✓	✗	✓
可查询与企业管理的应用、证书和配置文件相关的数据	✓	✗	✓

连接 Ivanti Neurons for MDM 与 Apple 商务管理

本部分介绍了启用适用于 Apple 商务管理的用户注册。

先决条件

- 您必须有 Apple 商务管理帐户。 请参见 **https://business.apple.com/**。
- 您必须请求并安装 Apple **MDM 证书**，才可以管理 iOS 设备。

创建本地用户以启用用户注册

本部分介绍了创建本地和 LDAP 用户，并设置未受监管的 Apple 设备的用户注册。 用户注册将不适用于受监管的设备，或在 Apple 设备注册中注册的设备。

创建手动管理（静态）的用户组

这是一次性程序。 如果您已创建此组，跳到“创建用户注册的用户”部分。

步骤

1. 转到**用户 > 用户组**。
2. 创建手动管理（静态）的用户组，例如用户注册组，以添加设备注册类型为用户注册的用户。
3. 单击**保存**。

创建设备注册类型设置

这是一次性程序。 如果您已创建此组，跳到“创建用户注册的用户”部分。 对于用户注册已注册的设备，默认的设备所有者设置将是“用户所有”。

步骤

1. 转到**用户 >** 用户设置。
2. 在设备注册设置部分中，单击 **+ 添加特定用户组的设置**。
3. 对于设备注册类型为用户注册的用户，创建新设置，例如 UE 注册。
4. 在 Apple 注册部分中，选择**用户注册**作为 Apple 注册类型。
5. 单击**下一步**。
6. 在用户设置分发页面中，选择新创建的用户组，例如用户注册组。
7. 单击**完成**。

创建用户注册的本地用户

作为先决条件，为用户注册创建手动管理的用户组和设备注册设置。

步骤

1. 转到用户。
2. 单击 + **添加** > **单用户**。
   输入新用户信息，并将其添加到新创建的用户组，例如用户注册组。 有关详细信息，请参阅用户主题中的*添加用户*。

导入 LDAP 用户，以启用用户注册

先决条件

- 作为先决条件，设置 Ivanti Neurons for MDM 连接器，以访问 **LDAP** 资源。
- 确保**托管 Apple ID** 设置已设为**模式**（用户电子邮件地址）。 请确保受管 Apple ID 的模式唯一。 否则，如果其他帐户包含相同受管 Apple ID，将不使用受管 Apple ID 更新帐户。
- （可选）包含 appleid 子域，以免与现有 Apple ID 冲突。
- 您可以从 LDAP 导入用户，并邀请其实施用户注册。 已导入 LDAP 用户将同步受管 Apple ID 与 Ivanti Neurons for MDM，这是用户注册的要求。

步骤

1. 转到**用户**。
2. 单击 **+ 添加 > 从 LDAP 邀请用户**。
3. 在 LDAP 服务器条目中单击**选择用户**。
4. 在“添加 LDAP 用户”页面，在搜索字段中输入用户、小组或 OU 的名称。
5. 要添加新用户或小组，单击您想要添加条目旁边的 **+ 添加**。
6. 单击**完成**。

导入 Entra ID 用户以启用用户注册

前提条件是连接 Ivanti Neurons for MDM 与 Microsoft Entra ID (Entra ID)。

您可以邀请 Entra ID 用户进行用户注册。 已导入的 Entra ID 用户将同步托管 Apple ID 与 Ivanti Neurons for MDM，这是用户注册的要求。

程序

1. 转到**管理员 > Entra ID 用户源**。
2. 编辑设置。
3. 选择**启用此 Entra ID**。
4. 在"托管 Apple ID"设置中，选择以下选项之一：
   - **模式**
     - **用户电子邮件地址** - 确保托管 Apple ID 的模式是唯一的。 否则，如果其他帐户包含相同受管 Apple ID，将不使用受管 Apple ID 更新帐户。
     - 或选择 **userUPN**。
5. （可选）包含 appleid 子域，以免与现有 Apple ID 冲突。
6. 选择**自动邀请从 Entra ID 导入的用户**。 从 Entra ID 导入 Ivanti Neurons for MDM 的用户会自动受邀通过电子邮件注册。
7. 单击**保存**。

使用用户注册进行注册的设备用户说明

本部分描述了设备用户注册 Apple 用户注册需要执行的操作。

步骤

1. 在要注册的 iOS 设备上，打开邀请电子邮件，其中包含链接，以及将最终用户引导至注册链接的文本，例如 mobileiron.com/go。
2. 在 Safari 中打开注册链接。
3. 显示登录页面。 设备用户将使用本地用户或 LDAP 凭据登录。
   系统将显示注册页面，并显示一则消息"配置文件已下载"。
   点击设置。 系统将显示设置页面。
4. 点击注册 [Your Company Name]。
5. 系统将显示用户注册页面。
6. 点击注册我的 [Your Device]。 例如，点击"注册我的 iPhone"。
   如果您点击"取消并删除配置文件"，您将需要重新开始注册过程。
   系统将为您提供 Apple 或联合帐户的登录方式。 输入受管 Apple ID 的密码。 （受管 Apple ID 将列在登录页面顶部。）
   系统将为您提供保持登录选项，以供选择。
   页面将显示"注册成功"。

使用设备日志进行故障排除

要对用户已注册设备的错误或问题进行故障排除，请通过查看设备日志开始。

步骤

1. 转到设备。
2. 单击设备，以显示设备详细信息页面。 您可以验证用户注册已注册和已注册受管 Apple ID 字段。
3. 选择日志选项卡。
4. 在筛选器区域中，使用基于操作名称（例如，签出、设备名称、设置启动令牌、获取启动令牌等）、状态、开始日期和结束日期的筛选器，缩小设备日志范围。
5. 在操作列中，单击眼睛图标，以显示设备日志详细信息，例如注册 ID。

6. 单击**确定**。

6.6. 用户许可证

基于 Ivanti Neurons for MDM 用户的许可证定义了您可以注册的用户数量、每个用户许可证允许的设备数量、可以配置用于分发到设备的内容数量，以及可以使用哪些功能。 如果达到用户限制，“管理员”页面上会显示红色三角形。 如果达到内容的限制，服务会阻止您添加更多内容并显示一条消息，提示您已达到限制。

要确定您的规划需要多少用户许可证，请考虑以下几点：

- 根据安全 UEM 或安全 UEM Premium 软件包购买的每个用户许可证允许注册最多 5 个设备。
- 在用户注册 5 个以上的设备后，将申请其他用户许可证。
- 一名用户可申请的用户许可证数量并无限制。
- 许可证将在设备停用或擦除后发放。

例如，用户 1 在工作第一天注册工作电话时，她需要申请用户许可证。 接下来的一周，她用同样的许可证注册了两部个人手机和一部平板电脑。 当她注册另一部平板电脑时，她现在有五个设备，所以她申请了第二个用户许可证。 私人电话被盗后，她可以擦除该设备，这将使第二个用户许可证空闲。

查看用户的设备/许可证数量

过程：

1. 转到**用户**。
2. 单击用户的链接。

左窗格中将列出包括许可证使用情况在内的用户详细信息。

6.7. 管理用户

本部分包含以下主题：

- 正在为 Cisco ISE 操作添加 API 用户
- 为用户分配角色
- 用户角色
- 查找并过滤用户
- 将用户分配到用户组
- 邀请用户
- 启用和禁用用户
- 管理多个管理员登录
- 更改密码
- 发送消息
- 将用户从用户组中移除
- 删除用户
- 导出用户
- 将自定义属性分配到用户
- 将自定义属性从用户中删除
- 更改用户区域设置
- 编辑用户名
- 选择退出位置数据收集
- 超时信息
- 选择退出系统使用情况分析
- 通过生成的 PIN 进行设备注册

6.7.1. 正在为 Cisco ISE 操作添加 API 用户

可以添加角色为“Cisco ISE 操作”的 API 用户，该角色允许 Cisco ISE 在 Ivanti Neurons for MDM 中与 Cisco ISE API 进行交互。 在创建此用户后，使用 Cisco ISE 中的该用户凭据，对 Ivanti Neurons for MDM 中的 API 调用进行身份验证。 这些 API 允许 Cisco ISE 获取设备信息；例如，在设备上采取操作、完全擦除、共同擦除和 Pin 锁定；并向设备发送消息。

> API 用户将无法登录管理员门户。 此用户仅用于启用 API 用法。

> 默认情况下，只有租户的超级管理员，才可以分配 Cisco ISE 操作角色。 超级管理员必须明确在系统中选择其他用户，而管理员必须拥有此角色，并将其分配到用户。 相反，具有已分配 Cisco ISE Operations 角色的用户可以将该角色分配到系统中的其他适当用户。

步骤

1. 转到**用户** > **用户**。
2. 单击**添加**。
3. 选择 **API 用户**。
4. 使用用户信息，填写结果表：
    - 电子邮件地址
    - 名字
    - 姓氏

> “用户名”字段显示您输入的电子邮件地址。 多数情况下，不可编辑默认值。 参见何时编辑用户名。

如果您想更改用户的显示名称，编辑**显示姓名**字段的默认文本。

6. 通过在**密码**中输入，以分配密码并**确认密码**字段。
7. 保持 **API 管理 Cisco ISE 操作**角色在**分配角色**部分中的选中状态。
8. 单击**完成**添加用户。

如果您无法在**用户**页面上执行任务，这可能是您没有所需权限。 您需要以下角色之一：

- 系统管理
- 用户管理

6.7.2. 为用户分配角色

可以通过分配角色，授予用户访问 Ivanti Neurons for MDM 数据和功能的权限。您可直接为用户或用户组分配角色。 为{{用户组}}分配角色将为该组中的所有用户分配该角色。

> 默认情况下，不会给用户分配“只读用户”角色。
> 对于有权访问 Ivanti Neurons for UEM 和 Ivanti Neurons for MDM 的租户，隐藏“角色”页面和关联选项。

用户无法分配自己没有的权限。 对于未分配到用户的权限和角色，系统将不会显示和选择。 在这种情况下，将显示错误消息。 在 Ivanti Neurons for MDM 管理员或合作伙伴管理员尝试将角色分配给合作伙伴管理员时，Ivanti Neurons for MDM 会显示一则消息，表示合作伙伴管理员必须在服务提供程序门户中执行此操作。

有关角色的更多信息，请查看 Roles_Management.htm。

程序：

1. 转到：
   - **用户 > 用户***或*
   - 用户 > 用户组。

选择一个或多个用户或用户组。

3. 单击**操作**。
4. 从用户详细信息页面或用户组详细信息页面中，单击**分配角色***或*
   在用户列表或用户组列表页面上，选择**附加角色**。
5. 选择一个或多个您想分配的以下角色：
   - 系统管理 | 跨空间
   - 系统只读 | 跨空间
   - 用户管理 | 跨空间
   - 用户只读 | 跨空间
   - LDAP 用户导入和邀请 | 跨空间
   - 设备管理 | 特定于空间
   - 设备只读 | 特定于空间
   - 应用和内容管理 | 特定于空间
   - 应用和内容只读 | 特定于空间
   - 设备操作 | 特定于空间
   - Cisco ISE 操作 | 跨空间
   - 计划任务管理 | 跨空间
   - 常见平台服务 (CPS) | 跨空间
   - 低用户影响迁移管理 | 跨空间
   - 自定义设备注册 | 跨空间
   - 编辑 Microsoft Graph | 跨空间
   - 发送/取消擦除 | 跨空间

- 查看 Microsoft Graph | 跨空间
- 管理 Access 集成 | 跨空间

单击**下一步**。

7. 如果所选角色与空间绑定，则需为所有与空间绑定的角色选择空间。

> 如果只有一个空间（默认空间），则在分配空间限制角色时，会跳过“指定空间”步骤。

摘要页面显示作为默认空间界定的空间的空间名称。
查看要分配的角色摘要，然后单击**完成**。

向帮助台人员授予使用基本设备操作的权限

帮助台的功能一般会允许员工查看数据。 但部分组织倾向于纳入以下基本设备操作：

- 强制签入
- 锁定
- 解除锁定
- 发送消息
- 停用
- 擦除

步骤

可以为操作提供权限。

1. 前往**用户 > 用户**或**用户 > 用户组**。
2. 选择一个或多个用户或用户组。
3. 单击**操作**。
4. 在用户详细信息页面或用户组详细信息页面上，选择**分配角色**或
   在用户列表或用户组列表页面上，选择**附加角色**。
5. 选择**设备只读**。
6. 选择**设备操作**。
7. 单击**完成**。

> 在选择“设备操作”之前，请确保选择“设备只读”，以便用户拥有所需权限。

6.7.3. 用户角色

用户角色决定了用户可以在 Ivanti Neurons for MDM 中看见的页面和用户可以执行的操作。 以下表格列出了您可以分配的角色以及角色所代表的意义。

角色	描述	特定于空间
系统管理	允许管理员管理租户级设置，例如 MDM 证书、App Catalog 设置等。	无
系统只读	允许管理员查看租户级设置，例如 MDM 证书、App Catalog 设置等。	无
用户管理	允许管理员添加和移除用户，分配角色并将用户添加到用户组。	无
用户只读	允许管理员查看用户和用户组，以及应用和内容目录。	无
设备管理	允许管理员管理设备组、配置和策略，以及执行所有设备操作。	“是”
设备只读	允许管理员查看设备组、配置和策略。	“是”
应用和内容管理	允许管理员添加、分发并移除应用和内容。	“是”
应用和内容只读	查看用户、应用、内容中的数据，其中包含 AppConnect 任务	“是”
设备操作	允许管理员启动设备操作，例如： • 强制签入 • 锁定 • 解除锁定 • 发送消息 • 停用 • 擦除 必须在选择“设备操作”之前选择“设备只读”。 否则，用户将无目标权限。	“是”
LDAP 用户导入和邀请	允许管理员注册 LDAP 用户，并向注册设备发送邀请	无
Cisco ISE 操作	允许管理员为 Cisco ISE 集成调用所需的 API。	无
计划任务管理	允许管理员创建和管理各种管理操作的计划任务。	无
通用平台服务 (CPS)	允许管理员使用通用平台服务。	无
低用户影响迁移管理	允许管理员管理低用户影响迁移设置。	无
自定义设备注册	允许管理员使用自定义设备注册对设备进行注册。	无
编辑 Microsoft Graph	允许管理员编辑用于 Office 365 应用保护的 Microsoft Graph API 设置。	无
查看 Microsoft Graph	允许管理员查看用于 Office 365 应用保护的 Microsoft Graph API 设置。	无
发送/取消擦除	允许管理员在执行前向设备发送擦除命令，或取消已发出的擦除命令。	无
管理 Access 集成	允许管理员管理 Access 集成。	无

有关更多信息，请查看**分配角色**

6.7.4. 查找并过滤用户

本部分包含以下主题：

- 搜索用户
- 针对用户使用高级搜索
- 加载用户的搜索查询
- 筛选用户

搜索用户

如果添加了多个用户，则使用筛选器或搜索快速定位用户条目很有用。

步骤

1. 转到**用户**。
2. 在搜索框中，键入字符。

针对用户使用高级搜索

您可以使用高级搜索选项，以按照规则搜索用户，识别和查看符合特定条件的用户。 使用任意（或）或全部（且）选项，规则选项可以全部进行嵌套。 符合规则的用户会显示在该小节下方。 可以使用下列运算符构建规则：

- 开头为
- 结尾为
- 包含
- 不包含
- 开头不为
- 结尾不为
- 小于
- 大于
- 在范围内
- 等于
- 不等于

从 Neurons for MDM 127 开始，在规则生成器中选择“用户组名称”属性后，Ivanti Neurons for MDM 管理员门户会显示重复用户组的数量和相应的 GUID 数量，以便标识重复组。 此外，此规则下方的表会显示重复用户组的列表及其详细信息，例如用户组名称、GUID、来源和可分辨名称 (DN)。

步骤

1. 从用户页面中，单击**高级搜索**链接。
2. 如果用户需要匹配其中至少一个规则，单击**任意**；或者，如果用户需要匹配所有规则，单击**全部**。
3. 创建定义搜索条件的规则，例如用户组、自定义用户属性和自定义 LDAP 属性。
4. （可选）单击 +，以创建其他规则（如果需要）。
5. （可选）单击**保存**，以保存查询。

6. 单击**搜索**。 页面会显示匹配搜索条件的用户列表。

加载用户的搜索查询

步骤

1. 从用户页面中，单击**高级搜索**链接。
2. 单击“文件夹”图标。 显示**高级搜索**窗口。 **加载查询**部分会显示已创建搜索查询的列表。 此部分会显示以下详细信息：
   - **查询名称** - 已加载查询的名称。
   - **查询内容** - 根据定义搜索查询的规则，显示内容。
   - **操作** - 选择对查询执行的操作。
3. 单击**操作**列中的**加载查询**，以查看匹配在已加载查询中定义的条件的用户列表。
   要删除已加载查询，单击删除图标。

筛选用户

“筛选器”侧面导航栏会列出可帮助您从整个用户列表中搜索特定用户的各个部分。 “管理筛选器”向导包含所有部分的列表，您可根据需求选择要在“筛选器”导航栏中显示的部分。

步骤

1. 转到**用户**。
2. 在“管理筛选器”向导列出的部分中，点击相关复选框。 可从下列部分进行搜索：
   - 管理员
   - Google 状态
   - 状态无效
     - 已完成（用户已接收并回复。）
     - 已过期（用户未及时回复。）
     - 未邀请（尚未邀请此用户。）
     - 等待（等待用户响应）

   密码到期

     - 过期（密码过期选项设置为有限日期的用户。）
     - 永不（密码过期选项设置为永不的用户。）
   - 用户组（选择感兴趣的{{用户组}}。）
   - 用户源
     - LDAP
     - Entra ID
     - 名册
     - Salesforce
     - 本地
   - 同步
     - 直接同步 - 列出从 LDAP 服务器直接同步的用户

- 未同步 - 列出从 LDAP 服务器中移除的用户
- 间接同步 - 列出从 LDAP 服务器间接同步的用户
- 不适用

3. （可选）点击**还原默认值**可将所选项还原为默认筛选器。 “筛选器”导航栏会显示选中的部分。 如果从“管理筛选器”向导中清除所有复选框，“筛选器”侧面导航栏将显示所有部分。
4. 点击“管理筛选器”向导以外的任何位置可退出向导。
5. 点击“x”图标可关闭“筛选器”侧面导航栏，点击**筛选器**可重新打开侧面导航栏。

6.7.5. 将用户分配到用户组

本部分包含以下主题：

- 从用户页面分配用户
- 从用户组页面分配用户

将用户分配到用户组是个非常好的方法，可将您需要重复执行的任务次数降到最少，比如：

- 分发应用
- 分配角色

从用户页面分配用户

1. 转到**用户**。
2. 选择您想要处理的用户。
3. 单击**操作**。
4. 选择**分配到组**。
5. 选择组或**新建**，开始一个新组。
6. 单击**保存**。

从用户组页面分配用户

1. 转至**用户 > 用户组**。
2. 选择您想要处理的用户组。
3. 单击**操作**（右上角）。
4. 选择**分配用户**。
5. 输入每个用户的电子邮件地址。
6. 单击**分配用户**。

6.7.6. 邀请用户

添加用户时，您有机会邀请该用户注册设备。 事实上，该选项默认选中。 受邀用户会收到一则电子邮件消息，其中包含注册所需的信息。 您也可以在**用户 > 用户**页面邀请（或重新邀请）用户。

步骤

1. 转到**用户**。
2. 选择您要邀请的用户。
3. 选择**操作 > 发送邀请**。 “邀请预览”随即出现，附带将设备所有权设置为**用户所有**或**公司所有**的选项。

4. 或者，打开**设备所有者设置**。
5. 单击**用户所有**或**公司所有**。 此设置会更改在注册过程中如何分类设备。 此仅适用于仅限 PIN，或密码 + PIN 注册类型。 如果已关闭**设备所有者设置**，设备将注册为“未设置”，对于受监督的设备，设备所有者设置将为“公司所有”。
6. 点击**发送**。 如果执行了基于 PIN 的设备注册，用户的注册电子邮件将收到 PIN。 如果设置基于 QR 码的注册，用户将收到 QR 码。
7. 点击**确定**。

> 如果注册确认电子邮件功能按照**配置和使用注册确认电子邮件**所述启用，您也将看到一则提醒，用户将在成功注册后收到一封注册确认电子邮件。 为了收到电子邮件，用户需要成为分发列表中的一员，该列表在**用户设置**的**配置用户注册确认电子邮件**中指定。

有关更多信息，请查看**导入 LDAP 用户**。

6.7.7. 启用和禁用用户

本部分包含以下主题：

- 启用和禁用本地用户
- 启用和禁用 LDAP 用户

本地用户和 LDAP 用户可以处于启用或禁用状态。 根据用户的状态，您可以使用“启用用户”条件创建自定义策略，并为规则构建器中的条件设置操作。 例如，使用自定义策略规则，以停用属于已禁用本地/LDAP 用户的设备。

启用和禁用本地用户

默认情况下，创建本地用户时，用户处于启用状态。

步骤

1. 转到**用户**。
2. 单击用户的显示名称。
3. 点击**编辑**。 将显示**需要身份验证**窗口。
4. 输入管理员密码，然后单击**身份验证**。

> 如果输入多个不正确的密码，并且超过在“密码复杂性设置”中设置的“失败登录阈值限制”，帐户将锁定，您将从当前会话中注销。

5. 选择或取消选择**已启用**选项，以便分别启用或禁用本地用户。
6. 单击**保存**。

启用和禁用 LDAP 用户

您可以仅为 Microsoft Active Directory 启用或禁用 LDAP 用户。 在 Microsoft Active Directory 中，当您打开用户账户的属性时，单击**账户**选项卡，然后选中或清除**账户**选项对话框中的复选框，将数值分配给 **UserAccountControl** 属性。 分配给该属性的值告诉 Windows 哪些选项已启用。 为 UserAccountControl 属性分配值后，用户状态将反映在与 with Ivanti Neurons for MDM 进行 LDAP 同步之后。

以下是您可以分配的可能值：

- 512 - 已启用。
- 514 - 已禁用。
- 66048 - 已启用，密码永不过期。
- 66050 - 已禁用，密码永不过期。

查看用户帐户

步骤

1.		**点击开始。**
	2.	**转到程序。**

	3. 转到管理工具。

4.	点击 **Active Directory 用户和计算机**。

有关更多信息，请参阅 https://support.microsoft.com/en-in/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-pro。

可以使用 Ldp.exe 工具或 Adsiedit.msc 管理单元查看和编辑属性。 只有经验丰富的管理员可以使用这些工具来编辑 Active Directory。 从原始 Windows 安装介质安装支持工具后，这两个工具都可用。

6.7.8. 管理多个管理员登录

支持多个 Ivanti Neurons for MDM 管理员门户会话，因此管理员可以同时查看门户的不同页面。 如果您是管理员，您可以查看上次登录日期，以帮助您跟踪多个登录。

查看上一次管理员登录信息

步骤

1. 点击**帐户** `
2. 查看**上次登录：**条目。

6.7.9. 更改密码

本部分包含以下主题：

- 从用户选项卡更改密码
- 将密码应用于永不过期
- 移除密码永不过期设置

> 如果用户具有系统管理角色，则仅超级用户或当前已登录用户可以查看**更改密码**选项。

可以更改 Ivanti Neurons for MDM 密码。 如果您有权限，还可以为其他用户更改密码。

步骤

1. 单击“账户”图标（右上角）。
2. 
   从下拉菜单中选择**更改密码**。
3. 输入当前密码。
4. 输入新密码。
5. 再次输入新密码。
6. 要将密码设置为不过期，选择**将密码设置为永不过期**。

> 将密码设置为永不过期会覆盖在用户 > 用户设置 > 密码复杂性设置中定义的**密码过期期限**。

7. 单击**完成**。

> 要将本地帐户密码重置为过期，请取消选择**将密码设置为永不过期**。 在取消选择该选项后，将出现弹出窗口，并显示上一个应用于用户的密码过期日期。

从用户选项卡更改密码

步骤

1. 转到**用户**。
2. 单击用户的显示名称。
3. 单击**编辑**（左上角）。 将打开**需要身份验证**窗口。 在编辑用户前，需要管理员（本地用户或 LDAP 用户）通过输入管理员密码进行身份验证。
4. 输入管理员密码，然后单击**身份验证**。

> 如果输入多个不正确的密码，并且超过在“密码复杂性设置”中设置的“失败登录阈值限制”，帐户将锁定，您将从当前会话中注销。

5. 在**当前密码**字段中输入当前密码。

> 如果您更改其他用户的密码，此字段将不会显示。

6. 在**更改密码**字段中输入新密码。
7. 确认新密码。
8. 单击**保存**（左上角）。

将密码应用于永不过期

1. 转到**用户**。
2. 选择一个或多个用户。
3. 单击**操作**。
4. 选择**分配密码永不过期**。 系统显示**将本地帐户密码设置为永不过期**窗口。
5. 单击**提交**。

移除密码永不过期设置

1. 转到**用户**。
2. 选择一个或多个用户。
3. 单击**操作**。
4. 选择**移除密码永不过期**。 系统显示**移除本地帐户密码永不过期**窗口。
5. 单击**提交**。 在移除此设置后，上一个密码过期日期将应用于用户。

6.7.10. 发送消息

本部分包含以下主题：

- 向用户发送消息
- 向设备发送消息

可以向任何已知用户发送消息。 消息可以通过电子邮件或{{推送通知}}的形式发送。 只有配备注册设备的用户才能接收推送通知。

先决条件

- 对于 iOS 设备，请确保已安装 Go 客户端。
- 对于 macOS 设备，请确保已安装 Mobile@Work 客户端。

向用户发送消息

1. 转至**用户 > 用户**。
2. 选择您要向其发送消息的用户。
3. 单击**操作**（右上角）。
4. 点击**发送消息**。
5. 如果您不希望发送电子邮件，请取消选中**发送电子邮件消息**复选框。
6. 如果发送电子邮件，请输入主题和消息文本。
7. 如果发送推送通知，请选中**发送推送通知**复选框并输入消息文本。
8. 单击**发送**。

向设备发送消息

1. 转至**设备 > 设备**。
2. 选择您要向其发送消息的设备。
3. 单击**操作**（右上角）。
4. 点击**发送消息**。
5. 或者，单击设备名称链接，转到“设备详细信息”页面，然后单击**发送消息** 图标。
6. 如果您不希望发送电子邮件，请取消选中**发送电子邮件消息**复选框。
7. 如果发送电子邮件，请输入主题和消息文本。
8. 如果发送推送通知，请选中**发送推送通知**复选框并输入消息文本。

> 推送通知消息也可以包含用户可访问的 URL。

9. 单击**发送**。
   在向用户发送推送通知时，该用户将能够在设备屏幕工具栏上看到钟图标。 点击钟图标，用户可以查看收到通知的历史记录，并执行操作或删除通知。

> 在**设备**和**用户**页面中均可使用，管理员可以将特定设备或用户属性插入消息中，然后将其排入队列等待最终用户传递。

6.7.11. 将用户从用户组中移除

本部分包含以下主题：

- 将用户从用户页面中移除
- 将用户从用户组页面中移除

删除用户组中的用户意味着：

- 从用户中移除分配给该组的任何角色
- 分配给该组的任何应用在用户的 {{{App Catalog}} 中不再可用
- 配置为可移除的应用将从用户设备中移除

将用户从用户页面中移除

1. 选择您要处理的用户。
2. 单击**操作**（右上角）。
3. 选择**从组中移除**。
4. 选择组。
5. 单击**移除**。

将用户从用户组页面中移除

1. 单击用户组以显示其详细信息。
2. 单击**编辑**（右上角）。
3. 单击要移除的用户旁边的**移除**链接。
4. 单击**保存**（右上角）。

6.7.12. 删除用户

本部分包含以下主题：

- 您删除本地用户后会出现的情况
- LDAP 用户将受何影响？

步骤

1. 转到**用户 > 用户**。
2. 选择用户条目。
3. 单击**操作**（右上角）。
4. 选择**删除**。

在 Ivanti Neurons for MDM 管理员或合作伙伴管理员尝试删除合作伙伴管理员时，Ivanti Neurons for MDM 会显示一则消息，表示合作伙伴管理员必须在服务提供程序门户中执行此操作。

> 如果用户具有与其账户关联的设备，则必须首先停用并删除这些设备，然后删除该用户。 如果用户没有设备，则在删除用户时可以删除用户信息。

您删除本地用户后会出现的情况

- 与已删除用户相关的所有信息都将从系统中删除。
- 与该用户相关的设备均停用。
- 该用户上传的内容仍然存在。
- 该用户帐户将不允许进一步设备注册。

LDAP 用户将受何影响？

- 如果已禁用 LDAP 服务器，则将不能永久删除 LDAP 用户。 下一次同步 LDAP 数据时将恢复已删除的 LDAP 用户。
- 如果已删除 LDAP 服务器或组，则 LDAP 用户将变成本地用户并可被删除。
- 从 LDAP 删除用户时，不会从 Cloud 删除该用户。 同步状态将切换为“NO_SYNC”，但不会删除用户。

6.7.13. 导出用户

作为管理员，您可以从 Ivanti Neurons for MDM 导出用户列表。

> 在用户设备注册 PIN 导出到 CSV 文件时，出于安全原因，PIN 将掩码处理为“”，而不是实际的 PIN。

步骤

1. 转至**用户 > 用户**。
2. 从列表中选择一名或多名用户。
3. 点击**导出为 CSV**。

将显示弹出窗口，提示需要一些时间来完成报告导出。 提交请求后，您必须等待请求完成才能提交另一个请求。 报告就绪后，您将收到提示消息，要求您下载或删除生成的报告。 您还将收到一封电子邮件，其中包含下载报告的链接。

> **自定义用户**和 **LDAP** 属性详细信息也可以与其他详细信息一起导出为 CSV 文件。

> 当向任何用户添加任何包含 +、-、= 或 @ 字符的字段值时，导出的 CSV 文件中的用户数据将自动在该字段前加上单引号 (')，并且竖线 (|) 符号前将添加反斜杠 (\)。 这样做是为了防止 Excel 注入漏洞。

6.7.14. 将自定义属性分配到用户

您可以将自定义用户属性分配到一个或多个用户。 每个属性都有一个对应值，可使用该值执行各类任务，比如创建配置和用户组。 可以将自定义属性分配给一个或多个用户。

步骤

1. 转到**管理员 > 系统 > 属性**，创建新的自定义属性（如果需要）。
2. 转到**用户**。
3. 选择一个或多个用户。
4. 单击**操作**。
5. 选择**分配自定义属性**。
6. 选择下列选项之一：
    - 强制分配（覆盖）所有属性，即使找到任何现有值。
    - 仅当值为空时覆盖，并跳过具有现有值的属性。

选择您想要分配的属性，并输入值（不允许空值）。

8. 单击**分配**。

相关主题：

- 属性
- 变量

6.7.15. 将自定义属性从用户中删除

可以从一名或多名用户中删除自定义属性。

> 请谨慎行事，因为此操作不可逆。

步骤

1. 转到**用户**。
2. 选择一个或多个用户。
3. 单击**操作**。
4. 选择**移除自定义属性**。
5. 选择您想要删除的属性。
6. 单击**移除**。

相关主题：

- 属性
- 变量

6.7.16. 更改用户区域设置

默认情况下，用户区域设置设为租户区域设置。 如果需要，可以更改单个用户的区域设置。

步骤

1. 转到**用户**。
2. 单击用户的显示名称。
3. 点击**编辑**。 将显示**需要身份验证**窗口。
4. 输入管理员密码，然后单击**身份验证**。

> 如果输入多个不正确的密码，并且超过在“密码复杂性设置”中设置的“失败登录阈值限制”，帐户将锁定，您将从当前会话中注销。

5. 在区域设置字段中，单击**更改**。
6. 在**更改用户区域设置**窗口中，从**将用户区域设置更改为:** 下拉列表中选择所需区域设置。
7. 单击**完成**。
8. 单击**保存**。

6.7.17. 编辑用户名

添加用户时，还将自动列出您为用户名输入的电子邮件地址文本。 在多数情况下，应保留默认用户名，因为：

- 用户名需要采用电子邮件地址格式。
- 虽然在{{配置}}中使用用户名变量便捷，但也可以使用电子邮件地址。

仅当发生与现有用户名冲突的稀有事件时才编辑用户名，因为整个设备管理系统中的用户名不得重复。 例如，当同一公司的两个部门注册设备管理系统时，可能发生冲突。

如果发生用户名冲突

如果由于用户名冲突而无法添加用户，则使用电子邮件地址格式输入不同用户名。 电子邮件地址不必与实际邮件帐号对应。 例如，可以更改以下电子邮件地址：

ksmith@mycompany.com

至

ksmith21@mycompany.com

如果编辑用户名，则此用户将无法使用包含用户名变量的所有配置。 相反，需创建使用电子邮件地址变量的其他配置。

6.7.18. 选择退出位置数据收集

本部分包含以下主题：

- 对于 iOS 设备
- 对于 Android 设备

如果已应用隐私配置以启用位置数据的收集，则设备用户可以覆盖该配置。

对于 iOS 设备

iOS 设备用户可以关闭位置服务，防止通过以下设置向设备管理系统发送位置数据：

设置 > 隐私 > 位置服务

对于 Android 设备

Android 设备用户可以关闭位置设置，防止收集位置数据。 此设置的位置因制造商的不同而不同。 还将提示 Android 设备用户接受位置数据的请求。

6.7.19. 超时信息

管理门户的非活动超时介于 5 至 60 分钟之间，超时为 24 小时。

步骤

1. 转到**用户 > 用户设置**。
2. 编辑默认**密码复杂性**设置。
3. 在密码策略部分中，移动**不活动超时**滑块，以指定用户在管理员门户或自助服务门户会话时间前处于非活动状态的时间。 数量范围介于 5 - 60（分钟）之间。
4. 单击**完成**。

6.7.20. 选择退出系统使用情况分析

收集匿名产品诊断和使用数据，帮助改进产品。

如果您希望保持使用数据的私有性，可以选择不发送系统使用分析。

步骤

1. 点击 Ivanti Neurons for MDM 管理门户页面底部的**使用数据**链接。显示**使用情况数据**窗口。
2. 清除**发送诊断和使用数据**复选框。
3. 单击**保存**。

6.7.21. 通过生成的 PIN 进行设备注册

本部分包含以下主题：

- 针对用户登录页面中的单个或多个用户
- 针对用户详细信息中的单个用户

无需发送邀请电子邮件，即可为用户生成设备注册 PIN，从而简化设备注册流程。

针对用户登录页面中的单个或多个用户

1. 转到**用户** > **用户**。
2. 选择要为其生成注册 PIN 的用户。 可以选择一个或多个用户。
3. 点击**操作**按钮。
4. 从下拉菜单中选择**生成 PIN**。
5. 生成的 PIN 将显示在**注册 PIN**列。
6. 要查看 PIN，请点击**查看 PIN**。

针对用户详细信息中的单个用户

1. 转到**用户** > **用户**。
2. 点击要为其生成注册 PIN 的用户名以打开用户详细信息。
3. 在“用户信息”部分，点击**生成 PIN**。
4. 点击**查看 PIN**来查看生成的 PIN。

> 请确保拥有适当的权限为用户生成注册 PIN。 仅设备注册状态为“密码和 PIN”的用户才可以启用“生成 PIN”选项。

7. 设备

本部分包含以下主题：

- 开始使用设备
- 设备组
- 应用库存
- 管理设备

7.1. 开始使用设备

本部分包含以下主题：

- 管理设备
- 对设备执行操作
- 设置设备的时区
- 按条件列出设备
- 显示详细的设备信息
- 为设备批量分配或更改用户和自定义属性
- 将设备导出到 CSV 文件
- 搜索设备日志

设备页面中的每个条目代表一台已注册到 Ivanti Neurons for MDM 的移动设备，并列出关于设备的重要信息。 设备列表页面显示具有以下信息的设备，例如：

- 名称
- 电子邮件地址
- 手机号码
- 操作系统
- 设备类型
- 状态
- 上次签入
- 违反计数
- 空间
- 合法所有者（适用于共享 iPad）

Wi-Fi IP 地址已向 Ivanti Neurons for MDM 服务器报告。 在每次签入时，报告 IP 地址的任何变动。 GDPR 合规 IP 地址在设备列表页面和设备详细信息页面中作为选项可用。 此功能需要设备通过 Go 5.5 for iOS 或更高版本，以及 Ivanti Neurons for MDM 支持的 Go 72 for Android 或更高版本进行注册。

> 鉴于 Ivanti Neurons for MDM 版本新增 GDPR 字段（例如 IP 地址和 eSIM ID），因此，对于配置 GDPR 的管理员，如果他们想要隐藏新字段，将需要编辑 GDPR 配置文件。

在设备列表导出为电子表格 (CSV) 格式时，设备标识符 (EID) 会显示为 iOS 属性。 EID 和移动 EID (MEID)（存在时）会分别以 EID 字符串或 MEID 字符串为前缀。

> Ivanti Neurons for MDM 服务器无法处理具有不同客户端标识符和在不同租户之间注册的相同设备。 服务器仅会处理具有不同客户端标识符及在相同租户中注册相同设备的实例。

管理设备

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 转到**设备**。
3. 选择一台或多台设备。
4. 在**操作**下拉列表中选择一项操作。

下表列出了在“设备”页面中可用的操作：

类别	操作
常见	• 添加到组 • AppConnect 解锁 > • 分配自定义属性 • 分配给用户 • 设备合规性状态同步 • 禁用远程桌面 • 启用远程桌面 • 启用/禁用 Bluetooth • 强制签入 • 锁定 • 删除自定义属性 • 重新启动/关闭 • 设备合规性状态同步 • 设备停用 • 发送消息 • 设置所有权 • 解除锁定 • 擦除
iOS macOS Android Windows	• 分配到合法所有者（适用于共享 iPad） • 重新安装 iOS 系统应用 • 设置时区 • 设置 macOS 自动管理员密码 • 设置/更改固件密码 • 设置/更改恢复锁定 • 进入自助服务终端模式 • 推出单应用模式 通过 Ivanti Bridge 的脚本和操作

对设备执行操作

“操作”菜单（省略号按钮）允许您对所选设备执行各种操作。

步骤

1. 点击设备名称。 设备详细信息页面打开。
2. 点击操作（省略号）菜单可执行以下设备操作之一：
   - 更改设备名称
   - 删除设备
   - 编辑群组成员身份
   - 启用/禁用 Bluetooth
   - 通过 Ivanti Bridge 的脚本和操作
   - 拉取 Ivanti Bridge 日志
   - 放弃所有权
   - 请求调试日志
   - 重新启动/关闭设备
   - 停用
   - 设置所有权
   - 设置/更改恢复锁定
   - 擦除
   - 设备合规性状态同步

设置设备的时区

适用于：iOS 14.0+ 和 tvOS 14.0+ 设备

此操作无需定位服务。 设备的设备详细信息页面也会显示时区设备操作。 Ivanti Neurons for MDM 服务器也将反映在设备中实施的时区更改。

> 如果在 iOS 限制配置中启用了**强制执行自动日期和时间**限制，此设备操作会引起错误。

步骤

1. 选择一台或多台设备。
2. 对于选定设备，点击**操作** > **设置时区**。
3. 使用 Olson 时区 ID 格式，输入时区字符串。 例如，Pacific/Midway。
4. 点击**设置时区**。

按条件列出设备

可以使用“筛选器”侧面导航栏搜索和查看整个设备列表中的特定设备。 使用“空间”下拉列表可选择所有空间或特定空间，以查看设备及其相关信息。 您也可以使用显示版本或绑定版本搜索设备。 “设备”页面将显示设备的绑定版本和显示版本。

> 在“设备组”页面中点击**设备数量**列下方列出的数字，或在**应用程序清单**页面中点击**已安装数量**列下方列出的数字，将显示一则消息，指示页面中列出的设备的空间名称。

显示详细的设备信息

单击条目“名称”列的链接，显示“设备详细信息”页面。 “设备详细信息”页面内含若干组织以下信息的选项卡：

- **概述** - 下表列出了“概述”选项卡中显示的所有详细信息：
- **配置** - 显示已应用 {{配置的详细信息。}}有关详细信息，请查看使用配置。

章节名称	说明
常规	• 设备位置 • 制造商 • Wi-Fi MAC 地址 • WiFi-IP 地址（Android 设备） • Network 绑定 -（iOS 设备） • 具有电池 -（仅适用于 macOS 13.3+） • IP 地址 • 公用 IP 地址 - 显示 Android 或 ChromeOS 设备的 IP 地址。 如果设备连接到 VPN 或代理服务器，则显示代理 WAN IP 地址。 • 型号 -（macOS 13.3+ 和 iOS 16.4+） • 序列号 • 备用序列号（Android 设备）- 制造商特定序列号适用于设备管理员或设备所有人模式中的 Samsung 设备。 • 锁定 PIN - 管理员可以远程锁定已托管设备并生成唯一的 PIN 以手动解锁。 选择**查看**以在**设备详情**页面上为具有管理员权限的用户显示 PIN。 仅适用于 macOS 设备。 • 存储使用情况 - 设备上的已用（Windows 除外）和可用内存 • 可用电池 (Android) • 电池状态 (Android) - 正在充电、正在放电、已充满和未在充电 • 电池剩余电量估算 (Windows) • 电池运行时间估算 (Windows) • 更新可用 (macOS) • 可用更新名称 (macOS) • 操作系统版本 • 操作系统版本 • 补充内部版本 • 补充操作系统/版本额外信息 • Apple Silicon 设备 • 固件版本 • 设备源 • 法定所有者 • 多用户模式 • 时区 • 上次已知设备解锁密码 • 安全锁定模式 • 系统更新（Android 设备） • Zebra 补丁版本（Android 设备）

章节名称	说明
	• 最后修补程序 ID -（Windows 设备） • 最后修补程序安装于 -（Windows 设备） • MDM 注册类型 • MDM 返回服务（iOS 27.0+ 和 visionOS 27.0+）
设置	• 设备名称 • 设备标识符 • 设备 GUID • 设备注册设备（Apple 设备） • 设备注册已注册（Apple 设备） • 自动化 Device Enrollment 已启用 • 自动化 Device Enrollment 已注册 • 用户注册已注册（Apple 设备） • 注册的受管 Apple ID（Apple 设备） • 设备组 • 语言 • MDM 设备标识符 • 设备客户端 ID • 客户端应用版本 • 客户端应用捆绑 ID • 客户端已注册 • EAS 设备标识符 • 激活锁定已启用 • Apple 声明式管理已启用 • Apple DDM 应用程序已启用 • 激活锁定跳过代码 • 服务条款 • 所有权 • iTunes 帐户活动 • 设备定位服务已启用 • 已隔离 • 已阻止 Sentry • 已阻止 Access • 已阻止合规性操作 • 支持 APNS

章节名称	说明
	• 受监管（iOS 和 macOS 设备）- 标识受监管设备。 IT 团队仍直接控制设备。 受监管模式启用其他设备功能（例如，现场服务部署、零售销售点设备）、用于招待和服务的“借贷人”设备，以及教室实验室中学生之间共享的设备。 • 擦除 PIN - 单击**查看**，以显示 PIN。 • 受管 MacOS 管理员用户（macOS 设备） • 本地 macOS 管理员密码（macOS 设备）- 选择**查看**，查看使用自动化设备注册的注册和受管设备的**管理员密码**、**密码上次轮换时间**、**下次轮换**和**原因**信息。 管理员查看密码后，可能还需要一个小时（下一次签入）才能从显示的**下次轮换**时间中轮换密码 • 设备加密状态（macOS 设备） ◦ FileVault 加密已启用 ◦ 个人恢复密钥已使用 ◦ 机构恢复密钥已使用 • 启动令牌可用 • 已启用系统完整性保护 • 固件密码 ◦ 密码 ◦ 更改等待处理 ◦ 命令状态 ◦ 允许选项 ROM • 恢复锁定 ◦ 密码 ◦ 恢复锁定已启用 • 采用 Mobile@Work for macOS 的脚本 • 防火墙设置（macOS 设备） ◦ 已启用防火墙 ◦ 阻止所有传入消息 ◦ 隐形模式 • 应用防火墙状态（macOS 设备） • 防火墙状态（Windows 设备） • 最后一次 iCloud 备份（iOS 设备） • 通行码锁定宽限期（iOS 设备） • Android ID • Android 安全补丁级别（Android 设备） • 自助服务终端模式（Android 设备） • Android SafetyNet 认证类型（Android 设备） • Android 企业版功能（Android 设备）

章节名称	说明
	• Android Work 已启用（Android 设备） • Samsung SAFE 功能（Android 设备） • 已启用 Android 工作托管设备（设备所有者） • 公司拥有设备上的 Android 工作配置文件已启用 • 防网络钓鱼本机状态 • 防网络钓鱼状态 • 防网络钓鱼 VPN 状态 • 带有工作配置文件的 Android 托管设备 • 公司拥有设备上的 Android 工作配置文件锁定已启用 • Help@Work 可用 • 支持 Zebra • Secure Apps 状态 • Secure Apps 加密状态 • 安全应用加密模式 • FCM 已启用 • MTD 激活状态
Windows 信息保护（Windows 设备）	• WIP • 应用 Locker 已配置 • EDP 强制设置
电话服务	**设备服务订阅** • 电话号码 • 移动电话技术 • IMSI • ICCID • IMEI • IMEI 2 -（仅适用于带有双 SIM 端口的 Android 设备。 适用于 Android 8.0 或更高版本） • MEID • 设备位置 • 载波 • 家用 MCC • 家用 MNC • 当前国家/地区名称 • 原籍国家/地区名称 • 移动电话技术 • 漫游

章节名称	说明
	• 当前操作员 • 当前 MCC • 当前 MNC • 数据漫游 • 语音漫游 • EID -（适用于支持的 Android 设备） **SIM 服务订阅** -（适用于支持的 iOS 设备） 对于支持的 iOS 设备，这些属性为多个 eSIM 活动服务订阅显示。 • 运营商设置版本 • 运营商设置网络 • 当前 MCC • 当前 MNC • EID • ICCID • IMEI • 数据优先 • 语音优先 • 标签 • 标签 ID • 电话号码 • SIM 卡槽 • 在漫游 • 订阅者运营商网络 **SIM 服务订阅** -（适用于支持的 Android 设备） 对于支持的 Android 设备，这些属性为多个活动服务订阅显示。 • 运营商设置版本 • 当前 MCC • 当前 MNC • ICCID • 数据优先 • 语音优先 • 订阅 ID • 电话号码 • SIM 卡槽 • 已嵌入 • 已托管

章节名称	说明
Azure 设备合规性	• Azure 设备标识符 • Azure 设备合规性状态 • Azure 客户端状态代码 • Azure 设备合规性报告时间 • Azure Intune 设备用户 UPN
Google BeyondCorp 设备合规性	• 设备标识符 • 合规性状态 • 合规性报告时间 • 用户
电池信息	• 电池电量 - 显示 Android 操作系统报告的当前电池电量 • 电池运行状况状态 - 由 Android、Mac、iOS 和 iPad 设备报告。 • 电池充电状态 - 由 Android 操作系统报告 • 电池运行状况百分比（特定于 OEM）- 设备（来自支持的设备制造商，如 Zebra）的电池运行状况百分比 • 电池制造日期 (OEM) - 设备（来自支持的设备制造商，如 Zebra）的电池制造日期 • 电池充电循环 (OEM) - 设备（来自支持的设备制造商，如 Zebra）总共完成的充电循环次数
设备组件健康状态（适用于 iOS 27.0+ 和 macOS 27.0+ 受监控设备）	• **基带**：指示设备基带健康状态。 • **相机**：指示设备相机健康状态。 • **显示**：指示设备显示健康状态。 • **Face ID**：指示设备 Face ID 健康状态。 • **近场**：指示设备近场通信 (NFC) 健康状态。 • **Touch ID**：指示设备 Touch ID 健康状态。 • **超宽带**：指示设备超宽带健康状况。

- **已安装的应用程序** - 显示设备上已安装应用程序的详细信息。 已安装应用程序的当前版本的安装日期会显示在**应用程序报告日期**列下。 按如下方式搜索设备上已安装的应用程序：
- 应用名称
- 捆绑包或程序包 ID

> 对于结束隔离的设备，其应用安装日期是设备从隔离中移除的日期。

> 如为 Android Enterprise 设备，还可查看按天、周、月或年排序的已安装应用程序使用详细信息。 要查看这些详细信息，必须在**配置设置**部分选择**启用应用程序使用数据收集**选项，然后选择**应用程序使用 - 天**、**应用程序使用 - 周**、**应用程序使用 - 月**、**应用程序使用 - 年**选项以查看应用程序使用详细信息。

- **可用的应用程序** - 显示设备可用的应用程序的详细信息。 按如下方式搜索设备的可用应用程序：
- 应用名称

- 捆绑包或程序包 ID

在**应用程序配置**列中，选择**配置名称**后，系统将定向到应用程序目录的**应用程序配置**选项卡，以便查看应用程序配置选项。 如果需要，可以在**应用程序配置摘要**页面上修改设备的应用程序配置。 有关配置应用程序的详细信息，请参阅应用配置。

在**应用程序配置**列中，当选择**配置名称**时，您将被定向到应用程序目录的**应用程序配置**选项卡以查看应用程序配置选项。 如果需要，可以在**应用程序配置摘要**页面上修改设备的应用程序配置。 有关配置应用程序的详细信息，请参阅应用配置。

> 请务必记住已分配设备的特定应用程序配置名称和类型，这些信息可以在**应用程序配置**页面上找到。

> **状态**列指示设备上的应用程序安装状态。 仅会为托管应用程序捕获应用程序安装状态。 非托管应用程序的应用程序安装状态会显示为“未安装”。 必须将应用程序转换为托管应用程序才能查看正确的安装状态。

- **AppConnect 应用程序** - 已安装 AppConnect 应用程序的详细信息。
- **策略** - 已应用{{策略}}的详细信息。 对于受影响的设备，请检查“违规”列中的违规原因。 如果设备已经生根，系统会显示**违规**列中显示的原因：

优先级（1 = 最高）	违反
1	插件受损
2	客户端被篡改
3	未知的设备制造商：未知
4	检测到可疑文件夹：[path]
5	可疑二进制文件位于：[path]
6	文件夹/数据可浏览或文件夹/数据/数据可浏览
7	Found /system/app/Superuser.apk
8	软件包管理器受损
9	发现可疑应用程序：[package]

- **证书** - 已安装证书的详细信息。
  要使用证书，请检查“使用类型”列。 如果证书是特定于设备的，则会将使用类型显示为“设备”。 如果证书是特定于用户的，则会将使用类型显示为“用户”。
- **Sentry** - Sentry 信息（ActiveSync 关联）
- **属性** - 自定义属性和设备属性
- **用户** - 显示受监管 MacOS 设备的活动用户的列表。

> **用户**选项卡已获得功能增强，并将受管 Apple ID 显示为超链接，点击该链接将重定向到共享 iPad 设备中的用户帐户详细信息页面。

- **日志** - 查看和自定义设备筛选条件。 可以从筛选器执行下列操作：
  - 选择操作名称，根据应用程序操作筛选设备。
  - 选择状态。

- 指定开始日期和结束日期。

- **硬件** - 硬件库存详细信息（系统、母板、BIOS、硬盘、CD ROM、处理器和物理内存）

为设备批量分配或更改用户和自定义属性

可以使用"通过上传进行批量分配"图标上传 CSV 文件，以批量向设备分配或更改用户和/或自定义属性。

步骤

1. 在"设备"页面上，单击**通过上传批量分配**图标（"操作"按钮旁边）。
2. （可选）单击**下载模板**以保存您可以编辑和上传的 CSV 模板文件。
3. 准备好 CSV 文件后，单击**选择文件**，浏览到 CSV 文件位置，或将 CSV 文件拖放到文件数据部分。
4. 选择下列选项之一：
   - **强制分配（覆盖）所有属性，即使已找到任何现有值**
   - **仅当值为空时才进行覆盖，并跳过具有现有值的属性**

单击**上传**。

将设备导出到 CSV 文件

可以使用**设备**页面中的**导出到 CSV** 选项，导出特定设备的设备详细信息。

步骤

1. 转到**设备**。
2. 选择全部或多个空间，可查看特定空间的相关信息。
3. 点击设备计数链接。 随即将显示与所选空间相关的设备列表页面。
4. 点击**导出到 CSV** 选项，可将设备列表和相关详细信息导出到 CSV 文件。 随即将显示一条弹出消息，提示需要一些时间来完成报告导出。等待请求完成后再提交另一个请求。 报告就绪后，您将收到下载或删除报告的提示消息。
5. 点击**下载**。 您还将收到一封电子邮件，其中包含下载报告的链接。
6. （可选）点击**删除**可删除报告。

搜索设备日志

步骤

1. 前往**设备** > **设备**，点击条目的**名称**列链接。
2. 单击**日志**选项卡。
3. 使用"操作"、"状态"、"开始日期"和"结束日期"筛选条件来缩小显示的设备范围。 可以从筛选器执行下列操作：
   1. 选择操作名称，根据应用程序操作筛选设备。
   2. 选择状态。
   3. 指定开始日期和结束日期。
4. "设备详细信息"列将显示应用程序的状态，如下所示：
   对于所有设备，状态将显示以下详细信息：
   - 应用名称、应用版本、捆绑包或包 ID
   - 安装状态

- 任何错误以及错误原因
  例如 - appOrConfigName=Name:<app name>;Identifier=<bundleid>;iTunesStoreId:<itunesid>;Status:<status or error reason from Apple>version: <app version>

对于 Windows 设备，状态将显示以下详细信息：

- 包括捆绑包 ID 或包 ID、状态和错误
  例如 -
- 对于类型 - 应用程序清单和状态 - 确认 - 显示 - appType
- 对于类型 - 应用程序清单和状态 - 发送中 - 不显示任何内容
- 对于类型 - 安装/卸载和状态 - 成功/失败/发送中 - 显示包括捆绑包 ID 或包 ID、状态、名称、版本和错误

如果您未看到**设备**页面，这可能是您没有所需权限。 您需要以下角色之一：

- 设备管理
- 设备只读

7.2. 设备组

本部分包含以下主题：

- 添加设备组
- 移除设备组
- 将设备导出到 CSV 文件
- 将自定义属性分配到设备组

在**设备组**页面中，可以创建要以相同方式进行处理的设备列表。 可以定义策略和配置并将它们分配至设备组。 以下是由 Ivanti Neurons for MDM 创建的默认设备组：

- 所有设备
- Android 设备
- Android Enterprise 设备
- iOS 设备
- 设备类型 (Apple)
- tvOS 设备
- macOS 设备
- visionOS 设备
- watchOS 设备
- Windows 设备

对于分配到特定设备组的应用的详细信息，将显示在特定设备组的**应用**选项卡下方。

添加设备组

> 添加设备组不适用于动态用户组。

基于您拥有的许可证类型，您可以根据规则添加新的设备组，以识别满足特定条件的设备。 符合规则的设备会显示在"规则生成器"小节下方。 规则可以使用 ANY (OR) 或 ALL (AND) 选项嵌套在一起。 可以使用下列运算符构建规则：

- 开头为
- 结尾为
- 包含
- 不包含
- 开头不为
- 结尾不为
- 小于
- 大于
- 在范围内
- 等于
- 不等于

- 不为空
- 为空

在规则生成器中选择"用户组名称"属性后，Ivanti Neurons for MDM 管理员门户会显示重复用户组的数量和相应的 GUID 数量，以便识别重复组。 此外，此规则下方的表会显示重复用户组的列表及其详细信息，例如用户组名称、GUID、来源和可分辨名称 (DN)。

Bronze 许可证：

规则可通过下列条件识别设备：

- 设备类型
- OS - 操作系统（预填充）
- 操作系统版本
- 操作系统及版本
- 用户组

Silver 许可证：

规则可通过下列条件识别设备：

- 已注册 Entra ID
- 备用序列号（仅限 Android - 适用于设备管理员或设备所有人模式中的 Samsung 设备）
- Android 专用设备
- Android 企业版能力
- 带有工作配置文件的 Android 托管设备
- Android SafetyNet 认证类型
- Android Work 已启用
- Android 安全补丁级别（Android 设备）
- 已启用 Android 工作托管设备（设备所有者）
- Android 工作配置文件已启用
- 公司拥有设备上的 Android 工作配置文件已启用
- 防网络钓鱼本机状态
- 防网络钓鱼状态
- 防网络钓鱼 VPN 状态
- 支持 APNS
- Apple Silicon 设备
- 自动化 Device Enrollment 已启用
- 自动化 Device Enrollment 已注册
- Azure 设备标识符
- Azure 设备合规性状态
- Azure 客户端状态代码
- Azure 设备合规性报告时间
- 基带健康状态

- BitLocker 加密
- 已阻止 Sentry
- 已阻止 Access
- 启动令牌可用
- 批量配置类型（Apple 配置器或无）
- 载波
- 相机健康状态
- 客户端上次签入
- 客户端已注册
- 合规性
- 已阻止合规性操作
- 当前国家/地区名称（从下拉列表中，选择当前国家/地区名称）
- 当前 MCC
- 当前 MNC
- 自定义设备属性
- 自定义 LDAP 属性
- 自定义用户属性
- 数据漫游
- 设备名称
- 已注册设备
- 设备源
- 设备类型
- 显示名称
- 显示健康状态
- 加密已启用
- Face ID 健康状态
- 硬盘驱动器分区
- 住宅所在国家/地区名称（从下拉列表中，选择住宅所在国家/地区名称）
- 家用 MCC
- 家用 MNC
- IMEI
- IMEI2（仅适用于具有双 SIM 端口的 Android 设备，并且设备必须为 Android 8.0 或更高版本）
- 机构恢复密钥已启用
- IP 地址
- 单应用模式
- 上次签入
- 仅限 MAM

- 制造商
- MDM 注册类型
- MDM 返回服务（iOS 27.0+ 和 visionOS 27.0+）
- 多用户模式 (iOS 27.0+)
- MTD 激活状态
- NFC 健康状态
- 操作系统
- 操作系统构建版本
- 操作系统版本
- 操作系统版本
- 操作系统及版本
- 所有权
- 手机号码
- 公用 IP 地址（Android 或 ChromeOS 设备）
- 个人恢复密钥已启用
- 已隔离
- 恢复锁定已启用
- 漫游
- Secure Apps 状态
- 安全锁定模式
- 序列号
- 状态
- 受监控
- 系统版本
- 设备总容量
- 总内存 (MB)
- TPM 版本
- Touch ID 健康状态
- 解锁令牌可用 (iOS)
- 用户注册已启用
- 用户组
- 超宽带无线电健康状态
- 语音漫游
- macOS 个人恢复密钥已托管
- macOS 恢复密钥类型

步骤

1. 单击**添加**。

2. 输入组的名称。
3. 输入组的可选描述。
4. 选择您要创建的设备组：
   - **动态管理**：使用规则定义组中的设备。
     - **从高级搜索加载**：选择此选项可打开已保存搜索的库。 选择查询将根据所选搜索自动填充设备组的名称和规则条件。

     > 您可以通过导航到**设备** > **设备** > **高级搜索**来创建和保存这些查询。 保存的任何查询将自动可用于在此处加载。

   手动管理：输入设备将纳入组的每个用户。
5. 对于动态管理组：
   1. 创建定义组的规则。
   2. **示例**：OS 是 iOS
      如果需要，单击 **+** 创建其他规则。
   3. **示例**：设备是 iPhone 5S
      如果设备需要与至少一个规则匹配，则单击**任意**。
   4. 如果设备需要匹配所有规则，则单击**所有**。
6. 对于手动管理组：
   1. 键入用户名称，此用户指您要将其设备添加的用户。
   2. 从显示的列表中选择设备。
   3. 重复步骤 a 和 b，直至所有设备都在列表中显示。

单击**保存**。

移除设备组

步骤

1. 转到**设备** > **设备组**。
2. 单击您想要移除设备组的复选框。
3. 单击**删除设备组**。

将设备导出到 CSV 文件

可以使用**设备组**页面中的**导出到 CSV** 选项，导出特定设备组的设备详细信息。

步骤

1. 前往**设备** > **设备组**。
2. 选择全部或多个空间，可查看特定空间的相关信息。
3. 点击设备组计数链接。 随即将显示与所选空间相关的设备列表页面。
4. 点击**导出到 CSV** 选项，可将设备列表和相关详细信息导出到 CSV 文件。 随即将显示一条弹出消息，提示需要一些时间来完成报告导出。等待请求完成后再提交另一个请求。
5. 点击**下载**。 您将收到一封电子邮件，其中包含下载报告的链接。
6. （可选）点击**删除**可删除报告。

如果您未看到**设备组**页面，这可能是您没有所需权限。 您需要以下角色之一

- 设备管理
- 设备只读

将自定义属性分配到设备组

管理员现在可以将自定义属性直接分配给设备组。 任何成为设备组成员的设备都会自动继承配置的自定义属性值，从而无需在注册后手动将属性分配给单个设备。 使用设备组自动将自定义属性值分配给成为组成员的设备。

步骤

1. 前往**设备** > **设备组**。
2. 选择现有组或创建一个组。
3. 在设备组详细信息页面中，单击**属性**。
4. 单击**新增**。
5. 选择自定义属性并指定所需值。

7.3. 未托管设备

本部分包含以下主题：

- 阻止设备
- 解除阻止设备
- 清除设备列表中的设备

许可证： Silver

如果您已经设置 Sentry 电子邮件访问控制，任何访问您的电子邮件系统的未注册设备均称为未托管设备。 **设置 Sentry** 时，您将定义默认情况下未托管设备是否可以访问电子邮件。 您可以手动选择允许或阻止这些设备访问电子邮件。

> 未托管设备页面每 5 分钟更新一次。 因此，管理上的变更不会立即反应出来。

阻止设备

步骤

1. 选择该设备。
2. 选择**操作 > 阻止**。

选择**操作 > 允许**或**操作 > 删除**之前，设备将一直被阻止。

解除阻止设备

步骤

1. 选择该设备。
2. 选择**操作 > 允许**。

选择**操作 > 阻止**或**操作 > 删除**之前，设备将始终可以访问电子邮件。

清除设备列表中的设备

步骤

1. 选择该设备。
2. 选择**操作 > 删除。**

设备下次尝试访问电子邮件系统时，设备将在列表中再次显示，您需要重复之前对设备执行的阻止或允许操作。

7.4. 应用库存

本部分包含以下主题：

- 筛选应用的显示
- 显示应用的已安装设备
- 显示应用的列表
- 显示设备上已安装的 Win32 应用程序或 Win32 应用商店应用程序
- 创建自定义视图权限
- 导出应用程序清单

应用清单是在注册设备上检测到的应用列表。 作为管理员，您可以使用此页面获取注册设备正在使用的应用程序的信息。 您可回答如下问题：

- 哪些应用是最流行的？
- iOS 设备是否直接从 App Store 获取应用？
- 有多少 Android 用户下载了可选{{内部应用}}？
- 多少设备在使用过期版本的应用？

筛选应用的显示

在您显示**设备 > 应用库存**页面时，将列出所有应用。 如要缩小列表中所显示应用的范围，请使用筛选器（左窗格）。 例如，要缩小列表范围以仅显示来自 Google Play 的私人应用，在**来源**部分中选择**私人**。

通过从下拉列表中选择多个空间，您可以查看所有或多个空间设备之间的应用库存。 在您将鼠标悬停在显示的应用上时，将显示设备计数。 您可以单击应用的计数，以显示包含应用的所有设备。 每个应用库存记录将按空间分组。

您可以使用应用程序名称或捆绑包/程序包 ID 进行搜索。

如果已选择多个空间，则将鼠标悬停在**已安装数量**列中的**总计**值上将显示每个设备空间的安装计数。

显示应用的已安装设备

点击**已安装数量**列中列出的**托管**、**未托管**或**全部**数量。

显示应用的列表

单击应用库存中针对应用的 **# 请求链接**，以查看请求应用的设备。 这仅适用于仅限 MAM 的设备。

显示设备上已安装的 Win32 应用程序或 Win32 应用商店应用程序

如果设备的隐私配置允许收集该设备上所有应用程序的信息，则应用程序清单会在该设备上显示 Win32 应用程序或 Win32 应用商店应用程序。 可以配置设备的隐私政策。

步骤

1. 通过遵守设备中的指示，确定将哪些隐私配置应用到所需的设备。
2. 转至**配置**。
3. 对于隐私配置，如步骤 1 中提到的那样：
    1. 选择配置。

2. 单击“编辑”。
3. 在**收集应用库存**中，选择**针对设备上的所有应用**。
4. 单击**完成**。

> Win32AppInventory CSP 在设备上运行清单扫描后，会每 24 小时返回设备上安装的所有 Win32 应用程序或 Win32 应用商店应用程序的列表。

创建自定义视图权限

可以为用户指定自定义查看权限。

步骤

1. 转至**管理员** 。
2. 转到**角色管理**。
3. 单击**添加自定义角色**。
4. 选择**特定于空间的角色**选项。
5. 在**名称**字段中输入用户名。
6. 从**设备**菜单中，单击**应用库存**。
7. 选中**视图**复选框。
8. 从**设备**菜单中，单击**设备操作**。
9. 单击**保存**。
10. 转到主菜单中的**用户**。
11. 单击您创建的新用户。
12. 单击**分配角色**。
13. 选择**应用 | 特定于空间**复选框，单击**下一步**。
14. **摘要**页面会显示分配到您创建的角色的权限。
15. 单击**完成**。
16. 以新用户身份登录。
17. 从主菜单中单击**设备**。
18. 单击**应用库存**。
19. 现在，**应用库存**页面仅为用户显示允许的应用。

导出应用程序清单

作为管理员，您可以使用**导出到 CSV** 选项请求应用程序清单报告。

步骤

1. 转到**设备 > 应用程序清单**。
2. 从列表中选择一个清单。
3. 点击**导出为 CSV**。
4. 选择下列选项之一：

- **将应用程序导出到 CSV** 可以导出应用程序清单中的所有应用程序。
- **将设备导出至 CSV** 可以按照下表导出特定的应用程序：

选项	描述
捆绑包 ID	输入应用程序的捆绑包/程序包 ID。
是否导出	选择下列选项之一： • 安装总计 • 托管 • 未托管 • 已请求（针对仅 MAM 设备）

5. 点击**导出**。

管理员将收到一个弹出窗口提示，通知报告的导出需要一些时间来处理。 提交请求后，管理员必须等待请求完成才能提交另一个请求。 报告就绪后，管理员将收到下载或删除已生成报告的提示消息。 管理员还将收到一封电子邮件，其中包含下载报告的链接。

如果您未看到**应用库存**页面，这可能是您没有所需权限。 您需要以下角色之一：

- 设备管理
- 设备只读

7.5. 管理设备

本部分包含以下主题：

- 部署 Windows 设备
- 在 macOS 设备上设置 Apple 远程桌面
- 设备注册（iOS、macOS 和 Android）
- 设备注册（Windows 10+ PC 和 Microsoft Hololens 2）
- 使用 PIN 配置软件包注册
- 使用针对 Windows 设备的批量注册
- 更改通行码设置
- 更改设备名称
- 查找并筛选设备
- 使用设备所有者
- 带有工作配置文件的托管设备
- 使用 Android 的批量注册
- 使用 CSV 文件上传进行批量注册
- 使用 Samsung Knox 移动注册
- 注册 Oculus 设备
- 启用设备上的 Bluetooth 功能
- 计划 iOS 更新
- 重新安装 iOS 系统应用
- 将设备分配到新用户
- 重新分配 Android 设备
- 强制设备进行签入
- 定位设备
- 锁定设备
- 管理遗失模式下的 Apple 设备
- 请求调试日志
- 停用设备
- 放弃设备的所有权
- 擦除设备
- 删除设备
- 解锁设备
- 重新启动或关闭设备
- 清除限制密码（仅 iOS）
- 删除设备的 Sentry 关联
- 将自定义属性分配到设备

- 将自定义属性从设备中删除
- 同步和获取应用反馈
- 设置固件密码
- 重新发布新个人恢复密钥
- 设置或更改恢复锁定
- Apple 访问管理
- 组策略注册

7.5.1. 部署 Apple 设备

Ivanti Neurons for MDM 支持管理所有 Apple 设备。 它是一个全面的解决方案，用于配置、管理、更新和保护您的设备组，为最终用户提供最佳的用户体验。

本部分包含以下主题：

- 安装您的 Apple MDM 证书
- 注册 Apple 设备
- Ivanti Go for iOS 客户端
- 管理 Apple 设备的应用程序
- 管理配置
- 管理软件更新
- 设置 iOS/iPadOS 设备
- 设置 watchOS 设备
- watchOS 设备支持的设备操作
- 设置 visionOS 设备
- visionOS 设备支持的设备操作
- 设置 macOS 设备
- 设置 TvOS 设备
- 支持声明式设备管理 (DDM)

安装您的 Apple MDM 证书

要管理 Apple 设备，首先请求并安装一个 Apple MDM 证书来管理 iOS 设备。 每年更新一次 Apple MDM 证书。 （接近到期日期时，用于创建证书的 Apple 帐户将收到 Apple 网站发送的通知。）使用“MDM 证书”页面来添加或更新此证书。

按照安装 MDM 证书中描述的步骤进行操作

注册 Apple 设备

您可以选择以下任意一种方法来注册设备：

- 自动设备注册
- Apple School Manager
- Apple Configurator

Ivanti Go for iOS 客户端

下一步是选择您的公司允许您的设备使用的注册类型。 Ivanti Neuros for MDM 目前支持：

- 设备注册（iOS、macOS 和 Android）
- 使用 Apple 商务管理进行用户注册
- 帐户驱动的用户注册
- 设置 (Apple)

管理 Apple 设备的应用程序

Ivanti Neurons for MDM 中的应用程序目录页面充当管理员有效管理其应用程序目录的界面。 此功能包括对最终用户可用的移动应用程序的编排，涵盖公共应用程序商店和指定为通过 Ivanti Neurons for MDM 分发的应用程序商店。

支持的应用程序：

应用目录页面聚合了各种类型的应用程序，包括公共 AppStore 应用程序、自定义应用程序、内部开发的应用程序、支持 AppConnect 的应用程序、GoClient for iOS 和 M@W for macOS，简化了后续配置和分发的导入流程。

在仅移动应用程序管理 (MAM) 配置下运行的设备上，系统会提示 iOS 用户在访问应用程序目录时选择身份验证证书。 此身份验证步骤对于保护对列出的应用程序的访问并符合稳健的安全实践至关重要。

> Apple 出品的 M1 芯片组 MacBook 为 [您的软件产品] 中的 iPhone 和 iPad VPP 应用程序提供专门支持。 值得注意的是，只有管理员有权推送支持的 iPhone 和 iPad VPP 应用程序，限制用户直接从应用程序安装它们。

有关详细的实施说明和配置选项，请参阅管理指南中提供的综合文档和以下资源：

- 管理应用程序
- 应用程序目录设置
- 设置 Apple Apps and Books
- Apps@Work 企业应用商店
- MacOS AppStore 限制

管理配置

配置是管理员发送到设备的设置集合。 例如，您可以使用配置自动设置设备上的 VPN 设置和通行码要求。 配置页面中列出了您系统的现有配置。 您可以从“配置”页面中选择多个配置，并将其一次性推送到多个设备。 可以将这些配置推送到特定空间的设备，而其他空间的设备不受影响。 可以将配置推送到单个空间或一次性推送到多个空间或所有空间。

Ivanti Neurons for MDM 中的大多数配置对于所有平台都是通用的。 有关如何使用配置的更多详细信息，请参阅使用配置。

某些配置仅受特定平台支持。 您可以按配置类型支持的平台查看列表

管理软件更新

您可以首先为 iOS 和 macOS 设备设置软件更新配置。

> 设置软件更新的计划窗口时，将每小时把操作系统更新命令推送到设备，以确保更新不会错过该窗口。 根据 Apple 的行为，每次设备收到操作系统更新命令时，都会弹出窗口通知用户进行升级。 用户最多可以推迟三次。 根据 Apple 的行为，第三次设备将强制升级。

MacOS 设备有一些可以应用的特定规则。 请参阅 macOS 软件更新规则配置

iOS 的操作系统更新命令

您还可以发送一次性命令以更新设备列表或设备页面中的一台或多台设备。 请参阅计划操作系统更新命令。

设置 iOS/iPadOS 设备

iOS/iPadOS 支持以下配置：

- iOS/iPadOS 限制
- eSIM 配置
  - 保留数据计划
- 移动网络配置
- 启用遗失模式
- 配置 iOS MDM 配置文件
- 单应用模式
  - 自动单应用程序模式
- 共享 iPad 企业版
- 教育配置
- iOS 自定义配置
- 锁屏消息

设置 watchOS 设备

现在可以在与 iOS 设备配对时，将 Apple watchOS 设备注册到 Ivanti N-MDM。

此功能目前支持：watchOS 10+。

Procedure程序

1. 您必须注册 iOS 17+ 受监督设备。
2. 将 Apple Watch 注册配置分配至 iOS 设备。
3. 您现在可以将 Apple Watch 与 iPhone 配对。

> 将手表配置推送到 iPhone 后，即可配对 Apple Watch。 如果是在 Apple Watch 与 iPhone 配对后才将手表配置推送到 iPhone，则无法为 Apple Watch 启用远程管理。

watchOS 设备支持以下配置：

- Cellular_Configuration
- 证书配置
- 证书透明度
- Identity_Certificate_Configuration
- iOS 限制
- Passcode_Settings
- Per-App_VPN_Configuration
- Wi-Fi_Configuration

watchOS 设备支持的设备操作

watchOS 设备支持以下设备操作：

- 清除密码

- 锁定 Apple watch
- 擦除 Apple watch
- 取消 Ivanti Neurons for MDM 上的 Apple Watch 注册

> 取消注册已配对的 iOS 设备将重置手表并取消与 iOS 设备的配对。

设置 macOS 设备

macOS 支持以下配置：

- macOS 限制
- 配置 macOS 设备。
- 使用脚本和 Mobile@Work 客户端
- 配置 macOS MDM 配置文件
- 设置固件密码
- 启用 FileVault
  - FileVault 恢复密钥
  - FileVault 选项配置
- 平台和可扩展的 SSO
- Active Directory macOS
- 防火墙
- 以太网
- Office 365 帐户创建
- macOS 系统扩展
- 媒体磁盘刻录限制
- 隐私设置

设置 TvOS 设备

tvOS 支持以下配置：

- Apple TV 配置
- Apple TV 限制
- 会议室显示
- AirPlay 镜像

设置 visionOS 设备

现在可以将 Apple visionOS 设备注册到 Ivanti Neurons for MDM。

此功能目前支持：visionOS 1.1+

或者，您可以使用以下任一方法注册 visionOS 设备：

- 账户驱动的设备注册

- 帐户驱动的用户注册
- 设备注册

visionOS 设备支持以下配置：

- CalDAV 配置
- CardDAV 配置
- 证书配置
- 证书吊销检查配置
- 证书透明度
- 创建 DNS 代理配置
- 加密的 DNS
- 电子邮件配置
- Exchange 配置
- Google 配置
- 身份证书
- iOS 限制
- LDAP 配置
- 托管域
- 网络中继配置
- Per-App VPN 配置
- 单点登录配置
- 订阅日历配置
- VPN 配置
- Web 内容筛选
- Wi-Fi 配置

visionOS 设备支持的设备操作

visionOS 设备支持以下设备操作：

- 擦除 Apple Vision Pro
- 停用 Apple Vision Pro
- 解锁 Apple Vision Pro

支持声明式设备管理 (DDM)

Apple 声明式设备管理是一种现代管理协议，允许受管理设备以更少的通信主动、自主地应用自己的管理设置。 在注册期间或已注册设备签入期间，新注册的设备上将启用声明式设备管理。

声明式设备管理将在符合以下条件的设备上自动启用：

- 运行 macOS 13 或更高版本的计算机
- 具有 iOS 16 或 iPadOS 16 或更高版本的设备

- 通过用户注册而注册的设备在 iOS 或 iPadOS 15 或更高版本上支持声明式设备管理。
- 运行 tvOS 16 或更高版本的 Apple TV 设备
- 运行 watchOS 10 或更高版本的 Apple Watch 设备
- 运行 visionOS 1.1 或更高版本的 Apple Vision Pro 设备

当前支持的声明式管理功能：

- **状态通道**
  - 操作系统版本变更
  - 密码合规性
  - 存在密码
- **配置**：
  - 声明式管理配置

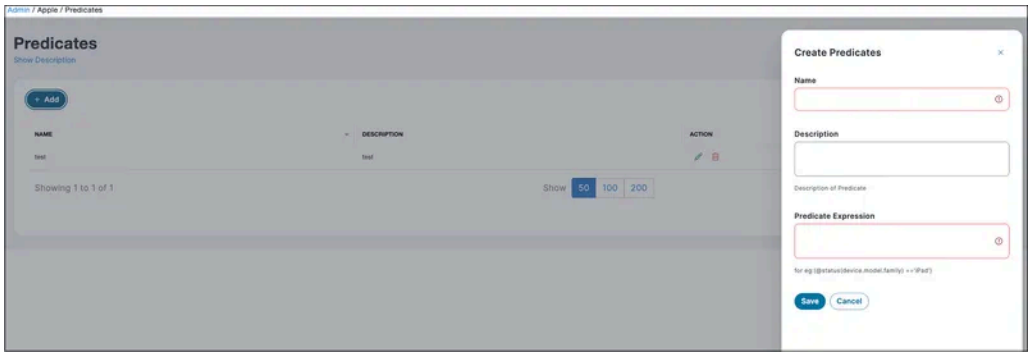
DDM 配置中的谓词

谓词是 Cocoa 语言中的表达式，有助于灵活、精细化地激活设备上的配置。 表达式位于设备上，将在满足相关谓词的条件时进行应用。 新功能已添加，可在其中创建、保存谓词，以及将谓词应用于任何 DDM 配置。

DDM 配置已在“分发”页面中显示新选项，可用于应用谓词。 在此部分，可从下拉列表中找到已创建的谓词。

创建谓词

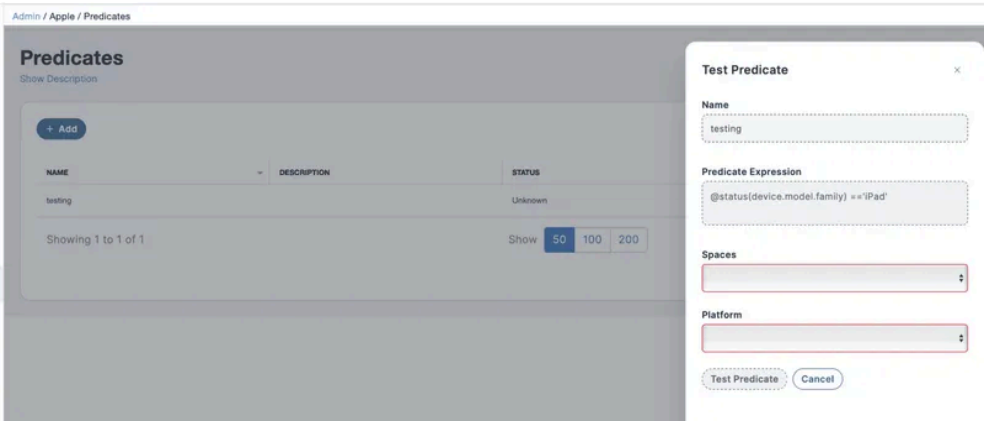
1. 转到**管理员** > **Apple** > **谓词**。
2. 单击**添加**。 **创建谓词**窗口随即显示在屏幕上。
3. 输入以下信息：
   - **名称** - 谓词的名称
   - **描述** - 添加相关描述
   - **谓词表达式** – 谓词表达式。 例如，@status(device.model.family) ==’iPad’



4. 单击**保存**。 屏幕上随即显示对话框，用于确认谓词的创建。
5. 通过刷新页面并观察状态字段中的值（值为：**未知**、**进行中**、**有效**、**无效**）来检查谓词语法的有效性。
   1. 单击**测试**。 **测试谓词窗口**随即显示在屏幕上。
   2. 输入以下信息：
      - **名称** - 默认
      - **谓词表达式** – 默认

- **空间** – 默认空间
- **平台** – iOS/macOS
- **设备名称** – 与谓词表达式相关。

> 只有从下拉菜单中选择了**空间**和**平台**字段详细信息后，**设备名称**字段才会出现在**平台**字段下方。



3. 单击**测试谓词**。
4. 屏幕上随即显示对话框，用于确认测试谓词的启动。
5. 刷新页面以查找谓词语法的状态。
   - 对于正确的谓词表达式，状态将按**未知** > **进行中** > **有效**进行更改。
   - 对于不正确的谓词表达式，状态将按**未知** > **进行中** > **无效**进行更改。
6. 如果要使用不同的谓词表达式创建多个谓词，请重复此过程。

分发 DDM 配置的谓词

1. 创建 DDM 支持的配置。
2. 将使用谓词激活切换为“打开”，然后使用 + 按钮来包含谓词（根据需要）。



要编辑或删除谓词，请转到**管理员** > **Apple** > **谓词**。 在此页面中可以找到可用的谓词列表。 点击**编辑**可更改现有谓词并保存。 同样，要删除现有谓词，请选择相关谓词并点击**删除**。

> 如果谓词已关联任何配置，则无法删除谓词。

DDM 配置的管理属性

管理员可以使用以下方式来创建谓词：

- 用户和设备变量
- 用户属性
- 设备属性

在谓词（自定义属性）中使用管理属性的示例：

用于检查用户的名字是否为 'test' 的谓词：@property（userFirstName）=='test'

更多示例

- 设备的硬件系列：（Mac、iPhone、iPad 等）
  @status(device.model.family) =='iPad'
  如果为 True，则设备上存在密码。 如果为 False，则设备上不存在密码。
  @status(passcode.is-present)==true
- 设备上使用的操作系统系列，例如 macOS 或 iOS。
  @status(device.operating-system.family)=='iPadOS'
- 设备上使用的操作系统版本，例如 15.0
  @status(device.operating-system.version)=='18.2'
  @status(device.operating-system.version)<'18.3'
  @status(device.operating-system.version)>='18.2'
- 用于指定设备上的“FileVault 已启用”状态的布尔值
  @status(diskmanagement.filevault.enabled)==true
- 管理属性（自定义属性）示例：
  用于检查用户的名字是否为 'test' 的谓词
  @property(userFirstName)=='test'

7.5.2. 部署 Windows 设备

本部分包含以下主题：

- 概述
- 设备管理
- Windows 设备注册和登记
- Windows 更新管理
- 应用程序管理和分发
- 应用程序控制
- Windows 设备管理配置
- Windows 设备合规性
- Windows 应用程序和硬件清单

概述

Ivanti Neurons for MDM 可帮助您管理所有 Windows 笔记本电脑和台式电脑，包括 HoloLens 2 端到端设备生命周期管理：从配置、注册、预配、保护、应用程序、管理、监控、软件、操作系统更新直至停用。

设备管理

支持的 Windows 设备：

- Windows PC 10+
- Microsoft HoleLens 2

有关设备管理和报告功能的更多信息，请参阅设备。

Windows 设备注册和登记

Ivanti Neurons for MDM 支持 Windows 设备的所有标准设备注册方法：

- 手动注册
- 批量注册
- 通过 SCCM 和 Ivanti EPM
- Windows Autopilot
- Entra ID 注册

有关注册方法的更多信息，请参阅使用 Microsoft Azure。

有关多用户支持的信息，请参阅 Windows 设备的多用户支持。

Windows 更新管理

- 配置和计划 Windows 更新 - 要配置和计划 Windows 更新，请使用“配置 - 软件更新”来创建配置。
- Windows 更新管理 - 您可以使用 Windows 更新管理来查看和批准要更新的 Windows 设备所报告的更新。 通过使用此功能，您可以防止在设备上安装不必要或未经测试的更新。 有关详细信息，请参阅 Windows 更新管理。

应用程序管理和分发

用户可以管理 Windows 应用程序的完整应用程序生命周期（导入、配置、计划、分发、更新和删除）。

支持的应用程序类型：

- 内部
- MSB
- 公共应用商店

支持的应用程序扩展名：

- MSI
- MSIX
- APPX
- APPX 捆绑包
- EXE (Bridge)

有关管理 Windows 应用程序的更多详细信息，请参阅应用配置。 要自动执行应用程序更新，请参阅 Windows 应用计划和使用配置。

应用程序控制

应用控制配置支持您在设备级将应用分类为允许列表或阻止列表。 已安装的应用将不可见且无法启动。 应用仍将在 App Store 中可见，但无法下载或启动。 向其分发应用程序控制配置的任何设备都将使用此配置并忽略任何允许的应用策略设置。 应用程序控制配置取代目标设备上同一应用程序所涉及的任何应用程序相关策略。

有关更多详细信息，请参阅应用控制配置：控制每个设备上安装哪些应用。

Windows 设备管理配置

Windows 10+ PC 和 Microsoft HoloLens 2 支持包括以下功能：

- 设备注册（Windows 10+ PC 和 Microsoft Hololens 2）
- 通行码配置
- Exchange 配置
- 配置
- 设备
- 应用
- Windows 应用计划
- 应用控制配置：控制每个设备上安装哪些应用
- Windows 更新管理
- 从 Ivanti Neurons for MDM 向 Azure 报告设备状态
- 配置 Windows Autopilot 配置文件
- 使用自定义配置向设备推送 SyncML
- 策略
- Windows 限制

- 身份证书
- Windows Hello for Business
- Wi-Fi 和 VPN 配置文件

> 分发到此设备类型不支持的 HoloLens 设备的配置将不会在“设备详细信息”的“配置”选项卡下报告为已分发的配置。

Windows 功能（仅 Windows PC 支持该支持）：

- Ivanti Bridge
- Windows BIOS 配置
- Windows BitLocker
- Windows 自助服务终端配置
- Windows 许可证配置
- EMA 服务器集成配置
- 打印机设置
- 删除 Bloatware 配置
- ADMX (GPO) 浏览器

Windows 设备合规性

可使用 Microsoft Azure 设置 Ivanti Neurons for MDM，以便用户在运行 Windows 10+ 的 Windows 台式电脑和平板电脑上实现无缝注册。要配置 Azure 租户集成以启用 Windows 设备合规性，请参阅使用 Microsoft Azure。

Windows 应用程序和硬件清单

Windows 应用程序清单

应用程序清单是在注册设备上检测到的应用程序的列表。 可通过该页面获取注册设备所使用的应用的信息。 有关详细信息，请参阅应用库存。

> 如果设备的隐私配置允许收集该设备上所有应用程序的信息，则应用程序清单会在该设备上显示 Win32 应用程序或 Win32 应用商店应用程序。

配置应用程序清单间隔。

您可以为多个应用程序源类型清单设置 Windows 10 应用程序清单收集间隔。 当隐私政策设置为从设备收集所有应用程序时，系统将使用该间隔。

有关详细信息，请参阅配置应用库存间隔。

Windows 硬件清单

您可以启用从 Windows10+ 设备收集硬件信息。 这些详细信息可使用 Bridge 进行检索。 有关详细信息，请参阅硬件库。

7.5.3. 在 macOS 设备上设置 Apple 远程桌面

本部分包含以下主题：

- 在 macOS 设备上启用 Apple 远程桌面
- 在 macOS 设备上禁用 Apple 远程桌面

在 macOS 设备上启用 Apple 远程桌面

可通过 Apple 远程桌面功能启用屏幕共享功能，进而对设备进行远程管理。 Apple 远程桌面功能适用于受监管的 macOS 10.14.4+ 设备。

步骤

1. 转到**设备**，选择一个或多个受监管的 macOS 设备。
2. 单击**操作** > 为设备**启用远程桌面**操作。
3. 单击**启用远程桌面**进行确认。

在 macOS 设备上禁用 Apple 远程桌面

程序

1. 转到**设备**，选择一个或多个受监管的 macOS 设备。
2. 点击**操作** > 为设备**禁用远程桌面**操作。 屏幕共享功能已禁用，您无法对设备进行远程管理。

7.5.4. 设备注册（iOS、macOS 和 Android）

本部分包含以下主题：

- 手动安装管理配置文件
- 发送邀请（iOS、macOS 和 Android）
- 指导最终用户下载应用（iOS 和 Android）

大多数用户在开始之前都必须先注册设备。 可使用以下任意方法开始注册流程：

- 向一位或多位最终用户发送邀请（iReg 注册）
- 指导最终用户下载 Go（应用内注册）

> 如果 iOS 和 macOS 设备 MDM 注册失败并显示*配置文件安装失败且 SCEP 服务器返回无效响应* 错误，则设备用户必须从头开始重新启动设备注册流程。 在配置文件下载到设备上以后，如果设备用户完成 iOS 和 macOS 设备 MDM 注册流程所需的时间比预期要长，则会出现这种情况。 请联系 Ivanti 支持以获取更详细的说明。

对于 macOS 设备中的单用户（本地用户或已注册的 Active Directory (AD) 用户），Ivanti Neurons for MDM 支持用户级管理。 管理员可为用户管理设备，应用设备配置文件和用户配置文件，因此也会使用 App Store、应用分发、配置和策略（包含 Apps@Work、限制、安全性等）。

要管理包含 AD 用户的 macOS 设备，AD 用户需要成为在注册期间登录的用户。 任何其他未注册的用户无法查看已注册的用户特定配置文件（例如身份认证、VPN）。 但任何登录用户可以查看和使用设备级配置。

> 最终用户必须具有 Ivanti Neurons for MDM 帐户，才能开始设备注册流程。 对 LDAP 用户而言，这意味着必须设置 Connector 和 LDAP 服务器，且必须从 LDAP 服务器中导入用户。 对本地用户而言，即添加用户。

> Ivanti Neurons for MDM 早期版本生成的设备注册 URL 将不再适用于当前版本。 管理员将需要重新生成设备注册 URL。

手动安装管理配置文件

适用于：

- iOS 12.2 至 Ivanti Neurons for MDM 支持的最新发布版本。
- macOS 11.0 至 Ivanti Neurons for MDM 支持的最新发布版本。

iOS 设备注册

在 iOS 设备中进行应用内注册期间：

- 设备注册期间，使用 Go app 说明页面安装显示的配置文件。
- 点击**安装下载的配置文件**选项，然后点击**我了解**。
- 下载的配置文件将在几分钟内有效；在此之后，需要重新注册。

macOS 设备注册

要在自助门户中进行 macOS 设备注册，用户必须执行以下步骤：

步骤

1. 使用其凭据登录。
2. 在安装管理配置文件页面中，配置文件会下载到用户的本地系统。
3. 双击下载的配置文件，以使其在用户的系统首选项中可见。

> 在配置文件无效前，用户的安装时间有限。

4. 在系统首选项中，打开**配置文件**。 在配置文件下载到设备时，用户可以查看包含配置文件链接的网页。 单击**配置文件**，以打开设置应用。
5. 点击**安装**以安装管理配置文件。
6. 继续并完成安装过程。 在提示时输入系统密码。

发送邀请（iOS、macOS 和 Android）

注册流程由发送邀请开始。 可通过 Ivanti Neurons for MDM 提供的以下方法，向最终用户发送设备注册邀请：

- 使用启动向导
- 添加一名或多名用户时
- 在“用户”页面（操作 > 发送邀请）中

> 如果最终用户错误放置邀请，您可以分享邀请中列出的 URL。 确保在 URL 的末尾添加 **/go**。

如果最终用户拥有含密码的 Ivanti Neurons for MDM 帐户，无需邀请即可开始注册流程。 可以将邀请中列出的 URL 发送给他们。

指导最终用户下载应用（iOS 和 Android）

Go 应用适用于 Android 和 iOS 设备。 您可以指导最终用户从公共应用商店下载应用，并从该应用开始注册流程。 电子邮件邀请包含以下信息：

- 注册页面的链接
- 一次性 PIN（如果由管理员设置）
- 后续步骤的基本说明

如果您已经为帐户设置了密码，可以将密码发送到最终用户的企业电子邮件地址。 如果使用 LDAP 进行身份验证，需通知最终用户需要网络凭据。

如果用户在注册期间未完成 MDM 配置文件的安装，Ivanti Neurons for MDM 会定期向设备发送推送通知，提示用户完成注册流程。

用户可以使用用户名和密码，或者扫描 QR 码以便从 Go app 开始设备注册。 详情如下：

- **用户名**：电子邮件地址
- **密码**：如果已在用户设置中指定且管理员定义了临时密码
- **QR 码**：从 Ivanti Neurons for MDM 自助门户生成 QR 码。 当您尝试使用**扫描 QR 码**选项扫描 QR 码时，屏幕上会出现提示，要求您授予访问设备摄像头的权限。 在您授予权限后，摄像头会扫描 QR 码，随后设备会完成注册。 仅 Android 9 和更高版本以及 iOS 14 和更高版本支持此选项。

最终用户在移动设备上接收注册电子邮件后，点击该链接即可开始注册流程。 如果您在笔记本电脑或台式电脑上接收电子邮件，则在移动设备上的浏览器中输入该 URL 即可开始注册流程。

如果您尚未为 Ivanti Neurons for MDM 用户帐户定义密码，或者用户设置需要注册 PIN，则会包含一次性 PIN。 输入 PIN 码后，如果密码不存在，系统将提示您设置帐号密码。

> 对于 Android Enterprise 设备，注册完成后，任何手动安装到公司拥有设备或工作受管设备的工作配置文件中的 CA 证书都会被卸载。

重新注册 iOS 设备

如要重新注册设备，可以按以下步骤操作：

1. 启动设备上的 Go 客户端。
2. 转至**设置** > **故障排除** > **重新注册设备**。 重新注册流程将启动并显示一些确认提示。
3. 出现提示时，点击**是**。

> 如果在配置文件安装过程中点击**取消**，则注册流程将停止，同时 Ivanti Neurons for MDM 服务器将禁用设备 MDM。

要重新启动重新注册流程，必须重新安装已下载的配置文件。 下载的配置文件仅在几分钟内有效，之后则必须从 Go 客户端执行重新注册。

重新注册 Android 设备

管理员可以通过停用、擦除或删除操作重新注册设备，而不需要手动清除现有活动条目。 此方法特别适用于新条目和现有条目属于同一租户的重新注册情况。 “设备”页面在 Ivanti Neurons for MDM 管理门户中显示设备的状态，如下所示：

- **活动** - 设备注册成功
- **已停用** - 设备完成重置并显示为“已停用”状态
- **已擦除** - 设备完成重置并显示为“已擦除”状态
- **已重置** - 设备完成重置，并将在下次注册之前在服务器上处于活动状态

“审计跟踪”页面列出 Android 设备的设备注册、重新注册和停用状态。 有关详细信息，请参阅使用小组件。

> 对于 Android 9.x 和更低版本，在重新注册后将显示一个条目。 对于 Android 10.x 和更高版本，将显示多个条目。 但是，仅最新条目会处于活动状态，而较旧的条目将处于停用状态。

7.5.5. 设备注册（Windows 10+ PC 和 Microsoft Hololens 2）

本部分包含以下主题：

- 手动注册
  - 发送邀请
  - 完成最终用户注册流程
- Windows Autopilot
- Entra ID 标准注册

设备注册流程有以下几种类型：

- 手动注册
  - 邀请
  - 最终用户注册
- Windows Autopilot
- 使用 SCCM 和 Ivanti EPM 并通过“使用 PIN 配置程序包注册”。 请参阅使用 PIN 配置程序包注册。
- 批量注册

手动注册

大多数用户在开始之前都必须先注册设备。 可使用以下任意方法开始注册流程：

- 电子邮件邀请
- 将用户定向至 URL，以便实施
- 最终用户必须具有 Ivanti Neurons for MDM 帐户，才能开始设备注册流程。 对 LDAP 用户而言，这意味着必须设置 Connector 和 LDAP 服务器，且必须从 LDAP 服务器中导入用户。 对本地用户而言，即添加用户。
- Ivanti Neurons for MDM 早期版本生成的设备注册 URL 将不再适用于当前版本。 管理员将需要重新生成设备注册 URL。

发送邀请

在多数情况下，注册流程由发送邀请开始。 可通过 Ivanti Neurons for MDM 提供的以下方法，向最终用户发送设备注册邀请：

- 使用开始向导
- 通过添加一名或多名用户
- 使用“用户”页面（操作 > 发送邀请）

如果最终用户在使用台式或笔记本电脑接收邀请时将其放错位置，或因故未收到邀请，可将最终用户发送至位于邀请之列的 URL 中。 只需添加 **\转至**服务 URL 端即可。

如果最终用户拥有已设置密码的 Ivanti Neurons for MDM 帐户，无需邀请即可开始注册流程。 可将这些用户发送至已位于邀请之列的 URL 中。

完成最终用户注册流程

告知设备用户如何完成注册流程。 您可以使用以下说明作为模版，并做出任何必要的更改：

步骤

1. 在 Windows 10+ PC 上打开浏览器。
2. 导航至 mobileiron.com/go。
   您将被重新定向至内含注册 URL 的新页面。
3. 复制注册 URL 至剪贴板。
4. 点触**设置**页面底部的**添加帐户**。
5. 输入与您收到的邀请相关的电子邮件地址。

> 如果用户的 Ivanti Neurons for MDM 用户名与 Ivanti Neurons for MDM 中输入的用户电子邮件地址不匹配，请在提示输入电子邮件地址时告诉用户输入用户名。

将您复制到下一个文本字段的Workplace 服务器 URL 粘贴。

7. 点触**登陆**。
8. 在下一个字段中输入您的密码。
9. 将其他字段留空。
10. 点触**登陆**。
11. 在**添加的帐户**屏幕单击**完成**。
    Workplace 起始屏幕显示已经添加一个帐号。

Windows Autopilot

Windows Autopilot 是一项 Microsoft 功能，可帮助管理员设置和预配置新设备，从而为业务做好准备。 借助 Autopilot 功能，可以快速可靠和无缝地配置 Windows 桌面或 HoloLens2 设备。 此外，Autopilot 功能有助于执行以下任务：

- 自动将设备加入 Entra ID (Entra ID)
- 将设备自动注册到 MDM 服务
- 根据设备的配置文件，创建并将设备自动分配到配置组
- 自定义注册体验
- 应用配置和策略
- 安装必需应用

Ivanti 支持 Autopilot 配置文件的所有模式：

- 用户驱动
- 用户驱动的预配置（之前为白手套）
- 自部署模式

有关更多信息，请查看**配置 Windows Autopilot 配置文件**。

> 为安全和未经授权地使用设备，所有 Autopilot Windows 设备可以使用 TenantLockdown CSP 功能锁定到租户。 要使用此功能，设备必须使用 Autopilot 选项注册。 此配置在设备级别应用。 请查看 **TenantLockdown CSP**。

Entra ID 标准注册

将用户添加到 Entra ID 租户后，这些用户可以通过工作账户直接注册设备。

步骤

1. 在 Windows 设备中，转到**设置 > 帐户 > 访问工作单位或学校**。
2. 选择添加工作或学校帐户，然后点击**连接**。
3. 提供您的工作帐户的电子邮件地址

设备会自动注册到 Ivanti Neurons for MDM。

7.5.6. 本地管理员密码解决方案 (LAPS)

本地管理员密码解决方案 (LAPS) 将 Windows 设备密码的安全管理自动化。 LAPS 强制执行随机、定期的密码更改，并将这些密码安全地存储在一个目录中，从而降低了在出现泄漏时发生横向移动的风险。

现代 LAPS 与 Azure 和最新的 Windows 设备管理平台集成，通过 Ivanti Neurons for MDM 和 Azure 门户实现安全的密码存储、检索和策略配置。 这可确保管理员凭据在旧版和云受管 Windows 端点上保持受保护和可审计状态。

> 若要将 LAPS 用于 Ivanti Neurons for MDM，Azure 管理员应确保使用所需的 LAPS 权限 (**DeviceLocalCredential.Read.All**) 将 N-DMD 应用程序添加到其 Azure 租户中。

> LAPS 配置可以通过使用策略设置**管理员帐户名称**指定它应用于哪个本地管理员帐户。 如果设备上不存在配置中指定的帐户名称，则无法管理该帐户名称。 但是，当**管理员帐户名称**为空时，策略默认为设备的内置本地管理员帐户，该帐户由其众所周知的相对标识符 (RID) 标识。

> 应用 LAPS 配置后，设备的本地管理员帐户密码将由管理员管理，密码将在 Azure Active Directory 中生成。

LAPS 的其他特性

- Azure 中的密码存储 - 本地管理员密码现在可以安全地存储在 Azure 设备对象中。
- 密码检索 - 管理员可以直接通过 Azure 门户检索设备密码。
- 可配置设置 - 可以在 Ivanti Neurons for MDM 门户中管理 LAPS 可配置设置。
- 按需密码轮换 - 管理员可以从 Ivanti Neurons for MDM 门户手动轮换设备密码。
- 使用时自动重置密码 - 一旦访问密码，就可以自动重置密码。

创建 LAPS 配置

先决条件

- 必须为您的设备启用 LAPS 解决方案。 默认情况下，并非所有人都可以使用此解决方案。 请联系技术支持团队寻求帮助。
- 设备必须在 Azure Device Operations (ADO) 中注册。

步骤

1. 在您的配置管理平台中，启动 LAPS 配置的创建。
2. **设置所需参数**：
    - **备份目录** - 选择仅将密码备份到 Microsoft Entra ID。
    - **本地管理员名称** - 指定系统上的管理员帐户名（例如，Admin）。
3. **配置其他设置** - 根据组织的安全策略设置这些设置。 如果未指定，将使用默认值。
    - **PasswordAgeDays** - 本地管理员密码自动轮换前的天数。
    - **PasswordComplexity** - 指定密码复杂度要求（例如，字母数字、特殊字符）。
    - **PasswordLength** - 设置所需的本地管理员密码长度。
    - **PostAuthenticationActions** - 定义身份验证后应执行的任何操作。
    - **PostAuthenticationResetDelay** - 设置延迟（以小时/分钟为单位）以在身份验证后重置密码。

4. **分发 LAPS 配置**
    - 将 LAPS 配置文件分配给 ADO 注册的用户/设备。
    - 应用配置后，将创建一个随机的本地管理员密码，并将其安全地存储在 Microsoft Entra ID 中：
      设备 → 管理设备 → 本地管理员密码恢复。
5. **密码轮换**
    - 密码会根据 **PasswordAgeDays** 中设置的值自动轮换。
    - 您可以在设备日志中查看密码轮换状态。

密码轮换

要强制立即轮换本地管理员密码，请执行以下步骤：

1. **导航到设备** - 转到管理控制台中的设备详细信息页面。
2. **启动密码轮换**
    - 点击三点菜单 (...)。
    - 选择**轮换本地管理员密码**。
    - 出现提示时确认操作。 这将提交密码轮换请求。
3. **签入和确认**
    - 该设备在下次强制签入时处理密码更改。
    - 刷新 Microsoft Entra ID 中的页面，在密码恢复部分查看更新的密码。

7.5.7. 使用 PIN 配置软件包注册

管理员可以将 SCCM 或 Ivanti Endpoint Manager 管理的设备注册到 Ivanti Neurons for MDM。 组织可利用部署包工具简化 Windows 设备向 Ivanti Neurons for MDM Modern Management 的过渡流程，并且不会导致停机或最终用户中断。 通过 Ivanti Neurons for MDM 控制台下载一个独特的部署包，然后用现有的管理工具或域进行部署，实现无缝过渡。 在执行程序包后，它会以静默方式将端点注册到 Ivanti Neurons for MDM，从而进行持续管理。 该方法支持管理员先轻松迁移设备，然后稍后通过无线方式灵活配置设备。 在设备静默注册到 Ivanti Neurons for MDM 后，将与 MDM 一同加入，并由两个管理机构共同管理。 管理员在 Ivanti Neurons for MDM 中配置所需 Windows 体验后，可停用旧管理平台，这样 Ivanti Neurons for MDM 将成为设备的唯一管理机构。

> 如果设备正在从 Microsoft Endpoint Manager (MEM)（以前称为 SCCM）过渡，则此规则有一个例外。 在共存模式下，现有 MEM 客户端将继续正常工作（与共同管理模式相反），直到 MEM 平台停用。 在启用共存模式后，MEM 客户端将自动禁用特定功能，以便 Ivanti Neurons for MDM 提供这些工作负载。 有关详细信息，请参阅**"Microsoft 的共存"文档**。

如需在使用 MEM 和其他第三方管理平台时执行更准确的行为，Ivanti 建议先在环境中测试 Ivanti Neurons for MDM 部署包工具。

先决条件

- 必须使用 LDAP、Entra ID (Entra ID)、本地用户上传或其他身份集成，在 Ivanti Neurons for MDM 上导入用户账户
- 所有设备必须安装 **Windows 配置设计器**。
- 在 Ivanti Neurons for MDM 上启用基于 PIN 的注册
- 用户的用户名中不得包含空格，这可能会导致用户设备过渡失败。
- 此工具可以部署在不使用 Entra ID 的环境中。
- Ivanti Neurons for MDM Modern Windows Management Suite 的主要元素不需要 Entra ID。 共同管理或共存可能需要在静默注册时部署某些工作负载/配置，避免过渡期间受到任何影响。
- 目前仅 SCCM 和 Ivanti Endpoint Manager 支持部署包。

步骤

1. 转到**管理员 > Windows > 部署包**。
2. 选择**用户**或**用户组**以生成 PIN，然后点击**下载部署包**（.zip 文件）。
3. 将部署包提供给 SCCM/Ivanti Endpoint Manager 管理员，解压并将文件传输给由这些管理员管理的相应设备。 有关如何执行此步骤的信息，请参阅 **Configuration Manager 中的包和程序**。
4. 传输后，管理员远程触发设备上的 setup.ps1 脚本。 有关触发脚本的详细信息，请参阅**从 Configuration Manager 创建和部署脚本**。
5. 设备会在 Ivanti Neurons for MDM 上注册。

>

为用户生成的 PIN 仅在 24 小时内有效。 在 PIN 过期后，需要生成新 PIN。

对于包含 PIN 的文件，它们将从设备注册尝试完成后进行删除。

将 SCCM 设备注册到 Ivanti Neurons for MDM

步骤

1. 从 Ivanti Neurons for MDM 为所选用户下载全部与部署相关的文件。
2. 选择应该注册的帐户或组。

3. 使用 SCCM 将程序包文件部署到客户端设备：
    1. 验证所需客户端是否存在于 SCCM 中。 如果客户端上没有 Windows 配置设计器，管理员应该将设计器推送给客户端并在客户端上部署。
    2. 在 SCCM 服务器上，创建文件夹并复制部署 zip 文件，然后提取文件的内容。
    3. 创建 .bat 文件以复制文件夹的内容，该文件夹中的文件被提取到客户端设备。
    4. 在 SCCM 中，转到**软件库 > 应用管理 > 程序包**，创建程序包，将文件夹的内容复制到客户端。 输入要复制这些内容的目标文件夹。
    5. 将程序包部署到设备或设备位置。
    6. 在“监控”部分下方，您可以监控部署状态，并确认文件是否已复制到客户端目标文件夹。
4. 执行脚本以注册设备：
    1. 转到**软件库 > 脚本**，然后创建脚本。
    2. 输入脚本名称，并从解压文件夹中导入 PowerShell 脚本 **setup.ps1**。
    3. 批准脚本并在目标设备上执行脚本。
    4. 选择**立即开始**，然后点击**保存**。 计划任务开始执行脚本。 成功执行后，状态将变为绿色。
5. 要验证设备注册，请访问**设置** > **添加或删除配置程序包** > **详细信息**。

将 Ivanti Endpoint Manager 设备注册到 Ivanti Neurons for MDM

步骤

1. 从 Ivanti Neurons for MDM 为所选用户下载全部与部署相关的文件。
2. 选择应该注册的帐户或组。
3. **案例 1**：使用相同用户名注册设备时要考虑设备名。在这种情况下，电子邮件地址不是有效的用户电子邮件地址。 将设备名与 AD 域连接的电子邮件视为注册电子邮件地址。 管理员必须将帐户设置为 LocalSystemAccount 并使用 setup.ps1 作为启动 PowerShell 执行的主文件。
   案例 2：注册设备时考虑使用有效的用户电子邮件地址，且不限制修改设备位置中的文件。使用登录用户的电子邮件地址进行注册。 要启用此注册，管理员必须将帐户设置为当前用户帐户，并使用 setup.ps1 作为启动 PowerShell 执行的主文件。
   案例 3：注册设备时考虑使用有效的电子邮件地址，对修改设备位置中的文件有限制。使用登录用户的电子邮件地址进行注册。 此案例可以分为两种情况：
    - 使用两个脚本注册 - 用 **setupEPMCopyContentsToTempFolderStep1.ps1** 创建分发程序包，并以当前用户帐户运行。 文件会复制到临时位置。 用 **setupEPMCopyContentsToTempFolderStep2.ps1** 创建另一个分发程序包，并以本地系统帐户运行。

      > 如果设备用户对修改包含程序包文件的文件夹设置了限制，则将文件复制到临时文件夹，检查用户 ID 并创建 PowerShell 程序包。 PowerShell 程序包由 **setupEPMCopyContentsToTempFolderStep2.ps1** 脚本执行。 安装完成后，将删除临时文件夹。

   禁用/启用 UAC

    1. 更新注册表项，以禁用 UAC 控件并重启计算机
    2. 通过当前用户帐户，使用 setup.ps1 执行 PowerShell 程序包
    3. 更新注册表项，以启用 UAC 控件并重启计算机

创建 PowerShell 程序包：

1. 验证 Endpoint Manager 中是否有所需客户端。

2. 将文件复制到 C:\Program Files\LANDesk\ManagementSuite\LANDesk\files\。 在此文件夹中创建子文件夹，并提取文件。
3. 创建程序包：**分发 > 分发程序包 > 新建 > Windows > PowerShell**。

   > 管理员可以根据设备上设置的限制级别将程序包分发到不同设备。

4. 在“主要”文件部分，输入程序包名称并从有复制文件的文件夹中上传 setup.ps1
5. 在“其他”文件部分，使用**添加**复制剩余文件（setup.ps1 脚本以外的文件）。
6. 在“帐户”部分选择当前用户帐户。
7. 单击**保存**。

4. 创建计划任务：
   1. 选择创建的程序包，右键点击并选择**创建计划任务**。 计划任务已创建。
   2. 拖动设备，并将其添加到计划程序包部分。
   3. 在计划程序包上，右键点击并选择**属性**。
   4. 验证程序包。
   5. 在“任务”类型下，选择**推送**。
   6. 选择**立即开始**，然后点击**保存**。 计划任务开始执行脚本。 成功执行后，状态将变为绿色。
5. 要验证设备注册，请访问**设置** > **添加或删除配置程序包** > **详细信息**。 或者，管理员也可以在设备的诊断日志中验证设备注册。

7.5.8. 使用针对 Windows 设备的批量注册

通过批量注册功能，您可以向 Ivanti Neurons for MDM 快速注册多个 Windows 设备。

先决条件:

- 必须使用 Entra ID (Entra ID) Premium 账户在 Ivanti Neurons for MDM 上导入用户账户。
- 所有设备必须安装 **Windows 配置设计器**。

程序：

1. 链接 Ivanti Neurons for MDM 和 Entra ID 租户。 请参阅**将 Entra ID 连接到适用于 Windows 10 设备的 UEM**。
2. 打开 **Windows 配置设计器**应用并选择**配置桌面设备**。 屏幕上将显示新的项目窗口。
3. 输入以下详细信息：
    - 名称 - 项目的唯一名称
    - 项目文件夹 - 设备上保存项目的位置
    - 说明 - 项目的可选说明

点击**完成**关闭新项目窗口，并执行一系列步骤。

5. **设置设备**
   输入设备的唯一名称。 名称可以包含一个序列号 (%SERIAL%) 或一组随机字符。
6. 如果您正在升级 Windows、配置要共享使用的设备或删除预安装的软件，也可以输入产品密钥。
7. **设置网络**
   您也可以配置设备首次启动时要连接的 Wi-Fi 网络。 如果未配置网络设备，则设备在首次启动时需要连接至有线网络。
8. **帐户管理**
   选择**注册 Entra ID**，输入**批量令牌到期**日期，然后点击**获取批量令牌**。
9. 输入 Entra ID 凭据以获取批量令牌。
10. 在**保持登录所有应用**页面，点击**否，仅登录此应用**。
    - 在成功获取批量令牌后点击“下一步”，创建程序包。
    - 将在 Azure 门户中创建带有配置程序包的用户 - 用户主体名称（例如 package_0ea893a5-1e93-4d21-a6b1-dc788946fd1d@miwinqe.onmicrosoft.com）。 将文件（运行时 ppkg 工具）复制到存储设备。

> 使用 Entra ID 用户创建批量令牌，程序包用户不应启用 MFA。 要进行验证，需要对该用户执行 OOBE + Entra ID 联接。

重新创建程序包用户（在 Azure 中创建）或将其同步到 Ivanti Neurons for MDM。

批量注册其闪存驱动器中包含配置程序包的设备。 也可以双击现有设备来执行 OOBE 后体验。 如果第一次程序包安装尝试失败，则第二次尝试也会失败。 检查新设备是否是在 Ivanti Neurons for MDM 中创建，以及 Entra ID 是否属于程序包用户。

7.5.8.1. Ivanti 批量注册

管理员可以使用前缀为 **windows-bulkenroll** 的通用用户（通过 ppkg）注册多个 Windows 设备，然后执行用户分配。

先决条件:

- 在 Ivanti Neurons for MDM 上，创建前缀为 **windows-bulkenroll** 的用户账户。 例如，**windows-bulkenroll**-user1@abc.com、**windows-bulkenroll**-user2@abc.com。

使用 Windows 配置设计器创建 PPKG 程序包

1. 下载并安装 **Windows 配置设计器**。
2. 创建新项目。
3. 点击**配置桌面**。
4. 输入项目名称，然后选择路径。
5. 在**设置设备**部分中，输入设备名称。
6. 在**设置网络**部分中，输入网络名称（用于设置网络，根据需要使用，也可以禁用）。
7. 在**账户管理**部分中，选择**注册本地管理员**。 输入**用户名**和**密码**，然后点击 **下一步**。
8. 在**添加应用程序**部分中，点击**下一步**。
9. 在**添加证书**部分中，选择**切换到高级编辑器**，然后点击**继续** >**是**。
10. 转到 **RuntimeSettings** > **Workplace 注册**。 输入 **UPN**（与在 Ivanti Neurons for MDM 的前提条件部分中创建的用户一致）。 选择以下选项：
    - AuthPolicy：OnPremise
    - DiscoveryServiceFullUrl: https://login.mobileiron.com
    - 密码：输入密码

点击**文件** > **保存**。

12. 点击 **导出** > **配置程序包**。
13. 在后续屏幕中点击**下一步**，然后点击**构建**。
    ppkg 文件会保存在指定位置。

在 OOBE 模式下使用 ppkg 配置设备

使用上一部分新建的 ppkg 程序包文件对设备进行配置。 设备成功注册并签入后，可在 MDM 服务器上找到前缀为 **windows-bulkenroll** 的用户的设备条目。

将设备分配到用户

1. 在“设备”页面上，点击前缀为 **windows-bulkenroll** 的用户。
2. 点击**分配给用户**。 “分配给用户”窗口随即打开。
3. 从列表中选择或搜索设备。
4. 选择所需的设备。
5. 点击**分配给用户**。 所选的设备将分配给用户。

用户首次登录设备时，必须更改密码。

"分配给用户"选项仅适用于 Ivanti 批量注册设备。

只有设备范围配置和应用程序适用于在此类别下注册的设备。 不支持用户范围配置和应用程序。

7.5.9. 更改通行码设置

本部分包含以下主题：

- 更改分配的通行码配置
- 分配不同的通行码配置

使用分配到设备的通行码配置更改通行码设置。 您还可以：

- 更改已分配配置的设置

或

- 分配不同的通行码配置

您对该配置所做的更改会影响所有已分配该配置的设备。

更改分配的通行码配置

步骤

1. 转到**设备**。
2. 在列表中查找设备条目。
3. 单击**名称**列中的链接。

> 如果已经分配了通行码配置，其将显示在“配置”选项卡中。

在“配置”选项卡中，单击**通行码配置**链接。

5. 单击**编辑**（右上角）。
6. 进行更改。

分配不同的通行码配置

步骤

1. 确保已有人创建了您所需要的配置。
2. 转到**设备**。
3. 在列表中查找设备条目。
4. 单击**名称**列中的链接。

7.5.10. 更改设备名称

管理员可以手动更改设备的名称（不使用“编辑设备名称”配置）。

适用于：

- iOS 受监控设备
- tvOS 受监控设备
- macOS 10.10+ 设备

步骤

1. 转到**设备**。
2. 在列表中查找设备条目。
3. 执行以下步骤之一：
    - 如果尚未添加**设备名称**列，单击右侧的设置齿轮图标，然后选择**设备名称**进行添加。
    - 单击**名称**列中的链接，转到设备详细信息页面。
4. 在设备名称旁边，点击**编辑**铅笔图标。
5. 输入新设备名称，然后单击勾选图标。
6. 在覆盖设备名称显示框中，查看备注，并单击**确定**。

更改后的名称将在下次签入时推送到设备。 此操作无法撤消。

> 如果此前已配置默认设备名称配置，此操作将覆盖在配置中设置的名称。

7.5.11. 查找并筛选设备

本部分包含以下主题：

- 搜索设备
- 筛选设备
- 使用高级搜索
- 加载搜索查询

搜索设备

在规则生成器中选择“用户组名称”属性后，Ivanti Neurons for MDM 管理门户会显示重复用户组的数量和相应的 GUID 数量，以便识别重复组。 此外，此规则下方的表会显示重复用户组的列表及其详细信息，例如用户组名称、GUID、来源和可分辨名称 (DN)。

步骤

1. 转到**设备**。
2. 在**搜索**字段中输入设备名称。 将列出名称中包含所输入字符的所有设备。

筛选设备

“筛选器”侧面导航栏会列出可帮助您从整个设备列表中搜索特定设备的各个部分。 “管理筛选器”向导包含所有部分的列表，您可根据需求选择要在“筛选器”导航栏中显示的部分。

步骤

1. 转到**设备**。
2. 在“筛选器”侧面导航栏列出的部分中，点击相关复选框。
   示例：
   - 在**用户已启用**部分中选择**是**，以仅显示用户处于启用状态的设备。
   - 如果您已将自定义属性分配到设备，则可通过点击设置图标（齿轮）来根据这些属性筛选设备。
   - 在**状态**部分中选择**已停用**和 **iOS**，以仅显示已停用的 iOS 设备。

（可选）点击**还原默认值**可将所选项还原为默认筛选器。 “筛选器”导航栏会显示选中的部分。 如果从“管理筛选器”向导中清除所有复选框，“筛选器”侧面导航栏将显示所有部分。

4. 点击“管理筛选器”向导以外的任何位置可退出向导。
5. （可选）点击“x”图标可关闭“筛选器”侧面导航栏，点击**筛选器**可重新打开侧面导航栏。
   - 如果使用 stopwords.txt 文件（该文件是 Apache SOLR 服务器配置的一部分）中列出的任何停止词，则系统将不会为这些词编制索引，因此名称中包含这些停止词的实体将不会显示在搜索结果中。
   - 实体的示例：设备、用户、组、属性、应用程序、证书、审计跟踪、内容和通知模块。
   - 停止词的示例：a、an、if、be、into 等等。

使用高级搜索

您可以使用高级搜索选项，以按照规则搜索设备，识别和查看特定条件的设备。 因此可获取规则可以使用适用的运算符进行构建，包括“开头为”、“结尾为”、“包含”、“不包含”、“开头不是”、“结尾不是”、“小于”、“大于”、“在以下范围内”、“等于”和“不等于”运算符。 使用任意（或）

或全部（且）选项，规则选项可以全部进行嵌套。 匹配规则的设备会显示在部分下方。

Ivanti Neurons for MDM在规则生成器中选择“用户组名称”属性后，管理门户会显示重复用户组的数量和相应的 GUID 数量，以便识别重复组。 此外，此规则下方的表会显示重复用户组的列表及其详细信息，例如用户组名称、GUID、来源和可分辨名称 (DN)。

步骤

1. 在“设备”页面中点击**高级搜索**链接。 “高级搜索”向导打开。
2. 点击下列选项之一：
   - 如果设备必须与至少一个规则匹配，则选择**任意**
   - **所有** - 设备必须匹配所有规则时使用

创建定义搜索条件的规则。 **示例**：“支持 APNS”等于“是”。

4. （可选）点击 **+** 可创建其他规则。
5. 单击**搜索**。 将显示匹配搜索条件的设备列表。
   - 对于 iOS 14.0+ 设备，设备的 eSIM ID (EID) 在设备详细信息页面中可用。 eSIM ID (EID) 允许运营商将 SIM 分配到特定设备。 eSIM ID (EID) 字段符合 GDPR。
   - 鉴于新版本Ivanti Neurons for MDM增加了新的 GDPR 字段（例如 IP 地址和 eSIM ID），因此，对于已配置 GDPR 的管理员，如果他们想要隐藏新字段，则必须编辑 GDPR 配置文件。
   - 高级搜索显示了设备恢复锁定的状态。

加载搜索查询

可以查看已保存的搜索查询的列表。

步骤

1. 点击“高级搜索”，然后点击文件夹图标。 **已加载查询**部分会显示已创建的搜索查询的列表，此外还会显示下列详细信息：
   - **查询名称** - 已加载查询的名称。
   - **查询内容** - 根据定义搜索查询的规则，显示内容。
   - **操作** - 选择对查询执行的操作。
2. 单击**操作**列中的**加载查询**，以查看匹配在已加载查询中定义的条件的设备列表。
3. 点击**删除**可删除加载的查询。

7.5.12. 使用设备所有者

本部分包含以下主题：

- 使用 QR 码或 NFC Bump 配置 Android Enterprise 设备
- 使用客户端令牌配置 Android Enterprise 设备

许可证：Gold

设备注册后，您可将其指定为公司所有或员工所有。 此指定有助于管理策略，而无论此策略是基于公司所有的设备还是员工所有的个人设备。 使用适当许可证，然后您可以使用规则中的所有权，以创建设备组。

从新的或出厂重置设备开始，使用 **Provisioner** 应用程序，以便使用以下选项之一配置设备所有者模式：

- NFC（近场通信）Bump
- QR 码扫描

NFC Bump 需要根据全新或出厂重置设备使用主或模板设备进行配置。

QR 码扫描涉及单击全新或出厂重置设备的屏幕，配置 WiFi 网络，以及在设备准备好配置时扫描代码。

在使用 NFC 或 QR 码配置设备所有人模式时，Provisioner 应用接受注册令牌。 在注册时，注册令牌发送到服务器。 如果已在服务器中且设备分配到用户，设备将成功注册。

Go 客户端将控制处于设备所有者模式的设备，并锁定屏幕，直到设备注册到 Ivanti Neurons for MDM，以防用户离开配置流程。 设备所有者模式还支持自助服务终端模式。 有关配置信息，请访问：锁定与自助服务终端配置。

重要信息

- 如果您在设备所有者模式停用设备，则该设备将恢复出厂重置。
- 设备所有者模式下的所有设备都可以选择启用所有系统应用程序。
- 设备一次仅拥有一个激活的设备所有者。
- 只有支持 Android Enterprise 的设备才能配置为设备所有者模式。
- 对于处于设备所有者模式的 Samsung Knox Standard 设备，系统将提示用户激活 Samsung ELM 许可证。 当 Go 客户端应用从以前的版本升级到 Ivanti Neurons for MDM 支持的最新发布版本时，此提示也将显示在处于设备所有者模式的 Samsung 设备上。 激活后，序列号显示在“设备详细信息”页面上，该页面与设备 > 设置> 序列号字段匹配。

使用 QR 码或 NFC Bump 配置 Android Enterprise 设备

要使用 QR 码或 NFC Bump 配置 Android Enterprise 设备，需要从 Google Play 下载并在主设备上安装 Provisioner 应用程序。

兼容组件

Provisioner 版本：1.3.0。

Provisioner 与以下内容兼容或使用：

个项目	版本
Android 操作系统 （在要设置的设备上）	• 5.0 - 如果使用 NFC，需要支持的较新版本。 • 7.0 - 如果使用二维码，需要支持的较新版本。 设备必须支持 Android Enterprise。
Android 操作系统（在主设备上）	5.1 - 至最新发布版本。 设备必须具有 NFC 才能使用 NFC Bump。 QR 码不需要该功能。
UEM 服务器产品，已为 Android Enterprise 启用	下列内容之一： Ivanti Neurons for MDM，或标记为允许的 Ivanti Neurons for MDM。
Android 客户端应用程序	Provisioner 会自动在配置的设备上安装最新的客户端应用程序版本。

先决条件

要将 Android Enterprise 设备配置为工作托管设备，需要：

- 确保已定义所需的 Android Enterprise 相关配置并将其应用于注册的设备。

> 默认的 Android Enterprise：必须为设备启用工作托管设备配置。

在服务器上启用 Android Enterprise。

- 拥有 NFC 功能的 Android 设备（仅在使用 NFC 的情况下）才能充当主设备，并安装了 Provisioner 应用程序。
- 配置支持 Android Enterprise 的设备。

若要使 Android Beam 能够与 NFC Bump 一起使用：

步骤

1. 转到设备上的**设置**。
2. 转至**网络 > 无线网络**。
3. 在**连接部分**中，选择**共享和连接**。
4. 将 **NFC** 开关滑动到**开启**。
5. 将 **Android Beam** 开关滑动到**开启** 。

> 启用 Android Beam 和 NFC 的步骤可能因不同设备而异。

将 Android Enterprise 设备配置为工作托管设备

步骤

1. 使用 Android 主设备，从 Google Play 下载 Provisioner 应用并安装该应用。
2. 在主设备上启动 Provisioner。
3. 为配置方法选择 NFC 或 QR 码。
4. 单击**要配置的应用程序**，然后选择要在已配置设备上安装的客户端应用程序：

选择该客户端应用程序：	要向此 UEM 服务器注册：
转到	Ivanti Neurons for MDM
At Work UEM	（标记为允许的）Ivanti Neurons for MDM

5. 填写 Provisioner 应用中的剩余字段。 如果存在支持的无线网络类型，则某些字段 可能会自动填充。 如果选择了 QR 码，则不会显示 WiFi 字段。 使用这些 指导原则：

字段	价值
选择要配置的应用程序	Go 或 At Work
时区	输入要在设备上配置的时区
区域设置	输入要在设备上配置的区域设置
启用所有系统应用程序	单击复选框，以便启用所有系统应用程序
WiFi 网络 SSID	输入目标设备要使用的 WiFi SSID
WiFi 安全类型	输入 WiFi 安全类型
WiFi 密码	输入 WiFi 密码
批量注册	批量注册功能是可选项。 若要使用批量注册，需要提供主机名。 可选地，可以输入用户名，并且可以选择快速启动选项。 要跳过批量注册功能，这些字段应该留空。

6. 点击**继续**。
7. 如果您选择了 **NFC**，请单击**继续**。 主设备上显示**接触设备！**屏幕。 继续下面的 **NFC Bump** 部分。
8. 如果选择 **QR 码**，主设备上将显示**扫描此 QR 码！**屏幕。 继续下面的 **QR 码**部分。

对 NFC Bump 使用下列步骤

确认目标设备正在显示 Android 欢迎屏幕。

9. 按下主设备背靠背，使用目标设备启动 NFC 传输。 如果 NFC 传输成功，目标设备会发出声音提示，然后继续下载客户端应用程序。 如果无法建立 WiFi 连接，或者设备无法下载客户端应用程序，设备将自动进行出厂设置。
10. 如果您听到声音或看到“欢迎”屏幕以外的屏幕，则可以将设备解耦。 这通常需要几秒钟。 如果该设备 未加密，则在继续前将开启加密过程。
11. 您可以通过将设备“碰撞”到主设备来继续设置其他设备。 目标设备必须显示“欢迎”屏幕，主设备必须显示“接触设备！”屏幕。

使用下列步骤进行二维码配置

确认目标设备正在显示 Android 欢迎屏幕。

12. 在屏幕上的同一位置单击目标设备上的 Android 欢迎屏幕 6 次。
13. 系统将提示您配置 WiFi 网络，以便安装向导可以将 QR 码阅读器下载到目标设备。
14. 下载 QR 码阅读器后，相机启动。

15. 将目标设备保持在主设备上方几英寸处，直到 QR 码扫描成功。 然后安装向导将继续下载客户端应用程序。 如果无法下载客户端应用程序，它将自动进行出厂设置。
16. 您可以通过扫描主设备上的 QR 码来继续设置其他设备。 目标设备必须具有可以扫描的摄像头，主设备必须显示“扫描此 QR 码！”屏幕。
17. 也可以通过单击共享图标导出 QR 码。 为导出提供的选项将因设备而异。

使用客户端令牌配置 Android Enterprise 设备

可以使用品牌客户端令牌（而不是 NFC Bump 或 QR 码方法）在设备所有者模式下配置 Android Enterprise 设备。 该方法支持您使用令牌登录设备，这有助于自动安装 Go 或 At Work 客户端并在设备所有者模式下进行配置：

> 使用 Android 6 或支持的较新版本的托管 Google Play 帐户配置的设备支持品牌化客户端令牌。 有关更多详细信息，请参阅 Android UEM 开发人员指南。 https://developers.google.com/android/work/prov-devices#Key_provisioning_differences_across_android_releases.

使用此方法时需满足的要求：

- 必须注册 Android Enterprise 帐户。
- 设备必须支持 Android Enterprise。
- 设备必须使用 Android 6 或最新发布版本。
- 您必须拥有全新或出厂重置设备。

配置（适用于运行 Android 5.0+ 的设备）

步骤

1. 在 Ivanti Neurons for MDM 门户中，转至**配置**。
2. 点击 **+ 添加**。
3. 选择**锁定和 Kiosk：Android Enterprise**。
4. **创建锁定和 Kiosk：Android Enterprise 配置**页面随即显示。

输入配置名称和说明。

5. 选择锁定类型。

单击**工作托管设备（设备所有者）**。

6. 系统将显示 Android 设备所有者锁定设置选项。

或者， 可选择

- 禁用 WIFI 或 WIFI 设置
- 禁用照相机
- 禁用蓝牙
- 不允许蓝牙设置
- 禁用屏幕捕获
- 静音主控音量
- 不允许应用控制

- 不允许使用凭据
- 不允许紧急广播
- 不允许移动网络
- 不允许数据共享
- 不允许 VPN
- 不允许出厂设置
- 启用出厂重置保护。

> 您可以选择指定授权 Google 账户 ID 的列（整数值），该列表可以在工厂重置后配置设备，或者将鼠标悬停在帮助图标上，以查看检索授权账户 ID 的帮助。

不允许修改账号

- 禁用 NFC（射出光束）
- 不允许拨出电话
- 不允许安全启动
- 不允许共享位置
- 禁止调试功能
- 确保验证应用程序
- 不允许短信
- 不允许取消静音麦克风
- 禁用自动时间
- 禁用自动时区
- 禁用数据漫游
- 禁用 Wi-Fi 休眠模式
- 限制输入方法
- 限制可访问性服务
- 禁用 USB 文件传输
- 禁用外部媒介
- 禁用密钥保护（如果设置了 PIN/通行码，则无效）
- 接通电源时保持屏幕打开
- 不允许创建窗口
- 跳过首次使用提示

在**启用/禁用系统应用**部分中，您可以选择启用或禁用以下系统应用：

7. 或者，可选择启用**自助终端服务模式**。

个项目	版本
预设系统应用程序	
内置相机	单击切换按钮，**打开**或**关闭**内置摄像头应用程序。
内置电话	单击切换按钮，**打开**或**关闭**内置电话应用程序。
系统应用软件包名称	要启用或禁用预设置系统应用之外的任何其他系统应用，单击 +（加号）图标，并添加系统应用软件包名称。 要删除系统应用程序，请单击 -（减号）图标。

将显示以下设置：

- 启用锁定任务模式
- 自动进入自助服务终端（仅在初始设置时）
- 禁用快速设置
- 允许用户访问 WiFi 设置
- 允许用户访问蓝牙设置
- 允许用户访问位置设置
- 允许用户延迟应用程序的更新
- 允许用户访问日期和时间设置
- 允许用户访问移动网络设置
- 允许用户选择语言
- 启用共享设备（选择以下任何选项）
  - 启用登录
  - 启用注销（提供超时设置，以小时单位）

或从下拉列表中选择默认或自定义加印品牌选项。

8. 或者，创建自助终端服务退出 Pin，以用于退出自助终端服务模式。
9. 或者，创建将在自助终端服务模式对用户可用的应用允许列表。

配置设备

步骤

1. 打开设备电源并输入您的 WIFI 密码。 您的设备可能会提示您输入不同的密码。
2. 在**验证帐户**屏幕中输入 Android Enterprise 令牌。 单击**下一步**。
3. 在 **Google 服务**屏幕上，单击**安装**。
4. 接受条款和条件。
5. 在设置工作设备屏幕上，单击**下一步**。 下载 Go 或 At Work 客户端，并在设备上安装。 设备现在进入设备所有者模式。

相关主题

- 使用 Android 的批量注册

- 设备组

7.5.13. 带有工作配置文件的托管设备

带有公司拥有设备上的工作配置文件的托管设备是指一种模式，Android Enterprise 设备在其中是企业所有的设备，个人数据彼此相互独立。此模式支持两种配置文件，您可在其中将工作应用部署到托管配置文件，并使用户将设备用于个人用途。 通过将带有工作配置文件的托管设备配置分发到在设备所有者模式中配置的设备，创建带有公司拥有设备上的工作配置文件的托管设备模式。

有关带有工作配置文件锁定设置的托管设备的更多信息，请查看**锁定和自助服务终端：Android Enterprise**。

> 此模式需要 Android 8.0 至最新发布的版本。

应用配置、应用在配置文件之间共享小部件、客户端证书别名和 ID 证书可以应用于带有工作配置文件的托管设备。

以下配置适用于带有工作配置文件的托管设备的设备：

- 高级通行码
- VPN 全局模式
- 证书
- 身份证书
- Google 帐号
- 通行码
- Samsung 手机限制
- 威胁防御
- Wi-Fi
- 默认应用程序运行时权限
- SafetyNet 认证
- 通行码
- Threat Defense 本地操作

7.5.14. 使用 Android 的批量注册

通过批量注册功能，您可以向 Ivanti Neurons for MDM 快速注册多台 Android 设备。

许可证：Silver

在使用批量注册前，执行以下任务：

1. 在用于注册设备的计算机上安装包含 Android Debug Bridge (adb) 的 Android SDK。
   有关 Android Debug Bridge 的详细信息，请参阅：http://developer.android.com/tools/help/adb.html。
2. 启用 USB 调试。
   在 Android 设备上启用 USB 调试的步骤因 Android 版本而异。 请查看：http://developer.android.com/tools/device.html，以了解有关启用 USB 调试的信息。
3. 在每个设备上安装 Go 客户端。
4. 通过 USB 连接线将设备连接到用于注册这些设备的配置计算机。

使用 Android 调试桥 (adb) Shell，启动 Go 并将其注册到服务器。 Android Debug Bridge 是一种可通过 Windows 中的命令行或在 iOS 中的“终端”实用程序中使用的工具。 它使您能够与连接的 Android 设备进行通信。 通过 adb 外壳程序的命令格式是：

> 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

> 注册协议 (**mirp**) 用于解码与注册的相关数据。

有效键和值是：

密钥	价值
用户	如果使用 iReg，用户的电子邮件地址将被输入到用户名字段中。 必选。
密码	用户密码
pin	用户的注册 PIN
quickStart	**当设置为 TRUE 时：将显示初始屏幕，但不会很长。** 在欢迎屏幕上，当微调框更改为“继续”按钮后，屏幕将自动移动，而无需点击“继续”。 此外，此简化的配置流程会应用到所有设备： • 针对用户的隐私和快捷方式提示已跳过。 • 在 Zebra 设备上，客户应为其授予管理员权限，而无需用户提示。 需要的最低版本为 Zebra MX 4.3。 **当设置为 FALSE 时：**初始屏幕将如常显示，且用户需要在欢迎屏幕上点击“继续”。 可选，默认为 FALSE。

> 要求使用密码、PIN 或令牌的用户使用批量注册。

此示例命令指定了服务器、用户、密码、PIN 和快速启动：

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

示例批量注册脚本

在设计您的批量注册脚本时，您可以使用此脚本作为示例。 此示例脚本使用相同用户名和密码，注册附加到配置机器的所有设备。

```
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
```

潜在错误消息

以下是您在使用批量注册时，可能会遇到的一些错误：

错误	解决方法
未找到 MIRP 方案	使用 mirp 方案的示例命令：am start -a android.intent.action.MAIN -d "xxxmirp://?
URL 无效	如果根本未发送数据字符串，将出现这种情况。 请确认 URL 正确。
未找到服务器信息	服务器信息丢失或输入错误。
未找到用户信息	验证是否已输入用户密钥。
未找到密码/PIN 信息	验证是否已输入 PIN 或者密钥。

当为批量注册创建了多个配置文件时：

- 本机注册的完全托管 Android Enterprise 设备会接收使用第一个配置文件创建的自定义属性。
- 迁移设备时，如果设备存在于批量注册配置文件中，则批量注册配置文件中为迁移设备定义的自定义属性将应用于迁移的设备。 对于迁移的完全托管 Android Enterprise 设备，此行为相同，因为它接收第一个配置文件的自定义属性。

此外，为该特定设备创建的所有配置文件都被视为活动的。

7.5.15. 使用 CSV 文件上传进行批量注册

批量注册允许您使用设备标识符注册多个 Android 设备。 您可以上传 CSV 文件，以批量添加设备。

步骤

1. 在**设备**页面中，单击**批量注册**选项卡。 将显示**批量注册**页面。
2. 单击**添加**。
3. 在**配置文件名称**文本字段中，输入配置文件的名称。 或者，单击 **+ 添加描述**，以为 CSV 文件提供描述。
4. 在**上传 CSV** 部分中，单击**下载 CSV 模板**，以下载 CSV 模板。 使用现有格式，您可以编辑文件，以添加设备。

> 批量注册 CSV 时一次最多允许 200,000 行。

5. 在编辑和保存 CSV 文件后，单击**上传 CSV**，以上传 CSV 文件。 上传成功后将显示确认消息。

> 信息不足的行可能导致 CSV 上传失败。 每条记录应至少包含序列号和制造商信息或 IMEI 值。

> 要移除添加的 CSV 文件，请单击"减号"图标。 要选择不同 CSV 文件进行上传，单击**选择不同文件**链接。

6. 可选：选择**在不使用令牌的情况下分配自定义属性**，以在不生成令牌的情况下批量注册所有类型的设备。 默认情况下不选中此选项。

当在已上传 CSV 文件中提供 IMEI 或序列号与制造商的组合（含或不含自定义属性）时，也可以应用不含令牌的批量注册。 但是设备的注册取决于上传到 CSV 文件中的属性值的正确性。 下表说明了基于为批量注册输入的属性值组合的结果方案：

方案	**输入的属性值**			**设备注册状态**
	IMEI	**序列号**	**制造商**	
1	正确	错误	错误	设备已注册
2	错误	正确	正确	设备已注册
3	错误	错误	正确	设备未注册
4	错误	正确	错误	设备未注册

> 制造商名称区分大小写。

7. 在**选择用户**字段中，您必须选择一个用户。
   注册令牌将显示在注册令牌列中。 要刷新注册令牌，点击**刷新**。
   令牌的有效期限将显示在**令牌到期时间**部分中。 要延长令牌有效期限，单击**延长**。 在**延长到**字段中，输入延长令牌的天数。

> 指定的天数应该在范围 7 到 999 之间。 默认令牌过期时间是 7 天后。
> 如果您选择选项**在不使用令牌的情况下分配自定义属性**，将不显示此页面。

8. 单击**完成**。

在上传后，已上传 CSV 文件的下列详细信息将显示在**批量注册配置文件**页面的表格中。

设置	说明
配置文件名称	配置文件的名称。
描述	关于配置文件的一些描述。
上次修改日期	上次在 CSV 文件中完成修改的日期。
类型	对于自我维护的配置文件 → 自我维护
设备编号	批量注册中的设备编号。
关联用户	关联用户的名称。
用户名	指定与设备关联的用户。 启用设备到用户映射时必填。 用户必须存在于 Ivanti Neurons for MDM 中。
操作	您可以执行以下任何操作： **下载现有清单** - 点击此按钮可下载配置文件中所有可用设备的详细信息。 **查看** - 点击此链接，可查看为注册批量上传的配置文件详细信息。 **编辑** - 点击此按钮可编辑配置文件详细信息。 此选项仅在选中单个设备选项时可用。 **删除** - 点击此链接，可删除配置文件。 在确认窗口中，点击**是**可确认删除上传的配置文件。

上传 CSV 时生成的令牌应用于注册。 输入错误的令牌将重定向到常规 IReg 流，并在其中输入 ID/密码。

操作

从“查看配置文件详细信息”部分查看“批量注册”配置文件时，可以从“操作”选项卡执行其他任务，该选项卡位于“查看配置文件详细信息”页面中。

- **添加更多设备** - 使用此选项可向配置文件添加更多设备。 您需要提供 **IMEI 编号**或**序列号**（或两者）、**制造商**以及可选的**自定义属性**信息，然后点击**保存**。
- **修改配置** - 使用此选项可修改现有配置。 可添加 **Ivanti 专用密钥**，更改**预先定义的 Android 系统附加程序**或**自定义 Android 系统密钥**，然后点击**更新**。
- **生成 QR 码** - 使用此选项可生成配置文件用于批量注册的 QR 码。
- **刷新令牌** - 使用此选项可刷新令牌或延长令牌的有效期。 有效期可以设置在 7 到 999 天的范围内，也可以设置为**永不过期**。
- **更改关联用户** - 使用此选项更改关联用户。 您需要从**更改关联用户**弹出窗口中搜索并选择用户，然后单击**应用**。
- **编辑** - 使用此选项可编辑所选配置文件中的设备。 需要选择设备，然后点击**编辑**按钮。
- **删除** - 使用此选项可删除所选配置文件中的设备。 选择设备并点击“删除”按钮后，屏幕上会显示确认弹出窗口。 单击**删除**。

自维护设备具有不同的设备状态。 您可以在使用 Samsung Knox 移动注册找到更多详细信息。

7.5.16. Device_to_User_BulkEnrollment

File not found!

7.5.17. 使用 Samsung Knox 移动注册

Samsung Knox Mobile Enrollment 使管理员能够将合格的 Samsung 设备注册到 Ivanti Neurons for MDM。 使用 Knox Mobile Enrollment，设备可以直接从经批准的经销商运送给最终用户，Go Android 客户端将自动下载并预先填充注册数据。 有关详细信息，请参阅 **Android Enterprise 的 Samsung Knox 移动注册**。

要求

- 按 IMEI 划分的设备列表
- 包含设备列表的 CSV 文件，其中包含 IMEI 或序列号，以及可选的用户名和注册密码。
- Ivanti Neurons for MDM（当前版本）。
- Samsung Knox 帐户已获批准用于移动注册
- Samsung 支持的设备。 此处提供了 Samsung 支持的设备列表。

7.5.18. 注册 Oculus 设备

Ivanti Neurons for MDM 现在可以管理 Quest for Business 设备（Oculus 设备）。 Meta 目前支持将 Oculus for Business (OFB) 和 Quest for Business (QFB) 设备用于 MDM。 需要在 Meta 控制台上执行一些基本任务，使设备为 MDM 做好准备，然后注册 Ivanti Neurons for MDM。

可以在 Meta Workplace 控制台下的设备管理器中注册 Oculus 设备组。 您需要使用注册电子邮件中共享的凭证登录 Oculus Business Workplace。 在主页上，所有设备信息将显示在“设备组”部分下方。 “设备组”部分提供了“设备管理”下所有可用设备的概要信息。 这些详细信息包括设备名称、设备状态、OS（操作系统）、型号等

本部分包含以下主题：

- 注册 Oculus 设备所需满足的先决条件
  - 在设备管理器中设置 MDM 应用程序
  - 设置 Oculus 设备

使用 MobileIron Go 注册 OFB 设备

  - 在 Ivanti Neurons for MDM 控制台上
  - 在 Go 客户端上

注册 Oculus 设备所需满足的先决条件

在设备管理器中设置 MDM 应用程序

设备/头戴式显示器完成配置，**Oculus for Business** 更新至 **v28** 及以上版本。 在 Meta 控制台上，管理员必须在设备管理器中设置 MDM，并将 Oculus 设备映射到此特定的 MDM 服务。

步骤

1. 在 **Oculus Business Workplace** 主页上，选择**应用程序**。
2. 在**应用程序库**下，点击要安装的第三方 MDM 应用程序，然后点击**更新**。
3. 从**移动设备管理**下的列表中为应用程序选择适当的 MDM，然后点击**更新应用程序**。
4. 点击要安装 MDM 的 Oculus 头戴式显示器设备。 屏幕上将显示设备信息。
5. 在**关于**选项卡下，向下滚动至**移动设备管理器**。
6. 点击 **MDM 颁发机构**选项旁边的**编辑**按钮。

> 默认情况下将选择“Oculus 设备管理器”选项。 需要选择“MDM 颁发机构应用程序”，然后从“MDM 颁发机构应用程序”列表中选择 **MobileIron Go**。

单击**保存**。 设备会自动重置，然后需要使用设置应用程序来设置 Oculus 设备。

设置 Oculus 设备

可以使用 Device Setup 应用程序添加 Oculus Quest 2 头戴式显示器设备。 必须将此应用程序分享给所需用户，以便用户可以在其 Android 设备上下载和安装该应用程序。

步骤

1. 在**设备组**部分下，点击**未配置设备**。
2. 点击**获得设置应用程序**。 屏幕上将显示**发送下载链接**页面。
3. 从列表中选择一个或多个团队成员，或点击**添加收件人**以从列表中选择成员。
4. 点击**发送连接**。 所选用户将收到一封电子邮件，其中包含安装 **Device Setup** 应用程序的链接。
5. 点击电子邮件中的**下载 Device Setup 应用程序**链接，以便在 Android 设备上安装 **Device Setup 应用程序**。

> 下载完成后，此应用程序将不会出现在设备的应用商店中。 需要从设备的“下载”部分获取该应用程序并进行安装。

在 Android 设备上打开 **Oculus for Business** 应用程序。

7. 按下电源按钮 2 秒以开启 Oculus 设备。
8. 打开蓝牙，将 Android 设备靠近 Oculus 设备，直至完成设置。
9. 使用 Android 设备的蓝牙功能搜索 Oculus 设备。
10. 找到所需的 Oculus 设备后，需要将其连接至 Wi-Fi 网络以完成设置。
11. 点击**输入 Wi-Fi 信息**并提供网络名称和密码，然后点击**保存**。 现在，Oculus 设备已连接至 Wi-Fi 网络。
12. 点击**开始设置**。 屏幕上将显示通知消息，提示正在进行设置，请勿在设置期间关闭应用程序或使用头戴式显示器。
    屏幕上将显示确认消息。 可以使用**查找更多设备**按钮继续搜索其他设备。

使用 MobileIron Go 注册 OFB 设备

在 Ivanti Neurons for MDM 控制台上

可以在 Ivanti Neurons for MDM 控制台上使用 MobileIron Go 注册 OFB 设备。 但是，必须将工作托管设备非 GMS 模式 (AOSP) 配置（位于**配置**下）分发到这些 OFB 设备组。

在 Go 客户端上

可以在 MobileIron Go 客户端上注册 OFB 设备。 若要注册 OFB 设备，需要执行以下任务：

- 使用 OFB Setup 应用程序完成设置后，继续按照 OFB 头戴式显示器屏幕上的说明进行操作，完成设备设置。
- MobileIron Go 应用程序会自动启动，您需要按照 MDM 说明提供登录凭据并完成注册。

现在，设备在 DO 模式下进行配置并设置为由 MDM 进行管理。

7.5.19. 启用设备上的 Bluetooth 功能

适用于：

- iOS 11.3+
- macOS 10.13.4+

您可以在设备上启用或禁用 Bluetooth 功能。

步骤

1. 在**设备 页面**导航至该设备。
2. 执行以下操作之一：
    - 从列表中选择设备。
    - 单击设备名称，以便显示“设备”详细信息页面。
3. 从**操作**菜单中，单击**启用/禁用 Bluetooth**。
4. 单击**确定**。

更改将在下次签入时推送到设备。

7.5.20. 计划 iOS 更新

适用于：

- iOS 9.0+ 受监管设备注册设备
- iOS 10.3+ 受监控设备。

计划 iOS 设备更新到可用的最新 iOS 版本。 受监管 iOS 设备的**设备** > **操作**菜单选项**更新操作系统版本**仅显示设备适用的 iOS 版本列表。

步骤

1. 在**设备页面**导航至该设备。
2. 单击设备名称，以便显示“设备”详细信息页面。
3. 在**操作**菜单中，点击**更新操作系统版本**。
4. 在**更新操作系统版本**向导中查看 iOS 版本信息，然后在**更新到版本**下拉列表中选择所需的操作系统版本。

> 如果输入相同版本或较旧版本，系统会显示错误消息，指示目标 iOS 版本应该高于当前版本。

5. 单击**更新**。

系统会计划将 iOS 设备更新到设备签入时可用的最新 iOS 版本。 如果设备具有密码，则在 MDM 将更新发送到设备后，设备会将更新排队，并提示用户输入密码以开始安装。 有关更多信息，请查看 **Software_Updates**。

7.5.21. 重新安装 iOS 系统应用

适用于：

- iOS 11.3+ 设备。

在 iOS 设备上重新安装删除的 iOS 系统应用。

步骤

1. 导航到**设备页面**。 或者，您可以单击设备的名称并从“设备详细信息”页面执行此操作。
2. 选择一个或多个 iOS 设备。
3. 在**操作**菜单中，单击**重新安装 iOS 系统应用**。
4. 在“重新安装 iOS 系统应用”显示框中，选择要安装在设备上的一个或多个可用系统应用。
5. 单击**重新安装应用**。

设备签入后，应用会安装到所选的兼容 iOS 设备上。 以这种方式安装的系统应用将不会被视为受管应用。 如果没有选择兼容的设备，您将收到一条消息，表明这些设备上不会安装系统应用。

有关更多信息，请查看 **Software_Updates**。

7.5.22. 将设备分配到新用户

如果用户角色发生改变或如何此前用户与公司的关系发生改变，现有注册设备可能需要重新为新用户配置。 这些步骤有助于避免停用并重新注册设备。

过程：

1. 在**设备 页面**导航至该设备。
2. 单击设备名称，以便显示“设备”详细信息页面。
3. 单击**分配到用户**  图标。

> 或者，可以从**设备**页面中选择一台设备，然后点击**操作**菜单中的**分配给用户**选项。

开始在**搜索用户**中输入用户名... 字段。

5. 选择目标用户。
6. 单击**分配到用户**。
   将为该用户配置设备。

> 您可能注意到，在基于用户和基于许可证的情景中，您可以为超过已分配设备限制的用户分配设备。 这是因为设置限制功能的意图旨在限制设备注册，以支持自带设备 (BYOD) 情景。

在基于设备和基于用户的许可证中，强制设备限制不合逻辑。 对于基于设备的许可证，最终客户的成本不会更改，因为系统中的设备总数量不会改变。 对于基于用户的许可证，缺少此检查实际上对客户有益。 例如，假设共有 5 位用户 U1 至 U5，每个配备 5 个设备。 凭借基于用户的许可，这会占用 5 个许可证。 如果相反，来自 U4 和 U5 的两个设备移到 U1 和 U2，然后许可证占用量会下降，从 5 个减少为 3 个。

7.5.23. 重新分配 Android 设备

管理员可以将 Android 设备的所有权从一位用户转给另一位用户。 在重新分配流程中，设备的管理配置文件将从当前用户重新配置或重新映射到 Android Enterprise 模式下的新用户。 重新分配可以在除 Android Management API (AMAPI) 设备之外的所有 Android Enterprise 设备上完成，但不能在 Google Domain Android Enterprise 设备上完成。

> 设备重新分配只能在相同模式的设备上进行。 例如，工作托管设备模式下的设备可以重新分配给同一模式下的另一位用户。

设备重新分配流程将具有以下状态：

- 已发起
- 成功
- 失败
- 挂起

可以在**设备详细信息**页面 → **概述**选项卡 → **上次重新分配状态**下查看设备的上次重新分配状态。

步骤

1. 转到**设备**。
2. 从列表中选择一个或多个设备。
3. 从**操作**列表中，点击**分配给用户**。
4. 或者，可以点击任何设备名称。 **设备详细信息**页面随即打开。 点击**分配给用户**图标以显示“分配给用户”屏幕并选择所需的用户。
5. 点击**分配给用户**。 将验证所选的选项，以检查所选设备是否可以重新分配给所选用户。
   成功验证和重新分配后，屏幕上会显示一条确认消息。

> 如果选择的设备数量达到上限 10 台，则屏幕上会显示“分配已启动”消息。 如果选择了 11 台或更多设备，屏幕上会出现“验证正在进行”弹出窗口。

> Android 设备重新分配是一种独特的创新解决方案，重点关注消除先前注册用户的剩余数据，并且仅在 SUEM-Premium SKU 中提供。

7.5.24. 强制设备进行签入

设备需要联系 Ivanti Neurons for MDM（签入），以提供和接收信息。 定期安排签入。 也可根据需要提示设备签入。 强制设备签入可提高应用{{配置}}，更新{{策略}}等流程速度

步骤

1. 转至**设备 > 设备**。
2. 选择设备。
3. 单击**操作**。
4. 选择**强制签入**。
5. （可选）单击设备名称链接，转到设备详细信息页面；单击**强制签入**  图标，并单击**确定**。

> 如果在签入期间处理配置安装命令时设备端出现故障，Ivanti Neurons for MDM 将不会在稍后的签入过程中自动重试将配置安装到设备。 管理员需要从设备的设备详细信息页面重新尝试手动安装配置。 为此，请转至“配置”选项卡，选择错误配置，然后单击**重试安装**。

7.5.25. 定位设备

如果您已启用了设备的“定位”功能，您可以显示设备的最后一个已知位置。 您必须编辑**隐私配置**，以便启用位置数据收集，并将配置应用于设备以启用此功能。 设备必须也支持该功能，且用户必须同意共享其定位数据。

步骤

1. 在**设备 页面**导航至该设备。
2. 单击**名称**列中的链接。
3. 在**概要**选项卡中，单击**设备位置**下的链接。

页面上会显示以下详细信息。

字段名称	描述
上次位于	显示设备上次定位的日期和时间。
坐标	显示设备的纬度（南北位置）和经度（东西位置）。

您还可以在页面中找到设备位置图。

7.5.26. 锁定设备

您可触发设备上的屏幕锁。 不同设备上的锁定工作方式有所不同。

步骤

1. 转至**设备 > 设备**。
2. 选择该设备。
3. 单击**操作**。
4. 选择**锁定**。
5. 或者，点击设备名称链接转到“设备详细信息”页面，然后点击**锁定**  图标，然后点击**确定**。
6. 对于 AppConnect Android 应用程序，“锁定”命令将用户锁定在容器之外，同时也会锁定设备。 用户可以分别使用设备密码和 AppConnect 密码重新登录设备和 AppConnect 应用程序。
7. 对于 iOS 7 设备，您可输入显示消息和电话号码（可选）。
   这些选项可为设备用户提供设备锁定原因的相关信息，以及呼叫哪些号码可将其解锁。
8. 对于 macOS 设备,会提示用户输入 6 位 PIN 作为访问设备的通行码。 要继续屏幕锁定，设备用户需要：
   1. 输入 PIN。
   2. 选中复选框，以确认锁定设备。
   3. 单击**是，发送锁定命令**。

> 在 macOS 中，用户可以在设备锁定通行码设置过程中添加可选的锁屏界面消息和电话号码。

9. 对于 ChromeOS 设备，执行锁定操作时，屏幕上会弹出一个窗口，其中显示消息“锁定设备操作可能需要用户输入密码，以访问设备。”点击**锁定**，设备状态将更新为**禁用已发送**，设备定期同步后会显示更新的设备状态。

用于锁定设备的备选方法：

- 设备用户可以从自助服务门户网站执行锁定操作。
- 管理员可以从管理员门户网站执行锁定操作。

7.5.27. 管理遗失模式下的 Apple 设备

本部分包含以下主题：

- 启用丢失模式
- 执行丢失模式操作
- 禁用丢失模式

适用于：iOS 10.3+ 被监控设备

可以通过 Ivanti Neurons for MDM 将受监管设备置于丢失模式。 这意味着您向 Apple 服务器报告设备丢失，允许您检索设备的最后记录位置，以及如果找到设备，则禁用丢失模式。

启用丢失模式

您可以通过将设备置于丢失模式来向 Apple 服务器报告设备丢失。 将设备置于丢失模式后：

- 如果设备已停用，则无法禁用丢失模式。
- 如果设备被擦除，则无法找到或跟踪设备。

步骤

1. 转到**设备**。
2. 选择该设备的复选框。
3. 选择**操作** > **通用** > **启用遗失模式**。
4. 您也可以通过选择设备名称链接导航到**设备详细信息**页面。 点击设备的操作图标，然后选择**启用遗失模式**。

执行丢失模式操作

启用丢失模式后，可以从“丢失设备模式”部分执行以下操作：

- 将消息/电话号码推送到 iPhone
  - 输入要在丢失设备的锁定屏幕上显示的消息。
  - 输入要在丢失设备的锁定屏幕上显示的联系号码。 如果有人找到该设备，他们可以呼叫该号码进行报告。

锁定设备

- **刷新设备位置**

> 如果设备被擦除，您将无法找到该设备。

- **播放丢失模式声音**

> 将播放声音，直到设备从丢失模式中移除或用户禁用设备上的声音。

- **刷新位置**
  遗失模式中添加了**刷新位置**选项以查看设备位置。 将显示以下详细信息：
  - **纬度**：设备位置的纬度。
  - **时间戳**：显示有效负载时的时间和日期时间戳。

- **经度**：设备位置的经度。

禁用丢失模式

如果检索到处于丢失模式的设备，或者错误地启用了丢失模式，则可以禁用丢失模式。

> 如果丢失的设备在 Ivanti Neurons for MDM 中已停用，则禁用丢失模式将不起作用。

步骤

1. 转到**设备**。
2. 选择该设备的复选框。
3. 选择**操作** > **通用** > **禁用遗失模式**。
4. 也可以点击设备名称链接导航到**设备详细信息**页面，然后选择**遗失设备模式：已启用** > **禁用遗失模式**。

7.5.28. 管理遗失模式下的 Android 设备

本部分包含以下主题：

- 启用遗失模式
- 禁用遗失模式

启用遗失模式

适用于：Android 8+ 设备

可以通过 Ivanti Neurons for MDM 将多个 Android 设备同时置于遗失模式。 此功能支持将设备置于遗失模式，以此将丢失的设备报告给 Ivanti Neurons for MDM，这样就可以在屏幕上显示自定义消息、电话号码和脚注，以及播放声音的选项。

> 此功能仅支持全托管设备，包括非 GMS 设备。

步骤

1. 转到**设备**。
2. 选中设备对应的复选框。
3. 选择**操作 > 启用遗失模式**。
4. 或者，点击设备名称链接转到“设备详细信息”页面，然后点击 ⋮ 图标。 选择**启用遗失模式**。
5. 输入锁屏消息和/或电话号码，以便在丢失设备的锁定屏幕上显示。 管理员还可以选择脚注和**播放遗失模式声音**选项。 如果有人发现设备，可以拨打该号码进行报告。

> 必须在相应字段中输入消息或电话号码才能激活**启用遗失模式**选项。

> “遗失模式”声音将播放 5 分钟，在这段时间内手机解锁、按下呼叫按钮或管理员禁用“遗失模式”时除外。 要重播声音，请在设备上重新启用遗失模式。

6. 选择**启用遗失模式**可将 Android 设备置于遗失模式。

激活遗失模式将禁用以下操作：

- 解除锁定
- 进入/退出 Kiosk
- 强制注销共享 Kiosk
- 分配给用户
- 发送消息
- 设置所有权

> 在设备中启用遗失模式后，将会禁用服务器中的“遗失模式”选项。

禁用遗失模式

如果已找回处于“遗失模式”的设备，或者“遗失模式”因误操作而启用，可禁用“遗失模式”。

如果丢失的设备已从 Ivanti Neurons for MDM 中擦除，则无法禁用“遗失模式”。

步骤

1. 转到**设备**。
2. 选中设备对应的复选框。
3. 选择**操作 > 禁用遗失模式**。
4. 也可以点击设备名称链接转到“设备详细信息”页面，然后选择**遗失设备模式：已启用 > 禁用遗失模式**。

在**详细信息**部分，只有在激活**启用遗失模式**后，**禁用遗失模式**才可见。 激活**禁用遗失模式**后，**遗失设备模式：已启用**字段（包括**禁用遗失模式**选项）将消失。

禁用“遗失模式”后，需要重新输入之前处于 Kiosk 模式的设备。

7.5.29. 请求调试日志

您可以向 iOS、macOS 和 Android 工作受管设备发送请求检索调试日志，以对设备问题进行故障排除。 使用设备页面中的“请求调试日志”命令，调试日志会捕获操作和事件的成功或失败。

此功能需要以下客户端：

- iOS 设备需要 Go 5.3.0 for iOS 或支持的更新版本。 对于从 Ivanti EPMM 迁移到 Ivanti Neurons for MDM 的设备，此功能需要适用于 iOS 的 Mobile@Work 12.2.0 或支持的较新版本。
- macOS 设备需要 Mobile@Work 1.5 for macOS 或支持的更新版本。
- Android 工作托管设备需要适用于 Android 的 Go 65 或支持的较新版本。

步骤

1. 转至**设备 > 设备**。
2. 选择设备并单击设备名称链接，以转到“设备”详细信息页面。
3. 单击 ⋮ 图标。
4. 选择**请求调试日志**，并单击**确定**。

当发送请求及日志在设备中准备就绪时，将向管理员发送通知，并在设备日志中显示通知。 通过单击链接，也可以下载设备日志。

7.5.30. Apple_Enhanced_Logging

File not found!

7.5.31. 停用设备

停用设备将结束其与 Ivanti Neurons for MDM 的关系。 如果发生以下情况，您可能需要停用设备：

- 用户离开公司
- 用户已更换设备
- 您需要撤消已完成的管理任务（重新开始）

步骤

1. 转至**设备 > 设备**。
2. 选择该设备。
3. 单击**操作**（右上角）。
4. 选择**停用**。
5. 或者，单击设备名称链接，转到“设备详细信息”页面，然后单击 ⋮ 图标。
6. 选择**停用**，然后单击**确定**。

当对处于活动状态的设备执行停用操作后，该设备将立即停用。

7.5.32. 放弃设备的所有权

适用于公司拥有设备上的工作配置文件模式中的 Android 设备。

在公司拥有设备上的工作配置文件模式中放弃设备的所有权会移除工作配置文件，并从 Ivanti Neurons for MDM 中停用设备，并且不会影响个人应用和数据。 然后，最终用户可将该设备用作个人设备，并对所有设备控制和设置拥有完全访问权限。

> 相关设备需要从 Google Zero Touch 或 Knox 移动注册门户中删除。

如果出现以下情况，您可以通过放弃设备的所有权：

- 用户离开公司
- 用户已更换设备

步骤

1. 转至**设备 > 设备**。
2. 选择该设备。
3. 单击**设备详细信息页面**，并单击 ⋮ 图标。
4. 选择、**放弃所有权**。

7.5.33. 擦除设备

擦除设备会移除所有数据，并将设备恢复为出厂默认设置。

步骤

1. 转至**设备 > 设备**。
2. 选择该设备。
3. 单击**操作**（右上角）。
4. 选择**擦除**。
5. 或者，单击设备名称链接，以转到设备详细信息页面，并单击 ⋮ 图标。 选择**擦除**，然后单击**确定**。
6. 默认选择**保留数据计划**选项。
   （可选，适用于 iOS 11.3+ 设备）选择**跳过邻近设置**选项。
7. 选择**返回服务**选项可在擦除数据后自动重新注册，这样您就不必在擦除后手动重新注册设备。 仅适用于以 DEP 模式注册的 iOS 17+ 设备。
   1. 从下拉菜单中选择 **Wi-Fi 配置**。 用户需要停用所有激活锁定。 仅适用于以 DEP 模式注册的 iOS 17+ 设备。
   2. （可选）如果您希望设备在保留现有应用的情况下恢复服务，请选择**保留应用程序**选项。 只有使用 Ivanti N-MDM 安装的具有高优先级的应用程序才会被保留。 仅适用于 iOS 26+ 设备。
8. 对于 macOS 设备，您可以向设备发送作为通行码的 6 位数 PIN。 在设备上，提示用户输入 PIN 以访问设备。 若要继续擦除操作，设备用户需要：
   1. 输入 PIN。
   2. 选中该复选框以确认设备擦除操作。
   3. 单击**是，擦除此设备**。
9. 对于 ChromeOS 设备，从**设备详细信息**或**设备列表**页面执行擦除操作时，屏幕上将弹出窗口消息“擦除设备将使其恢复出厂设置，这可能会导致设备数据丢失。 擦除操作因平台而异。”
   1. 选中“我了解擦除无法撤消”复选框，确认设备擦除操作。
   2. 点击**擦除**，执行设备擦除。

设备状态更改为“**擦除已发送**”。设备定期同步后会显示更新的设备状态。

在 Android Enterprise 设备上，即使在设备重新启动并保持锁定状态后，也可以执行**擦除**设备操作。

可以使用**设备详细信息**页面上提供的**删除设备**选项，删除处于**待擦除**状态的 Android 设备。 被删除的设备会立即失去与服务器的连接，并变为不合规。 所以用户在执行出厂重置后必须重新注册设备。

7.5.34. 删除设备

停用设备后，可将它删除。 将它删除会将其从所有页面移除。 仅当设备状态为“已停用”、“待停用”、“已擦除”或“待擦除”时，才能删除设备。

步骤

1. 转到**设备 > 设备**。 屏幕上将显示设备列表。
2. 选择要删除的设备。
3. 点击**操作**。
4. 在**通用**部分下，选择**删除设备**选项。 屏幕上将显示弹出消息。
5. 选择“本人了解删除无法撤销”选项，然后点击**删除设备**。
6. 您也可以按照以下步骤删除设备：
    - 转到**设备 > 设备**。
    - 点击**用户显示名称**列下的任意链接。 屏幕上会显示**设备详细信息**页面。 点击**设备详细信息**。 屏幕上将显示弹出消息，如果您知悉警告并点击**确定**，则系统会删除特定设备。

删除多个设备

可以通过选择要删除的所有设备来删除多个设备。

步骤

1. 转至**设备 > 设备**。
2. 从可用设备列表中选择设备。
3. 点击**操作**选项卡，在**通用**标题下选择**删除设备**选项。
4. 在**删除设备**窗口中：
    1. 选中**我了解删除无法撤销**复选框。
    2. 点击**删除有效设备**以删除所选设备。

7.5.35. 解锁设备

本部分包含以下主题：

- 解锁 Android 设备
- 解锁 AppConnect for Android 应用程序
- 解锁 iOS 设备
- 解锁 ChromeOS 设备

解锁设备：

您可以取消设备的屏幕锁定。 解除锁定功能在不同设备上的作用稍有不同。

步骤

1. 转至**设备 > 设备**。
2. 选择设备。
3. 单击**操作**。
4. 选择**解除锁定**。
5. 或者，点击设备名称链接转到“设备详细信息”页面，然后依次点击**解锁**  图标和**确定**。

解锁 Android 设备

当收到解锁命令时，Android 应用程序会尝试重置密码。 在“设备管理员”和“设备所有者”模式下，解锁代码将被重置，而在“配置文件所有者”和“公司拥有个人启用”模式下，工作配置文件解锁代码将被重置。

解锁命令为管理员提供了一个选项，可以设置由字母数字字符组合构成的解锁代码。 默认选项将解锁代码设置为“0000”，可以在多个设备上执行。 但是，新选项“为 Android 设备设置自定义解锁代码”一次只能在一台设备上执行。 最少 6 个字符，最多 8 个字符。 可在**操作**选项卡下方以及**设备详细信息**页面中找到此选项。 从**操作**选项卡或**设备详细信息**页面选择“解锁”选项时，系统会显示以下两个选项。

- 默认
- （仅限 Android）提供解锁代码 - 您可在此部分中输入解锁代码，然后点击**解锁**。
    - 跳过设备上的密码重置提示 - 如果将密码配置推送到设备，请选择跳过密码重置。

设置解锁代码后，管理员可以在**审计跟踪**页面和**设备日志**页面中找到解锁代码。

> 直接启动解锁仅适用于默认解锁选项，即“0000”解锁代码。 不支持使用自定义解锁代码进行直接启动。

解锁 AppConnect for Android 应用程序

对于 AppConnect 应用，**AppConnect 解锁**命令有助于解锁因用户尝试输入错误通行码多次登录而锁定的容器。 此解锁不会解锁设备。

解锁 iOS 设备

收到解锁命令后，iOS 应用将从设备中删除通行码。 如果通行码配置指定需要新通行码，则会提示设备用户设备一个新通行码，该通行码需要遵守通行码配置中定义的规则。 用户必须在 60 分钟内进行此更改，否则应用程序将强制用户设置新通行码。

解锁 ChromeOS 设备

选中 ChromeOS 设备并点击**解锁**选项后，屏幕上将弹出窗口消息“解锁可清除现有密码，使用户能够访问设备。 解锁操作因平台而异。”点击**解锁**，设备状态将更新为“解锁已发送”，设备定期同步后会显示更新的状态。

7.5.36. 重新启动或关闭设备

本部分包含以下主题：

- 重新启动设备
- 关闭设备

适用于： Android 7.0+（受管设备）、受监控 iOS 10.3+、受监控 tvOS 10.3+，macOS 10.13+ 和 Windows 10+ 设备。

管理员可以从设备详细信息页面单独或从设备列表页面批量重启或关闭 iOS 受监控设备。

重新启动设备

步骤

1. 转到**设备**。
2. 导航至设备。
3. 单击**名称**列中的链接。
4. 单击**操作**按钮。
5. 单击**重新启动/关闭设备**。

> 无法重新启动不支持的设备。

6. 阅读显示的警告。
7. （可选）选择在重新启动时清除设备通行码的选项。 如果通行码未被清除，则设备将需要通行码，并且重新启动后将不会连接到 WiFi。
8. 如果未选择，选择**重新启动设备**。
9. 如果仍要重新启动设备，单击**发送到设备**。 否则，单击**取消**。

> 对于 Android 设备，管理员可以在"设备详细信息"页面中的**正常运行时间**下查看关于设备重启时间的信息。

您可以从**设备**列表页面重新启动多个受支持的设备。 为此，请选择设备，单击**操作> 重新启动/关闭设备**，然后按照屏幕上的说明进行操作。

关闭设备

步骤

1. 转到**设备**。
2. 导航至设备。
3. 单击**名称**列中的链接。
4. 单击**操作**按钮。
5. 单击**重新启动/关闭设备**。

> 无法重新启动不支持的设备。

6. 阅读显示的警告。
7. 选择**关闭设备**。

8. 如果仍要关闭设备，单击**发送到设备**。 否则，单击**取消**。

您可以从**设备**列表页面关闭多个受支持的设备。 为此，请选择设备，单击**操作> 重新启动/关闭设备**，然后按照屏幕上的说明进行操作。

7.5.37. 清除限制密码（仅 iOS）

在受监控的 iOS 8 设备上，您可以清除用户设置的限制密码。 此操作仅适用于活动设备。

步骤

1. 转至设备 > 设备。
2. 选择设备条目。
3. 选择“操作”>“清除限制密码”。
4. 出现提示时确认操作。

7.5.38. 删除设备的 Sentry 关联

Sentry 关联是针对 App Tunneling 或启用ActiveSync 的电子邮件系统的设备进行的，控制对设备的电子邮件访问。 如果需要，可以将与 Sentry 关联的任何设备从其关联中删除，如下所示：

步骤

1. 转到**设备**。
2. 在**名称**列中，单击要删除 Sentry 关联的设备的设备链接。
3. 单击 **Sentry** 选项卡。
4. 在**操作**列中，点击**删除**。

7.5.39. 将自定义属性分配到设备

您可以将内部 ID 等自定义设备属性分配到一个或多个设备。 每个属性都有一个对应值，您可使用该变量创建配置和设备组等任务。 创建自定义属性后，可以将其分配给设备。 有关管理属性的详细信息，请参阅**属性**。

步骤

1. 登录到管理门户。
2. 转到**设备**。
3. 选择一台或多台设备。
4. 单击**操作**。
5. 选择**分配自定义属性**。
6. 选择下列选项之一：
    - 强制分配（覆盖）所有属性，即使找到任何现有值。
    - 仅当值为空时才进行覆盖，并跳过已有值的属性。

选择您想要分配的属性，并输入值（不允许空值）。

8. 单击**分配**。

> 可以从**设备详细信息**页面，将**自定义设备属性**及其值导出为 CSV 格式。

7.5.40. 将自定义属性从设备中删除

继续注意，因为此操作不可逆。 要将自定义属性从一个或多个设备中删除：

步骤

1. 转到**设备**。
2. 选择一台或多台设备。
3. 单击**操作**。
4. 选择**移除自定义属性**。
5. 选择您想要删除的属性。
6. 单击**移除**。

7.5.41. 同步和获取应用反馈

您可以向在 Android 设备上安装的应用发送请求，以获取应用的当前应用配置状态的详细信息。 在发送请求时，您会收到该设备的应用配置反馈报告。

步骤

1. 转到**设备**。
2. 单击您想要发送请求的设备。
3. 单击**操作**。
4. 选择**同步和获取应用反馈**。发送请求，以同步并获取应用配置反馈。 客户端上次签入字段旁边的应用反馈上次同步字段将更新。
5. 在**安装的应用**选项卡中，点击**应用反馈**列中应用的**查看详细信息**链接。 将显示**应用反馈**窗口。
   项 - 提供相关详细信息，并根据从应用程序收到的反馈提供报告设置的布置（在应用程序的托管应用程序配置中）。
   时间戳 - 密钥的时间和日期。
   严重性 - 指定密钥的严要性。 示例：“信息”、“错误”。
   消息 - 从应用配置反馈收到的消息类型。 示例：“失败”。
   数据 - 从应用配置反馈收到数据的详细信息。

从 App Catalog 中查看应用配置反馈

从 App Catalog 中，您可以查看特定应用的应用配置反馈报告。

步骤

1. 转至**应用 > 应用目录**。
2. 选择您想要查看详细信息的应用。
3. 单击**应用配置反馈**选项卡。 **设备计数**列会显示应用配置反馈报告的每个密钥的设备数量（超链接）。
4. 单击设备数量超链接，以查看设备的详细信息。 例如，通过单击超链接 5，显示 5 个设备的详细信息。 对于“密钥”和“严重性”组合，在表格上方显示以下详细信息：
   电子邮件地址 - 指定用户名。 单击用户名链接会导航到**设备 > 设备详细信息**中的**已安装应用**选项卡。
   设备类型 - 指定设备模型。
   OS - Android OS 版本号。
   序列号 - 设备的序列号。
   时间戳 - 上次更新的时间和日期。
   消息 - 从应用配置反馈收到的消息类型。 示例：“失败”。
   数据 - 从应用配置反馈收到数据的详细信息。

通过单击铃铛图标（右上角），或在**仪表板 > 通知**页面中，您可以查看 Android 设备的应用配置反馈错误通知。 单击通知链接会导航到**应用配置反馈**选项卡，并查看应用反馈报告。

> 在设备擦除或停用时，应用配置反馈报告将移除，并且不会显示。 每 24 小时运行一次的后台作业会清除 7 天之前的数据。

7.5.42. 设置固件密码

适用于：macOS 10.13 或支持的更新版本。

管理员可以设置或更新 macOS 设备的固件 (EFI) 密码。 固件密码可防止从设备用户选择的启动盘以外的任何内部或外部存储设备启动 macOS 设备。 因此，它也阻止了使用大多数启动组合键的能力。

过程：

1. 转到**设备**。
2. 要设置或更改单个设备的固件密码，请执行以下操作：
    1. 单击与设备相关联的用户名，查看设备详细信息页面。
    2. 在常规部分中，展开**固件密码**并在设备操作菜单中单击**设置密码**或者单击**设置/更改固件密码**。
    3. 本部分显示以下信息：
        1. **密码：**密码或可能密码的列表。

            > 当管理员设置固件密码时，该命令将发送到设备。 如果设备没有及时响应，密码将暂时存储并显示在此字段中。 直到有来自设备的确认并重新启动设备，新密码才会生效。 直到那时，才会显示所有可能的密码。 设备重新启动并确认密码更改后，将清除所有不需要的密码。

        2. **更改待处理 -** 指示密码更改是否待处理。
        3. **命令状态 -** 指示密码更改是成功还是失败。
        4. **允许 OptionROM -** 指示是否启用选项 ROM。 此项默认设置为“否”。

要设置或更改多个设备的固件密码，请执行以下操作：

1. 选择设备。
2. 从操作菜单中，单击**设置/更改固件密码**。

输入当前密码和新密码。

如果这是第一次，当前密码可以留空。

要重置密码，请将新密码字段留空。

5. 单击**保存**。

> 只有支持 macOS 版本的设备才会使用新密码进行更新。 不支持的设备将被跳过。

7.5.43. 重新发布新个人恢复密钥

适用于：安装 Mobile@Work for macOS 1.66 或支持的更新版本的 macOS 设备。

在从其他 MDM 解决方案迁移到 Ivanti Neurons for MDM 时，如果此前已在注册前发布 PRK，管理员可以在注册时请求 OS 重新发布新个人恢复密钥 (PRK)。 这会使密钥存储在 Ivanti Neurons for MDM 中。

您可以查看 PRK 活动的审计线索日志条目，如下所示：

1. 转到**仪表板 > 审计跟踪**。
2. 在“类型”筛选器中，选择**个人恢复密钥**。PRK 条目将显示在“设备管理”类别和活动中，例如“已查看的个人恢复密钥”。

先决条件

在执行此步骤前，将以下配置分发到设备：

- Mobile@Work for macOS 配置。
- FileVault 恢复密钥配置。

步骤

1. 请联系支持，以在设备上请求脚本生成新 PRK。
2. 创建设备自定义属性，名称为“deviceprk”并在脚本中使用。
3. 将脚本上传到**管理 > 脚本和文件 > 所有脚本**中的存储库。 在执行此操作时，选择“deviceprk”自定义属性。
4. 对于未从旧 MDM 解决方案中检索 PRK 的设备，创建动态设备组。 按以下方式，选择设备组规则：“**平台 =macOS** 和**密码已启用等于是**和 **macOS 个人恢复密钥托管等于否**和 **macOS 恢复密钥类型等于个人**”。
5. 创建您可以从存储库中选择 PRK 脚本的 Mobile@Work for macOS 脚本配置。 将配置分发到新设备组。
6. 计划脚本，以便每天运行一次，或根据需要运行。 此脚本将在每次运行时要求提供用户密码。 默认情况下，脚本执行的超时时段是 60 秒。 建议将**最长运行时间**字段设置为 300 秒，以此来延长相应 Mobile@Work for macOS 配置中的超时期限。

- 请从“设备加密状态”部分中设备的“设备详细信息”页面，获取解密密钥。 点击“FileVault 加密已启用”字段旁边的**查看**。
- 在获取 PRK 时，设备会移出设备组。 因此，脚本配置将不再适用，并从设备中删除。
- 在 MDM 使用脚本检索设备的恢复密钥后，脚本将从设备卸载。

相关主题：

- 属性
- 所有脚本
- 设备组
- Mobile@Work for macOS
- FileVault 恢复密钥

7.5.44. 设置或更改恢复锁定

适用于：macOS 11.5+

对于在 Apple 芯片上运行的 macOS 设备，管理员可以设置或更改设备重启的恢复锁定。 除非输入密码，否则恢复锁定可以防止在恢复模式中启动 macOS 设备。

过程：

1. 转到**设备**。
2. 要设置或更改重启的恢复锁定：
    1. 单击与设备关联的用户显示名称，查看设备详细信息页面。 执行以下步骤之一：
    2. 在**概览**部分中，展开**恢复锁定**，并单击**设置密码**或单击**更改密码**。 或单击**操作**省略号，并单击**设置/更改恢复锁定**。
    3. 在**设置/更改恢复锁定**对话框中执行以下操作：
        1. **当前密码**：在此处输入当前密码。 如果首次设置，将其留空。
        2. **密码**：输入要设置的密码。
        3. **确认密码**：重新输入要设置的密码。

单击**设置/更改恢复锁定**。

> 在概览中，**恢复锁定已启用**显示了恢复锁定密码的状态。

> 管理员也可以通过移除现有通行码清除通行码，并单击**设置/更改恢复锁定**。

7.5.45. Apple 访问管理

必备项：

- 在 Apple Business Manager 或 Apple School Manager 上验证并锁定域。
- 从 Apple Business Manager 或 Apple School Manager 组织中配置至少一个 MDM 服务器，其中受管 Apple ID 存在于 Ivanti Neurons for MDM 中。

登录受管 Apple ID 允许组织控制用户可以访问哪些 Apple 服务和功能。

在 Apple Business Manager 或 Apple School Manager 中，**允许受管 Apple 帐户的位置**设置控制用户可以在何处使用其受管 Apple ID 登录。 管理员可以配置此设置以限制登录托管或受监控的设备，或允许在任何设备上登录。

- **任何设备**（默认）：用户可以在任何设备上使用他们的受管 Apple ID 登录，无论该设备是否由 MDM 解决方案管理。
- **仅限托管设备**：用户只能登录由支持 Get Token 端点的 MDM 解决方案管理的设备。
- **仅限受监控设备**：用户只能在由支持 Get Token 端点的 MDM 解决方案监督（和托管）的设备上登录。

这些设置是 Apple Business Manager 和 Apple School Manager 中 Apple 服务更广泛“访问管理”的一部分。

> 通过增强安全性，限制登录到托管或受监控设备，从而可以通过确保与工作相关的数据只能在受控设备上访问来提高数据安全性。

如果**设备注册**选项卡中存在零个或多个设备注册 MDM 服务器组织，并且管理员在 Apple Business Manager 或 Apple School Manager 中将**访问管理** > **Apple 服务**下的**允许托管 Apple 帐户的位置**设置为“仅限受监管设备”或“仅限托管设备”，则受管 Apple 帐户登录将失败。

> 如果 Ivanti Neurons for MDM 设备注册 MDM 服务器中不存在**受管 Apple** 帐户，则设备将无法登录。

7.5.46. 组策略注册

可以使用组策略在 Ivanti Neurons for MDM 中注册 Windows 10/11 设备。 如果创建组策略，则将自动注册所有混合式加入 Azure AD 的设备。

Procedure使用组策略注册设备

	1.	确保您的设备已混合式加入 Azure AD。 有关详细信息，请参阅 Microsoft 文档：混合式加入 Azure AD 的设备。
2.		创建组策略对象。 有关详细信息，请参阅 Microsoft 文档：配置一组设备的自动注册。
3.		创建一个包含要注册的设备的安全组。 有关详细信息，请参阅 Microsoft 文档：Active Directory 安全组。
	4.	将组策略对象链接到安全组。 有关详细信息，请参阅 Microsoft 文档：将 GPO 链接到域。

用户体验

当用户使用 Azure AD 中的凭据登录设备时，Microsoft 会找到属于其组织的基于 Azure AD 的 MDM 配置。 该设备已在 Ivanti Neurons for MDM 中注册，可以接收策略和命令。

8. 应用

本部分包含以下主题：

- 应用目录
- Apps@Work
- iOS Apps@Work AppStore 功能
- 查看应用详细信息
- 应用配置
- 将自定义属性分配给应用程序
- Android 的托管配置
- 管理 Google Play 应用
- 从 App Catalog 中删除应用
- 升级内部应用
- 查找 Android 应用程序的软件包名称
- 类别
- 分配过滤器
- 排除或分发应用程序
- 评论
- AppleApp 和图书
- 目录设置
- 部署应用依赖性
- 使用 Android Enterprise 部署 Divide Productivity
- 设置配置器应用程序
- 管理 Windows 应用程序
- Ivanti Bridge

8.1. 应用目录

本部分包含以下主题：

- 应用功能的许可
- 在列表和网格视图之间切换
- 为 Android Enterprise 添加 Google Play 商店应用
- 从公共商店添加应用
- 添加内部应用程序
- 为 Android Enterprise 内部应用委派设备权限
- 显示 iOS 内部应用的配置文件状态
- 更新 iOS 内部应用的预配配置文件
- 将内部应用部署到 Google Play
- 为 Android Enterprise 设备添加 Web 应用
- 为 iOS 设备添加 Web 应用
- 使用高级搜索
- 将应用程序导出到 CSV 文件

使用 App Catalog 页面管理您的应用目录。 应用目录可列出您已为您的用户提供的移动应用。 这包括用户可以从公共应用商店下载的应用和您打算用 Ivanti Neurons for MDM 分发的应用（内部应用）。 启用 AppConnect 的应用程序、GoClient for iOS 和 M@W for macOS 也在“应用程序目录”页面上作为企业应用程序提供，从而简化了导入它们以进行配置和分发的过程。 在 MAM Only 设备中，将提示 iOS 用户选择证书，以在打开 App Catalog 时对这些应用的访问权限进行身份验证。

Apple 生产的 M1 芯片组 MacBook 支持 iPhone 和 iPad VPP 应用。 只有管理员可以推送支持的 iPhone 和 iPad VPP 应用。 用户无法使用此选项从 App Catalog 安装。

对于使用 Android 设备的 Ivanti Neurons for MDM 租户，如果未在 2021 年 3 月底之前启用 Android Enterprise，管理员将无法使用名称搜索应用程序。 在访问 App Catalog 页面时，将显示此变更的通知，以及一则横幅消息。 此横幅消息将继续显示，直到在这些租户上启用 Android Enterprise 且未选中“不再显示此内容”复选框选项。

- 静默应用安装方法不适用于公共 macOS 应用。 macOS 应用也可以通过 Apple App 和图书并经由基于设备的许可证和注册时使用静默应用安装方法进行部署。
- 在将 Go 应用上传到 Ivanti Neurons for MDM 服务器时，如果您需要选择**转换到托管应用**选项，则还需要启用**安装在设备上**选项。
- Sonim XP5s 设备不支持 App Catalog 和应用安装。
- Android 不允许卸载具有主动管理员权限的应用程序。 要卸载此类应用，请转到**设备设置 > 安全 > 设备管理员**，并禁用设备管理员权限。然后，卸载应用程序。
- 如果 Android Enterprise 应用程序是使用设备的 Android Enterprise Play Store 手动安装的，并且如果管理员稍后取消分发该应用程序，则也必须手动卸载应用程序。
- 如果应用已压缩或混淆，无法上传内部 Android 应用。
- 共享 iPad 不支持公共应用。
- 由于 Apple 相关限制，对于应用程序目录中可用的企业对企业 (B2B) iOS 应用程序，**详细信息**选项卡中不提供这些应用程序的描述和截图。

- 在应用程序目录或管理员门户中搜索应用程序时，将基于**应用程序名称**、**评论**、**描述**、**显示版本**和**新增功能**显示搜索结果。 如果搜索到的应用程序数据与这些字段中的任何一项相匹配，则将显示为搜索结果。

应用功能的许可

以下应用目录功能需要额外授权：

- 静默应用安装/卸载：Silver 许可证
- Per-app 配置：Gold 许可证
- AppConnect 自定义配置：Gold 许可证
- **Android Enterprise** 自定义配置：Silver 许可证

如果 Android 设备处于"自助服务终端模式"：

设备处于"自助服务终端模式"时，才可安装内置应用。 您可以安装公共应用，但设备必须在退出"自助服务终端模式"之后才可安装这些应用。 此外，对于自助服务终端模式中的设备，您可将对其可用的应用限制为仅由贵公司批准或已加入允许列表的应用。 在使用 Android 4.1 的设备中，如果批准的应用启动允许列表未包含的应用，该应用将启动，然后快速最小化。 在使用 Android 5.0. 的设备中，从已加入允许列表的应用启动的未批准应用仍可用。

在列表和网格视图之间切换

单击应用程序类别屏幕右侧的列表或网格图标。

为 Android Enterprise 添加 Google Play 商店应用

- 您可以将 Google Play 商店中的应用程序添加到应用程序目录并将其提供给用户。 要在 Android Enterprise 中从 Google Play 商店添加应用，需要批准 App Catalog 包含应用。
- 适用于 Android Enterprise 设备的 Google Play 商店布局为迁移的设备提供了主页，该主页将从 Core 进行管理，并提供 Ivanti Neurons for MDM 的快速链接，从而显示从 Ivanti Neurons for MDM 管理的所有应用。 在将 Android Enterprise 设备从 Core 迁移到 Ivanti Neurons for MDM 时，设备的工作配置文件 Google Play 商店中仅会列出 Core 与 Ivanti Neurons for MDM 应用程序目录之间的常见应用。 可以点击 Ivanti Neurons for MDM 按钮，查看 Ivanti Neurons for MDM 应用程序目录提供的所有应用的列表。

适用于 Android Enterprise 设备的 Google Play 商店布局为迁移的设备提供了主页，该主页将从 Core 进行管理，并提供 Ivanti Neurons for MDM 的快速链接，从而显示从 Ivanti Neurons for MDM 管理的所有应用。 在将 Android Enterprise 设备从 Core 迁移到 Ivanti Neurons for MDM 时，设备的工作配置文件 Google Play 商店中仅会列出 Core 与 Ivanti Neurons for MDM 应用程序目录之间的常见应用。 可以点击 Ivanti Neurons for MDM 按钮，以查看在 Ivanti Neurons for MDM 应用程序目录中可用的所有应用程序。

先决条件

- 您必须启用 Android Enterprise，才可以访问 Google Play 商店应用，并将其添加到 App Catalog。

Procedure程序

1. 转至**应用 > 应用目录**。
2. 单击**添加**（左上角）。

> 从下拉列表中选择 Google Play，并在 Google Play 商店中搜索应用。 注册 Android Enterprise 时会显示 Google Play iFrame。

3. 在搜索栏中搜索该应用，然后点击该应用。
4. 单击**完成**。

之后，可以通过点击**取消批准**，取消批准已批准的应用程序。

选项	说明
批准设置	
应用请求新权限时保持批准	允许用户安装更新的应用程序
当此应用请求新权限时撤销应用批准	**将应用从商店中删除，直到重新获得批准。**
批准设置	
添加订阅者	输入电子邮件地址，当您批准的应用请求新权限时，将订阅者添加到电子邮件通知中。

从公共商店添加应用

您可以将公共商店中的应用添加到 App Catalog 并将其提供给用户。

步骤

1. 转至**应用 > 应用目录**。
2. 单击**添加**。
3. 选择您想要添加的应用：
4. 选择公共应用商店。
5. 输入应用名称。
6. 从列表中选择应用。
7. 单击**下一步**。
8. 描述用户应用：
9. 添加或移除类别。
10. 输入可选说明。
11. 单击**下一步**。
12. 定义应用分配：
13. 选择分配选项。
14. 展开**高级选项与应用配置**部分。
15. 按照以下指导方针完成相关选项：

设置	流程
在设备上安装	选择此选项在注册后立即开始安装。 用户将看到提示，确认应用的安装，但出现以下情况时除外： • 对于新应用安装和应用更新，设备是受监控的 iOS 设备。 • 对于应用更新，设备是 iOS 非受监控的设备。 • 注册 App 和图书计划的用户。 • 此设备是 Samsung Knox 设备，已选中以下静默安装选项。 对于 iOS 公共应用，首次在设备中安装时，App Catalog 会显示“重新安装”按钮，允许用户再次安装应用。 如果设备上的应用版本与 iOS App Store 上的版本不同，将执行重新安装。
不在最终用户应用目录中显示	选择此选项，如果您不希望用户在设备的 App Catalog 中看到此应用。
设置应用安装优先级	选择“高”、“中”或“低”，设置在用户加入过程中应用安装的优先级。 只有高优先级应用，才可以在用户加入过程中安装。
在尝试失败一定次数后，暂停应用重新推送（仅 iOS）	使用以下设置，将切换开关切换为“打开”，以在失败重新推送尝试达到一定次数后，暂停应用重新推送： **停止重新推送后** - 输入重新推送尝试失败次数，然后应停止重新推送。 输入的值应介于 **1** 与 **999** 之间 **尝试失败并重试后** - 输入重新推送失败后重新执行重新推送操作所需的小时数。 输入的值应介于 **3** 至 **48** 小时之间。
（仅 Android）在 Samsung Knox 设备上进行静默安装	此选项不适用于公共应用。
（仅 iOS 和 macOS）启用此应用的 Per-App VPN	选择此选项以使用该应用的 Per-App VPN 配置。 从下拉列表中选择要使用的 Per App VPN 配置。 对于 macOS，请仅选择 Tunnel Per App VPN 配置。
（仅 iOS）阻止备份到 iCloud 和 iTunes	选择此选项以阻止将同该应用相关的数据备份到 iCloud 和 iTunes 中。
（仅 iOS）在取消注册后，移除该应用	选择此选项，以当设备不再由 Ivanti Neurons for MDM 管理时移除此应用。
（仅 iOS）AppConnect 自定义配置	对于支持 AppConnect 的应用，输入指定自定义配置首选项的键和值。 请参阅应用文档，了解可用的键。
iOS 7+ 托管的应用设置	输入将此应用作为 iOS 7+ 托管的应用时为其定义的键和值。 请参阅应用文档，了解支持键的信息。

> Android Enterprise 应用程序将具有不同的选项。

单击**下一步**

4. 选择升迁选项：
5. 单击 **+添加描述**，输入配置的简要描述。

- 无特色

- 特色列表
- 特色横幅
- 如果选择特色横幅，请指定以下详细信息：
    1. **标题** - 指定应用程序标题
    2. **描述** - 指定应用程序详细信息
    3. **横幅样式** - 选择横幅颜色
6. 您可以选择是否改变配置的分配情况。
7. 单击**完成**保存应用配置。
8. 单击**完成**。

> 当在"应用程序目录"中搜索 Windows 应用程序时，可以通过下拉列表中的**应用程序名称**或 **AppStore ID** 选项搜索高度匹配的应用程序：

- **应用程序名称** - 选择此选项并提供应用程序名称
- **AppStore ID** - 选择此选项并提供 AppStore ID

Windows 应用商店应用程序搜索支持 Win32 应用商店应用程序。

确保设备上有可用于管理 Win32 应用商店应用程序的 Winget 工具。

添加内部应用程序

您可以使用以下文件格式将内部应用程序上传到 App Catalog。 上传大文件可能需要几分钟。 内部应用版本的数量限制为 100。 如果超过该数量，Ivanti Neurons for MDM 系统将清除应用的最旧版本。 审核线索页面会列出和显示应用上传和清除的状态。

对于小部分应用，Mobile@Work 返回的 MIP 应用库存不正确。 对于未安装到默认位置的应用，Mobile@Work 无法检测到其安装状态。 对于此应用，添加检测脚本将有助于在设备上找到应用的正确状态。 如果检测脚本的退出代码为 0，Mobile@Work 确定应用是否存在。 对于任何其他退出代码，该应用将确定为未安装。 基于检测到的应用，Mobile@Work 将为设备准备库存报告。

- IPA (iOS)
- MIP（Packager macOS 应用）
- PKG (macOS)
- APK (Android)
- APPX、APPXBUNDLE、EXE 和 MSI (Windows)

> 对于带有脚本的 PKG 或拥有带有脚本的 PKG 的 DMG 等应用，Mobile@Work for macOS 仅可以检测成功的安装请求。 如果应用已删除，或如果移除已安装脚本，将不会报告。 因此，Ivanti Neurons for MDM 服务器将无法重新发送安装命令。 如果在下载应用时断开连接，请通过执行签入操作重试应用安装。 对于 MIP 应用，如果 PKG 的条目位于客户端设备的收件人文件夹中，Mobile@Work 将不会安装 MIP 应用，即使应用从由 PKG 或 DMG（其中 PKG 包含脚本）设备中移除。

步骤

1. 转至**应用 > 应用目录**。
2. 单击**添加**（左上角）。
3. 在**选择要上传文件的平台**下，选择您的平台类别（例如 **Apple 应用程序**），然后从 Apple 应用程序下拉列表中选择特定操作系统（例如 iOS 或 macOS）。

> 如果用户选择平台并尝试上传冲突的文件类型（例如，选择 Apple 但上传 .apk），系统将触发“不是有效的文件格式”错误。

4. 将应用文件拖动到虚线框中，或者单击**选择文件**以从文件系统中进行选择，然后单击**确认**。
5. 单击**下一步**（右下方）。
6. 描述用户的应用，并配置必备应用：
7. 添加类别。
8. 在添加 macOS 软件包时，如果软件包文件包含多个应用（例如，Microsoft Office 和 Cisco AnyConnect 软件包），则选定的主应用将用于标识软件包已安装。 Per-app VPN（如果已配置）将应用于这些应用程序。
9. 输入可选说明。
10. **MSI 产品代码**：在上传 MSI 应用时，MSI 应用的产品代码将在此字段中自动填充。

> 必须选择“我已检查 MSI 产品代码”选项，以确保填充正确的 GUID。

覆盖 URL：输入可选的应用源 URL 覆盖，以允许从其他来源下载应用或允许从本地网络（HTTP 和 HTTPS）获取大型文件，例如 Microsoft Office 安装介质。 此选项需要访问安全的内部网络，并手动同步存储应用程序的备用服务器。 除非已经建立了必要的基础设施，否则不要输入值。 您可以在编辑特定应用程序的应用程序设置时编辑此值。

   - 对于 iOS 应用程序，应用程序覆盖 URL 必须为 HTTP 或 HTTPS 格式。
   - 对于 Android 和 macOS 应用程序，应用程序覆盖 URL 必须为 HTTPS 格式。
   - 对于 macOS 应用程序，URL 应以扩展名“.pkg”结尾。

6. **命令行**（仅限 Windows 32 位 MSI 应用）：在部署 MSI 文件时，输入可选命令行开关，以指定不属于软件包部分的其他信息。 例如，要将安装日志写入输出文件，可以在此字段中输入“/ log output.txt”。 这将在 C:\Windows\System32 文件夹中创建 output.text 文件。 默认情况下，在 MSI 应用上传过程中，静默安装的命令行选项 /qn 将自动填充。

> 对于要上传 MSI 应用的软件包名称，不得添加为命令行参数的一部分。 如果添加，在该应用的软件包名称从命令行参数中移除前，上传将受限。 对于所有支持的命令行选项的列表，将在其他链接下方提供。 此链接将在应用的查看和编辑模式中可见。

适用于 Win32 的 .EXE：使用 Admin PowerShell 模式通过 Bridge 安装。 系统将自动使用 Bridge 功能（如有）。

   - 更新版本，保持**显示版本**和**绑定版本**的一致性
   - 安装程序 (.EXE) 位置
   - 安装程序命令行参数：以静默方式运行文件（例如 /SILENT 或 /VERY SILENT）时所使用的参数，为必填项
   - 以用户身份运行安装程序：要使用用户凭据进行安装，请选择“以用户身份运行”选项

适用于 Win32 应用商店应用程序：使用 Admin PowerShell 模式通过 Bridge 安装。

9. 对于 Packager macOS 应用，配置必备应用（可选）。 请查看了解 Packager 内部 macOS 应用，以了解必备应用功能概述。
10. **启动 URL**：输入在 AppStation 中启动应用的自定义 URL。 仅在添加非 AppConnect 应用以在带有 AppStation 的仅限 MAM 部署中分发时需要；并仅适用于 iOS 应用。
11. 配置应用委派。

> 在您委派必备应用并成为非默认空间内部应用的必备应用后，您无法取消委派该应用，除非您先移除必备关系。

单击**下一步**。

13. 单击**下一步**。
14. （可选）添加应用截图。
15. （可选）添加或替换应用程序的图标（iOS、MacOS 和 Windows 应用程序）。
16. 单击**下一步**。
17. 对于 Packager macOS 应用，定义或选择要在应用安装之前和/或之后运行的安装脚本。 通过在搜索框中键入或单击链接，选择以下其中一个或两个脚本，以查看脚本列表。 单击**下一步**。
18. 您可以在**管理 > 脚本和文件 > 所有脚本**页面中创建脚本。 如果您升级应用，您可以选择从早期应用复制脚本，并为已升级应用运行脚本。 如果您跳过本部分，您可以通过稍后编辑应用进行脚本配置。

- **安装前脚本** - 输入脚本名称，以选择要在应用安装之前运行的脚本。 运行或重新尝试安装前脚本，直到从客户端收到脚本执行成功状态。 仅在此之后发送应用安装命令。 在**日志**选项卡中，您可以在设备详细信息页面上查看脚本运行状态。
- **安装后脚本** - 输入脚本名称，以选择要在应用安装之后运行的脚本。
- **卸载脚本**：输入服务器在检测到应用不再分发到设备时发送到设备的脚本名称。
- **检测脚本**：输入服务器发送到设备的脚本名称，以便检测应用。 应用的检测脚本结果将覆盖设备中应用的默认库存结果。 无论应用是否分发到设备，所有应用的检测脚本将发送到设备，评估设备是否存在应用。
  示例检测脚本如下所示：

```
#!/bin/bash
app_name="Name of the App"
count="$(system_profiler SPApplicationsDataType | grep "$app_name" -c)"
echo "$app_name count $count"
if [ $count -ge 1 ]
then
echo "$app_name is installed"
else
echo "$app_name is not installed"
exit 1
fi
exit 0
```

定义应用分配：

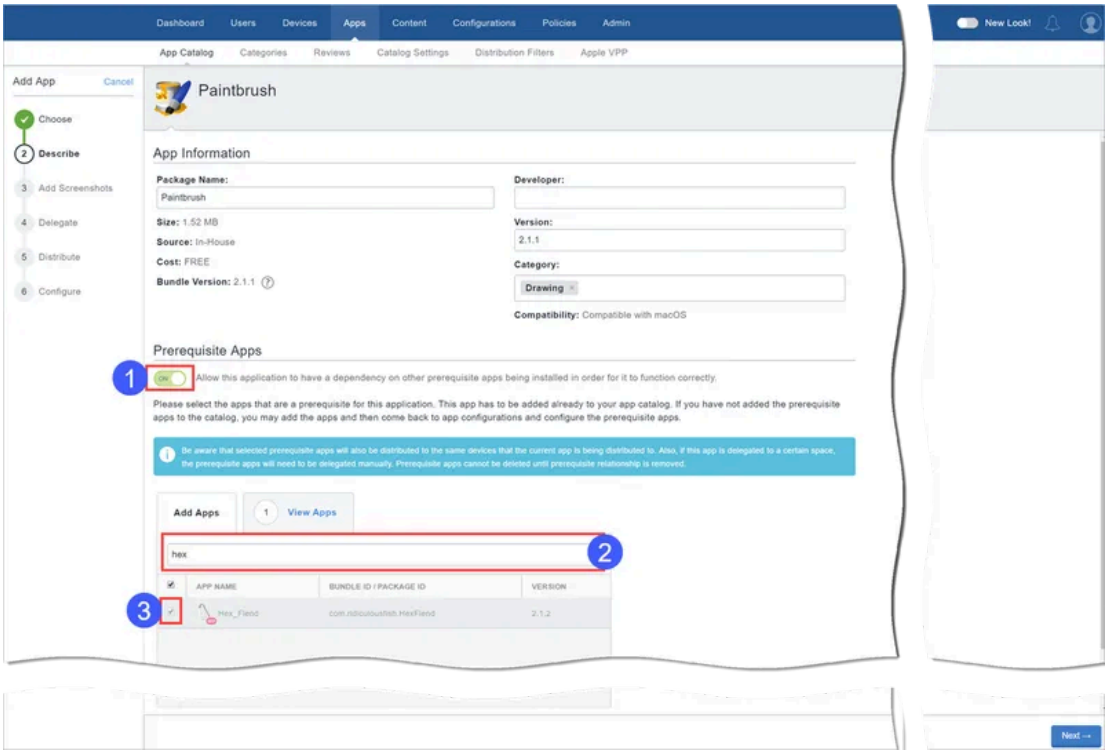
12. 选择升迁选项：
13. 选择分配选项。
14. 展开**高级选项与应用配置**部分。
15. 按照以下指导方针完成相关选项：
16. 单击**下一步**。

设置	流程
在设备上安装	选择此选项在注册后立即开始安装。 用户将看到提示，确认应用的安装，但出现以下情况时除外： • 此设备是受到监督的 iOS 设备。 • 此设备是 Samsung Knox 设备，已选中以下静默安装选项。
不在最终用户应用目录中显示	选择此选项，如果您不希望用户在设备的 App Catalog 中看到此应用。
设置应用安装优先级	选择“高”、“中”或“低”，设置在用户加入过程中应用安装的优先级。 用户登录期间仅安装高优先级应用程序。
在尝试失败一定次数后，暂停应用重新推送（仅 iOS）	使用以下设置，将切换开关切换为“打开”，以在失败重新推送尝试达到一定次数后，暂停应用重新推送： **停止重新推送后** - 输入重新推送尝试失败次数，然后应停止重新推送。 输入的值应介于 **1** 与 **999** 之间 **尝试失败并重试后** - 输入重新推送失败后重新执行重新推送操作所需的小时数。 输入的值应介于 **3** 至 **48** 小时之间。
（仅 Android）在 Samsung Knox 设备上进行静默安装	如果您不希望用户收到确认在 Samsung Knox 设备上安装的提示，选择此选项。
（仅 iOS 和 macOS）启用此应用的 Per-App VPN	选择此选项以使用该应用的 Per-App VPN 配置。 从下拉列表中选择要使用的 Per App VPN 配置。 对于 macOS，请仅选择 Tunnel Per App VPN 配置。
（仅 iOS）阻止备份到 iCloud 和 iTunes	选择此选项以阻止将同该应用相关的数据备份到 iCloud 和 iTunes 中。
（仅 iOS）在取消注册后，移除该应用	选择此选项，以当设备不再由 Ivanti Neurons for MDM 管理时移除此应用。
（仅 iOS）AppConnect 自定义配置	对于支持 AppConnect 的应用，输入指定自定义配置首选项的键和值。 请参阅应用文档，了解可用的键。
iOS 7+ 托管的应用设置	输入将此应用作为 iOS 7+ 托管的应用时为其定义的键和值。 请参阅应用文档，了解支持键的信息。

17. 单击**完成**。
    - 无特色
    - 特色列表
    - 横幅

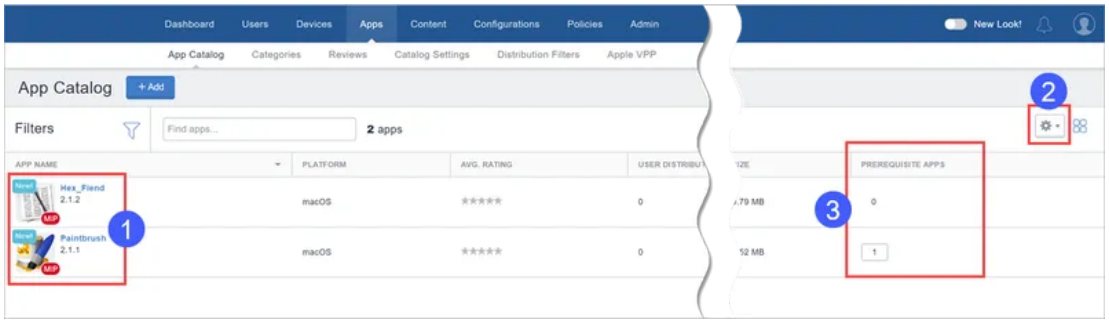
了解 Packager 内部 macOS 应用

在导入 Packager 内部 macOS 应用时，管理员可以启用 1 待搜索的必备应用功能 2，并选择 3，才可以安装必须在管理员导入之前安装到客户端的必备应用。



在导入后，Packager macOS 内部应用将显示在 App Catalog 中并显示MIP徽章1，如下所示。 然后，您可以使用列设置，2以添加必备应用列3，并快速查看带有依赖项的应用，即包含必备应用。

- 您可以搜索并将 MIP、非 MIP 和公共应用（App 和图书与 macOS App Store 公共应用）选为必备应用。
- 用户需要接受 App 和图书必备应用的 App 和图书许可证，才可以进行静默安装。
- 对于非 App 和图书公共必备应用，管理员需要明确分发公共应用，用户需要安装公共应用。 公共应用（App 和图书和非 App 和图书应用）需要导入 App Catalog，才可以显示在必备应用列表中。 来源列表示必备应用的类型。
- 对于安装具有非 MIP 必备应用的非 MIP 内部应用，将需要 MDM 签入。
- 用户需要手动安装公共非 App 和图书必备应用。
- 如果 App 和图书令牌移除或许可证用完，App 和图书应用选择为必备应用，因此不会安装主应用。 管理员需要遵循最佳实践，以提前通知用户这些任何 App 和图书应用的案例。



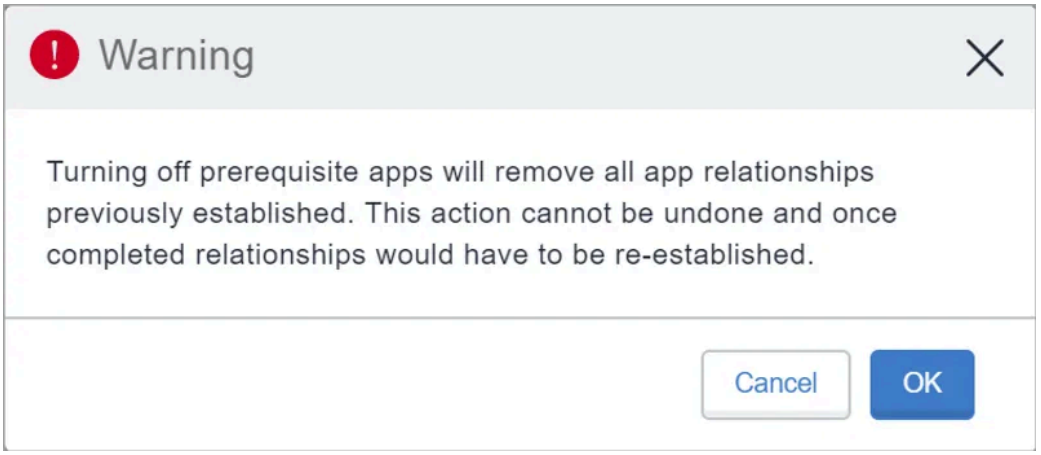
必备应用也可以作为独立应用提供，以便用户在明确分发时进行下载。 如果用户尝试卸载必备应用：

- 确保在下次设备签入时再次安装必备应用程序。
- 如果未在相同设备上安装依赖主应用，将卸载必备应用。
- 如果未明确分发必备应用，该必备应用将与主应用一起卸载。

- 如果必备应用已明确分发，该必备应用将保留在设备上。
- 如果必备应用包含依赖应用，该必备应用将保留在设备上。

关闭必备应用功能

在与具有依赖关系和必备应用的应用交互时，例如在更新、删除或委派此类应用时，您将看到系统提示，并指导您应用的依赖关系或必备状态如何影响您要执行的操作。 例如，在您尝试关闭应用的必备应用功能时，将显示以下提示：



- 如果您关闭应用的必备应用功能，将清除有关必备应用的详细信息。 这包含从子空间自动委派和取消委派必备应用。
- 在 Apps@Work 中，对于未在所含的客户端中安装必备应用的依赖应用，将不显示安装按钮。
- 在用户设备上，当用户尝试安装带有依赖项的内部应用时，将先安装必备应用（如果未安装），然后再安装主应用；这将需要几分钟时间。 系统将向用户显示依赖应用列表，以及安装状态。

从空间委派和取消委派必备应用

- 在主应用委派到子空间时，将自动委派绑定到应用（主应用）的必备应用。
- 如果主应用未从子空间委派，必备应用也将在未明确分发必备应用的情况下取消委派。 但与多个主应用绑定的必备应用并未取消委派。
- 如果必备应用已明确委派，将不会自动取消委派。

为 Android Enterprise 内部应用委派设备权限

可以将委派权限分配给可应用于 Android Enterprise 托管设备和 AMA 设备的内部应用程序。

步骤

1. 转至**应用 > 应用目录**。
2. 在 **App Catalog** 中，选择您想要委派设备权限的应用。
3. 单击**应用配置**选项卡。
4. 在委派权限（内部 Android Enterprise 应用程序）中，选择应用程序所需的权限：

> 只有 COSU 部署使用 AMAPI。 有关更多信息，请参阅 AMAPI 部分。

   - **配置第三方应用运行时权限**
   - **隐藏并暂停第三方应用**
   - **管理证书**

- **管理应用配置**
- **管理阻止应用卸载**
- **管理启用系统应用**
- **管理证书选择**（AMAPI 模式不支持）
- **管理保留卸载应用**（AMAPI 模式不支持）
- **管理网络日志收集**（一次仅支持在一个应用程序中使用）
- **管理安全日志收集**（一次仅支持在一个应用程序中使用）
- **管理安装现有应用**（AMAPI 模式不支持）
- **安装和移除软件包**（AMAPI 模式不支持）

安装和移除软件包选项在所有支持的 Android 设备所有者模式设备（7.0 或更高版本）上可用。 其他委派权限仅适用 Android 8.0 或更高版本。
配置分配选项，从**具有应用程序的所有人**、**没有人**或**自定义**中选择。

6. 单击**保存**。

显示 iOS 内部应用的配置文件状态

显示 iOS 内部应用的 App Catalog 页面上的配置文件状态。 配置文件名称旁边的工具提示会显示配置文件过期的天数。 在内部应用的配置文件即将过期时，此状态可用于检查。

该状态有助于对因配置文件过期而无法安装的应用进行故障排除。 如果没有适合的配置文件，应用虽然可以安装，但无法打开或启动。

步骤

1. 转至**应用 > 应用目录**。
2. 单击右上角的齿轮图标，以显示列。
3. 选择**配置文件**，以在 App Catalog 页面上显示应用列表的列。

配置文件详细信息也可在"配置文件设置"部分中的应用详细信息页面上可用。

更新 iOS 内部应用的预配配置文件

配置文件应用于特定的 iOS 内部应用。 可以在应用详细信息页面中找到应用的配置文件详细信息。 iOS 内部应用需要配置的配置文件（未过期），才能在设备上启动。 如果配置文件过期，您可以通过在应用详细信息页面上传配置文件来更新它。

步骤

1. 转至**应用 > 应用目录**。
2. 单击需要更新配置文件的应用。 将显示应用详细信息页面。
3. 单击**编辑**。
4. 在**配置文件**部分，单击**选择文件**。
5. 选择要上传的配置文件文件 (.mobileprovision file extension)，然后单击**保存**。

将内部应用部署到 Google Play

将内部应用上传到 Google Play Private 通道，然后将其导入 Ivanti Neurons for MDM，以便部署到启用 Android Enterprise 的设备。

步骤

1. 登录到 Goople 私有应用程序控制台：https://play.google.com/apps/publish。
2. 单击左侧菜单中的**所有应用**。
3. 单击**新建应用程序**，然后为该应用程序输入名称。
4. 单击**上传 APK**,以便上传您创建的 .apk 文件。
5. 单击**存储列表**：
   - 输入简短描述和完整描述。
   - 上传所有选项卡的截图。
   - 上传高分辨率图标。
   - 上传功能图形图标（graphic.png）
   - 为分类、联系人详情和隐私政策输入必要信息。
   - 完成应用程序的评价问卷。
6. 单击**定价和分发**。
   如果已经输入所有必要信息，“准备发布”将显示在页面顶部。
7. 转到 Ivanti Neurons for MDM 中的“应用”选项卡。
8. 单击**刷新可用类别**，以便同步您的私有应用程序。

> 发布应用可能需要几小时。

为 Android Enterprise 设备添加 Web 应用

Web 应用是指向任何网站的链接，作为快捷方式安装在设备上。 Web 应用的行为与任何其他应用的行为类似，这意味着 Web 应用可以按照与应用相同的标准进行分发。 它出现在 App Catalog 中，并可以由用户像任何其他应用程序一样安装。 但是，Web 应用只能有一个版本，并且不支持静默安装。 Web 应用使用 Web 剪辑并作为配置安装到设备上，但表现为应用。

在 App Catalog 中将 Web 剪辑设置为应用，以使 Web 应用在用户的 App Catalog 中可用。 Web 剪辑可以定义为配置，但配置只能由管理员分发。 用户可以选择在其设备上安装 Web 应用或退出，而用户无权选择退出 Web 剪辑配置。

在 Android Enterprise 中，Web 应用程序是一种嵌入式 Web 应用程序，在工作配置文件内的 Google Chrome 上运行。 它可以与 Android Enterprise 中的 VPN 或 SSO 解决方案相结合。 在创建 Web 应用后，应用的工作方式如同任何其他 Android 应用，您可以根据需要进行分发。 只有在公司拥有设备上的工作配置文件中安装 Chrome，Web 应用才可以运行。

> 如果使用此功能出现任何问题，管理员可以联系支持。

步骤

1. 转至**应用 > 应用目录**。
2. 单击 **+ 添加**。
3. 从下拉列表中选择 **Google Play**，在 Google Play Store 中搜索应用。 如果已注册 Android Enterprise，则会显示 Google Play iFrame。
4. 单击 **Web 应用程序**。
5. 描述用户应用：
   1. 应用标题或名称。
   2. 应用程序 URL。
   3. 显示 Web 应用的类型。

4. 上传图标，这可以是 512px 方形 PNG 或 JPEG 图像。

单击**创建**。 等待应用发布 iFrame。 这需要几分钟时间。 您可以将其关闭，并稍后返回。

7. 在发布 Web 应用后，将应用导入 App Catalog 进行分发。 单击 Web 应用图标。
8. 向下滚动，并单击**选择**。
9. 添加类别和可选描述。
10. 单击**下一步**。
11. 为应用程序授权选择以下选项之一：
    - 将该应用程序授权给所有空间。
    - 不要将该应用程序授权给所有空间。

单击**下一步**。

13. 为应用程序选择分配选项。
14. 单击**完成**。

在添加 Web 应用后，您可以随时根据需要编辑 Web 应用。 为此：

1. 在 **App Catalog** 页面上，单击现有 Web 应用的名称。
2. 单击**编辑**，以编辑 Web 应用字段。

为 iOS 设备添加 Web 应用

Web 应用是指向任何网站的链接，作为快捷方式安装在设备上。 Web 应用的行为与任何其他应用的行为类似，这意味着 Web 应用可以按照与应用相同的标准进行分发。 它出现在 App Catalog 中，并可以由用户像任何其他应用程序一样安装。 但是，Web 应用只能有一个版本，并且不支持静默安装。 Web 应用使用 Web 剪辑并作为配置安装到设备上，但表现为应用。

将 Web 剪辑设置为应用程序目录中的应用程序，方便用户通过应用程序目录使用该 Web 应用程序。 Web 剪辑可以定义为配置，但配置只能由管理员分发。 用户可以选择在其设备上安装 Web 应用或退出，而用户无权选择退出 Web 剪辑配置。

> 如果使用此功能出现任何问题，管理员可以联系支持。

步骤

1. 转至**应用 > 应用目录**。
2. 单击 **+ 添加**（左上角）。
3. 单击 **Web 应用**。
4. 描述用户应用：
    1. 应用程序名称。
    2. 应用程序 URL。
    3. 平台类型。
    4. 应用程序图标。
    5. 添加或移除类别。
    6. 全屏 - 选择以将 Web 应用显示为全屏应用。
    7. 可移除 - 选择以将 Web 应用移除。

8. 单击**下一步**。

为应用程序授权选择以下选项之一：

- 将该应用程序授权给所有空间。
- 不要将该应用程序授权给所有空间。

单击**下一步**。

7. 为应用程序选择分配选项。
8. 单击**完成**。

编辑 Web 应用

在添加 Web 应用后，您可以随时根据需要编辑 Web 应用。

步骤

1. 在 **App Catalog** 页面上，单击现有 Web 应用的名称。
2. 单击**编辑**，以编辑 Web 应用字段。

缓慢推出分发

缓慢推出分发设置让管理员可以自动逐渐向设备推出新版本的应用。 在推出应用的后续版本时，使用缓慢推出分发方法选项可用。 即使暂停缓慢推出，您也可以通过 Ivanti Neurons for MDM 管理门户编辑应用。

在为一个版本设置缓慢推出后，这也适用于与上次设置的百分比相同的后续版本。 如果分发设置为 100%，可以暂停分发应用。 但如果将分发目标设置为 100%，您必须手动设置下一个版本的分发目标百分比，这是因为 UI 会将百分比重置为 0%。

步骤

	1.	**转到 App Catalog、应用，选择其中一个分发模式选项。**
	2.	**选择在选择摘要中自定义设备百分比（缓慢推出）选项。**
	3.	**从缓慢推出设置中，拖动指定分发目标百分比中的滑块。**
	4.	**点击确认，然后点击完成。 已显示最新应用版本的状态。 App Catalog 页面在表格中显示缓慢推出状态。**

如果您无法在 **App Catalog** 页面上执行任务，这可能是您没有所需权限。 需要“应用和内容管理”角色。

使用高级搜索

可以使用“高级搜索”选项根据规则搜索应用程序，以识别和查看满足特定条件的应用程序。 可以使用适用的运算符来构建这些规则，包括“等同”、“小于”、“大于”、“等于”和“不等于”。 使用任意（或）或全部（且）选项，规则选项可以全部进行嵌套。 符合规则的应用程序会显示在该小节下方。

> 在搜索中使用的自定义属性值区分大小写。

步骤

1. 在“应用程序目录”页面中，点击**高级搜索**链接。 “高级搜索”向导打开。
2. 点击下列选项之一：
   - 如果应用程序必须与至少一个规则相匹配，则选择**任意**
   - 如果应用程序必须匹配所有规则，则选择**所有**

要创建定义搜索条件的规则，请选择以下选项之一并选择适当的关联操作：

   - AppConnect 已启用
   - 平均评分
   - 捆绑包 ID
   - 类别
   - 成本
   - 自定义属性
   - 添加到 AppCatalog 的日期
   - 修改日期
   - 设备分发
   - 设备组分发
   - 设备类型
   - 组分发
   - 最低操作系统版本
   - 名称
   - 操作系统平台
   - 设置配置文件
   - 大小
   - 来源
   - 用户分发
   - 用户组名称
   - 版本
4. （可选）点击 **+** 可创建其他规则。
5. 单击**搜索**。 将显示匹配搜索条件的应用程序列表。

加载搜索查询

可以查看已保存的搜索查询的列表。

步骤

1. 点击“高级搜索”，然后点击文件夹图标。 **已加载查询**部分会显示已创建的搜索查询的列表，此外还会显示下列详细信息：
   - **查询名称** - 已加载查询的名称。
   - **查询内容** - 根据定义搜索查询的规则，显示内容。

- **操作** - 选择对查询执行的操作。

2. 点击**操作**列中的**加载查询**，可查看与已加载查询中定义的条件相匹配的应用程序列表。
3. 点击**删除**可删除加载的查询。

将应用程序导出到 CSV 文件

您可以使用应用程序目录页面中的“导出到 CSV”选项导出应用程序。

步骤

1. 前往**应用程序** > **应用程序目录**。
2. 点击**导出到 CSV**可将应用程序列表和相关详细信息导出到 CSV 文件。

> 仅包括所选空间中列出的应用，所有分页结果都汇编到单个文件中。

> 使用筛选器或搜索功能得到的结果将仅导出相关的应用程序。

3. 将显示带有**继续**和**取消**按钮的弹出消息，表明导出过程已开始，并且很快就会生成报告。
4. 点击**继续**并等待请求完成后再提交另一个请求。
5. 系统将显示一条消息，指明**应用程序目录 - CSV 报告已完成**，并提供**下载**和**删除**按钮。
6. 点击**下载**以下载报告。
7. （可选）点击**删除**可以删除报告。

> 只有在选择**下载**或**删除**选项后，**导出到 CSV** 选项才会重新启用。

> 如果应用程序有多个版本，则每个应用程序版本都会显示一个条目。

相关主题

- 用户角色
- 从 App Catalog 中删除应用
- 部署应用依赖性

8.2. 声明式设备管理 (DDM) 应用程序管理

概述

声明式设备管理 (DDM) 应用程序管理引入了对 Apple 声明式管理框架的支持，以便在 iOS 和 iPadOS 设备上进行应用程序部署和生命周期管理。 DDM 不依赖于连续命令交付和周期性拉取，而是允许设备在本地应用声明并主动报告状态更改。

使用 DDM，服务器仅向设备发送一次声明。 然后，设备应用配置，监控其状态，并向服务器报告状态更改。 这种设备驱动的方法可减少服务器通信，提高可扩展性，并为应用程序部署提供更及时的状态更新。

DDM 应用程序管理目前专注于支持的 Apple 设备的核心应用程序管理功能。

DDM 应用程序管理工作流程

在 DDM 工作流程中，服务器向设备提供所需的状态，设备负责维护和报告该状态。

将应用程序分配给启用 DDM 的设备时：

1. 服务器向设备发送应用程序声明。
2. 设备在本地处理声明。
3. 设备根据分配的配置安装、更新或维护应用程序。
4. 设备持续监控应用程序状态。
5. 任何安装状态或状态更改都会立即报告回服务器。

此声明式模型可近乎实时地查看应用程序部署进度，而无需定期提取状态。

启用 DDM 应用程序管理

DDM 应用程序管理通过用户设置启用，并分配给特定用户组。

启用 DDM 应用程序管理：

1. 转到**用户** > **用户设置**。
2. 在 **Apple DDM 设置**下，单击特定用户组的 **+添加**设置。 这时将打开 **Apple DDM 设置**页面。
3. 输入名称并切换**启用 DDM 应用程序管理**滑块。
4. 单击**下一步**。 **用户设置分发**页面随即打开。
5. 选择将使用 DDM 应用程序管理的用户组。
6. 单击**完成**。

为用户组启用 DDM 后，通过 DDM 应用程序管理处理分配给该组中用户的所有受支持应用程序。 DDM 配置是租户范围的，但通过用户组分配来应用，使组织能够逐渐向所选用户或组推出 DDM。

支持的注册方法

DDM 应用程序管理支持使用以下方式注册 iOS / iPadOS 设备：

- iReg/托管的 Ivanti Go 客户端
- 设备注册配置文件 (DEP)
- 账户驱动的设备注册

支持的应用程序类型

DDM 应用程序管理支持以下应用程序类型：

- 公共应用程序
- VPP 应用程序（仅适用于设备注册）
- 内部应用程序。

应用程序分配和部署工作流程与传统的 N-MDM 部署基本相同。 现有的应用程序分发流程继续有效，同时受益于 DDM 增强状态报告功能。

8.2.1. DDM 应用程序管理设置

通常，应用程序管理包括以下设置：

- 防止备份到 iCloud
- 请勿在新注册的设备上安装应用程序
- 蜂窝 5G
- DNS 代理
- 托管应用程序配置
- 业务应用程序 – Apps@Work、Email+ 等
- 每个应用程序 VPN
- 网络中继
- Webcontent 筛选器
- 允许 Appstore 更新

除了上面列出的设置外，DDM 应用程序管理还引入了几个功能，这些功能仅适用于 DDM 管理的设备。

应用程序版本固定

应用程序版本固定允许管理员跨 DDM 托管设备部署和维护特定应用程序版本。

启用版本固定时：

- 设备安装指定的应用程序版本。
- 禁止自动升级到较新版本。
- 在管理员明确选择新版本之前，应用程序会保留在分配的版本上。

此功能可以更严格地控制应用程序版本一致性和分阶段升级部署。

步骤

1. 前往**应用程序** > **应用程序目录**。
2. 单击显示列表中的应用程序。 **应用程序详细信息**页面随即打开。
3. 在**应用程序配置**选项卡下，单击 **Apple 应用程序设置**。
4. 单击列出的任何现有设置。
5. 单击**编辑**。
6. 在**将应用程序版本固定到设备**部分下，选择**固定应用程序版本**选项。
7. 从**选择应用程序版本**列表中，选择所需的应用程序版本。

> 如果设备具有应用程序的现有版本，则无法将其替换为旧版本。

8. 单击**更新**。

自动 App Store 更新控件（自动应用程序更新）

管理员可以配置如何为托管应用程序处理 App Store 更新。 此功能可更好地控制应用程序更新行为，并帮助组织将更新与内部验证和推出流程保持一致。

允许通过移动电话网络下载

DDM 引入专用设置，以控制通过移动电话网络进行的应用程序下载和更新。

程序

1. 前往**应用程序** > **应用程序目录**。
2. 单击显示列表中的应用程序。 **应用程序详细信息**页面随即打开。
3. 在**应用程序配置**选项卡下，单击**在设备上安装**。
4. 单击列出的任何现有设置。
5. 单击**编辑**。
6. 在**允许通过移动电话下载**部分下，选择以下选项之一：
    - **存储设置** – 默认选项。 下载应用程序时，设备会使用相应商店的设置。
    - **始终开启** – 即使设备没有 Wi-Fi 连接，也允许下载应用程序。
    - **始终关闭** – 如果设备没有 Wi-Fi 连接，则不允许下载应用程序。
7. 单击**更新**。

应用程序安装工作流程

分发应用程序的流程与传统的 N-MDM 应用程序管理流程保持相似。

管理员可以：

- 分配应用程序
- 分发应用程序
- 安装应用程序

但是，DDM 会更改部署状态的通信方式。 设备不会依赖服务器拉取，而是在操作完成后立即报告应用程序状态更改。 这提供了有关安装进度和部署结果的更准确和更及时的信息。

状态报告和监控

DDM 应用程序管理的主要优势之一是主动状态报告。

对于 DDM：

- 设备在本地监控应用程序状态。
- 立即检测安装和更新事件。
- 状态更改会自动报告给服务器。
- 部署信息变为可用，无需等待计划的轮询间隔。

这为管理员提供了更快的可见性：

- 应用程序安装进度
- 成功安装

- 应用程序更新完成
- 应用程序状态更改
- 部署失败

实时报告可改善故障排除，并提供响应更快的应用程序管理体验。

要求

DDM 应用程序管理仅在以下情况下受支持：

- iOS 26 或更高版本
- iPadOS 26 或更高版本
- 托管 Ivanti Go 客户端 126 或更高版本

不符合这些要求的设备继续使用传统的 N-MDM 应用程序管理。

> 通过 DDM 应用程序管理处理设备后，禁用或更新此策略分发不会将设备还原到 MDM 应用程序管理。 要将设备返回到 MDM 应用程序管理，请删除策略分配并重新注册设备。

8.3. Apps@Work（iOS、Android、Windows 和 macOS）

Apps@Work 是企业应用店面，协助软件和应用的安全分发。 Apps@work 适用于 iOS、Android、macOS 和 Windows 设备。 Apps@Work 企业应用商店集成在 Ivanti Go app 以及 iOS 版、Android 版和 macOS 版 Mobile@Work 客户端中。 对于 Windows 设备，这是一款本地独立应用。 本部分包含以下主题：

- iOS Apps@Work
- Android Apps@Work
- macOS Apps@Work
- Windows Apps@Work

iOS Apps@Work

Apps@work 本地应用商店会与 Go 客户端一起自动部署。 无需管理员进行任何操作。 Apps@work 选项卡会显示在 Go 客户端的任务栏上。 最终用户可以进入此选项卡，查看和安装其公司批准的应用。 有关详细信息，请参阅 iOS Apps@Work AppStore 功能。

默认情况下启用针对应用更新的 iOS Apps@Work 最终用户通知。 如果要更改设置，请参阅目录设置中的**通知**主题。

使用 iOS Apps@Work Webclip 的现有客户

部署了旧版 iOS Apps@Work webclip 的客户将不会默认获得本地集成的 AppCatalog。 如果要过渡到 iOS Apps@Work 本地目录，并从设备中删除 Apps@work webclip，请执行以下步骤：

推送配置

管理员必须向设备推送“适用于本地客户端的 App Catalog”配置，以使用户可以通过 Go 客户端应用在本地 Appstore 中获得 Apps@Work。 有关详细信息，请参阅使用配置。

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 转到**配置** > 筛选器，选择**客户端服务**。 随后会列出所有客户端配置。
3. 选择**适用于本地客户端的 App Catalog**。 系统将打开“适用于本地客户端的 App Catalog”配置页面。
4. 点击**编辑分发**图标。 将打开“编辑分发”页面。
5. 选择下列选项之一：
    - **所有设备**
    - **无设备** - 如果您不想分发给任何设备
    - **自定义** - 可选择设备、设备组、用户、用户组
6. 分发配置后，用户必须将 Go 客户端版本升级到 83 或更高版本。 Apps@Work 选项卡现已在 Go app 客户端中可见。

> 无法为使用 iReg 注册的设备推送配置，因为设备上没有 Go 客户端。 必须安装 Go app 客户端才能获得本地应用目录。 有关详细信息，请参阅设备注册（iOS、macOS 和 Android）。

移除 iOS Apps@Work Webclip

对于其设备已获分发 Apps@Work Webclip 且已经迁移到 Apps@Work 本地体验的客户，他们可以移除 iOS Apps@Work webclip。

步骤

1. 转至**配置**。
2. 筛选配置 – **Apple App Catalog**。
3. 点击**编辑**。
4. 从**分发**中选择**不分发给任何设备**。
5. 点击**保存**。

Android Apps@Work

Apps@work 本地应用商店会与 MI Go 客户端一起自动部署。 无需管理员进行任何操作。 Apps@work 选项卡会显示在 Mi Go 客户端的任务栏上。 最终用户可以进入此选项卡，查看和安装其公司批准的应用。 有关详细信息，请参阅**管理员 - Android Enterprise**。

macOS Apps@Work

macOs Apps@work 集成在 macOS Mobile@Work 客户端中。 设备在 Ivanti Neurons for MDM 中注册后，客户端会切换并显示为 Apps@Work。 对于新创建的租户，Apple App Catalog Webclip 配置将不会推送到 macOS 设备。 如果需要，管理员可以向 macOS 设备分发 Apps@work Webclip 配置。 有关详细信息，请参阅**配置 macOS 设备**。

分发 macOS 应用

- Ivanti 通过 Apple 的 MDM 协议并使用 Mobile@Work 应用支持 macOS 应用分发。 管理员可以选择使用以下其中一种或两种方法：
  - Apple 的 MDM 协议 - 管理员仅可将特定 PKG 格式（分发格式）作为内部应用上传，并且也可以从 Mac App Store 分发应用（包含 Apple 的 Apps 和图书许可支持）。 但此方法不允许管理员分发 DMG 和其他 PKG 格式。
  - Mobile@Work for macOS 应用 - 作为一种向用户分发应用的方式，管理员可以使用 MobileIron Packager (MIP) 应用，以将任何 PKG、DMG 或 .app 文件转换为 MIP 文件。 将 MIP 文件作为内部应用程序上传到 Ivanti Neurons for MDM

可以从**软件下载网站**下载实用程序。

- 管理员可以使用 Mobile@Work，以分发格式为 DMG、PKG 或 .app 的内部应用。 对于仅在 Mac App Store 中提供的应用，管理员可以继续使用 Apple 的本地 MDM 功能，其中包含 Apple App 和图书许可证功能。 有关详细信息，请参阅**配置 macOS 设备**。

Windows Apps@Work

Apps@Work 是一款独立本地应用，可以从 Microsoft Store 下载，也可以直接从 Ivanti Neurons for MDM 推送。 它支持在 Ivanti Neurons for MDM 中的 Windows 10+ 设备上使用 Windows 公共和内部应用。 Apps@Work 在支持的 Windows 10+ 设备上静默安装。

有关详细信息，请参阅**应用配置**。

使用 Windows Apps@Work

Apps@Work 支持在 Ivanti Neurons for MDM 中的 Windows 10 设备上使用 Windows 公共和内部应用程序。 Apps@Work 在支持的 Windows 10 设备上静默安装。

Apps@Work 证书身份验证

要使用 Windows Apps@Work 的证书身份验证功能：

1. 前往 **管理员 > Windows > Apps@Work 证书身份验证**
2. 将设置切换为**打开**。

> 将设置切换为**关闭**，强制使用用户名和密码。

> Apps@Work for Windows 不支持 SAML。

要为 Apps@Work 配置应用：

1. 选择 Windows 应用。
2. 单击**应用配置**选项卡。
3. 点击**在设备上安装**。
   Windows 内部应用配置可设置为静默安装标志，或使用 Apps@Work 安装。 公共应用不能设置为静默安装。
4. 或者，选择在 Apps@Work 目录中显示或隐藏应用。
   该选项仅适用于内部应用。
5. 点击**推广**选项卡。

> Apps@Work 当前不支持横幅推广，因此可用的选项为：**特别推荐**和**未特别推荐**。
>
> 对于公共应用，仅显示**促销**选项。

8.4. iOS Apps@Work AppStore 功能

Apps@Work 选项卡具有以下功能：

- 从 Go 应用访问 Apps@Work 选项卡
- 搜索
- 安装应用 - 按钮状态
- 特别推荐应用和横幅
- 应用更新通知
- 设置 - 我的设备

从 Go 应用访问 Apps@Work 选项卡

步骤

1. 从 iOS 设备登录 Go app。
2. 点击 **Apps@Work** 图标。 有两个默认选项卡 –“所有应用”和“类别”。

3. 点击**所有应用**选项卡。 “所有应用”选项卡按字母顺序列出所有应用。
4. 点击**类别**选项卡。 “类别”选项卡将仅显示其中有应用的类别，如下所示：
    - 每个类别都会显示其中包含的应用数量。
    - “类别”选项卡下的 MyApps 行是包含所有已安装应用的列表项。 MyApps 行将始终是第一个类别，其余类别按字母顺序排列。
    - 如果没有安装应用，MyApps 列表将显示“无”。
    - 点击某个类别时，特定于该类别的所有应用都会列出，且显示“安装”选项。 点击**安装**分别安装每个应用，或者也可以点击**安装所有**安装该类别中的所有应用。 系统会提示您允许安装每个应用。

搜索

步骤

1. 从 iOS 设备登录 Go app。
2. 点击 **Apps@Work** 图标。
3. 点击搜索（镜片）图标搜索以下项：
    - **新版本** - 搜索栏中没有输入任何文本时，就会显示新版本的应用列表

    - 输入任何文本，然后搜索字段会动态预测和显示匹配的应用。
    - 搜索结果计数显示为子标题
    - 可以点击**安装**按钮安装应用，无需导航到详细信息页面。


安装应用 - 按钮状态

由于应用安装需要服务器处理请求，并将应用推送到设备，“安装”按钮将不会实时显示进度。 “安装”按钮的状态变化顺序：安装 > 已请求 > 已安装。

步骤

1. 从 iOS 设备登录 Go app。
2. 点击 **Apps@Work** 图标。
3. 点击**安装**，状态通知显示如下：
    - 系统首次显示警报消息，表明已请求安装。
    - 点击“已请求”按钮。 随即显示警报消息。

        > “已安装”状态不是按钮。



特别推荐应用和横幅

根据管理推送的配置，“特别推荐”选项卡可见。 没有更新可用时，“特别推荐”选项卡即为默认登录页面。



步骤

1. 从 iOS 设备登录 Go app。
2. 点击 **Apps@Work** 图标。
3. 点击**特别推荐**选项卡。
    - “特别推荐应用”横幅在横幅中显示一个应用。
    - “特别推荐应用”包含所有特别推荐应用的列表。



应用更新通知

有任何可用的应用更新时，最终用户会在设备上收到通知。 通知中包含有更新可用的应用数量。 用户点击通知后，Apps@Work 将打开。

步骤

1. 从 iOS 设备登录 Go app。 Apps@Work 图标将显示有待处理更新的应用数量。
2. 点击应用更新通知后，将重定向至 Apps@Work 中的“所有应用”选项卡。 将显示以下指示：
    - “所有应用”选项卡下的“可用更新”子部分将显示可进行更新的应用数量。
    - 每个需要更新的应用都将显示红点图标。



设置 - 我的设备

步骤

1. 从 iOS 设备登录 Go app。
2. 点击**设置**图标。
    - “设置”下方会显示“我的设备”选项卡。
    - “我的设备”现已列为“身份验证”下的行项目。

8.5. iOS Go 高级功能

键值对 (KVP) 是由键（设置的名称）和值（要应用的配置）组成的简单应用程序设置。 在 Ivanti Go for iOS 中，组织使用 KVP 启用或禁用功能，并调整应用程序行为，无需更新应用程序。

当 Ivanti Go 在组织管理的 iPhone 或 iPad 上运行时，它会在启动时或签入期间读取这些 KVP 设置。 应用程序会立即应用更新，确保配置更改快速、一致地交付给正确的用户。

在 Ivanti Go 应用程序配置中使用 KVP

Ivanti Go 应用程序支持用于自定义违规消息的 KVP。 您可以在 Ivanti Go 应用程序设置中配置 KVP 以自定义应用程序。

程序

1. 在 AppCatalog 中打开 **Ivanti Go 应用程序**。
2. 选择**配置**。
3. 单击**添加**以创建新的 **Apple 应用程序配置**。
4. 手动添加 KVP：
    - 在**密钥**列中，输入要自定义的配置密钥。
    - 在**值**列中，输入要在设备上强制使用的值。
5. （可选）上传包含要应用的预定义 KVP 的现有 *.plist* 文件。
6. **保存**配置。
7. 更新后的 KVP 将在下次签入期间应用于设备。

将 plist 添加到特定的 iOS 应用程序（用于多个键值对）

管理员可以使用应用程序序列号、捆绑标识符、版本详细信息或其他元数据为 iOS 应用程序配置多个键值对 (KVP)。 这可以通过经由 Ivanti Neurons for MDM 控制台上传 .plist 文件来高效完成。

程序

1. 转至**应用** 。
2. 打开**应用程序目录**。
3. 选择并打开要配置的**特定 iOS 应用程序**。
4. 转到应用程序配置选项卡。
5. 选择 **Apple 托管应用程序配置**。
6. 单击**添加按钮**。
7. 为您的配置输入**名称**。
8. 单击**使用 .plist**。
9. 选中**选择这些选项之一**。
10. 浏览至您的 plist 文件，选择它，然后单击**打开**。 系统将自动使用 plist 中的键值对填充配置表。
11. 选择应接收配置的用户组或设备组。
12. 单击**分发此应用程序配置**。

13. 单击**保存**以完成该过程。

> 上传的文件必须具有 .plist 扩展名。 如果手动创建文件（例如，在文本编辑器中），请确保在上传之前将扩展名从 *.txt* 更改为 *.plist*。

在注册期间以单一应用程序模式启动 Ivanti Go

此功能使管理员能够在设备注册期间使用键值对，以在单一应用程序模式 (SAM) 下自动启动 Ivanti Go for iOS。 设备开始注册时，配置的键值对会触发 Ivanti Go 立即打开。 在此过程中，将向用户显示一条消息：

正在配置设备，请稍候。

要激活此行为，必须在注册工作流程之前或期间安装单应用程序模式配置，并明确针对 Ivanti Go for iOS。 成功完成注册后，将自动退出单一应用程序模式。 然后，设备将发布给最终用户以进行正常操作，确保安全设置，而不会限制注册后使用。

此功能支持 Ivanti Mobile@Work 环境，为受监督的 iOS 设备提供安全的注册流程。

设置 Zero Touch 激活

要为 Ivanti Go 启用 Zero Touch 激活，请完成以下步骤：

1. 设置仅包含 *Client Registered = No* 的设备的组。
2. 为 Ivanti Go 应用程序创建单一应用程序模式 (SAM) 配置。 仅将此配置分配给*步骤 1*中创建的设备组。
3. 将 zero_touch_activation 键值对 (KVP) 添加到 Ivanti Go 应用程序配置。 以之前步骤中使用的相同设备组为目标。

KVP 配置

密钥	价值	类型	说明
zero_touch_activation	True	布尔值	当值设置为 true 时，Ivanti Go 应用程序通过 SAM 配置识别它正在单应用程序模式 (SAM) 下运行。 SAM 配置启动 Ivanti Go 应用程序，而此值用作附加设置，使应用程序能够在 SAM 模式下正常运行。 成功注册后，设备将退出单一应用程序模式，并可供最终用户正常使用。

在 Ivanti Go 中启用恢复按钮 (iOS 18+)

恢复服务功能允许设备在擦除数据后自动重新注册，从而减少在擦除后手动重新注册设备的需求。

管理员可以使用可配置的键值对 (KVP) 启用或禁用“恢复服务”按钮。 当 KVP 作为应用程序配置的一部分部署到 Ivanti Go 时：

- 恢复服务选项对最终用户可见。
- 用户可直接从 Ivanti Go 启动重置过程。
- 设备执行 Apple 托管恢复服务重置。
- 管理配置文件和所需应用程序保持不变。
- 设备完成其重新配置流程，并准备好供重新使用。

在 DEP 模式中注册的 Ivanti Go for iOS、iOS 18 和更高版本设备上支持此功能。

KVP 配置

将以下 KVP 添加到 Ivanti Neurons for MDM 中的 Ivanti Go 托管应用程序配置：

密钥	价值	说明
ReturnToServiceEnabled	true	启用 Ivanti Go 中的**恢复服务**按钮。 设置为 false 或省略时，该功能将保持隐藏状态。

在 SAML 身份验证屏幕上禁用屏幕截图保护

Ivanti Go for iOS 包含内置屏幕截图保护，以在设备注册期间增强安全性。 默认情况下，使用 SAML 身份验证注册屏幕会阻止：

- 屏幕截图
- 屏幕录制
- 屏幕共享

此保护可确保在未经授权的情况下无法捕获或共享敏感的身份验证数据 - 例如用户名、密码和基于 SAML 的登录内容。

管理员可以使用 KVP 配置禁用托管设备上的屏幕截图保护。 应用此配置后，Ivanti Go 应用程序将仅在 SAML 身份验证屏幕上允许屏幕截图和录制，同时在整个应用程序维持所有其他安全机制。

KVP 配置

要禁用 SAML 身份验证屏幕的屏幕截图保护，请将以下 KVP 应用于 MDM 中的 Ivanti Go 应用程序配置：

密钥	价值	说明
SCREENSHOT_PROTECTION_DISABLED	True	在 SAML 身份验证屏幕上禁用屏幕截图、屏幕录制和屏幕共享保护。 省略或设置为 False 时，默认情况下仍会启用保护。

用于自定义违反策略消息的 KVP

这些 KVP 使管理员能够自定义检测到违反策略时发送给最终用户的消息。

这些用于自定义的 KVP 描述了管理员可用于自定义 Ivanti Go for iOS 应用程序行为的 KVP 和违规类型。 这些 KVP 定义了应用程序行为，例如向设备用户提供详细通知，以及从 Ivanti Go for iOS 导出联系人。

违规类型不是相互排斥的。 如果存在一组违规，则 Ivanti Go for iOS 中将显示消息列表。

键值对 (KVP)	默认消息
compliance.message.COMPROMISED	• 您的设备因被越狱而遭到破坏。 请正确地将您的设备恢复到非越狱状态，或联系您的管理员以帮助您解决此问题。
compliance.message.DATA_PROTECTION_DISABLED	• 已禁用企业访问以进行数据保护。 请联系您的管理员，以帮助您解决此问题。
compliance.message.OUT_OF_CONTACT	• 您的 iOS 设备失去联系。 请联系您的管理员，以帮助您解决此问题。
compliance.message.APPS	• 您的设备缺少所需的应用程序和/或存在受禁的应用程序。 请添加/删除必要的应用程序，或联系管理员，以帮助您解决此问题。
compliance.message.MDM_DISABLED	• 您的设备不合规，因为 MDM 功能已停用。 请重新注册您的设备，或联系管理员以帮助您解决此问题。
compliance.message.ROAMING	
compliance.message.generic	• 由于未指明的原因，公司访问已被禁用。 请联系您的管理员，以帮助您解决此问题。
compliance.message.header	由于以下原因，您的设备不合规： 当违规类型为“自定义”或“自定义通知”时，系统会显示没有标题的独立消息。
compliance.message.CUSTOM	可能需要在您的设备上执行操作。 请根据需要联系您的管理员。
compliance.message.CUSTOM_NOTIFY_ONLY	您的设备不合规，并且已发送通知。 有关详细信息，请参阅通知选项卡或电子邮件。

如果违规类型列表不包括任何带有映射消息的违规，但至少包括一个没有映射消息的违反，则显示默认消息：

- 由于未指明的原因，公司访问已被禁用。 请联系您的管理员，以帮助您解决此问题。

如果消息列表至少包含一条违规消息，请在列表上方显示以下标题：
由于以下原因，您的设备不合规：

如果不想更改默认消息，请不要对其加入键值对 (KVP)。 仅定义要修改的消息的 KVP。

使用托管应用程序配置来配置默认浏览器和电子邮件客户端

键值对 (KVP) 使管理员能够配置 **Ivanti Go** 在打开 web 链接和通过托管应用程序配置撰写电子邮件 时使用的浏览器和电子邮件客户端。

作为管理员，您可以使用托管应用配置 KVP 来控制在**支持**选项卡中处理链接的方式：

密钥	值	类型	说明
default_browser	safari, edge, chrome, firefox, brave, opera, webatwork, duckduckgo	字符串	Browser Ivanti Go 用于在“支持”选项卡中打开 web 链接。 http/https 链接被重定向到配置的浏览器方案。 **如果未配置，则为默认设置**：系统默认浏览器。
Allow_browser_fallback	true、false	布尔值	**未安装默认浏览器时的行为**： **True**：回退至默认系统浏览器。 **False**：链接未打开，用户看到“<Browser> 未安装”警报。 **如果未配置，则为默认设置**：True
restrict_log_sharing_to_email	true、false	布尔值	日志/支持共享是否仅限于电子邮件（使用默认电子邮件）。 自动附加日志适用于 Email+ 和原生邮件 与 **allow_email_fallback** 配合使用。 **True**：仅共享到电子邮件。 **False**：标准共享选项可用。 **如果未配置，则为默认设置**：false。
default_email	nativemail, outlook, gmail, yahoo, citrixmail.emailplus, spark, protonmail	字符串	电子邮件客户端 Ivanti Go 用于从支持选项卡中的 mailto 链接撰写邮件。 mailto 转换为客户端的撰写 URL **如果未配置，则为默认设置**：默认邮件应用程序。 未安装默认电子邮件客户端时，链接解析和日志共享中的双重角色。
Allow_email_fallback	True、False	布尔值	**未安装默认电子邮件时的行为**。 **True**：如果未安装配置的电子邮件客户端，电子邮件组成会回退到默认邮件应用程序，并且日志共享可以使用其他交付方法。 **False**：如果配置的电子邮件客户端不可用，电子邮件组成被阻止，用户看到“**未安装**”的警报。 日志共享限制在没有还原选项的情况下被强制执行。 **如果未配置，则为默认设置**：true。 （回退行为已启用）

8.6. 查看应用详细信息

您可以从 App Catalog 深入了解目录中任何应用的应用详细信息。 在应用详细信息页面上，显示关于应用的详细信息，例如显示版本（例如 1.5.0）、捆绑版本（例如 1.5.0.42）和所需的最低 OS 版本（例如适用于 Android 的 5.0）。

对于不符合所需最低 OS 版本中指定版本的应用，Apps@Work 目录将不会显示。 因此，无法将此类应用分发到设备。 所需最低 OS 版本字段也会显示为应用的审计线索的一部分。

步骤

1. 单击**应用**。
2. 单击**应用目录**。
3. 选择应用。

“应用程序详细信息”窗口随即出现。

> 对于 iOS 内部应用程序，可以在应用程序详细信息页面查看**设置配置文件到期日期**。

> 应用信息显示**在分发时允许在 M1 设备上安装应用**作为所有 iOS 和 iPadOS VPP 应用的选项。 对于可安装到 M1 macOS 设备的 iOS 或 iPad VPP 应用，管理员必须仅为其启用选项**在分发时允许在 M1 设备上安装应用**。 只有在启用此选项后，管理员才可以在应用安装过程中看到 M1 macOS 设备。 M1 Mac 设备上的 iOS VPP 应用程序支持托管应用配置。

> 对于 iOS 和 macOS App Store 应用程序，包括企业对企业，**同步新版本**检查并从 App Store 同步应用程序更新。 根据应用程序同步计划，更新的应用程序版本将在 12 至 24 小时内显示。

> 设备详细信息增加**必备应用**的切换按钮。 管理员可以选择此选项，并将应用添加为主应用的必备应用。

将应用程序分发到不同设备后，可以在**设备摘要**选项卡下查看应用程序分发状态。 “设备摘要”选项卡还包含有关符合条件的设备数量、已安装应用程序的设备数量、待安装应用程序的设备数量以及应用程序安装失败的设备数量的信息。 这些框中的设备计数基于具有所需应用程序安装的设备，因此管理员可以跟踪必要应用程序的初始部署情况。

对于一般应用程序计数（包括用户安装的应用程序），请使用“应用程序清单”搜索。

> 从设备中排除的应用程序具有“待处理”分发状态。

下表列出了 iOS/OSX 应用程序安装失败的原因：

原因	说明
AppAlreadyInstalled	“应用程序已安装。”
AppStoreDisabled	“应用程序商店已禁用。”
CouldNotVerifyAppID	“无法验证应用程序 ID。”
失败	“应用程序安装失败，发生未知错误。”
ManagedButUninstalled	“应用程序受到管理，但已被用户删除。 当应用程序再次安装时（即使是由用户安装），它将再次受到管理。”
ManagementRejected	“用户拒绝将非托管应用程序转换为托管应用程序。”
NotAnApp	“由于无效的应用程序标识符解析为资产而非应用程序，因此 InstallApplication 命令被拒绝。”
NotSupported	“应用程序不受支持。”
Other	“新添加错误的原因。”
PurchaseMethodNotSupported	“对于 iOS 7 及更高版本，由于购买方式无效（仅适用于 VPP 应用程序）而无法安装应用程序。”
UserInstalledApp	“用户已在执行托管应用程序安装之前安装该应用程序。”
UserRejected	“用户已拒绝安装应用程序的建议。”
UpdateRejected	“用户已拒绝更新应用程序的建议。”

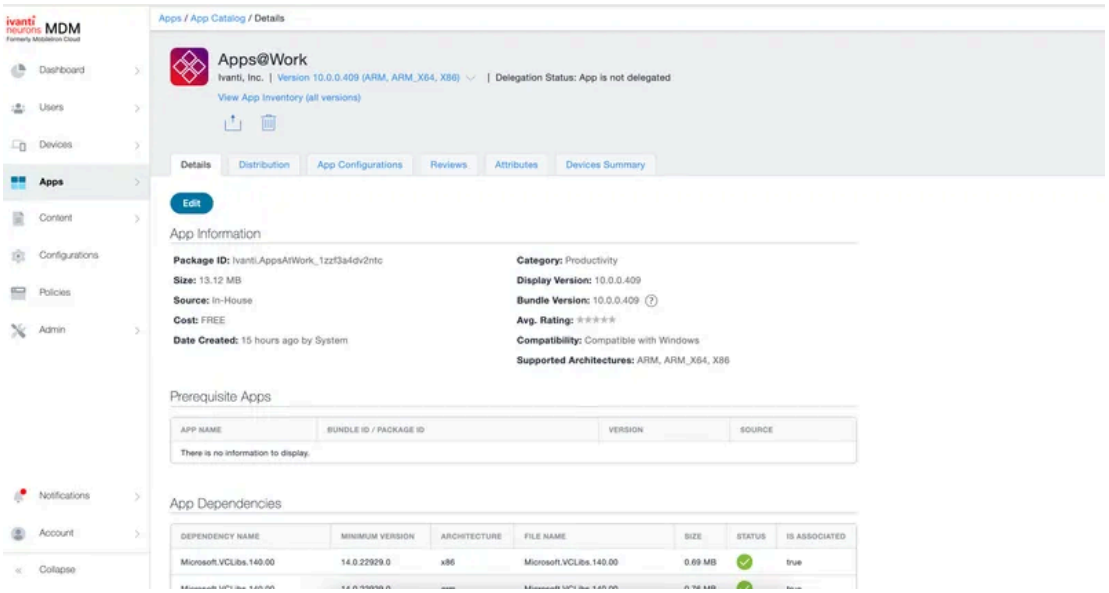
下表列出了 Android 应用程序安装失败的原因：

原因	说明
USER_INSTALLED	“已安装在设备上（MDM 之外）。”
UNSUPPORTED	“不受支持”
USER_REJECTED_INSTALL	“用户拒绝安装应用程序。”
ERROR_INSTALL	“尝试安装时检测到错误，安装失败。”
UNRECOGNIZED	“找不到项目或不再被跟踪（例如，错误/从设备中卸载并从跟踪中删除）。”
UNSUPPORTED_INSTALL	“已针对 3.0 Android 客户端/22.0.0 服务器进行更新：需要特定状态来跟踪安装与卸载。”
HIDDEN	“在隔离期间，将发送 HIDDEN/UNINSTALLED 状态。 取消隔离应该将其恢复到已安装状态。”
OTHER	“新添加错误的原因。”

对于 Windows 设备，如果应用程序在“应用程序配置”中设置为静默安装，则“设备摘要”会显示该应用程序的符合条件的设备、已安装设备、待处理设备或失败设备的数量。

从应用程序详细信息页面查看应用程序清单信息

要查看应用程序清单信息，请点击**查看应用程序清单（所有版本）**，在**设备 > 应用程序清单**中查看按该应用程序的捆绑包 ID 筛选的列表。



8.7. 应用配置

本部分包含以下主题：

- 应用功能的许可
- 多个应用通用的配置步骤
- 隐藏和挂起应用程序（仅限 Android）
- 配置网络中继
- 配置蜂窝 5G 切片
- 使用 Web 内容筛选器配置分发应用程序
- 使用 DNS 代理分发应用程序
- 清除 Android Enterprise 设备的应用程序缓存

通过应用配置，您可以自定义部署到用户设备上的每款应用的安装、推广和分配。 应用可以是您的内部应用、公共商店中的应用或 Ivanti Neurons for MDM 应用。 通过唯一名称和为每个收件人定制的配置，您可以将应用灵活地部署到多个不同用户和组。 内部应用版本的数量限制为 100。 如果超过该数量，Ivanti Neurons for MDM 系统将清除应用的最旧版本。 审核线索页面会列出和显示应用上传和清除的状态。

> 当您在 App Catalog 或受管应用配置配置文件中更改应用的应用配置值时，设备需要一个或两个设备签入才会收到新配置值。

应用功能的许可

> 以下特性需要额外授权：

- 静默应用安装/卸载：Silver 许可证
- Per-app 配置：Gold 许可证
- AppConnect 自定义配置：Gold 许可证

多个应用包需要良好的组管理，因为未来的设备类型无法由 Windows OS 定义。 在这种情况下，对于管理员而言，安装适当应用版本的唯一方式是使用正确群组的正确应用。

多个应用通用的配置步骤

首先执行这些步骤，然后针对您要部署的每个应用执行其他配置步骤。 您可以为同一应用设计多个配置，并给予每个配置唯一的名称。 每个配置都拥有各自的分发和推广水平，以适应您的部署战略。 内部应用版本的数量限制为 100。 如果超过该数量，Ivanti Neurons for MDM 系统将清除应用的最旧版本。 审核线索页面会列出和显示应用上传和清除的状态。 一次可以将一个应用部署到最多 100 个用户、用户组、设备或设备组。 可以选择要添加到应用程序目录的应用。 Ivanti Neurons for MDM 具有一个异步进程，可针对 iOS 应用“发送安装/更新请求”命令。 当使用“发送安装/更新请求”命令时，Ivanti Neurons for MDM 管理门户会显示消息以指示：

- 进程将继续在后台运行
- 进程已完成
- 状态是进程成功还是有任何错误

步骤

1. 转到**应用 > App Catalog**，然后单击 **+ 添加**。

2. 使用下拉菜单选择 App Store、Google Play 或内部 App Store，并选择要添加到目录的应用。
   根据许可协议，您也可以将可用应用添加至目录。
3. 您可以选择是否编辑应用的“类别”。
4. 您可以选择是否在**描述**字段中添加应用的简要描述。
5. 单击**下一步**。
6. 选择此应用配置的分配水平：
   - **每个人** — 将应用添加至所有用户兼容设备。
   - **无** — 将应用暂存，以便稍后进行分配。
   - **自定义分发** - 选择以下任意选项：
     - **用户/用户组** - 应用仅分发到您选择的用户或用户组。
       单击**用户**选项卡，以选择用户。
       单击**用户组**选项卡，以选择用户组。
     - **设备/设备组** - 应用仅分发到您选择的设备或设备组
       单击**设备**选项卡，以选择设备。
       单击**设备组**选项卡，以选择设备组。
7. 单击**下一步**。

配置安装选项

可以选择安装配置选项。

步骤

1. 单击**安装应用配置设置**或单击 **+** 图标添加其他配置，以查看**配置设置**页面。
2. 在**名称**字段中，输入此配置的名称。
3. 您可以选择是否在**描述**字段中输入安装配置的简要描述。
4. 选择**设备安装配置**选项。
5. 选择下列选项之一：
   - **需要在设备上安装**
   - **只在设备注册时安装一次**
6. 选择**不需要特定应用程序版本**选项，以避免将已安装的应用程序降级到较低版本。 此选项仅适用于现代应用程序。
7. 选择以下选项：
   - **在 Samsung Knox 工作区和 Zebra 设备上静默安装**（仅限 Android）
   - **不在最终用户应用目录中显示应用**。
   - **请勿在新注册的设备上安装应用程序**：现有设备不受影响，仍会在设备应用程序目录中显示应用程序。
     - 对于此分发中任何新注册的设备，则不会列出或推送应用程序。
     - 如果管理员触发发送安装/更新命令，则系统会将命令发送到设备。
   - **延迟应用程序更新时间**：您可以使用此选项延迟新应用程序版本安装。 此设置会根据配置的持续时间延迟新应用程序版本的自动安装。
   - **应用更新模式**（也支持 AMAPI 设备）。 （仅限 Android）
     使用此选项可以通过以下三种模式中的其中一种模式，将应用更新到最新版本：

- **默认**：在选择“应用更新模式”选项后，此模式也将处于选中状态。 在此模式中，更新将在应用可用时的 24 小时内实施。
- **推迟 90 天**：如果选择此更新模式，您可将应用更新推迟 90 天。 在 90 天后，根据在托管 Google Play 配置中实施的其他设置自动更新应用。
- **高优先级**：如果选择此更新模式，并且用户的设备处于在线状态，应用将在 Google Play 商店提供时立即更新。

- **设置应用安装优先级** - 请参阅“配置应用优先级”主题了解更多详细信息

> 在 Android 设备上，即使未选择“静默安装”选项，也可以使用“自动更新”选项来更新应用程序。 对于非强制性应用程序或用户自行安装的应用程序，管理员可控制其更新流程。

- **应用程序正在使用时请勿更新**：选择此选项可防止在用户主动使用应用程序时更新应用程序。 启用此选项时：
  - 在前台运行应用程序时，应用程序更新会延迟。
  - 用户可继续使用应用程序，而不会中断。
  - 当应用程序关闭或移至后台时，将自动安装待处理更新。

删除分发时删除应用程序 (Android)
对于受管 Google Play 应用程序，当应用程序不再分配给设备时，Ivanti Neurons for MDM 会自动从 Android 设备中删除应用程序。
应用程序在以下场景中被删除：

- 应用程序分发已更改为“无人”。
- 将从应用程序目录中删除应用程序。
- 将从应用程序分发中排除设备。

应用不同，附加配置选项也不同。 这些选项可能包括添加多个键值对的功能。 在这种情况下，点击 **+ 添加**输入键值对。 有关详细信息，请参阅应用目录中的**从公共商店添加应用**。

9. (macOS 11+) 选择选项，将应用安装和配置为托管应用：
   - **作为托管应用进行安装**
   - **转换为托管应用**

   > 在 macOS 12.0+ 中，用户注册的设备支持托管应用。

隐藏和挂起应用程序（仅限 Android）

对于处于以下模式的 Android 设备、**工作配置文件**、**完全托管设备**、**具有工作配置文件的完全托管设备**以及**公司所有设备上的工作配置文件**，您现在可以在安装后隐藏或挂起应用程序。

步骤

	1.	**在要应用“隐藏”或“挂起”操作的设备上安装一个或多个应用程序。**
	2.	**创建 App Control 配置，并将受管应用程序添加到隐藏或挂起列表中。**
	3.	**将更改应用于设备。**

> 如果某个应用程序同时出现在“隐藏”和“挂起”列表中，则该应用程序将被隐藏，因为“隐藏”列表将被优先处理。

配置应用优先级

在首次注册（特别是，在注册日期和时间之后的前 20 分钟内）时，您可以定义在设备上收到应用的顺序，所需的应用将会推送安装。 您可以在其他应用之前优先下载特定应用。 例如，在其他非重要应用之前，优先下载 Tunnel 和电子邮件应用。 此功能适用于公用和专用应用。 必备应用会在依赖应用之前推送。

iOS（AppStation for iOS 除外）、Android（Android for Enterprise 除外）、macOS（内部 PKG 应用程序、Apple 应用程序和 Books 应用程序）和 Windows 设备支持此功能。

> 此功能对新注册设备可用。 默认情况下，所有应用程序都设置为“中等”优先级。 在此过程中，虽然应用程序将争取安装所需的资源并且可能会排在高优先级的应用程序之前，用户也可以选择手动安装目录中的任何应用程序。

> 如为 Windows 应用程序，则 Bridge 应用程序的优先级高于任何其他应用程序。

请查看上一个章节适用于步骤的“配置安装选项”，以使用**设置应用安装优先级**选项设置应用的优先级。 可以为应用程序设置“高”、“中”或“低”优先级。 对于优先级相同的应用，安装顺序并无特定要求。 在用户已安装应用时，应用优先级不会在应用更新期间使用。

选择 Apple 应用程序管理配置设置

这些设置将仅应用于此应用，并将覆盖在**应用 > 目录设置**中选择的任何全局设置。 选择 **Apple App 管理**设置。

步骤

1. 单击 **Apple 应用设置**或单击 **+** 图标，添加其他配置，并查看**配置设置**页面。
2. 在**名称**字段中，输入此配置的名称。
3. 在**描述**字段输入配置的简要描述。
4. 在 **Apple 管理设置**中选择或取消选择以下选项中的一项或多项：
   - **阻止备份到 iCloud 和 iTunes**
   - **在取消注册时移除应用**
   - (iOS 14.0+) **允许移除和卸载此应用** - 您可以取消选择此选项，以防止用户移除和卸载受管应用。
   - （可选）添加 **Apple 托管应用配置**
5. 单击**更新**。

选择应用推广水平

可以设置应用的推广级别。

步骤

1. 单击**推广分配配置设置**或单击 **+** 图标添加其他配置，以查看**推广配置**页面。
2. 单击**编辑**。
3. 在**名称**字段中，输入推广分配配置设置的名称。
4. 您可以选择是否在**描述**字段中输入配置的简要描述。
5. 选择您希望应用收到的推广水平，**未特别推荐**、**特别推荐列表**或使用**特色横幅**。 如果选择**未特别推荐**，则此应用将不会列出。

6. 如果选择特色横幅，请指定以下详细信息：
    1. **标题** - 指定应用程序标题
    2. **描述** - 指定应用程序详细信息
    3. **横幅样式** - 选择横幅颜色
7. 单击 **+添加描述**，输入配置的简要描述。
8. 您可以选择是否改变配置的分配情况。
9. 单击**完成**保存应用配置。

配置 AppTunnel 流量规则

使用 AppTunnel 配置定义流量规则，以允许使用 Sentry 访问服务。

有关添加 AppTunnel 配置的信息，请查看*适用于 Ivanti Neurons for MDM 的 AppConnect 指南*中的“添加 AppTunnel 配置”。

配置托管应用

步骤

1. 单击 **+** 图标打开配置页面。
2. 单击 **+添加描述**，输入配置的简要描述。
3. 单击 **+ 添加**，输入键和值。
4. 选择分配水平。
5. 单击**下一步**。

使用 Per App VPN 配置每个应用的 VPN

步骤

1. 单击 **+** 图标打开配置页面。
2. 在**名称**字段中，输入此应用的 VPN 名称。
3. 单击 **+添加描述**，输入配置的简要描述。
4. 单击**启用此应用的 Per-App VPN** 选项，并选择可用 Per-App VPN 配置。
5. （可选）对于 macOS 应用，输入格式为**指定要求**的字符串，标识符是“\%s\”。 例如，标识符“com.google.Chrome”。 使用此字段启用多个软件包 macOS 应用，使用 Per-App VPN，例如 Tunnel。
6. 选择如何**分配此应用配置**。
7. 单击**下一步**。

使用 Apple 托管应用配置

使用 Apple 托管应用配置，可为已安装的托管应用配置特定设置。 应用可能包含开发人员实施或限制的一些配置参数。 对于包含此限制的应用，您的配置选项可能会受到限制。 可以配置 Apple 受管应用。

步骤

1. 转至**应用 > 应用目录**。
2. 选择一个应用程序。

3. 单击**应用配置**选项卡。
4. 单击 **Apple 托管应用配置**，或单击 **+** 按钮。
   在 Apple 托管应用配置中，共有一些默认配置设置。
5. 单击**添加**，以添加其他配置（如果需要）。 或者，单击配置的名称，以编辑配置。
6. 在**配置源**中，选择任何**源类型**选项

- **AppConfig 社区** - 此选项仅适用于在社区存储库中具有应用配置规范的应用。 如果此选项可用，将默认选中。
- **使用 .xml 规范** - 选择此选项可上传应用的架构，以推送特定版本的应用配置。 单击**选择文件**，上传 .xml 文件。 确保 .xml 文件包含捆绑 ID 和版本。 如果文件中的捆绑 ID 与应用的捆绑 ID 不匹配，将显示一条错误消息。
- **备注** - 如果您不想为该应用应用任何架构，请选择此选项。 如果 **AppConfig 社区**选项不可用，将默认选择此选项。
  配置源部分将显示上传的 .xml 文件。 单击删除图标，以删除上传的 .xml 文件。

7. 在 **Apple 托管应用设置**中，您可以设置配置选项，并输入键值对。

- 点击**添加**将项值对添加到托管应用程序配置，以便在 iReg 或 Apple 设备注册期间通过 Go 客户端检索注册名称身份。
  您可以选择适用于键值对的数据类型（字符串、整数、布尔值、长浮点、双精度、日期、字符串数组、整数数组、双精度数组、浮点数组、长数组）。

将以下键值对添加到受管应用配置，以检索 Go 客户端在 iReg 或 Apple 设备注册期间发现的注册名称信息：

密钥	值	类型
registration.username	$	字符串
registration.token	$	STRING
registration.token.expirationSeconds	$	字符串
registration.url	$	字符串

将以下项值对添加到托管应用程序配置，以便在 iReg 或 Apple 设备注册期间通过 Mac 代理 (Mobile@Work) 检索注册名称身份：

密钥	值	类型
客户端注册 URL	$	字符串
令牌	$	字符串
令牌过期时间	$	字符串

如果最终用户终止 Ivanti Go 应用程序，请点击**编辑**将应用程序设置为执行以下操作之一：

密钥	价值	类型
要显示默认通知，请使用以下值：		
enableAppTerminationNotification	True/False 或 1/0	布尔或字符串
要显示自定义通知，请使用以下值：		
appTerminationNotificationMessage	自定义通知	字符串
enableAppTerminationNotification	True/False 或 1/0	布尔或字符串

- **使用 .plist** - .plist 文件包含多个要批量上传的键值对。 单击**选择文件**，上传 .plist 文件。 已验证的 plist 数据将显示在 **Apple 托管应用设置**表中。

> 带有嵌套词典的 plist 无效。

8. 单击**更新**，以保存您的输入。

配置网络中继

增强应用程序网络流量的私密性和安全性，而无需连接 VPN。 有关详细信息，请参阅网络中继配置。

1. 点击**网络中继 + 图标**以打开配置页面。
2. 在"名称"字段中输入此应用程序的**网络中继**名称。
3. 点击 +**添加描述**以输入配置的简短描述。
4. 点击此应用程序的**启用网络中继**选项，然后选择可用的**网络中继配置**。
5. 选择如何**分发**此应用程序配置。
6. 单击**下一步**。

配置蜂窝 5G 切片

蜂窝 5G 网络切片支持允许将各个托管应用程序（所有 iOS 应用程序）分配到网络切片，以便利用切片来提供特定的网络功能和特性，从而优化应用程序体验。 分配操作使用 MDM 应用程序安装命令或声明式应用程序配置中的全新 **CellularSliceUUID** 应用程序属性完成。 要放入密钥的网络切片字符串值需要由支持的运营商提供。

> 如果特定应用程序或整个设备配置为使用 VPN，则不会使用 5G 网络切片。

Procedure程序

1. 前往**应用程序 > 应用程序目录 > 应用程序配置 > 蜂窝 5G 切片**，然后点击**添加**。
2. 在**配置设置**部分，更新以下字段：
   - 名称
   - 选择**启用 5G 网络切片**选项
   - 选择 **DNN** 或**应用程序类别**（根据网络提供商）
3. 选择此应用配置的分配水平：
4. 单击**保存**。

使用 Web 内容筛选器配置分发应用程序

可以使用 Web 内容筛选器配置来分发应用程序，而无需借助 DNS 代理服务器。 创建 Web 内容筛选器配置后，可以将该配置添加到应用程序以进行分发。 有关 Web 内容筛选器配置的详细信息，请参阅**Web 内容筛选**。

步骤

1. 前往**应用程序** > **应用程序目录**。
2. 选择一个应用程序。
3. 点击**下一步**。
4. 选择委派选项，然后点击**下一步**。
5. 选择所需的分发选项，然后点击**下一步**。
6. 选择 **Web 内容筛选器配置**并点击 **+** 图标。
7. 指定**名称**。
8. 选中**启用此应用程序的 Web 内容筛选器**复选框。
9. 从下拉菜单中选择 Web 内容筛选器。
10. 选择此应用配置的分配水平：
    1. **每个人** — 将应用添加至所有用户兼容设备。
    2. **无** — 将应用暂存，以便稍后进行分配。
    3. **自定义分发** - 选择以下任意选项：
        - **用户/用户组** - 应用仅分发到您选择的用户或用户组。
          单击**用户**选项卡，以选择用户。
          单击**用户组**选项卡，以选择用户组。
        - **设备/设备组** - 应用程序仅分发到您选择的设备或设备组。
          单击**设备**选项卡，以选择设备。
          单击**设备组**选项卡，以选择设备组。
11. 单击**下一步**。
12. 单击**完成**。 所选应用程序通过 Web 内容筛选器配置分发给特定用户。

使用 DNS 代理分发应用程序

可以使用 DNS 代理配置来分发应用程序。 创建 DNS 代理配置后，可以将该配置添加到应用程序以进行分发。 有关 DNS 代理配置的详细信息，请参阅**创建 DNS 代理配置**。

步骤

1. 前往**应用程序** > **应用程序目录**。
2. 选择一个应用程序。
3. 点击**下一步**。
4. 选择委派选项，然后点击**下一步**。
5. 选择所需的分发选项，然后点击**下一步**。
6. 选择 **DNS 代理配置**并点击 **+** 图标。
7. 指定**名称**。

8. 选中**启用此应用程序的 DNS 代理**复选框。
9. 从下拉菜单中选择 DNS 代理。
10. 选择此应用配置的分配水平：
    1. **每个人** — 将应用添加至所有用户兼容设备。
    2. **无** — 将应用暂存，以便稍后进行分配。
    3. **自定义分发** - 选择以下任意选项：
        - **用户/用户组** - 应用仅分发到您选择的用户或用户组。
          单击**用户**选项卡，以选择用户。
          单击**用户组**选项卡，以选择用户组。
        - **设备/设备组** - 应用程序仅分发到您选择的设备或设备组。
          单击**设备**选项卡，以选择设备。
          单击**设备组**选项卡，以选择设备组。
11. 单击**下一步**。
12. 单击**完成**。 所选应用程序通过 DNS 代理配置分发给特定用户。

克隆应用配置设置

可以克隆受管应用的配置设置，以便可以将相同设置应用到其他设备。 甚至可以重命名克隆设置并对其进行更改。

Android

可以在 Android 设备上克隆配置设置。

步骤

1. 转至**应用 > 应用目录**。
2. 选择要克隆配置设置的应用。
3. 单击**应用配置**。
4. 在**应用配置摘要**部分，您将看到可用于 Android 设备的配置列表（**Android 的托管配置**、**在设备上安装**、**推广**、**委派设备权限**和 **Google Play 版本**）。
5. 点击任意可用配置。
6. 在**操作**下，点击**克隆**开始克隆流程。
7. 默认情况下，克隆的配置名称将为 <Copy of the Cloned Configuration name>。 但是，您可以修改名称，在**名称**框输入自选的名称即可。
8. （可选）在**描述**框中，输入一些关于克隆设置的描述。
9. 单击**继续**。

系统将显示确认窗口，指出克隆应用配置设置已完成。 可以在“应用配置摘要”下方和克隆的应用中查看克隆的版本。

iOS

可以在 iOS 设备上克隆受管应用配置设置。

步骤

1. 转至**应用 > 应用目录**。
2. 选择要克隆配置设置的应用。

3. 单击**应用配置**。
4. 在**应用配置摘要**部分下方，您将看到可用于 iOS 设备的配置列表（**在设备上安装**、**Apple 应用设置**、**推广**、**AppConnect 自定义配置**、**应用隧道**、**Apple 受管应用配置**和**每个应用 VPN**）。
5. 点击要克隆的所需配置。
6. 在**操作**下，点击**克隆**开始克隆流程。
7. 默认情况下，克隆的配置名称将为 <Copy of the Cloned Configuration name>。 但是，您可以修改名称，在**名称**框输入自选的名称即可。
8. （可选）在**描述**框中，输入一些关于克隆设置的描述。
9. 从**源类型**列表中选择配置源。
10. 在 **Apple 受管应用设置**部分下方，输入**密钥**、**值**，并从列表中选择**类型**。
    有关**密钥**、**值**和**类型**的信息，请参阅**使用 Apple 受管应用配置**。
11. 单击**继续**。
    系统将显示确认窗口，指出克隆应用配置设置已完成。 可以在 **Apple 受管应用配置**部分中查看克隆的版本。

Windows

可以在 Windows 设备上克隆应用配置设置：

步骤

1. 转至**应用 > 应用目录**。
2. 选择要克隆配置设置的应用。
3. 单击**应用配置**。
4. 在**应用配置摘要**部分下方，您将看到**在设备上安装**和**推广**配置。
5. 点击要克隆的所需配置。
6. 在**操作**下，点击**克隆**开始克隆流程。
7. 默认情况下，克隆的配置名称将为 <Copy of the Cloned Configuration name>。 但是，您可以修改名称，在**名称**框输入自选的名称即可。
8. （可选）在**描述**框中，输入一些关于克隆设置的描述。
9. 单击**继续**。

系统将显示确认窗口，指出克隆应用配置设置已完成。 可以在“应用配置摘要”下方和克隆的应用中查看克隆的版本。

为内部目录选择 Windows 10 应用

选择应用，以添加到内部应用目录。 Windows 10 支持内部、Microsoft Store 和 Microsoft for Business 应用。 根据您选择允许或禁止的应用，Windows 10 会直接在设备上强制执行合规性。

> 默认情况下，Windows 10 签入间隔是每 60 分钟一次。 您可能想要执行强制设备签入，以获取设备和应用状态更新。

支持这些操作：

- 上传新应用
- 静默安装
- 从 Apps@Work 手动安装

- 添加应用的新版本
- 删除应用

支持这些格式：

- APPX
- APPXBUNDLE
- MSI 压缩 Win32 - 预捆绑 Win32 应用
- MSIX（RS5 和以上 Windows 10 设备支持）
- .EXE（使用 Bridge）

> **Ivanti Neurons Agent** 应用程序在 **Windows** 设备的**应用程序目录**中可用。 管理员可以将 **Ivanti Neurons Agent** 应用程序部署为内部应用程序，并且该应用程序可以相应地分发到 Windows 设备上。

配置 Windows 10 应用

步骤

1. 点击主导航栏上的**设备**。
2. 选择您已在 Ivanti Neurons for MDM 中注册的 Windows 10 设备。
3. 点击**应用 > App Catalog**。
4. 选择一个应用程序。
5. 使用**操作**下拉菜单，以添加应用或从目录删除应用。
   或者，添加应用的新版本。
   - 点击**操作**下拉菜单。
   - 选择**添加新版本**。
   - 转到目录，并选择应用的新版本。
   - 点击**更新并保存**可查看应用信息屏幕。
6. 使用**版本**下拉菜单，以选择要使用哪个版本。
7. 点击**编辑**可更改详细信息。
   - 根据需要编辑**类别**。
   - 根据需要输入**描述**。
   - 如有需要，请添加截图。
8. 点击**保存**。
9. 点击**分发**选项卡，然后点击**编辑**即可更改分发级别。
10. 点击**保存**。
11. 点击**应用配置**选项卡，以查看当前配置的摘要。
12. 如有需要，输入应用的描述。
13. 在“应用配置”摘要页面中，点击**在设备上安装**。
    静默安装是默认设置，且无法更改。
14. 点击左侧导航窗格中的**推广**，然后点击**推广分发配置设置**，以更改推广级别。

- 点击**编辑**可更改推广级别设置。
- 输入配置的名称。
- 输入配置的描述。
- 选择推广水平。
- 单击**更新**保存您的更改。

15. 点击**评论**选项卡可查看关于评论的信息。
    如有需要，请将评审数据导出至电子表格。

编辑 Windows 10 应用配置设置

步骤

1. 点击**策略 > 配置**。
2. 点击 **+ 添加**。
3. 选择 **Windows 应用控制**，查看**创建 Windows 应用控制配置**屏幕。
4. 为配置输入**名称**和**描述**。
5. 将应用类型定义为如下方式：
   - 允许（已加入允许列表）- 仅允许这些应用。 如果未出现在设备上，这些应用会静默安装。
   - 不允许（已加入阻止列表）- 如果设备已有，将阻止这些应用（如果启动）。
6. 为应用类型和应用标识符指定规则定义。
7. 点击**查找应用**可查看**搜索 Windows 10 应用**屏幕。
8. 输入应用名称，以搜索 Windows Store。
9. 从显示的选项中选择应用，以将其添加到应用标识符。
10. 或者，使用“应用类型”下拉菜单，以设置在应用标识符中定义的路径，从而允许或禁用使用指定路径的应用，或阻止所用应用安装到该路径。
    应用程序类型**发布者/PFN 等于**适用于 Windows 10+ 设备且支持 PFN。 **EXE/Win32 等于**。
11. 点击**下一步**。
12. 选择分配水平。
    - **所有设备**。
    - **无设备**。
    - **自定义** — 输入接收应用的用户或小组。
13. 点击**完成**。
14. 您可以编辑规则定义，以选择应用类型并指定应用标识符。
    - 点击**操作**下拉菜单。
    - 选择**添加新版本**。
    - 选择应用的新版本。
    - 点击**更新并保存**可查看**应用信息**屏幕。

配置适用于 Windows 的“安装之后重新启动设备”选项

可以使用**安装之后重新启动设备**选项，将设备配置为在安装应用程序之后重新启动。

步骤

1. 转至**应用 > 应用目录**。
2. 从列表中选择任何特定于 Windows 的应用程序。
3. 前往**应用程序配置 > 安装在设备上 > 安装应用程序配置设置**。
4. 点击**编辑**，将**安装之后重新启动设备**选项设置为“开启”。
5. 选择以下重新启动设备的时间计划选项之一：

设置	采取何种措施
安装后立即	选择此选项可在安装应用程序后立即重新启动设备。
在一天中的特定时间	选择此选项可于安装应用程序后在一天中的特定时间重新启动设备。
几分钟后	选择此选项可在安装应用程序后的 **15**、**30**、**60** 或 **120** 分钟后重新启动设备。

6. 点击**更新**。

设备将在计划时间重新启动。

> 对于公共应用程序和适用于企业的 Microsoft Store (MSB) 应用程序，需要在**应用程序配置**部分中将**在 Windows 设备上静默安装**设置设为“开启”。

使用 Apps@Work 安装应用

要使用 Apps@Work 安装应用：

1. 点击 **Apps@Work** 应用。
   您的管理员电子邮件地址和服务器 URL 已预先在 Apps@Work 登录对话框中填写。
2. 输入您的密码，然后单击“登录”，以显示应用页面。
3. 选择要安装的应用。 如果未在客户端中安装这些必备应用，您将无法安装依赖于必备应用的应用。
   对于 Apps@Work for iOS 设备，您可以选择单击**全部安装**按钮，以安装所有应用。 此选项在**新版本**、**特色应用**和**类别**屏幕中可用。

> 如果之前未接受 App 和图书应用许可证，将不会安装 App 和图书应用。

4. 点击**更新并保存**可查看**应用信息**屏幕。

Android Enterprise 设备的应用程序安装和更新

管理员可以将应用程序发布到目录以进行常规访问，同时将其部署到特定设备以供立即使用。 这允许用户直接接收应用程序，同时它也可以在目录中供其他人根据需要安装。

安装应用程序和更新

1. 导航至**应用程序 > 应用程序目录**。
2. 选择您想要添加的应用程序。
3. 单击**详细信息**屏幕上的**操作**。 将显示**发送安装/更新请求**。
4. 单击发送安装/更新请求。 将显示**发送安装/更新请求**对话框。

5. 在**向此应用程序的设备发送安装和更新通知**下执行以下操作：
   - 选中**发送新应用程序请求（适用于尚未安装该应用程序的设备）**复选框以安装新应用程序。
   - 选中**发送更新请求（适用于已安装应用程序但有更新可用的设备）**复选框以更新安装的应用程序。
6. 在**选择要发送请求的用户**下执行以下操作：
   - 单击**所有人**可将配置分发给所有兼容用户。 该应用程序出现在其应用程序目录中。
   - 单击**自定义**以定义可在应用程序目录中看到应用程序的用户组或用户。

> **发送安装/更新请求**分发是应用程序分发过程的一部分。 您在**分发**屏幕上选择的设置决定了哪些设备将接收该应用程序。

系统将显示确认窗口，指出应用程序安装已完成。

来自新安装或更新的更改显示在**仪表板** > **审计跟踪**中。

> 对于公共和私有应用程序，会禁用**发送更新请求（适用于已安装应用程序但有更新可用的设备）**。 只允许**发送新应用程序请求**。

相关主题：

- 应用目录

清除 Android Enterprise 设备的应用程序缓存

清除应用程序缓存请求允许管理员远程清除使用 Ivanti Neurons for MDM 安装在 Android Enterprise 设备上的选定应用程序的缓存数据。 此操作有助于解决常见的应用程序问题，例如性能缓慢、意外错误或过时的临时数据，而无需卸载或重新安装应用程序。 请求仅要求清除应用程序缓存并保存用户数据、应用程序设置和配置。 管理员使用此功能快速恢复正常的应用程序行为，同时最大限度地减少对最终用户的干扰。

步骤

1. 导航至**应用程序** > **应用程序目录**。
2. 选择并打开应用程序。
   此时将显示应用程序**详细信息**页面。
3. 单击应用程序**详细信息**页面上的操作菜单（⋮）。
4. 选择**清除应用程序缓存请求**选项。
   随即显示**清除应用程序缓存请求**窗格。
5. 在**选择发送请求的用户**部分中执行以下操作之一，以分发应用程序缓存清除请求：
   - 选择**所有人**将请求发送到已安装应用程序的所有兼容设备。
   - 选择**自定义**以将请求发送到特定用户、用户组、设备或设备组。
6. (可选) 在**其他分发筛选器选项**下搜索现有分发列表。
7. （可选）选择 **+ 添加分发筛选器**以在**创建分发筛选器**窗格中创建分发筛选器。

> 使用此选项可将 **清除应用程序缓存请求**发送到特定设备集，例如 DO 或 EPO 模式设备。

8. 单击**发送**。
9. 在**清除应用程序缓存确认**对话框中单击确定。
   Ivanti Neurons for MDM 将显示一条通知，其中列出收到**清除应用程序缓存请求**的设备数量。

完成**清除应用程序缓存**请求后，所有应用程序详细信息（版本、名称、platformAppId、displayVersion 和 bundleVersion）都将记录在**审计跟踪**页面中。

8.8. 将自定义属性分配给应用程序

创建自定义属性后，可以将其分配给一个或多个应用程序。 每个属性都有一个对应值，可使用该值执行各类任务，比如创建应用程序组。 有关管理属性的详细信息，请参阅属性。

创建自定义属性并分配给单个应用程序

可以将自定义属性分配给单个应用程序。

程序

1. 登录到管理门户。
2. 导航至**应用程序** > **应用程序目录**。
3. 选择一个应用程序，然后点击**属性**。
4. 点击 **+ 新增**从**属性名称**下拉菜单中选择一个值。
5. 在**值**字段指定属性值。
6. 单击**保存**。 自定义属性已添加到应用程序。

将自定义属性分配给多个应用程序

可以将自定义属性分配给一个或多个应用程序。 选择多个应用程序时，自定义属性将应用到应用程序的每个版本。 可以选择特定的应用程序，接着转到“属性”选项卡，然后更改特定应用程序版本的自定义属性详细信息。

程序

1. 登录到管理门户。
2. 导航至**应用程序** > **应用程序目录**。
3. 选中一个或多个应用程序的复选框。
4. 点击**操作**。
5. 选择**分配自定义属性**。 随即将显示“将自定义属性分配给应用程序”向导。
6. 选择下列选项之一：
   - 强制分配（覆盖）所有属性，即使找到任何现有值。
   - 仅当值为空时才进行覆盖，并跳过已有值的属性。
7. 选中一个或多个属性的复选框。
8. 在“值”字段指定值（不允许使用空值）。
9. 点击**分配**。 自定义属性将分配给所选应用程序的所有版本。
10. （可选）如果要更改单个应用程序版本的自定义属性，请从版本下拉列表中选择应用程序版本，并点击“编辑”。

> 可以从**设备详细信息**页面，使用**自定义应用程序属性**及其值来创建报告和导出为 CSV 格式。

8.9. Android 的托管配置

本部分包含以下主题：

- 使用 Android Enterprise 托管配置
- 适用于内部应用程序的应用程序限制和权限
- 使用 Android Enterprise 设置 Gmail

如果 Ivanti Neurons for MDM 已启用 Android Enterprise，则 Android Enterprise 配置可按应用进行使用。

使用 Android Enterprise 托管配置

1. 单击**应用**。
2. 单击**应用目录**。
3. 选择要配置 Android Enterprise 配置的应用。
4. 单击**应用配置**。
5. 单击 **Android 的托管配置**。
6. 为配置提供名称。
7. 您可以选择提供描述。
8. 使用“托管配置”字段，配置托管配置行为：
9. 使用**隧道配置设置**将隧道应用程序直接与适用于 Android 设备的 Ivanti Go 应用程序集成。 选择**启用隧道配置**选项以应用此设置。 通过此增强功能，管理员可以通过 Ivanti Go 启用隧道功能，并使用现有隧道配置配置安全连接。 此功能适用于新注册的 Android 设备。 为确保无缝过渡，独立隧道应用程序将继续受支持。 但是，安装独立隧道应用程序的设备不会在 Ivanti Go 中显示集成隧道体验。 删除独立隧道应用程序后，集成隧道功能将在 Go 应用程序内变为可用。 一次只能将一个隧道配置应用于设备。

设置	描述
阻止应用在配置文件之间共享小组件 阻止用户卸载应用 最低版本代码	启用以仅在未静默安装应用时，阻止应用在配置文件之间共享小组件。 保持禁用，允许部署到 Android Enterprise 配置文件的受信应用在主屏幕上显示小组件，以便用户访问信息，无需登录。 启用此功能可阻止用户在 Ivanti Neurons for MDM 静默安装应用程序后卸载应用程序（公开、私人或内部）。 对于应用覆盖默认更新行为，设置其所需的最低版本代码。 如果当前在设备上安装的应用的版本代码低于指定的最低版本代码，该应用会立即更新到最新版本。
在安装时自动启动	如果要在安装后自动启动应用，选择此选项。 仅在应用是新安装到设备而非版本更新时，此功能才可用。 对于工作配置文件和公司拥有设备上的工作配置文件，Go 应用应保持活动状态并置于前台。 由于 Android 10+ 的局限性，如果用户将多个应用推送到工作配置文件和公司拥有设备上的工作配置文件，仅有一个应用将自动启动。

10. 管理员可以控制哪些应用配置字段可以发送到设备，以及哪些应用配置字段不可以发送到设备。 通常，在将配置推送到不同设备时设置默认值。 在“托管配置”部分下，选择**推送到设备**设置中的**推送所有设置**或**只推送已定义值的设置**。

受管配置

每个 Android Enterprise 应用配置会为每个文本字段显示证书启用按钮；在单击时，证书的下拉列表将替换文本字段。 在配置时，这些证书会静默应用，没有任何用户交互。

单击字段旁边的相同按钮，可将现有启用证书的字段更改为启用文本。 对于更改为证书启用字段的文本启用字段，单击相同按钮，可将其更改回文本启用字段。 （默认下拉字段无法更改回启用文本字段。）

> 如果未在租户中配置任何 ID 证书，且在使用启用证书的按钮从文本切换为下拉列表时，下拉列表仅显示"无"选项。

单击**管理权限**，为面向 API 23 或更高版本以及Android 6.0+ 的应用程序选择并配置运行时权限。

仅列出适用于特定应用程序的危险权限以供选择。 危险权限的完整列表（例如，读取您的联系人，在设备上查找帐户，写入呼叫日志等）请参见：https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups。

11. 您可以分配给每个权限的权利包括：
    - 仅当应用程序请求权限时才应用权限。
    - 如果用户以前接受或拒绝了权限，则不应用权限。
    - 自动授权
    - 自动拒绝。 请谨慎使用此设置。
    - 默认/全局

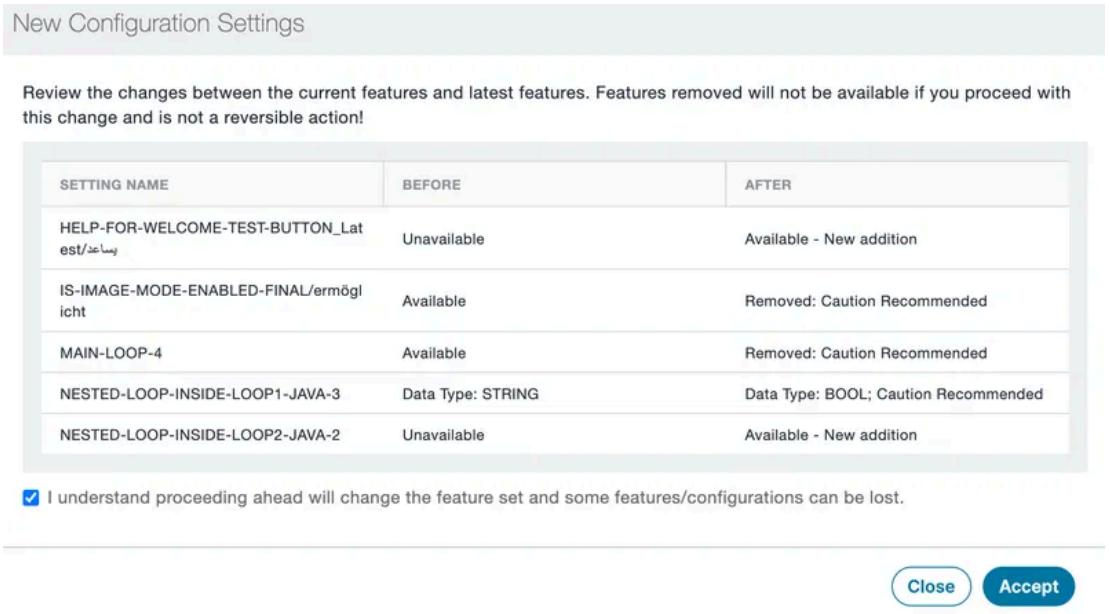
配置分配选项，从**具有应用程序的所有人**、**没有人**或**自定义**中选择。

12. 单击**保存**。

新的配置设置

应用程序版本更新且现有配置出现更改时，编辑"配置详细信息"页面后，**更新至最新功能**按钮会出现。

1. 点击**更新至最新功能**。
   屏幕上会出现一条警告消息，说明更新至最新功能后，用户将无法再访问旧版应用程序。 警告消息会显示建议步骤，以便无缝集成最新版本的应用程序。
2. 单击**下一步**。
3. 屏幕上会显示**新的配置设置**页面。



新的配置设置窗口会列出配置中存在的不同设置，以及更新后每个设置的状态。 “新的配置设置”窗口会列出数据库的所有限制，而 Google 架构会列出以下状态：

- 已添加
- 已删除
- 已修改

选中复选框，然后点击**接受**继续进行更新。
屏幕上会出现一条确认消息，说明配置已成功更新到最新功能。 现在可以分发并保存配置，以便让更改生效。

适用于内部应用程序的应用程序限制和权限

管理员可以设置一些应用程序限制，并限制内部应用程序的权限或向其授予权限。 此功能之前仅适用于公共应用程序。 但此功能已得到扩展，现在也适用于内部应用程序。

> 管理员必须重新上传内部应用程序，才能在这些应用程序上使用**应用程序限制**和**权限**功能。 建议删除现有应用程序之后再上传新版本。

步骤

1. 前往**应用程序** > **应用程序目录**。
2. 从列表中选择**内部**应用程序。
3. 单击**应用配置**。
4. 点击 **Android 的受管配置**。
5. 单击**添加**。
6. 屏幕上将显示**应用程序限制**部分。
   为可用限制输入所需值。
7. 选择**管理权限**。
8. 屏幕上将显示**选择权限**窗口。
   从列表中选择所需权限，然后点击**选择**。
9. 在**运行时权限**部分下方，设置所选权限的值。
10. 在**分发此应用程序配置**部分下方，选择以下**应用程序分发**选项之一：
    - **每人都有应用**
    - **无**
    - **自定义**
11. 单击**保存**。
    所选限制和权限将应用于内部应用程序。

使用 Android Enterprise 设置 Gmail

如果已为 Android Enterprise 设置 Ivanti Neurons for MDM，可将 Gmail 部署到 Android Enterprise 设备。 使用 Android Enterprise 设置 Gmail

1. 转至**应用 > 应用目录**。
2. 选择要配置 Android Enterprise 配置的 Gmail 应用。 此时将显示“配置设置”部分。
3. 为配置提供名称。

4. 您可以选择提供描述。
5. 使用**受管配置**字段，以配置受管配置行为：

全部展开和**全部折叠**选项仅可用于嵌套或分层限制。

设置	说明
推送至设备	推送所有设置 - 选择此选项可启用所有切换开关，包括没有值的切换开关 只推送已定义值的设置 - 选择此选项可启用所有具有已定义值的切换开关，并针对没有值的设置禁用切换开关 在许多情况下，默认设置已经可用。 但是，管理员可以选择所需的应用配置设置，或编辑必须发送到设备的变量。
电子邮件地址	输入替换变量，以定义电子邮件地址。 通常，您需要输入 $emailaddress$。 UEM 可以使用此字段，以从 Active Directory 提取用户凭据。
主机名或主机	输入 Active Sync 服务器的主机名，例如 hostname.company.com:443/path。
用户名	将变量用于可指定为直接用户名 (janedoe) 或模板化值 ($username$) 的用户的 Active Directory 用户名。
身份验证类型	选择包含允许身份验证类型的字符串列表。
SSL 必填	选中后，请在与主机名一起使用的端口号上启用并要求 SSL。
信任所有证书	仅在您要让应用自动接受不信任证书时选择。 在测试环境中使用时，仅将此选项用于调试或开发。
登录证书别名	对于用于对 ActiveSync 服务器进行身份验证的登录证书，输入其别名。
允许未受管帐户	选择此选项，以允许用户添加或移除任何 Exchange 帐户，但在此受管配置中指定的帐户除外。
默认电子邮件签名	输入包含默认电子邮件签名的字符串，该字符串将附加到所有出站电子邮件消息文本的底部。
默认同步时间段	输入 0-5 之间的值，表示与 EAS (Exchange Active Sync) 同步的时间范围。

单击**下一步**。

7. 配置分配选项，从**具有应用程序的所有人**、**没有人**或**自定义**中选择。
8. 单击**保存**。

8.10. 管理 Google Play 应用

您可以定义应该将 Google Play 应用中的哪些二进制文件部署到特定组或个人。此部署适用于 Android 企业版部署。 应用开发人员也必须将贵组织加入允许列表，才可以部署 Alpha 或 Beta 版信道应用。

1. 单击**应用**。
2. 在**应用目录**中，选择要配置 Google Play 版本配置的应用。
3. 单击**应用配置**选项卡。
4. 单击 **Google Play 版本**。

> Google 版本配置仅适用于 Android Enterprise 应用。 默认情况下，如果未为新添加的应用选择 Google 版本配置，则应用“生产”选项。

单击**添加**。

6. 为配置提供名称。
7. 您可以选择提供描述。
8. 从下拉列表中选择选项，以选择可用于接收此应用的用户和设备的二进制文件。 选项有：
    - 生产
    - Alpha
    - 试用版

    > 生产选项默认应用于已推送到设备的应用。
9. 配置分配选项，从**具有应用程序的所有人**、**没有人**或**自定义**中选择。
10. **自定义**将用户组中的应用与设备筛选器一起分配。
    单击**保存**。

确定多个版本配置的优先级

当添加多个 Google 版本配置时，您可以确定应用 Google 版本配置的优先顺序。

1. 在**应用配置**中，单击**优先配置**。

> 该按钮仅在列出多个配置时显示。

从列出的配置中，将应该优先应用的配置拖放到列表顶部。

3. 单击**更新**。

> 当删除最高优先级的配置时，以下较早列出的配置将成为最高优先级。

8.11. 从 App Catalog 中删除应用

您可以从应用目录中删除公共和内置应用。 您无法删除必备应用。 您需要编辑应用，以在删除此类应用前移除必备关系。 如果设备上已安装应用，下次设备签入时会将此应用移除。 处于设备管理员模式的 Samsung 和 Zebra 设备或处于设备所有者模式的所有设备都支持静默应用安装/卸载。

如果是内部应用程序，屏幕上将显示确认窗口。 您需要选择您确认要继续“删除”操作，并点击**删除应用程序**。 尝试删除多个应用程序但部分应用程序无法删除时，屏幕上将显示窗口，包含有关无法删除的应用程序的信息及无法删除的原因。

尝试从“应用程序目录”删除一个或多个应用程序时，会出现以下情况：

- 如果无法删除内部应用程序的某个版本，则将无法删除该应用程序的任何版本。
- 如果内部应用程序的某个版本是必备应用程序，则将无法删除该应用程序，也无法删除该应用程序的任何版本。
- 选择所有或部分内部应用程序并将其从“应用程序目录”中删除时，所选内部应用程序的所有版本都将被删除。
- 无法删除从“空间”委派的内部应用程序。

步骤

1. 转至**应用 > 应用目录**。
2. 单击应用的链接。
3. 选择**操作 > 从目录中删除**。
4. 阅读警告，了解删除应用会发生哪些情况。
5. 警告会解释 App 和图书许可证 (iOS) 和应用评论（所有 OS）也将删除。
   选择“我了解删除应用程序的后果”复选框即可继续删除操作。
6. 单击**删除应用**。

8.12. 升级内部应用

使用以下过程更新内部应用：

1. 转至**应用 > 应用目录**。
2. 选择要更新的应用。
3. 选择**操作 > 添加新版本**。
4. 将应用拖放到**上传应用**区域，或者单击**选择文件**，从文件系统中选出该应用。
5. 根据您对以前版本的应用要执行的操作，选择以下选项之一：
   - **保持描述、截图、分发、应用先决条件和应用配置相同：**替换 App Catalog 中之前的版本。
   - **更改描述、截图、分发、应用先决条件或应用配置**：在 App Catalog 中包含两个版本。
6. 在**新增功能**中输入文本，向用户介绍新版本的优越之处。
7. 用户选好要安装的应用后，设备上将显示此文本。
   如果您选择更改描述、截图或分配选项，请完成这些更改。
8. 单击**完成**。

如果选择在目录中保留旧版本应用，在**应用 > 应用目录**中将仅显示一个条目。 最左侧窗格将显示该条目所涉及应用的数量。 如果您随后决定删除新版本，旧版本将自动替换设备上安装的新版本。

显示应用程序版本列表

允许管理员上传版本相同但架构不同的应用。

Procedure步骤

1. 单击**应用 > App Catalog** 中应用的链接。
2. 点击**版本**选项卡。
   如果目录中有多个版本的应用程序，则下拉列表会显示版本。 如果上传多个版本号相同但架构不同的应用，下拉列表会显示支持的架构详细信息。 **应用信息**下也会显示应用支持的架构。

8.13. 查找 Android 应用程序的软件包名称

如为可从 Google Play Store 上取得公共应用：

1. 使用网络浏览器定位 Google Play Store 上的应用。
2. 选择应用。
3. 检查浏览器上显示的 URL。

URL 包含软件包名称，位于 id= 之后；如下所示：

https://play.google.com/store/apps/details?id=<package name>

对于内部应用和 Play Store 中不可用的其他应用，请尝试下载软件包名称查看器或 Google Play Store 中的相似应用。

8.14. 类别

本部分包含以下主题：

- 添加类别
- 移除类别

类别描述了应用的类型，并在用户浏览应用目录时帮助组织应用。 每个应用必须至少分配有一个类别。 当您开始使用 Ivanti Neurons for MDM 时，可以使用常见应用类别列表。 通过该页面管理应用类别。

添加类别

您可在此处添加新类别，或者向应用类别中添加应用时，添加新类别。

1. 单击**添加**（左下角）
2. 输入类别名称。
3. 类别不区分大小写，因此“MINE”与“Mine”是相同名称。
   单击**保存**。

移除类别

- 单击类别旁边的“X”。

如果您无法在**应用类别**页面上执行任务，这可能是您没有所需权限。 您需要以下其中一个角色：

- 应用和内容管理

8.15. 分配过滤器

本部分包含以下主题：

- 配置分发筛选器
- 为委派管理员配置分发筛选器

使用分配过滤器限制可以安装的应用。 通过分配过滤器，您可以在应用目录中仅显示适用于设备的应用。

许可证：Silver

这些过滤器默认可用：

- **启用了 Android 企业版的应用** - 将应用分发限制到仅启用了 Android 企业版的设备。
- **仅限 iPad 应用** - 应用分配仅限 iPad 设备。
- **仅限 iPhone 应用** - 应用分配仅限 iPhone 设备。

配置分发筛选器

1. 转到**应用 > 分配过滤器**。
   默认应用过滤器和任何已创建的应用过滤器在此列出。
2. 单击 **+添加**，访问**创建分配过滤器**对话框。
3. 在相应字段输入名称和描述。
4. 选择规则定义。这些规则可以使用适用运算符构建，包括“包含”、“小于”、“大于”、“在以下范围”、“等于”和“不等于”运算符。 规则可以使用 ANY (OR) 或 ALL (AND) 选项嵌套在一起。 应用程序分发筛选器如下：
   - 已阻止 Access
   - 支持 APNS
   - 带有工作配置文件的 Android 托管设备
   - Android Work 已启用
   - Android 安全补丁级别（Android 设备）
   - 已启用 Android 工作托管设备（设备所有者）
   - 公司拥有设备上的 Android 工作配置文件已启用
   - 客户端上次签入
   - 客户端已注册
   - 合规性
   - 已阻止合规性操作
   - 当前国家/地区名称
   - 当前 MCC
   - 当前 MNC
   - 自定义设备属性
   - 自定义 LDAP 属性
   - 自定义用户属性
   - 自定义 IDP 属性

- 设备类型
- 原籍国家/地区名称
- 家用 MCC
- 家用 MNC
- IMEI
- IMEI2（仅适用于具有双 SIM 端口的 Android 设备，并且设备必须为 Android 8.0 或更高版本）
- 单应用模式
- 制造商
- 操作系统版本
- 所有权
- 手机号码
- 漫游
- Secure Apps 状态
- 受监控
- 已阻止 Sentry
- User Enrollment 已注册
- 自动化 Device Enrollment 已注册
- 自动化 Device Enrollment 已启用

5. 单击**创建分配过滤器**。
6. 如有需要，选择要更新的自定义过滤器。
    1. 单击**编辑**，显示**更新分配过滤器**页面。
    2. 在相应字段输入名称和描述。
    3. 使用下拉菜单定义过滤器的规则。
    4. 单击**更新分配过滤器**。
7. 选择一个应用程序。
8. 在“应用详细信息”页面选择**分配**选项卡。
9. 单击**编辑**。
10. 选择“应用分配”选项：
    - **每人**
    - **无人**
    - **自定义**

    > “分发筛选器”部分只有在选择**所有人**或**自定义**分发选项时才可见。

11. 选择分配过滤器选项：
    1. 在**搜索现有分发筛选器**中输入筛选器名称... 以查找已创建的筛选器。
    2. 单击 **+添加分配过滤器**，添加新过滤器。

分发筛选器可以在添加至目录前创建或指派给某应用。 对分配过滤器所做的更改将影响正在使用该过滤器（在所有空间中）的应用程序的分配。

在设置筛选器时，并且如果启用**在分发时允许在 M1 设备上安装应用**，结果将填充 macOS M1 设备。 如果启用**在分发时允许在 M1 设备上安装应用**，分发筛选器为**每个人**或**自定义**，iOS VPP 应用将对所有 Mac 设备可用。 iOS 应用不支持 macOS 相关属性的分发筛选器。

为委派管理员配置分发筛选器

授权管理员可以在授权空间中分配过程中管理和编辑已添加到各个应用程序的已创建过滤器。 但是，授权管理员不能在任何其他空间中使用在默认空间中创建的分配过滤器，但可以将其用于授权的应用程序。

授权管理员可以在他们有权访问的特定空间中创建、管理和编辑分配过滤器。 分配过滤器仅在其创建的空间中可用。 应用程序分配过滤器不能被授权。

当具有应用程序和系统管理角色的授权管理员使用分发筛选器在授权空间中添加应用时，可以查看其空间中的设备和其他空间中的设备的设备详细信息。

具有系统管理或系统只读角色的用户将无法在任何空间创建、更新或删除分配过滤器。

具有应用程序和内容管理员角色的授权管理员可能无权访问分配过滤器。 因此，您无法：

- 使用分配过滤器创建应用程序。 当您以授权管理员身份登录并添加应用程序时，会发生这种情况。
- 只有拥有系统只读角色或更高权利的授权管理员可以使用分配过滤器添加应用程序。 没有系统管理角色的授权管理员可以添加没有分配过滤器的应用程序。

授权管理员可以通过选择以下选项来筛选 App Catalog 中的授权状态：

- 已授权
- 未授权

8.16. 排除或分发应用程序

从设备中排除或分发托管应用程序，而无需更改 iOS、macOS 和 Windows 设备上的内部和公共应用程序的应用程序分发配置。 对于所有托管应用程序，可在所有设备**可用应用程序**部分的**操作**列中找到这些选项。

权限

要从设备中排除应用程序或将应用程序分发至设备，您需要拥有以下授权：

- 访问空间（分区）中的设备
- 访问设备的可用应用程序。

排除

所选应用程序的排除选项会卸载应用程序，并从设备中删除关联数据。 按照工作流程排除必备应用程序。 弹出确认消息提示您正在排除必备应用程序，此操作将从设备中排除主应用程序。

如果您排除具有多个版本的内部应用程序，则会从设备中排除所有未分发的应用程序版本。 如果您从设备中排除某个应用程序，该应用程序将从 Apps@Work 和 Ivanti Go 中删除。 如果从应用程序目录中排除和删除某个应用程序，之后又再次添加，则该应用程序不再被设备排除。 如果从设备中排除某个托管应用程序，则该应用程序应显示在**设备** > **设备** > **可用应用程序**列表中，以便管理员在排除该应用程序后对其进行分发。

分发

管理员从应用程序触发**发送安装**命令时，只有在管理员决定从设备的**可用应用程序**中分发应用程序后，该应用程序才会安装。 对于尚未安装该应用程序的设备，会显示一条新的排除消息。 在管理员分发可用的应用程序后，下次同步时会在设备上安装分发的应用程序。

8.17. 评论

本部分包含以下主题：

- 查看评级和评论
- 禁用评级和评论
- 删除评论
- 将评价导出到 CSV 文件

评论是您的用户在应用目录中提供的有关应用的评论和评分（星级）。 评论为您和正考虑安装应用的用户提供了有价值的信息。 使用**评论**页面浏览或删除评级和评论。 如果评论过久或不适当，您可将其删除。

- 只有设备用户可以创建和编辑应用评级和评论。
- 设备用户可编辑但不能删除自己的评级和评论。
- 只有管理员可以删除应用的评论。
- 无法删除应用评级。 即使您稍后禁用用户的评级和评论功能，也会在**应用 > App Catalog** 页面上保留对应用的评级（星级）。

查看评级和评论

- 转到**应用 > 评论**，阅读用户对您分发的应用进行的完整评论和评级（星级）。
- 转到**应用 > App Catalog**，并查看**平均。 评级**列，了解评论总数和平均评级。
- 转至**应用 > 应用目录**，单击**应用名称**，并查看**评级**选项卡，以浏览特定应用的评级和评论。

禁用评级和评论

1. 转至**应用 > 目录设置**。
2. 取消选择**在最终用户应用目录中启用评级和评论**。
3. 单击**保存**。

删除评论

1. 转至**应用 > 评论**。
2. 选择评论。
3. 单击页面右上角的**操作**按钮。
4. 选择**删除**。
5. 单击**删除评论**确认对话框中的**是**。

如果您无法在**审核**页面上执行任务，这可能是您没有所需权限。 您需要以下其中一个角色：

- 应用和内容管理

将评价导出到 CSV 文件

可以使用**评价**页面中的**导出到 CSV** 选项导出应用程序评价。

步骤

1. 转至**应用 > 评论**。
2. 点击**导出到 CSV** 选项，可将评价列表和相关详细信息导出到 CSV 文件。
3. 将显示带有**继续**和**取消**按钮的弹出消息，表明导出过程已开始，并且很快就会生成报告。
4. 点击**继续**并等待请求完成后再提交另一个请求。
5. 将显示一条消息表明**应用程序评价 - CSV 报告已完成**，并提供**下载**和**删除**按钮。
6. 点击**下载**以下载报告。
7. （可选）点击**删除**可以删除报告。

8.18. AppleApp 和图书

本部分包含以下主题：

- 空间中多个 Apple App 和图书帐户之间的应用许可证分发
- 基于设备和基于用户的许可证分发
- 使用基于设备的许可证选项
- 使用基于用户的许可证选项
- 将 App 和图书应用添加到目录
- 添加 App 和图书帐户
- 更新 App 和图书安全令牌
- 更新 App 和图书帐户的优先级
- 删除 App 和图书安全令牌
- 为目录中的 App 和图书应用分发许可证
- 查看每个用户的应用许可证
- App 和图书许可证使用情况通知
- 查看 App 和图书许可证使用情况
- 撤销应用的 App 和图书许可证
- macOS 和 iOS 设备的 App 和图书行为
- 在设备移动空间时使用的 App 和图书许可证授权

许可证： Silver

只有当您在 App Catalog 设置中设置 Apple App 和图书后，**Apple App 和图书**屏幕才可用。此屏幕显示通过 Apple App 和图书为 Apple 设备购买的应用许可证，以及使用数量。 使用此屏幕：

- 选择要在您的目录中包含的 App 和图书应用
- 为 App 和图书应用分发许可证

有关利用 Apps and Books 分发应用的详细信息，请参阅 Ivanti 社区文章 Ivanti Neurons for MDM：如何利用 VPP 分发应用。

> Apple 图书并非在所有国家或地区可用。 要通过 Apple App 和图书为应用分发许可证，您必须输入 Apple 提供的 sToken。

空间中多个 Apple App 和图书帐户之间的应用许可证分发

- 如果多个 App 和图书帐户存在相同应用，许可证将按照帐户优先顺序从帐户中进行分发。
- 如果多个 App 和图书帐户存在相同应用，及如果优先级较高的 App 和图书帐户中的应用许可证用完，然后仅在用户或设备显示在下一个优先帐户的许可证分发列表中时，将从下一个优先帐户中为应用分发许可证。
- 在更改 App 和图书帐户的优先级时，许可证将不会撤销和重新分配。 应用将从第一个帐户分发许可证。 如果许可证在第一个帐户中用完，应用将从下一个优先帐户中分发许可证，以此类推。
- 从“App Catalog”页面中，用户可以选择撤销应用的所有许可证。 此操作会从所有可用 App 和图书帐户中撤销应用的许可证。
- 保留的许可证优先于 App 和图书帐户的优先级。

基于设备和基于用户的许可证分发

应用的许可证基于设备或基于用户，取决于您的分配方式。 在将应用许可证分配到设备时，则会变为基于设备的许可证。 在将应用许可证分配到用户时，则会变为基于用户的许可证。

在设备上安装 Apps and Books 应用或为该应用发放令牌时，会分发许可证。 如果该应用无可用的许可证，则用户可选择自行安装并支付应用。 如果用户已为请求的 App 和图书应用分配基于用户的许可证，将使用基于用户的现有许可证安装应用，而不是 App 和图书许可证。

> 至于共享 iPad，将根据基于设备的许可证安装 App 和图书，无论是否选择基于设备的许可证。

使用基于设备的许可证选项

凭借基于设备的许可证，用户不需要注册 App 和图书。 将自动安装需要的应用。 受企业监管的设备无需处理 IT 拥有的 Apple ID。

在设备签入期间，通过序列号识别设备并在具备可用许可证的情况下，安装需要的应用。 如果无可用许可证，则不能安装应用程序。 如果保留应用的许可证，则在应用安装时不会分配基于设备的许可证。

> 管理员使用基于设备的 App 和图书许可，控制已部署应用的应用更新。

要控制应用的更新方法，在**应用 > App Catalog** 中，导航到**应用配置/在设备上安装**选项卡。 您可以选择将在下一次设备签入时立即实施的即时更新，或您可以选择在新版本可用时自动更新应用。

重要事项：在将基于设备的许可证分配到企业对企业 (B2B) 或效率应用之前，请向应用开发商确认此应用有资格使用基于设备的许可证。

使用基于用户的许可证选项

如果需要从一个设备移到另一个设备（万一设备丢失或被盗，或用户升级到新设备），基于用户的许可证仍对该用户有效。 使用基于用户的许可证，用户必须先注册 Apple App 和图书。 注册是终端用户必须在“ App Catalog ”中完成的手动操作。 所需的 App 和图书应用不会安装到设备，直到用户注册 App 和图书。

如果应用是所需的 App 和图书应用并且许可证分发基于用户：

- 如果用户未注册 App 和图书计划，将不会安装所需的应用。
- 如果用户注册 App 和图书计划并且许可证可用，将安装所需的应用。
- 如果用户已注册 App 和图书，但没有可用的许可证，将无法安装应用。

将 App 和图书应用添加到目录

步骤

1. 转至**应用 > 应用目录**。
2. 选择应用并单击**添加到目录**。 单击**下一步**。
3. 还可选择添加应用程序的说明。 单击**下一步**。
4. 选择分配选项。 单击**下一步**。
5. 单击**应用配置**选项卡。
6. 还可选择**在设备上安装**。 在受监管的 iOS 设备上，此配置选项安装应用，且不会向用户发出提示。
7. 如果需要，选择其他配置选项。

在 App 和图书安全令牌信息页面中，将显示以下令牌详细信息：

- 创建日期
- 位置（如果令牌包含此信息）
- 到期日期

添加 App 和图书帐户

Ivanti Neurons for MDM 允许添加多个 App 和图书帐户，在单个空间内添加多个 Apps and Books 安全令牌即可。

请执行以下步骤，以在空间中添加 App 和图书安全令牌：

1. 转到**应用 > Apple App 和图书**。
2. 单击 **+ 添加 App 和图书 sToken**。
3. 输入名称，并选择令牌文件。
4. 或者，取消选择**向所有用户自动分发 App 和图书应用**选项。 此选项默认选中；在这种情况下，所有用户组用于分发 FCFS 许可证。
5. 或者，选择**清除此前 App 和图书许可证中的所有数据**选项，以移除与此令牌关联的所有应用许可证。
6. 单击**保存**。

在添加帐户后，所有添加的 App 和图书帐户列表将显示在表格中。

更新 App 和图书安全令牌

步骤

1. 转到**应用 > Apple App 和图书**。
2. 单击 App 和图书帐户名称。
3. 在"令牌"选项卡中，单击**更新 sToken**（.stoken 文件）。
4. 输入令牌名称，并选择令牌文件。
5. 或者，取消选择**向所有用户自动分发 App 和图书应用**选项。 此选项默认选中；在这种情况下，所有用户组用于分发 FCFS 许可证。
6. 或者，选择**清除此前 App 和图书许可证中的所有数据**选项，以移除与此令牌关联的所有应用许可证。
7. 单击**更新**。

从"令牌"选项卡中，单击**重新同步 App 和图书许可证使用信息**，以从 Apple App 和图书服务执行所有应用和许可证信息的完整同步。 此操作仅在 Ivanti Neurons for MDM 中的许可证分配信息不正确时必需。 此不准确性可能是由于 Apple App 和图书 API 的不一致性。

更新 App 和图书帐户的优先级

管理员可以为空间中的每个 App 和图书帐户分配优先级，这取决于使用哪些许可证。 App 和图书帐户的优先级用于拥有可预测的许可证分发系统，并在用户或设备有资格从相同应用的多个 App 和图书帐户中接收许可证时解决冲突。

步骤

1. 转到**应用 > Apple App 和图书**。
2. 根据所需的 App 和图书帐户名称，单击**编辑优先级**。
3. 在"编辑优先级"窗口中，选择新优先级。
4. 单击**保存**。

删除 App 和图书安全令牌

移除 App 和图书安全令牌不可逆且具有破坏性。 在移除令牌时：

- 有保留令牌的应用将移除其令牌。
- 已经购买的应用将仍然在目录中，用户可以自行购买这些应用。
- 如果最终用户希望使用通过企业 App 和图书帐户安装的应用，用户需要将其转换到个人帐户。 在此方面，用户拥有 30 天宽限期。

步骤

1. 转到**应用 > Apple App 和图书**。
2. 单击 App 和图书帐户名称。
3. 在"令牌"选项卡中，单击**删除**。
4. 在 App 和图书安全令牌删除窗口中，选择**是，删除 App 和图书安全令牌**选项进行确认。
5. 单击**删除**。

为目录中的 App 和图书应用分发许可证

1. 从主菜单中，选择**应用 > Apple App 和图书**。
2. 系统将显示 App 和图书帐户的列表。 在每个帐户中，将显示通过 App 和图书计划购买的应用列表。
   选择应用并单击**分配许可证**。
3. 在 App 和图书许可证区域的**先到先得**、**已保留**或**已禁止**中，选择分发选项。

查看每个用户的应用许可证

通过"许可证使用"选项卡，您可以查看用户的许可证首选项。

1. 单击**用户**选项卡
2. 选择一名用户。
3. 单击**许可证使用**选项卡。
   显示应用列表，以及 App 和图书许可证类型和许可证分配详细信息。

要查看每个用户的每个应用程序的许可证使用情况：

1. 转到 Ivanti Neurons for MDM 主菜单中的**用户**。
2. 选择一名用户。
3. 默认显示**设备**选项卡。
   单击**许可证使用**选项卡。
   显示用户设备上已安装的所有应用的列表，包括许可证状态。 基于设备的许可证的 App 和图书许可证类型列会列出设备的序列号。
   - 应用程序名称
   - 应用程序版本
   - 应用程序成本
   - 应用程序的分配日期
   - App 和图书许可证类型
   - 操作（许可证状态）
   - 许可证详细信息的平台信息。

您也可以查看每个应用的 App 和图书许可证使用情况：

1. 转到 Ivanti Neurons for MDM 主菜单中的**应用 > 应用程序目录**。
2. 选择一个应用程序。
3. 如果存在，单击 **App 和图书许可证**选项卡。
4. 单击帐户名称。 此选项卡仅显示通过 App 和图书计划购买的应用。

为每个 App 和图书许可证类型显示单独的选项卡。

许可证类型和日志	描述
先到先得 (FCFS) — 您可以选择将获得此类型许可证的用户群体。	• 用户要求的应用 — 用户选择安装的应用。 默认基于用户的许可证 • 所需应用 - 需要以及使用**在设备上安装**设置由管理员配置安装的应用。 这些应用默认使用基于设备的许可证。
保留	保留的许可证优先级高于 FCFS 许可证。 您可以在此选择对该应用拥有保留许可证的用户或设备。
禁止	输入禁止对此应用拥有许可证的用户。 用户仍可以安装应用，但必须购买。
活动日志	显示用户、分配到用户的 App 和图书许可证类型、分配日期，以及对许可证的最新操作。

要查看每个设备上每个应用程序的许可证使用详细情况：

1. 转到 Ivanti Neurons for MDM 主菜单中的**设备**。
2. 选择设备。
3. 单击**已安装的应用**选项卡。
4. 显示已安装到所选设备的所有可管理应用的列表，包括许可证状态。
    - 应用名称
    - 应用程序版本
    - 支持的平台
    - 应用程序的源
    - 应用程序的大小
    - App 和图书许可证类型
    - iOS 应用的应用报告（安装）日期

按如下方式搜索设备上已安装的应用程序：

- 应用名称
- 捆绑包或程序包 ID

App 和图书许可证使用情况通知

App 和图书通知会帮您跟踪 App 和图书许可证使用情况。 通知阈值会定义为如下：

- 在使用超过 50% 的许可证时，系统会发出信息通知。
- 在使用 70-80% 的许可证时，系统会发出警告通知。
- 在使用 90-100% 的许可证时，系统会发出临界通知。

- 在使用情况低于 50% 时，系统会清除通知。

要查看每个应用的许可证信息：

1. 单击**应用 > Apple App 和图书**。
2. 显示的许可证信息包含：
    - 应用程序名称。
    - 许可证成本。
    - 可用许可证数量。
    - 兑换许可证数量。

转到**仪表板 > 通知**，以查看许可证通知的详细信息。

3. 显示“通知”页面。
   单击通知标题，以查看详细信息。 请查看仪表板，以了解可用通知。

App 和图书许可证使用情况通知

触发器	严重等级	通知类型	组件类型
已兑换 50%	信息	许可证使用情况	App 和图书
已兑换 70%	警告	许可证使用情况	App 和图书
已兑换 80%	警告	许可证使用情况	App 和图书
已兑换 90%	提醒	许可证使用情况	App 和图书
已兑换 100%	提醒	许可证使用情况	App 和图书

查看 App 和图书许可证使用情况

特定于用户的许可证使用详细信息在许可证使用情况表的许可证列中显示。

1. 单击应用。
2. 单击**许可证使用**选项卡。
3. 在搜索字段中输入用户名。

撤销应用的 App 和图书许可证

在以下情况时，撤销 App 和图书许可证：

- 设备处于非活动状态（已停用或注销）。
- 删除 App 和图书应用。
- 在设备停用后，将撤销基于设备的许可证。
- 删除 App 和图书令牌。

要撤销应用的 App 和图书许可证：

1. 在**应用 > 应用目录**下选择应用。

2. 如果存在，单击 **Apple App 和图书许可证**选项卡。
3. 请执行以下其中一个任务：
    1. 单击**撤销所有许可证**，以撤销所有用户或设备中的所有许可证。
    2. 单击**活动日志**选项卡。 使用**操作**列，以根据用户或设备撤销个人许可证。

- 对于 iOS 设备，Apple 允许在撤销 App 和图书许可证后，App 和图书应用享有 30 天的宽限期。 因此，App 和图书应用仍可以安装。
- 对于 macOS 设备，在撤销 App 和图书许可证后，该应用仍会保留在设备上。

要撤销用户的 App 和图书许可证：

1. 单击应用。
2. 单击**许可证使用**选项卡。
3. 对于要移除其许可证访问的用户，单击**撤销许可证**。

> 如果删除用户，或用户从设备中移除 MDM 配置文件，将自动撤销 App 和图书许可证。

App 和图书身份验证错误通知

一些身份验证错误可能会在使用 Apple App 和图书服务时发生。 这些 App 和图书身份验证错误通知是：

错误通知	操作
无效身份验证令牌	上传有效 App 和图书 sToken
失效的令牌	使用您公司的帐号生成在线新令牌
此 sToken 已被撤销	上传有效 App 和图书
必须登录	登录 App 和图书服务

macOS 和 iOS 设备的 App 和图书行为

适用于 iOS 的 App 和图书

操作	基于设备的许可证	基于用户的许可证
对于用户，将 App 和图书应用从分发中移除	应用程序在用户设备上卸载	应用程序在用户设备上卸载
取消委派 App 和图书应用	从非默认空间中的所有设备卸载应用程序	从非默认空间中的所有设备卸载应用程序
将 App 和图书应用从默认或自定义空间中删除	从所有设备卸载应用程序	从所有设备卸载应用程序

适用于 macOS 的 App 和图书

操作	基于设备的许可证	基于用户的许可证
对于用户，将 App 和图书应用从分发中移除	应用程序在用户设备上未被卸载	不适用
取消委派 App 和图书应用	在非默认空间中，应用不会从所有设备卸载	不适用
将 App 和图书应用从默认或自定义空间中删除	应用不会从所有设备卸载	不适用

在设备移动空间时使用的 App 和图书许可证授权

在设备移到新空间时，将撤销分配到设备或设备所有者的 App 和图书许可证。 根据新空间的可用性，分配新 App 和图书许可证。

以下是 App 和图书许可证授权方案：

情景	授权
App 和图书许可证分配到源空间中的设备或设备所有者，相同应用的 App 和图书许可证在目标空间中可用。	从目标空间中的 App 和图书令牌分配许可证。
App 和图书许可证分配到源空间中的设备或设备所有者，相同应用的 App 和图书许可证在目标空间中不可用。	从源空间中的 App 和图书令牌撤销许可证。
未将 App 和图书许可证分配到源空间中的设备或设备所有者，安装的任何 App 和图书应用的 App 和图书许可证在目标空间中可用。	从目标空间中的 App 和图书令牌分配许可证。

如果您无法在**应用类别**页面上执行任务，这可能是您没有所需权限。 您需要以下其中一个角色：

- 应用和内容管理

8.19. 目录设置

本部分包含以下主题：

- 更改 Apple 应用管理设置
- 设置默认 App Store 地区
- 启用/禁用 iOS 应用更新
- 启用/禁用应用评级和评论
- 上传或更新 iOS/macOS App 和图书 sToken（许可证：Gold）
- 将 iOS/macOS App 和图书 sToken 从 Ivanti Neurons for MDM 服务中移除

在**应用** > **目录设置**页面中，配置要应用于应用程序目录中所有应用的偏好设置。 可以执行以下操作：

- 包括在设备签入期间的应用更新
- 阻止备份到 iCloud 和 iTunes（仅限 iOS）
- 设置默认应用商店地区（Apple 和 Microsoft）
- 设备取消注册时移除 iOS 应用
- 启用 Ivanti Neurons for MDM“评级和评论”
- 上传 iOS 和 macOS Apps and Books 令牌（需要 Gold 许可证）

更改 Apple 应用管理设置

这些设置将适用于所有应用程序，除非已经为单一应用程序创建了应用管理配置。

1. 选择或清除以下一个或多个复选框：
    - **在设备签入期间更新应用**（默认选中）
    - **阻止备份到 iCloud 和 iTunes**
    - **在取消注册时移除应用**

单击**保存**。

通知

1. 点击**Apple App Store 和 Google Play 商店中提供新的应用程序版本时生成系统通知**下的下拉列表，然后选择以下选项之一：
    - **一周一次**
    - **每天一次**

选择**针对 AppCatalog 中可用的新应用程序更新生成最终用户通知**下的下拉列表，然后选择以下选项之一：

- **一周一次**
- **每天一次**

设置默认 App Store 地区

在 App Catalog 设置中，设置 Apple 和 Microsoft 应用商店的默认地区。

1. 在默认应用商店地区部分中：

- 选择 **Apple App Store 地区**。
- 选择 **Microsoft App Store 地区**。

2. 选择或清除选项，以将上次选择的应用商店地区选择为每个管理员的默认地区。 如果选择此选项，应用商店地区将设置为每个管理员上次选择的地区，并将覆盖之前的设置。 如果这是管理员首次使用此功能，默认应用商店地区将设置为此步骤中之前的设置。
3. 单击**保存**。

启用/禁用 iOS 应用更新

1. 选择或清除**在设备签入期间更新应用。**
   - 默认情况下，此选项被选中。
   - 清除时，任何设备签入（包括通过管理员强制签入）不包含应用更新。
   - 但是，用户可以通过单击设备应用程序目录上的强制检查操作来手动更新应用程序。
   - 新的应用程序安装和所有其他配置和设置将在设备签入期间更新。

单击**保存**。

对于托管应用程序，管理员可以单击应用详细信息页面中的**更新**按钮，以手动从 App Store 中将应用更新到最新版本。

在用户的设备上，用户可以单击“ App Catalog ”菜单上的**强制签入**按钮，以允许设备签入并让应用与其他配置和更新一同更新。

这些设置允许最终用户在应用更新时选择：

- 请等待，直到连接到 Wi-Fi，以避免产生数据费用。
- 在应用更新时，避免在错误时间锁定。

启用/禁用应用评级和评论

这将允许用户对该应用程序进行评分和评论，以供其他用户阅读这些评论。

1. 选择或清除**在最终用户 App Catalog 中启用评分和评论**。
2. 单击**保存**。

> App 和图书 sToken 的格式已更改。 它和之前版本中的字符串不同，现在是以 vpptoken 文件格式保存在文本文件中的字符串。 直接将此文件上传至管理操作台进行处理。 更新 App 和图书帐户页面，以显示 App 和图书组织名称和过期日期。

上传或更新 iOS/macOS App 和图书 sToken（许可证：Gold）

1. 选择**添加 App 和图书 sToken**。
2. 在**别名**字段输入 sToken 文件的名称。
3. 将 sToken 文件拖放到特定区域，或单击**选择文件**，以导航到 sToken 文件。
4. 单击**保存**，或者如果您更新 sToken 文件，单击**更新**。
5. 转到 Apple App 和图书页面，以查看与此令牌关联的应用。

> 如果在 Ivanti Neurons for MDM 的之前版本中为个人用户保留了 Apps and Books 令牌，必须验证令牌仍为这些用户保留，并且可根据需要再次保留这些令牌。

将 iOS/macOS App 和图书 sToken 从 Ivanti Neurons for MDM 服务中移除

您可以撤销用户不再需要的应用，并在需要时重新分配。 如果使用 MDM for iOS/macOS 将应用部署为受管应用，您可以选择立即移除应用和所有数据。

1. 选择要移除的应用。
2. 单击**删除**。
   将显示警告对话框。
3. 或者，您可以为用户授予 30 天优惠期：
   - 保存数据。
   - 购买应用的个人副本。
   - 将本 App 和图书帐户安装的应用转移到个人帐户，以继续使用。

如果您无法在**目录设置**页面上执行任务，这可能是您没有所需权限。 需要以下角色：

- 应用和内容管理

8.20. 部署应用依赖性

在上传内部应用捆绑包时，Ivanti Neurons for MDM 将扫描应用以找出依赖项。 如果找到任何依赖性，将其列在添加应用向导的第三步中。 对于任何应用依赖项，管理员可以选择上传依赖文件。 但在未上传依赖文件的情况下，一些应用可能无法安装。

管理员可以在安装特定应用时选择设置应用依赖关系。 在这种情况下，可以将一个或多个应用与主应用相关联。 用户试图安装主应用时，系统将会通知用户有依赖应用将与主应用一起安装。

> 此功能适用于 iOS、Android、Windows 和 macOS 设备。

请留意以下几点关于应用依赖项和必备项的事项：

- 在应用安装到设备前，管理员可以设置作为必备项的依赖应用。 必备应用可以是内部应用、公共应用、私人应用 (Android) 或 VPP 应用。
- 现在，App Catalog 页面的必备应用列会显示必备应用的计数。 您可将鼠标悬停在数字上，查看必备应用的列表。
- 在触发安装主应用后，必备应用可以直接下载。
- 如果委派主应用，将自动委托关联的必备应用。
- 在移除必备关系前，无法将必备应用从 App Catalog 中删除。
- 多个应用版本可以使用不同的必备应用。
- “审计跟踪”页面将记录 iOS、Android 和 macOS 设备的必备应用的添加、移除和自动委派。
- 如果管理员或最终用户安装具有必备应用的应用，必备应用将在安装主应用之前安装。 如果在安装所有必备应用前签入设备，将卸载所有必备应用。

> 虽然应用需要依赖文件，但 Ivanti Neurons for MDM 不需要您上传任何文件以部署应用。

> 对于 Samsung 设备，管理员应向“Kiosk 模式允许的应用”列表添加必备应用。 添加到允许的应用列表的必备应用不会添加到列入黑名单的应用列表。

> 对于非 Samsung 设备，如果已将主应用添加到“Kiosk 模式允许的应用”列表，则必备应用应在后台静默运行。 只有管理员将必备应用设置为 kiosk 模式时，才可以查看处于 kiosk 模式的必备应用。

> **Windows 设备** - 如果 Bridge 应用是未分发的必备应用，且主应用是以静默方式分发的 .exe 文件。 在移除依赖项后，Bridge 应用将被卸载，但 .exe 会在此步骤后失败。 管理员应确保 Bridge 应用在默认情况下不会被取消分发。

> **Windows 设备** - 当以非静默方式分发主应用且主应用具有未分发的必备应用时，会先成功安装必备应用。 但是，如果主应用安装失败，随后会立即卸载必备应用。 仅当用户触发安装请求时，才会重试失败的主应用。

添加内部应用

1. 转至**应用 > 应用目录**。
2. 单击**添加**。
3. 将应用文件拖动到虚线框中，或者单击**选择文件**以从文件系统中进行选择，然后单击**确认**。
4. 单击**下一步**（右下方）。 Ivanti Neurons for MDM 会扫描应用以查找依赖文件，并将其列在**应用依赖项**表中。

5. 查看应用信息，并确认您已选择正确应用。
6. 单击**操作**列中的上传图标。 系统将显示**上传依赖项**窗口。
7. 单击**选择文件**，以浏览并查找文件的本地副本，然后单击**上传**。
8. Ivanti Neurons for MDM 会扫描可选程序包以查找应用，并将其列在“可选程序包”表中。 如果列出，单击操作列中的上传图标。 系统将显示上传可选软件包窗口。
9. 请核对应用信息，并确认您选择的应用正确无误。
10. 单击**选择文件**，以浏览并查找文件的本地副本，并单击“上传”。
11. 单击**下一步**。
12. （可选）添加应用屏幕截图，并单击**下一步**
13. 如果应用需要其他必备应用。
    1. 从**必备应用**部分中，选择选项**打开**。
    2. 在**添加应用**选项卡下方，搜索必备应用。
    3. 选择应用。
    4. 单击**保存**。
14. 定义应用分发，并单击**下一步**。
15. 定义“应用配置”部分并点击**完成**。在设备下次与 Ivanti Neurons for MDM 同步时，应用将与依赖文件一同部署到设备中。

> 通过单击“添加依赖性”按钮，您可以添加其他依赖性。 在上传时，这些其他依赖性也会列在应用依赖性表格下方。 管理员也可以手动添加仅限内容类型的可选软件包。 此类型的软件包不依赖于版本。

添加必备应用

您可将必备应用添加到主应用。 您可为不同版本的主应用添加不同必备项。 App Catalog 页面将提供选项，支持您保留与现有应用版本相同的描述、脚本、屏幕截图、分发、必备应用和应用配置，或更改关联的所需应用。 在未移除与主应用的关联关系的情况下，无法删除必备应用。

现在，审核线索页面将在特定字段中显示支持的必备应用，如下所示：

“审计跟踪”页面中受支持的 iOS、Android 和 macOS 应用的“必备应用”部分将显示以下字段：

appVersionId

名称

platformAppId

系统将显示包含以下字段的自动委派或取消委派的必备应用：

dmPartitionDistributionType

dmPartitionDistributionReason

步骤

1. 从 **App Catalog** 中，选择应用。
2. 单击**编辑**。
3. 向下滚动到**应用委派**，并选择**将此应用委派到所有空间**选项。
4. 单击**保存**。

如果委派多个应用，并选择从主应用中删除委派，必备应用不会自动从委派中移除。

8.21. 使用 Android Enterprise 部署 Divide Productivity

Divide Productivity 是一个 PIM 应用程序，可以部署到 Android Enterprise 设备上。

1. 转至**应用 > 应用目录**。
2. 在**企业应用**下方，点击 **Divide Productivity**。
3. 输入其他目录或说明。
4. 单击**下一步**。
5. 接受已显示的权限。
6. 单击**下一步**。
7. 选择分配选项。
8. 展开**高级选项与应用配置**。
9. 按照以下指导方针启用相关选项：
10. 选择升级选项。

设置	流程
阻止用户卸载此应用	选择以阻止最终用户在此应用静默安装时将其卸载。
邮件地址	使用变量定义电子邮件地址，以将其与应用关联。
密码	使用变量为电子邮件帐户定义密码。 如果您将此字段留空，系统会提示用户输入密码。
主机	输入要使用的邮件服务器主机名。 输入 ActiveSync 服务器的完整合格域名。 如果您正在使用独立式 Sentry，则需要输入完整合格域名 (FQDN)。 示例： mySentry.mycompany.com
服务器类型	选择邮件服务器的类型。
用户名	使用变量为电子邮件帐户定义用户名。
需要 SSL	在将使用 https 安全通信连接到您在“主机”字段中指定的服务器时选择。
信任所有证书 默认电子邮件签名	仅在您要让应用自动接受不信任证书时选择。 通常，仅在测试环境中工作时选择此选项。 输入所有电子邮件的默认电子邮件签名。 最终用户可随时对此进行更改。 设备用户更改后，则对此字段的后续更改均无效。
电子邮件最大附件大小	输入允许附加文件的最大大小。
启用任务	选择以同步任务。
登录证书别名	输入登录证书的别名。
签名证书别名	目前不支持。
Smime 加密证书别名	目前不支持。
高级选项	
在设备上安装	选择以提示用户安装应用。
在 Samsung Knox 设备上进行静默安装 不在最终用户应用目录中显示	选择以便自动在 Samsung Knox 设备上安装应用程序。 在您不想让应用显示在设备上的应用目录中时选择。

11. 单击**完成**。

8.22. 设置配置器应用程序

本部分包含以下主题：

- 配置要求
- 启用 Android Beam 使用 NFC Bump
- 配置企业拥有的设备
- 注册设备
- 验证设备注册状态

Provisioner 是 Ivanti Neurons for MDM 应用程序，用于配置企业拥有的设备，使其可注册为工作托管设备并置于设备所有者模式。

企业托管的设备仅包含企业配置文件，而没有个人配置文件。 管理员可在设备上设置 20 多个锁定，从而限制设备功能，例如照相机、电话、短信、网络和更多内容。

使用 NFC bump 初始化 Android Enterprise 目标设备配置的设备需要 Provisioner 应用程序。 要配置企业拥有的设备，请在主设备上安装 Provisioner 应用，并使用 NFC（近场通信）Bump 配置新设备。 Bump 可将两个设备绑定。 使用其中一个客户端应用配置设备：

- Go 与 Ivanti Neurons for MDM 一起使用
- At Work UEM，非品牌的客户端应用，可与 Ivanti Neurons for MDM 一起使用。

配置要求

要将企业拥有的 Android Enterprise 设备配置为工作托管设备：

- 企业拥有的原生 Android Enterprise 设备必须在配置前恢复出厂设置。
- 必须定义 Android Enterprise 配置并应用于 Android 设备组。
- 安装 Provisioner 应用后，启用 NFC 的 Android 设备旨在用作主设备或模板。
- 配置 Android Enterprise 设备。
- Provisioner 应用程序
  从 Google Play 下载适用于 Android 的 Provisioner 应用。

启用 Android Beam 使用 NFC Bump

步骤

1. 转到设备上的**设置**。
2. 转到**无线和网络**，然后点击**更多**。
3. 选择 **NFC** 复选框。
4. 单击 **Android Beam 并滑动开关以开启**。

> 具体步骤会因您的设备而异。

配置企业拥有的设备

步骤

1. 在设备上安装的 Provisioner 应用可用作 Android 主设备。
2. 在主设备上启动 Provisioner。
3. 从下拉菜单中选择应用程序。
4. 输入 Provisioner 应用程序所需的信息。 如果存在支持的无线网络类型，则某些字段 可能会自动填充。 使用这些 指导原则：

字段	值
选择要配置的应用程序	Go（选择与 Ivanti Neurons for MDM 一起使用） At Work UEM，非品牌的客户端应用，可选择与品牌 Ivanti Neurons for MDM 一起使用。
WiFi 网络 SSID	输入主设备要使用的 WiFi SSID。
WiFi 安全类型	输入 WiFi 安全类型
WiFi 密码	输入 WiFi 密码
时区	输入当地的当前时区
区域设置	输入区域设置

5. 单击**继续**。
   将在主设备上显示**接触设备**屏幕。
6. 开启目标设备并显示 Android 欢迎 屏幕后，将主设备与目标设备背对背放置， 以开始 NFC 传输。
   如果 NFC 传输成功时，目标设备会发出声音提示， 然后继续下载选定的客户端应用。 如果该设备 未加密，则在继续前将开启加密过程。
7. 通过接触设备，继续配置其他设备。 目标设备必须显示“欢迎”屏幕，主设备必须显示**接触设备**屏幕。

注册设备

在使用 NFC Bump 配置企业拥有的设备后，将安装选定客户端应用。 启动客户端应用并注册设备。

验证设备注册状态

步骤

1. 转至**设备 > 设备**。
2. 单击设备的链接，以查看详细信息。
3. 左侧窗格中列出了设备的状态。

8.23. 管理 Windows 应用程序

用户可以管理（导入、配置、计划、分发、更新和移除）Windows 应用程序的完整应用程序生命周期。 MDM 控制台支持应用程序分发和应用程序更新流程。 有关管理 Windows 应用程序和其他应用程序的更多详细信息，请参阅应用配置、应用见解和应用目录。

支持的应用程序类型

- 内部（选中应用目录部分的**添加内部应用程序**选项）
- MSB（Microsoft Store for Business 集成）
- 公共商店（通过本机 Microsoft Store 集成）Microsoft Store 地区可以在"应用程序">"目录设置"中设置。 有关详细信息，请参阅应用目录部分的**从公共商店添加应用程序**。

支持的应用程序扩展名

- MSI
- MSIX
- APPX
- APPX 捆绑包
- EXE（通过 **Ivanti Bridge**）

应用程序控制

应用程序控制配置可以控制每个设备的应用程序安装。 有关详细信息，请参阅**应用控制配置：控制每个设备上安装哪些应用**。

程序包和依赖项

具有以下不同功能：

1. Windows 应用程序可以设置为所有应用程序类型的先决条件。 有关如何设置应用程序先决条件的信息，请参阅**部署应用依赖性**。
2. APPX 和 APPX 捆绑应用程序依赖项和其他程序包依赖项。 在**查看应用详细信息**页面，查看**应用程序依赖项和其他包**部分。
3. Win32 应用程序支持选择正确的产品代码 (MSI) 以及命令行和变量。 常见命令行选项列表请参见**此处**。

脚本

通过 Ivanti Bridge 客户端支持脚本。 有关设置脚本的信息，请参阅 **Ivanti Bridge**。

在设备上安装 Ivanti Bridge 后，可以按照如下方式分发脚本：

- 在设备级别通过 Ivanti Bridge 操作的脚本和操作
- 通过 Ivanti Bridge 配置（转到**配置 >Bridge**）

检查设备上的现有版本复选框，可在内部 MSI 和 EXE 应用程序的**脚本和文件** 选项卡中使用，它控制应用程序在 Windows 设备上的安装方式。 启用此选项时，设备会运行签入以验证应用程序是否已安装并识别其版本。 Ivanti Neurons for MDM 仅在应用程序不存在或安装的版本早于所需版本时安装或升级应用程序。 如果存在相同或更新的版本，则会跳过安装。 此选项要求在启用应用程序之前至少将应用程序安装在一台设备上。

安装前和安装后脚本与文件

对于 .exe 文件和 .MSI 文件

您可以配置安装前和安装后 PowerShell 脚本、注册表脚本和 Windows 可执行 (.exe) 文件，并在应用程序详细信息级别为 Windows 应用程序下载其他类型的文件。

在添加新的安装前或安装后脚本或文件时，将显示 Ivanti Bridge 屏幕。 您可以附加脚本或文件，添加脚本参数，还可以为文件提供目标位置。 必须在设备上成功执行安装前脚本，然后才能向设备发送应用程序安装命令。 安装前和安装后脚本与文件的执行/安装顺序将与它们上传至控制台的顺序相同。 如果安装前脚本下载或安装失败，应用程序将无法继续安装。

如果安装后脚本失败，可以在“设备日志”小节下方的“设备详细信息”页面中查看错误。 此外，如果安装后操作失败，则无法还原安装前脚本/下载的文件和安装的 .exe 文件。

可以使用“为脚本和文件排定优先顺序”选项对安装前或安装后脚本和文件进行重新排序。 仅当至少有两个或更多脚本或文件可用时，才能使用此选项。 通过此选项，可以将文件或脚本拖放到其各自的安装前或安装后部分，而不是从一个部分拖放到另一个部分。

安装行为和配置

Windows 应用程序支持以下功能：

- 无提示安装
- **Windows 应用计划**
- 重新启动选项

有关管理安装行为选项的更多详细信息，请参阅**应用配置**。

> MSI 应用程序和 EXE 应用程序（使用 Bridge 安装）支持通过无用户 MDM 会话进行安装。

例如，在以下情景中：

- 设备重新启动，尚无用户登录
- 用户从 Windows 会话注销
- 设备注册加入 Autopilot 无用户（自助部署或预配置）模式
- 应用程序安装在设备级别

> 这可以实现更高效的 MSI 应用程序安装，例如，Auto-pilot 注册期间或无人使用 Windows 设备的夜间。 在 MSI 中对 EXE 使用简单封装时，可以进行安装操作，但不能升级和删除。 实际 MSI 程序包与 CSP 有关联。 用户登录后将安装其他应用程序类型。

Tunnel Windows 版（依应用程序 VPN）

Tunnel 是一款独立原生 Windows 应用程序。 该应用程序当前在 Microsoft Store 提供，可分发到设备。 创建依应用程序 VPN 配置。 需要 Sentry 部署。 要配置 Tunnel 应用程序，请转到**配置** > **+添加** > 搜索 Tunnel（选择支持 Windows 设备的配置）。 选择 Sentry 配置文件和配置设置，通过 Sentry 开始为应用程序数据创建隧道。 要设置 Sentry 服务器，请转到**管理员** > **基础设施** > **Sentry**。

应用库存

Windows 设备组上安装的应用程序和软件清单可以按两个级别进行跟踪：

- 要检查设备上安装的应用程序，请转到**设备** > **应用程序清单**
- 要按设备级别查看清单，请转到“设备”> 选择设备 > 点击“安装的应用程序”

管理员可以设置 Windows 应用程序清单收集间隔。 转到“管理员”>“应用程序清单间隔”。当隐私配置设置为从设备收集所有应用程序时，系统将使用该间隔。 要配置“隐私配置”，请转到“配置”>“+添加”> 搜索“隐私”> 选择“收集设备上所有应用程序的清单”。 选择要收集的设备类型。

企业应用程序目录 (Apps@Work)

客户可以使用 Apps@Work 在 Windows 设备上启用企业目录。 Apps@Work 可以通过 Neurons for UEM 中的“应用程序目录”进行部署。 有关详细信息，请参阅**Apps@Work（iOS、Android、Windows 和 macOS）**。

8.24. Ivanti Bridge

本部分包含以下主题：

- Bridge 支持的文件类型
- Bridge 设置
- Bridge 日志
- Bridge 上次签入
- Bridge 服务故障恢复

Ivanti Bridge 利用单个控制台和通信通道针对 Windows 10 统一移动端和桌面操作。 它会将 UEM 功能扩展为管理电脑，并允许组织充分利用显著减少的成本和提高的效率，同时确保电脑和移动设备之间实现一致的安全性。 利用 Ivanti Bridge，企业能够像对支持的 Windows 移动设备那样，对 Windows 10 桌面设备使用单一协议，以便向操作系统上的旧版应用程序发送信息。

Ivanti Bridge 让 IT 部门可以在 UEM 上实现 Windows 操作的现代化，而不牺牲关键功能。 IT 部门可以应用已有的策略和脚本，而无需系统图像、域加入或与设备的多个通信通道。

利用 Ivanti Bridge，组织现在可以：

- 通过 UEM 完全控制 PC
- 远程无线管理 PC
- 降低对台式计算机的需求
- 通过由 UEM 部署的 PowerShell 脚本，利用基于 GPO 的命令
- 轻松编辑和管理注册表
- 轻松部署非 MSI 封装的 Win32 应用程序和 Win32 应用商店应用程序
- 获取文件系统的可视性

> Windows 11+ 设备和 ARM 处理器支持 Ivanti Bridge。 Ivanti Bridge 不支持 Windows 10 家庭版桌面设备。

Bridge 支持的文件类型

Ivanti Bridge 支持以下文件类型：

- PowerShell
  PowerShell 脚本会推送到使用 Bridge 支持命名参数的设备。
  64 位Windows 10 桌面设备支持 64 位PowerShell 脚本。

> 将 PowerShell 脚本发送到设备后，服务器端等待结果的 Bridge 超时时间约为 20 分钟。 超时记录为失败。 但是，设备上的脚本会继续工作。

> 设备端等待 PowerShell 脚本进程执行的 Bridge 超时时间约为 60 分钟。 60 分钟后，进程将被终止，脚本的输出不会被保存，并且会向服务器发送新的失败消息。

> 服务器端和设备端超时记录为失败。 如果第二个超时时间已过，并且脚本生成了一些输出，则服务器端不会记录任何输出。

注册表

- VB 脚本
- .EXE for Win32 应用部署
- Win32 应用商店应用程序使用 WinGet 工具来安装和卸载应用程序。

> 如果管理员需要将 Win32 (.EXE) 文件推送到设备（例如，作为 Windows 内部应用），则将自动使用 Bridge 功能（如果可用）。 必须输入参数以静默运行该文件（例如，/SILENT 或/ VERYSILENT）。
> .EXE 应用使用管理员 PowerShell 模式通过 Bridge 安装。 对于 Windows 设备，要使用用户凭据安装，选择“以用户身份运行”选项。

> 管理员应在**应用程序安装程序 - 设置**中选中**以用户身份运行安装程序**复选框，以便为用户安装应用程序。 如果您希望在系统级别安装应用程序，请勿选中该复选框。

使用 Ivanti Bridge 可以增强设备的以下关键领域。

- **注册表：**读取、写入和更新注册表值。
- **文件：**验证、读取和更新文件内容。
- **应用部署：**增加将基于 .EXE 的应用部署到桌面设备的功能。 这些应用程序可以位于 Ivanti Neurons for MDM 服务器中，也可以位于 Cloud 的内容交付网络 (CDN) 中。

Bridge 设置

设置 Ivanti Bridge 要求管理员按以下顺序完成下列步骤：

1. 激活 Bridge 许可证
2. 安装 Bridge 应用程序
3. 将脚本上传到设备以供设备永久或一次性使用

激活 Bridge 许可证

Ivanti Bridge 在旧版 Gold 程序包和现行版 Secure UEM 程序包中。

安装 Bridge 应用程序

激活 Ivanti Bridge 许可证后，Bridge 移动应用程序可以按如下方式安装：

1. 转至**应用 > 应用目录**。
2. 点击 **+ 添加**。
3. 点击“企业应用程序”部分中的 **Ivanti Bridge**。
4. 根据获取的许可证，添加详细信息、自定义并将 Bridge 移动应用分配到所需的设备。
   如果已启用**在 Windows 设备上静默安装**选项，将以静默方式安装 Bridge 移动应用，并且 Bridge 服务将开始在设备上运行。

> Bridge 应用会默认添加到 App Catalog，并且也默认分发到所有设备。

> 将最新版本的 Ivanti Bridge 导入租户目录后，管理员可以查看新调整的应用程序版本。

将脚本上传到设备

通过创建新 Bridge 配置，管理员可以将脚本上传到设备，以供永久使用：

1. 转到**配置 > + 添加**。
2. 选择 **Ivanti Bridge for Windows 脚本和操作配置**。
3. 输入配置的名称。
4. 输入描述。
5. 在配置 Ivanti Bridge 部分中，使用以下两个选项之一上传脚本：
   - 从脚本库中选择脚本 - 从列表中选择一个可用脚本。
   - 或者
     上传脚本 - 按照步骤 7 中的表格所述指定设置。
     - 输入**脚本文件**类别设置，以指定要推送或在设备上执行的安装脚本。
     - （可选）输入**撤销脚本文件**类别设置，以指定要推送或在设备上执行的卸载脚本。 这将在设备停用或配置删除等情景中非常有用。
     - （可选）选择选项**配置 Outlook**，以使用 Bridge 将 Microsoft Outlook 配置到设备。

       > 仅在 Outlook 2010 和 2013 上支持。

点击**下一步**。

7. 选择此配置的分配水平。
   将自动为这些设备操作完成强制签入。

类别	设置	流程
	名称	输入用于识别此配置的名称。
	说明	输入阐明此配置目的的说明。
脚本文件	**所有版本（Windows 10+ 桌面）**	
	脚本文件	选择有效的脚本或可执行文件（.ps1、.reg、.exe）。 • 指定脚本文件或可执行文件（.ps1、.reg、.exe）将自动执行。 • 其他文件类型将仅复制到目标文件夹。
	脚本参数	为脚本文件指定参数列表。 • 对于 Win32 (.exe) 文件，输入参数以静默运行文件（例如 /SILENT 或 /VERYSILENT）。 这是必要操作。
撤消脚本文件	目标文件夹	为脚本文件指定目标文件夹。 • 如果目标文件夹未指定，则 %TEMP% 系统环境变量的值会用作目标文件夹。
	所有版本（Windows 10+ 桌面）	
	脚本文件	选择有效的脚本或可执行文件（.ps1、.reg、.exe）。 • 指定脚本文件或可执行文件（.ps1、.reg、.exe）将自动执行。 • 其他文件类型将仅复制到目标文件夹。
	脚本参数	为脚本文件指定参数列表。 • 对于 Win32 (.exe) 文件，输入参数以静默运行文件（例如 /SILENT 或 /VERYSILENT）。 这是必要操作。
	目标文件夹	为脚本文件指定目标文件夹。 • 如果未指定目标文件，则将默认使用 %TEMP% 系统环境变量的值。

将脚本上载到设备，以供一次性使用

管理员可以将脚本上传到设备，以便一次性（临时）使用。

1. 转至**设备 > 设备**。
2. 单击设备名称连接，以转到“设备”详细信息页面。 这是将推送/执行的一次性脚本的 Windows 10 桌面设备。
3. 点击 ⋮ 图标，然后点击**通过 Ivanti Bridge 的脚本和操作**。
4. 输入名称。
5. 在“脚本文件”部分中，按照上述表格中的描述指定要在设备上推送/执行的脚本。
6. 点击**应用**。
   脚本执行将加入队列，并可能需要一段时间才能完成。 转到“日志”选项卡，以检查并查看状态（输出或故障消息）。 将自动为这些设备操作完成强制签入。

Bridge 日志

此功能让您可以拉取单个设备的 Ivanti Bridge 日志，从而对应用程序进行故障排除和诊断。 日志将在下一次设备签入时发送。 您可以等待下一次计划的同步或执行强制设备签入，以快速获取日志。

要从设备提取日志：

1. 转至**设备 > 设备**。
2. 单击设备名称连接，以转到“设备”详细信息页面。 这是将推送/执行的一次性脚本的 Windows 10 桌面设备。
3. 点击 ⋮ 图标，然后点击**拉取 Ivanti Bridge 日志**。 随即将显示**拉取 Ivanti Bridge 日志**窗口。
4. 选择下列选项之一：
   单一日志 - 请求 Ivanti Neurons for MDM 提取设备上的最新 Bridge 日志。
   全部日志 - 请求 Ivanti Neurons for MDM 提取设备上的日志（至多 30 天）。
5. 单击**提取日志**。 在设备将日志发送到 Ivanti Neurons for MDM 后，您可以在“设备详细信息”页面的“日志”选项卡中查看 Bridge 日志。

> 只有使用**所有日志**选项发送的日志，才可以下载为 zip 文件。

Bridge 上次签入

“Bridge 上次签入”列中列出了 Bridge 服务在“设备”页面上的最后一次签入日期和时间。 可以使用“自定义列”选项将该列添加到“设备”页面，默认情况下此列不可见。

要显示此列，请选择**设备** > **自定义列** > 选择 **Bridge 签入**。

> 在适用的情况下，导出的数据还将包含 Bridge 上次签入的详细信息。

Bridge 服务故障恢复

Bridge 服务故障恢复已引入 Bridge 2.1.14 版本。 默认情况下，此版本将针对所有用户导入到 App Catalog 中。 在极少数情况下，Bridge 服务可能会在没有任何已知原因的情况下发生故障。 这种情况下，Bridge 2.1.14 和更新版本中提供相关支持。

9. 内容

使用“内容”页面，以分发由外部来源托管的内容。 内容可能包括用户可以下载的文件，例如销售演示文稿、图像、电子表格和文档。

本部分包含以下主题：

- 管理内容
- 类别

9.1. 管理内容

本部分包含以下主题：

- 分发托管内容
- 删除内容

托管内容支持使用外部 URL 分发可下载的内容。 外部 URL 应仅定向到可下载的 PDF 或 EPUB 或 IBOOK 文件，外部 URL 必须有这些扩展名。

不支持分发 VPP 图书许可证，因此不支持根据 iTunes Store ID 分发 Apple Books。

使用设备中的 Books 或 Pages 应用，访问 Ivanti Neurons for MDM 推送的内容。 您可以在 Library 部分访问。

可将 **iBook 和 EPUB** 内容分配到 iOS 8+ iPad 设备（Gold 许可证）。 这些格式仅限于 iPad，因为 Apple 仅支持针对 iPad 的上述格式的内部分发。 此限制不适用于 iOS 9 设备。

> 内容预览不支持这些格式。

针对 **PDF** 内容，您可选择将文档推送到 iOS 8+ 设备上的 iBook 应用。

分发托管内容

虽然您无法将新文档上传到 Ivanti Neurons for MDM，但您可以提供路径 (URL)，内容可以在其中托管并分发到设备组。

步骤

1. 转到**内容 > 托管内容**。
2. 单击 **+ 添加**。
3. 输入以下信息：
   - 标题
   - 作者
   - 类别
   - （可选）描述
4. 在**托管内容路径**字段中，输入您要上传的文件的 URL。
5. 单击**下一步**。
6. 对分配做出必要的更改。
7. 单击**完成**。

要修改托管内容，需要删除以前的内容，并添加和分发新托管内容。

要修改 URL 以外的设置：

1. 转到**内容 > 托管内容**。
2. 单击**名称**列中的文档链接。
3. 单击“编辑”图标。
4. 进行所需的更改。

5. 单击**下一步**。
6. 对分配做出必要的更改。
7. 单击**完成**。

删除内容

1. 单击**名称**列中的文档链接。
2. 选择**操作 > 删除此文档**。
3. 单击复选框以确认。
4. 点击**删除文档**。

删除文档时：

- 会将它从系统中移除。
- 它不会再存在于内容目录中。
- 会将它从下载设备中移除。

如果您无法在**内容**页面上执行任务，这可能是您没有所需权限。 需要以下角色：

- 应用和内容管理

9.2. 类别

本部分包含以下主题：

- 添加类别
- 移除类别

> 作为 2017 年 4 月 15 日公布的“内容支持终止”的一部分，添加新内容的功能已被禁用。 目前上传的内容仍然可以分发到 Apple iBooks 应用程序并使用。

类别描述了{{内容目录}}中的{{内容}}的类型。 类别可帮助组织内容，因此易于用户查找所需内容。 添加至内容目录中的每一项必须至少分配有一个类别。

添加类别

步骤

1. 单击**添加**（左下角）
2. 输入类别名称。 类别不区分大小写。
3. 单击**保存**。

移除类别

可以点击类别旁边的 X 来删除类别。

如果您无法在**类别（内容）**页面上执行任务，这可能是您没有所需权限。 需要以下角色：

- 应用和内容管理

10. 配置

配置是发送到设备的设置的集合。 例如，您可以使用配置自动设置设备上的 VPN 设置和通行码要求。 系统的现有配置在“配置”页面列出。

本部分包含以下主题：

- 使用配置
- 创建用户自助服务门户配置
- 自定义配置
- 使用自定义配置向设备推送 SyncML
- 主屏幕布局配置
- 应用控制配置：控制每个设备上安装哪些应用
- 应用通知配置
- 导出配置
- 确定配置的优先级
- 管理配置

10.1. 使用配置

本部分包含以下主题：

- 筛选配置的显示
- 添加配置
- 分发配置
- 配置的缓慢推出分发
- 将配置推送到多个设备
- 排除配置
- 推送已排除配置
- 导出配置
- 导入配置
- 编辑配置
- 删除配置
- 计划内部应用更新
- 需要活动用户会话的 Windows 配置

配置是管理员发送到设备的设置集合。 例如，您可以使用配置自动设置设备上的 VPN 设置和通行码要求。 配置页面中列出了您系统的现有配置。 您可以从“配置”页面中选择多个配置，并将其一次性推送到多个设备。 可以将这些配置推送到特定空间的设备，而其他空间的设备不受影响。 可以将配置推送到单个空间或一次性推送到多个空间或所有空间。

有多种可用的配置类型。 它们分为以下基本类别：

- 安全
- 用户资源
- 企业网络访问
- 移动电话网络
- 其他（更多配置）

对于大部分配置，您可以执行下列操作：

- 添加
- 编辑
- 克隆
- 删除
- 从特定设备排除一个或多个配置
- 将一个或多个排除的配置推送到特定设备

某些配置有操作限制：

- 一些配置无法添加或克隆。 iOS 激活锁定是此类型配置的示例。 因此，在您添加配置时，这些配置不会出现在列出的磁贴中。 这些配置仅在“配置”页面列出。
- 系统定义的配置不能进行编辑或删除。 针对 iOS 注册的 SCEP 是此类配置的示例。

- 某些配置可以标记为无法从设备中删除或重新安装。 这些配置不能排除或推送到设备。

筛选配置的显示

在查看**配置**页面时，将列出所有配置。 要将此列表缩小为特定配置，请使用 OS 和配置类型中的筛选器（左侧窗格）。 例如，要缩小列表仅显示 macOS 配置，请在 **OS** 部分中选择 **macOS**。

通过从下拉列表中选择多个空间，您可以查看所有或多个空间设备之间的配置。 在您将鼠标悬停在显示的配置上时，系统将显示带有空间列表的弹出窗口。 您可以单击空间，以显示配置详细信息页面。

在 **Apple DDM** 下应用**受支持**的筛选器，以轻松识别与 DDM 相关的配置，并更好地区分配置类型。

要按名称搜索现有配置，请在**搜索**字段中输入配置名称。

从 Ivanti Neurons for MDM 81 版本开始，全局管理员可以委派空间管理员，并为所有设备和自定义分发选项编辑动态生成的身份证书。

添加配置

仅在下拉列表中选择一个空间时，才启用此选项。

> 您一次可以分发最多 100 个配置文件。

步骤

1. 单击**添加**。
2. 选择您要创建的配置类型。
3. 单击**下一步**。
4. 如果您不希望立即启用此配置，请清除**启用此配置**选项。
5. 选择配置的分配水平。
    - **所有设备** - 将配置分发到所有可用设备。 要跨空间委派配置，请选择以下其中一个选项：
        - **不应用到其他空间**。
        - 要跨空间委派配置，选择**分发摘要** > **应用于其他空间中的设备**。
            - 选中**允许空间管理员编辑分发**复选框，允许委派空间管理员编辑特定空间的分发。
    - **无设备** - 选择此配置，以便在稍后某个时间分发。
    - **自定义** - 定义将为其发送此配置的特定设备集。 要跨空间委派配置，请选择以下其中一个选项：
        - **不应用到其他空间**。
        - **分发摘要** > **应用于其他空间中的设备**。
            - 选中**允许空间管理员编辑分发**复选框，允许委派空间管理员编辑特定空间的分发。

      > 管理员可以使用自定义分发选项，将自定义配置分发到设备、设备组、用户和用户组。 下列配置不支持对用户或用户组进行配置分配或分发：

        - Android Enterprise：工作配置文件 (Android for Work)
        - Android Enterprise：工作托管设备 (Android for Work)
        - Android Enterprise：带有工作配置文件的托管设备/公司拥有设备上的工作配置文件
        - 适用于工作托管设备非 GMS 模式 (AOSP) 设备的 Android 工作托管设备（设备所有者）

6. 如果服务已定义空间，指定配置是否应应用于其他空间，以及优先级。
7. 单击**完成**。

> 如果配置负责向设备发出命令，而不是在设备上安装配置文件，配置详情将不会在应用至任何设备时列出此配置。

分发配置

全局管理员可以委派空间管理员，并为所有设备和自定义分发选项编辑动态生成的身份证书。 对于动态生成的证书，您可以选择**允许此配置在所有空间中可用**选项。 启用此选项，所有空间可以使用动态生成的身份证书，并且可在 Exchange、Wifi、VPN 和任何其他适用配置中使用，其中包含托管应用配置。 此选项可用于仅将动态生成的身份证书作为关联配置的一部分分发给（非默认空间中的）设备且不作为单独配置分发的情况。

程序

1. 根据适用情况，使用表中为单独配置指定的信息指定设置字段。
2. 单击**下一步**。
3. 选择**启用此配置**选项。
4. （可选）选择**允许此配置在所有空间中可用**。
5. 选择下列分配选项之一：
    - **所有设备**。 选择下列选项之一：
        - **不应用到其他空间**。
        - **应用于其他空间中的设备**。
        - **以最高优先级应用于其他设备空间中的所有设备**。 （这仅适用于 Wi-Fi 配置。）
        - **以最低优先级应用于其他设备空间中的所有设备**。 （这仅适用于 Wi-Fi 配置。）
            - 选中**允许空间管理员编辑分发**复选框，允许委派空间管理员编辑特定空间的分发。
    - **无设备**（默认）
    - **自定义**选择以下其中一个选项：
        - **不应用到其他空间**。
        - **应用于其他空间中的设备**。
        - **以最高优先级应用于其他设备空间中的所有设备**。 （这仅适用于 Wi-Fi 配置。）
        - **以最低优先级应用于其他设备空间中的所有设备**。 （这仅适用于 Wi-Fi 配置。）
            - 选中**允许空间管理员编辑分发**复选框，允许委派空间管理员编辑特定空间的分发。

> 无论空间如何，动态生成的身份证书可以配置到所有空间，分发到所有设备并应用于其他设备空间中的所有设备。

6. 单击**完成**。

配置的缓慢推出分发

使用**自定义**选项分发配置时，您可以使用慢速推出流程分发配置，以便及时推出配置。 可以手动或计划的方式计划缓慢推出分发。

> 缓慢推出分发目前仅支持 VPN 和 Wi-Fi 配置。

步骤

1. 转到**配置** > **添加**。
2. 搜索所需的配置。
3. 输入**名称**、**描述**等详细信息。 根据配置，然后单击**下一步**。
4. 选择**自定义**作为分发选项。 屏幕上将显示**缓慢推出分发**部分。
5. 选择**使用缓慢推出分发方法**。 **手动推出**和**按计划推出**选项显示在屏幕上。
   - **手动推出** - 使用此选项，您可以手动设置分发目标的百分比。 将仅完成指定的分发百分比。 或者，您可以选择**选择摘要中的所有设备**，将配置分发到所有设备。
   - **按计划推出** - 使用此选项分四个阶段推出分发。 对于每个阶段，您可以指定推出百分比，确保每个后续阶段的百分比高于上一个阶段。 阶段之间的持续时间必须至少为一天，且不能超过 30 天。 最近保存的配置将自动预加载为可编辑模板，以供将来配置使用。
6. 选择配置必须分发到的所需组。
7. 单击**完成**。

您可以从**配置** > 新创建的配置 > **详细信息**来查看详细信息。 在详细信息页面中，您可以暂停和恢复推出。

> 使用计划部署创建新配置时，在创建现有配置时提供的百分比会转移到新配置。 您可以编辑详细信息或以相同的百分比继续操作。

将配置推送到设备

如果要在设备上重新安装任何排除的配置，您可以推送配置。

步骤

1. 转到**设备** > **设备**。
2. 单击设备名称可查看详细信息页面。
3. 转至**配置**。
4. 选中复选框，以便选择要推送到设备的特定配置。
5. 单击**推送配置文件**。
6. 要推送单个配置，单击**操作**列下方的**推送**。

将配置推送到多个设备

在配置页面中，您可以选择多个配置，并将其一次推送到多个设备。

步骤

1. 登录到 Ivanti Neurons for MDM 管理员门户。
2. 转至**配置**。
3. 选中复选框，选择特定配置。
4. 单击**操作**，选择**将选定配置推送到设备**。 系统将打开推送配置向导，并显示所有配置及其推送状态。
5. 单击**推送有效配置**。 配置会批量推送到所有设备。 对于从**设备** > **配置**选项卡为特定设备排除的配置，它们将不会推送。

排除配置

通过将一些之前分发的配置排除，可手动将其从设备中移除。

步骤

1. 转到**设备** > **设备**。
2. 单击设备名称可查看详细信息页面。
3. 转至**配置**。
4. 选中复选框，选择特定配置。
5. 单击**排除配置文件**。

要排除单个配置，单击**操作**列下方的**排除**。 现在，已排除配置选项卡下方会显示选定配置。

推送已排除配置

步骤

1. 转到**设备** > **设备**。
2. 单击设备名称可查看详细信息页面。
3. 转到**配置** > **已排除配置**。
4. 选择要推送到设备的一个或多个配置。
5. 单击**推送配置文件**。
6. 要推送单个配置，单击**操作**列下方的**推送**。

导出配置

您可将选定配置或所有配置的详细信息从选定空间导出到单个文件。

步骤

1. 转至**配置**。
2. 选中复选框，选择特定配置。
3. 单击**操作** > **导出选定配置及详细信息**。 如果要导出所有配置，选择**导出所有配置及详细信息**。
   .ZIP 文件包含一组 YAML 文件。 报告包含选定空间中的所有现有配置的详细信息。

导出所有配置

导出要发送的配置文件，以支持用作诊断帮助。 您可以将单个配置文件导出为 Yaml 格式文件，或将所有配置导出为 .zip 文件。 您可以从配置页面的不同区域导出文件，这取决于您想要导出的配置。

步骤

1. 转至**配置**。
2. 选中复选框，选择特定配置。
3. 单击**操作** > **导出选定配置及详细信息**。 如果要导出所有配置，选择**导出所有配置及详细信息**。
   .ZIP 文件包含一组 YAML 文件。 该报告包含选定空间中的所有现有配置的详细信息。

导出自定义配置

步骤

1. 转至**配置**。
2. 单击 **+添加**，以选择配置。
3. 请按照自定义配置的步骤。
4. 单击**下一步**。
5. 选择分配水平。
6. 单击**完成**。
7. 选择仅从**配置**页面上的列表创建的配置。
8. 点击**操作**下拉菜单，并点击 **“导出”。**

带有配置名称和时间戳 _yyyymmdd.yaml 的文件会下载到您的设备。

导出现有配置

步骤

1. 转至**配置**。
2. 选择现有配置。
3. 单击**操作**下拉菜单，并单击**导出**。
   将会下载带有配置名称和时间戳 _yyyymmdd.yaml 的文件。

导入配置

您可以导入包含配置详细信息的 YAML 文件。 要编辑配置，您可以编辑 YAML 文件中的详细信息，选择配置并导入文件，更新的值会显示在配置中。 如果选择了多个配置或空间，则“导入”按钮将被禁用。 如果选择了不正确的文件类型，则会出现错误消息。 如果所选 YAML 文件中包含的详细信息与配置所需的详细信息不同，则会出现错误消息。

步骤

1. 转至**配置**。
2. 选择一个配置，点击**导入**，再点击**选择文件**，选择 YAML 文件，然后点击**导入**。 包含配置详细信息的 YAML 文件即被导入。

支持的允许列表中的配置

- CERTIFICATE
- VPN
- WEBCLIP
- IDENTITY_CERTIFICATE_DG
- RESTRICTIONS
- ANDROID_WORK_DEVICE_OWNER_LOCKDOWN
- PASSCODE
- HOME_SCREEN_LAYOUT
- ANDROID_ADVANCED_PASSCODE_AND_LOCK_SCREEN
- IOS_APP_CONTROL

- SCEP
- ANDROID_SAMSUNG_SAFE_LOCKDOWN
- ANDROID_WORK_DEVICE_OWNER_WITH_WORK_PROFILE_LOCKDOWN
- ANDROID_WORK_LOCKDOWN
- DEVICE_NAME
- MOBILE_THREAT_DEFENSE
- PRIVACY
- APP_LOCK
- GOOGLE_ACCOUNT
- ANDROID_WORK_APP_RUNTIME_PERMISSION
- IDENTITY_PREFERENCE
- MAC_OS_AGENT
- MANAGED_GOOGLE_PLAY
- ANDROID_MI_TUNNEL
- ANDROID_ENCRYPTION
- ANDROID_APP_CONNECT
- APPCONNECT_DEVICE_SETTINGS
- ANDROID_WORK_DEVICE_OWNER_SYSTEM_UPDATE
- DOMAINS
- END_USER_PRIVACY
- EXCHANGE
- MI_CLIENT_PRIVACY
- APP_UPDATE_SCHEDULE
- ZERO_PASSWORD
- WINDOWS_PRINTER
- PRINTING
- AUTH_ONLY
- SAFETYNET
- OSX_RESTRICTIONS
- WATCH_OS_RESTRICTIONS
- VISION_OS_RESTRICTIONS
- ANDROID_APP_CONTROL
- WINDOWS_APP_CONTROL
- ANDROID_SAMSUNG_PHONE_RESTRICTIONS
- MAM
- ANTI_PHISHING
- SETUP_ASSISTANT

- DNS_SETTINGS
- WINDOWS_KIOSK
- FIDO_AGENT
- WINDOWS_BITLOCKER
- WINDOWS_DEVICE_ADMIN_RESTRICTIONS
- TELECOM_SETTINGS
- IDENTITY_CERTIFICATE_UP
- IDENTITY_CERTIFICATE_DC
- WIFI
- NOTIFICATIONS
- WEB_CONTENT_FILTER
- WINDOWS_AI_MANAGEMENT
- WINDOWS_ENERGY_SAVER
- WINDOWS_BROWSER
- WINDOWS_DESKTOP
- WINDOWS_PHONE_RESTRICTIONS
- WINDOWS_UPDATE
- WINDOWS_GPO_ADMX
- WINDOWS_LICENSE
- WINDOWS_ATP
- WINDOWS_LAPS
- WINDOWS_EDP
- WINDOWS_BIOS
- WINDOWS_BLOATWARE_REMOVER
- WINDOWS_HELLO
- WINDOWS_START_MENU

使用 YAML 文件创建配置

您可以从 YAML 文件创建配置。 分发相关规范不是 YAML 文件的一部分。 默认情况下，分发设置为“无设备”。

步骤

1. 转至**配置**。
2. 点击**导入**，再点击**选择文件**，选择 YAML 文件，然后点击**导入**。 包含配置详细信息的 YAML 文件即被导入。 系统将打开“创建配置”页面，其中显示在 YAML 文件中添加的所有详细信息。
3. 选择*一种*分发类型：
   - **所有设备**
   - **无设备**
   - **自定义**

4. 确认配置详细信息，然后选择以下“分发摘要”选项之一：

> 分发摘要并不适用于所有配置。

   - **不适用于其他空间**
   - **适用于其他空间中的设备**

5. 如果配置的新名称与现有配置的名称相匹配，则会出现错误消息，请点击**确定**，再点击**后退**并编辑配置名称。
6. 点击**下一步**，然后点击**完成**。

编辑配置

您可以打开配置并直接编辑配置详细信息，或导入包含所有必要详细信息的 YAML 文件。 如果选择了多个配置或空间，则“导入”按钮将被禁用。

步骤

1. 转至**配置**。
2. 选择并打开配置，点击编辑（铅笔）图标并编辑配置。
3. 或者，从编辑配置页面点击**导入**图标，选择 YAML 文件，然后点击**导入**。 系统将打开“编辑配置”页面，其中显示了在 YAML 文件中添加的所有详细信息。
4. 确认配置详细信息，然后选择以下“分发摘要”选项之一：

> 分发摘要并不适用于所有配置。

   - **不应用到其他空间**。
   - **适用于其他空间中的设备**

     > 默认情况下，分发设置为“无设备”。

5. 单击**完成**。

删除配置

您可以删除选定配置。

步骤

1. 选中复选框，选择特定配置。
2. 单击**操作** > **删除**。

计划内部应用更新

设备签入时，Ivanti Neurons for MDM 将自动更新内部应用。 管理员现在可以根据服务器时区计划内部应用更新。 仅当设备在计划时间内签入时，应用才可以更新。 默认情况下，禁用应用更新的计划。

> 此配置仅适用于更新，不适用于新安装。 您可以使用发送安装/更新命令，覆盖 iOS 应用的自动更新计划。 如果在应用程序级别或目录级别启用自动更新，其将优先于计划的应用程序配置，并且应用程序会在签入后立即更新。

该配置仅适用于以下应用程序类型：

- iOS 内部应用。
- 仅处于 DO 模式的 Android 内部应用。
- macOS 应用的格式是 .pkg 和 .MIP。
- Windows 应用。

先决条件

请确保，满足以下先决条件，配置才可以如预期正常运行：

- 应用必须针对 iOS 和 Android 进行管理。 对于 macOS，应用可以处于托管或非托管状态。
- 请确保，启用应用配置下方的在设备上安装选项。
- 设备必须在计划时间内签入。

步骤

1. 登录到 Ivanti Neurons for MDM 管理员门户。
2. 转至**配置**。
3. 单击**添加**。 系统将打开添加配置页面。
4. 搜索**应用自动更新**。 系统将打开创建应用自动更新配置页面。
5. 在**名称**字段中，指定名称。
6. 在**配置设置**部分中，从下拉列表中选择**时区**。
7. 从下拉列表选择**开始时间**，然后从下拉列表选择**持续时间**。
8. 单击**下一步**。
9. 选择所需用户和设备组，然后单击复选框**启用此配置**。
10. 单击**完成**。 配置已应用；现在，应用将仅按指定计划进行更新。

如果您未看到配置页面，这可能是您没有所需权限。 您需要以下角色之一：

- 设备管理
- 设备只读

相关主题：

- 空间
- 设置配置优先级

需要活动用户会话的 Windows 配置

某些 Windows 配置需要有活动的用户会话（即有用户已登录设备）才能进行配置。 如果没有用户登录，则在 MDM 用户登录设备后应用这些配置。

以下配置需要活动用户会话：

- 通行码
- 用户证书（用户范围身份证书）
- Windows 防火墙

- Exchange
- VPN
- Windows 许可证
- Microsoft Defender for Endpoint
- Windows 设置（用户范围）
- Bridge 服务依赖型配置
- 现代/UWP 应用程序

Bridge 服务依赖型配置

仅当活动用户会话可用时，才会配置需要 Ivanti Bridge 服务的配置。 示例包括 Windows 桌面限制、浏览器设置、开始菜单、自助服务终端模式、BIOS、Windows 脚本、GPO 和其他依赖 Bridge 服务的配置。

异常：以下默认 Bridge 脚本不需要活动用户会话，无论 MDM 用户是否已登录，都会发送到设备：

- get-device-data.ps1
- get-bitlocker-status.ps1
- device-hardware.ps1

现代/UWP 应用程序

仅当活动用户会话可用时，才会配置现代/UWP 应用程序。 这包括：

- 打包为 .appx 或 .appxbundle 的内部应用程序
- Microsoft Store/UWP 应用程序

传统 MSI 和 EXE 应用程序不受此要求的约束。

> 如果计划部署配置时所需的用户会话不可用，则在 MDM 用户登录到设备后，系统会自动配置。

10.2. 创建用户自助服务门户配置

作为企业用户，您可以使用自助服务门户，管理设备和证书。 我的设备选项卡显示了您已注册的设备。

您可以从“我的设备”选项卡执行以下任务：

- 锁定
- 解除锁定
- 停用
- 重置您的安全应用程序通行码

您可以从“我的证书”选项卡执行以下任务：

- 上传证书

> 您一次可以分发最多 100 个配置文件。

步骤

1. 登录 Ivanti Neurons for MDM 管理员门户。
2. 单击**添加**。
3. 搜索**创建用户自助服务门户配置**。
4. 单击**下一步**。
5. 如果您不希望立即启用此配置，请清除**启用此配置**选项。
6. 选择配置的分配水平。
    - **所有设备** - 将配置分发到所有可用设备。 要跨空间委派配置，请选择以下其中一个选项：
        - **不应用到其他空间**。
        - 要跨空间委派配置，选择**分发摘要** > **应用于其他空间中的设备**。
            - 选中**允许空间管理员编辑分发**复选框，允许委派空间管理员编辑特定空间的分发。
    - **无设备** - 选择此配置，以便在稍后某个时间分发。
    - **自定义** - 定义将为其发送此配置的特定设备集。 要跨空间委派配置，请选择以下其中一个选项：
        - **不应用到其他空间**。
        - **分发摘要** > **应用于其他空间中的设备**。
            - 选中**允许空间管理员编辑分发**复选框，允许委派空间管理员编辑特定空间的分发。
7. 如果服务已定义空间，指定配置是否应应用于其他空间，以及优先级。
8. 单击**完成**。

> 如果配置负责向设备发出命令，而不是在设备上安装配置文件，配置详情将不会在应用至任何设备时列出此配置。

10.3. 自定义配置

本部分包含以下主题：

- 定义自定义配置
- 自定义配置设置

许可证：Silver

适用于：iOS、macOS、tvOS、Android 和 Windows

描述

可让您导入并分配预定义配置文件。

有效配置文件格式如下：

操作系统	有效配置文件格式
iOS 和 tvOS	• .plist • .mobileconfig • .xml
macOS	• .plist • .mobileconfig
Android	.xml。 目前，此功能仅支持 Zebra 设备的 .xml 配置文件。
Windows	SyncML。

定义自定义配置

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中键入“自定义”，然后单击**自定义**配置。
   将显示“自定义配置”详细信息页面。
4. 在此页面上配置设置。 请参阅自定义配置设置部分中的表格，以了解有关值的指南。
5. 单击**下一步**，配置分配设置。
6. （macOS 设备）根据您对此配置的所需行为，选择其他选项，以确定**谁进行此配置应用于**设置：
   - 设备范围（常用）。
   - 用户特定（当前注册用户）。

单击**完成**。

自定义配置设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
选择操作系统	单击操作系统图标，以上传选定图标对应的配置文件：
选择文件	此选项将在您选择操作系统后显示。 将配置文件拖放到“拖放框”，或单击**选择文件**按钮，以选择配置文件。

自定义 CSP 配置（仅限 Windows）

只能在 Windows 设备上创建自定义 CSP 配置。 从“选择操作系统”部分选择 Windows 操作系统后，将获得两个选项：

选项 1 - CSP XML 文件 - 选择此选项并按照与**选择文件**设置相同的所述流程进行操作。

选项 2 - 自定义 CSP OMA-URI 架构节点

步骤

1. 从列表中选择“自定义 CSP OMA-URI 架构节点”选项。 屏幕上将显示“自定义 CSP 配置”部分。
2. 在**操作**下，点击“+”按钮开始创建具有不同 OMA-URI 字段的配置。
3. 屏幕上随即会显示**添加行**弹出窗口，其中包含以下字段：
    - 描述 - 输入有关设置的任何一般信息
    - OMA-URI - 输入要用作设置的 OMA-URI
    - 数据类型 - 选择将用于此设置的数据类型 - DATE、FLOAT、BASE64、NODE、XML、BINARY、CHARACTER、TIME、BOOLEAN、INTEGER
    - 值 - 输入与所选数据类型关联的值
    - 访问类型 - 添加、删除、执行、替换、获取

点击**保存并关闭**可关闭带有所提供详细信息的窗口。 点击**保存并添加**可另行创建新行。

5. 单击**下一步**。
6. 选择分发模式并点击**完成**。

相关主题

- 使用自定义配置将 SyncML 推送至设备
- 如何创建配置

10.4. 使用自定义配置向设备推送 SyncML

您可以通过添加至自定义配置，创建您自己的同步标记语言 (SyncML) 配置文件，或从第三方来源获得，以便实现自定义特性。

支持的平台：

- Windows

支持的设备：

- Windows 10+
- Microsoft HoloLens 2

步骤

1. 转至**配置**。
2. 点击 **+ 添加**。
3. 单击**自定义配置配置**，以便显示**创建自定义配置**页面。
4. 输入配置的名称。
5. 单击 Windows 操作系统图标。
6. 将 SyncML 文件拖放至界面，或单击**选择文件**，导航至文件，以便选择上传至设备的文件。

> Ivanti Neurons for MDM 不会对文件中的代码执行任何验证检查。

7. 单击**下一步**。

自定义 SyncML 日志

可以在“设备日志”选项卡下查看发送到 Windows 设备的 SyncML 命令，以及设备对这些命令的 SyncML 响应。 此日志信息将在发送 **Windows 自定义 SyncML** 配置后可用。 系统发送自定义 SyncML 配置时，无论 SyncML 响应如何，该配置的设备“配置”选项卡上将始终显示“已安装”状态。

10.5. 主屏幕布局配置

主屏幕布局配置将定义主屏幕的应用程序、文件夹和 Web 剪辑的布局。

本部分包含以下主题：

- 定义主屏幕布局配置
- 主屏幕布局配置设置

许可证：Silver

符合条件的设备：

- iOS 9.3+ 仅监测
- 仅受监控 tvOS

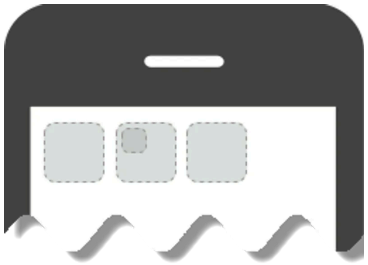
定义主屏幕布局配置

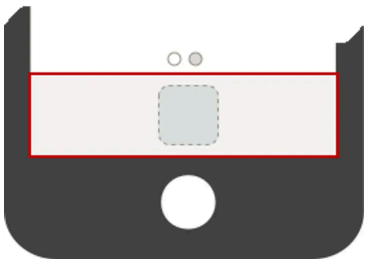
步骤

1. 前往**配置** > 点击 **+ 添加**。
2. 在搜索字段中输入“主页”，然后点击**主页屏幕布局**配置。 随即将打开“主页屏幕布局配置”详细信息页面。
3. 在此页面上配置设置。 请参阅部分 Home_Screen_Layout_Configuration_Settings 中的表格，以了解有关值的指南。
4. 点击**下一步**以配置分发设置。 对于共享 iPad 设备，请选择**设备**渠道或**用户**渠道。 有关详细信息，请参阅使用配置。
5. 单击**完成**。

主屏幕布局配置设置

设置	采取何种措施
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
停靠栏	点击 + 图标将应用程序或 Webclip 添加到主屏幕的 Dock（此处突出显示），然后按照后续屏幕上的说明进行操作： 可以通过输入 Apple 捆绑包 ID（以 com.apple 开头）来手动添加系统应用程序。 例如，输入“com.apple.DocumentsApp”添加“Files”应用程序。
第 1 页	单击 ⊕，以将应用或网络剪辑添加到主屏幕的页面区域（如此处高亮显示），然后遵照后续屏幕中的指示： 可点击“添加页面”将另一个页面添加到电话显示。







10.6. 应用控制配置：控制每个设备上安装哪些应用

应用控制配置支持您在设备级将应用分类为允许列表或阻止列表。 已安装的应用将不可见且无法启动。 应用仍将在 App Store 中可见，但无法下载或启动。 分发此配置的任何设备将使用此配置，并忽略任何允许的应用策略设置。 此配置会取代引用目标设备上相同应用的任何应用相关策略。

此配置会取代引用目标设备上相同应用的任何应用相关策略。 对于 Windows 10 设备，限制发生在设备级别上，因此配置是强制执行应用规则的唯一方式。

应用控制配置允许您创建：

- **允许列表**：仅允许明确添加到此列表的应用。 其他应用将不会安装到设备上。
- **阻止列表**：不允许特定应用安装到设备。

支持的设备

您可以使用应用控制配置，将以下设备中的不同应用加入允许列表或阻止列表：

- 公司拥有设备上的 Android 工作配置文件
- iOS9.3+ 仅监测
- tvOS 11+
- Windows

创建应用控制配置

步骤

1. 选择**配置**。
2. 单击**+添加**
3. 在生成的**选择配置**字段中，输入**应用控制**，然后选择**应用控制**配置。
4. 为配置输入名称和描述。
5. 选择操作系统，然后在下方适合您的操作系统的区块中继续操作。

公司拥有设备上的 Android 工作配置文件

用户可将最多 50 个应用 ID 加入允许列表或阻止列表组。

步骤

1. 选择**创建个人应用的允许列表**或**创建个人应用的阻止列表**，添加要加入允许列表或阻止列表的适当应用的列表。
2. 输入应用 ID (com.example.com)，并单击添加。
3. 单击**下一步**，并选择分发选项。
4. 单击**完成**。

iOS 9.3 监管设备

步骤

1. 选择是否创建允许列表或阻止列表。

2. 单击**添加应用**。
3. 单击以下其中一个或两个选项卡，选择要加入允许列表或阻止列表的应用：
    - 单击**查找后添加**，从 App Store 或 App Catalog 中搜索并选择应用程序。
    - 单击**手动添加**，以通过仅为 Apple 系统应用输入 Apple 捆绑 ID（以 "com.apple" 开头）选择应用。

单击**允许列表**或**阻止列表**选项卡，查看选择加入允许列表或阻止列表的应用列表。

5. （可选）选择**包括所有网页剪辑**选项。
6. 单击**下一步**，然后选择分配选项。
7. 单击**完成**。

Windows 设备

步骤

1. 选择**允许**或**阻止**，将适用应用的列表加入允许列表或阻止列表。
2. 在**规则定义**部分下方，从列表中选择**应用类型**。
3. 在**应用标识符**框中，输入标识符名称，搜索特定应用。 您也可以使用**查找应用**链接，打开新对话框并搜索特定于 Windows 的应用标识符。
4. （可选）在**应用描述**框中，输入一些关于应用的描述。
5. 使用 **+ 添加**链接，添加更多规则定义，并将应用加入允许列表或阻止列表。
6. 单击**下一步**，并选择分发选项。
7. 单击**完成**。

10.7. 应用通知配置

选择用户如何接收来自选定应用的通知。

适用于：iOS 9.3+ 被监控设备

创建应用通知配置

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中键入通知，然后单击**应用通知**配置。 将显示应用通知配置设置页面。
4. 命名并描述配置。
5. 通过在 App Store 中查找，或手动输入捆绑 ID，添加应用。
6. 选择要应用应用通知设置的应用。
7. 配置通知设置。 您可以选择以下通知：
    - 允许通知
        - 显示在通知中心中
        - 声音
        - 徽标应用图标
        - 显示在锁定屏幕上
        - （iOS 12.0+ 受监控）在使用 CarPlay 时显示重要提醒
        - （iOS 12.0+ 受监控）允许启用重要提醒（忽略“勿扰模式”）
    - 解锁报警样式
        - 横幅
        - 模式报警
        - 无
    - （iOS 12.0+ 受监控）允许分组类型
        - 自动
        - 按应用程序
        - 关闭
    - (iOS 14.0+) 通知预览类型 - 选择要在设备通知消息预览中显示的预览类型。
        - 用户控制 - 按照设备中应用的用户设置，显示消息预览。
        - 始终 - 显示消息预览。
        - 解锁时 - 仅在设备解锁时显示消息预览。
        - 从不 - 阻止应用在通知中显示消息预览。
8. 单击**下一步**，配置分配设置。
9. 点击**完成**。

有关更多信息，请查看如何创建配置。

10.8. 导出配置

导出要发送的配置文件，以支持用作诊断帮助。 您可以将一个配置文件导出到 Yaml 格式文件，或将所有配置导出到 .zip 文件。

步骤

导出配置

您可以从配置页面的不同区域导出文件，这取决于您想要导出的配置。

导出所有配置：

1. 转至**配置**。
2. 选中复选框，选择特定配置。
3. 单击**操作** > **导出选定配置及详细信息**。 如果要导出所有配置，选择**导出所有配置及详细信息**。
   .ZIP 文件包含一组 YAML 文件。 该报告包含选定空间中的所有现有配置的详细信息。

导出自定义配置：

1. 转至**配置**。
2. 单击 **+添加**，以选择配置。
3. 请按照自定义配置的步骤。
4. 单击**下一步**。
5. 选择分配水平。
6. 单击**完成**。
7. 选择仅从**配置**页面上的列表创建的配置。
8. 点击**操作**下拉菜单，并点击 **“导出”。**

带有配置名称和时间戳 _yyyymmdd.yaml 的文件会下载到您的设备。

导出现有配置：

1. 转至**配置**。
2. 选择现有配置。
3. 单击**操作**下拉菜单，并单击**导出**。
   将会下载带有配置名称和时间戳 _yyyymmdd.yaml 的文件。

10.9. 确定配置的优先级

如果为配置选择多个设备组，多个类型相同的配置可能会分配到指定设备。在类型相同的配置应用于相同设备时，定义的优先级将决定应用哪个配置。 优先级最高的配置编号最小。 例如，优先级为 1001 的配置的优先级高于优先级为 1002 的配置的优先级。 服务自动分配编号。

> WIFI 优先级无法应用于设备，并且从优先级排除。

仅在页面包含两个或多个类型相同的配置并且在下拉列表中选择一个空格时，此选项才可用。 您可以更改配置的优先级。

步骤

1. 转至**配置**。
2. 未选择配置时，请选择**操作 > 优先级配置**。
   如果**操作**未显示，需要优先级的类型没有多个配置。
3. 使用箭头移动配置，以便优先级最高的配置出现在顶部。

> 锁定图标表示，未在配置中编辑所有设备分发设置的情况下，无法更改配置优先级。

单击**保存**。

> 优先级可以完成最多 400 个配置。

如果您未看到配置页面，这可能是您没有所需权限。 您需要以下其中一个角色：

- DeviceManagement
- DeviceReadOnly

10.10. 管理配置

本部分包含以下主题：

- AppConnect 配置
- 安全配置
- 用户资源配置
- 企业网络访问配置
- 移动电话
- 其他配置

10.10.1. 配置类型

本部分包含以下主题：

- 搜索配置
- 安全性
- 用户资源
- 企业网络访问
- 蜂窝网络
- 更多配置
- 设备同步配置

搜索配置

使用**选择配置**页面上的搜索和筛选功能来查找要应用的配置。

步骤

1. 选择**配置**。
2. 选择其中一个列出的配置，或单击 **+ 添加**按钮。
3. 将显示**选择配置**页面
   单击其中一个列出的配置或者：
   - 在搜索框中输入配置名称
   - 单击搜索框右侧筛选图标，以显示兼容平台的配置类型。

单击配置按钮，以访问配置设置选项。

有关详细信息，请参阅使用配置。

安全性

类型	功能	适用于以下设备	需要以下许可证
Android Enterprise	指定 Android Enterprise 选项	Android Enterprise	Silver
AppConnect 设备	指定设备上启用 AppConnect 的应用程序的安全设置	• Android • iOS	Gold
Apple 密钥认证	在 Apple 设备上为特定密钥启用 WebAuthn 企业证明。	• macOS	
Entra ID（Azure 租户）	通过将 Ivanti Neurons for MDM 连接到 Entra ID，您可以使用托管设备的设备合规性状态有条件地访问 Microsoft 365 应用程序。	• iOS • Android	• 对于新客户：Secure UEM Premium • 对于现有客户：Platinum
证书	与服务器建立信任	• Android • iOS • macOS • watchOS • visionOS • tvOS	
证书透明度	控制只能出现在设备配置文件中的证书透明度实施。	• iOS • macOS • tvOS • watchOS • visionOS	
设备日志记录	检索其他日志，如设备中的网络和安全日志。	• Android Enterprise	
磁盘管理配置	定义用于管理外部和网络存储设备的策略。	• 受监管 macOS 15.0+	
Android 加密	提示用户开始加密。	Android	
加密的 DNS	允许您增强安全性，无需配置 VPN。	• iOS • macOS • visionOS	Gold
外部智能设置	允许外部智能集成	• iOS 26.4+	

类型	功能	适用于以下设备	需要以下许可证
		• macOS 26.4+ • visionOS 26.4+	
移动威胁防御 威胁防御本地操作	保护托管设备免受影响设备、网络和应用的移动威胁和漏洞的破坏。 创建和分发设备配置，并定义当启用 Threat Defense 的客户端检测到威胁时在支持的 Android 设备上要采取的本地操作。	• Android • iOS Android	
FileVault 2	提供对卷的内容执行完整 XTS-AES 128 磁盘加密的能力。	macOS	Gold
FileVault 恢复密钥	确定将 FileVault 恢复密钥重定向到公司服务器的设置。	macOS	Gold
身份证书	• 验证连接到服务器的设备。 • 验证连接到网络资源的设备。	• Android • iOS • macOS • watchOS • visionOS	
iOS 激活锁定	在监控的设备上启用 Apple 激活锁定特性。	iOS	Silver
iOS 自定义配置	分发由不同应用创建的 iOS 配置的配置文件。	iOS	
iOS 限制	• 锁定设备功能。 • 启用设备功能。	• iOS • watchOS • visionOS	
智能设置	允许 Apple Intelligence 集成。	• iOS 26.4+ • macOS 26.4+ • visionOS 26.4+	
会议室显示	在 Apple TV 上打开会议室显示模式。	tvOS 10.2+	
键盘设置	允许设备管理键盘行为、输入选项和相关用户体验设置。	• iOS 26.4+ • macOS 26.4+	
锁定和自助服务终端：Android	• 锁定设备功能。 • 重新启用设备功能。	Android	

类型	功能	适用于以下设备	需要以下许可证
	• 应用自助服务终端功能。		
锁定和自助服务终端：Android Enterprise	• 定义在 Android 企业版设备上受限制的功能和应用。 • 应用自助服务终端功能。	Android 5.0 +	
锁定和自助服务终端：Samsung Know Standard	• 定义在 Samsung Know Standard 设备上受限制的功能和应用。 • 应用自助服务终端功能。	Samsung Knox	
本地管理员密码解决方案配置	允许管理员以设定的时间间隔在受管的 macOS 设备上自动重新生成本地管理员密码	macOS	
macOS 防火墙	管理可在 macOS 设备上的“安全首选项”窗格中访问的应用防火墙设置。 管理员可以通过指定 ping 命令无法发现的设备来启用隐藏模式。	macOS 10.12+	Gold
macOS 限制	确定 macOS 设备上启用的限制。	macOS	Gold
macOS AppStore 限制	定义在 macOS AppStore 上启用哪些限制。	macOS	Gold
macOS 磁盘刻录限制	管理 macOS 中的磁盘刻录限制。	macOS	Gold
Mobile@Work for macOS	创建并分发适用于 Mobile@Work for macOS 的执行规则。	macOS	Gold
Mobile@Work for macOS 脚本	创建用于分发到 Mobile@Work for macOS 中的脚本。	macOS	Gold
身份首选项	在用户的密钥链中识别引用包含在同一配置文件中的身份有效内容的身份首选项。	macOS	Gold
证书首选项	在用户的密钥链中识别引用包含在同一配置文件中的证书有效内容的证书首选项。	• macOS	Gold
允许的介质控制	配置物理媒体的安装、卸载和弹出选项。	macOS	Gold
macOS Finder 设置	管理 macOS 中 Finder 应用程序的设置。	macOS	Gold
macOS 内核扩展策略	控制加载用户批准内核扩展的限制和设置。	macOS	Gold
Active Directory (macOS)	配置高级选项，以将 macOS 设备绑定到 Active Directory (AD) 域，以访问依赖 AD 进行身份验证和保障安全的软件服务。	macOS	Gold
Office 365 自动帐户创建 (macOS)	配置用户信息和选项，以设置所有 Microsoft Office 365 应用的初始配置。	macOS	Gold

类型	功能	适用于以下设备	需要以下许可证
Apple App Catalog	管理通过 Web 剪辑访问 Apple 应用程序目录的情形。	• iOS • macOS	
托管的域	指定受信任的电子邮件和 Web 域。	• iOS 8+ • visionOS 1.1+	Silver
通行码	• 强制使用通行码。 • 指定通行码长度和内容。 • 更改通行码要求。	• Android • iOS • macOS • watchOS	
隐私首选项 (macOS)	配置允许访问系统服务、系统文件和系统资源的应用程序。	macOS	Gold
认证	为云服务和/或桌面登录提供无密码身份验证。	• macOS • Windows	
隐私配置	指定是否收集位置数据。	• iOS • Android • Windows	
客户端隐私声明信息	向 Go 客户端中的用户显示隐私政策。	• Android • Android 企业 • iOS	
Ivanti Go Client 设置	配置通过 MixPanel 收集数据，包含故障排除和保持最高服务质量所需的设备和使用信息。	• iOS • macOS	
Safari 扩展设置配置	管理来自各种域的 Safari 浏览器扩展。	• 受监管 iOS 18.0+ • 受监管 macOS 15.0+	
Siri 设置	允许设备访问和使用 Siri 设置。	• iOS 26.4+ • macOS 26.4+ • watchOS 26.4+	

类型	功能	适用于以下设备	需要以下许可证
		• visionOS 26.4+	
服务配置文件配置	管理员可以集中管理和部署各种系统服务的配置文件。	macOS	
软件更新	创建和分发操作系统更新规则。	• iOS • macOS • Windows	
软件更新设置配置	创建和更新软件更新强制执行设置。	• 受监管 iOS 18.0+ • 受监管 macOS 15.0+	
时间服务器	允许设备连接到自定义时间服务器。	macOS	Gold
Web 内容筛选	控制 Safari 内容。	• 受监督 iOS 7 • visionOS 1.1+	Silver
Windows_Firewall	Windows 防火墙配置有各种防火墙限制。 根据管理员应用的防火墙限制，防火墙状态会导致 Windows 设备上的“安全首选项”窗格中出现以下防火墙状态之一： • 防火墙已开启并且正在监控。 • 防火墙已被禁用。 • 防火墙未监控所有网络或某些规则已关闭。 • 防火墙暂时未监控所有网络 • 不适用。	Windows 10+	
Windows 信息保护	定义 Windows 信息保护 (WIP) 设置，以保护企业数据。	Windows 10+	Gold
Windows 限制	确定哪些功能可在 Windows 10+ 设备上使用。	Windows 10+	
Windows AI 管理配置	允许管理 Windows AI 设置和配置。	Windows 10+	

用户资源

类型	功能	适用于以下设备	需要以下许可证
CalDAV	• 设置对 CalDAV 服务器（例如 Google 日历）的访问权限	• iOS • visionOS	
CardDAV	• 设置对 CardDAV 服务器（例如 Google 联系人）的访问	• iOS • visionOS	
Email+	• 对 POP/IMAP 电子邮件（例如 Gmail）的访问进行设置	• iOS • visionOS	
Exchange	• 为 Android 和 iOS 移动设备设置基于 ActiveSync 的电子邮件的访问（例如 Outlook） • 为 macOS 设备设置基于 Exchange Web Services (EWS) 的电子邮件 • 定义与设备同步的数量 • 定义电子邮件安全性	• Android • iOS • macOS • visionOS	• macOS 操作系统不支持 Exchange via sentry • 同步过去天的电子邮件标志不适用于 macOS
Google	• 创建 Google 帐号配置，将 iOS 9.3.2+ 设备添加到 Google 帐号。 • 指定用来在 Google 系统中呼叫联系人的应用程序。	• iOS • visionOS	
字体	• 为正确显示文档安装非标准字体	• iOS	
已订阅日历	• 对订阅互联网日历进行设置	• iOS • visionOS	
Web 剪辑	• 显示到网页的快捷方式（图标）	• iOS • macOS	
内容缓存	• 提供内容缓存服务，以启用 App Store 软件的本地副本 • 使连接的客户端更快地下载软件和应用。	• macOS	

企业网络访问

类型	功能	适用于以下设备	需要以下许可证
AirPlay	• 对用于媒体显示的备用设备的访问进行设置	• iOS • macOS	Silver
AirPrint	• 设置无线打印	• iOS • macOS	Silver
VPN 全局模式	• 对 VPN 服务器的访问进行设置，无需用户交互	• Android 7.0 + • iOS 8+	• Gold for Android 企业版 • Silver for iOS
默认应用程序运行时权限	• 为部署到 Android 企业版设备的应用程序设置运行时权限配置。	• 针对 Android API 23+ 构建并在 Android 企业版设备上运行 Android 6.0+ 的应用程序。	
教育	• 为领导和成员配置 Apple 教育有效负载和课堂应用。	• supervised iOS 9.3+	Gold
全局代理	• 对将 HTTP 流量转发至代理服务器的设备进行设置	• 受监控的 iOS 7 • 受监控的 tvOS	Silver
LDAP	• 对公司目录的访问进行设置	• iOS • visionOS	
Tunnel	• 使用隧道定义客户端和 Sentry 之间的每个应用 VPN 连接	• iOS 7+ • macOS 10.13+ • Windows 10+ • Android	
Bridge	• 允许 IT 部门在 UEM 上将 Windows 操作现代化，而不放弃关键功能	• Windows 10+ 台式计算机	Bridge 许可证
macOS 服务器	• 使用配置的帐号类型和相关设置，定义 macOS 服务器帐号。 允许用户激活服务器上的文件共享。	• iOS 10+	
Per-App VPN	• 对指定应用和 VPN 服务器之间的连接进行设置	• iOS • watchOS • visionOS • tvOS	Silver
网络中继配置	• 添加配置以定义网络中继的设置	• iOS • macOS • visionOS	

类型	功能	适用于以下设备	需要以下许可证
单点登录	• 对指定托管应用的单点登录进行设置	• iOS • macOS • visionOS	
多用户安全登录	• 通过网络剪辑设置了安全的多用户登录	• iOS	
VPN	• 对访问 VPN 服务器进行设置	• Android • Windows • iOS • macOS • visionOS • tvOS	
按需 VPN	• 对基于域、主机名等的 VPN 服务器的访问进行设置	• iOS	
Wi-Fi	• 对到无线网络的访问进行设置	• Android • Windows • iOS • macOS • watchOS • visionOS • tvOS	

蜂窝网络

类型	功能	适用于以下设备	需要以下许可证
APN	• 对设备的移动电话接入点名称进行设置	• iOS	
移动电话	• 对移动电话网络访问进行设置	• iOS • watchOS	
蜂窝专用网络配置	• 设置负载以提供专用网络部署上的设备信息	• iOS	
iOS 电信预置配置	• 设置漫游限制默认值 • 设置个人热点限制默认值	• iOS	

更多配置

类型	功能	适用于以下设备	需要以下许可证
Apple TV	• 定义 Apple TV 的语言和区域	• 受监控的 iOS 7	Silver
默认设备名称	• 使用变量定义默认设备名称	• 受监控的 iOS 8	Silver
iOS 壁纸	• 安装主屏幕并锁定屏幕背景	• 受监控的 iOS 7	Silver
macOS 壁纸	• 在设备上安装主屏幕和锁屏壁纸。 壁纸可以由用户更改，但在分发后，不可从设备中移除		不需要
迁移助手设置	帮助管理员和用户在设备设置或迁移期间传输数据、应用程序和设置。	• macOS 26.4+	
单应用模式	• 限制设备使用指定应用	• 受监控的 iOS 7 • 受监控的 tvOS	Silver
关联域配置	• 关联域配置是将应用程序映射到其关联域的词典。 • 关联域可与可扩展 AppSSO、通用链接和密码自动填充等功能一起使用。	• macOS 10.15+	Gold
屏幕共享主机设置配置	• 使管理员能够跨受管设备安全地控制 macOS 屏幕共享功能。	• macOS 14+	

设备同步配置

设备同步设置提供可在设备上监控的数据点列表。 设备同步配置无法编辑。 可以查看已检查的设置的列表。

步骤

1. 转至**配置**。
2. 点击**设备同步配置**。显示**设备同步配置**页面的“详细信息”选项卡以及选中项目列表。

设置	读数之间的时间（以分钟计算）
证书列表	
设备信息	60
已安装应用列表	60
托管应用列表	60
配置文件列表	60
部署配置文件列表	60
限制	60
安全信息	60
iOS 9+	
检查更新	1440

相关主题

- 变量
- 使用配置

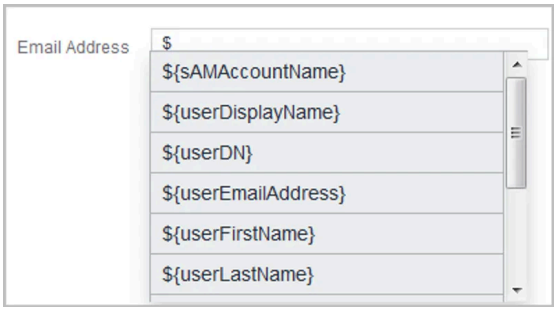
10.10.2. 变量

您可使用某些配置字段中的变量，以表示给定用户特定的值。 如果您在任何支持变量的字段中输入 $，该字段将显示支持的变量列表。 本部分包含以下主题：

- 支持的用户账户变量
- 支持的设备变量

支持的用户账户变量

用户变量

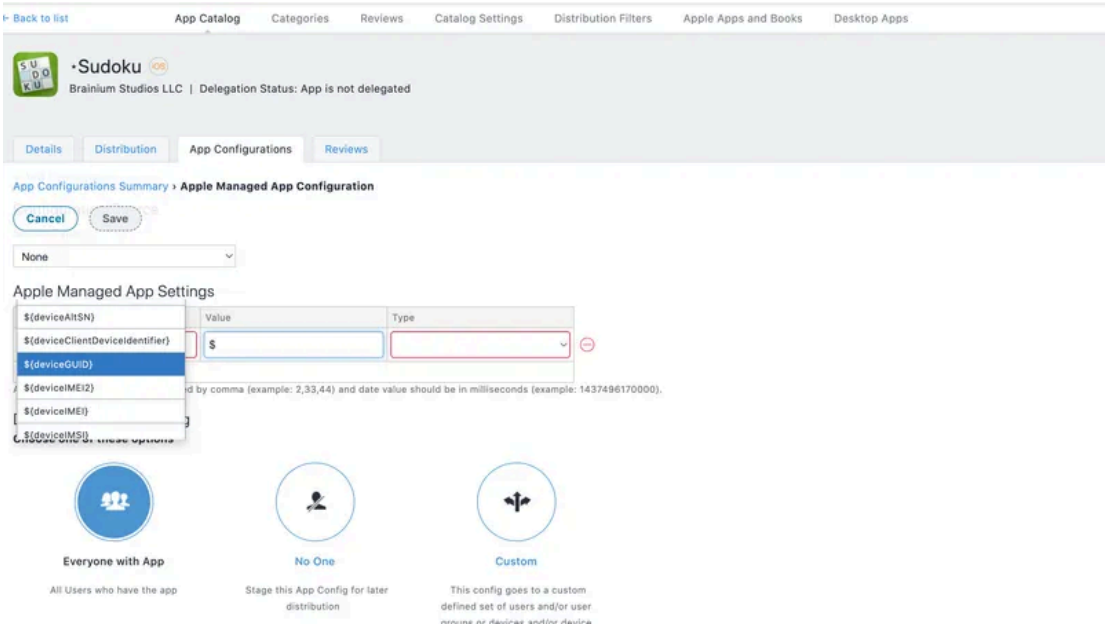


可变密钥	值描述
$	部门属性（需要 Entra ID）
$	电子数据交换 - 个人标识符
$	用户的受管 Apple ID
$	sAMAccountName 属性（需要 Active Directory）
$	从可分辨名称中提取的通用名称 (CN) 属性（需要 LDAP）
$	显示名称
$	可分辨名称（需要 LDAP）
$	电子邮件地址的域部分（“@”后面的部分）
$>	电子邮件地址的本地部分（“@”前面的部分）
$	电子邮件地址
$	名字
$	姓氏
$	区域设置
$	从可分辨名称中提取的组织单位 (OU) 属性（需要 LDAP）
$	Kerberos 领域信息（需要 Active Directory）
$	登录 ID 的域部分（“@”后面的部分）
$	登录 ID 的本地部分（“@”前面的部分）
$	登录 ID（电子邮件格式）
$	userPrincipalName 属性（需要 Active Directory）

支持的设备变量

使用设备变量指定移动设备的相关信息。

设备变量


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

可变密钥	值描述
$	客户端上次签入日期（最近签入 - MDM 或客户端）
$	替代序列号
$	客户端应用使用的标识符
$	全局唯一设备标识符
$	ICCID
$	IMEI2
$	IMEI
$	IMSI
$	设备上次签入日期（最近签入 - MDM 或客户端）
$	内部设备标识符
$	MDM 使用的标识符
$	MEID
$	型号
$	设备名称
$	设备电话号码
$	群集唯一设备标识符
$	序列号
$	iOS UDID
$	Wi-Fi MAC 地址

电子邮件模板变量

可变密钥	值描述
$	电子邮件正文
$	电子邮件主题

时间戳变量

可变密钥	值描述
$	当前时间戳（自 Epoch 起的毫秒数）

策略模板变量

可变密钥	值描述
$	违规策略名称
$	发送消息后要采取的下一层合规操作（与等待和停用不同）
$	设备处于不合规状态的天数
$	初次触发策略违规时的时间戳（UTC DD-MM-YYYY 格式）
$	规则定义（查询字符串当前的显示方式）

相关主题：

- 属性

10.10.3. AppConnect 配置

本部分包含以下主题：

- AppConnect 概述
- AppConnect 通行码

10.10.3.1. AppConnect 概述

AppConnect 是一项可对应用进行封装的功能，以保护 iOS 和 Android 设备上的数据。 每个启用 AppConnect 的应用会变为安全容器，其中数据已加密、防止未经授权的访问且可以移动。 鉴于每位用户拥有多个企业应用程序，因此每个应用程序容器也会连接到其他安全应用程序容器。 此连接允许启用 AppConnect 的应用共享数据，例如文档。 Ivanti Neurons for MDM 会使用策略管理启用 AppConnect 的应用。

有关 AppConnect 及如何配置和部署 AppConnect 应用的详细信息，请查看*适用于 Ivanti Neurons for MDM 的 AppConnect 指南*。

安全应用的状态

从**设备 > 设备**页面，单击设备，以查看**概述**页面。 在此页面上，用户可以查看安全应用的状态，其中包含以下信息：

- **安全应用状态** - 表示 AppConnect 启用或禁用。
- **安全应用加密状态** - 表示 AppConnect 通行码启用或禁用。
- **安全应用加密模式** - 表示加密模式（例如 AES 256）。

此外，这些字段可用作：

- 筛选器（左侧窗格），以缩小在用户尝试查找/筛选设备时显示的设备条目。
- 作为创建动态托管设备组时的规则。
- 作为分配筛选器，可调整根据定义规则分配应用的设备。

对于每个安全应用程序，管理员都可以在设备详细信息页面的**配置**选项卡中查看容器策略和配置状态（已安装、已应用、已发送或待安装）。

10.10.3.2. AppConnect 通行码

本部分包含以下主题：

- 更改/重置通行码
- 生成一次性 PIN 以重置 iOS 设备的安全应用通行码

您可以要求 AppConnect 通行码，也称为安全应用通行码。 使用 AppConnect 通行码进行单次登录后，设备用户可以访问所有安全应用。 在管理员门户上，您可以为 AppConnect 通行码配置规则。 AppConnect 通行码不得与用于解锁设备的通行码相同。

更改/重置通行码

如果在 AppConnect 配置中允许，用户可以在适用于 Android 设备的 Secure Apps Manager 应用和 Go for iOS 应用中更改或重置安全应用通行码。 对于 iOS 设备：

步骤

1. 打开 Go for iOS 应用。
2. 单击**安全应用**。
3. 单击**身份验证**。
4. 单击**更改安全应用通行码**，并按照说明更改/重设通行码。

对于 Android 设备：

1. 打开安全应用管理器应用。
2. 单击选项菜单中的**更改通行码**。
3. 单击**忘记密码**，以重置通行码。

生成一次性 PIN 以重置 iOS 设备的安全应用通行码

管理员可以配置 Ivanti Neurons for MDM，以允许 iOS 设备用户在忘记安全应用 (AppConnect) 通行码时重置该通行码。 在配置此选项时，使用用户名和密码注册到 Ivanti Neurons for MDM 的设备用户可以在 Go 3.1.0 for iOS 或支持的较新版本中输入这些凭据，以对自己进行身份验证，然后重置其安全应用通行码。 但是，忘记密码和 PIN 的设备用户需要使用不同的身份验证机制。

步骤

1. 在 Ivanti Neurons for MDM 上，管理员打开默认 iOS AppConnect 配置（或任何其他 iOS AppConnect 配置）中的**安全应用通行码**选项。
2. 用户通过单击**重置安全应用通行码**选项并按照说明为自助服务用户门户上的特定 iOS 设备生成一次性 PIN。 一次性 PIN 有效期为 30 分钟。
3. 在 Go for iOS 上，用户按照说明重置被遗忘的安全应用通行码。
4. 当提示输入用户凭证时，用户输入用户名和一次性 PIN，而不是常规通行码。
5. 用户重置安全应用通行码。

10.10.4. 安全配置

本部分包含以下主题：

- Android Enterprise
- 编辑 Android Enterprise 默认配置
- 设置 Android Enterprise
- Android 工作认证 (Work Challenge)
- 证书配置
- 证书透明度
- 证书吊销检查配置
- 创建自主单应用程序模式配置
- 创建 DNS 代理配置
- 设备日志记录配置
- 磁盘管理配置
- Android 加密
- 加密的 DNS
- 外部智能设置
- 威胁防御
- FileVault 2
- FileVault 恢复密钥
- FileVault 选项配置
- 身份证书
- Apple 激活锁定配置
- iOS 自定义配置
- 智能设置
- 键盘设置
- iOS 限制
- 会议室显示
- 锁定和自助服务终端：Android 设备管理模式
- 设置 Android 的自助服务终端模式
- 设置 Android 共享设备自助服务终端
- 锁定和自助服务终端：Android Enterprise
- 锁定和自助服务终端：Samsung Knox Standard
- macOS 防火墙
- macOS 限制
- macOS AppStore 限制
- macOS 磁盘刻录限制

- 允许的媒体控制（已弃用）
- macOS Finder 设置
- macOS 内核扩展策略
- Mobile@Work for macOS
- macOS 软件更新规则配置
- 证书首选项
- Active Directory (macOS)
- 身份首选项
- Office 365 自动帐户创建 (macOS)
- 认证
- Apple 应用目录
- 托管域
- 通行码配置
- 隐私首选项 (macOS)
- Ivanti Go Client 设置
- 隐私配置
- 客户端隐私声明信息
- Safari 扩展设置配置
- 软件更新
- 软件更新设置配置
- 安全首选项配置
- Siri 设置
- 时间服务器
- Web 内容筛选
- Windows 防火墙
- Windows 信息保护
- Windows 限制
- Windows 桌面限制
- Windows 10 的桌面设置
- Windows Hello for Business 配置
- Windows AI 管理配置
- Play Integrity（原 SafetyNet Attestation）
- 高级 Android 密码和锁屏
- Microsoft Defender for Endpoint
- 基于证书的身份验证

10.10.4.1. Android Enterprise

许可证：Silver

Android Enterprise 配置定义了为支持的设备启用的 **Android Enterprise** 选项。 您可以为不同的设备组创建备用配置，或者仅编辑默认配置。 有关支持 Android Enterprise 的设备的列表，请访问 **Android** 官方网页。

Android Enterprise 设置

设置	采取何种措施
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
禁用屏幕捕获 (Android 5.0 +)	选择以阻止设备使用本机屏幕捕获功能。
禁用应用程序控制 (Android 5.0 +)	选择以阻止用户修改“设置”或“启动器”中的应用程序。
禁止配置凭据 (Android 5.0 +)	选择以防止用户设置用户凭据。
禁止跨配置文件复制/粘贴 (Android 5.0 +)	选择以阻止设备复制并粘贴到其他 Android Enterprise 工作配置文件。
禁止修改帐户 (Android 5.0 +)	选择以阻止用户添加和删除帐户。
不允许传出 Beam (Android 5.0 +)	选择以阻止用户使用 NFC 传输应用程序数据。
禁止共享位置 (Android 5.0 +)	选择以防止网站和应用提示设备用户共享设备位置。
限制输入法 (Android 5.0+)	选择以通过指定允许的包名称列表来限制输入方法。 如果没有列入允许列表的包，则仅允许系统输入法。 输入法不仅限于工作应用程序，而是整个设备。
限制访问性服务 (Android 5.0 +)	选择以通过指定允许的包名称列表来限制输入方法。 如果没有列入允许列表的包，则仅允许系统辅助服务。 输入法不仅限于工作应用程序，而是整个设备。
禁用 Caller ID (Android 6.0 +)	设置在来电时是否在设备中显示工作配置文件中的呼叫者 ID 信息。

相关主题

- **设置 Android Enterprise**

10.10.4.2. Apple 密钥认证

使用密钥证明配置将设备配置为允许对某些密钥进行 WebAuthn 企业证明。

当用户使用密钥对其设备进行身份验证和注册时，Apple 密钥认证配置使用企业管理凭据，通过企业证书证明密钥。 支持的凭据包括 SCEP、ACME 和身份凭据。

密钥认证支持以下项：

- 支持的最低操作系统版本：macOS 14
- 支持的注册方法：设备注册
- 需要受管 Apple 帐户来控制密钥的同步。
- 可以与 ABM 的访问管理结合使用。

> Mac 上的密钥有效负载失败。

创建密钥配置时，您必须首先创建身份证书配置，并将其链接到密钥配置。 此外，请在“安全密钥认证配置”部分提供以下详细信息：

字段	描述
名称	密钥名称。
说明	有关配置的任何信息。
证明身份资产引用 • 认证身份密钥是可提取的	提供您创建的资产参考标识，以链接到密钥配置。 选择此选项以确认身份密钥是否可提取。
依赖者	输入经过身份验证的域的详细信息。

10.10.4.3. 应用程序隐私默认值

使用**应用程序隐私默认值**定义受监控设备上应用程序的默认隐私权限。 管理员可以识别应用程序使用的隐私组件，在配置中列出应用程序及其组件，并设置隐私默认值。 当用户启动应用程序时，应用程序会检查配置的隐私默认值，并提示用户授予权限，同时允许用户稍后在设备设置中推迟或管理权限。

适用于：

- iOS 27.0+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- iPad 27.0+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- macOS 27.0+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**应用程序隐私默认值**配置。
3. 在**名称**字段中输入标识此配置的文本。
4. 在**说明**字段中，输入说明以阐明此文件的目的。
5. 在**配置设置**窗格中，选择**按查找添加**。
6. 通过选择以下选项之一，输入要为其配置**应用程序隐私默认值**的应用程序名称：

- iOS Store
- 应用目录
- visionOS Store
- OS X Store (macOS)

> 您可以选择多个应用程序。

7. （可选）选择**手动添加**以选择应用程序。
8. （可选）输入应用程序的**程序包名称**。
9. （可选）单击**添加应用程序**。
10. 选择**查看应用程序**。

查看应用程序窗格列出所有选定的应用程序。

11. 单击每个应用程序上的**添加默认值**以单独配置应用程序隐私默认值。

随即显示**添加默认值**窗格。

12. 按照下表选择**默认值**和**限制**：

默认值	设置限制
摄像机	选择下列选项之一： • 允许 • 无
蓝牙	选择下列选项之一： • 允许 • 无
无障碍功能	选择下列选项之一： • 允许 • 无
听写	选择下列选项之一： • 允许 • 无
麦克风	选择下列选项之一： • 允许 • 无
定位	选择下列选项之一： • 使用时 • 无 • 始终
定位精度	选择下列选项之一： • 近似值 • 精确 • 无
本地网络	选择下列选项之一： • 允许 • 无
组织理由	**组织说明**提示可以显示组织名称、应用程序名称、管理员提供的理由，以及具有推荐隐私默认值的每个组件的详细信息。 如果用户选择**允许**，系统会应用到建议的隐私默认值。 如果用户选择**暂时不用**，当应用程序访问用户设备中的指定组件时，会出现同意提示。

13. 单击**保存**。
14. 单击**下一步**，配置分配设置。
15. 选择一个分发选项以设置**应用程序隐私默认值**配置。 有关配置分发选项的详细信息，请参阅使用配置。
16. 单击**完成**。

10.10.4.4. 编辑 Android Enterprise 默认配置

全局管理员可以允许空间管理员在自定义空间中编辑以下任何 Android Enterprise 默认配置的分发。

- Android Enterprise：公司拥有设备上的工作配置文件 (Android for Work)
- Android Enterprise：工作托管设备 (Android for Work)
- Android Enterprise：带有工作配置文件的托管设备
- Android Enterprise：AOSP

编辑上述任何配置的分发

步骤

1. 在“配置”选项卡中，选择要编辑的配置。
2. 单击编辑图标。
3. 单击**下一步**
4. 选择以下任何分发级别从分发页面进行编辑和配置：
    - **所有设备**：选择以下选项之一以将配置分发到所有兼容的设备：
        1. 不适用于其他空间
        2. 适用于其他空间中的设备。
    - **无设备**（默认）
    - **自定义**：选择以下选项之一将配置分发给所有兼容的设备或用户：
        1. **用户/用户组**：选中用户或用户组旁边的复选框。 或者，您可以键入并搜索用户或用户组。
        2. **设备/设备组**：选中设备或设备组旁边的复选框。 或者，您可以键入并搜索设备或设备组。
           在**分发摘要**中，选择以下选项之一以跨空间启用或禁用配置：
            - 不应用到其他空间。
            - 适用于其他空间中的设备。

            > 如果选择**适用于其他空间中的设备**选项，则会显示复选框**允许空间管理员编辑分发**，并且该复选框允许委派的空间管理员编辑特定空间的分发。

> 如果您编辑分发选项，则必须选中复选框“**我了解，如果从现有设备中删除配置，更改 Android Enterprise 设备模式配置的分发可能会导致设备报废或擦除**”。

5. 单击**完成**。

在此配置应用于空间时，空间管理员将可以通过单击自定义空间中的分发图标编辑分发。

10.10.4.5. 设置 Android Enterprise

本部分包含以下主题：

- 支持的设备
- 连接 Ivanti Neurons for MDM 和 Android Enterprise
- 获取 Android Enterprise 凭据
- 将 Android Enterprise MDM 令牌添加到 Ivanti Neurons for MDM
- 在 Ivanti Neurons for MDM 与 Google 之间同步用户
- Active Directory/LDAP 用户
- 本地用户
- 向支持的设备部署 Android Enterprise
- 停用注册的设备
- 部署设备
- 确认部署
- 部署 Android Enterprise 应用
- 配置商业应用

许可证：Silver

Android Enterprise 是 Google 提供的程序，让移动管理员能够：

- 区分工作和个人数据
- 保护并管理企业应用
- 控制系统应用程序（例如相机和图库）
- 在 Android Enterprise 容器中集中部署和配置应用
- 防止数据丢失（屏幕捕获）

可以将 Ivanti Neurons for MDM 配置为 UEM 服务器，用于管理 Android Enterprise。 Android Enterprise 至少需要 Android 3.0。 Android Enterprise 支持两种配置，“设备所有者”和“托管配置文件 – 员工所有”。

支持的设备

Ivanti Neurons for MDM 当前仅在运行 Android 5.0 和制造商已启用 Android Enterprise 的设备上支持 Android Enterprise。 运行 Android 5.0 的设备需要 Android Enterprise 来启用 Kiosk 模式。

先决条件

如果您尚未通过 Google 注册您的域，则首先必须在 Google 网站上注册该程序，网站地址如下：

https://admin.google.com.

在此过程期间，您将：

- 申请域（必须匹配用户电子邮件地址的域）
- 收到令牌
- 下载 JSON 客户端 ID

在 Ivanti Neurons for MDM 上设置 Android Enterprise 时，将同时需要这两项。

在此过程后，您将收到一封电子邮件，其中包含用于验证您对所申请域的所有情况说明。

如果公司已使用其域名注册 Google Apps for Work，请参阅 https://support.google.com/work/android/answer/6174062，以了解有关启用 Android Enterprise 的信息。

连接 Ivanti Neurons for MDM 和 Android Enterprise

注册 Android Enterprise 后，将 Ivanti Neurons for MDM 设置为 UEM 服务器。

获取 Android Enterprise 凭据

步骤

1. 转到**管理员 > Android Enterprise**。
2. 单击 **Google 开发人员控制台**。
3. 单击显示的第一个链接转到 Google 开发人员控制台。
4. 从下拉菜单中选择**创建项目**。
5. 输入项目名称。
6. 接受服务条款。
7. 单击**创建**。
8. 单击 **API**。
9. 选择 **API**。
10. 在搜索字段中输入 **emm**，以查找 Google Play EMM。
11. 单击 **Google Play EMM API** 链接。
12. 单击**启用 API**。
13. 单击**凭据**。
14. 选择**服务帐户**。
15. 单击**创建**，以保存 JSON 文件。

将 Android Enterprise MDM 令牌添加到 Ivanti Neurons for MDM

步骤

1. 登录 https://admin.google.com。
2. 点击**安全**。
3. 如果没有看到 Android Enterprise 设置，请点击**显示更多**。
4. 选择 **Android Enterprise 设置**。
5. 在**管理企业移动管理提供商**下，复制 MDM 令牌。
6. 返回 Ivanti Neurons for MDM 门户。
7. 点击**完成**。
8. 在框 2 中，粘贴您刚刚复制的 MDM 令牌。
9. 在**域**字段中，输入您向 Google 申请的域。

10. 点击**选择文件**，上传下载的 JSON 文件。
11. 点击**连接**。
    连接成功后，系统会显示**已连接到 Google** 消息。
12. 在框 3 中，点击**授权**，以表明您要授予 Ivanti Neurons for MDM 对 Google 用户数据的访问权限。
13. 点击**接受**。
    系统会在 Ivanti Neurons for MDM 门户中显示**已连接到用户**消息。

在 Ivanti Neurons for MDM 与 Google 之间同步用户

向由 Ivanti Neurons for MDMIvanti Neurons for MDM 管理的 Android 用户部署 Android Enterprise 时，每位用户都必须在 Google 管理员门户上拥有相应的记录。 在 Ivanti Neurons for MDM 和 Google 管理员门户之间同步用户信息所需要的步骤，取决于您是否已设置与组织目录服务 (AD/LDAP) 的集成。

Active Directory/LDAP 用户

如果您已设置 AD/LDAP 与 Ivanti Neurons for MDM 的集成，则必须使用 Google Apps Directory Sync 设置 AD/LDAP 与 Google 管理员门户的集成。 有关更多信息，请查看 https://support.google.com/a/answer/106368?hl=en。

本地用户

如果您在 Ivanti Neurons for MDM 中只创建本地用户，并且不打算将其与目录服务集成，请完成以下步骤，以便通过 Google 管理员门户同步这些用户：

步骤

1. 请访问 https://admin.google.com 并登录 Google 管理门户。
2. 点击**用户**。
3. 点击右下角的**添加用户**或**添加多个用户**图标。
4. 为每位要使用 Android Enterprise 的 Ivanti Neurons for MDM 用户，添加具有与 Ivanti Neurons for MDM 用户相同用户名和电子邮件地址的 Google 用户。
5. 在 Ivanti Neurons for MDM 门户中，针对每个刚刚添加到 Google 管理员门户的 Ivanti Neurons for MDM 用户：
   a. 点击“用户”选项卡中的用户名链接，显示用户详细信息。
   b. 选择**将用户与 Google 用户目录同步**。
   c. 点击**与 Google 用户目录同步**。
   d. 确认 Google 状态列为“已启用”。

向支持的设备部署 Android Enterprise

部署 Android Enterprise 需要两个配置：

- Android Enterprise：公司拥有设备上的工作配置文件配置启用了 Android Enterprise。
- 锁定和 Kiosk 配置定义要应用的 Android Enterprise 限制。

停用注册的设备

在 BYOD 情景下，在公司拥有设备上从设备管理员切换为 Android Enterprise 工作配置文件，不需要停用和重新注册设备。 从设备管理员切换到设备所有者模式仅需要设备擦除或停用。

选择在“设备所有者”/“增强配置文件所有者”/“公司拥有个人启用”模式中注册的设备进行停用操作时，屏幕上会弹出窗口，指出“组织拥有的设备不支持停用命令”。

部署设备

步骤

1. 在 Ivanti Neurons for MDM 门户中，前往**配置**。
2. 点击 **Android Enterprise：工作配置文件**。
3. 点击**编辑**。
4. 点击**下一步**。
5. 选择**所有设备**或**自定义**。
6. 如果选择**自定义**，请搜索并选择应接受 Android for Work 设置的设备组。
7. 点击**完成**。
8. 点击**返回列表**（左上角）。
9. 点击 **+ 添加**。
10. 点击**锁定和 Kiosk：Android Enterprise**。
11. 在**名称**字段中输入标识配置的文本。
12. 在**选择锁定类型**下，选择**工作配置文件**。
13. 选择您要应用到目标设备中的锁定设置。
14. 点击**下一步**。
15. 选择**所有设备**或**自定义**。
16. 如果已选择“自定义”，请搜索并选择要接收 Android Enterprise 设置的设备组。
17. 点击**完成**。

> 在部署后，您无法对生成的配置文件进行更改。 相反，您需要创建新的 Android Enterprise 配置并进行部署。

确认部署

可以使用以下方式确认 Android Enterprise 已部署：

- 在**用户 > 用户**下，找到用户条目，然后检查 **Google 状态**是否为**启用**。
- 在**设备 > 设备**下，点击设备链接，然后确认 **Android Enterprise** 的状态是否为**已启用**。

用户的 **Google 状态**应列为**已启用**。 如果未启用，用户将无法注册设备。

> 对于非 G Suite 订阅企业，托管 Google Play 帐户方法允许用户注册 Android Enterprise。 如果 Android Enterprise 已设置为托管 Google Play 帐户，则只有在注册 Android Enterprise 设备后，用户才会显示为 **Google 状态：已启用**。 请参阅托管的 Google Play 账户，了解与 Google Play 账户有关的更多信息。

部署 Android Enterprise 应用

任何针对 Android Enterprise 开发的应用程序都可能包括可以通过 Ivanti Neurons for MDM 配置的选项。

步骤

1. 在 Ivanti Neurons for MDM 门户中，前往**应用程序 > 应用程序目录**。
2. 在 Google Play 商店中查找应用程序。
3. 单击应用程序条目。
4. 代表 Android Enterprise 用户接受权限。
5. 单击**下一步**。
6. 选择分配选项。
7. 展开**高级选项与应用配置**。
8. 按照以下指导方针完成相关选项：
9. 单击**下一步**。

设置	说明
在设备上安装	选择此选项在注册后立即开始安装。 除非设备是 Samsung Knox 设备，并且选择以下静默安装选项，否则将提示用户确认应用安装。
不在最终用户 App Catalog 中显示	选择此选项，如果您不希望用户在设备的 App Catalog 中看到此应用。
在 Samsung Knox 设备上进行静默安装	如果您不希望用户收到确认在 Samsung Knox 设备上安装的提示，选择此选项。
设置应用安装优先级	对于 Android Enterprise 应用程序，可以优先下载特定应用程序，然后再下载其他应用程序。 例如，您可以优先下载 Tunnel 和电子邮件应用，然后再下载其他非关键应用。 以下是可用的优先级选项： • **高** • 中（默认选择） • **低** 此设置适用于内部、公共、私有和 Web 应用程序。 内部应用通过客户端安装，公共和私人应用通过 Google 安装。 应用优先级仅适用于通过相同渠道安装的应用。
仅在连接到 Wi-Fi 时安装	选择此选项，以仅在设备连接到 Wi-Fi 时安装应用。
仅在充电时安装	选择此选项，以便仅在设备充电时安装应用。
仅在空闲时安装	选择此选项，以仅在设备空闲时安装应用（用户未主动使用）。
在安装时自动启动	选择此选项，在安装后自动启动应用。 仅在应用是新安装到设备而非版本更新时，此功能才可用。

10. 选择升级选项。
11. 单击**完成**。

配置商业应用

应用程序目录的“企业应用程序”部分中提供 Android Enterprise 应用程序，包括以下应用程序：

- Divide Productivity

- Email+
- 隧道
- GMail

10.10.4.6. Android Enterprise：工作托管设备非 GMS 模式 (AOSP)

Ivanti Neurons for MDM 支持“工作托管设备非 GMS 模式”(AOSP) 设备的设备所有者注册，无需 Google 移动服务 (GMS)。 这是一项系统配置，管理员无法添加配置。 管理员可以分发或取消分发。

步骤

1. 使用用户凭据登录 Ivanti Neurons for MDM。
2. Android Enterprise 的搜索配置：工作托管设备非 GMS 模式 (AOSP)。
3. 编辑配置，并将其分发到适合的设备组。 例如：Android 设备。
4. 单击**完成**。

10.10.4.7. Android 工作认证 (Work Challenge)

本部分包含以下主题：

- 创建 Android 工作认证 (Work Challenge) 配置：
- 设置配置设置

许可证：Silver

Android 工作认证 (Work Challenge) 配置可为用户定义安全密码，以访问工作配置文件数据和应用。 需要 Android Enterprise 工作配置文件。

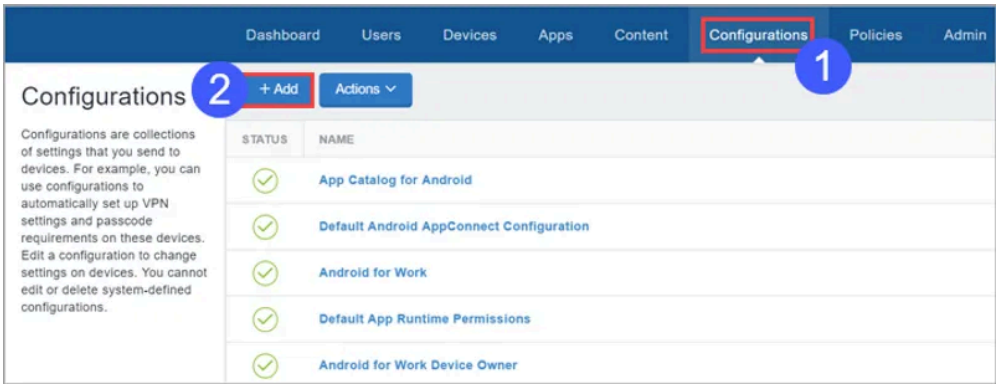
实施说明：

- 管理员可以独立应用设备密码策略和工作配置文件密码策略。
- Ivanti Neurons for MDM 不会将此配置发送到早于 Android 7.0 的客户端，因为此类设备不支持此功能。
  Ivanti Neurons for MDM 只会将此配置发送到具有 Android Enterprise 工作配置文件的设备。

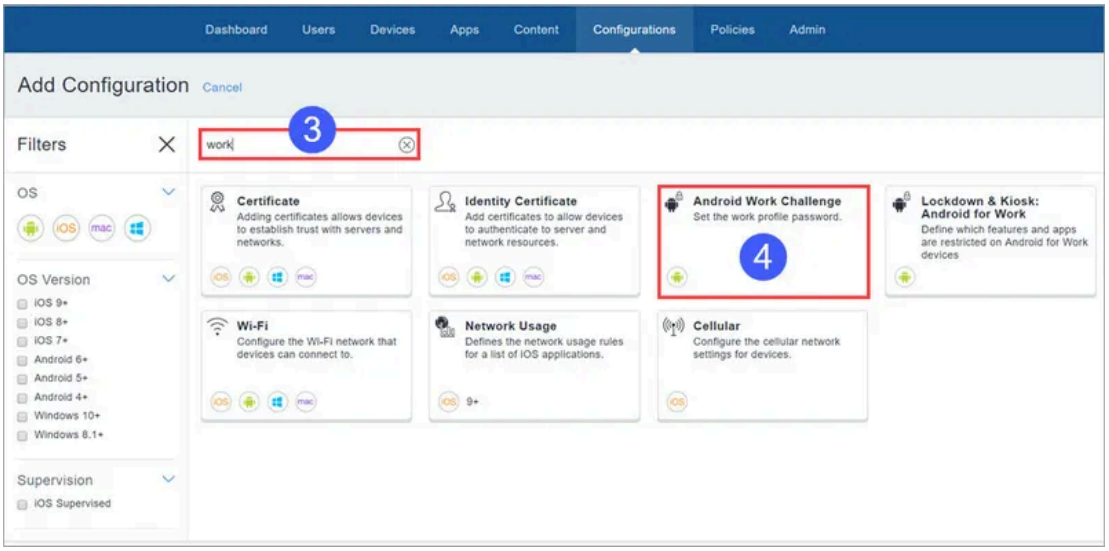
创建 Android 工作认证 (Work Challenge) 配置：

步骤

1. 单击**配置**。

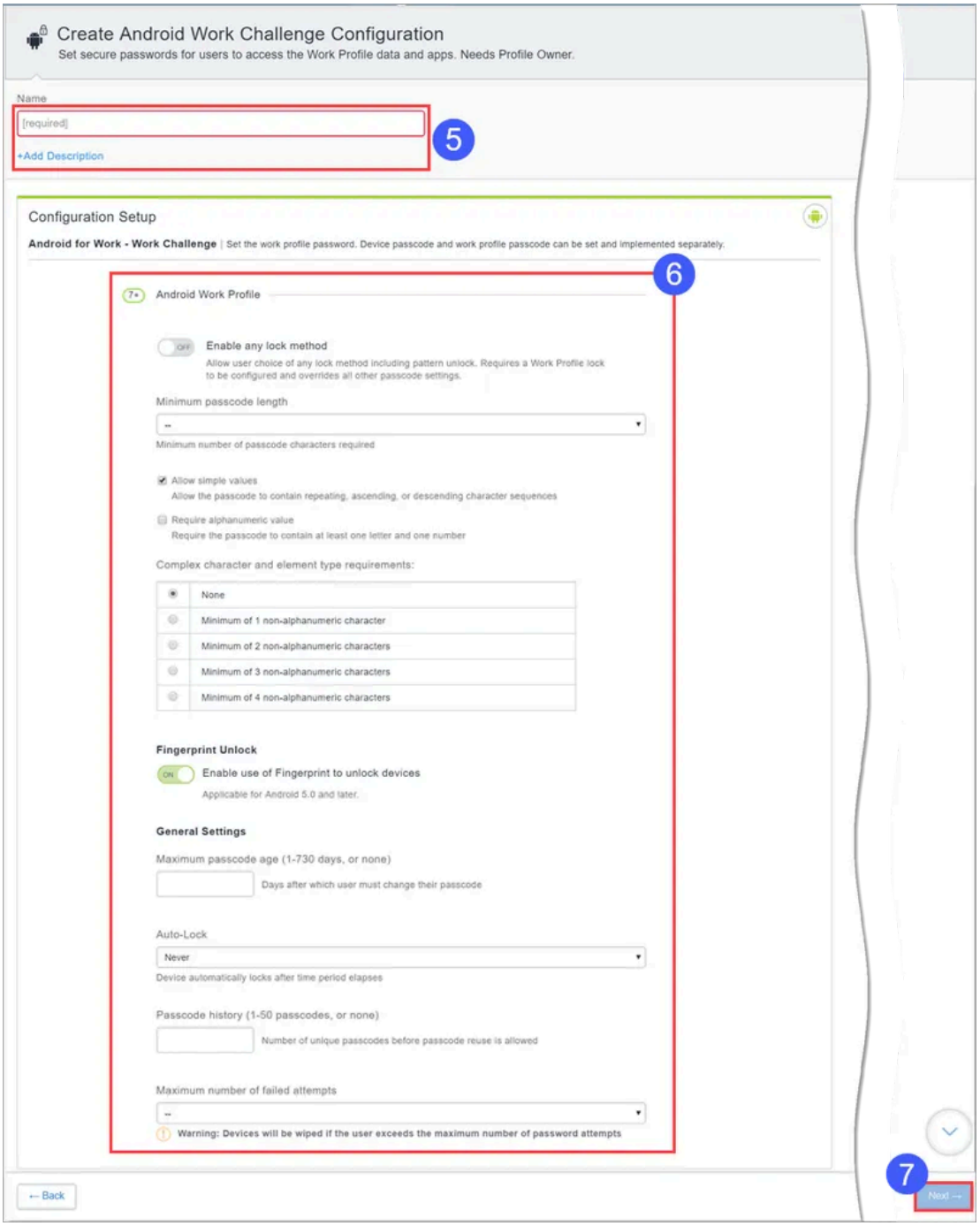


点击 **+ 添加**。



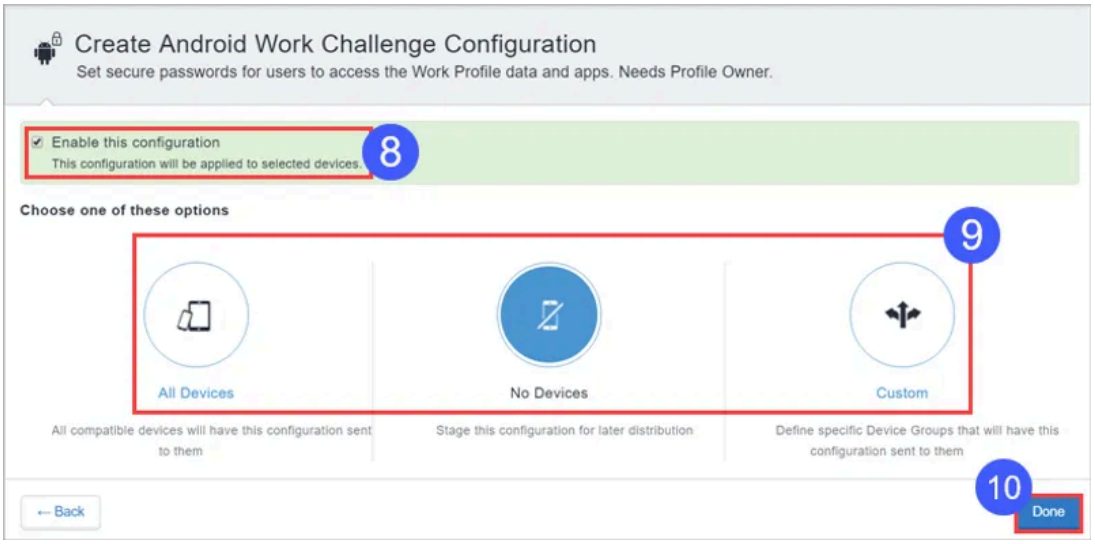
在搜索字段中输入“工作 (work)”。

4. 选择 **Android 工作认证 (Work Challenge)**配置。



输入配置的名称，以及可选的说明。

6. 使用"配置设置"字段创建配置。 请参考**设置配置设置**，了解有关设置的详细信息。
7. 单击**下一步 →**。



如果需要，启用配置。

9. 将分配设置配置为所有设备、无设备或自定义设备集。
10. 单击**完成**。

设置配置设置

设置	采取何种措施
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
启用任何锁定方法	允许用户选择任何锁定方法，包括图案解锁。 覆盖所有其他通行码设置。
最小通行码长度	选择最小通行码长度，从 4 到 16 个字符。
允许简单值	启用以便允许通行码包含重复、升序或降序字符序列。
需要字母数字值	启用以便要求通行码至少包含一个字母和一个数字。
复杂的字符和元素类型特征	配置复杂的字符和元素类型要求，范围为： • 无 • 最少 1 个非字母数字字符 • 最少 2 个非字母数字字符 • 最少 3 个非字母数字字符 • 最少 4 个非字母数字字符
指纹解锁	启用以便允许用户使用指纹解锁设备。
最大通行码寿命	配置最大通行码寿命，从无至 730 天。
自动锁屏	选择设备自动锁屏之前经过的时间段。 时间范围从无到 15 分钟。
通行码历史记录	指定允许密码重用之前所需的唯一通行码数量，范围从无至 50 个通行码。
最大失败尝试次数	选择最大失败尝试次数。 **警告：Ivanti Neurons for MDM 会擦除用户超过最大密码尝试次数的设备！**

10.10.4.8. 证书配置

证书配置可识别将要分发给设备的证书。 证书使设备可以建立与服务器和网络资源间的信任。 从版本 76 开始，我们仅支持 v3 证书。

作为管理员，您现在可为智能卡登录和自定义对象 ID (OID) 生成 Ivanti Neurons for MDM 证书。 您可为下列身份验证选项生成证书：

- 客户端身份验证 - 默认启用
- IPSEC – 可选，管理员可启用
- 智能卡登录 - 可选，管理员可启用
- 自定义 OID - 可选，管理员可启用

> 此功能仅适用于以下证书颁发机构 (CA)：

- 本地证书颁发机构
- 中间证书颁发机构
- 外部证书颁发机构 - 在 NDES 服务器中配置 CA 模板的应用策略，支持 IPSEC、智能卡登录和自定义 OID
- 本地 SCEP 证书颁发机构

分配配置

从 Ivanti Neurons for MDM 91 版本开始，全局管理员可以委派空间管理员来为所有设备和自定义分发选项编辑证书配置。 对于证书配置，可以视需要选择“允许在所有空间中提供此配置”。 此选项使证书配置适用于所有空间，且可用于 Exchange、Wi-Fi、VPN、依应用程序 VPN 和任何其他适用配置。 此选项适用于仅需要将证书配置作为关联配置的一部分来分发到设备（在非默认空间中）而不是作为单独配置分发的情况。

程序

1. 在名称字段中输入名称。
2. 上传证书文件。
3. 单击**下一步**。
4. 选择**启用此配置**选项。
5. 选择下列分配选项之一：
    - **所有设备**。 选择下列选项之一：
        - **不应用到其他空间**。
        - **应用于其他空间中的设备**。
            - 选中**允许空间管理员编辑分发**复选框，允许委派空间管理员编辑特定空间的分发。
    - **无设备**（默认）
    - **自定义**选择以下其中一个选项：
        - **不应用到其他空间**。
        - **应用于其他空间中的设备**。
            - 选中**允许空间管理员编辑分发**复选框，允许委派空间管理员编辑特定空间的分发。

> 无论空间有多少，证书配置可以配置到所有空间，分发到所有设备，并应用到其他设备空间中的所有设备。

6. 单击**完成**。

证书设置

作为管理员，您可以配置本地非 SCEP 证书颁发机构。

步骤

1. 登录 Ivanti Neurons for MDM 管理员门户。
2. 转到**管理** > **基础设施** > **证书管理** > **证书颁发机构**。
3. 单击 **+ 添加**。 将列出以下选项：

- **创建 Ivanti Neurons for MDM 提供的本地证书颁发机构**
- **使用您自己的现有 CA 签署 Ivanti Neurons for MDM 的本地 CA**
- **连接到公共可信 Cloud 证书颁发机构**。
- **连接本地 SCEP 证书颁发机构**。
- **连接本地非 SCEP 证书颁发机构**。

4. 填写以下相关字段：
5. 单击**完成**。

设置	流程
名称	输入用于识别此配置的名称。
URL	管理员必须从 OpenTrust 获得的 OpenTrust CA URL。
密码	输入身份验证证书的密码
身份验证证书	接受 OpenTrust/ IDnomic 提供的 .p12 文件格式。
TLS CA 证书链	接受 OpenTrust/IDonomic 提供的 PEM 文件格式。

在配置本地非 SCEP 证书颁发机构后，您必须创建身份证书。 根据配置文件 ID，填写完成设置所需的所有必填字段。

> 如果 SCEP CA 证书的生成由于以下两个原因失败，且阶段 2 的超时达到时，系统会生成一个通知：

1. 无法访问 Connector
2. 无法访问 CA 服务器

10.10.4.9. 证书透明度

适用于： iOS 12.1.1、macOS 10.14.2、tvOS 12.1.1、watchOS 10.0+、visionOS 1.1+ 以及支持的更高版本。

控制仅可在设备配置文件中显示的证书透明度强制实施。 您可以根据需要包含多个证书并禁用域。

创建证书透明度配置

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中，键入**证书**，然后单击**证书透明度**配置。
4. 输入名称并描述配置。
5. 指定**将禁用的域**。 单击 **+ 添加域**，以添加多个域。 前导句点可用于匹配子域，但域匹配规则不得匹配顶级域中的所有域。 例如，允许 ".example.com" 和 ".example.co.uk"，但不允许 ".com" 和 ".co.uk"。 不支持通配符域。
6. 在选择算法 (SHA 256) 后，指定**证书哈希**。 单击 **+ 添加**，以添加多个证书哈希。
7. 单击**下一步**，配置分配设置。
8. 单击**完成**。

要生成由 subjectPublicKeyInfo 字典中的哈希密钥指定的数据，将以下命令用于 PEM 编码的证书：

```
openssl x509 -pubkey -in example_certificate.pem -inform pem | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

如果证书使用 DER 编码，使用以下命令：

```
openssl x509 -pubkey -in example_certificate.der -inform der | openssl pkey -pubin - outform der | openssl dgst -sha256 -binary | base64
```

有关更多信息，请查看如何创建配置。

10.10.4.10. 证书吊销检查配置

此配置支持管理员检查从设备吊销的一系列证书。 管理员可以指定证书颁发机构 (CA)，这允许配置为链接到该 CA 的所有证书启用吊销检查。

适用于：iOS 14.2+ 和 visionOS 1.1+

步骤

1. 转到配置 > + 添加。
2. 在搜索字段中，键入证书，然后单击证书吊销检查配置。
3. 输入配置的名称和描述。
4. 将算法选为 SHA 256，并输入根证书的哈希。

> 在哈希中，您需要输入证书公钥的 Base64 编码（二进制）SHA-256 哈希。 有关 Apple 操作系统的可用受信任根证书，请查看 **Apple 文档**。 在此配置中，您可以添加多个根证书。

5. 单击下一步。
6. 选择启用此配置选项。
7. 选择下列分配选项之一：
   - 所有设备
   - 无设备（默认）
   - 自定义。
8. 单击完成。

10.10.4.11. 创建自主单应用程序模式配置

自主单应用程序模式配置可确保设备上只运行特定应用程序。 即使用户尝试启动其他应用程序，配置也只会启动特定应用程序。

程序

1. 转到**配置** > **添加** > **自主单应用程序模式**。
2. 使用以下指导原则定义应用和相关设置。
3. 单击**下一步**。

设置	流程
名称	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
配置设置	**捆绑标识符** -（必填）唯一捆绑标识符。 如果两个词典包含相同的 BundleIdentifier 值，但 TeamIdentifier 值不同，则将视为错误，且不会安装该配置文件。
	团队标识符 -（必填）开发人员的团队标识符，需要在签发应用程序时使用。

4. 在**分发**屏幕中，选择接收此配置的组。
5. 单击**完成**。

10.10.4.12. 创建 DNS 代理配置

作为 Ivanti Neurons for MDM 管理员，您可以使用面向 iPhone 和 iPad 设备用户的 DNS 代理配置来配置 DNS 代理设置。 可以使用 DNS 代理负载来指定提供 DNS 代理网络扩展和其他供应商特定值的应用程序。

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 转到**配置**
3. 在搜索字段中输入 **DNS**，然后点击 **DNS 代理配置**。
4. 输入名称并描述配置。
5. 输入以下 DNS 代理配置设置：
    - 应用程序捆绑标识符（必填）。
    - 提供程序捆绑标识符。
    - 提供程序配置（键值）。
6. 单击**下一步**。
7. 选择**启用此配置**选项。
8. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义

单击**完成**。

10.10.4.13. 设备日志记录配置

设备日志记录配置让您可以启用 Android 设备的网络和安全日志。

创建设备日志记录配置

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中，输入**设备日志记录**并选择配置。
4. 输入名称并描述配置。
5. 在**配置设置**部分，选择一个或两个选项：
    - 启用网络日志记录
    - 启用安全日志记录

> 有关支持的 Android 版本安全和网络日志记录，请参阅下面**安全日志记录矩阵**下的表格。

单击**下一步**，配置分配设置。

7. 单击**完成**。

安全日志记录矩阵

设备类型	支持的 Android 版本
工作托管设备和工作托管设备非 GMS 模式 (AOSP)	7、8、9、10、11、12、13
带有工作配置文件的托管设备	8、9、10
工作配置文件	不适用
公司拥有设备上的工作配置文件	11、12、13

网络日志记录矩阵

设备类型	支持的 Android 版本
工作托管设备和工作托管设备非 GMS 模式 (AOSP)	8、9、10、11、12、13
带有工作配置文件的托管设备	8、9、10
工作配置文件	12、13
公司拥有设备上的工作配置文件	12、13

在设备上安装设备日志记录配置后，用户会收到一个通知，其中有关于设备管理和网络日志记录的信息。 点击**确定**确认通知。

请求调试日志

步骤

1. 登录 Ivanti Neurons for MDM。
2. 前往**设备** > **设备详细信息**。
3. 在**概述**部分，点击**强制签入**旁边的三竖点按钮。
4. 选择**请求调试日志**。
5. 选择下列两个选项之一：
   - 排除错误报告 - 选择此选项并点击“下一步”，屏幕上将出现一个确认窗口。 点击**请求调试日志**。 用户无需对此选项予以同意，而且这些日志将排除所选 Android 设备的错误报告。
   - 包含错误报告 - 选择此选项并点击“下一步”，屏幕上将出现一个确认窗口。 点击**请求调试日志**。 用户必须对共享错误报告予以同意。如果是 Android 设备，系统将提示用户提交设备日志，以便包含错误报告。

10.10.4.14. 磁盘管理配置

Ivanti Neurons for MDM 磁盘管理配置设置可定义用于有效管理外部和网络存储设备中数据的策略。

适用范围：macOS 15.0 受监管设备至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**磁盘管理**配置。
3. 根据下表配置**磁盘管理**设置：

设置	描述
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
磁盘管理	
外部存储	从下拉列表中选择以下其中一个值： • **允许**：允许读取和写入存储。 • **只读**：允许读取存储。 • **不允许**：不允许访问存储。
网络存储	从下拉列表中选择以下其中一个值： • **允许**：允许读取和写入存储。 • **只读**：允许读取存储。 • **不允许**：不允许访问存储。

4. 单击**下一步**，配置分配设置。
5. 选择其中一个分发选项来设置**磁盘管理**配置。 有关配置分发选项的详细信息，请参阅使用配置。
6. 单击**完成**。

10.10.4.15. Android 加密

加密配置定义 Android 设备在设备管理员模式中的设备加密要求。 设备加密可确保已知的越狱和已获得 root 权限的产品无法访问敏感的公司数据。 加密可以不可读形式保存设备数据，即使设备丢失，也无法访问数据。

启用加密会提示设备用户加密设备，并需要设置设备密码。 要读取数据，必须使用通行码解密数据。 在设置密码时，设备加密将在 Android 企业（工作配置文件或受管设备）或 iOS 设备上自动启用。 加密时无法使用设备。 一旦启用加密，关闭它时会要求恢复设备的出厂设置。

加密设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
启用设备加密	选择该设置，为接收此配置的所有可加密 Android 设备开启加密。

> Android 11 设备管理模式下的 Samsung 设备不支持 Android 加密配置。 如果设置了设备密码，则 Android Enterprise 设备默认支持此加密。

有关更多信息，请查看**如何创建配置**。

10.10.4.16. 加密的 DNS

许可证：Gold

适用于：

- iOS 14.0 或支持的更新版本。
- macOS 11.0 或支持的更新版本。
- visionOS 1.1 或支持的更高版本。

配置加密的 DNS，这将帮您增强安全性，并且无需配置 VPN。

本部分包含以下主题：

- 加密的 DNS 配置
- 加密的 DNS 配置设置

加密的 DNS 配置

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中，键入 **DNS**，然后单击**加密的 DNS** 配置。
4. 输入名称并描述配置。
5. 输入加密的 DNS 配置设置。
6. 单击**下一步**。
7. 选择**启用此配置**选项。
8. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义
9. 单击**完成**。

加密的 DNS 配置设置

使用下表中的设置，以配置加密的 DNS。 有关这些设置的更多信息，请查看 Apple 文档。

设置	描述
DNS 设置	词典，用于定义加密的 DNS 服务器的配置。
DNS 协议	指定用于与 DNS 服务器通信的加密传输协议。 选择以下其中一个协议： • HTTPS • TLS
服务器 URL	如 RFC 8484 定义，HTTP-over-HTTPS 服务器的 URI 模板。 此 URL 必须使用 https:// scheme，并且 URL 中的主机名或地址将用于验证服务器证书。 如果未提供服务器地址，URL 中的主机名或地址将用于确定服务器地址。 仅在 DNS 协议是 HTTPS 时，此密钥才必须存在。
服务器地址	DNS 服务器 IP 地址字符串的未排序列表。 这些 IP 地址可以是 IPv4 和 IPv6 地址的组合。 单击**添加**，以添加一个或多个服务器地址。
补充匹配域	域字符串的列表用于确定哪些 DNS 查询将使用 DNS 服务器。 如果未提供此数组，所有域将使用 DNS 服务器。 单击**添加**，以添加一个或多个域。
禁止用户禁用 DNS 设置	禁止用户禁用 DNS 设置。 此密钥仅在受监管的设备中可用。
需求规则	一组定义 DNS 设置的规则。 如果规则不存在，系统会始终应用 DNS 设置。 单击 **+ 添加需求规则**，以添加一组或多组需求规则。
网络	如果此词典匹配当前网络，将采取的操作。 选择以下其中一个操作： • **连接：**在词典匹配时，应用 DNS 设置。 • **断开连接：**在词典匹配时，不应用 DNS 设置。 • **评估连接：**在词典匹配时，应用 DNS 设置及每个域例外。

评估连接	此网络选项拥有以下设置：
	• **域操作** - 指定域的 DNS 设置行为。 选择以下其中一个操作：
	  ◦ **从不连接** - 请勿将 DNS 设置用于指定域。
	  ◦ **按需连接** - 允许将 DNS 设置用于指定域。
	• **域** - 此评估应用的域。 单击 **+ 添加**，以添加一个或多个域。

规则	单击 **+ 添加**，以添加一个或多个规则，从而将以下参数与对应的指定值匹配。
DNS 域匹配	一组域名。 如果指定列表中的任何域名与设备搜索域列表中的任何域匹配，此规则匹配。
DNS 服务器地址匹配	一组 IP 地址。 如果任何网络的指定 DNS 服务器与数组中的任何条目匹配，此规则匹配。
SSID 匹配	一组匹配当前网络的 SSID。 如果网络不是 Wi-Fi 网络，或 SSID 未显示在此数组中，匹配失败。 忽略此密钥和对应的数组，以与任何 SSID 匹配。
接口类型匹配	接口类型。 如果指定，仅在主网络接口硬件与指定类型匹配时，此规则才会匹配。 选择以下其中一种类型： • 以太网

设置	描述
	• WiFi • 移动电话
URL 字符串探针	探测的 URL。 如果成功获取此 URL（返回 200 个 HTTP 状态代码）而不重定向，此规则匹配。

有关更多信息，请查看**如何创建配置**。

10.10.4.17. 外部智能设置

使用**外部智能设置**以配置受监控设备上的外部智能集成。 此配置可帮助管理员应用基于策略的一致设置，以控制设备连接和使用支持的外部智能服务的方式。

适用于：

- iOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- macOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- visionOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**外部智能设置**配置。
3. 按照下表配置**外部智能设置**配置：

设置	采取何种措施
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
允许外部情报集成	选中复选框以启用外部智能集成。 切换**推送至设备**按钮，以在受监控设备上启用外部智能集成。
允许外部智能集成登录	选中复选框以启用外部智能集成登录。 切换**推送至设备**按钮，以在受监控设备上启用外部智能集成登录。
允许外部智能工作区 ID	输入工作区 ID 以启用外部智能。 切换**推送至设备**按钮，以在受监控设备上为输入的工作区 ID 启用外部智能。

4. 单击**下一步**，配置分配设置。
5. 选择一个分发选项以设置**外部智能设置**配置。 有关配置分发选项的详细信息，请参阅使用配置。
6. 单击**完成**。

10.10.4.18. 威胁防御

适用于：

- Go for iOS 客户端版本 3.2.0 或支持的较新版本。
- Go for Android 客户端版本 52 或支持的较新版本。

Ivanti Neurons for MDM 包含分发激活令牌的功能，以启用集成到 Go for Android 和 iOS 客户端的威胁防御技术。 Threat Defense 可以避免托管设备受到影响设备、网络和应用的移动威胁和漏洞的破坏。

在 Ivanti Neurons for MDM 中启用此配置并应用于设备后，将在 Go 客户端上启用威胁防御库。 通过移除许可证令牌并向客户端重新发送许可证配置，Threat Defense 服务可以取消激活。

Threat Defense 监视：

- 在设备级别：系统参数、配置、固件和库来识别可疑或恶意活动。
- 在网络级别：网络流量和移动设备之间的可疑连接。
- 在应用程序级别：通过风险评估和代码分析，泄漏应用程序（可能会将企业数据置于危险之中）和恶意应用程序。

最新文档

有关最新的威胁防御指示，请查看产品文档网站上 **Ivanti Neurons for MDM 产品文档**中的 *Ivanti Neurons for MDM 威胁防御解决方案指南*。

10.10.4.19. FileVault 2

许可证：Gold

FileVault 2 提供对卷的内容执行完整 XTS-AES 128 磁盘加密的能力。

启用 FileVault 2 时，以下设置可用于配置：

类别	设置
FileVault 用户设置	• 在 SetupAssist 期间启用 FileVault **默认值**：False • 如果为 True，并且在设置助手中注册 Ivanti Neurons for MDM 后安装负载，则它会在设置时请求设置助手启用 FileVault。 此外，系统会忽略此负载中除 ShowRecoveryKey 之外的所有其他密钥。 **先决条件**：在设置助手中启用 FileVault 之前，请确保在设备注册配置文件中已启用**在设备注册设置期间等待设备配置**。 • 推迟启用 FileVault，直到指定的用户注销 ◦ 始终提示用户启用 FileVault ◦ 用户可以绕过启用 FileVault 的最大次数 在用户注销时不要请求启用 FileVault
输出路径	输入将存储恢复密钥以及计算机信息 plist 的所在位置的路径。
个人恢复密钥	• 创建个人恢复密钥 • 启用 FileVault 后向用户显示个人恢复密钥 只有在**创建个人恢复密钥**启用时，此选项才可见。 选项默认禁用。 • 启用机构恢复密钥：使用密钥链 - 如果该有效载荷中没有提供证书信息，将使用已经在 /Library/Keychains/FileVaultMaster.keychain 中创建的密钥链。 选择下列选项之一： ◦ 上传证书 ◦ 证书 ◦ 在用户系统上使用密钥链
__ 天后轮换 FileVault 密钥	管理员可以为 macOS 设备配置 FileVault 密钥的定期轮换，以此降低已部署设备的安全风险。 管理员可以按天设置轮换间隔。 仅轮换个人恢复密钥。

10.10.4.20. FileVault 恢复密钥

许可证：Gold

FileVault 恢复密钥配置确定将 FileVault 恢复密钥重定向并托管到企业服务器。

> 由于 macOS 设备在重新推送配置时停止发送恢复密钥，因此禁用排除和重新推送 FileVault 恢复密钥配置。

您可以设置以下选项：

设置	描述
名称	输入用于识别此配置的名称。
说明	（可选）输入阐明此配置目的的说明。
适用于 macOS <10.13 的配置设置	
将恢复密钥存储到 Ivanti Neurons for MDM 租户	选择以启用 Ivanti Neurons for MDM，以便将密钥存储在租户上。 需要时，密钥可以从设备详细信息页解密。
将 URL 重定向到服务器 **适用于 macOS 10.13+ 的配置设置** 定位	输入以下设置： • 输入应向其发送 FDE 恢复密钥的**重定向 URL**，而不是 Apple。 URL 必须以 https:// 开头。 • 从下拉列表中选择证书。 仅支持 PKCS1 格式的证书。 （必需）针对恢复密钥将被托管的位置，输入简短说明。 此文本将插入到用户启用 FileVault 时可以看到的消息中。
设备密钥	（可选）如果用户似乎忘记了密码，则可以在帮助文本中包含可选字符串。

10.10.4.21. FileVault 选项配置

此配置支持管理员在系统进入待机状态时，启用或禁用 FileVault 并销毁 FileVault 密钥。

适用于：macOS 10.7+

程序

1. 转到**配置** > **+添加**。
2. 在搜索字段中，键入 FileVault，然后单击 FileVault 选项配置。
3. 输入配置的名称和描述。
4. 在配置设置中，选择所需选项：
    - 在系统进入待机模式时，销毁 FileVault 密钥
    - 不允许禁用完整磁盘加密
    - 不允许启用完整磁盘加密
5. 单击下一步。
6. 选择启用此配置选项。
7. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义。
8. 单击完成。

10.10.4.22. 身份证书

本部分包含以下主题：

- 身份证书设置
- 分配配置

身份证书配置可定义移动设备的证书身份验证机制。 身份证书是 X.509 证书（.p12 或 .pfx）。 此外，可以使用证书颁发机构作为源来动态生成身份证书。 开始前，您应已知道计划如何将证书分发给您的移动设备。 您也应已对任何必需的证书颁发机构进行配置。

> 从版本 91 开始，Apple 设备的设备身份证书会在到期后 30 天内自动续订。 iOS 设备将从 Ivanti Neurons for MDM 接收更新的 MDM 证书，这会成为常规设备签入流程的一部分。 然而，如果 iOS 设备离线太久，导致 MDM 证书在签入之前便已过期，则需要重新注册 Ivanti Neurons for MDM 才能在过期前更新证书。

- 创建身份证书时，不推荐使用 SHA-1 证书。 您可以选择其他算法。 更新证书时，如果旧的证书使用 SHA-1，则可以使用相同的 SHA-1 算法。 如果较旧的证书使用 SHA-1 以上的算法，则不允许切换到 SHA-1。
- 在配置身份证书后，您可以单击**测试证书**，并继续发布和验证测试证书的有效性。 如果主题名称与本地证书颁发机构相同，将通过对全新或现有动态生成的身份证书配置执行此测试的方式显示错误。 在显示此错误消息时，您应修改身份证书主题名称；该名称应与本地证书颁发机构主题名称不同。 对于使用主题名称修改的现有身份证书配置，将重新颁发证书，并重新推送配置。
  如果设置选项，创建配置，而不为**动态生成**的证书分发颁发测试证书，单击**继续**。
- 将隐式重新颁发证书。
- 将身份证书分配给 Android 应用程序时，用户的应用程序将获取身份证书，而不会提示用户授予使用证书的权限（而不是应用程序）。 它包括所有的应用程序，如 Email+、Gmail 等。
- Email+ 可以通过用户提供的身份证书进行配置，并作为应用配置推送和分配到 Android Enterprise 设备。 仅适用于公司拥有设备上的工作配置文件和设备所有者模式。

身份证书设置

设置	采取何种措施
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
证书分发	选择要设置的证书分发类型： • **单一文件**：将现有要分发的证书上传至设备。 • **动态生成**：使用本地或外部证书颁发机构，根据请求创建证书。 • **用户提供**：为要由用户上传的证书类型创建标签。 创建后，用户将能够在自助服务门户中查看创建的标签（选项），并上传与这些标签相对应的证书。 • **派生凭据：**指定以下其中一种派生证书用法： ◦ 身份验证 ◦ 加密 ◦ 签名 ◦ 解密 • **SCEP 配置**：指定从 SCEP 服务器请求证书的方式。 选择下列配置之一： ◦ Apple 配置 ◦ Windows 配置 您的选择决定在表格剩余部分显示的选项。
允许所有应用访问私钥 (macOS 10.10+) 单个文件 身份证书数据 密码 **动态生成** 来源 创建配置而不颁发测试证书 仅 Windows - 目标证书存储	**适用于：**单文件身份证书、动态生成的身份证书、用户提供的身份证书和 SCEP Apple 配置身份证书。 （可选）对于 PKCS#12 证书，启用**允许所有应用访问私钥**选项，以允许所有应用访问私钥。 例如，对于用户请求密码，才允许访问用于 VPN 的证书，此密钥可以在此情况下使用。 将证书文件拖动到虚线框中，或者单击**选择文件**以从文件系统中进行选择。 输入保护 PKCS#12 证书文件的密码。 此密码用于不提示安装。 从下拉菜单中，选择本地证书颁发机构。 您应已在**管理员 >** 证书管理中创建此 CA。 选中复选框，以创建配置，而非颁发测试证书。 现在，管理员可以在 Windows 设备上选择目标证书存储。
用户提供	
证书显示名称	输入证书的名称。 此证书名称对于租户而言是唯一的，用户在上传证书时将能够在自助服务门户中查看该名称。
删除私钥	选择此选项，以在 *n* (1-30) 天后删除证书的私钥。 您也可以使用 Ivanti Neurons for MDM 为这些操作提供的 API。 请参考 Ivanti Neurons for MDM *API 指南*，了解与 API 有关的更多信息。

设置	采取何种措施
	如果您尝试在删除私钥后在任何配置中使用此证书（例如，对应用进行身份验证或推送 WiFi 或 VPN 配置），任务将失败。 确保在删除私钥之前执行任务。
删除几天后的私钥	选择清除证书私钥后的天数（1 - 30 天）。 默认值为 2 天。
派生凭据	
衍生证书使用情况	选择以下任一选项： • **身份验证** - 指定用于身份验证的派生凭据。 • **加密** - 指定将派生凭据用于加密。 • **签名** - 指定用于签名的派生凭据。 • **解密** - 指定将派生凭据用于解密。
品牌	从下列选项中选择您使用的派生凭据提供商： • **Entrust** • **Intercede** • **Purebred** 要添加您使用的自定义派生凭据提供商，请查看派生凭据提供商。
ACME 配置 - 仅适用于 iOS/iPadOS16+ /macOS14+	
客户端标识符	标识特定设备的唯一字符串
目录 URL	（必填）ACME 服务器的目录 URL。 URL 必须使用 https 方案。
扩展密钥用法	此值为字符串数组。 每个字符串都是以点式表示法表示的 OID。 例如，["1.3.6.1.5.5.7.3.2", "1.3.6.1.5.5.7.3.4"] 表示客户端身份验证和电子邮件保护。 设备为 ACME 服务器颁发的证书请求此字段。 ACME 服务器可以在其颁发的证书中覆盖或忽略此字段。
密钥大小	（必填）KeySize 的有效值取决于 KeyType 和 HardwareBound 的值。 请查看这些密钥了解具体要求。
密钥类型	（必填）要生成的密钥对的类型。
主题	（必填）输入以逗号分隔的 OID 和值数组表示的 X.500 名称。 通常，主题设置为用户的完全限定域名。 例如，C=US、DC=com、DC=MobileIron、OU=InfoTech 或 CN=www.mobileiron.com。 您也可以将变量附加到 OID，从而自定义主题。 例如，CN=www.mobileiron.com-$。 为了便于配置，您还可以使用 $ 变量来用用户的 FQDN 填充主题。 请勿在主题名称中使用反斜杠字符 (\)。
主题备用名称	设备为 ACME 服务器颁发的证书请求的主题备用名称。 ACME 服务器可以在其颁发的证书中覆盖或忽略此字段。
密钥用法	此值为 bit 字段。 Bit 0x01 表示数字签名。 Bit 0x10 表示密钥协议 设备为 ACME 服务器颁发的证书请求此密钥。 ACME 服务器可以在其颁发的证书中覆盖或忽略此字段。

设置	采取何种措施
硬件绑定	如果硬件绑定设置为 true，则表示已将私钥绑定到设备，此时密钥类型必须为 ECSECPrimeRandom，密钥大小必须为 256 或 384。
证明	如果为 true，设备会向 ACME 服务器提供描述设备的认证和生成的密钥。 证明为 true 时，硬件绑定必须也为 true。
SCEP 配置 - Apple 配置	
身份证书(SCEP)	选择以指定 SCEP 服务器。
本地证书颁发机构	选择以指定您已在**管理员 >** 证书管理中创建的本地证书颁发机构。 选择此选项时会出现下拉菜单，在该下拉菜单中选择本地证书颁发机构。
URL	输入 SCEP 服务器的 URL。
CA 标识符	输入证书颁发机构提供的标识符。
主题	输入 X.500 名称，并用 OID 和值的逗号分隔数组表示。 通常，主题设置为用户的完全限定域名。 例如，C=US、DC=com、DC=MobileIron、OU=InfoTech 或 CN=www.mobileiron.com。 您也可以将变量附加到 OID，从而自定义主题。 例如 CN=www.mobileiron.com-$DEVICE_CLIENT_ID$。 为简化配置，您还可以使用 $USER_DN$ 变量，根据用户的 FQDN 填充主题。 请勿在主题名称中使用反斜杠字符 (\)。
主题备用名称类型	根据证书模板的属性，选择 RFC 822 名称、DNS 名称、统一资源标识符或无。
主题备用名称值	输入相应类型的值。 如果输入的第一个字符为 $，则系统会显示下拉列表，其中可能包含自定义 LDAP 和 Entra ID 属性。 从列表中选择适当的自定义属性。 如果使用 Entra ID 值，则仅支持 onPremisesImmutableId。 输入 fn:base64tohex($)
NT 主体名称	输入 Microsoft 环境的主题备用名称。 此项通常配置为包括用户的 UPN（用户主体名称）。
质询	（可选）用作自动注册的预共享机密
重试	在列表中选择，以设置第一次返回“待处理”状态后将尝试的身份验证次数。
重试延迟	在列表中选择，以设置在重试前等待的秒数。
密钥大小	选择 1024、2048 或 4096 位。
用作数字签名	选择是否可将证书用于签名。
用作密钥加密	选择是否可将证书用于加密。
CA 指纹	如果您的证书颁发机构使用 HTTP，输入十六进制字符串，以用作 CA 证书的指纹。 支持 MD5 指纹。 如果您愿意，您可以从证书创建指纹。 只需将证书拖放到指定区域，或单击**从证书创建**，从文件系统中选择证书。
SCEP 配置 - Windows 配置	

设置	采取何种措施
CA（证书颁发机构）	选择以指定您已在**管理员 >** 证书管理中创建的本地证书颁发机构。 在选择此选项时会出现下拉菜单，在该下拉菜单中选择证书颁发机构。
主题	输入 X.500 名称，并用 OID 和值的逗号分隔数组表示。 通常，主题设置为用户的完全限定域名。 例如，C=US、DC=com、DC=MobileIron、OU=InfoTech 或 CN=www.mobileiron.com。 您也可以将变量附加到 OID，从而自定义主题。 例如 CN=www.mobileiron.com-$DEVICE_CLIENT_ID$。 为简化配置，您还可以使用 $USER_DN$ 变量，根据用户的 FQDN 填充主题。 请勿在主题名称中使用反斜杠字符 (\)。
主题备用名称类型	单击 **+ 添加**，以根据证书模板的属性，选择 RFC 822 名称、DNS 名称、统一资源标识符或无。
重试	在列表中选择，以设置第一次返回“待处理”状态后将尝试的身份验证次数。
重试延迟	在列表中选择，以设置在重试前等待的秒数。
密钥长度	选择密钥大小（1024、2048 或 4096 位）。
选择用法	选择至少一个选项： • 用作数字签名 - 选择证书是否可用于签名。 • 用作密钥加密 - 选择证书是否可用于加密。
有效性	选择有效期（天、月或年）。
CA 拇指指纹	如果您的证书颁发机构使用 HTTP，输入十六进制字符串，以用作 CA 证书的指纹。 支持 MD5 指纹。 如果您愿意，您可以从证书创建指纹。 只需将证书拖放到指定区域，或单击**从证书创建**，从文件系统中选择证书。
哈希算法系列	选择 SHA-2 或 SHA-3 算法。

在将身份证书应用于设备上的工作配置文件而不设置工作认证 (Work Challenge) 通行码时，设备会提示输入设备通行码，而不是工作认证 (Work Challenge) 通行码。

有关详细信息，请参阅使用配置。

10.10.4.23. Apple 激活锁定配置

许可证： Silver

本部分包含以下主题：

- 启用 iOS 激活锁定
- 在受监管设备上启用 iOS 激活锁定功能
- 启用 macOS 激活锁定
- 在受监管设备上启用 macOS 激活锁定功能
- 使用 iOS 激活锁定绕过代码
- 清除 iOS 激活锁定绕过代码

激活锁定是阻止任何人使用丢失或被盗设备的 Apple 特性。 在启用查找我的后，iCloud 帐户与此设备硬件标识符之间的映射会保存到 Apple 的激活服务器。 从那时起，在不输入现有 Apple ID 和密码的情况下，没有人可以禁用查找、清除设备，或重新激活。 如果有除用户之外的人擦除设备，并尝试重新启动和使用，将会出现提示，要求在“设置助手”中输入 Apple ID 和密码。

如果最终用户已经启用“查找我的设备”，则禁用激活锁定不会在被监控设备上禁用此特性。 当设备重置或者远程擦除后，“设置助手”将提示用户做出操作。

“激活锁定”为管理员提供更多阻止被监控设备被盗的选择。 但是，大部分企业的管理员很可能不会启用“激活锁定”特性，因为该特性主要是供个人使用。 下表概括企业有责任部署的选项：

设备类型	结果
企业有责任且被监控	• 默认在被监控设备禁用激活锁定。 • 设备用户无法打开“激活锁定”。
企业有责任且未被监控	• 一旦最终用户使用其 Apple ID 登录 iCloud，并打开“查找我的设备”，激活锁定就将启用。 • MDM 服务器（含 Ivanti Neurons for MDM）无法在未受监管的设备上控制激活锁定。 设备用户可以使用其个人凭据锁定激活，在他们离开公司后您将无法追索。

启用 iOS 激活锁定

适用于： iOS 7+ 受监管

此配置将应用于启用查找功能的受监管设备（iOS 7 和更高版本）。 如果管理员或其他用户尝试擦除、激活或者禁用此设备上的“Find My Device”，将显示 Apple 的激活锁定屏幕。 要继续操作，必须输入 iTunes 凭据或者跳过代码。

被监控设备的跳过代码将在激活后保存，可以在设备详细信息中查看。 对于受监管的设备，使用“清除激活锁定”命令远程发送绕过代码。 但是，重新激活设备或者关闭“Find My Device”特性时，必须手动输入代码。

> 对于所有空间，您仅可以创建一个激活锁定配置。

在受监管设备上启用 iOS 激活锁定功能

步骤

1. 在设备上，启用**查找我的**功能。

2. 转至**配置**。
3. 从现有配置的列表，选择 **Apple 激活锁定**配置。
4. 单击**编辑**。
5. 在 iOS 7+ 受监管部分中，单击**启用激活锁定**。
6. 单击**完成**。
7. 注册设备。

启用 macOS 激活锁定

适用于： macOS 10.15+ 受监管

此配置将应用于安装 macOS 10.15 和更高版本的受监管设备。 macOS 中的激活锁定应用于具有 Apple T2 Security Chip 的 Macs。 激活锁定会在监管设备（不论升级或新安装）和升级当前注册的设备上默认关闭。 启用查找不会在这些设备上自动启用激活锁定

如果管理员或其他用户尝试在设备上擦除、激活或禁用查找功能，将显示 Apple 激活锁定屏幕。 要继续操作，必须输入 iTunes 凭据或者跳过代码。 被监控设备的跳过代码将在激活后保存，可以在设备详细信息中查看。 对于受监管的设备，使用"清除激活锁定"命令远程发送绕过代码。 但在重新激活设备或关闭查找功能时，必须手动输入代码。

> 对于所有空间，您仅可以创建一个激活锁定配置。

在受监管设备上启用 macOS 激活锁定功能

步骤

1. 在设备上，启用查找功能。
2. 转至**配置**。
3. 从现有配置的列表，选择 **Apple 激活锁定**配置。
4. 单击**编辑**。
5. 在 macOS 10.15+ 受监管部分中，单击**启用激活锁定**。
6. 单击**完成**。
7. 注册设备。

使用 iOS 激活锁定绕过代码

在擦除启用 iOS 激活锁定的设备时，旁路代码会保留在 Apple 激活服务器和 Ivanti Neurons for MDM 管理界面中。

步骤

1. 转到**设备**。
2. 选择该设备。
3. 单击**操作 > 擦除**。 设备重启可能需要数分钟。
4. 在设备提示您输入 Apple ID 和密码时，将 **Apple ID** 留空。
5. 在**密码**字段中，输入绕开代码。
6. 单击**下一步**。
7. 继续设置。

清除 iOS 激活锁定绕过代码

当 iOS 激活锁定在 Ivanti Neurons for MDM 管理界面中清除时，旁路代码将从 Apple 激活服务器中移除，但仍会显示在 Ivanti Neurons for MDM 管理界面的设备详细信息中。

步骤

1. 转到**设备**。
2. 选择该设备。
3. 选择**配置**。
4. 选择 **Apple 激活锁定**。
5. 单击**编辑**。
6. 在 iOS 7+ 受监管部分中，禁用**启用激活锁定**。
7. 单击**完成**。
8. 转到**设备**。
9. 选择该设备。
10. 单击**操作 > 擦除**。 设备重启可能需要数分钟。 该设备现在可以使用新用户的 Apple ID 和密码进行设置。
11. 继续设置。

界面会显示清除 iOS 激活锁定的状态，如下所示：

状态	结果
挂起	• 服务器正在向 Apple 发送清除激活锁定代码。
已发送	• Apple 确认收到清除激活锁定代码。
失败	• 服务器无法将代码发送到 Apple。 • Apple 报告错误。

10.10.4.24. iOS 自定义配置

通过 iOS 自定义配置，您可以上传并分发 iOS 配置配置文件，该文件由其他应用创建而成，如 Apple 的 iPhone 配置实用程序。

iOS 自定义设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
文件数据	拖放配置文件，或单击**选择文件**，从文件系统中选择。

有关更多信息，请查看**如何创建配置**。

10.10.4.25. 智能设置

使用智能设置配置受监控设备上的 Apple Intelligence 设置。 此声明可帮助管理员应用基于策略的一致控件，以管理设备访问和使用 Apple Intelligence 功能的方式。

适用于：

- iOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- macOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- visionOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**智能设置**配置。
3. 按照下表配置**智能设置**：

设置	采取何种措施
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
允许 Apple Intelligence 报告	选中复选框以启用 Apple Intelligence 报告。 切换**推送至设备**按钮，以在受监控设备上启用 Apple Intelligence 报告。
允许 Genmoji	选中复选框以启用 Genmoji。 切换**推送至设备**按钮，以在受监控设备上启用 Genmoji。
允许 Image Playground	选中复选框以启用图像播放区。 切换**推送至设备**按钮，以在受监控设备上启用图像播放区。
允许 Image Wand	选中复选框以启用图像操作棒。 切换**推送至设备**按钮，以在受监控设备上启用图像操作棒。 此设置不适用于 macOS 设备。
允许个性化手写结果操作棒	选中该复选框以启用个性化手写结果操作棒。 切换**推送至设备**按钮，以在受监控设备上启用个性化手写结果。 此设置不适用于 macOS 和 visionOS 设备。
允许视觉情报摘要	选中复选框以启用视觉智能摘要。 切换**推送至设备**按钮，以在受监控设备上启用视觉智能摘要。 此设置不适用于 macOS 和 visionOS 设备。
允许书写工具	选中复选框以启用写入工具。 切换**推送至设备**按钮，以在受监控设备上启用写入工具。
强制仅设备上听写	选中复选框以启用“仅设备上听写”。 切换**推送至设备**按钮，以在受监控设备上启用仅设备上听写。
强制仅设备上翻译	选中复选框以启用仅设备上翻译。 切换**推送至设备**按钮，以在受监控设备上启用仅设备上翻译。 此设置不适用于 macOS 和 visionOS 设备。
应用	
日历	
允许自然语言编辑	选中该复选框以在日历和提醒中启用自然语言编辑。 切换**推送到设备**按钮，以在受监督设备上的日历和提醒中启用自然语言编辑。
邮件	
允许智能回复	选中复选框以启用智能回复。 切换**推送至设备**按钮，以在受监控设备上启用智能回复。
允许摘要	选中复选框以启用摘要。 切换**推送至设备**按钮，以在受监控设备上启用摘要。

设置	采取何种措施
注释	
允许转录	选中复选框以启用转录。 切换**推送至设备**按钮，以在受监控设备上启用转录。 此设置不适用于 visionOS 设备。
允许转录摘要	选中复选框以启用转录摘要。 切换**推送至设备**按钮，以在受监控设备上启用转录摘要。 此设置不适用于 visionOS 设备。
Safari	
允许摘要	选中复选框以启用摘要。 切换**推送至设备**按钮，以在受监控设备上启用摘要。

4. 单击**下一步**，配置分配设置。
5. 选择其中一个分发选项来设置**智能设置**配置。 有关配置分发选项的详细信息，请参阅使用配置。
6. 单击**完成**。

10.10.4.26. iOS 限制

iOS 限制可通过设置，帮助设备主要用户控制其他用户可以对 iOS、watchOS 和 visionOS 设备执行的操作。 这些设置由 Apple 进行定义，并由 Ivanti Neurons for MDM 管理。

在将此配置分发到**共享 iPad** 期间，您可以选择设备渠道或用户渠道。 对于分发单独配置并强制实施仅适用于设备或用户渠道的限制，这非常有用。

全局管理员可以委派空间管理员，以便为**所有设备和自定义分发**选项编辑配置。 对于 iOS 限制配置，可以视需要选择**允许在所有空间中提供此配置**。

> 分发更改仅适用于特定空间。 所有其他空间会继续继承默认空间分发设置。

iOS 限制设置

类别	设置	采取何种措施
设备功能	名称	输入用于识别此配置的名称。
	说明	输入阐明此配置目的的说明。
	iOS 所有版本	**启用设备功能。**
	允许屏幕截图和屏幕录制	选择以允许设备用户使用内置 iOS 屏幕捕获功能捕获屏幕。
	允许远程屏幕观察（iOS 9.3 及更高版本）	选择以允许用户观看远程屏幕。
	允许强制不提示受管教室屏幕观察（仅限受监管 - iOS 10.3+）	（仅适用于 iPad）当被监控的 iPad 配置有托管类时，选择此选项可允许屏幕上显示无提示信息。
	允许漫游时自动同步	选择以允许设备不在其本国/地区时同步邮件帐号。
	允许 Siri	选择以允许在受支持设备上启用个人助理应用。
	允许设备锁定时启用 Siri	选择以允许个人助理应用在设备锁定时执行任务。
	启用 Siri 脏话过滤（仅限监管）	选择启用 Siri 脏话过滤。
	允许语音拨号	选择此项可允许用户通过与设备对讲拨通联系人电话或拨号。
	允许应用内购买	选择以允许用户通过设备上运行的应用进行购买。
	允许设备锁定时启用 Passbook	选择以允许在设备锁定时显示通行证通知。
	允许锁定屏幕“控制中心”	选择以允许从锁定屏幕访问“控制中心”。
	允许锁定屏幕“通知”视图	选择以允许在锁定屏幕上显示通知。
	允许锁定屏幕“今日”视图	选择此项以允许从锁定屏幕访问“今日”视图。
	允许从托管应用到未托管应用的打开方式	**需要 Gold 许可证**。 选择以允许托管应用和帐号中的文档在非托管应用和帐号中打开。 禁用此项可防止文档从托管应用和帐号交换到非托管应用和帐号。 例如，您可能要防止个人应用打开企业文档。 您还可以使用此选项（禁用）以及托管的域配置，从而确保只能在托管应用中打开从托管的域中下载的数据。

类别	设置	采取何种措施
	允许从未托管应用到托管应用的打开方式	**需要 Gold 许可证**。 选择以允许非托管应用和帐号中的文档在托管应用和帐号中打开。 禁用此项可防止文档从非托管应用和帐号交换到托管应用和帐号。 例如，您可能要防止用户使用公司电子邮箱发送个人文档。 您还可以使用此选项（关闭）以及托管的域配置，从而确保在托管应用中无法打开从非托管的域中下载的数据。
	首次 AirPlay 配对要求有通行码	选择后要求 Apple TV 显示密码，用户必须在 iOS 设备上输入此密码，以便对设备的初始配对授权。
	在 AirPlay 传入请求上强制使用密码（tvOS 10.1 以上版本）	对于所有传入 AirPlay 请求，选择需要用户输入密码。 默认：取消选择
	iOS 26+	
	不受评级限制的应用程序（适用于 iOS 26.1+）	仅当捆绑包 ID 包含在多个有效载荷和家长控制应用程序（如 ScreenTime）的所有豁免列表的交集中时，才输入您想要豁免基于年龄的评级限制的应用程序列表。 默认：选定
	iOS 所有监管版本	
	允许 Apple Books	选择以允许访问 Apple Books 应用。
	允许 iBooks Store 出现限制级色情内容（iOS 和 tvOS 11.3 及更高版本）	选择以允许用户下载标记为色情作品的 iBook Store 材料。
	允许账户修改	选择以允许使用受监控 iOS 7 设备的用户添加电子邮件帐号并更改已配置的电子邮件帐号。
	允许应用移动电话数据修改	选择以允许用户更改应用的蜂窝数据设置。
	允许“查找我的朋友”修改	选择以允许用户更改“查找我的朋友”应用设置。
	允许与非配置器主机配对	选择以允许主机配对，以便同步 iTunes。 事实上，启用此项可允许受监控的设备与 Mac（而非监控主机）上的 iTunes 同步。 禁用此项可禁用除监控主机外的所有主机配对。 如果未配置监控主机证书，所有配对都将禁用。
	允许 AirDrop	选择以允许在设备上使用 AirDrop。 AirDrop 是 Apple 的临时 Wi-Fi 系统，支持与附近用户的文件共享。 通过限制此功能，可确保敏感文档不会泄露给未授权或不安全的设备。
	允许 Touch ID/Face ID 解锁设备	选择以允许 Touch ID 或 Face ID 解锁设备。
	允许聚焦搜索返回 Internet 搜索结果	选择以允许 Spotlight 搜索返回 Internet 搜索结果。
	允许应用采用单个应用模式	输入可在 iOS 受监控设备上自主进入单应用模式的应用捆绑 ID 列表，以逗号分隔。 例如，您可以为学生指定自定义考试应用。 学生启动该应用程序后，应用程序进入单应用程序模式，以确保

类别	设置	采取何种措施
		学生在考试时无法使用其他资源。 该功能适用于为自主单应用模式开发的应用。 使用 Apple Configurator 建立监控。
	iOS 8+	
	允许备份企业书籍	选择以允许个人备份使用 MDM 推送到设备上的 iBooks、ePub 和 PDF 文档。
	允许同步企业书籍的注解和突出显示	选择以允许将添加到企业书籍中的注解和突出显示同步到 iTunes 中。
	强制执行 Apple Watch 手腕感应	选择后将隐藏屏幕上的通知，除非有人戴着 Apple Watch。
	iOS 8+ 监测	
	允许预测键盘	选择后用户就可以启用 iOS 单词输入预测，用户输入三个预测中的一个补全单词。
	允许键盘自动更正	选择后允许使用 Bluetooth 键盘的自动纠正。
	允许键盘拼写检查	选择后允许使用 Bluetooth 键盘的拼写检查。
	允许键盘定义查找	选择后允许使用 Bluetooth 键盘进行定义查询。
	允许修改 Touch ID 指纹/Face ID 面孔	选择以允许更改 Touch ID 或 Face ID 设置。
	iOS 9+ 监测	
	允许 iPad 上的键盘快捷键	选择以允许在 iPad 上使用键盘快捷键。
	允许修改壁纸	选择允许用户更改壁纸图片
	允许与 Apple Watch 配对	选择允许 iPhone 与 Apple Watch 配对。
	允许修改设备名称	选择以便允许用户更改设备名称。
	允许修改企业应用程序信任设置	选择以允许用户更改企业版应用的信任设置。
	iOS 9.3+ 监测	
	允许修改通知设置	选择以允许用户更改通知设置。
	iOS 9.3.2+ 监测	
	允许诊断提交修改	选择以允许用户更改与向 Apple 提交诊断数据相关的设置。
	iOS 10+ 监测	
	允许 Bluetooth 修改	选择以便允许用户修改被监控设备上的 Bluetooth 设置。 该功能在用于教育专用教室应用程序的共享 iPad 上有用，在此类情况下，必须使用 Bluetooth 运行应用程序。

类别	设置	采取何种措施
	iOS 10.3+ 监测	
	允许口授	选择以便允许用户与 iPhone 或 iPad 通话，而不是打字。
	iOS 11+ 监测	
	允许 AirPrint	选择以便允许 AirPrint 功能进行无线打印。
	允许 AirPrint 凭据存储	选择以便允许钥匙串存储 AirPrint 的用户名和密码。
	允许 AirPrint iBeacon 发现	选择以便允许用户设置 iBeacon 发现 AirPrint 打印机。
	允许添加 VPN 配置	选择以便允许用户创建 VPN 配置。
	强制 AirPrint 可信 TLS 要求	选择以便允许 TLS 打印通信的可信证书。 默认：取消选择
	允许删除系统应用程序	选择以便允许删除系统应用。
	允许修改蜂窝计划设置	选择以便允许用户修改蜂窝计划设置。
	允许设置新的附近设备	选择以便允许用户设置新的附近设备。
	在不提示的情况下自动加入课堂课程	选择以便允许用户在没有任何提示的情况下自动加入课堂课程。 默认：取消选择
	允许课堂在不提示的情况下锁定应用程序，并锁定设备	选择以便允许课堂在不提示用户的情况下锁定应用程序和设备。 默认：取消选择
	强制用户进行身份验证，然后才能在 Safari 和应用程序中自动填充密码或信用卡信息	设备所有者必须进行身份验证，然后才能在 Safari 浏览器和应用程序中自动填充密码或信用卡信息。 默认：假
	iOS 11.3+	
	允许与 Remote 应用配对（tvOS 11.3 和更高版本）	选择以允许通过 Remote 应用配对设备。
	允许传入 AirPlay 请求（tvOS 11.3 和更高版本）	选择以允许传入 AirPlay 请求。
	iOS 11.3+ 监测	
	允许 USB 限制模式	选择以允许用户访问 USB 限制模式。
	将软件更新推迟 30 天（仅适用于 iOS 11.3、tvOS 12.2 和更高版本的受监管设备）	选择以输入要推迟软件更新的天数。 默认值是 30 天，最大值是 90 天。 默认：取消选择

类别	设置	采取何种措施
	要求具有教师权限才可以离开课堂非托管班 iOS 12+ 监测	选择以便允许用户获得必要的教师权限来离开课堂未托管班。
	强制执行自动日期和时间（iOS 12.0 和 tvOS 12.2 及更高版本）	选择开启日期和时间“自动设置”功能。 用户无法关闭。 默认：假
	允许修改 eSIM 设置（iPhone XS、iPhone XS Max 和 iPhone XR - iOS 12.1 及更高版本） **iOS 12.2+ 受监管**	选择以允许用户修改支持设备上的 eSim 配置。 此选项也阻止用户在设备的“设置”中添加或移除蜂窝计划。 默认：真
	允许修改个人热点设置	选择以允许用户修改个人热点设置。 默认：真
	iOS 13.0+	
	允许文件网络驱动器访问 允许文件 USB 驱动器访问 **iOS 13.0+ 受监管** 允许连续路径键盘	选择以允许用户在文件应用中连接到网络驱动器。 默认：真 选择以允许用户在文件应用中连接到任何连接的 USB 驱动器。 默认：真 选择以启用连续路径键盘（滑动或跟踪键入）。 默认：真
	允许设备休眠	选择以启用设备休眠。 默认：真
	允许查找设备 允许查找我的朋友 强制 WiFi 开启 **iOS 13.4+**	选择以在 Find My 应用中启用查找我的设备。 默认：真 选择以在 Find My 应用中启用查找我的朋友。 默认：真 选择以使 WiFi 功率处于开启状态。 默认：假
	允许共享 iPad 的来宾会话	如果为假，临时会话在共享 iPad 上不可用。 默认：真

类别	设置	采取何种措施
	iOS 14.0+	
	允许 Apple 个性化广告	如果为假，限制 Apple 个性化广告。 这将阻止 Apple 使用用户信息进行定向广告。 这可能不会减少收到的广告数量，但广告与用户的相关性将会降低。 默认：真
	iOS 14.0+ 受监管	
	允许应用剪辑	如果为假，阻止用户添加任何应用剪辑，并移除设备中的任何现有应用剪辑。 默认：真
	iOS 14.2+ 受监管	
	允许 NFC	如果为假，禁用 NFC。 需要受监管设备。 在 iOS 14.2 和更高版本中可用。 默认：真
	iOS 14.5+	
	允许自动解锁	管理员可以使用现有 allowAutoUnlock 限制，管理此功能。 若为假，不允许自动解锁。 适用于 macOS 10.12 和更高版本，以及 iOS 14.5 和更高版本。 默认：真
	对设备强制实施仅听写	若为真，出于听写的目的，禁用与 Siri 服务器连接。 默认：假
	iOS 14.5+ 受监管	
	允许不成对的外部启动实施恢复	若为真，支持未配对的设备引导设备进入恢复状态。 默认：假
	强制 WiFi 使用仅允许的网络	若为真，将设备限制为仅通过配置文件加入 WiFi 网络设置。 默认：假 如果启用**强制 WiFi 加入仅允许的网络**限制，并且 WiFi 配置未分发到设备，WiFi 连接将丢失。
	iOS 15+	
	对仅设备强制实施转换	若为真，设备将不会出于翻译目的连接到 Siri 服务器。 默认：假
	需要托管粘贴板	若为真，复制并粘贴功能需要遵守 allowOpenFromManagedToUnmanaged 和 allowOpenFromUnmanagedToManaged 限制。 默认：假
	iOS 15.2+	
	允许邮件隐私保护	若为 False，将在设备上禁用邮件隐私保护。 适用于 iOS 15.2 和更高版本。 在 Ivanti Neurons for MDM 管理门户中安装并启用“允许邮件隐私保护”配置后，将在设备上启用“保护邮件活动”切换开关，并且提供以下选项： • **隐藏 IP 地址** - 电子邮件发送者无法将电子邮件链接到您的在线活动或确定您的位置

类别	设置	采取何种措施
		• **阻止所有远程内容** - 阻止电子邮件发件人查看您的电子邮件活动 默认值：True
	iOS 15.4+	
	允许 Apple TV 的自动屏幕保护程序(tvOS 15.4 和更高版本)	若为 False，将禁用 Apple TV 的自动屏幕保护程序。 适用于 tvOS 15.4 及更高版本。 默认值：True
	iOS 16.0 至 26.0	
	允许背景安全改进安装	禁用响应。 用户无法安装背景安全改进。
	允许删除背景安全改进	阻止用户撤消响应。 用户无法删除背景安全改进。
	受监督的 iOS 17.0+ 设备	
	允许在 Mac 设备上使用 iPhone 小组件	选择此选项可允许在 Mac 设备上使用 iPhone 小组件，其中两种设备上的 iCloud 使用相同的 iPhone AppleID。
	受监督的 iOS 17.2+ 设备	
	允许实时语音邮件	选择在设备上启用实时语音邮件。
	擦除时强制保留 eSIM	选择在系统因密码尝试失败次数过多或**设置** > **常规** > **重置**中的“清除所有内容和设置”选项而需要擦除设备时保留 eSIM。 如果是**查找我的**发起设备擦除操作，则系统不会保留 eSIM。
	受监督的 iOS 17.4+ 设备	
	允许 Marketplace 应用程序安装	选择此选项可允许用户从其他市场下载应用程序。 此限制设置为 false 时，系统将阻止用户安装新的替代市场应用程序和从这些市场安装的应用程序。
	允许自动调暗	选择此选项可允许在带有 OLED 显示屏的 iPad 上使用自动调暗选项。
	受监督的 iOS 17.5+ 设备	
	允许安装 Web 分发应用程序	**allowWebdistributionAppInstallation** 限制设为 false 时，将阻止用户直接从新的替代网站安装应用程序。 仅适用于受监督的设备。
	受监督的 iOS 18.0+ 设备	
	允许 eSIM 传出传输	选择此选项可允许将 eSIM 从已安装限制的设备传输到另一台设备。
	允许 Genmoji	选择此选项可允许创建 Genmoji。
	允许 Image Playground	选择此选项可允许使用图像生成功能。
	允许 Image Wand	选择此选项可允许使用 Image Wand。
	允许 iPhone 镜像	选择此选项可允许 iPhone 在 macOS 设备中执行镜像操作。

类别	设置	采取何种措施
	允许个性化手写结果	选择此选项可允许系统使用用户的手写输入生成文本。
	允许书写工具	选择此选项可启用 Apple Intelligence 书写工具。
	允许隐藏应用程序	选择此项可隐藏应用程序。
	允许锁定应用程序	选择此项可锁定应用程序。
	iOS 18.1+ 受监管设备	
	允许通话录音	选择此项可允许通话录音。 默认：真
	允许邮件摘要	选择此项可手动创建电子邮件摘要。 默认：真
	允许 RCS 消息传送	选择此项可允许 RCS 消息传送。 默认：真 在 iOS 26 设备和具有 iPadOS 26 的移动电话网络 iPad 型号上，RCS 消息的使用可能会在移动电话网络计划与 ICCID 关联的设备上受到限制。
	iOS 18.2+ 受监管设备	
	允许外部情报集成	选择此项可通过 Siri 使用外部云端情报服务。
	允许外部情报集成登录	选择此项可使外部情报提供者进入匿名模式。 如果用户已登录外部情报提供者，则应用此限制将导致其注销。
	允许修改默认浏览器	选择此项可启用默认浏览器首选项修改。 Ivanti Neurons for MDM 设置允许您设置默认 Web 浏览器。
应用程序	**iOS 所有版本**	启用对设备上应用的访问。
	允许安装应用	选择以允许用户从 Apple App Store 安装应用程序。 取消选中可禁用 App Store 并将其图标从主屏幕中移除。
	允许使用照相机	选择以允许用户操作照相机。 取消选择可禁用相机，并将其图标从主屏幕中移除。 在 iOS 26+ 设备中，如果将应用程序添加到例外列表中，则不会应用“允许相机”限制。
	允许使用 Safari	选择以允许使用 Safari Web 浏览器。 取消选择可禁用 Safari Web 浏览器，并将其图标从主屏幕中移除并防止用户打开 Web 剪辑。
	启用自动填充	选择以打开 Safari 中所显示字段的自动填充功能。
	强制欺诈警告	选择以提示 Safari 尝试阻止用户访问标识为欺诈或不安全的网站。
	启用 JavaScript	选择以打开支持 Safari 的 JavaScript。

类别	设置	采取何种措施
Safari	阻止弹出窗口	选择以阻止 Safari 的弹出窗口。
	仅监测 - 版本 26+	
	允许清除 Safari 历史记录	选择此项可允许用户清除浏览历史记录。
	允许 Safari 私人浏览	选择此项可允许使用私人浏览。
	iOS 所有监管版本	
	允许移除应用	选择以允许用户移除设备上的应用。
	允许使用 Game Center	选择以允许访问游戏中心。
	允许添加游戏中心好友	选择以允许用户添加游戏中心好友。
	允许多人游戏	选择以允许用户与其他用户共同玩游戏。
	允许 iMessage	选择以允许使用 iMessage。 在 iOS 26 设备和具有 iPadOS 26 的移动电话网络 iPad 型号上，如果设备被添加到拒绝列表中，iMessage 的使用可能会受到限制。
	接受 cookies	选择“从不”、“始终”或“来自被访问的网站”。
	允许 FaceTime	选择以允许用户在启用照相机时运行 FaceTime。 在 iOS 26 设备和具有 iPadOS 26 的移动电话网络 iPad 型号上，如果设备被添加到拒绝列表中，Face Time 的使用可能会受到限制。
	iOS 8+	
	允许托管的应用程序使用云同步	选择以允许托管的应用使用云同步。
	允许活动延续	选择以允许活动在支持切换的应用上延续。
	iOS 8+ 监测	
	允许使用播客	选择以允许使用播客。
	iOS 9+	
	允许信赖新企业应用创建者	选择允许用户访问新企业应用。
	iOS 9+ 监测	
	允许 App Store	选择允许用户访问 Apple App store。
	允许自动下载应用	选择允许应用下载文件、数据，并根据用户提示内容进行更新。
	允许新闻应用	选择允许使用新闻应用。

类别	设置	采取何种措施
	iOS 9.3+ 监测	
	允许 iTunes Radio	选择以允许使用 iTunes 广播。
	允许 Apple 音乐	选择以允许使用 Apple Music。
	允许列出的应用程序包 ID	选择仅允许显示或启动数组列出的捆绑 ID。 包含值 com.apple.webapp，允许所有网络剪辑。
	阻止的应用程序包 ID	选择以防止显示或启动数组列出的捆绑 ID。 包含值 com.apple.webapp，限制所有网络剪辑。
	iOS 13.0+ 受监管	
	允许使用 iTunes Store	选择以允许使用 iTunes Music Store。 取消选择可禁用 iTunes Music Store，并将其图标从主屏幕中移除。

类别	设置	采取何种措施
iCloud	iOS 所有版本	启用对 iCloud 服务的访问。
	允许备份	选择以允许设备通过 Apple 的 iCloud 服务备份数据。
	允许文档同步	选择以允许通过 Apple 的 iCloud 服务同步文档。
	允许照片流	选择以允许照片通过 Apple 的 iCloud 同步到您的其他 iOS 设备。
	已允许共享照片流（不允许会导致数据丢失）	选择以允许同步共享的照片。 取消选择此选项，会使照片丢失。
	允许 keychain 同步	选择以允许同步您的 keychain。
	iOS 9+	
	允许 iCloud 照片库	选择允许用户访问 iCloud 照片库。
	iOS 15+ 受监管	
	允许 Cloud 私人中继	若为假，禁用 iCloud 私人中继。 默认：真

类别	设置	采取何种措施
安全和隐私	**iOS 所有版本**	启用安全和隐私策略。
	允许无线证书更新	选择以允许无线更新根证书。
	强制限制和跟踪	选择以要求使用限制和跟踪功能。
	iOS 所有监管版本	
	允许配置配置文件安装	选择以允许用户交互式安装配置的配置文件和证书。
	允许助手用户生成的内容	选择以允许 Siri 在 Web 中查询用户生成的内容。
	iOS 8+ 监测	
	允许用户在重置界面中擦除所有内容和设置	选择以启用设备上的 iOS 重置用户界面中的“擦除所有内容和设置”选项。
	允许屏幕时间	选择以允许屏幕使用时间（设置 > 屏幕使用时间）。
	允许将诊断数据发送给 Apple	选择以允许将诊断数据自动提交给 Apple。
	允许用户接受不受信任的 TLS 证书	选择以允许设备用户接受不受信任的 HTTPS 证书。 选择以允许设备用户接受不受信任的 HTTPS 证书。如果此项未选中，设备将在不提示设备用户的情况下自动拒绝不受信任的 HTTPS 证书。
	强制加密备份	选择以要求通过 iTunes 加密备份。 应 SCEP 要求自动选中该项。
	强制用户为所有事务输入 iTunes Store 密码	选择以强制设备用户输入各个 App Store 事务的 iTunes 密码。 如果此项未选中，设备用户可通过一次验证执行多项事务。
	iOS 9+	
	将 AirDrop 作为未托管目标	选择以允许用户访问 AirDrop 文件共享。 默认：假
	iOS 9+ 监测	
	允许修改设备通行码	选择允许用户更改设备的通行码。
	iOS 12+	
	允许受管的应用程序将联系人写入未受管的联系人帐户	选择以允许受管的应用程序将联系人写入未受管的联系人帐户。 默认：假
	iOS 12+ 监测	
	允许自动填充密码	选择以允许用户在 iOS 上使用自动填充密码功能，并在 Safari 或应用中提示使用保存的密码。
	允许附近设备共享密码请求	选择以允许用户的设备从附近设备请求密码。

类别	设置	采取何种措施
	允许密码共享	选择以允许用户使用 Airdrop 密码功能共享密码。
	允许未受管的应用程序从受管的联系人帐户读取联系人 iOS 18.3	选择以允许未受管的应用从受管的联系人帐户读取。 默认：假
	允许外部情报工作区 ID	输入允许的外部情报工作区 ID。
	允许笔记转录摘要	选择以启用从转录创建摘要。 默认：真
	允许视觉情报摘要	选择以启用使用图像或视觉内容从 Apple 视觉智能功能创建摘要。 默认：真

类别	设置	采取何种措施
内容评级		控制对应用和媒体的访问。
	允许播放限制级音乐、播客和 iTunes U 媒体（仅限受监管 iOS 13+ 和 tvOS 11.3 及更高版本）	显式内容在 iTunes Store 上出售时被唱片公司等内容提供商标记为显式内容。
	评级区域	从下拉列表中选择区域，可更改与应用、电视节目和电影的评级选项相关联的区域。
	电影	为设备上存储的电影选择评级限制： • 不允许电影 • G • PG • PG-13 • R • NC-17 • 允许所有电影
	电视节目	为设备上存储的电视节目选择评级限制： • 不允许电视节目 • TV-Y • TV-Y7 • TV-G • TV-PG • TV-14 • TV-MA • 允许所有电视节目
	应用	为设备上的应用选择评级限制： • 不允许应用 • 4+ • 9+ • 12+ • 17+ • 允许所有应用

有关更多信息，请查看[如何创建配置]

10.10.4.27. 会议室显示

适用于：tvOS 10.2 或支持的更新版本。

此配置将在 Apple TV 上打开会议室显示模式。 会议室显示模式会将 Apple TV 锁定为该模式，以阻止其他使用方式。

从 tvOS 10.2 开始，您可以将受监管的 Apple TV 设备设置为会议室模式。 会议室显示会将范围内的 Apple TV 设备锁定为黑色壁纸屏幕，并下载默认屏幕保护程序，除非在 Apple TV 设备设置中手动定义背景图像和屏幕保护程序。 此模式也可以显示在会议室显示配置中配置的消息。

在设备处于此模式时，会议室显示配置可以自动部署，并可以安装应用。 对于设置为会议室显示模式并需要重新启动的设备，将自动恢复锁定屏幕，并且不会先显示主屏幕。

> 如果 Apple TV 设备在单应用模式中运行，或者如果使用会议室显示部署单应用模式，会议室显示将覆盖单应用模式。 此外，如果 Apple TV 设备通过以太网连接到网络，会议室显示将不会自动显示 Wi-Fi 网络，以加入进行 AirPlay 共享。 通过会议室显示配置的自定义消息字段，此说明可以显示在屏幕上。

创建会议室显示配置

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中，键入**会议**，然后单击**会议室显示**配置。
4. 输入名称并描述配置。
5. 指定**自定义消息**。 在会议室显示模式中，这是在屏幕上显示的自定义消息。
6. 单击**下一步**，配置分配设置。
7. 单击**完成**。

有关更多信息，请查看如何创建配置。

10.10.4.28. 键盘设置

使用**键盘设置**配置受监控设备上的键盘设置。 此声明可帮助管理员应用基于策略的一致控件，以管理键盘行为、输入选项和相关用户体验设置。

适用于：

- iOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- macOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**键盘设置**配置。
3. 根据下表配置各项**键盘设置**：

设置	采取何种措施
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
允许自动更正	选中复选框以启用自动更正。 切换**推送至设备**按钮，以在受监控设备上启用自动更正。 此设置不适用于 macOS 设备。
允许定义查找	选中复选框以启用定义查找。 切换**推送至设备**按钮，以在受监控设备上启用定义查找。
允许听写	选中复选框以启用听写。 切换**推送至设备**按钮，以在受监控设备上启用听写。
允许数学键盘建议	选中复选框以启用数学键盘建议。 切换**推送至设备**按钮，以在受监控设备上启用数学键盘建议。
允许预测文本	选中复选框以启用预测文本。 切换**推送至设备**按钮，以在受监控设备上启用预测文本。 此设置不适用于 macOS 设备。
允许滑动输入	选中复选框以启用滑动输入。 切换**推送至设备**按钮，以在受监控设备上启用滑动输入。 此设置不适用于 macOS 设备。
允许拼写检查	选中复选框以启用拼写检查。 切换**推送至设备**按钮，启用受监控设备上的拼写检查。 此设置不适用于 macOS 设备。
允许文本替换	选中复选框以启用文本替换。 切换**推送至设备**按钮，以在受监控设备上启用文本替换。 此设置不适用于 macOS 设备。

4. 单击**下一步**，配置分配设置。
5. 选择其中一个分发选项来设置**键盘设置**配置。 有关配置分发选项的详细信息，请参阅**使用配置**。
6. 单击**完成**。

10.10.4.29. 锁定和自助服务终端：Android 设备管理模式

锁定和 Kiosk：一项 Android 设备管理模式配置，可禁用 Android 设备的某些功能，并创建用户在 Kiosk 模式下可以使用的应用程序允许列表。

> Android 设备管理模式配置已停用，在运行 Android 8 及以上版本的设备上不受支持。 对于 Android 8 及以上版本，建议使用 Android Enterprise 锁定来进行 Kiosk 锁定。

您可以限制在 Android 设备处于 Kiosk 模式时修改设置或应用程序的选项。

- 在“创建锁定与自助服务终端：Android 设备管理员模式配置”页面中，添加应用并选择设置。
- 使用设置图标更改设置选项将在自助服务终端模式中可用。
- 选择应用程序，而不选择任何设置配置选项，设置图标将不在 Kiosk 模式下显示。
- 如果您选择在配置中不包括任何应用程序，那么将显示该设置图标。

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
锁定设置： 禁用所有 Android 设备的功能。	
禁用 Wi-Fi	选择以关闭对无线局域网 (WLAN) 的访问。
禁用照相机	选择以关闭对照相机的访问。
禁用蓝牙	选择以关闭蓝牙功能。 谨慎使用该选项。 Ivanti 建议不要禁用音频，因为该操作会禁用对免提 Bluetooth 的访问权限。 在开车出行越加普及的同时，设备的免提使用也有了相应的法律要求。
自助服务终端模式设置：支持设备用作自助服务终端，操作限于一些特定应用。 自助服务终端模式设置将不应用于安装 Android 8.0 和更高版本的设备。 对于此类设备，设备详细信息页面中的自助服务终端状态会将 UNSUPORTED_ON_DEVICE 报告为自助服务终端状态。	
启用自助服务终端模式	选择以便在 Android 设备上配置自助服务终端模式。
禁用快速设置	选择以在自助服务终端模式中禁用快速设置。
允许用户访问 Wi-Fi 设置	选择 以允许用户更改 Wi-Fi 设置并访问首选 无线网络。
允许用户访问蓝牙设置	选择 以允许用户更改蓝牙设置并配对其他 蓝牙设备。
允许用户访问位置设置	选择以允许用户访问位置设置。
允许用户延迟应用程序的更新	选择 以允许用户延迟应用程序更新。
退出自助服务终端 PIN	输入该四位代码，最终用户才能退出自助服务终端模式。
创建应用的允许列表：通过将应用添加到允许的应用列表，这些应用将在自助服务终端模式中对用户提供。 拖放应用程序，使其按照在自助服务终端模式启动栏中显示的顺序排列。 将应用添加到允许的应用列表不会在设备上安装该应用。 确保将每个应用程序分配给应用目录中正确的用户和用户组。	
内置应用	单击“+添加”可将列出的本机应用包括到自助服务终端模式中允许的应用组中。 如果您在上述锁定设置中禁用拨号器或相机，则无法将其添加至允许的应用列表。
应用目录	单击“+添加”可将应用目录中列出的应用纳入自助服务终端模式中允许的应用组中。

设置	流程
其他应用	单击 + 添加，以包含在 Google Play Store 上不可用的应用的软件包名称。
自助服务终端模式允许的应用程序	单击 X 从自助服务终端模式允许的应用组中移除应用。 拖放以更改应用的顺序，此应用是指出现在自助服务终端设备上的应用。

> 对于使用 Knox Standard 4.0 或更高版本的 Samsung 设备，多用户功能会在自助服务终端模式下自动锁定。

对于非 Samsung 设备，Android 8.0 或更高版本不支持自助服务终端模式。 Ivanti 建议在 Android 8.0 或更高版本上使用适用于自助服务终端模式的 Android Enterprise 锁定。

相关主题：

- 设置 Android 的自助服务终端模式
- 如何创建配置

10.10.4.30. 设置 Android 的自助服务终端模式

本部分包含以下主题：

- 远程启动自助服务终端模式
- 退出自助服务终端模式

许可证：Silver

利用 Android 设备的自助服务终端模式，您可以限制将设备用于特定应用。 您可以使用自助服务终端模式设置仅使用特定工作应用的员工设备。

在准备适用于自助服务终端模式的 Android 设备，或通过自助服务终端模式准备设备所有者时，您将需要创建要用户可在自助服务终端模式中使用的应用允许列表。 对于使用设备所有者的设备，通过在配置应用时拖放，以按照在自助服务终端模式启动器中显示的顺序对应用进行排列，您可以将应用添加到允许的应用列表。 请查看锁定和自助服务终端配置，以了解更多信息。

先决条件

在为 Android 设备配置自助服务终端模式前，请确保您已执行以下任务：

- 已在设备上安装 Go。
- 已配置应用目录，该应用目录内应包含自助服务终端配置需要的应用。
- 已将应用目录分配给将在自助服务终端模式下运行的设备。

> SonimXP5S 设备不支持自助服务终端模式。

- 已安装自助服务终端配置需要的应用。
- （可选）设置 Android 自助服务终端品牌化。

> Android 5.1 和 6.0 支持 Kiosk 模式。 非 Samsung Knox 必须处于设备所有者模式，才能防止不必要应用的使用。

重要提示：一些设备具有的功能会使设备在屏幕上绘制，或以其他方式退出自助服务终端模式。 Samsung Galaxy S6 Edge 的 People Edge 功能是此功能的示例。 我们建议，在设备部署前，请管理员关闭这些功能类型。

步骤

1. 转至**配置**。
2. 点击 **+ 添加**。
3. 单击**锁定和自助服务终端：Android 设备管理员模式**。
4. 在**创建设置**屏幕中，请至少完成**自助服务终端模式设置**部分。
5. 在**分配**屏幕，选择接受此配置的设备组。
6. 单击**完成**。
7. 若不是 Samsung 设备，请继续完成下列步骤：
    1. 转到**设备** > **设备**。
    2. 选择您要启用自助服务终端模式的设备。
    3. 选择**操作**、**强制签入**。
    4. 在设备上，点击**自助服务终端模式**按钮。

5. 按下设备上的**主页**按钮。
6. 如果出现**选择启动程序**对话框，请单击 **Go 自助服务终端启动程序**，然后选择**始终**。 该步骤中，必须确保为此功能使用正确的启动程序。 否则，会提示用户选择一个启动程序。

远程启动自助服务终端模式

步骤

1. 转至**设备 > 设备**。
2. 将自助服务终端模式列添加到显示屏。
3. 选择启用但并未启动自助服务终端模式的设备。
4. 选择**操作 > 进入自助服务终端模式**。

退出自助服务终端模式

如果在配置中设置 PIN，您可以退出设备的自助服务终端模式。

步骤

1. 单击**设置**图标。
2. 选择**退出自助服务终端模式**。
3. 出现提示时，单击**自助服务终端 PIN** 字段。
4. 输入自助服务终端 PIN。

您可以从门户将特定设备退出自助服务终端模式。

步骤

1. 转至**设备 > 设备**。
2. 显示设备的详细信息。
3. 选择**操作 > 退出自助服务终端模式**。

您也可以使用以下方法退出自助服务终端模式：

- 删除配置
- 禁用配置
- 从配置中删除设备组

10.10.4.31. 设置 Android 共享设备自助服务终端

对于任务工作者部署，公司可以提供针对特定用户角色定制的专用 Android 设备。 根据用户的配置文件，可能会在设备上显示不同的应用和配置。 例如，处于技术角色的用户可能具有为其使用而呈现的特定应用程序集，而具有维护角色的另一用户可以访问不同的应用程序集。

Android 共享设备 Kiosk 模式为共享设备的不同用户组充当应用程序筛选器。 登录到共享设备自助服务终端的用户只能查看适合其角色的应用程序。 共享设备自助服务终端的一个主要优点是，您可以允许不同的用户组从同一设备访问不同的应用程序集。 当用户退出 Android 共享设备 Kiosk 模式时，他们的应用程序和用户数据（包括历史记录）将被清除，不会对下一个登录设备的用户显示（如果应用程序已标记为重新安装）。 共享设备自助服务终端仅适用于具有托管 Google Play 账户的 Android 企业部署。

共享设备自助服务终端需要两种类型的用户，即登台用户和共享自助服务终端用户，以及至少两个与这些用户对应的策略。 登台用户用于提示登录屏幕显示在共享设备上。 此外，登台用户是一种特殊类型的管理员用户，允许其他用户登录实际的自助服务终端设备。 共享设备自助服务终端用户成功登录后，登台策略将被共享自助服务终端策略替换。 自助服务终端户可以根据分配给它的策略访问设备上安装的应用程序。 虽然您可以创建多个共享自助服务终端策略，但一次只能在自助服务终端设备上激活一个自助服务终端策略。 当自助服务终端用户注销共享自助服务终端时，设备将恢复到登台用户，从而恢复到登台策略。

登台用户只能访问登录页面。 因此，您需要创建专用于此用户的登台策略。 相反，共享设备自助服务终端用户可以访问您在其策略中定义的一组应用程序。 （当然，您还需要在共享设备 kiosk 设备上安装允许的应用。）共享设备 kiosk 策略允许您从以前安装的所有应用中创建允许应用筛选器。 您无法直接将应用程序上传到 Android 共享自助服务终端策略中。 通常，您希望将共享自助服务终端策略专用于某种类型的共享自助服务终端用户或用户组，具体取决于您的组织。 例如，公司可能有白班和夜班员工，他们具有不同的角色并需要访问单独的应用程序集。 在这种情况下，您需要创建白班策略和夜班策略。

有关启用共享设备自助服务终端的更多信息，请查看**锁定和自助服务终端：Android Enterprise**

10.10.4.32. 锁定和自助服务终端：Android Enterprise

锁定和 Kiosk：一项 Android Enterprise 配置，可禁用 Android Enterprise 设备的某些功能，并创建用户在 Kiosk 模式下可以使用的应用程序允许列表。

本部分包含以下主题：

- 锁定设置
- 工作配置文件
- 工作托管设备（设备所有者和自助服务终端模式设置）
- 具有工作配置文件/公司拥有设备上的工作配置文件的受管设备锁定设置

锁定设置

设置	说明
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
选择锁定类型	选择您要配置的锁定设置类型： • 工作配置文件 • 工作托管设备（设备所有者和自助服务终端模式设置） • 具有工作配置文件/公司拥有设备上的工作配置文件的受管设备锁定设置 公司拥有设备上的工作配置文件锁定设置仅适用于 Android 11+ 设备。 每个配置仅允许一个类型。 此选项的显示取决于您选择的类型。 如果工作托管设备（设备所有者）和带有公司拥有设备上的工作配置文件的托管设备配置分发到相同设备，带有工作配置文件的托管设备优先。

工作配置文件

仅禁用 Android Enterprise 设备的特定功能。

设置	采取何种措施	适用设备
禁用屏幕捕获	选择后不能使用设备内置屏幕截图功能。	• Android 5.0 +
不允许应用控制	选择阻止用户修改设置或启动器中的应用程序。	• Android 5.0 +
不允许配置凭据	选择阻止用户配置用户凭据。	• Android 5.0 +
不允许跨过配置文件复制粘贴	选择阻止在两个配置文件之间复制/粘贴信息。	• Android 5.0 +
不允许修改账号	选择阻止用户添加或移除账户。	• Android 5.0 +
不允许出射光束	选择以阻止用户使用 NFC 传输应用数据。	• Android 5.1+
不允许共享位置	选择阻止用户将设备位置传输至应用。	• Android 5.0 +
禁止调试功能	选择以便禁用设备上的调试功能。 该选项默认打开。	• Android 5.0 +
确保验证应用程序	选择以便允许使用设备上的应用程序验证功能。 该选项默认打开。 该选项关闭后，该设备将返回到默认行为，这可能因设备而异。	• Android 5.0 +
禁用设备上的未知来源	选择以防止设备安装来自未知来源的应用程序。 此设置在设备上生效取决于预期的 Google Play 更新，以启用此功能。	• Android 5.0 +
限制输入方法	选择以通过**软件包名称**字段指定已加入允许列表软件包名称的列表，限制已加入允许列表的 IME 软件包名称。 设备将可以同时使用已加入允许列表的软件包输入法和默认系统输入法。 用户可以在默认系统输入法和已加入允许列表的软件包输入法之间切换。 对于 Android 10+，允许列表仅适用于工作配置文件端上的 IME 应用。 对于 Android 早期版本，允许列表适用于 IME 应用设备范围（工作配置文件内部和外部）。	• Android 5.0 +
限制可访问性服务	选择以通过**软件包名称**字段指定已加入允许列表软件包名称的列表，限制工作应用的无障碍服务。 如果没有已加入允许列表的软件包，仅允许系统无障碍服务。	• Android 5.0 +
在工作配置文件中禁用未知来源	选择以禁止在工作配置文件中从未知来源下载。	• Android 5.0 +
启用/禁用系统应用程序	选择以启用和禁用通过**系统应用软件包名称**字段指定两个软件包名称列表部署系统应用。 使用此功能管理对 Google Play 中未发布的系统应用程序的访问。 不支持将应用添加到 App Catalog 和系统应用列表。	• Android 5.0 +
禁用来电显示	设置是否在来电设备中显示工作配置文件中的来电者 ID 信息。	• Android 6.0+

设置	采取何种措施	适用设备
禁用“通过蓝牙共享联系人”	选择以便防止设备通过 Bluetooth 与其他设备共享联系人。	• Android 6.0+
禁用“通过搜索共享联系人”	选择以便防止用户从个人电话拨号程序中搜索工作联系人。	• Android 7.0 +
不允许自动填充	选择以禁止自动填充	• Android 8.0+
在个人配置文件中，不允许工作应用通知	选择以限制工作配置文件通知。	• Android 8.0+
不允许打印	选择以限制从所有应用打印。	• Android 9.0+
不允许共享到配置文件	选择以阻止用户将个人数据共享到设备中的工作配置文件。	• Android 9.0+
允许访问工作配置文件日历	选择以下任一选项，以允许所有应用或在个人端选择一组应用，从而访问在工作配置文件中显示的日历信息： • **个人配置文件中的所有应用** - 允许所有应用访问工作配置文件中的日历信息 • **仅限个人配置文件中的以下应用** - 在以下文本字段中，输入应用的捆绑 ID，用逗号分隔。只有个人端的这些选定应用才能访问工作配置文件中的日历信息。个人端的应用应实施特定 API，以访问共享日历。	• Android 10.0+
启用应用的跨配置文件允许列表	通过选中复选框，用户可以将特定应用中的信息从工作配置文件共享到设备的个人端。 在**已加入允许列表的应用**字段中，键入要加入允许列表的应用的软件包 ID，并使用逗号隔开。 此选项默认禁用。	• Android 11.0+
启用 5G 网络切片	选择此项以在公司拥有设备的工作配置文件中提供 5G 网络切片选项。 此选项默认禁用。	• Android 12.0+
禁止共享管理员配置的 Wi-Fi	选择此选项可防止用户共享管理员设置的 Wi-Fi 配置。	• Android 13.0+
禁用 AI 辅助	选择此选项可禁止用户使用 AI 辅助功能。 此选项默认禁用。	• Android 15.0+

工作托管设备（设备所有者和自助服务终端模式设置）

为 Android 5.0+ 禁用工作托管设备（设备所有者）上的某些功能。

设置	说明
禁用 Wi-Fi	选择以关闭对无线局域网 (WLAN) 的访问。
禁用 Wi-Fi 设置	选择以关闭对无线设置的访问。
禁用照相机	选择以关闭对照相机的访问。
禁用蓝牙 (Android 8.0+)	选择以关闭蓝牙功能。 谨慎使用该选项。 Ivanti 建议不要禁用音频，因为该操作会禁用对免提 Bluetooth 的访问权限。 在开车出行越加普及的同时，设备的免提使用也有了相应的法律要求。
不允许蓝牙设置 (Android 8.0+)	选择以关闭对 Bluetooth 设置的访问。
禁用屏幕捕获	选择后不能使用设备内置屏幕截图功能。
禁用网络重置	选择此项可防止重置网络。 （适用于 Android 7.0+ 设备，“公司自有设备上的工作配置文件”模式不支持）。
静音主控音量	选择以将主音量静音。
不允许应用控制	选择阻止用户修改设置或启动器中的应用程序。
不允许使用凭据	选择阻止用户配置用户凭据。
不允许紧急广播	选择以防止紧急广播。
不允许移动网络	选择以关闭对移动网络的访问。 如果禁用 Wi-Fi，则此选项将无法禁用。
不允许数据共享	选择即可关闭将网络共享选项，也就是使用一台设备互联网连接为另一台设备提供互联网连接。
不允许 VPN	选择以关闭对 VPN 连接的访问。
不允许出厂设置	选择以阻止用户将设备恢复为出厂设置。
启用出厂重置保护	选择以允许用户将设备恢复为出厂设置。 您可以选择指定授权 Google 帐户 ID 的列（整数值），该列表可以在恢复出厂重置后配置设备，或者将鼠标悬停在帮助图标上以查看检索授权帐户 ID 的帮助。
不允许修改账号	选择阻止用户添加或移除账户。
不允许 NFC（射出光束）	选择以阻止用户使用 NFC 传输应用数据。
不允许拨出电话	选择以阻止用户呼出电话。
不允许安全启动 (Android 6.0+)	选择以阻止用户将设备重新启动为安全启动模式。
不允许共享位置	选择阻止用户将设备位置传输至应用。
禁止调试功能	选择以便禁用设备上的调试功能。 该选项默认打开。

设置	说明
确保验证应用程序	选择以便允许使用设备上的应用程序验证功能。 该选项默认打开。 该选项关闭后，该设备将返回到默认行为，这可能因设备而异。
不允许短信	选择以阻止用户发送和接收短信。
不允许取消静音麦克风	选择 以阻止用户取消设备的麦克风静音。
不允许自动时间	选择 以阻止用户启用自动时间变化。
不允许自动时区	选择以阻止用户随时区变化启用自动设备时间调整。
与服务器同步时间 (Android 9.0+)	选择以允许设备在首次注册时与 Ivanti Neurons for MDM 服务器同步时间，此后在每次签入后每 24 小时同步一次。 此选项仅在选择**禁用自动时间**时可用。
设置时区 (Android 9.0+)	指定奥尔森时区 ID 格式中的时区字符串（例如，太平洋/中途岛）。
禁用数据漫游	选择以在设备处于漫游状态时关闭数据交换。
禁用 Wi-Fi 休眠模式	选择 以确保在设备处于休眠模式时，WiFi 处于开启状态。
限制输入方法	选择以通过**软件包名称**字段指定已加入允许列表软件包名称的列表，限制已加入允许列表的 IME 软件包名称。 设备将可以同时使用已加入允许列表的软件包输入法和默认系统输入法。 用户可以在默认系统输入法和已加入允许列表的软件包输入法之间切换。 对于 Android 10+，允许列表仅适用于设备端上的 IME 应用。 对于 Android 早期版本，允许列表适用于设备范围中的 IME 应用。
限制可访问性服务	选择以通过**软件包名称**字段指定已加入允许列表软件包名称的列表，限制工作应用的无障碍服务。 如果没有已加入允许列表的软件包，仅允许系统无障碍服务。
禁用 USB 文件传输	选择以禁用 USB 文件传输。
禁用外部媒介	选择以禁用外部媒介。
禁用密钥保护（如果设置了 PIN/通行码，则无效）	选择以禁用键盘保护。 如果当前设置了密码、PIN 或图案，则此选项无效。 如果在键盘保护禁用后设置密码、PIN 或图案，键盘保护将停止禁用。
接通电源时保持屏幕打开。	选择此选项可在接通电源时保持屏幕打开。 当设备连接到电源时，屏幕可能会变暗，但不会关闭。 仅当通行码配置中的自动锁定或不活动超时未用于设置超时时，此设置才会生效。
不允许创建窗口	选择此选项可防止应用程序显示某些类型的覆盖窗口，例如提醒和祝酒。
跳过首次使用提示	选择此项可使系统针对应用程序进行的推荐在首次启动时跳过用户教程和其他介绍性提示。
设备不允许未知来源	选择以禁止用户安装来自未知来源的应用。
设置锁屏界面消息 (Android 7.0+)	选择以设置在设备上显示的锁定屏幕消息。 在文本字段中，键入锁定屏幕消息（最多 256 个字符）。 通过启用此选项，阻止用户在“设置”中设置消息，并向用户显示管理员设置的消息。

设置	说明
	如果管理员未在启用“设置锁定屏幕消息”之后提供任何锁定屏幕消息，将阻止用户在“设置”中设置消息，但不会向用户显示任何消息。
设置屏幕亮度	选择此项以设置设备屏幕的亮度。 • 手动 - 选择此项以手动输入数字（0 至 255） • 自适应 - 选择此项以允许设备自行设置亮度 建议启用“禁止配置亮度”选项后再设置设备的屏幕亮度。
设置屏幕超时	选择此项以设置屏幕超时持续时间（以秒为单位）。 建议启用“禁止配置屏幕超时”选项后再设置设备的屏幕亮度。
设置屏幕方向	选择此项以设置屏幕方向。 可以使用下拉列表将屏幕方向设置为 0、90、180 或 270 度。 默认未选中此选项。 对于 Go 应用程序 89 及以上版本，必须选择此选项，并将值设置为 0，使设备处于 Kiosk 纵向模式。
启用/禁用系统应用程序	选择以启用和禁用通过**系统应用软件包名称**字段指定两个软件包名称列表部署系统应用。 使用此功能管理对 Google Play 中未发布的系统应用程序的访问。 不支持将应用程序添加到应用程序目录和系统应用程序列表。
Android 8.0+	
不允许自动填充	选择以不允许用户使用自动填充服务。
不允许 Bluetooth 共享	选择以不允许用户在设备上共享传出 Bluetooth。
禁用备份服务	选择以禁用备份服务。
Android 9.0+	
不允许打印	选择以不允许用户打印。
不允许飞行模式	选择以在整个设备中禁用飞行模式。
不允许环境显示	选择以不允许用户的环境显示。
不允许配置亮度	选择以不允许用户配置亮度。 建议在定义“设置屏幕亮度模式”后再选择此选项。
不允许配置日期时间	选择以不允许日期、时间和时区配置。
不允许配置位置	选择以不允许用户禁用位置提供商。
不允许配置屏幕超时	选择以不允许用户更改屏幕关闭超时。 建议在定义“设置屏幕超时”值后再选择此选项。
Android 12.0+	
仅为充电启用 USB	选择以仅允许 USB 端口用于充电。
Android 13.0+	

设置	说明
设置最低 Wi-Fi 安全要求	使用此选项可设置最低 Wi-Fi 安全要求： • 无最低安全要求 - 如果无最低安全要求，请选择此选项 • 基于个人网络的安全 - 选择此选项可阻止个人 Wi-Fi 网络，如 WEP、WPA/WPA2/WPA3 等。 • 基于企业 EAP 网络的安全 - 选择此选项可阻止基于 EAP 协议的 Wi-Fi 网络 • 基于企业 192 网络的安全 - 选择此选项可阻止基于 EAP 企业的 Wi-Fi 网络 不符合最低标准的所有现有设备将断开连接。 设备详细信息将在**常规 > Wi-Fi 安全等级**下显示最低 Wi-Fi 安全等级要求（如有）。
禁止共享管理员配置的 Wi-Fi **Android 15.0+**	选择此选项可禁止用户共享管理员设置的 Wi-Fi 配置。
禁用 AI 辅助 **自助服务终端模式设置：**自助服务终端模式对设备应用附加限制，包括限制通过自定义启动栏访问应用程序。	选择此选项可禁止用户使用 AI 辅助功能。 此选项默认禁用。
启用自助服务终端模式	选择以在 Android 设备上配置自助服务终端模式。 • 在用户登录共享自助服务终端模式并注销时，用户名可以与 Go 客户端一起使用，以便将来登录。 在共享自助服务终端模式中，Go 客户端将保留最近使用的 7 个用户名。 • 现在，共享自助服务终端模式支持 IDP 身份验证。 因此，如果 Ivanti Neurons for MDM 使用 IDP 进行配置，则共享 Kiosk 模式可以与 IDP 身份验证一起使用。
启用锁定任务模式	选择此项可在 Android 设备上启用锁定任务模式。 在启用时，设备可以显示锁屏、状态栏和安全模式。 此选项默认禁用。 以下是在对 Android 9 或支持的较新版本启用锁定任务模式时显示的其他设置： **设置图标** - 允许应用访问依赖于设备设置应用的系统功能。 允许设备设置帮助避免在从应用配对 Bluetooth 等情景中违反锁定任务模式。 建议为特定应用启用此设置。 **系统信息** - 在状态栏上，显示日期/时间、连接、电池和振动模式。 此选项默认禁用。 **锁屏**（默认启用）- 在锁定任务模式期间，启用锁屏。 **全局操作**（默认启用）- 启用在用户长按电源按钮时显示的菜单。 如果禁用此选项，用户可能无法关闭设备。 **主页按钮** - 启用主页按钮。 此选项默认禁用。 在启用时，显示以下子选项： • **概览按钮**（默认禁用）- 在锁定任务模式中，启用概览按钮和概览屏幕 • **通知**（默认禁用）- 在锁定任务模式中启用通知。 这包含状态栏、提醒通知和可扩展通知栏上的通知图标。 如果未启用主页按钮选项，用户将无法使用多窗口功能。

设置	说明
自动进入自助服务终端（仅在初始设置时）	选择此项可在应用配置时自动允许自助服务终端模式。
政策更新后维护自助服务终端模式	选择此项可在应用锁定政策更新后自动将设备返回到自助服务终端模式。 此设置有助于保持不间断的 kiosk 操作，并减少策略更改后手动干预的需求。 以前，更新锁定策略可能导致设备退出 kiosk 模式。 启用后，设备会在处理更新的策略后自动重新进入 kiosk 模式。
禁用 Android 5 设备的快速设置	选择以为在 Android 5 上运行的设备禁用自助服务终端模式中的快速设置。
禁用 Android 6+ 和所有 Samsung 设备的快速设置	选择以为 Android Enterprise 设备版本 6 至最新发布版本和所有 Samsung 设备禁用自助服务终端模式中的快速设置。 禁用此设置不会屏蔽设备上的通知图标和声音。
允许用户访问 Wi-Fi 设置	选择 以允许用户更改 Wi-Fi 设置并访问首选 无线网络。
允许用户访问蓝牙设置	选择 以允许用户更改蓝牙设置并配对其他 蓝牙设备。
允许用户访问位置设置	选择以允许用户访问位置设置。
允许用户延迟应用程序的更新	选择 以允许用户延迟应用程序更新。
允许用户访问日期和时间设置	选择以允许用户访问日期和时间设置。
允许用户访问移动网络设置	选择以允许用户访问移动网络设置。
允许用户选择语言	选择此项可允许用户访问语言设置。
启用共享设备	在共享设备自助服务终端中，设备在多个最终用户之间共享。此选项可在设备处于自助服务终端模式时启用设备进行共享： • **启用登录**：此选项适用于自助服务终端管理员用户。 在使用此选项配置设备时，将显示用户登录屏幕，并允许最终用户登录共享设备自助服务终端。 当且仅当用户创建为 Android Enterprise 设备账户用户（登台用户）时，才会显示“启用登录”选项。 选择使用域替代，并视情况输入域。 此选项会检查域后缀的用户名。 如果缺少域后缀，系统会自动将域后缀附加到用户名。 • **启用注销**：在使用此选项配置设备时，登录的最终用户将可以访问已加入允许列表的应用。 此用户可以看到注销选项，但无法退出自助服务终端。 当用户注销共享设备自助服务终端时，另一位用户可以登录共享设备自助服务终端并查看管理员配置的应用程序。 • 应用程序显示为“回收”图标，该图标用于在每次登录时强制重新安装应用程序。 此选项可用于本地缓存数据的应用程序。 如果管理员提供退出自助服务终端 PIN，用户可以退出自助服务终端模式。 • **超时**：以小时为单位指定超时持续时间。 例如，当超时持续时间配置为 2 小时且最终用户无法注销共享设备自助服务终端时，将在 2 小时后自动在设备上执行注销操作。 **超时**字段仅在选择**启用注销**选项时显示，并且是可选项。

设置	说明
	您还可以单击设备详细信息页面中的**注销 Android 企业版自助服务终端**选项，从共享自助服务终端模式注销最终用户。
允许 FIDO 身份验证（需要在设备上安装 Google Chrome 应用程序）	选择此选项后，用户在使用共享 Kiosk 时可使用 FIDO 身份验证。 允许用户使用 FIDO 密钥登录设备。 Google Chrome 是唯一支持的浏览器，设备上必须安装此浏览器才能在共享 Kiosk 中使用 FIDO 身份验证。
允许用户配置亮度并自动旋转	选择以允许用户配置亮度和自动旋转。
启用多窗口	选择以允许使用 Samsung 设备同时显示多个应用（设备所有者自助终端服务）。 要在锁定任务模式中允许多窗口，以下锁定任务模式选项也应启用： • **主页按钮** • **概览按钮**
启用非活动保护	选择启用 Kiosk 模式下的非活动保护。 如果选中，默认值为 30 秒，在此之前 Kiosk 屏幕将保持活动状态。 您可以设置 30 到 3600 之间的任意值。
自助服务终端品牌化	从下拉列表中选择默认或自定义加印品牌选项。
退出自助服务终端 PIN	输入用户必须键入才可以退出自助服务终端模式的 6 位 PIN。 PIN 必须介于 6-10 位数字，最少 6 位，最多 10 位。 此 PIN 适用于自助服务终端模式中的所有设备。 此前，自助服务终端 PIN 长度为 4 位数字。 即使在从早期版本升级到 Ivanti Neurons for MDM 82 之后，用户也可以继续使用 4 位 PIN。 但如有任何配置更改，需要按照新要求设置 PIN 长度（即最少 6 位和最多 10 位）。 Go 应用将保护设备避免暴力攻击。 有关更多信息，请查看 Go for Android 文档。
启用单一应用程序启动器 Kiosk	选择使用 Kiosk 模式将应用程序保留在 GMS 和非 GMS 设备的前台。 需要从应用程序目录中选择应用程序或输入程序包 ID。
允许用户访问 Ivanti 代理设置	选择以在设备保持在**单一应用程序 Kiosk 模式**下时访问 **Ivanti 代理设置**。 以前，管理员必须退出 kiosk 模式才能访问代理设置。 启用设置并分发给设备后，用户可以通过同时按住音量调高和音量调低按钮来打开 Ivanti 代理设置页面。 该功能仅在以工作托管设备模式下注册的 Android 设备上受支持。
启用驾驶员安全	选择以便为“Kiosk 模式允许应用程序”部分下的所有应用程序启用“驾驶员安全”图标 。 如果速度超过限制，请点击“驾驶员安全”图标禁用该应用程序。
创建应用的允许列表：通过将应用添加到允许的应用列表，这些应用将在自助服务终端模式中对用户提供。 拖放应用，使其按照在自助服务终端模式启动栏中显示的顺序排列。 将应用添加到允许的应用列表不会在设备上安装该应用。 确保将每个应用程序分配给应用目录中正确的用户和用户组。	
内置应用	单击“+添加”可将列出的本机应用包括到自助服务终端模式中允许的应用组中。 在自助服务终端模式允许的应用的设置下方，以下选项可用：

设置	说明
	• **清除应用用户数据**：启用此选项允许在用户注销自助服务终端时自动清除所有应用数据，并且没有任何提示。 在自助服务终端模式设置中，选择启用共享设备，以便此选项适用于应用。 ◦ 对于 Google Chrome 和 Webview 软件包，应用数据不会清除，即使它们添加到应用允许列表并启用清除用户数据。 这是因为如果清除这 2 个软件包的应用数据，自助服务终端可能会崩溃。 ◦ 对于不支持应用启动器的系统应用（自助服务终端内部和外部），不会清除应用数据。 • **隐藏**：启用此选项允许其他应用访问该应用，但在自助服务终端启动器中不可用。 如果您在上述锁定设置中禁用拨号器或相机，则无法将其添加至允许的应用列表。
应用目录	单击“+添加”可将应用目录中列出的应用纳入自助服务终端模式中允许的应用组中。
其他应用	单击 + 添加，以包含在 Google Play Store 上不可用的应用的软件包名称。 对于 Samsung 设备，管理员应将以下拨号程序/系统软件包加入允许列表，以使其在自助服务终端模式中正常工作，从而在自助服务终端模式中启用拨号程序功能。 • 呼叫 – com.samsung.android.incallui • 手机 – com.samsung.android.dialer（应加入允许列表；管理员应为此软件包选择隐藏选项，以避免用户出现 2 个拨号程序选项问题） • 呼叫 – com.sec.phone • 呼叫设置 – com.samsung.android.app.telephonyui • 辅助拨号 – com.sec.providers.assisteddialing • 呼叫日志备份/还原 – com.android.calllogbackup • 拨号程序存储 – com.android.providers.telephony • 手机 – com.android.server.telecom • 手机 – com.android.phone • 智能呼叫 – com.samsung.android.smartcallprovider • WiFi 呼叫 – com.sec.unifiedwfc
自助服务终端模式允许的应用程序 **创建应用的允许列表**：通过将应用添加到允许的应用列表，这些应用将在自助服务终端模式中对用户提供。 拖放应用，使其按照在自助服务终端模式启动栏中显示的顺序排列。 将应用添加到允许的应用列表不会在设备上安装该	单击 X 从自助服务终端模式允许的应用组中移除应用。 拖放以更改应用的顺序，此应用是指出现在自助服务终端设备上的应用。 **添加文件夹** - 可以使用此选项在此部分下创建文件夹，并将一个或多个应用程序移动到此文件夹。 最多可以创建两层文件夹。 已复制到一个文件夹的应用程序无法再复制到另一文件夹。 一个文件夹内仅支持 25 个应用程序。

设置	说明
应用。 确保将每个应用程序分配给应用目录中正确的用户和用户组。	
内置应用	单击“+添加”可将列出的本机应用包括到自助服务终端模式中允许的应用组中。 在自助服务终端模式允许的应用的设置下方，以下选项可用： • **清除应用用户数据**：启用此选项允许在用户注销自助服务终端时自动清除所有应用数据，并且没有任何提示。 在自助服务终端模式设置中，选择启用共享设备，以便此选项适用于应用。 ◦ 对于 Google Chrome 和 Webview 软件包，应用数据不会清除，即使它们添加到应用允许列表并启用清除用户数据。 这是因为如果清除这 2 个软件包的应用数据，自助服务终端可能会崩溃。 ◦ 对于不支持应用启动器的系统应用（自助服务终端内部和外部），不会清除应用数据。 • **隐藏**：启用此选项允许其他应用访问该应用，但在自助服务终端启动器中不可用。 如果您在上述锁定设置中禁用拨号器或相机，则无法将其添加至允许的应用列表。
应用目录	单击“+添加”可将应用目录中列出的应用纳入自助服务终端模式中允许的应用组中。
其他应用	单击 + 添加，以包含在 Google Play Store 上不可用的应用的软件包名称。 对于 Samsung 设备，管理员应将以下拨号程序/系统软件包加入允许列表，以使其在自助服务终端模式中正常工作，从而在自助服务终端模式中启用拨号程序功能。 • 呼叫 – com.samsung.android.incallui • 手机 – com.samsung.android.dialer（应加入允许列表；管理员应为此软件包选择隐藏选项，以避免用户出现 2 个拨号程序选项问题） • 呼叫 – com.sec.phone • 呼叫设置 – com.samsung.android.app.telephonyui • 辅助拨号 – com.sec.providers.assisteddialing • 呼叫日志备份/还原 – com.android.calllogbackup • 拨号程序存储 – com.android.providers.telephony • 手机 – com.android.server.telecom • 手机 – com.android.phone • 智能呼叫 – com.samsung.android.smartcallprovider • WiFi 呼叫 – com.sec.unifiedwfc
自助服务终端模式允许的应用程序	单击 X 从自助服务终端模式允许的应用组中移除应用。 拖放以更改应用的顺序，此应用是指出现在自助服务终端设备上的应用。 **添加文件夹** - 可以使用此选项在此部分下创建文件夹，并将一个或多个应用程序移动到此文件夹。 最多可以创建两层文件夹。 已复制到一个文件夹的应用程序无法再复制到另一文件夹。 一个文件夹内仅支持 25 个应用程序。

设置	说明
启用单一应用程序启动器 Kiosk **创建应用的允许列表**：通过将应用添加到允许的应用列表，这些应用将在自助服务终端模式中对用户提供。 拖放应用，使其按照在自助服务终端模式启动栏中显示的顺序排列。 将应用添加到允许的应用列表不会在设备上安装该应用。 确保将每个应用程序分配给应用目录中正确的用户和用户组。	选择使用 Kiosk 模式将应用程序保留在 GMS 和非 GMS 设备的前台。 需要从应用程序目录中选择应用程序或输入程序包 ID。
内置应用	单击“+添加”可将列出的本机应用包括到自助服务终端模式中允许的应用组中。 在自助服务终端模式允许的应用的设置下方，以下选项可用： • **清除应用用户数据**：启用此选项允许在用户注销自助服务终端时自动清除所有应用数据，并且没有任何提示。 在自助服务终端模式设置中，选择启用共享设备，以便此选项适用于应用。 ◦ 对于 Google Chrome 和 Webview 软件包，应用数据不会清除，即使它们添加到应用允许列表并启用清除用户数据。 这是因为如果清除这 2 个软件包的应用数据，自助服务终端可能会崩溃。 ◦ 对于不支持应用启动器的系统应用（自助服务终端内部和外部），不会清除应用数据。 • **隐藏**：启用此选项允许其他应用访问该应用，但在自助服务终端启动器中不可用。 如果您在上述锁定设置中禁用拨号器或相机，则无法将其添加至允许的应用列表。
应用目录	单击“+添加”可将应用目录中列出的应用纳入自助服务终端模式中允许的应用组中。
其他应用	单击 + 添加，以包含在 Google Play Store 上不可用的应用的软件包名称。 对于 Samsung 设备，管理员应将以下拨号程序/系统软件包加入允许列表，以使其在自助服务终端模式中正常工作，从而在自助服务终端模式中启用拨号程序功能。 • 呼叫 – com.samsung.android.incallui • 手机 – com.samsung.android.dialer（应加入允许列表；管理员应为此软件包选择隐藏选项，以避免用户出现 2 个拨号程序选项问题） • 呼叫 – com.sec.phone • 呼叫设置 – com.samsung.android.app.telephonyui • 辅助拨号 – com.sec.providers.assisteddialing • 呼叫日志备份/还原 – com.android.calllogbackup • 拨号程序存储 – com.android.providers.telephony • 手机 – com.android.server.telecom • 手机 – com.android.phone • 智能呼叫 – com.samsung.android.smartcallprovider

设置	说明
	• WiFi 呼叫 – com.sec.unifiedwfc
自助服务终端模式允许的应用程序	单击 X 从自助服务终端模式允许的应用组中移除应用。 拖放以更改应用的顺序，此应用是指出现在自助服务终端设备上的应用。 **添加文件夹** - 可以使用此选项在此部分下创建文件夹，并将一个或多个应用程序移动到此文件夹。 最多可以创建两层文件夹。 已复制到一个文件夹的应用程序无法再复制到另一文件夹。 一个文件夹内仅支持 25 个应用程序。
启用单一应用程序启动器 Kiosk	选择使用 Kiosk 模式将应用程序保留在 GMS 和非 GMS 设备的前台。 需要从应用程序目录中选择应用程序或输入程序包 ID。
创建应用的允许列表：通过将应用添加到允许的应用列表，这些应用将在自助服务终端模式中对用户提供。 拖放应用，使其按照在自助服务终端模式启动栏中显示的顺序排列。 将应用添加到允许的应用列表不会在设备上安装该应用。 确保将每个应用程序分配给应用目录中正确的用户和用户组。	
内置应用	单击“+添加”可将列出的本机应用包括到自助服务终端模式中允许的应用组中。 在自助服务终端模式允许的应用的设置下方，以下选项可用： • **清除应用用户数据**：启用此选项允许在用户注销自助服务终端时自动清除所有应用数据，并且没有任何提示。 在自助服务终端模式设置中，选择启用共享设备，以便此选项适用于应用。 ◦ 对于 Google Chrome 和 Webview 软件包，应用数据不会清除，即使它们添加到应用允许列表并启用清除用户数据。 这是因为如果清除这 2 个软件包的应用数据，自助服务终端可能会崩溃。 ◦ 对于不支持应用启动器的系统应用（自助服务终端内部和外部），不会清除应用数据。 • **隐藏**：启用此选项允许其他应用访问该应用，但在自助服务终端启动器中不可用。 如果您在上述锁定设置中禁用拨号器或相机，则无法将其添加至允许的应用列表。
应用目录	单击“+添加”可将应用目录中列出的应用纳入自助服务终端模式中允许的应用组中。
其他应用	单击 + 添加，以包含在 Google Play Store 上不可用的应用的软件包名称。 对于 Samsung 设备，管理员应将以下拨号程序/系统软件包加入允许列表，以使其在自助服务终端模式中正常工作，从而在自助服务终端模式中启用拨号程序功能。 • 呼叫 – com.samsung.android.incallui • 手机 – com.samsung.android.dialer（应加入允许列表；管理员应为此软件包选择隐藏选项，以避免用户出现 2 个拨号程序选项问题） • 呼叫 – com.sec.phone • 呼叫设置 – com.samsung.android.app.telephonyui • 辅助拨号 – com.sec.providers.assisteddialing

设置	说明
	• 呼叫日志备份/还原 – com.android.calllogbackup • 拨号程序存储 – com.android.providers.telephony • 手机 – com.android.server.telecom • 手机 – com.android.phone • 智能呼叫 – com.samsung.android.smartcallprovider • WiFi 呼叫 – com.sec.unifiedwfc
自助服务终端模式允许的应用程序	单击 X 从自助服务终端模式允许的应用组中移除应用。 拖放以更改应用的顺序，此应用是指出现在自助服务终端设备上的应用。 **添加文件夹** - 可以使用此选项在此部分下创建文件夹，并将一个或多个应用程序移动到此文件夹。 最多可以创建两层文件夹。 已复制到一个文件夹的应用程序无法再复制到另一文件夹。 一个文件夹内仅支持 25 个应用程序。

对于使用 Knox Standard 4.0 或更高版本的 Samsung 设备，多用户功能会在自助服务终端模式下自动锁定。

带有工作配置文件的托管设备

对带有适用于 Android 8.0+ 的工作配置文件的托管设备，禁用特定功能。

对于公司拥有设备上的工作配置文件，可以禁用特定功能（适用于 Android 11+ 设备）。

设置	说明
托管设备锁定设置	
禁用 Wi-Fi	选择以关闭对无线局域网的访问。（不适用于 Android 11+ 设备）
禁用 Wi-Fi 设置	选择以关闭对无线设置的访问。
禁用照相机	选择以关闭对照相机的访问。
禁用蓝牙	选择以关闭蓝牙功能。 谨慎使用该选项。 Ivanti 建议不要禁用音频，因为该操作会禁用对免提 Bluetooth 的访问权限。 在开车出行越加普及的同时，设备的免提使用也有了相应的法律要求。
不允许蓝牙设置	选择以关闭对 Bluetooth 设置的访问。
禁用网络重置	选择此项可防止重置网络（适用于 Android 7.0 及以上版本的设备）。
静音主控音量	选择以将主音量静音。 （不适用于 Android 11+ 设备）
不允许紧急广播	选择以防止紧急广播。
不允许移动网络	选择以关闭对移动网络的访问。 如果禁用 Wi-Fi，则此选项将无法禁用。
不允许数据共享	选择即可关闭将网络共享选项，也就是使用一台设备互联网连接为另一台设备提供互联网连接。
不允许 VPN	选择以关闭对 VPN 连接的访问。 （不适用于 Android 11+ 设备）
禁用恢复出厂设置	选择以阻止用户将设备恢复为出厂设置。 （不适用于 Android 11+ 设备）
启用出厂重置保护	选择以允许用户将设备恢复为出厂设置。 您可以选择指定授权 Google 帐户 ID 的列（整数值），该列表可以在恢复出厂重置后配置设备，或者将鼠标悬停在帮助图标上以查看检索授权帐户 ID 的帮助。
不允许拨出电话	选择以阻止用户呼出电话。
不允许安全启动 (Android 6.0+)	选择以阻止用户将设备重新启动为安全启动模式。
禁止调试功能	选择以便禁用设备上的调试功能。 该选项默认打开。
确保验证应用程序	选择以便允许使用设备上的应用程序验证功能。 该选项默认打开。 该选项关闭后，该设备将返回到默认行为，这可能因设备而异。
不允许短信	选择以阻止用户发送和接收短信。
不允许取消静音麦克风	选择 以阻止用户取消设备的麦克风静音。
不允许自动时间	选择 以阻止用户启用自动时间变化。
不允许自动时区	选择以阻止用户随着时区变化启用自动设备时间调整。
禁用数据漫游	选择以在设备处于漫游状态时关闭数据交换。

设置	说明
与服务器同步时间 (Android 9.0+)	选择以允许设备在首次注册时与 Ivanti Neurons for MDM 服务器同步时间，此后在每次签入后每 24 小时同步一次。 此选项仅在选择**禁用自动时间**时可用。
设置时区 (Android 9.0+)	指定奥尔森时区 ID 格式中的时区字符串（例如，太平洋/中途岛）。
禁用 Wi-Fi 休眠模式	选择以确保在设备处于休眠模式时，WiFi 处于开启状态。 （不适用于 Android 11+ 设备）
限制输入方法	选择以通过**程序包名称**字段指定已加入允许列表的程序包名称列表，进而限制工作应用的输入方法。 （不适用于 Android 11+ 设备） 设备将可以同时使用已加入允许列表的软件包输入法和默认系统输入法。 用户可以在默认系统输入法和已加入允许列表的软件包输入法之间切换。 在 Android 10+ 中，输入方法仅适用于设备侧，否则将受限于整个设备。
限制可访问性服务	选择以通过**软件包名称**字段指定已加入允许列表软件包名称的列表，限制工作应用的无障碍服务。 如果没有已加入允许列表的软件包，仅允许系统无障碍服务。 在 Android 10+ 中，输入方法仅适用于工作设备，否则将受限于整个设备。
禁用 USB 文件传输	选择以禁用 USB 文件传输。
禁用外部媒介	选择以禁用外部媒介。
设备不允许未知来源	选择以防止设备安装来自未知来源的应用程序。 此设置在设备上生效取决于预期的 Google Play 更新，以启用此功能。
设置锁屏界面消息 (Android 7.0+)	选择以设置在设备上显示的锁定屏幕消息。 在文本字段中，键入锁定屏幕消息（最多 256 个字符）。 通过启用此选项，阻止用户在“设置”中设置消息，并向用户显示管理员设置的消息。 如果管理员未在启用“设置锁定屏幕消息”之后提供任何锁定屏幕消息，将阻止用户在“设置”中设置消息，但不会向用户显示任何消息。
设置屏幕亮度	选择此项以设置设备屏幕的亮度。 • 手动 - 选择此项以手动输入数字（0 至 255） • 自适应 - 选择此项以允许设备自行设置亮度 建议启用“禁止配置亮度”选项后再设置设备的屏幕亮度。 如果允许用户进行更改，这些设置将在下次签入时重置为管理员定义的设置。 对于公司拥有设备上的工作配置文件模式，运行 Android 11 和更高版本的设备不支持此设置。
设置屏幕超时	选择此项以设置屏幕超时持续时间（以秒为单位）。 建议启用“禁止配置屏幕超时”选项后再设置设备的屏幕亮度。 如果允许用户进行更改，这些设置将在下次签入时重置为管理员定义的设置。 对于公司拥有设备上的工作配置文件模式，运行 Android 11 和更高版本的设备不支持此设置。
设置屏幕方向	选择此项以设置屏幕方向。 可以使用下拉列表将屏幕方向设置为 0、90、180 或 270 度。 对于公司拥有设备上的工作配置文件模式，运行 Android 11 和更高版本的设备不支持此设置。
不允许自动填充 (Android 8.0+)	选择以不允许自动填充。 （不适用于 Android 11+ 设备）
不允许 Bluetooth 共享 (Android 8.0+)	选择以不允许用户在设备上共享传出 Bluetooth。

设置	说明
禁用备份服务 (Android 8.0+)	选择以禁用备份服务。 （不适用于 Android 11+ 设备）
不允许打印 (Android 9.0+)	选择以限制从所有应用打印。（不适用于 Android 11+ 设备）
不允许飞行模式 (Android 9.0+)	选择以在整个设备中禁用飞行模式。
不允许息屏显示 (Android 9.0+)	选择以不允许用户的环境显示。 （不适用于 Android 11+ 设备）
不允许配置亮度 (Android 9.0+)	选择此项以禁止用户配置亮度（不适用于 Android 11+ 设备）。 建议在定义“设置屏幕亮度模式”后再选择此选项。
不允许配置日期时间 (Android 9.0+)	选择以不允许日期、时间和时区配置。
不允许配置位置 (Android 9.0+)	选择以不允许用户禁用位置提供商。
不允许配置屏幕超时 (Android 9.0+)	选择此项以禁止用户更改屏幕关闭超时。 （不适用于 Android 11+ 设备） 建议在设置“设置屏幕超时”值后再选择此选项。
不允许系统错误对话框 (Android 9.0+)	选择以不允许显示系统错误对话框。（不适用于 Android 11+ 设备）
禁用屏幕捕获 (Android 11.0+)	选择以禁用设备内置屏幕截图功能。 在选择时，屏幕捕获将在设备的个人端禁用。
Android 12.0+	
仅为充电启用 USB	选择以仅允许 USB 端口用于充电。
Android 13.0+	
设置最低 Wi-Fi 安全要求	使用此选项可设置最低 Wi-Fi 安全要求： • 无最低安全要求 - 如果无最低安全要求，请选择此选项 • 基于个人网络的安全 - 选择此选项可阻止个人 Wi-Fi 网络，如 WEP、WPA/WPA2/WPA3 等。 • 基于企业 EAP 网络的安全 - 选择此选项可阻止基于 EAP 协议的 Wi-Fi 网络 • 基于企业 192 网络的安全 - 选择此选项可阻止基于 EAP 企业的 Wi-Fi 网络 不符合最低标准的所有现有设备将断开连接。 设备详细信息将在**常规 > Wi-Fi 安全等级**下显示最低 Wi-Fi 安全等级要求（如有）。
禁止共享管理员配置的 Wi-Fi	选择此选项可防止用户共享管理员设置的 Wi-Fi 配置。
工作配置文件锁定设置	
禁用屏幕捕获	选择后不能使用设备内置屏幕截图功能。
不允许应用控制	选择阻止用户修改设置或启动器中的应用程序。
不允许配置凭据	选择阻止用户配置用户凭据。

设置	说明
不允许跨过配置文件复制粘贴	选择阻止在两个配置文件之间复制/粘贴信息。
不允许修改账号	选择阻止用户添加或移除账户。
不允许 NFC（出站 Beam）(Android 5.1 +)	选择以阻止用户使用 NFC 传输应用数据。
不允许共享位置	选择以防止网站和应用提示设备用户共享设备位置。
禁止调试功能	选择以便禁用设备上的调试功能。 该选项默认打开。
确保验证应用程序	选择以便允许使用设备上的应用程序验证功能。 该选项默认打开。 该选项关闭后，该设备将返回到默认行为，这可能因设备而异。
在工作配置文件中禁用未知来源	选择以禁止在工作配置文件中从未知来源下载。
启用/禁用系统应用程序	选择以启用和禁用通过**系统应用软件包名称**字段指定两个软件包名称列表部署系统应用。 使用此功能管理对 Google Play 中未发布的系统应用程序的访问。 不支持将应用添加到 App Catalog 和系统应用列表。
禁用 Caller ID (Android 6.0 +)	设置是否在来电设备中显示工作配置文件中的来电者 ID 信息。
禁用通过 Bluetooth 共享联系人 (Android 6.0+)	选择以便防止设备通过 Bluetooth 与其他设备共享联系人。
禁用通过搜索共享联系人 (Android 7.0+)	选择以便防止用户从个人电话拨号程序中搜索工作联系人。
不允许自动填充 (Android 8.0+)	选择以不允许自动填充。 （不适用于 Android 11+ 设备）
在个人配置文件中不允许工作应用通知 (Android 8.0+)	选择以限制工作配置文件通知。
不允许打印 (Android 9.0+)	选择以限制从所有应用打印。 （不适用于 Android 11+ 设备）
不允许共享到配置文件 (Android 9.0+)	选择以阻止用户将个人数据共享到设备中的工作配置文件。
限制输入法 (Android 10.0+)	选择以通过**软件包名称**字段指定已加入允许列表软件包名称的列表，限制已加入允许列表的 IME 软件包名称（不适用于 Android 11+ 设备）。 设备将可以同时使用已加入允许列表的软件包输入法和默认系统输入法。 用户可以在默认系统输入法和已加入允许列表的软件包输入法之间切换。 输入法将适用于在工作配置文件端安装的 IME 应用。 对于在工作配置文件端使用的应用，这些允许列表将不可用，即使为此锁定将在设备端安装的应用加入允许列表。
允许访问工作配置文件日历 (Android 10.0+)	选择以下任一选项，以允许所有应用或在个人端选择一组应用，从而访问在工作配置文件中显示的日历信息：

设置	说明
	• **个人配置文件中的所有应用** - 允许所有应用访问工作配置文件中的日历信息 • **仅限个人配置文件中的以下应用** - 在以下文本字段中，输入应用的捆绑 ID，用逗号分隔。 只有个人端的这些选定应用才能访问工作配置文件中的日历信息。 个人端的应用应实施特定 API，以访问共享日历。
启用应用的跨配置文件允许列表 (Android 11.0+)	通过选中复选框，用户可以将特定应用中的信息从工作配置文件共享到设备的个人端。 在**已加入允许列表的应用**字段中，键入要加入允许列表的应用的软件包 ID，并使用逗号隔开。 此选项默认禁用。
启用最大配置文件超时 (Android 11.0+)	选择以设置可以在 Ivanti Neurons for MDM 于设备上暂停个人应用前关闭工作配置文件的最大时间范围。 您可以设置 72-8760 小时之间的时间。 8760 小时是一年的时间。 如果选择选项，默认值会设置为 72 小时。 设备用户会看到一则消息，并提示您打开工作配置文件，以启用暂停的应用。 适用于公司拥有设备上的工作配置文件中的 Android 11+ 设备。 如果配置文件关闭的时间较长，个人应用程序将在设备上暂停。
启用 5G 网络切片 (Android 12.0+)	选择此项以在公司拥有设备的工作配置文件中提供 5G 网络切片选项。 此选项默认禁用。
禁用 AI 辅助 (Android 15.0+)	选择此选项可禁止用户使用 AI 辅助功能。 此选项默认禁用。

有关更多信息，请查看如何创建配置

10.10.4.33. 锁定和自助服务终端：Samsung Knox Standard

锁定和自助服务终端：Samsung Knox Standard 配置会禁用 Samsung Knox Standard 设备的特定功能，并创建将在自助服务终端模式中对用户可用的应用允许列表。

> Samsung KNOX 标准配置已停用，在运行 Android 9 及以上版本的设备上不受支持。

锁定设置

设置

流程

名称

输入用于识别此配置的名称。

说明

输入阐明此配置目的的说明。

Samsung Knox 锁定设置：仅禁用 Samsung Knox 设备上的特定功能。

禁用 Wi-Fi

选择以关闭对无线局域网 (WLAN) 的访问。

禁用照相机

选择以关闭对照相机的访问。

禁用蓝牙

选择以关闭蓝牙功能。

仅允许蓝牙音频

选择仅打开 Bluetooth 音频功能。

禁用手机数据

选择以关闭在设备与其他设备联系时的数据交换。

如果禁用 Wi-Fi，则此选项将无法禁用。

禁用 GPS

选择以关闭 GPS。

禁用电话拨号器

选择以关闭手机应用。

禁用 SD 卡

选择以关闭对 SD 卡的访问。

禁用 Google 备份

选择以关闭备份至 Google 服务器。

禁用复制/粘贴

选择以关闭对复制/粘贴功能的访问。

禁用 NFC

选择以关闭设备与其他设备联系时的 NFC （近场通讯）数据交换。

禁用麦克风

选择以关闭对设备麦克风的访问。

禁用屏幕捕获

选择以禁用设备内置屏幕截图功能。 打开此选项后，不允许使用 Go 的屏幕截图功能。 此类屏幕截图功能会被禁用。

禁用蓝牙数据共享

选择以关闭将蓝牙作为捆绑选项，为一台设备接入另一台设备提供互联网连接。

禁用 USB 调试

选择以关闭 USB 调试功能。

禁用 USB 数据共享

选择以关闭将 USB 作为捆绑选项，为一台设备接入另一台设备提供互联网连接。

禁用 Wi-Fi 数据共享

选择以关闭将 Wi-Fi 作为捆绑选项，为一台设备接入另一台设备提供互联网连接。

禁用本机浏览器

选择以阻止用户访问 Android 浏览器。

禁用 YouTube

选择以阻止用户访问 YouTube。

禁用恢复出厂设置

选择以阻止用户将设备恢复为出厂设置。

禁用 OTA 升级

选择以关闭对设备固件的无线升级。

警告：如果启用了 **OTA 升级**，请勿禁用**禁用设置更改**功能。 启用 **OTA 升级**时，如果禁用了**禁用设置更改**将导致设备无法正常工作，因为升级需要更改设置。

禁用语音漫游

选择以在设备处于漫游状态时，关闭对语音通话的访问。

禁用 USB 媒体播放器

选择以关闭 USB 媒体播放器。

禁用 Google Play

选择以关闭对 Google Play 的访问。

禁用数据漫游

选择以在设备处于漫游状态时关闭数据交换。

禁用未知来源

选择以便禁用 Google Play Store 以外的任何地方安装应用程序，但 Go 应用程序除外。

禁用设备管理员权限删除

选择以禁止用户从 Go 关闭设备管理员权限。

禁用设置更改

选择以关闭对设备设置应用的访问。

警告：如果启用了 **OTA 升级**，请勿禁用**禁用设置更改**功能。 启用 **OTA 升级**时，如果禁用了**禁用设置更改**将导致设备无法正常工作，因为升级需要更改设置。

自助服务终端模式设置： 自助服务终端模式对设备应用附加限制，包括限制通过自定义启动栏访问应用。

仅适用于 Android 8.1 及以下版本。 对于 Android 9.0 版本，请使用 Android Enterprise 托管设备 Kiosk 配置。

启用自助服务终端模式

选择以便在 Android 设备上配置自助服务终端模式。

允许用户访问 Wi-Fi 设置

选择 以允许用户更改 Wi-Fi 设置并访问首选 无线网络。

允许用户访问蓝牙设置

选择 以允许用户更改蓝牙设置并配对其他 蓝牙设备。

允许用户延迟应用程序的更新

选择 以允许用户延迟应用程序更新。

GPS 位置设置

选择以下其中一种 GPS 位置设置：

- 禁用位置
- 启用位置
- 允许用户选择

退出自助服务终端 PIN

输入该四位代码，最终用户才能退出自助服务终端模式。

创建应用的允许列表：通过将应用添加到允许的应用列表，这些应用将在自助服务终端模式中对用户提供。 拖放应用程序，使其按照在自助服务终端模式启动栏中显示的顺序排列。

将应用添加到允许的应用列表不会在设备上安装该应用。 确保将每个应用程序分配给应用目录中正确的用户和用户组。

内置应用

单击“+添加”可将列出的本机应用包括到自助服务终端模式中允许的应用组中。

如果您在上述锁定设置中禁用拨号器或相机，则无法将其添加至允许的应用列表。

应用目录

单击“+添加”可将应用目录中列出的应用纳入自助服务终端模式中允许的应用组中。

其他应用

单击 + 添加，以包含在 Google Play Store 上不可用的应用的**软件包名称**。

自助服务终端模式允许的应用程序

单击 X 从自助服务终端模式允许的应用组中移除应用。 拖放以更改应用的顺序，此应用是指出现在自助服务终端设备上的应用。

> 至于在 Android 4.4 或支持的更新版本上使用自助服务终端模式，支持多用户的 Samsung 设备将在自助服务终端模式中自动锁定多用户功能。

有关更多信息，请查看**如何创建配置**

10.10.4.34. 本地管理员密码解决方案配置

本地管理员密码解决方案 (LAPS) 配置设置使 Ivanti Neurons for MDM 管理员能够以设定的时间间隔在受管的 macOS 设备上自动重新生成本地管理员密码。 有关 on LAPS 的更多信息，请参阅本地管理员密码解决方案 (LAPS)。

适用于：使用自动化设备注册而注册和受管的 macOS 设备。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**本地管理员密码解决方案 (LAPS)** 配置。
3. 根据下表配置 **LAPS** 设置：

设置	描述
名称	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
平台	从下拉列表中选择 macOS。
轮换间隔	从下拉列表中选择以下选项之一以定义密码的自动轮换： • 不轮换（**默认**） • 15 天 • 30 天 • 60 天 • 90 天 • 120 天 • 180 天
在查看间隔后轮换	从下拉列表中选择以下选项之一，以便在从**设备详细信息**页面查看密码后自动旋转密码： • 1 至 24 小时 • 36 小时 • 48 小时 默认值设置为 **2 小时**。

4. 单击**下一步**，配置分配设置。
5. 选择其中一个分发选项来设置**本地管理员密码解决方案 (LAPS)** 配置。 有关配置分发选项的详细信息，请参阅使用配置。
6. 单击**完成**。

10.10.4.35. macOS 防火墙

许可证：Gold

macOS 防火墙管理可在 macOS 设备上的“安全首选项”窗格中访问的应用防火墙设置。

适用于：macOS 12.3+

- **允许内置软件接收传入的连接** - 若为 True，将允许内置软件接收传入的连接。
- **允许已下载的签名软件接收传入的连接** - 若为 True，将允许已下载的签名软件接收传入的连接。

适用于：macOS 12.0+

- **启用日志记录** - 若为 True，将启用日志记录
- **指定日志记录类型**
  - **限制**
  - **简要**
  - **详细信息**

适用于：macOS 10.12+

点击**启用防火墙**后，您可以选择以下一个或多个选项：

- **阻止所有传入** - 选择此选项可阻止所有共享服务（例如屏幕共享或文件共享）接收 macOS 设备上的传入连接。 以下系统服务可能仍会接收传入的连接：
  - configd，用于实现 DHCP 等网络配置服务
  - mDNSResponder，用于实现 Bonjour
  - racoon，用于实现 IPSec
- **启用隐藏模式** - 选择此项可防止 macOS 设备响应探测请求。 托管 macOS 设备仍会响应授权应用程序的传入请求，同时忽略意外请求，例如 ICMP (ping)。
- **应用程序** - 连接由防火墙控制的应用程序的列表 选择要在 macOS 设备上为之接收传入连接的特定应用程序。

选择**添加+** 向应用程序列表添加一行。 选择**捆绑包 ID** 下的单元格，以选择要显式允许其传入连接的应用程序。 选中**允许连接**单元格中的复选框，以允许来自所选应用程序的传入连接。

> 配置必须存在于系统范围的配置文件中。 如果多个配置文件包含此配置，则将使用最严格的设置联合。

> 不支持**自动允许签名的下载软件**和**自动允许内置软件**选项。 但是，当此配置可用时，这两个选项将强制为 ON。

> 管理员可以通过指定 ping 命令无法发现的设备来启用隐藏模式。

10.10.4.36. macOS 限制

许可证：Gold

macOS 限制决定在 macOS 服务上启用启用哪些限制。

您可以设置在 macOS 设备上启用或禁用以下功能：

macOS 版本	功能
macOS 10.11+ **macOS 10.11.2+**	• 允许相机 • 允许 iCloud 文档同步 **仅监测：** • 允许 Spotlight Internet 结果
	• 允许定义查找
macOS 10.12+	
macOS 10.12.4+	• 允许 iCloud 密钥链同步 • 允许返回到我的 Mac • 允许查找我的 Mac • 允许共享到备注、提醒或 LinkedIn • 允许书签同步 • 允许 macOS 邮件 iCloud 服务 • 允许 macOS iCloud 日历服务 • 允许 macOS iCloud 地址簿服务 • 允许 iCloud 提醒服务 • 允许自动解锁 **仅监测：** • 允许 Apple 音乐
	• 允许指纹解锁
macOS 10.13+	
	• 允许 iTunes 文件共享 • 允许内容缓存 • 允许修改壁纸 **仅监测：** • 允许 AirPrint • 允许 AirPrint iBeacon 发现

macOS 版本	功能
	• 强制 AirPrint 可信 TLS 要求 • 允许 AirDrop • 允许游戏中心
macOS 10.13.4+	
macOS 10.14+	**仅监测：** 将软件更新推迟一段时间（30 到 90 天） 默认：30 天。
	仅监测： 允许附近设备共享密码请求
macOS 10.14.4+	
macOS 11.0+	• 允许屏幕截图 • 允许远程屏幕观察 **仅监测：** • 允许自动加入教室 • 允许教室请求离开课堂的权限 • 允许课堂在不提示的情况下锁定应用和设备 • 允许强制无人管理教室屏幕观察 **仅监测：** 允许强制延迟应用程序软件更新
macOS 11.3+	
macOS 11.3+	强制指纹超时 默认：48 小时 先决条件：必须在设备上配置 Touch ID **仅监测：** • 强制实施软件更新主操作系统延迟安装推迟 • 强制实施软件更新次要操作系统延迟安装推迟 • 强制实施软件更新非操作系统延迟安装推迟 • 强制实施延迟主软件更新

macOS 版本	功能
macOS 12+	
macOS 13.0 至 26.0	• allowCloudPrivateRelay：如果您在 macOS 设备中将“Private Relay”设置为“ON”，则网络流量将被加密，以确保 Internet 活动的隐私性和安全性。 此限制需要使用受监督设备。 • 允许 iCloud 照片库 **仅限受监管设备**： • 允许擦除内容和设置

macOS 14.0+	• 允许背景安全改进安装：禁用响应。 用户无法安装背景安全改进。
	• 允许删除背景安全改进：阻止用户撤销响应。 用户无法删除背景安全改进。
	• 允许通用控制：
	  ◦ 如果为 **True**，则该配置允许使用主设备的输入设备来控制辅助显示设备。
	  ◦ 如果为 **False**，则可以添加辅助显示设备，但不能使用主输入设备对其进行控制。
	  仅限受监管设备：
	• 允许 UI 配置的配置文件安装：如果为 False，则该配置不允许在 macOS 设备上安装配置文件、配置或证书。
	• 允许 USB 限制模式：如果为 True，则该配置将锁定设备，使其无法使用远程连接的输入设备。 设备上的“允许附件连接”选项会变为灰色。
	• 允许修改 ARD 远程管理
	  ◦ 如果为 False，则阻止修改系统设置中的远程管理共享设置。
	  ◦ 默认：真
	• 允许修改蓝牙共享
	  ◦ 如果为 False，则阻止修改系统设置中的蓝牙设置。
	  ◦ 默认：真
	• 允许云自由格式
	  ◦ 如果为 False，则不允许 iCloud 自由格式服务。
	  ◦ 默认：真
	• 允许修改文件共享
	  ◦ 如果为 False，则阻止修改系统设置中的文件共享设置。
	  ◦ 默认：真
	• 允许修改互联网共享
	  ◦ 如果为 False，则阻止修改系统设置中的 Internet 共享设置。
	  ◦ 默认：真
	• 允许创建本地用户

macOS 版本	功能
macOS 15.0+	◦ 如果为 False，则阻止在系统设置中创建新用户。 ◦ 默认：真 • 允许修改打印机共享 ◦ 如果为 False，则阻止修改系统设置中的打印机共享设置。 ◦ 默认：真 • 允许修改远程 Apple 事件 ◦ 如果为 False，则阻止修改系统设置中的远程 Apple 事件共享设置。 ◦ 默认：真 • 允许 Siri ◦ 默认：真 • 允许修改启动磁盘 ◦ 如果为 False，则阻止修改系统设置中的启动磁盘设置。 ◦ 默认：真 • 允许时间机器备份 ◦ 如果为 False，则阻止修改系统设置中的时间机器设置。 ◦ 默认：真 **仅限受监管设备**： • 允许账户修改 ◦ 如果为 false，则阻止帐户修改。 ◦ 默认：真 • 允许修改设备名称 ◦ 如果为 false，则阻止更改设备名称。 ◦ 默认：真 • 允许修改 TouchID 指纹 ◦ 如果为 false，则阻止修改 Touch ID 指纹。 ◦ 默认：真
	仅限受监管设备： • 允许 Genmoji ◦ 选择此选项可允许创建 Genmoji。 ◦ 默认：真 • 允许 Image Playground ◦ 选择此选项可允许使用图像生成功能。 ◦ 默认：真 • 允许 iPhone 镜像

macOS 版本	功能
macOS 15.1+ macOS 15.2+	◦ 选择此选项可允许 iPhone 在 macOS 设备中执行镜像操作。 ◦ 默认：真 • 允许书写工具 ◦ 选择此选项可启用 Apple Intelligence 书写工具。 ◦ 默认：真 **仅限受监管设备**： • 允许邮件摘要 ◦ 选择此项可手动创建电子邮件摘要。 ◦ 默认：真 • 允许修改媒体共享 ◦ 选择此项可修改媒体共享设置。 ◦ 默认：真
macOS 15.3	**仅限受监管设备**： • 允许外部情报集成 ◦ 选择此项可通过 Siri 使用外部云端情报服务。 ◦ 默认：真 • 允许外部情报集成登录 ◦ 选择此项可启用默认浏览器首选项修改。 应用此项后，用于设置默认浏览器首选项的 Ivanti Neurons for MDM 设置命令仍然有效。 ◦ 默认：真 **安全性和隐私**： • 允许外部情报工作区 ID ◦ 输入允许的外部情报工作区 ID • 允许笔记转录摘要 ◦ 选择以启用从转录创建摘要。 ◦ 默认值：true

10.10.4.37. macOS AppStore 限制

许可证：Gold

macOS AppStore 限制定义在 macOS AppStore 上启用哪些限制。

您可以设置以下选项：

设置	**流程**
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
配置设置	
macOS 版本	**功能**
10.9+	将应用程序安装限制为管理员用户。
10.10+	• 将应用程序安装限制为仅软件更新。 • 禁用用户采用应用程序。 • 禁用软件更新通知。
10.11+	将应用程序安装限制为 MDM 安装的应用程序和软件更新。

分配配置

步骤

1. 使用前表，设置选项。
2. 单击**下一步**。
3. 选择**启用此配置**选项。
4. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义

单击**完成**。

10.10.4.38. macOS 磁盘刻录限制

许可证：Gold

macOS 磁盘刻录限制管理 macOS 中的磁盘刻录限制。 您可以配置 **macOS Finder 设置**来启用或禁用 macOS 上的 Finder 应用程序中的光盘刻录选项。

您可以设置以下选项：

设置	**流程**
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
配置设置	
设置	**采取何种措施**
允许磁盘刻录	• 打开 • 关闭 • 需要身份验证

分配配置

步骤

1. 使用前表，设置选项。
2. 单击**下一步**。
3. 选择**启用此配置**选项。
4. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义

单击**完成**。

10.10.4.39. 允许的媒体控制（已弃用）

许可证：Gold

允许的媒体控制配置管理在 macOS 中各种物理媒体的安装、卸载和注销时弹出。

您可以设置以下选项：

设置	流程
名称 说明 **配置设置** **针对介质类型的安装控制** 打开每种介质类型的安装控制，并设置安装设置。 如果关闭安装控制，则将应用操作系统默认设置。 **介质类型** • CD • DVD • BD	输入用于识别此配置的名称。 输入阐明此配置目的的说明。 **安装设置** • 只读，带身份验证 • 拒绝安装 • 弹出介质
• 空 CD • 空 DVD • 空 BD • DVD-RAM • 磁盘映像 • 内部硬盘 • 外部硬盘 • 网络磁盘	• 只读 • 拒绝安装 • 弹出介质 • 认证
• 外部硬盘包括 USB HDD、USB 闪存驱动器存储和 SD 卡。 • 默认情况下，只读媒体安装为只读，例如 CD、DVD 和 BD 等。	
针对媒体类型的卸载控制	
打开每种介质类型的卸载控制，并设置卸载设置。 如果关闭卸载控制，则将应用操作系统默认设置。 为介质类型设置“拒绝卸载”设置时，请务必小心。 **介质类型** • CD • DVD • BD • 空 CD • 空 DVD • 空 BD • DVD-RAM • 磁盘映像	**安装设置** • 拒绝卸载 • 认证

设置	流程
• 内部硬盘 • 外部硬盘 • 网络磁盘 **在注销时弹出设置**	
介质类型在用户注销时自动弹出。	
介质类型	
• CD • DVD • BD • 空 CD • 空 DVD • 空 BD • DVD-RAM • 磁盘映像 • 外部硬盘 • 网络磁盘	

分配配置

步骤

1. 使用前表，设置选项。
2. 单击**下一步**。
3. 选择**启用此配置**选项。
4. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义

单击**完成**。

10.10.4.40. macOS Finder 设置

许可证：Gold

macOS Finder 设置在 macOS 中管理 Finder 应用程序的设置。

您可以设置以下选项：

设置	**流程**
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
配置设置	
设置	**采取何种措施**
在 Finder 中禁用光盘刻录支持	• 开启 • 关闭

分配配置

程序

1. 使用前表，设置选项。
2. 单击**下一步**。
3. 选择**启用此配置**选项。
4. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义

单击**完成**。

10.10.4.41. macOS 内核扩展策略

适用于：macOS 10.13.2 或支持的更新版本。

控制加载用户批准内核扩展的限制和设置。

创建 macOS 内核扩展策略配置

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中键入**内核**，然后单击 **macOS 内核扩展策略**配置。
4. 命名并描述配置。
5. 选择**允许用户覆盖**选项，以允许用户批准下列配置未明确允许的其他内核扩展。
6. 在允许的团队标识符和内核扩展部分中，单击 **+ 添加**，以添加允许的团队标识符和内核扩展。 内核扩展是软件包的捆绑包标识符。 对于每个团队标识符，您可在弹出窗口中添加一些有效签名的内核扩展名称。
7. 单击**添加**。
8. 单击**下一步**，配置分配设置。
9. 点击**完成**。

有关更多信息，请查看如何创建配置

10.10.4.42. Mobile@Work for macOS

本部分包含以下主题：

- Mobile@Work for macOS 配置和脚本执行工作流
- 创建 Mobile@Work for macOS 配置
- 为 macOS 设备启用用户加入
- 创建 Mobile@Work for macOS 脚本配置
- 完全卸载 Mobile@Work for macOS
- 应用采用 macOS Mobile@Work 的脚本

Ivanti Neurons for MDM 允许您自行创建 macOS Shell 脚本，您可将其上传到 Ivanti Neurons for MDM，并在受管 macOS 设备上运行。 有关创建、上传和管理脚本存储库的信息，请查看所有脚本。

通过 Mobile@Work for macOS 1.1 或更高版本，macOS 设备用户可以发起停用设备。 当您在关于 Mobile@Work 屏幕中单击**卸载**时，停用选项可用。 在 Ivanti Neurons for MDM 中，您可以在**设备**页面和设备详细信息页面中确认设备状态。

Mobile@Work for macOS 1.5 或更高版本将在注册后立即打开 Apps@Work，无需等待 MDM 注册完成。

在 Mobile@Work for macOS 中，单击应用磁贴，以显示该应用的应用详细信息页面。 该页面包含应用描述、屏幕截图、评分和评论。

如果 Packager 内部 macOS 应用已安装或未在库存报告中，Mobile@Work for macOS 会通知 Ivanti Neurons for MDM 服务器。

先决条件

在 App Catalog 中，Mobile@Work for macOS 客户端可用作企业应用。 在 macOS 设备上运行 Shell 脚本前，请指示用户使用 Mobile@Work for macOS 在 Ivanti Neurons for MDM 中注册其设备。

步骤

1. 下载 macOS 应用的 Mobile@Work。 它可以作为 PKG 文件提供，请访问：https://support.mobileiron.com/support/CDL.html。 请参阅此 Ivanti 客户论坛文章，了解有关获取下载站点凭据的信息。
2. 将适用于 Mobile@Work for macOS 的 PKG 文件上传到安全服务器。 设备用户必须能够访问此服务器。
3. 通过电子邮件或消息，与设备用户共享适用于 Mobile@Work for macOS 的安全文件 URL。
4. 指示用户：
    1. 在他们的设备上下载和安装 Mobile@Work for macOS。
    2. 使用 Mobile@Work for macOS 在 Ivanti Neurons for MDM 中注册设备。

Mobile@Work for macOS 配置和脚本执行工作流

步骤

1. 设置并分发 Mobile@Work for macOS 配置。
2. 设置和分发 Mobile@Work for macOS 脚本配置，以将脚本上传至 Ivanti Neurons for MDM。 脚本将使用签名证书加密和签名，每个租户的脚本唯一。 解密脚本的密钥将与脚本的下载 URL 一同发送到设备（均已加密和签名）。
3. Ivanti Neurons for MDM 使用 Mobile@Work for macOS 在 macOS 设备上执行脚本。 Mobile@Work for macOS 会定期轮询 Ivanti Neurons for MDM，以查看是否有任何脚本正在等待执行。 如果队列中有脚本，Mobile@Work 会根据您在 Ivanti Neurons for MDM 中定义的设置在 macOS 设备上下载并运行脚本。

4. Mobile@Work for macOS 会将脚本执行结果返回到 Ivanti Neurons for MDM，并将显示在设备日志中。 在**日志**选项卡中，您可从 macOS 设备的设备详细信息页面查看设备日志。

创建 Mobile@Work for macOS 配置

Mobile@Work for macOS 配置的默认系统配置可用。 但并非由任何设备默认分发。

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中键入**工作**，然后单击 **Mobile@Work for macOS** 配置。
4. 命名并描述配置。
5. 输入**最大运行时间**（以秒为单位），以指定脚本的运行时间。 默认值是 60 秒。
6. 输入**最大响应大小**（以千字节 KB 为单位），以指定返回到 Ivanti Neurons for MDM 的脚本输出的最大响应大小限制。 这是在运行脚本时返回的 stdout 或 stderr 数据。 默认值为 1 KB。
7. 输入**签入频率**（以分钟为单位），以指定 Mobile@Work for macOS 必须通过 Ivanti Neurons for MDM 签入的频率。 默认值为 15 分钟。
8. （可选）您可以使用**为 macOS 设备启用用户加入**部分，为 macOS 设备启用用户加入。
9. 点击**下一步**以配置分发设置。
    1. 选择分发级别：
    2. **每个人** — 将应用添加至所有用户兼容设备。
    3. **无** — 将应用暂存，以便稍后进行分配。
    4. **自定义分发** - 选择以下任意选项：
        - **用户/用户组** - 应用仅分发到您选择的用户或用户组。
          单击**用户**选项卡，以选择用户。
          单击**用户组**选项卡，以选择用户组。
        - **设备/设备组** - 应用仅分发到您选择的设备或设备组
          单击**设备**选项卡，以选择设备。
          单击**设备组**选项卡，以选择设备组。
10. 点击**完成**。

为 macOS 设备启用用户加入

在自动设备注册过程中，您可以为 macOS 设备启用用户入门，如下所示：

- 在 Device Enrollment 完成后，Mobile@Work for macOS（需要版本 1.68 或更高版本） 会推送到设备，以及配置文件、配置和应用。
- Mobile@Work for macOS 客户端和其他应用仅在满足以下条件时推送到设备：
    - 这些应用是内部 PKG 应用或 Apple App 和图书公共应用。
    - 对于应用的静默安装设置，将其设置为真。 **应用** > **应用详细信息** > **应用配置** > **在设备上安装**页面提供该设置。
    - **应用的首选项**设置为“高”。 默认情况下，Mobile@Work for macOS 客户端应用程序的优先级会设置为高（并且无法修改），**否则用户入门过程可能会失败**。
    - 这些应用配置为分发到设备、用户组或设备组。

- 在安装和注册 Mobile@Work for macOS 后，macOS 设备会进入自助服务终端模式（用户没有设备的控制权限），直到配置和安装剩余的配置文件、配置和应用。 进度会分步显示。

对于 Mobile@Work for macOS 1.73 和 Ivanti Neurons for MDM 支持的更高版本，支持以下附加功能：

- 在设备的设备注册完成后，用户启动过程将立即完成。 即使管理员在 Mobile@Work 配置中启用用户启动，用户启动过程也不会在触发用户启动的时段到期后（通常在设备注册后 20 分钟）开始。 在设备处于常规使用情况时，这会防止设备进入用户启动自助服务终端模式。
- 在 Mobile@Work for macOS 客户端中，用户加入过程会分步显示。 配置将作为步骤 1 的一部分进行安装。
- 高优先级应用将优先安装。 每个高优先级应用将视为一个步骤。 Packager 应用不视为该步骤的一部分。
- 即使完成用户加入，剩余应用将继续在后台安装。 在设备上初始化安装后，或在设备上实际安装应用后，应用会标记为已安装。
- 在用户加入后，您可以转到设备详细信息页面，以验证推送到每个设备的配置和应用。 有关更多信息，请查看日志。

步骤

1. 使用**创建 Mobile@Work for macOS 配置**，创建 Mobile@Work for macOS 配置。
2. 选择**启用用户入门**选项。
3. 输入以下详细信息：
   - **用户加入超时值** - 输入设备在初始设备设置期间安装应用和配置需要的大概时间。 默认情况下，macOS 设备上的用户加入流程会在 120 秒内超时，您可以根据需要进行修改。
   - **用户登录页面 URL** - 提供在完成加入后向用户显示的登录页面 URL。
4. 单击**下一步**，配置分配设置。
5. 点击**完成**。

创建 Mobile@Work for macOS 脚本配置

您可以创建并将多个 Mobile@Work for macOS 脚本配置分发到设备。 使用此配置，您可以从存储库中选择一个脚本（**管理 > 脚本和文件 > 所有脚本**）分发到 Mobile@Work for macOS。

在使用 Mobile@Work for macOS 1.66 或更高版本的设备上，您可以计划脚本执行。 对于 Mobile@Work for macOS 客户端版本为 1.66 之前的设备，如果您计划在该设备上运行脚本执行，脚本将仅执行一次。 如果 Mobile@Work for macOS 客户端从 1.4 升级到 1.66，所有 macOS 客户端配置将再分发到设备。

先决条件

- 转到**管理 > 脚本和文件 > 所有脚本**上传和管理可用于此配置并分发到设备的脚本。
- 在设备上配置和分发 Mobile@Work for macOS 配置。 否则，Mobile@Work for macOS 脚本配置将处于“错误”状态。

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中键入**工作**，然后单击 **Mobile@Work for macOS 脚本**配置。
4. 命名并描述配置。
5. 在**选择脚本**字段中，输入脚本的名称，以从下拉列表中查找并选择该脚本。
6. 在脚本输入部分中，将显示与脚本关联的脚本输入标签和脚本变量。 如果您需要覆盖，输入替代脚本变量（例如，{$userWorkEmailAddress}）及其替代默认值（例如，john.doe@company.com）。
7. 在脚本执行部分中，选择以下其中一个计划选项：

- 在部署时执行一次
- 重复执行

8. 如果您选择重复执行，指定以下详细信息：
   - 要使用的时区 - 选择设备的当地时间或 UTC 时间。 脚本将按照在此字段中选择的时间执行。
   - 执行开始日期 - 选择开始日期。
   - 执行结束日期 - 选择结束日期（大于或等于开始日期）。
   - 执行脚本 - 选择每天或每周，并输入小时（24 小时制）、分钟和天数（适用）。
9. 单击**下一步**，配置分配设置。
10. 点击**完成**。

完全卸载 Mobile@Work for macOS

如果您在 Mobile@Work for macOS 安装过程中启用**在取消注册时移除应用选项（仅适用于受管应用）**，以及如果从 Ivanti Neurons for MDM 管理门户启动待停用的设备，Mobile@Work for macOS 应用和卸载脚本将从设备中删除。 如要避免进程和脚本在后端运行，请确保在新用户的设备注册过程中或现有用户的停用过程中，从 Ivanti Neurons for MDM 管理门户中取消选择以下选项，以确保卸载脚本运行并将关联进程和脚本从后端删除。

步骤

1. 登录 Ivanti Neurons for MDM 管理员门户。
2. 转到**应用** > **Mobile@Work** > **应用配置** > **应用配置摘要列表** > **Apple 应用设置** > **Apple 应用管理配置设置**。
3. 从**配置设置**页面中，取消选择以下选项：
   - **在取消注册时移除应用（仅适用于受管应用）**。

应用采用 macOS Mobile@Work 的脚本

采用 macOS Mobile@Work 的脚本允许管理员在托管的 macOS 设备上远程部署和运行 shell 脚本。 这有助于自动执行任务、应用修补程序、执行策略并简化配置，而无需用户干预，从而确保大规模的一致和高效设备管理。

必备项：

- 设备必须运行 macOS。
- Mobile@Work for macOS 必须已安装在设备上。
- 确保正确创建、分发和分配 Mobile@Work for macOS 配置。 有关详细信息，请参阅为 macOS 配置创建 Mobile@Work。

> 如果设备没有安装和配置 Mobile@Work 客户端，或者设备平台不支持脚本执行，则无法通过 macOS Mobile@Work 应用脚本。 确保 macOS 客户端处于活动状态，并且您仅选择受支持的 macOS 设备。

步骤

1. 登录 Ivanti Neurons for MDM 管理员门户。
2. 转到**设备**，然后选择要为其执行脚本的 macOS 设备列表。
3. 在**设备**页面中，导航至**操作** > **macOS** > **采用 macOS Mobile@Work 的脚本**。
   采用 macOS Mobile@Work 的脚本窗格出现。
4. 要应用脚本，请在**选择脚本**字段中，输入并选择脚本名称。
   有关创建脚本的详细信息，请参阅所有脚本。

5. 选择**确定**以在设备上执行脚本。

相关主题：

- 管理员 > 脚本和文件 > 所有脚本
- 如何创建配置

10.10.4.43. macOS 软件更新规则配置

通过定义 **macOS 软件更新规则**，管理员可以配置设备的软件更新策略。

适用于：macOS 10.7 至 26.0。

1. 转到配置 > + 添加。
2. 在搜索字段中键入 macOS，然后单击 macOS 软件更新设置配置。
3. 输入配置的名称和描述。
4. 从 **macOS 软件更新规则**中，选择所需配置。
5. 单击下一步。
6. 选择启用此配置选项。
7. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义。
8. 单击完成。

macOS 软件更新规则

管理员可以从规则列表中选择，如下所示：

> 在这些规则应用于设备时，用户无法更改这些设置。

- 允许预发行软件安装。
- 自动：
    - 检查更新
    - 在可用时下载新更新
    - 安装 macOS 更新
    - 从应用商店安装应用更新
    - 安装系统数据文件和安全更新。
- 将应用安装限制为管理员用户。
- 添加软件更新目录 URL 的选项（macOS 11+ 不支持）。

10.10.4.44. 证书首选项

适用于：

- macOS 10.12 至 Ivanti Neurons for MDM 支持的最新发布版本。

在用户的密钥链中识别引用包含在同一配置文件中的证书有效内容的证书首选项。

此配置用于将证书绑定到电子邮件地址或 URL。 在您将证书绑定到电子邮件地址后，邮件应用将其用于该电子邮件帐户。 如果网站的 SSL 证书不受信任，添加证书首选项将确保浏览器在您尝试访问网站时不会通过警告消息提示您。

> 管理员必须持有证书。 有关添加和分发证书的更多信息，请参阅证书配置。

创建证书首选项配置

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中，键入**首选项**，然后单击**证书首选项**配置。
4. 命名并描述配置。
5. 在配置设置部分中，在**名称**字段中，输入请求首选证书的电子邮件 ID 或名称。
6. 在**证书 UUID** 字段中，选择证书。
7. 单击**下一步**，配置分配设置。
8. 点击**完成**。

相关主题：

- 身份首选项
- 证书配置
- 如何创建配置

10.10.4.45. Active Directory (macOS)

适用于：macOS 10.9 或支持的更新版本。

配置高级选项，以将 macOS 设备绑定到 Active Directory (AD) 域，以访问依赖 AD 进行身份验证和保障安全的软件服务。

本部分包含以下主题：

- 创建 Active Directory 配置
- Active Directory 设置

创建 Active Directory 配置

程序

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中键入**隐私**，然后单击 **Active Directory** 配置。
4. 命名并描述配置。
5. 按以下 Active Directory 设置表格所述，输入设置。
6. 单击**下一步**，配置分配设置。
7. 单击**完成**。

Active Directory 设置

设置	采取何种措施
Active Directory 设置 - 基础	
主机名	（必填）输入主机名，这是要加入的 Active Directory 域。
用户名	输入用于加入域的帐户的用户名。
密码	输入用于加入域的帐户的密码。
AD 组织单位	输入已添加加入计算机对象的组织单位 (OU)。
AD 安装样式	选择以下其中一个选项，以表示要使用的网络家庭协议： • AFP • SMB
Active Directory 设置 - 高级	
启用 ADCreateMobileAccountAtLogin 密钥	启用或禁用 ADCreateMobileAccountAtLogin 密钥。 其他选项：在登录时创建移动帐户。
启用 ADWarnUserBeforeCreatingMA 密钥	启用或禁用 ADWarnUserBeforeCreatingMA 密钥。 其他选项：在创建移动帐户前警告用户。
启用 ADForceHomeLocal 密钥	启用或禁用 ADForceHomeLocal 密钥。 其他选项：强制使用本地主目录。
启用 ADUseWindowsUNCPath 密钥	启用或禁用 ADUseWindowsUNCPath 密钥。 其他选项：从 AD 使用 UNC 路径，以派生网络家庭位置。
启用 ADAllowMultiDomainAuth 密钥	启用或禁用 ADAllowMultiDomainAuth 密钥。 其他选项：允许从森林中的任何域进行身份验证。
默认用户 Shell	输入默认用户 Shell，例如 /bin/bash。
将用户 UID 映射到属性	选择以将用户 UID 映射到特定属性。
将用户 GID 映射到属性	选择以将用户 GID 映射到特定属性。
将组 GID 映射到属性	选择以将组 GID 映射到特定属性。
首选域服务器	首选此域服务器。
命名空间约定	选择以下其中一个用户帐户命名约定： • 域（默认） • 森林
数据包签名	选择以下其中一个数据包签名选项： • 允许（默认） • 禁用 • 需要

设置	采取何种措施
数据包加密	选择以下其中一个数据包加密选项： • 允许（默认） • 禁用 • 需要 • SSL
允许按指定 Active Directory 组管理	选择以允许按指定 Active Directory 组管理。 单击**添加**，以添加一个或多个组。
限制动态 DNS	选择以将动态 DNS 更新限制为特定接口（例如 en0、en1 等）。 单击**添加**，以添加一个或多个接口名称。
更改密码间隔	指定需要更改计算机信任帐户密码的频率（天数）。 零值已禁用。

有关更多信息，请查看**如何创建配置**

10.10.4.46. 身份首选项

适用于：macOS 10.12 或支持的更新版本。

在用户的密钥链中识别引用包含在同一配置文件中的身份有效内容的身份首选项。

在 macOS 设备上，身份首选项允许您选择要用于网站的身份（键值对）。 在您将身份首选项（其中包含 URL 和身份）推送到设备后，该首选项将列在**密钥链访问 > 所有项目**（“类型”将是“身份首选项”）中。 下次尝试从 Safari 连接到该 URL 时，设备将显示配置的证书。

Ivanti Neurons for MDM 创建默认系统身份首选项配置，以及 AppStore URL 的有效负载和要使用的证书。

当在 macOS 10.12 及更高版本上使用 Safari 访问 macOS App Catalog 时，用户将获取系统密码提示，以缓存身份证书。 用户需要首次选择“始终允许”，以避免在访问 macOS App Catalog 时出现的后续提示。

当从 macOS 设备访问新浏览器会话中的 macOS App Catalog 时，macOS 版本低于 10.12 的 Safari 和其他浏览器将显示证书和系统密码提示。

创建身份首选项配置

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中，键入**首选项**，然后单击**身份首选项**配置。
4. 命名并描述配置。
5. 在配置设置部分中，在**名称**字段中，输入电子邮件 ID、DNS 主机名，或者唯一识别服务的名称。
6. 在**证书 UUID** 字段中，选择证书。
7. 单击**下一步**，配置分配设置。
8. 点击**完成**。

相关主题：

- 证书首选项
- 如何创建配置

10.10.4.47. Office 365 自动帐户创建 (macOS)

适用于：

- 支持的 macOS 设备。
- 推荐的 Microsoft Office 365 应用版本是 16.13.x 或更高版本。

配置用户信息和选项，以设置所有 Microsoft Office 365 应用的初始配置。

本部分包含以下主题：

- 创建 Office 365 自动帐户创建配置
- Office 365 自动帐户创建设置

创建 Office 365 自动帐户创建配置

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中键入 **Office**，然后单击 **Office 365 自动帐户创建**配置。
4. 命名并描述配置。
5. 按以下 Office 365 自动帐户创建设置表格所述，输入设置。
6. 单击**下一步**，配置分配设置。
7. 单击**完成**。

Office 365 自动帐户创建设置

设置	采取何种措施
Office 激活电子邮件地址	输入用户电子邮件地址。
Office 自动登录	选择以禁止首次运行 Windows。 仅提示用户所需的信息，例如 O365 身份验证。
默认设置为本地打开/保存	选择以将打开/保存面板强制设置为“在我的 Mac 上”，而不是“离线位置”。
在启动时显示新增内容	选择以在启动时显示新增功能信息。
Visual Basic Macro Execution 状态	选择下列选项之一： • 禁用且显示警告 • 禁用且没有警告 • 启用且没有警告
禁用 Visual Basic External Dylibs	选择以禁用 Visual Basic 外部依赖性。
允许 Visual Basic 绑定系统	选择以允许宏使用 DECLARE 绑定到 system() OS API。 此 API 允许宏执行任意外部进程，并在命令行上为其传输任意数据。
禁用 Visual Basic 绑定到 Popen	选择以允许宏使用 DECLARE 绑定到 popen() OS API。 此 API 允许宏执行任意外部进程，并在命令行上为其传输任意数据。
禁用 Visual Basic Mac 脚本	选择以允许宏调用 Apple Script Visual Basic API。

有关更多信息，请查看**如何创建配置**

10.10.4.48. 认证

适用于：

- macOS 10.13 和支持的较新版本。
- Windows 10 和支持的较新版本。

使用身份验证配置，以为云服务和/或桌面登录提供无密码身份验证。 每个设备将仅有一个身份验证配置。

先决条件

- Zero Sign-On 许可证是必填项。
- Ivanti Neurons for MDM 应向 Access 注册（应配置 Access 配置文件）。
- 在配置身份验证配置后，您无法取消注册 Access 配置文件，因为身份验证配置将引用 Access 配置文件。
- 如果 Access 配置文件实施任何更改，将身份验证配置重新分发到 macOS 设备。 对于 Windows 设备，请在新应用中复制并使用新 CLI 值。

创建身份验证配置

Procedure

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中键入**身份验证**，然后单击**身份验证**配置。
4. 命名并描述配置。
5. 从下拉列表中，选择**桌面身份证书**。
6. 选择以下 OS 选项其中 1 个或 2 个选项：
    - macOS
    - Windows
7. 对于 macOS：
    1. 在自定义数据区域中，单击 **+ 添加**，以添加要推送到设备的自定义数据的密钥和字符串值。
    2. 单击**下一步**，配置分配设置。
    3. 单击**完成**。
8. 对于 Windows 10 设备，此配置有助于为适用于 Windows 的 Authenticator MSI 应用生成命令行参数，如下所示：
    1. 单击**完成**，完成身份验证配置。
    2. 在**配置**页面中，查看身份验证配置，以复制显示的命令行文本。 在向 Windows 设备分发身份验证应用时，此文本是必填项。

> 在将身份验证配置应用于 Windows 设备时，该配置会一直处于“等待安装”状态。 您可以忽略此设置，因为不会对功能产生任何影响。

有关更多信息，请查看如何创建配置

10.10.4.49. Apple 应用目录

适用于： iOS 和 macOS

Apple App Catalog 配置会通过 Web 剪辑管理 Apple App Catalog 的访问权限。 从 Ivanti Neurons for MDM 83 版本开始，可从 Go 应用过渡到 Apps@Work 本地体验。 对于新创建的租户，不会在默认情况下为通过 iReg 或客户端安装的 iOS 设备分发 Apps@work Webclip 配置。管理员必须为通过 iReg 或客户端注册的设备手动分发 webclip 配置。

> 即使搜索请求的行参数超过 10，Apps@Work Webclip 搜索结果也仅在 iOS 和 iPad 设备上显示 10 个应用程序。

步骤

管理员可按如下方式编辑此系统定义配置的分配：

1. 转至**配置**。
2. 单击 **Apple App Catalog**。
3. 单击**编辑分发**。
4. 选择下列分配选项之一：
    - 所有设备 - 所有兼容设备将为其发送此配置。
    - 无设备 - 禁用 Apple 应用目录的访问权限或为稍后分配堆栈此配置。
    - 自定义 - 定义将为其发送此配置的特定设备组。

单击**保存**。

10.10.4.50. 托管域

许可证：Silver

托管域配置可用于指定 iOS 8+ 和 visionOS 1.1+ 设备上邮件和 Safari 的可信域。 将配置应用到设备后，配置中未指定的域将在设备的 Mail 和 Safari 中突出显示（不受信任）。 结合使用此配置与**限制配置**，可控制 Safari 中允许的数据下载。

托管的域设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
托管的电子邮件域	单击 **+ 添加**，输入域，如 mycompany.com。
托管的 Web 域	单击 **+ 添加**，输入域，如 mycompany.com。

有关更多信息，请查看**如何创建配置**

10.10.4.51. 通行码配置

您在 Ivanti Neurons for MDM 中设置的第一件事（使用启动向导）是通行码配置。 该配置定义了锁定设备屏幕功能的设置。

通行码设置

设置	采取何种措施
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
允许简单值	限制 PIN 或密码是否包含有序字符或数字。 **对于 iOS、macOS、watchOS 和 Android：**选择此项可允许使用安全系数较低的密码，这些密码中包含重复、升序或降序字符序列。 示例： 1111、1234、abcd。 如果为 Android 设备取消选择这个选项，系统会执行含有复杂 PIN 的通行码。 例如，用户不能配置重复、升序或降序的字符序列。 **对于 Windows 10+：**选择此项以允许使用不太安全的密码，这些密码中包含重复或升序数字序列。 示例：1111、1234。
需要字母数字值	要求通行码至少包含一个字母和一个数字。 **对于 iOS 和 Android**：选择此项以确保密码包含字母和数字。 **对于 Windows 10+：**选择此项以确保使用基于 Microsoft 标准的强密码。
最小通行码长度	从列表中选择一个数字，以设置最小通行码长度。 **对于 Windows 10 桌面**：本地帐户将强制执行最小通行码长度 6。
复杂字符的最小数目	**对于 iOS 和 Android**：从列表中选择一个数字以设置非数字或字母字符的最小数目。 **对于 Windows 10+**：本地账户将强制使用 3 个复杂字符。
最大通行码寿命	输入一个数字用于设置几天后设备用户必须重置通行码。 如果不想设置通行码寿命，将该字段保留为空。
自动锁定	在列表中选择一个区间，用于定义设备自动锁屏前待机的时间。
任何锁定方法	**仅限 Android**。 允许用户选择任何锁定方法，包括图案解锁。 上述通行码设置将不会应用于此设备。
通行码历史记录	输入一个数字，该数字是用户重新使用通行码之前必须输入的唯一通行码个数。 例如，如果您将字段设置为 4，则用户在重新使用第一个通行码之前必须输入了 4 个通行码。
设备锁定的宽限期	从列表中选择一个区间，用于设置锁屏出现和设备用户需要输入通行码解锁设备之间的持续时间。
最大失败尝试次数	从列表中选择一个数字，用于设置重置并擦除设备前，设备用户可连续输入错误通行码的次数。 **警告：**如果用户超过最大密码尝试次数，设备将被擦除 使用此选项时，请格外注意。
（仅 macOS） 启用密码正则表达式 (macOS 14+)	指定与密码匹配的表达式字符串，以确定其是否与策略匹配。
（仅限 macOS） 语言	指定描述的语言。
（仅限 macOS） 说明	描述密码复杂性。 例如，数字、特殊字符、字符串等。

设置	采取何种措施
（仅 macOS） 在下次登录时，强制执行通行码规则	选择以启用 macOS，以提示用户更改密码，从而在用户下次登录时使密码符合密码策略。 默认情况下，此选项未选中。 适用于 macOS 10.13 和更高版本。
（仅 macOS） 登录失败重置延迟（分钟）	指定达到最大登录尝试失败次数后重置登录之前的分钟数。 要启用此字段，请确保已设置最大尝试失败次数。 适用于 macOS 10.10 及更高版本。
SmartLock	**对于 Android 5.0 设备（Android 企业版工作配置文件除外）：** **对于 Android 6.0 及以上版本：** 允许或禁止用户选择智能锁定功能来解锁设备。 智能锁定功能会在某些情况下自动解锁设备，例如用户接近设备、设备在某个位置或设备与信任设备配对时。
指纹解锁	**对于 Android 5.0 设备（Android 企业版工作配置文件除外）：** **对于 Android 6.0 及以上版本：** 允许或禁止用户选择指纹来解锁设备。
锁定屏幕通知（仅适用于 Android 企业版）	**为工作托管设备启用通知（针对设备所有者）** 允许或禁止工作管理设备锁屏上的通知 **为工作配置文件启用未编制的通知** **对于 Android 6.0 及以上版本：** 允许或禁止工作配置文件设备的锁定屏幕上的未编辑通知。 启用此设置后，您将收到通知，但内容显示为“内容被策略隐藏”。您只能从应用查看内容（邮件/推送通知）。

有关更多信息，请查看[如何创建配置]

10.10.4.52. 隐私首选项 (macOS)

适用于：macOS 10.14 或支持的更新版本。

配置允许哪些应用获取对系统服务、系统文件和系统资源的访问权限。 在“系统首选项”>“安全性和隐私”>“隐私”中，此配置控制 macOS 设备上的设置。

创建隐私首选项配置

Procedure

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中键入**隐私**，然后单击**隐私首选项**配置。
4. 命名并描述配置。
5. 导航到其中一个在页面上列出的应用。 有关相关信息，请查看 **Apple 文档**。
    1. 对于 macOS 10.14+，适用于配置的应用和设置包含：
        - 无障碍 - 通过无障碍子系统指定应用的策略。
        - 地址簿 - 指定由 Contacts.app 管理的联系人信息的策略。
        - 指定向其他进程发送受限 AppleEvents 的应用的策略。
        - 日历 - 指定由 Calendar.app 管理的日历信息的策略。
        - 相机 - 系统相机。 无法在配置文件中授予对相机的访问权限；仅可以拒绝。
        - 麦克风 - 系统麦克风。 无法在配置文件中授予对麦克风的访问权限；仅可以拒绝。
        - 照片 - 照片由照片应用在 ~/Pictures/.photoslibrary 中管理。
        - 事件后 - 指定应用使用CoreGraphics API 将 CGEvents 发送到系统事件流的策略。
        - 提醒 - 指定提醒应用管理提醒信息的策略。
        - 系统策略（所有文件）- 允许应用访问所有受保护的文件，其中包含系统管理文件。
        - 系统策略（管理员文件）- 允许应用访问在系统管理中使用的一些文件。
    2. 对于 macOS 10.15+，适用于配置的应用和设置包含：
        - 允许文件提供商应用了解用户何时使用文件提供商管理的文件。
        - 从所有进程监听事件 - 允许应用使用 CoreGraphics 和 HID API 从所有进程监听（接收）CGEvents 和 HID 事件。 无法在配置文件中授予对这些事件的访问权限；仅可以拒绝。 取消选中允许的选项。
        - 访问媒体库 - 允许应用访问 Apple Music、音乐和视频活动及媒体库。
        - 系统显示的屏幕捕获 - 允许应用捕获（读取）系统显示的内容。 无法在配置文件中授予对内容的访问权限；仅可以拒绝。 取消选中允许的选项。
        - 识别向 Apple 发送语音数据 - 允许应用使用系统语音识别设施并向 Apple 发送语音数据。
        - 访问用户桌面文件夹中的文件 - 允许应用访问用户桌面文件夹中的文件。
        - 访问用户文档文件夹中的文件 - 允许应用访问用户文档文件夹中的文件。
        - 访问用户下载文件夹中的文件 - 允许应用访问用户下载文件夹中的文件。
        - 访问网络卷中的文件 - 允许应用访问网络卷中的文件。

- 访问可移除卷中的文件 - 允许应用访问可移除卷中的文件。

6. 对于您想要配置的每个应用，单击**操作 > 添加**。
7. 输入以下标识字典键的值：
   - 标识符 - 设置的名称。 例如："us.zoom.ZoomPresence"。
   - 标示符类型 - 选择绑定 ID 或路径。 例如：“绑定 ID”。
   - 代码要求 - 指定绑定 ID 或路径的值。 例如：“标示符 "us.zoom.ZoomPresence" 和锚 Apple 通用”。
   - 静态代码（真或假）
   - 允许（真或假）
   - 评论
8. 单击**保存**。
9. （可选）在任何应用中，单击**操作 > 删除**，以移除任何现有隐私首选项设置。
10. 单击**下一步**，配置分配设置。
11. 单击**完成**。

有关更多信息，请查看**如何创建配置**

10.10.4.53. 隐私配置

隐私配置定义：

- 是否收集设备上的位置数据，并将其发送给设备管理系统
- 是否允许管理员擦除设备
- 为所有应用采集应用清单还是仅为显示在应用目录中的应用采集应用清单

隐私设置

> 设备擦除操作和在设备上收集所有应用的库存不适用于用户注册的设备。

设置	流程
名称	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
收集位置数据	选择以启用收集位置数据。 在设备页面查看设备位置。 • 对于 iOS 设备，设备显示的位置仅基于网络位置。 • 对于 Android 设备，位置基于网络位置和 GPS 位置（如果可用）。 • 对于 Windows 设备，位置基于在设备签入期间获得的纬度和经度值。 设备上启用位置采集后，每 4 小时就会更新一次当前位置。 设备停用或策略配置被禁用或移除后，位置数据将从设备管理系统中移除。 设备用户可关闭收集设备上的位置数据。
禁用设备擦除操作	选择以防止管理员擦除设备。 对于用户所有的设备（员工所有）可考虑选择此选项。
提示用户启用定位服务 **收集应用清单**	选择此项可允许用户根据需要选择性地启用允许或禁止使用位置服务，包括定位设备、Wi-Fi 和 MTD。 在全托管设备中，如果管理员选择禁用该选项，则可自动授予此权限。 选择**采集应用清单**以采集设备上安装的所有应用的相关信息，无论应用是否显示在 App Catalog 中。 选择**设备上属于 App Catalog 的应用**，从而仅收集安装在设备上且属于该应用目录的应用的相关信息。 选择**应用于设备上的所有应用**，以收集设备上所有应用的信息。 此选项适用于 Windows 10+ 设备。 默认显示并选择以下应用来源类型库存。 • **启用非 App Store 库存** - 适用于通过 MDM 推送的内部应用（通用应用），或由最终用户通过手动解压应用并在本地安装的方式直接安装到设备的内部应用。 • **启用 App Store 库存** - 适用于从 Microsoft Store 手动安装或通过 Apps@work 商店安装的应用。 • **启用系统库存** - 适用于由 Microsoft 报告为与 Windows 10 OS 一同预安装的应用。 • **启用 Win32 清单** - 适用于基于 System32 的应用程序，例如 MSI、EXE、Win32 应用商店应用程序等应用程序，这些应用程序通过 MDM 推送进行安装或由最终用户直接安装在设备上。 （可选）您仅可以选择这些应用来源类型库存，以收集有关选择性应用的信息。 即使您没有选择非 App Store 或 Win32 应用程序清单，MDM 安装的应用程序也会显示在应用程序清单中。 当隐私配置使用默认配置，仅收集 AppCatalog 的应用程序清单时，也会收集 .EXE 清单。 当仅收集 AppCatalog 应用程序的清单时，必须始终收集所有应用程序的清单。 仅当分发至少一个属于全部变体的应用程序时，才会提取应用程序目录中可用的 Modern、MSI 和 EXE 应用程序清单。
Android Enterprise 设备 (7.0+) 的设置 配置下面给定的设置，以便将隐私政策设置为 Android Enterprise 设备。	

设置	流程
组织名称	输入管理设备的组织的名称。
组织颜色	选择应在用户屏幕背景中显示的组织颜色。
短消息	输入一则简短的消息，当用户试图使用被管理员锁定的功能时，系统会显示这条消息。
长消息 **一直隐藏 Go 应用程序屏幕**	输入应在用户单击短消息时显示的长消息。 此消息提供有关对用户限制的更多详细信息。 从列表中选择 True 或 False。 • **True** - 在远程共享期间，Ivanti Go 应用程序屏幕将不可见。 • **False** - 在远程共享期间，Ivanti Go 应用程序屏幕将可见，以提供故障排除方面的任何帮助以及查看文档。

有关更多信息，请查看**如何创建配置**

10.10.4.54. 客户端隐私声明信息

适用于： Android、Android Enterprise 和 iOS 设备或支持的更新版本。

将隐私声明信息分发到 Go 客户端中的用户的配置。 这是可编辑的系统定义配置，以仅配置分发设置。

对用户显示的信息，将包含配置为以下部分配置的详细信息：

- 隐私
  - 收集位置数据
  - 收集应用清单
  - Android 7.0+：
    - 组织名称
    - 组织颜色
    - 短消息
    - 长消息
- 客户端隐私
  - SLC - 重要地点变更定期唤醒设备
  - 基于位置的最小唤醒间隔
  - 启用 MixPanel 状态
- 移动设备管理 - MDM 访问权限（不适用于用户注册的设备）
  - 设备锁定和密码移除
  - 设备擦除
  - 网络信息（电话/SIM 号、MAC 地址）

10.10.4.55. Ivanti Go Client 设置

配置匿名最终用户数据的收集，包括设备和使用信息，以帮助识别产品问题并确保高服务质量。 此设置还启用支持联系人配置选项。

创建 Ivanti Go 客户端设置配置

适用于：

- Mobile@Work for macOS 1.67 或支持的较新版本。
- Go for iOS 3.5.0 或支持的较新版本。
- Mobile@Work for Android 12.9.0.0 或支持的更新版本。
- 选择 Android 124 或支持的更新版本。

步骤

1. 前往**配置** > **添加配置** > **Ivanti Go 客户端配置**。 **创建 Ivanti Go 客户端设置配置**页面出现。
2. 在**名称**框中输入配置名称。
3. 输入配置的**描述**。
4. 在**基于位置的唤醒**下，选择**启用 SLC** 选项。 重要变更地点服务提供功能更加友好的替代方案，以仅在用户的定位频繁变更（最少 15 分钟后（默认时间间隔））时向 Go for iOS 应用提供地点更新。 如果启用此服务，在地点变更时，系统会在后台唤醒 Go 应用并签入。
5. 在**通过分析为客户收集数据**下，选择**启用分析**选项（如果已禁用）。 默认情况下，此选项已启用。
6. 单击**下一步**，配置分配设置。
7. 点击**完成**。

配置支持选项卡设置

适用于：

- Mobile@Work for macOS 1.67 或支持的较新版本。
- Go for iOS 3.5.0 或支持的较新版本。
- Mobile@Work for Android 12.9.0.0 或支持的更新版本。
- 选择 Android 124 或支持的更新版本。

步骤

1. 前往**配置** > **添加配置** > **Ivanti Go 客户端配置**。 **创建 Ivanti Go 客户端设置配置**页面出现。
2. 在**名称**框中输入配置名称。
3. 输入配置的**描述**。
4. 在**平台**选项下，选择相应的平台。
5. 在**配置支持选项卡设置**部分，单击**启用支持选项卡**。

> **启用支持选项卡**字段仅适用于 iOS 设备。

> 您可以启用**支持选项卡**，可启用该选项卡的 Go for iOS 版本为 118.0.0 或以上，Android 版本为 124 或以上。 早期版本的设备将不会显示或支持此功能。

在**支持联系人配置**部分，提供以下详细信息：

- **选项卡名称** - 输入 Ivanti 应用程序导航中显示的选项卡名称。 默认值为“支持”。 （最大长度：10 个字符）
- **最终用户说明** - 输入有关如何使用支持联系人的说明。 （最大长度：40 个字符）
- **添加联系人** - 单击**+添加**以添加联系人。 （联系人最大数目：5）
  - **名称** - 输入联系人姓名。 （最大长度：20 个字符）
  - **电话号码** - 输入有效的电话号码。 （带国家呼叫代码）
- **添加 URL** - 单击 **+添加**以添加 URL。 （URL 最大数目：5）
  - **URL 名称** - 输入 URL 名称。 （最大长度：20 个字符）
  - **URL** - 输入有效的 URL。
- **附加信息** - 输入要在此处显示的任何其他与支持相关的消息。 （最大长度：120 个字符）
- **电子邮件地址** - 输入您可以发送电子邮件寻求支持的电子邮件地址。 （最大长度：40 个字符）

  > 您必须按照 alias@domainname.com 格式输入有效的电子邮件地址。

- **支持票证系统 URL** - 添加了“**提交支持票证**”按钮到 **Ivanti Go for iOS** 和 **Ivanti Go for Android** 应用程序的**支持**选项卡。 启用切换以在支持选项卡上显示按钮，然后在提供的字段中输入相应的 URL，以将用户重定向到支持系统。

  > 此 URL 用于 Ivanti Go **支持选项卡**，以将用户重定向到指定的支持系统。 为了提高安全性，建议使用以 *https://* 开头的 URL，而不是以 *http://* 开头的 URL。

单击**下一步**，配置分配设置。

8. 点击**完成**。

有关详细信息，请参阅配置。

10.10.4.56. Siri 设置

使用 **Siri 设置**配置受监控设备上的 Siri 设置。 此配置可帮助管理员应用基于策略的一致控件，以管理设备访问和使用 Siri 功能的方式。

适用于：

- iOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- macOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- watchOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- visionOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- 受监督的 tvOS 27+，直至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择 **Siri 设置**配置。
3. 根据下表配置各项 **Safari 设置**：

设置	采取何种措施
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
已启用	选中复选框以启用 Siri。 切换**推送至设备**按钮，以在受监控设备上启用 Siri。
允许 Siri AI	选中复选框以启用 **Siri AI** 特定功能。 切换**推送到设备**按钮，以在受监督设备上启用 **Siri AI** 特定功能。
允许用户生成的内容	选中复选框以启用用户生成的内容。 切换**推送至设备**按钮，以在受监控设备上启用用户生成的内容。 此设置不适用于 macOS 和 visionOS 设备。
允许“锁定时”	选中复选框以启用“锁定时”。 切换**推送至设备**按钮，以在受监控设备上启用“锁定时”。 此设置不适用于 macOS 和 visionOS 设备。
强制不雅用语筛选器	选中复选框以启用强制不雅用语筛选器。 切换**推送至设备**按钮，以在受监控设备上启用强制不雅用语筛选器。 此设置不适用于 visionOS 设备。
强制减少敏感内容	选中复选框以强制 Siri 减少敏感内容。 切换**推送到设备**按钮，强制 Siri 减少受监督设备上的敏感内容。

4. 单击**下一步**，配置分配设置。
5. 选择其中一个分发选项来设置 **Safari 设置**配置。 有关配置分发选项的详细信息，请参阅使用配置。
6. 单击**完成**。

10.10.4.57. 服务配置文件配置

服务配置文件配置管理员用于集中管理和部署注册设备上各种系统服务的配置文件。 此外，管理员可以通过在防篡改环境中将文件传递到安全的、特定于服务的目录来确保服务设置保持一致，并防止未经授权的修改。

适用于：macOS 设备

开始之前：

- 您可以用 *ZIP* 文件格式上传各种配置。 有关添加文件的详细信息，请参阅文件。
- 扩展存档中的所有文件都设置为 *-r-r-r- unix* 文件权限。 存档中的任何链接都将仅限于引用服务特定位置内的文件。
- zip 存档中的文件需要反映服务期望从文件系统根目录开始出现的文件夹结构和配置文件。 该服务仅使用声明提供的文件，而忽略其默认目录中的文件。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**服务配置文件**配置。
3. 根据下表配置**服务配置文件**设置：

设置	描述
名称	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
选择文件	输入文件名称。
选择服务类型	从下拉列表中选择一种**服务类型**： • SSHD • SUDO • PAM • CUPS • HTTP_D • BASH • ZSH

4. 单击**下一步**，配置分配设置。
5. 选择其中一个分发选项来设置**服务配置文件**配置。 有关配置分发选项的详细信息，请参阅使用配置。
6. 单击**完成**。

10.10.4.58. 软件更新

适用于：

- iOS 10.3 至 26.0 和 tvOS 12.0 至 26.0 受监督设备
- macOS 设备
- Windows 10+ 设备

创建和分配操作系统更新规则。

本部分包含以下主题：

- 配置 iOS/tvOS 设备的软件更新
- 配置非 DEP 和 DEP macOS 设备的软件更新
- 配置 Windows 设备的软件更新
- 使用声明式设备管理强制执行软件更新

配置 iOS/tvOS 设备的软件更新

步骤

要允许 iOS/tvOS 设备在监控模式下发送操作系统更新：

1. 转至**配置**。
2. 单击 **+添加**
3. 单击**软件更新**。
4. 单击 **iOS/tvOS**，以查看“配置设置”部分。
5. 选择**允许操作系统更新自动在被监控设备上安装**选项。
6. 选择下列选项之一：
    - 更新到最新版本
    - 更新到特定版本 - 例如，将 iOS 版本号输入为 11.3.0。
7. 选择以下其中一个安装操作：
    - 默认
    - 仅下载
    - 立即安装
8. 选择以下时间选项进行更新：
    - 开始时间
    - 结束时间
    - 时区
9. 单击**下一步**。
10. 选择**启用此配置**选项。
11. 选择下列分配选项之一：
    - 所有设备

- 无设备（默认）
- 自定义

12. 单击**完成**。

- 在为 iOS 设备安装 OS 更新的特定版本时，您必须选择对设备可用的版本。 如果您选择无效或不可用的版本，将忽略设备的软件更新。
- 如果设备设有通行码，在 MDM 向设备发送更新后，设备会将更新加入队列，并提示用户输入通行码，才可以开始安装。
- 启用 **iOS 限制**中的 `enforcedSoftwareUpdateDelay` ，确保手动扫描设备上的软件更新时不会删除此配置下载的特定版本。

配置非 DEP 和 DEP macOS 设备的软件更新

设备注册配置文件是 Apple Business Manager 的一部分，其支持客户批量购买设备，并在激活过程中自动将这些设备注册到 MDM。 有关详细信息，请参阅**设备注册**。

以下步骤可帮助您将操作系统更新发送到非 DEP macOS 设备和 DEP macOS 设备。

步骤

1. 转至**配置**。
2. 单击 **+添加**
3. 单击**软件更新**。
4. 单击 **macOS**，以查看“配置设置”部分。
5. 选择**启用 macOS 软件更新**选项。
6. 选择设备的更新类型。 对于这些更新，您也可以选择不需要重启的更新。
   - 操作系统更新
   - 关键更新
   - 配置数据更新
   - 固件更新
   - 非重要更新

     > 通过启用**启用非重要更新**，管理员可以管理（安装/计划）非重要 macOS 更新。 对于现有租户，默认禁用此选项，并且需要管理员明确启用发布更新（如果需要）。

     > 在 **OS 更新**中，管理员可将设备更新为 macOS 的特定版本。

     > 所有 macOS 更新可以使用以下操作配置：

     - 默认
     - 仅通知
     - 稍后安装
     - 安装强制重新启动
     - 仅下载
     - 立即安装
   -

可能的值 - 低、高

默认 - 低

优先级

- 最大用户延迟
  可能的值 - 整数
  只有选中“稍后安装”选项时才支持。

7. 选择以下时间选项进行更新：
   - 开始时间
   - 结束时间
   - 时区
8. 单击**下一步**。
9. 选择**启用此配置**选项。
10. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义
11. 单击**完成**。

配置 Windows 设备的软件更新

步骤

要配置 Windows 安装更新计划：

1. 转至**配置**。
2. 单击 **+添加**
3. 单击**软件更新**。
4. 单击 **Windows** 以便查看“配置设置”部分。
5. 根据 Windows 设备的版本，输入以下选项。
6. 单击**下一步**。
7. 选择**启用此配置**选项。
8. 选择下列分配选项之一：
   - 所有设备
   - 无设备（默认）
   - 自定义

单击**完成**。

Windows 10+ 设备的软件更新

- 更新来源 - 选择以下来源之一：
  - Enterprise WSUS

- Microsoft Update 和/或 Enterprise WSUS

驱动程序更新源

- 功能更新源
- 其他更新源
- 质量更新源
- Enterprise WSUS 服务器的 URL
- 备用内联网 Microsoft 更新服务器
- 允许"受信任的发布商"进行更新 - 将更新来源限制到仅受信任的发布商。
- 自动更新策略 - 从下拉菜单中选择一个选项。
- 计划安装日 - 设置更新频率。
- 计划安装时间 - 选择更新的安装时间。
- 允许通过按流量计费的连接自动下载更新 - 启用或禁用选项。
- 不允许更新延迟策略会对 Windows Update 进行扫描 - 启用或禁用选项。
- 约定重新启动截止日期 - 选择重新启动截止日期的天数。
- 暂停约定重新启动截止日期 - 选择暂停约定重新启动截止日期的天数。
- 约定重新启动迁移计划 - 选择重新启动迁移计划的天数。
- 更新/填充空内容 URL。
- MO 应用下载限制 - 选择以下其中一个选项：
  - 请勿忽略应用及其更新的 MO 下载限制
  - 忽略应用及其更新的 MO 下载限制（允许无限制下载）
- MO 更新下载限制 - 选择以下其中一个选项：
  - 请勿忽略 OS 更新的 MO 下载限制
  - 忽略 OS 更新的 MO 下载限制（允许无限制下载）
- 管理预览版本 - 选择以下其中一个选项：
  - 禁用预览版本
  - 在下一个版本公开后，禁用预览版本
  - 启用预览版本
- 更新的自动重新启动警告通知计划 - 选择自动重新启动警告通知所需的分钟数。
- 重新启动警告提醒 - 选择设置重新启动警告提醒的小时数。
- 自动更新计划 - 选择自动更新的频率。
- 更新的自动重新启动通知 - 开启更新的自动重新启动通知。
- 产品版本 - 输入 Windows 更新版本页面（URL：aka.ms/WindowsTargetVersioninfo）上列出的产品版本。 例如，"Windows 11"或"11"或"Windows 10"。
- 目标发布版本 - 在 Windows 更新版本页面上输入目标发布版本。
- 活动时段开始 - 如果启用此选项，则在活动时段内完成的更新之后，电脑不会自动重新启动。 在非活动时段，则电脑会尝试重新启动。
- 活动时段结束 - 如果启用此选项，则在活动时段内完成的更新之后，电脑不会自动重新启动。 在非活动时段，则电脑会尝试重新启动。
- 活动时段最大范围 - 启用此选项可指定从开始时间起用户可设置活动时段的最大小时数。

- 活动时段内无更新通知 – 更新通知选项如下。
  - 默认 Windows 更新通知
  - 关闭所有通知，并排除重新启动警告
  - 关闭所有通知，并包含重新启动警告
- 禁用驱动程序更新 - 启用此选项可排除具有 Windows 质量更新的驱动程序。 如果禁用或不配置此选项，则 Windows 更新会包含分类属于驱动程序的更新。
- 质量更新截止时间 - 质量更新自动安装到设备前等待的天数，与活动时段无关。
- 质量更新截止宽限期 – 从更新安装到质量更新自动重新启动所间隔的最少天数。
- 功能更新截止时间 – 功能更新自动部署到设备前等待的天数，与活动时段无关。
- 功能更新截止宽限期 – 功能更新自动部署到设备前等待的最少天数，与活动时段无关。
- 在宽限期结束前不自动重新启动 - 启用后，即使更新已准备好重新启动，设备仍不会在活动时段之外自动重新启动，会一直等到截止时间和宽限期以后。 禁用后，如果在截止时间以前更新已准备好重新启动，则设备可能会在活动时段外尝试自动重新启动。

Windows 10.0.14393 之前版本设备的软件更新

如果在设备上禁用遥测限制，以下设置将无法工作：

- 暂停升级/更新 - 打开以便将更改延迟到稍后的日期
- 延迟更新 - 选择以便最多延迟 4 周
- 延迟更新 - 开启延迟更新
- 延迟更新 - 选择以便最多延迟 8 个月

Windows 10.0.14393+ 设备的软件更新

- 安装更新的分支 - 允许 IT 管理员设置设备从哪个分支接收更新。 “安装更新的分支”字段包含以下选项：
  - Windows Insider 版本 – 快
  - Windows Insider 版本 – 慢
  - 发布 Windows Insider 版本
  - 半年通道（目标）
  - 半年通道
  - 仅发布质量更新预览
  - Canary Channel

功能更新（升级）- 仅在 Windows Professional、Windows Enterprise 和 Windows Education 中受支持。

  - 暂停更新
  - 延迟更新 - 选择以便最多延迟 180 天。

质量更新（更新）- 仅在 Windows Professional、Windows Enterprise 和 Windows Education 中受支持。

  - 暂停更新
  - 延迟更新 - 选择以便最多延迟 30 天。

Windows 10.0.17083+ 设备的软件更新

- 功能更新：
  - 功能更新卸载期限 - 选择卸载功能更新所需的天数。

Windows 10.0.17763+ 设备的软件更新

- 按用户禁用“暂停更新”访问权限
- 按用户禁用 UXWU 访问权限（Windows 更新扫描、下载和安装）
- 更新通知级别 - 选择以下其中一个选项：
  - 使用默认 Windows 更新通知
  - 关闭所有通知，并排除重新启动警告
  - 关闭所有通知，并包含重新启动警告
- 功能更新：
  - 更新安装的自动重新启动之前的截止日期 - 选择更新安装的自动重新启动之前截止日期的天数。
  - 约定重新启动截止日期 - 选择约定重新启动截止日期的天数。
  - 暂停约定重新启动截止日期 - 选择暂停约定重新启动截止日期的天数。
  - 约定重新启动迁移计划 - 选择重新启动迁移计划的天数。

使用 DDM 强制执行软件更新

管理员可以使用 DDM 在 iOS、macOS 和 iPadOS 设备上强制安装软件更新。

支持：

- iOS 17+
- iPadOS 17+
- macOS 14+

步骤

1. 从“配置”部分创建**软件更新强制执行**配置。
2. 执行强制签入以确保在设备上安装“软件更新强制执行”配置。

打开设备时，系统会显示有关所需软件更新的通知，其中包含版本号、截止日期等详细信息。

> 如果不想强制执行软件更新，则需要将配置分发选项设置为**无**。

分发软件更新强制执行配置的谓词

1. 创建“软件更新强制执行”配置。
2. 将使用谓词激活切换为“打开”，然后使用 + 按钮来包含谓词（根据需要）。



要编辑或删除谓词，请转到**管理员** > **Apple** > **谓词**。 在此页面中可以找到可用的谓词列表。 点击**编辑**可更改现有谓词并保存。 同样，要删除现有谓词，请选择相关谓词并点击**删除**。

> 如果谓词已关联任何配置，则无法删除谓词。

10.10.4.59. 软件更新设置配置

Ivanti Neurons for MDM 允许创建软件更新强制执行设置，并针对更新节奏和延迟为最终用户定义更新的行为。

适用于：

- iOS 18.0 受监管设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- macOS 15.0 受监管设备至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**软件更新设置**配置。
3. 根据下表配置**软件更新设置**的设置：

设置	描述
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
受监管 iOS 18+ 和 macOS15+	
测试版注册 计划注册（可选） **受监管 iOS 18+ 和受监管 macOS15+**	 选择下列选项之一： • **允许**：用户可以注册与其登录的 Apple 帐户相关的任何适用测试版程序。 • **始终开启**：使用组织指定的测试版程序，用户无法使用登录的 Apple 帐户注册测试版程序。 **提供程序** - 通过“提供程序”，可强制执行所需的程序。 强制执行时，您可以为 iOS 和 macOS 设备设置所需的版本。 **需要程序** - 设备会自动注册此测试版程序。 • **始终关闭**：该设备不允许注册任何测试版程序。 如果已注册，系统会从任何测试版程序中删除该设备。
通知 自动操作 下载 安装操作系统更新	选中**通知**和**显示所有软件更新强制执行通知**复选框，以便在用户设备中显示所有软件更新强制执行通知。 如果仅选中**通知**复选框，设备将在强制截止日期前一小时显示单个强制通知。 如果未选中任一复选框，设备将显示触发的通知，以显示用户设备中的所有软件更新执行通知。 选择下列选项之一： • **允许**：用户可以打开或关闭自动下载。 • **始终开启**：用户的自动下载始终“开启”。 • **始终关闭**：用户的自动下载始终“关闭”。 选择下列选项之一： • **允许**：用户可以打开或关闭自动安装操作系统更新。 • **始终开启**：用户的自动安装操作系统更新始终“开启”。 • **始终关闭**：用户的自动安装操作系统更新始终“关闭”。
背景安全改进	
背景安全改进	选中**背景安全改进**复选框以控制更新的安装和回滚。 选择以下选项： • **启用**：如果选中，它可为用户提供**背景安全改进**安装。 • **启用回滚**：如果选中，它可向用户提供**背景安全改进**回滚。
iOS 18+ 受监管设备	
节奏建议	选择以下选项之一，以此指定在有多个更新可用时如何向用户显示软件更新： • **全部**：显示所有软件更新版本。

设置	描述
	• **最早**：仅显示最早（编号较低）的软件更新版本。 • **最新**：仅显示最新（编号最高）的软件更新版本。
延迟	可以选择推迟所有受监管设备的软件更新。 无法推迟**背景安全改进**。
合并周期（以天为单位） **macOS 15+ 受监管设备** 允许标准用户操作系统更新	设置推迟设备上主要或次要系统更新的天数。 配置完成后，主要或次要软件更新将在发布后指定的天数显示。 可以设置 1 到 90 之间的任意值。 选中**允许标准用户操作系统更新**复选框，以此允许用户执行操作系统更新。 选中**允许标准用户执行主要和次要软件更新**复选框，以此允许标准用户执行次要和主要软件更新。 如果不选中该复选框，则只有管理员可以执行次要和主要软件更新。
延迟	
主要更新周期（以天为单位） 次要更新周期（以天为单位）	设置推迟设备上主要操作系统软件更新的天数。 配置完成后，主要软件更新将在发布后指定的天数显示。 可以设置 1 到 90 之间的任意值。 设置推迟设备上次要操作系统软件更新的天数。 配置完成后，主要软件更新将在发布后指定的天数显示。 可以设置 1 到 90 之间的任意值。
系统更新周期（以天为单位）	设置推迟设备上系统操作系统更新的天数。 配置完成后，主要软件更新将在发布后指定的天数显示。 可以设置 1 到 90 之间的任意值。
自动操作 安装安全性更新	 选择下列选项之一： • **允许**：用户可以打开或关闭安全性更新的安装。 • **始终开启**：用户的安全性更新安装始终“开启”。 • **始终关闭**：用户的安全性更新安装始终“关闭”。

4. 单击**下一步**，配置分配设置。
5. 选择其中一个分发选项来设置**软件更新设置**配置。 有关配置分发选项的详细信息，请参阅使用配置。
6. 单击**完成**。

10.10.4.60. 安全首选项配置

通过安全首选项配置，管理员可以管理和控制用户在设备上对防火墙设置、锁定消息和密码更改实施的任何更改。

适用于：macOS 10.10+

Procedure

1. 转到配置 > + 添加。
2. 在搜索字段中，键入安全，然后单击安全首选项配置。
3. 输入配置的名称和描述。
4. 选择所需的配置：
    - 禁用对防火墙设置实施更改
    - 禁用对锁定消息实施更改
    - 禁用对密码实施更改
5. 单击下一步。
6. 选择启用此配置选项。
7. 选择以下其中一个渠道选项，以应用配置：
    - 设备渠道（最常见）
    - 用户渠道（当前注册用户）
8. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义。
9. 单击完成。

10.10.4.61. 时间服务器

适用于：macOS 10.12.4 或支持的更新版本。

创建时间服务器配置，以允许设备连接到自定义时间服务器。

创建时间服务器配置

步骤

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中，键入**时间**，然后单击**时间服务器**配置。
4. 输入名称并描述配置。
5. 指定 **NTP 服务器**。
6. 指定 Olson 时区 ID 格式的**时区**字符串（例如 Pacific/Midway）。 要获取奥尔森时区模式，请在管理员的 macOS 设备上运行 `“/usr/sbin/systemsetup -listtimezones` " 命令。
7. 单击**下一步**，配置分配设置。
8. 单击**完成**。

有关更多信息，请查看如何创建配置

10.10.4.62. Web 内容筛选

许可证：Silver

网络内容筛选器配置限制了 iOS 7+、macOS 10.15+ 和 visionOS 1.1+ 设备的 Web 访问。

Web 内容筛选器设置

设置	采取何种措施
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
允许的网站	**限制的成人内容：**如果您想基于 iOS 自动筛选结果阻止对网站的访问，则选择该选项。 这些具有高精确度的筛选器会尝试阻止带有不当内容的网站。 **仅指定网站：**如果您想手动将可访问网站加入列表，则选择该选项。 **插件（仅适合 iOS8 受监管版和 macOS 10.15+）：**选择此选项可使用第三方插件。
允许的 URL	该选项仅在您选择“限制成人内容”之后可用。 输入允许的 URL。 每个 URL 必须以下列其中一项内容开始： • http:// • https:// 如果您希望同时允许同一网站的 http:// 和 https:// 内容，则包括两个独立的 URL。 初始字符与给定允许的 URL 相匹配的所有 URL 均可访问。 示例：http://www.someCompanySite.com 允许访问以下网址： • http://www.someCompanySite.com • http://www.someCompanySite.com/jobs 即使 iOS 自动筛选阻止，仍然可访问这些 URL。
使用拒绝列表 URL	该选项仅在您选择“限制成人内容”之后可用。 输入已加入阻止列表的 URL。 每个 URL 必须以下列其中一项内容开始： • http:// • https:// 如果您希望同时阻止同一网站的 http:// 和 https:// 内容，则包括的每个 URL 成一行。 阻止初始字符与指定已加入阻止列表的 URL 匹配的所有 URL。 示例：http://www.someCompanySite.com 阻止访问以下网址： • http://www.someCompanySite.com • http://www.someCompanySite.com/jobs 即使 iOS 自动筛选器允许访问，仍然可阻止这些 URL。
已加入允许列表的书签	该选项仅在您选择“仅特定网站”之后可用。 可选择将文件夹输入应添加至 Safari 的书签中。 示例： /销售/产品/ 如果不存在，则将书签添加到默认书签目录。
筛选器名称	该选项仅在您选择“插件”之后可用。 输入将显示的文本，以识别此筛选器。
标识符	该选项仅在您选择“插件”之后可用。 输入提供筛选服务的插件的捆绑软件 ID。
服务地址	该选项仅在您选择“插件”之后可用。 可选：输入插件有必要使用的任何服务器地址。 请参阅插件的文档以确定该值是否必要。

设置	采取何种措施
组织	该选项仅在您选择“插件”之后可用。 可选：输入插件所需的任何组织字符串。 请参阅插件的文档以确定该值是否必要。
用户名	该选项仅在您选择“插件”之后可用。 可选：输入插件服务所需的任何用户名。 请参阅插件的文档以确定该值是否必要。
密码	该选项仅在您选择“插件”之后可用。 可选：输入插件服务所需的任何密码。 请参阅插件的文档以确定该值是否必要。
证书	该选项仅在您选择“插件”之后可用。 可选：输入插件服务所需的任何证书以验证用户身份。 请参阅插件的文档以确定该值是否必要。
筛选器 Webkit 流量	该选项仅在您选择“插件”之后可用。 选择此项可在筛选器中包含 Webkit 流量。
筛选器套接字流量	该选项仅在您选择“插件”之后可用。 选择此项可在筛选器中包含套接字流量。
自定义数据	该选项仅在您选择“插件”之后可用。 可选：添加插件服务所需的任何密钥/值对。 请参阅插件的文档以确定该值是否必要。

有关更多信息，请查看**如何创建配置**。

10.10.4.63. Windows 防火墙

通过 Windows 防火墙配置，您可以配置 Windows 防火墙配置文件设置，以及在设备上强制执行的自定义规则目标集。 此配置可用于管理非域设备，并降低所有连接到企业网络的系统内部的网络安全威胁。

配置 Windows 防火墙配置

步骤

1. 转到**配置 > + 添加**。
2. 选择**防火墙**配置。
3. 单击 **Windows** 图标。
4. 输入配置的名称。
5. 输入防火墙配置描述。
6. 在“配置设置”部分中，按照下表所述指定剩余设置。

设置	流程
配置文件	
启用	将开关滑到开启，以启用配置文件。
类型	显示配置文件的类型。 示例：域。
默认入站操作	选择应对入站流量执行默认操作的选项。 **允许**：允许流量 **阻止**：阻止流量。
默认出站操作	选择应对出站流量执行的默认操作。 **允许**：允许流量 **阻止**：阻止流量。

7. 点击 **+添加**可添加规则并配置以下设置：

设置	流程
规则	
打开	滑动开关，以启用配置文件。
规则名称	输入可识别此规则的名称。
说明	输入阐明此规则目的的描述。
方向	选择应用规则的流量方向： • **入站**：适合入站流量 • **出站**：适合出站流量 • **双向**：双向。
操作	选择执行的操作 • **允许**：允许流量 • **阻止**：阻止流量。
配置文件	选择应用规则的配置文件： • **全部** • **域** • **私人** • **公开**
应用程序	键入软件包系列名称 (PFN) 或可执行应用的完整路径。
协议	选择以下任何应用规则的协议： • **TCP** • **UDP** • **ICMP**
本地地址范围	键入本地 IPv4/IPv6 地址范围或子网掩码。
本地端口范围	键入本地端口或端口范围的逗号分隔列表。 示例：20,50,100-120。
远程地址范围	键入远程 IPv4/IPv6 地址范围或子网掩码。
远程端口范围	键入本地端口或端口范围的逗号分隔列表。 示例：20,50,100-120。
接口类型	选择以下任何接口类型选项： • **全部** • **远程访问** • **无线** • **LAN**

设置	流程
	• **手机宽带** 如果没有选择任何界面类型选项，将应用默认选项**所有**。

8. 单击**下一步**。
9. 选择下列分配选项之一：
   - 所有设备
   - 无设备（默认）
   - 自定义
10. 单击**完成**。

10.10.4.64. Windows 信息保护

许可证：Gold

适用于：Windows 10+

Windows 信息保护 (WIP) 配置会定义 WIP 设置，以保护企业数据。 此配置可以应用到在管理中登记的设备。 您也可以查看 WIP 详细信息，以了解有关该设备概述页面的配置设备。

设置 Windows 的 Windows 信息保护

步骤

1. 转到**配置 > + 添加**。
2. 选择 **Windows 信息保护**配置。
3. 输入配置的名称。
4. 输入描述。
5. 在"配置设置"部分中，按照下表所述指定剩余设置。
6. 点击**下一步**。
7. 为此配置选择一个分发方案。

类别	设置	采取何种措施
	名称	输入用于识别此配置的名称。
	说明	输入阐明此配置目的的说明。
企业信息	**所有版本（Windows 10+）**	
	受保护的域名	指定配置数据保护策略的身份列表。 与这些身份相关的电子邮件和其他数据将视为企业数据并受到保护。 • 这是一个由 | 隔开的域列表，其中列表中的第一个域会出于 Windows UI 目的而视为主要身份。 • 例如："domain1.com|domain2.co.uk"
	网络域名	指定包含企业边界的域列表。 从这些域发送到设备的数据将视为企业数据并受到保护。 • 这些位置将视为企业待共享数据的安全目的地。 • 这是由逗号隔开的域列表。 • 例如："mail.domain3.com, domain4.com"
	云资源	包含托管在云中需要保护的企业资源域列表。 这些资源的连接应视为企业数据。 使用括号中的可选代理地址指定一个或多个域名。 • 例如："domainname1.com，domainname2（10.0.0.1）"。 • 如果代理与云资源配对，则云资源的流量将通过指定代理服务器（在端口 80 上）路由至企业网络。 • 在此字段中指定的所有代理地址也应在以下内部代理服务器字段中输入。
	IP 范围	设置在企业网络中定义计算机的企业 IP 范围。 来自这些计算机的数据将视为企业的一部分，并受到保护。 这些位置将视为企业待共享数据的安全目的地。 这是由逗号隔开的 IPv4 和 IPv6 范围列表。 • 这是由逗号隔开的 IPv4 和 IPv6 范围列表。 • 在客户端必须接受配置列表，且不采用探试法尝试查找其他子网时，选择 **IP 范围具有权威性**选项。
	中性资源	指定可用于工作或个人资源的域名列表。
	代理服务器	指定由逗号隔开的代理服务器列表。 此列表上的任何服务器不应视为企业资产。 • 例如："157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59"。 • 在客户端必须接受代理配置列表并尝试不检测其他工作代理时，选择**代理服务器具有权威性**选项。
	内部代理服务器	指定由逗号隔开的内部代理服务器列表。 • 例如："157.54.14.28, 157.54.11.118, 10.202.14.167, 157.53.14.163, 157.69.210.59"。 • 这些代理由管理员配置，以连接到 Internet 上的特定资源。 这些内容视为企业网络位置。 代理仅在配置 EnterpriseCloudResources 时利用，以将流

类别	设置	采取何种措施
		量通过这些代理强制到匹配的云资源。
数据保护	**所有版本（Windows 10+）**	
	执行级别	选择以下其中一个实施级别： • 关闭 - 无保护（此前加密的数据将取消加密）。 • 静默 - 在数据受保护后，在设备上加密数据并审计活动。 不会提示用户考虑有关任何负面数据/应用信息。 • 覆盖 - 与静默模式相似。 此外，如果正在错误使用应用或数据，则系统会提示用户继续，或取消用户目前正在执行的操作。 • 阻止 - 与静默模式相似。 如果正在错误使用应用或数据，用户目前正在执行的操作将会被阻止，并为用户显示警告以及阻止操作的原因。 除了在关闭模式中，任何不应使用企业数据或资源的数据或应用将会记录在设备上。 该数据将会使用其他配置服务提供商 (CSP) 从设备中移除。
	数据恢复证书	指定可用于加密文件数据恢复的恢复证书。 • 这与用于加密文件系统 (EFS) 的数据恢复代理 (DRA) 证书完全相同。 但此证书会通过 MDM 交付，而不是群组策略。 您也可以从以下一个或多个选项选择： • 允许用户解密 • 取消注册时撤消 • 显示 EDP 图标 • 锁定下需要保护（仅限 Windows 10 Mobile）
RMS	**所有版本（Windows 10+）**	
	允许 Azure RMS	指定是否允许 Azure Rights Management (Azure RMS) 加密或 WIP。
	RMS 模板 ID	指定用于 RMS 加密的 TemplateID GUID。 RMS 模板允许管理员配置有关谁能够访问 RMS 保护的文件及访问频率。
应用程序控制	**所有版本（Windows 10+）**	
	指定使用 WIP 值在**应用 > App Catalog** 页面中构建的应用集合。 使用以下参数集，指定应用的规则定义：	
	应用类型	选择以下应用程序类型之一： • 发布者/PFN 等于 - 适用于支持 PFN 的 Windows 10+。 • EXE/Win32 等于 - 仅适用于 Windows 桌面。
	应用标识符	从显示的选项中选择应用，以将其添加到应用标识符。 您也可以单击**查找应用**。

类别	设置	采取何种措施
	应用说明	为应用输入描述。

10.10.4.65. Windows 限制

Windows 限制可决定在 Windows 10+ 设备上启用哪些功能。

Windows 限制设置

类别	设置	采取何种措施
	名称	输入用于识别此配置的名称。
	说明	输入阐明此配置目的的说明。
设备能力	**所有版本（Windows 10+）**	
	禁用 Wi-Fi 卸载	选择阻止设备访问兼容网络，以传输专用于授权无线网络的数据。
	禁用 Internet 共享	选择以阻止设备通过其他无线设备访问互联网。
	禁用位置	选择禁用定位服务。
	禁用手机网络数据漫游	选择在设备处于蜂窝模式时禁用数据漫游。
	禁用蓝牙	选择以阻止设备建立蓝牙连接。
	在漫游或手机网络中禁用 VPN	选择以阻止设备未处于 WiFi 模式时建立 VPN 连接。
	禁用手动配置 Wi-Fi	选择此项可防止用户在设备上手动配置 Wi-Fi 设置。
	禁用 Wi-Fi	选择此项可允许或拒绝 WiFi 连接。
遥测 - 允许设备发送诊断和使用状况遥测数据。	**仅限 Windows 10**	
	遥测等级	选择以下数据报告的遥测级别之一： • **安全** - 发送有关连接的用户体验、遥测组件设置、恶意软件删除工具和 Windows Defender 的信息。 • **基本** - 发送基本设备信息，包括质量相关数据、应用程序兼容性、应用程序使用数据和安全级别的数据。 • **增强** - 发送更多信息，包括 Windows、Windows Server、System Center 和应用程序的使用和性能。 还包括高级可靠性数据，以及基本和安全级别的数据。 • **完整（默认）** - 发送用来识别和帮助解决问题的所有数据，以及安全、基本和增强级别的数据。
数据丢失防护 (DLP)	**所有版本（Windows 10+）**	
	禁用照相机	选择以阻止最终用户使用照相机应用。
	禁用内存卡 (SD) 访问	选择阻止设备访问内存卡。
	禁用屏幕捕获（仅限桌面）	选择此项可防止使用设备内的屏幕捕获应用程序来捕获屏幕。
	禁用 USB 大容量存储（仅限 HoloLens）	选择此项可阻止 HoloLens 访问大容量存储设备。
数据使用情况	**Windows 10+**	

类别	设置	采取何种措施
Defender 设备保护	3G 连接成本 4G 连接成本 **Windows 10+** 禁用 Defender 实时监控功能 **Windows 10+** 禁用基于虚拟化的安全性 (VBS)	选择下列选项之一： • **无限制** - 连接是无限制的，不受资费和容量限制的限制。 • **固定** - 在某个数据限制之后，连接受到资费和容量限制的限制。 • **可变** - 连接按字节计费。 选择以禁用 Windows Defender 实时监控功能 选择以防止基于虚拟化的安全性提供对安全服务的支持。
	基于虚拟化安全的证书保护 平台安全级别（需要平台安全功能）	选择下列选项之一： • **已禁用** - 禁用基于虚拟化安全的证书保护。 • **启用 UEFI 锁定** - 通过统一可扩展固件接口 (UEFI) 锁定，启用基于虚拟化安全的证书保护。 • **启用但无锁定** - 启用基于虚拟化安全的证书保护，无需 UEFI 锁定。 选择下列选项之一： • **具有安全启动的 VBS** - 选择此选项可通过安全启动启用基于虚拟化的安全性。 • **具有安全启动和直接内存访问的 VBS** - 选择此选项可通过安全启动和直接内存访问 (DMA) 启用基于虚拟化的安全性。
隐私	**Windows 10+**	
	禁用广告 ID	选择以禁用广告 ID。
Windows 和应用程序	禁用通过应用程序/操作系统发布活动源 **所有版本（Windows 10+）** 禁用 Microsoft 服务账户，而不是电子邮件 禁用非 Microsoft 账户 禁用 Cortana 个人助手 禁用基于位置的搜索	选择以阻止应用程序/操作系统发布到活动源。 选择以阻止最终用户使用 Microsoft 帐户对非电子邮件服务进行身份验证。 选择以阻止最终用户使用非 Microsoft 帐户配置电子邮件。 选择以阻止最终用户访问 Microsoft 个人助理。 选择以阻止搜索利用设备位置。
	禁用开发商解锁	选择以阻止最终用户启用应用分载。 在 MDM 中注册设备时，默认模式会在 SideLoad 中启用。

类别	设置	采取何种措施
	仅限 11+ 支持的版本	
	任务栏中的团队聊天图标的配置 **仅限 Windows 10+ 支持的版本**	选择下列选项之一： • **显示**：任务栏会默认显示聊天图标。 用户可以在设置中显示或隐藏。 • **隐藏**：聊天图标默认隐藏。 用户可以在设置中显示或隐藏。 • **禁用**：聊天图标未显示，用户无法在设置中显示或隐藏。 • **未配置**：聊天图标的行为以 Windows 版本的默认设置为准。 更改会在 Windows 设备重新启动后生效。
	禁止从 Microsoft Store 自动更新应用程序	选择以防止从 Microsoft Store 自动更新应用程序。
	禁止从 Microsoft Store 启动预先安装或已下载的所有应用程序 让应用程序在后台运行	选择以防止最终用户从 Microsoft Store 启动所有预安装或下载的应用程序。仅支持 Windows 企业版和教育版。 选择下列选项之一： • **用户控制**：允许用户在后台控制应用的运行。 • **强制允许**：允许在后台运行应用。 • **强制拒绝**：阻止在后台运行应用。
其他限制	**所有版本（Windows 10+）**	
	禁用从 UEM 取消注册以及删除工作场所帐号的功能。	选择阻止最终用户从 UEM 中取消注册并删除公司帐号图像。
	禁止用户设置设备锁定宽限期（仅限 HoloLens）。 **仅限 Windows 10+ 支持的版本**	选择此项可防止用户设置设备锁定宽限期。
	禁用用户使用控制面板和硬件密钥组合对设备执行恢复出厂设置	选择以防止最终用户设置设备锁定宽限期。
	要求用户在设备设置期间连接到网络（需要 Autopilot 配置文件） **仅限 Windows 11+ 支持的版本**	选择此选项启用 TenantLockdown，锁定使用 Autopilot 功能注册的所有 Windows 设备。
	禁止用户通过用户界面对 eSIM 进行更改。	选择此选项可限制用户对 eSIM 配置文件进行任何更改。

10.10.4.66. Windows 桌面限制

适用于：Windows 10 桌面

本部分包含以下主题：

- 配置 Windows 桌面限制
- 创建可移动存储设备的允许列表

通过限制用户在设备上访问以下区域，管理员可以控制在托管 Windows 10 桌面设备上的 OS 信息：

- 控制面板
- 任务管理器
- 文件资源管理器
- 注册表编辑器

以上功能可让用户对设备进行大量更改。 使用此功能，管理员可以限制对这些系统级控制的访问权限，从而保障访问。

此功能需要 Bridge。 请查看 Ivanti Bridge，以了解详细信息。

配置 Windows 桌面限制

步骤

1. 转到**配置 > + 添加**。
2. 选择 **Windows 桌面限制**配置。
3. 输入配置的名称。
4. 输入描述。
5. 在"配置设置"部分中，按照下表描述指定剩余设置。

设置	采取何种措施
任务管理器	对于应拒绝访问的设置，选择**拒绝访问**复选框。
控制面板	
注册表编辑器	
文件资源管理器	选择**限制功能**复选框，以限制文件浏览的功能。 示例：移除映射网络驱动器。 单击提供的链接，以查看限制功能的列表。
可移动存储	
可移动存储的访问模式	• **限制读取访问权限**：这会阻止任何访问，并且是最具有限制性的配置。 • **限制写入访问权限**：这允许有限访问，但阻止未经授权地移除数据，或将病毒等 添加到设备。

6. 单击**下一步**。
7. 选择下列分配选项之一：

- 所有设备

- 无设备（默认）
- 自定义

8. 单击**完成**。

> 要使配置完全生效，设备应在应用配置后重启。

创建可移动存储设备的允许列表

如果要创建允许存储设备的允许列表，请先完成以下步骤：

- 将您想要允许的 USB 存储设备附加到 PC。
- 打开设备管理器，并单击 USB 控制器。
- 查找每个控制器的设置，以了解设备信息。
- 在创建允许列表时，存储要使用的设备信息。

要创建可移动存储设备的允许列表：

步骤

1. 在 **Windows 桌面限制**配置页面中，单击**已加入允许列表的可移动存储**部分中的 **+ 添加**。
2. 在**添加硬件 ID** 窗口中，输入要从允许列表中删除并作为存储设备阻止的一个或多个设备的硬件 ID。
3. 单击**添加硬件 ID**。 **已加入允许列表的可移动存储**部分会显示已加入允许列表的硬件 ID 列表。

> 要编辑或删除列表中的硬件 ID，请选择**操作**列下的“编辑”或“删除”选项。
>
> 要使配置完全生效，设备应在应用配置后重启。

10.10.4.67. Windows 10 的桌面设置

通过 Windows 10 桌面设置配置，您可以定制桌面设置并将它们推送到 Windows 10 设备。 使用此配置，您可以配置以下桌面设置：

- 桌面背景图像
- 锁屏图像
- 上传自定义屏幕保护程序
- 桌面快捷方式

> 此功能需要 Bridge。 请查看 Ivanti Bridge，以了解详细信息。

步骤

1. 在**配置**下点击 **+ 添加**。
2. 选择 **Windows 10 的桌面设置**配置。 显示 **Windows 10 桌面设置**页面。
3. 在**名称**字段中，为设置键入恰当的名称。
4. （可选）点击 + **添加描述**链接，为配置添加描述。
5. 在**配置设置**部分，配置以下设置：

设置	说明
文件传输	为桌面设置选择以下任意文件交付选项： • **上传文件** - 将设置上传至 Ivanti Neurons for MDM。 • **覆盖 URL** - 提供带有要下载的设置文件的覆盖 URL。
桌面壁纸设置	点击**选择文件**以查找和上传壁纸图像。支持的文件格式有 BMP、JPG、JPEG、PNG。
锁屏壁纸设置 （Windows 10 Pro 设备**不**支持锁屏壁纸设置）	单击**选择文件**来定位和上传壁纸图像。 支持的文件格式 BMP、JPG、JPEG、PNG。
屏幕保护程序设置	点击**选择文件**以查找和上传屏幕保护程序文件。 仅上传 Windows 兼容的 .SCR 文件。 如果要为解锁屏幕保护程序模式设置密码，请选择**屏幕保护程序密码保护**。 选择**屏幕保护程序超时**期限（分钟）。
桌面快捷方式	单击**添加快捷方式**，设置桌面快捷方式以添加到设备桌面。 将显示**添加快捷方式**窗口。 使用以下选项填写表格： • **位置** - 键入快捷方式将出现在 Windows 设备上的位置。 • **目标路径** - 键入快捷方式将指向的本地路径、UNC 路径或驱动器号。 目标路径也可以是 URL。 • **参数** - 键入打开目标文件时要使用的任何参数。 • **工作目录** - 键入包含目标所需文件的文件夹路径。 • **图标文件** - 上传有效的 Windows .ico 文件。 配置选项后，单击**添加快捷方式**。

6. 单击**下一步**。
7. 选择下列分配选项之一：
   - 所有设备
   - 无设备（默认）
   - 自定义
8. 单击**完成**。

10.10.4.68. Windows Hello for Business 配置

此配置支持管理员在设备中设置 Windows Hello。 设置 Windows Hello 需要设置 PIN，才可以登录设备。

适用于：Windows 10

Procedure步骤

1. 转到配置 > + 添加。
2. 在搜索字段中输入 windows，然后单击 Windows Hello for Business 配置。
3. 输入配置的名称和描述。
4. 将启用/禁用适用于 Windows 10 设备的 Windows Hello for Business 切换为打开。

> 切换按钮默认设置为打开。 禁用 Windows Hello for Business 不会将 PIN 从设备中移除 。

5. 设置 PIN 复杂度。
6. 选择所需的配置：
   - 需要适用于 Windows Hello for Business 的受信任的平台模块
   - 将 Windows Hello for Business 证书用作智能卡证书
   - 使用生物特征手势（例如面容和指纹）作为 Windows Hello for Business 的 PIN 手势替换
   - 需要增强式防欺骗，才可以在 Windows Hello 人脸身份验证中识别人脸特征
   - 动态锁
   - 支持用户使用 FIDO2 安全密钥登录。
7. 单击下一步。
8. 选择启用此配置选项。
9. 选择下列分配选项之一：
   - 所有设备
   - 无设备（默认）
   - 自定义。
10. 单击完成。

10.10.4.69. Windows AI 管理配置

Ivanti Neurons for MDM 允许管理员管理 Windows AI 设置和配置。 Windows AI 管理借助强大的 AI 助手增强创造力和生产力。 使用 **Windows AI 管理**配置管理已注册 Windows 设备上的 Windows AI 功能。 此配置允许管理员通过 Windows AI 配置服务提供商 (CSP) 策略控制 Microsoft Copilot、Windows Recall 和 Microsoft Paint AI 功能。

管理员可以禁用选定的 AI 功能、移除 Copilot 功能的访问权限、控制 Windows Recall 行为，并管理 Microsoft Paint 中由 AI 驱动的图像生成功能。

适用于：Windows 10+

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择 **Windows AI 管理**配置。
3. 输入配置的**名称**和**描述**。
4. 在**配置设置**部分，从以下选项中进行选择： ### Copilot 设置

设置	说明
禁用 Windows Copilot	阻止用户访问 Windows Copilot。
禁用 Copilot 硬件按键	禁用受支持设备上的专用 Copilot 硬件按键。
删除 Microsoft Copilot 应用程序	从设备中删除 Microsoft Copilot 应用程序。

Recall 设置

设置	说明
禁用 AI 数据分析	禁用 Windows Recall 使用的基于 AI 的数据分析。
设置 Recall 快照的最大存储空间 (GB)	指定 Windows Recall 可用于存储快照的最大存储量。

Paint AI 设置

设置	说明
禁用 Image Creator	禁用 Microsoft Paint 中的 Image Creator 功能。
禁用 Cocreator	禁用 Microsoft Paint 中的 Cocreator 功能。
禁用 Generative Fill	禁用 Microsoft Paint 中的生成填充功能。

Microsoft 已弃用此配置使用的 **TurnOffWindowsCopilot** 策略。 因此，此配置不再影响驻留在设备上的 Copilot 应用程序。

如果未选中**禁用 Windows Copilot** 复选框，则该配置将覆盖设备上先前的配置选择，以启用 Windows AI 管理。

5. 单击**下一步**，配置分配设置。
6. 选择其中一个分发选项来设置 **Windows AI 管理**配置。 有关配置分发选项的详细信息，请参阅使用配置。
7. 单击**完成**。

10.10.4.70. Play Integrity（原 SafetyNet Attestation）

Play Integrity（原 SafetyNet）有助于使用 Google 的 Play Integrity API 评估 Android 设备的安全性和兼容性。 配置后，您可以在固定的时间间隔后分析设备，以确定设备是否被篡改。

> 现在，所有 Android 版本都支持 Play Integrity。

步骤

1. 在**配置**选项卡中，点击 **+添加**。
2. 选择 **Play Integrity** 配置。 随即会显示 **Play Integrity 配置**页面。
3. 在**名称**字段中，为 Play Integrity 配置输入恰当的名称。
4. 点击“**+添加描述**”链接，为配置添加描述。 此字段为可选。
5. 在**配置设置**部分，键入用于评估设备安全性和兼容性检查的最小时间间隔（以小时为单位）。 该值必须在 1 到 24 之间。
6. 单击**下一步**，然后选择以下分发选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义

单击**完成**。

> 当 Play Integrity 和 SafetyNet 随机数将发送到设备时，Play Integrity 随机数将优先于 SafetyNet 随机数。

10.10.4.71. 高级 Android 密码和锁屏

Couldn't convert your doc.

10.10.4.72. Microsoft Defender for Endpoint

Microsoft Defender for Endpoint (MDE) 配置以前称为 Windows 高级威胁防护，允许客户将设备加入和退出 MDE 服务。

步骤

1. 转到**配置 > + 添加**。
2. 选择 **Microsoft Defender for Endpoint** 配置。
3. 输入配置的名称。
4. 输入描述。
5. 在"配置设置"部分中，按照下表描述指定剩余设置。

设置	说明
板内或板外 Blob	粘贴从 Microsoft Defender for Endpoint Security Center 站点取得的加入或退出 Blob

6. 单击**下一步**。
7. 选择下列分配选项之一：

- 所有设备
- 无设备（默认）
- 自定义

8. 单击**完成**。

10.10.4.73. 基于证书的身份验证

Ivanti Neurons for MDM支持基于证书的身份验证，这允许管理员使用数字证书和租户指定的（虚）主机名进行登录。 在启用并配置时，管理员可以使用数字证书进行登录，而非基本身份验证（用户名和密码）。

> 此功能默认禁用。 管理员应联系支持，以在租户中启用此功能。 此功能仅在 NA3 群集环境中可用，并且仅在由支持启用时可用。 请确保，您已测试超级管理员用户名和密码并将其准备就绪，因为在启用基于证书的身份验证后，这些凭据将是您用于登录的唯一凭据，直到您成功配置虚域。

步骤

1. 在**管理员**选项卡中，选择**虚主机配置**。
2. 在虚主机配置页面中，配置以下选项：
3. 单击**保存**。
   虚主机可能需要几分钟，才可以访问。

设置	流程
创建虚域	键入虚域的名称。 这是可能与企业品牌形象更贴近的域名，并且您可以使用数字证书进行登录。
上传受信签发 CA 证书	单击**选择文件**，以选择并上传向管理员颁发证书的 CA 证书。 要启用证书吊销检查，选择**为此证书启用证书状态验证设置**（可选）。 此选项默认禁用。 取消选择此选项，以禁用证书吊销。 单击**添加更多**，以添加更多证书。 请确保证书格式是 .p7b、.pem、.der、.crt 或 .cer。
证书属性映射	证书属性映射会配置证书标识元素到管理员的帐户属性的映射。 在**自证书**字段中，选择以下任一证书元素： • **NTPrincipalName** • **RFC 822 名称** 在**至变量**字段中，选择以下管理员的任意帐户属性： • **UserUPN** • **$UserEmailAddress** • **$EDIPI**

10.10.5. 用户资源配置

本部分包含以下主题：

- CalDAV 配置
- CardDAV 配置
- Google 配置
- 电子邮件配置
- Exchange 配置
- 字体配置
- 订阅日历配置
- 创建 Web 剪辑配置
- Office 365 安装
- Windows GPO 设置
- BitLocker 加密配置

10.10.5.1. CalDAV 配置

CalDAV 配置使用 CalDAV 互联网标准定义了对网络日历的访问。

CalDAV 设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
主机名和端口	输入日历服务器的主机名和端口。
主 URL	输入访问日历服务的 URL。
用户	输入用于访问的用户名称。
密码	输入用于访问的密码。
使用 SSL	选择此项可仅在设备与服务器之间使用安全套接层协议进行通信。
每个 App VPN	**先决条件**：在 CalDAV 配置中配置 Per-App VPN 前，配置 Tunnel 或任何 Per-App VPN 配置。 从下拉菜单中，选择预配置的 Per App VPN 配置。 **适用于**：iOS 14+

有关更多信息，请查看如何创建配置

10.10.5.2. CardDAV 配置

CalDAV 配置使用 CardDAV 互联网标准定义了对网络通讯录的访问。

CardDAV 设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
主机名和端口	输入通讯录服务器的主机名和端口。
主 URL	输入访问通讯录服务的 URL。
用户名	输入用于访问的用户名称。
密码	输入用于访问的密码。
使用 SSL	选择此项可仅在设备与服务器之间使用安全套接层协议进行通信。
每个 App VPN **iOS 10+**	**先决条件**：在 CardDAV 配置中配置 Per-App VPN 前，配置 Tunnel 或任何 Per-App VPN 配置。 从下拉菜单中，选择预配置的 Per App VPN 配置。 **适用于**：iOS 14+
通信服务规则	选择要用来在 CardDAV 系统内音频呼叫联系人的默认应用程序。

有关更多信息，请查看如何创建配置

10.10.5.3. Google 配置

Google 账户配置将 iOS 9.3.2 与 visionOS 1.1 或 Android 6.0+ 设备或者运行更新版本的设备连接到 Google 账户。 Google 帐号需要 Android 企业版。 该配置可以设置多个 Google 电子邮件地址以及经过身份验证后用户启用的任何其他 Google 服务。

步骤

1. 转到**配置 > + 添加**。
2. 选择 **Google 帐户**配置。
3. 输入配置的名称。
4. 输入描述。
5. 在配置设置部分中，请按下表所述指定剩余设置：

设置	采取何种措施
iOS 9.3.2+ 、Android 6.0+	
名称	输入用于识别此配置的名称。
帐号说明	输入帐号的显示名称。
帐号名称	输入帐号用户的完整名称。
电子邮件地址	输入帐号的 Google 电子邮件地址。
每个 App VPN	**先决条件**：在 Google 帐户配置中配置 Per-App VPN 前，配置 Tunnel 或任何 Per-App VPN 配置。 从下拉菜单中，选择预配置的 Per App VPN 配置。 **适用于**：iOS 14+
iOS 10+	
通信服务规则	通过选择以下任何选项，选择默认应用，以用于在 Google 系统中向联系人拨打音频电话： • **从 App Catalog 和系统应用中**：通过键入应用名称的前几个字母，搜索应用。 • **输入捆绑 ID（仅适用于 Apple 系统应用）**：键入系统应用捆绑 ID。 捆绑 ID 必须以 'com.apple' 开头。

6. 单击**下一步**。
7. 选择下列分配选项之一：

- 所有设备
- 无设备（默认）
- 自定义

8. 单击**完成**。

在 Google 帐户配置应用于设备时，Go 客户端提示用户登录 Google。

有关更多信息，请查看如何创建配置

10.10.5.4. 电子邮件配置

可通过电子邮件配置在设备上设置 POP 或 IMAP 电子邮件。

电子邮件设置

设置	采取何种措施
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
账户说明	输入用于识别此电子邮件帐号的文本。
账户类型	选择 IMAP 或 POP。 如果选择 IMAP，还可输入路径前缀。 互联网服务提供商 (ISP) 将提供可用帐号类型信息。 如果所有 IMAP 文件夹都出现在“收件箱”下，通常需要前缀。 需要前缀的 ISP 通常会提供配置特定前缀的信息。
用户显示名称	输入用于识别电子邮件帐号用户的文本。 注意，用户也可在设备上设置此值。
电子邮件地址	输入指定帐号电子邮件地址的变量。
允许移动	如果不希望阻止此帐号中的电子邮件移动，则选择此设置。
启用 S/MIME	选择以开启 S/MIME 加密支持。 然后，您可以选择签名和加密证书。 需要证书缓存。 确保在身份证书配置使用的证书颁发机构中启用缓存。 **iOS 10.3+：** 为 **S/MIME 签名**和 **S/MIME 加密**字段选择以下选项之一： • 关闭 • 打开 • 用户选择 **iOS 12.0+：** • 使用户覆盖 S/MIME 签名设置 • 使用户选择 S/MIME 签名身份 • 使用户覆盖 S/MIME 加密设置 • 使用户选择 S/MIME 加密身份 **如果需要，启用 S/MIME 每消息签名和加密**。
允许信箱	选择允许此帐户使用 Mail Drop。 Mail Drop 可使用户通过将附件存储在 iCloud 中并在电子邮件中置入链接，发送包含大型附件的电子邮件。 有关邮件投递的更多信息，请转到：https://support.apple.com/
每个 App VPN	Apple 支持在邮件域上关联多个不同 Per-App VPN 配置文件的功能。 现在，Per-App VPN 支持 IMAP 和 POP3 电子邮件配置。 **先决条件**：在电子邮件配置中配置 Per-App VPN 前，配置 Tunnel 或 Per-App VPN 配置。 在下拉菜单中，**选择 Per-App VPN 配置**。

传入邮件

设置	采取何种措施
邮件服务器和端口	互联网服务提供商 (ISP) 将提供此地址。
用户名	输入用于访问传入邮件服务器的用户名。 通常与电子邮件地址相同。 ISP 将提供格式。
身份验证类型	选择由 ISP 定义的身份验证类型。
密码	输入用于访问传入邮件服务器的密码。
使用 SSL	选择此项可仅在设备与服务器之间使用安全套接层协议进行通信。

传出邮件

设置	采取何种措施
邮件服务器和端口	互联网服务提供商 (ISP) 将提供此地址。
用户名	输入用于访问传出邮件服务器的用户名。 通常与电子邮件地址相同。 ISP 将提供格式。
身份验证类型	选择由 ISP 定义的身份验证类型。
密码	输入用于访问传出邮件服务器的密码。
传出密码与传入密码相同	如果 SMTP 身份验证使用与 POP/IMAP 相同的密码，则选择此设置。
仅在邮件中使用	如果仅希望电子邮件客户端使用此配置，则选择此设置。 其他发送电子邮件的应用，包括使用本地电子邮件客户端发送内容的应用，均无法使用此配置。
使用 SSL	选择此项可仅在设备与服务器之间使用安全套接层协议进行通信。

10.10.5.5. Exchange 配置

Exchange 配置为 Android、iOS 和 visionOS 设备设置基于 ActiveSync 的电子邮件，为 macOS 设备设置基于 Exchange Web Services (EWS) 的电子邮件。

> Samsung Android 9 设备不支持 Exchange 配置。 对于运行 Android 9 及更高版本的 Samsung 设备，设备管理模式不支持 Exchange 配置。

Exchange 设置

设置	用途
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
Exchange 主机	如果您正使用 **Sentry** 控制电子邮件访问，请输入 Sentry 服务器主机名。 或者，输入 ActiveSync 服务器的地址。*
允许移动	**对于 iOS 和 Android：** 如果不希望阻止此账号中的电子邮件移动，则选择此设置。 **Windows 10：**不适用。
启用 S/MIME	选择，以开启 S/MIME 加密支持。 然后，您可以选择签名和加密证书。 需要证书缓存。 确保在身份证书配置使用的证书颁发机构中启用缓存。 **iOS 10.3+：** 为 **S/MIME 签名**和 **S/MIME 加密**字段选择以下选项之一： • 关闭 • 打开 • 用户选择 **iOS 12.0+：** • 使用户覆盖 S/MIME 签名设置 • 使用户选择 S/MIME 签名身份 • 使用户覆盖 S/MIME 加密设置 • 使用户选择 S/MIME 加密身份 **如果需要，启用 S/MIME 每消息签名和加密。**
同步最近的电子邮件地址	选择以在设备与服务器之间同步最近联系的电子邮件地址。
仅在邮件中使用	选择您是否仅希望电子邮件客户端使用此配置。 其他发送电子邮件的应用，包括使用本地电子邮件客户端发送内容的应用，均无法使用此配置。
使用 SSL	选择此项可仅在设备与服务器之间使用安全套接层协议进行通信。
启用适用于交换负载的 OAuth	iOS 12.0+ 和 macOS 10.14+： 选择以启用使用 OAuth 进行身份验证。 如果启用此选项，以下其他设置对支持使用 OAuth 进行身份验证的电子邮件应用程序可用： • OAuth 登录 URL • OAuth 令牌请求 URL
域	输入此电子邮件账号的域，如果希望系统提示用户输入，则不在此输入。
用户	输入代表此帐户的电子邮件地址的变量。*
账户密码	输入此账号的密码，如果希望系统提示用户输入，则不在此输入。
电子邮件地址	输入代表此帐户的电子邮件地址的变量。*
同步邮件的过去天数	选择在设备与服务器间同步的电子邮件的天数。

设置	用途
每个 App VPN	**先决条件**：在 Exchange Active Sync 配置中配置 Per-App VPN 前，配置 Tunnel 或任何 Per-App VPN 配置。 从下拉菜单中，选择预配置的 Per App VPN 配置。 **适用于**：iOS 14+
Android 和 Windows	
同步日历	**Android 和 Windows 10：**选择在设备和服务器之间同步日历项目。 **对于 Samsung 设备：**未使用此设置（默认开启）。 **对于 Android Email+ 应用：**使用此设置。
同步联系人	**Android 和 Windows 10：**选择在设备和服务器之间同步联系人。 **对于 Samsung 设备：**未使用此设置（默认开启）。 **对于 Android Email+ 应用：**使用此设置。
同步电子邮件	**Android 和 Windows 10：**选择在设备和服务器之间同步电子邮件。 **对于 Samsung 设备：**未使用此设置（默认开启）。 **对于 Android Email+ 应用：**未使用此设置（默认开启）。
同步任务	**Android 和 Windows 10：**选择在设备和服务器之间同步任务。 **对于 Samsung 设备：**未使用此设置（默认开启）。 **对于 Android Email+ 应用：** 不适用。
iOS 13.0+	
• 同步日历 • 同步联系人 • 同步邮件 • 同步注释 • 同步提醒	指定单独同步 Outlook Exchange 项目，例如日历、联系人、邮件、备注和提醒。 对于每个项目，选择或取消选择**启用**和**允许用户覆盖**选项。 必须为其中一个项目启用同步。 如果您禁用其中一个选项的同步，但允许用户覆盖，该用户仍将可以启用。
身份证书	如果希望设备使用证书对服务器进行身份验证，则从列表中选择身份证书。 仅当使用身份证书配置进行配置后，证书才显示在此列表中。
Android	
仅使用基于身份验证的证书	使用所选身份证书作为对 Exchange 服务器进行身份验证的唯一方法。
接受所有 SSL 证书	选择此项可允许设备用户将 Android 设备设置为接受所有 SSL 证书。 此设置适用 Android Email+ 和 Samsung Knox 电子邮件。 • 启用此设置时请谨慎，设备用户可能会在不知情的情况下遭到设备攻击。 • 如果 Sentry 证书是自签名证书或未知证书，则需要启用此选项。
Exchange 应用优先级	选择在 Android 设备上默认配置的电子邮件客户端 - Android Email+ 和 Samsung 电子邮件。 对于启用 Exchange 应用优先级的所有租户，Email+ 应用会添加到 App Catalog。
iOS 10+	

设置	用途
通信服务规则	选择要用来在 CardDAV 系统内音频呼叫联系人的默认应用程序。
仅限 Windows 10+	
配置 Outlook	选择此选项，以将 Microsoft Outlook 配置为设备。 此选项仅在启用 Bridge 时支持。

*键入 $ 查看此字段支持的变量列表（如果有）。

10.10.5.6. 字体配置

字体配置支持您为 iOS 7 设备提供额外 TrueType 或 OpenType 字体文件。 下表介绍了字体设置：

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
上传字体	将字体文件拖放到虚线框，或单击**选择文件**，从文件系统中选择。 字体文件必须为 .otf 或 .ttf 文件。

有关更多信息，请查看**如何创建配置**

10.10.5.7. 订阅日历配置

订阅日历配置对公共网络日历的访问进行定义。

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
URL	输入用于访问日历的 URL。*
用户	输入用于访问的用户名。*
密码	输入用于访问的密码。
使用 SSL	选择此项可仅在设备与服务器之间使用安全套接层协议进行通信。

键入 $ 以查看此字段支持的变量列表（如果有）。

有关更多信息，请查看如何创建配置

10.10.5.8. 创建 Web 剪辑配置

Web 剪辑是来自 iOS 设备网站或网页的快捷方式。 使用网络剪辑配置可在设备上创建标准的网络剪辑。 可以向要启动特定网站的 iOS 设备添加 Web 剪辑图标。 Web 剪辑有助于在设备主屏幕上快速查找和使用书签。 此外，还可以控制该网站在 Mobile Safari 上的参数，调整观看体验。

> 此配置支持带自定义分发选项的委派。 有关详细信息，请参阅使用配置中的*分发配置*主题。

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 单击**配置**。
3. 点击 **+添加**。
4. 搜索和选择 Web 剪辑配置。
5. 在此页面上配置设置。 请参阅 **Web 剪辑配置设置**主题中的表格，了解有关值的指南。
6. 单击**下一步**，配置分配设置。
7. 选择**自定义**，然后选择**设备/设备组**。
8. 单击**完成**。

Web 剪辑配置设置

下表列出了 Web 剪辑配置设置：

设置	流程
名称	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
标签	输入您希望在设备屏幕上的快捷方式下显示的文本。*
URL	输入 Web 剪辑要访问的 URL。*
可删除	选中复选框，允许设备用户删除 Web 剪辑。
图标	将图标文件拖放到虚线框，或单击**选择文件**，从文件系统中选择。
复合图标	选择此项可消除 Safari 的较新版本添加的特殊效果。
全屏	选择此项可以全屏模式显示 Web 剪辑，而不是在浏览器中显示内容。
忽略清单范围	选中即可允许导航到外部网站，而不显示 Safari 浏览器。 未选中“全屏”时，此选项无效。
目标应用程序捆绑标识符	应用程序捆绑标识符用于指定打开 URL 的应用程序。 **示例**：com.google.chrome.ios

> 键入 $ 以查看此字段支持的变量列表（如果有）。

相关主题：

- iOS 的多用户安全登录
- 如何创建配置

10.10.5.9. Office 365 安装

许可证：Silver

适用于：Windows 10+

设置 Office 365 安装

Office 365 安装是一种配置设置，可以应用于选定的设备以安装或卸载 Office 365。 您可以使用 Microsoft Office 部署工具定义 xml 格式的配置设置，然后上传文件。 上传文件后，您可以将配置选项推送到所选设备。

步骤

1. 在**配置**选项卡中，单击**+添加**。
2. 选择 **Office 365 安装**。 将显示 **Office 365 安装**页面。
3. 在**名称**字段中，为配置输入恰当的名称。
4. 单击 +**添加描述**链接，以便为配置添加描述。该字段是可选项。
5. 在**配置设置**部分，更新以下字段：

字段名称	描述
用于安装 Office 365 的配置文件	单击**选择文件**按钮，以浏览并选择 XML 格式的配置文件，其中包含用于 Office 365 安装的定义设置。 示例：<Configuration> <Add OfficeClientEdition="64" Channel="Current"> <Product ID="O365ProPlusRetail"> <Language ID="en-us"/> </Product> </Add> </Configuration> 确保配置文件为 xml 格式，并在添加配置设置文件后显示绿色对号。
用于卸载 Office 365 的配置文件	单击**选择文件**按钮，以浏览并选择 XML 格式的配置文件，其中包含用于卸载 Office 365 的定义设置。 示例：<Configuration> <Remove All="TRUE"/><Display Level="None" AcceptEULA="TRUE" /> </Configuration> 确保配置文件为 xml 格式，并在添加配置设置文件后显示绿色对号。

6. 单击**下一步**。
7. 选择以下任何选项将设置分配到设备。

选项	描述
启用此配置	选中该复选框可以对所选设备进行此配置。 取消选中该复选框将删除配置（如果已经应用于设备）。
所有设备	将设置分配给所有设备。
无设备	保留要分配给设备的设置。
自定义	为定义的设备组分配设置。 选中要分配设置的设备类型旁边的复选框。 您还可以通过在**搜索设备组**搜索字段中键入设备组名称来搜索设备组。 如果您想创建新的设备组，请单击页面底部的**创建新设备组**链接。 有关详细信息，请参阅**设备组**。 选择设备类别时，可以在**分发摘要**部分下方，针对所选设备类别，查看设备用户列表的详细信息（**姓名**、**电话号码**和**设备类型**）。

8. 单击**完成**，以便将设置推送到所选设备。

10.10.5.10. Windows GPO 设置

许可证：Bridge

适用于：Windows 桌面

设置 Windows GPO 设置

组策略对象 (GPO) 是一个设置集合，可针对允许或不允许设备执行的操作来定义相应的权限。 这是使用 Bridge 设置管理 GPO 设置是先决条件。 有关详细信息，请参阅 Ivanti Bridge。

如果 GPO 元数据未上传到数据库，请与站点管理员联系。 通过 Bridge，使用 PowerShell 脚本将 GPO 配置部署到设备。 使用 GPO 设置，您可以配置并将特定设置推送到设备。

步骤

1. 在**配置**选项卡中，点击 **+添加**。
2. 选择 **Windows GPO 设置**配置。 将显示 **Windows GPO 设置**页面。
3. 在**名称**字段中，为 Windows GPO 设置键入适当的名称。
4. 单击 + **添加描述**链接，以为配置添加描述。 此字段可选。
5. 在**配置设置**部分中，单击 + **添加**。 将显示**添加 Windows 组策略对象 (GPO)** 窗口。
6. 通过从左窗格中的 GPO 层次结构树中，单击相关组件来搜索并选择 GPO。 GPO 层次结构树表示策略设置的路径。 您也可以通过在搜索字段中键入 GPO 设置的名称来搜索特定的 GPO 设置。
   选择 GPO 设置后，您可以在右窗格中查看所选 GPO 设置的详细信息。
7. 在**设置状态**字段中，可以使用以下设置选项：

选项	说明
未配置	删除现有的 GPO 设置。
已启用	启用 GPO 设置。
已禁用	禁用 GPO 设置。

8. 在**设置值**字段中，键入给予 GPO 的适当名称。
   要添加其他设置值，请点击 **+** 图标。 某些 GPO 设置可能不需要任何其他设置值。 有些则可能需要在设置值下，以文本值的形式指定其他数据。 在这些设置中，可以从可用的下拉列表中选择任意值。

> 仅在选中**设置状态**下的**已启用**选项时，才可编辑此字段。

9. 单击**保存并关闭**，以便保存 GPO 并关闭窗口。 如果您要添加其他 GPO，单击**保存并添加另一项**，保存并保持 GPO 窗口打开。
   配置设置部分中将显示添加的 GPO 设置。

> 可以点击**操作**列中的相关图标，以编辑或删除 GPO 设置。

选项描述启用此配置选中该复选框可以对所选设备进行此配置。 取消选中该复选框将删除配置（如果已经应用于设备）。**所有设备**将设置分配给所有设备。**无设备**保留要分配给设备的设置。**自定义**为定义的设备组分配设置。 选中要分配设置的设备类型旁边的复选框。 您还可以通过在

搜索设备组搜索字段中键入设备组名称来搜索设备组。 如果您想创建新的设备组，请单击页面底部的**创建新设备组**链接。 有关详细信息，请参阅**设备组**。

选择设备类别时，可以在**分发摘要**部分下方，针对所选设备类别，查看设备用户列表的详细信息（**姓名**、**电话号码**和**设备类型**）。

10. 单击**完成**，以便将 GPO 设置推送到所选设备。

10.10.5.11. BitLocker 加密配置

许可证：Bridge

适用于：Windows 桌面

本部分包含以下主题：

- 设置 BitLocker 加密
- 查看 BitLocker 设置

设置 BitLocker 加密

BitLocker 加密是一种可在硬盘驱动器和可移动驱动器上执行加密，以进行数据保护的功能。 使用 Bridge 设置管理 BitLocker 加密是先决条件。 请查看 **Bridge**，以了解更多详细信息。 BitLocker 加密配置可帮助您配置设备的加密设置。

步骤

1. 在**配置**选项卡中，点击 **+添加**。
2. 选择 **BitLocker 加密**配置。 显示 **BitLocker 加密**页面。
3. 在**名称**字段中，为 BitLocker 加密输入适当名称。
4. 单击 **+ 添加描述**链接，以为配置添加描述。 此字段可选。
5. 在“配置设置”部分中，配置以下设置：

设置	说明
加密方法和类型	根据加密的密钥大小选择加密算法的类型。 以下选项可用： • **AES-CBL 128 位** • **AES-CBL 256 位**
加密所有硬件驱动器	单击切换按钮， **打开**或**关闭**用于加密所有硬件驱动器的设置。 如果任何硬件驱动器已在设备上加密，将不会应用编辑此配置，因为加密过程不可逆。
选择驱动器	选择需要加密的驱动器。 示例：**C:** 单击 **+ 添加**，添加更多驱动器。 如果您打开**加密所有硬件驱动器**设置，将不会显示此字段。
基于硬件的驱动器类型加密	可信平台模块 (TPM) 是计算机主板上的一个芯片，有助于防篡改加密。 如果在具有 TPM 的计算机上使用 BitLocker 加密或设备加密，则密钥的一部分会存储在 TPM 中。 您可以从下拉列表中选择以下基于硬件的加密设置选项： • **启动时需要 TPM** • **需要使用 TPM 启动 PIN** • **不使用 TPM** TPM 选项仅适用于 OS 驱动器和 TPM 版本 1.2 及更高版本。 如果您将基于硬件的加密设置应用于设备，则无法再对设备编辑该设置。 如果设备已使用 BitLocker 配置进行设置，则不能使用不同的 TPM 选项推送第二个 BitLocker 配置。
选择下列配置复选框选项（可选）： • **拒绝对不受 BitLocker 保护的固定驱动器进行写入访问** • **拒绝对不受 BitLocker 保护的可移动驱动器进行写入访问**	
加密前设备操作	选择以下任一选项，以定义处理未完全解密或已有密钥保护器的驱动器的方式。 • 停止加密 - 如果任何选定的驱动器已经加密，则停止加密。 • 解密在 Ivanti Neurons for MDM 中没有恢复密码存储的选定驱动器 - 如果选择此选项，则仅会应用于在 Ivanti Neurons for MDM 中没有恢复密码的驱动器。
恢复选项	如果用户忘记密码，则使用恢复选项。 从设备详细信息页面中，您可以进行检索。 您可以配置以下恢复选项： • **禁用恢复** • **使用密码并存储在 AD 中** • **使用密码并存储在 AD 和 MobileIron 中**
重新启动间隔	将配置推送到设备后，将提示重新启动。 然后在重新启动之后开始加密。 要配置重新启动间隔，从下拉列表中，选择设备重新启动所需的持续时间。 最小重新启动间隔为 1 分钟，最大重新启动间隔为 120 分钟（2 小时）。

设置	说明
重新启动消息	输入应在设备中显示的重新启动消息。 如果适用，也会向用户显示启动密码或启动 PIN。 用户可以将其记下，以便在重新启动后提示时将其输入。

6. 单击**下一步**。
7. 选择以下任何选项将设置分配到设备。

设置	说明
启用此配置	选中该复选框可以对所选设备进行此配置。 取消选中该复选框将删除配置（如果已经应用于设备）。
所有设备	将设置分配给所有设备。
无设备	保留要分配给设备的设置。
自定义	为定义的设备组分配设置。 选中要分配设置的设备类型旁边的复选框。 您还可以通过在**搜索设备组**搜索字段中键入设备组名称来搜索设备组。 如果您想创建新的设备组，请单击页面底部的**创建新设备组**链接。 有关详细信息，请参阅设备组。 选择设备类别时，可以在**分发摘要**部分下方，针对所选设备类别，查看设备用户列表的详细信息（**姓名**、**电话号码**和**设备类型**）。

8. 单击**完成**，以便将设置推送到所选设备。

查看 BitLocker 设置

在 **BitLocker 设置**部分中，您可在"设备"详细信息页面（**设备 > 设备 > [设备名称]**）中查看为设备设置的 BitLocker 设置。 默认情况下，隐藏详细信息。

通过点击每个字段旁边的查看（眼睛形状）图标，可以查看以下详细信息：

设置	说明
恢复密码	选择此选项后，Windows 将生成恢复密码，并在推送 BitLocker 配置后返回到 Ivanti Neurons for MDM。 如果设备进入恢复模式，系统将提示用户输入此密码。 如果加密多个驱动器，应使用相同恢复密码。 只有在选择恢复选项**使用密码并存储在 AD 和 MobileIron 中**，才会发布恢复密码。
PIN	显示启动 6 位数 PIN。 只有在 BitLocker 配置设置中选择了选项**需要使用 TPM 启动 PIN**才会显示 PIN。
启动密码	为设备设置启动密码。 仅当您在 BitLocker 配置设置中选择选项**请勿使用 TPM**，才会显示启动密码。
TPM 版本	显示配置的 TPM 版本。

根据 BitLocker 配置设置中配置的设置，一些字段可能显示 **不适用**。

- 加密状态显示在设备详细信息页面的设备加密状态下。
- 相同的启动密码或 PIN 将用于要应用 BitLocker 的设备的所有驱动器。
- 如果您正在创建一个配置来加密已经加密驱动器并保存恢复密码的设备的第二个驱动器，则早期的密码将被覆盖。 因此，建议将恢复密码选项仅用于设备中的一个驱动器。

10.10.6. 企业网络访问配置

本部分包含以下主题：

- AirPlay 配置
- AirPrint 配置
- Always-on VPN 配置
- 默认应用程序运行时权限
- 教育
- 全局代理配置
- LDAP 配置
- macOS 服务器配置
- 网络中继配置
- Tunnel
- 设置 AppTunnel
- Per-App VPN 配置
- 单点登录配置
- iOS 的多用户安全登录
- Android APN 设置配置
- VPN 配置
- 按需 VPN
- Wi-Fi 配置

10.10.6.1. AirPlay 配置

许可证：Silver

Airplay 配置可设置用于媒体显示备用设备的访问权限。 下表列出了 Airplay 设置：

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
允许列表	输入各已许可 AirPlay 目标设备 ID。 如果您未列出 ID，则 AirPlay 目标不受限制。 **适用于**：iOS 7.0+ 和 macOS 10.10+（受监管）。
设备设置	请为每个已知 AirPlay 目的地输入设备 ID (macOS) 或设备名称 (iOS) 和密码。

有关更多信息，请查看如何创建配置

10.10.6.2. AirPrint 配置

许可证：Silver

AirPrint 配置可设置无线打印。 下表列出了 AirPrint 设置：

设置	用途
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
Airprint 设置	**IP 地址：**输入 AirPrint 打印机的 IP 地址。 **资源路径：**输入与 AirPrint 打印机关联的资源路径。 这与 ipps.tcp Bonjour 记录的 rp 参数相对应。 示例： • printers/Canon_MG5300_series • printers/Xerox_Phaser_7600 • ipp/print • Epson_IPP_Printer. 资源路径区分大小写。 **端口：** 输入 AirPrint 目标的监听端口。 如果未指定，AirPrint 将使用默认端口。 有关 Apple 标准端口的详细信息，请访问 https://support.apple.com/en-us/HT202944 **强制执行 TLS**：允许启用传输层安全性 (TLS) 保护的连接。 默认情况下，它被禁用。

在 **AirPrint** 配置安装到 macOS 后，打印机详细信息会通过 **AirPrint** 配置推送到设备。 通过单击系统首选项 > 打印机和扫描仪 > +，用户可以查看自动填充的打印机详细信息。 在**添加**屏幕中，用户必须选择**默认**，然后选择所需的打印配置文件。 此操作会将所需的打印机添加到**打印机和扫描仪**。

有关更多信息，请查看如何创建配置

10.10.6.3. Always-on VPN 配置

许可证：

- **Gold for Android Enterprise**
- **Silver for iOS**

Always-on VPN 配置可确保用户自动连接至 VPN（如果可用），无需进行任何操作。 此功能需要 Android 7.0 + 或 iOS 8+，以及支持 IKEv2 协议的 VPN 提供商。

适用于 Android 的 Always-on VPN 设置

Always-on VPN 配置已发送到运行 Android 7.0 + 的 Android Enterprise 设备。 在拥有工作配置文件 (Android 8.0+) 的托管设备上，VPN 配置会应用于工作配置文件。

> 当设备在 **COSU** 模式下部署且设备注册类型为 **AMA** 时，如果具有 **Always-on** 配置的应用程序推送至该设备，则其上的 **Always-on** 配置也会推送至该设备。

要启用此配置，从“App Catalog”中选择应用或输入程序包名称。

适用于 iOS 的 Always-on VPN 设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
蜂窝网络和 Wi-Fi 使用相同的隧道配置	选择此项可为 VPN 连接定义一个服务器标识符对，无论该连接是通过蜂窝网络还是 Wi-Fi 网络建立。
服务器	输入 VPN 服务器的主机名或 IP 地址。
本地标识符	采用下列格式之一的 IKEv2 客户端标识符： • FQDN • UserFQDN • 地址 • ASN1DN
远程标识符	采用下列格式之一的远程标识符： • FQDN • UserFQDN • 地址 • ASN1DN
启用 EAP	选择此项可启用扩展的身份验证。
计算机身份验证	只有未选择“启用 EAP”时可用。 选择下列选项之一： • 证书 • 共享密钥
EAP 身份验证	只有选择“启用 EAP”时可用。 选择下列选项之一： • 证书 • 用户名/密码
共享密钥	仅当选择共享密钥进行计算机身份验证时可用。 输入用于连接的共享密钥。
凭据	仅当选择证书进行计算机身份验证时可用。 选择要使用的证书。 将发送此证书，进行 IKE 客户端身份验证。 如果使用扩展的身份验证，此证书可用于 EAP-TLS。
账户	仅当选择用户名/密码进行 EAP 身份验证时可用。 输入 VPN 服务器的帐号 ID。
密码	仅当选择用户名/密码进行 EAP 身份验证时可用。 输入 VPN 服务器的密码。
对等体存活检测间隔	选择下列选项之一： • 无（禁用） • 低（每 1 小时发送一次 keepalive） • 中（每 30 分钟发送一次 keepalive）

设置	流程
	• 高（每 10 分钟发送一次 keepalive）
加密算法	选择下列选项之一： • DES • 3DES • AES-128 • AES-256 • AES-128-GCM • AES-256-GCM • ChaCha20-Poly1305
完整性算法	选择下列选项之一： • SHA1-96 • SHA1-160 • SHA2-256 • SHA2-384 • SHA2-512
迪菲-赫尔曼分组	选择 D-H 密钥交换小组。
以分钟为单位的生存期	输入以分钟为单位的 SA 使用时间（密钥更新间隔）。 有效值为 10 到 1440。
声音邮件	选择“允许通过隧道传输流量”可针对 Always-on VPN 免除语音邮件。 选择丢弃流量，以避免豁免。
Airprint	选择“允许通过隧道传输流量”可针对 Always-on VPN 免除 Airprint 流量。 选择丢弃流量，以避免豁免。
蜂窝服务	选择“允许通过隧道传输流量”可针对 Always-on VPN 免除蜂窝服务流量。 选择丢弃流量，以避免豁免。
允许流量来自 VPN 隧道外已捕获的 Web 表	选择此项可允许流量来自 VPN 隧道外已捕获的 Web 表。
允许流量来自 VPN 隧道外所有已捕获的联网应用	选择此项可允许流量来自 VPN 隧道外所有已捕获的联网应用，以执行已捕获网络处理。
被捕获联网应用包标识符	列出已捕获联网应用的捆绑软件 ID，将允许这些应用的流量在 VPN 隧道外执行被捕获网络处理。 已捕获联网应用可能需要额外权利，以在被捕获环境中操作。

有关更多信息，请查看[如何创建配置]

10.10.6.4. 默认应用程序运行时权限

适用于：针对 Android API 23+ 构建并在 Android Enterprise 设备上运行 Android 6.0+ 的应用。

对于部署到 Android Enterprise 设备的应用，管理员可以为其设置运行时权限配置。 针对 API 23（或更高版本）和运行 Android 6.0 或更高版本构建的应用程序能够在运行时提示用户获得权限。 默认应用程运行时权限配置为这些应用运行时权限设置默认值。 Ivanti Neurons for MDM 默认创建此配置。 您可以根据需要编辑此默认系统配置或创建新配置。

应用特定权限优先于通用应用权限配置。 内部应用程序受到全局权限的约束。 不支持为内部应用程序设置每个应用程序的权限。

设置全局运行时权限

管理员可以编辑默认的应用程序运行时权限和此配置的分配，操作如下：

Procedure步骤

1. 转至**配置**。
2. 执行以下操作之一：
   - 要编辑默认系统配置，单击**默认应用运行时权限**，并单击**编辑**。
   - 要添加新配置，单击**添加 > 默认应用运行时权限**。

输入配置的名称。

4. 输入描述。
5. 在“配置设置”部分中，设置以下默认运行时权限之一：
   - 用户提示（默认选项）
   - 自动授权
   - 自动拒绝（谨慎使用）

单击**下一步**。

7. 选择**启用该配置选项**。

> 如果取消选择此选项，则此配置将不会应用于任何设备。 如果先前已应用该配置，会将其从所有设备中删除。

8. 选择下列分配选项之一：
   - 所有设备
   - 无设备（默认）
   - 自定义

单击**完成**。

设置应用程序特定运行时权限

管理员可以设置单个应用程序的默认运行时权限，如下所示：

步骤

1. 转至**应用** 。

2. 单击应用程序名称。
3. 单击**应用配置 > Android Enterprise**。
4. 单击**添加**或单击配置名称，以编辑现有配置。
5. 设置配置选项，例如名称、说明和限制。
6. 在运行时权限部分，单击**管理权限**。
7. 在显示的窗口中选择权限，并单击**选择**。
   仅列出适用于特定应用程序的危险权限以供选择。 危险权限的完整列表（例如，读取您的联系人，在设备上查找帐户，写入呼叫日志等）请参见：https://developer.android.com/guide/topics/permissions/requesting.html#perm-groups。
   - 仅当应用程序请求权限时才应用权限。
   - 如果用户以前接受或拒绝了权限，则不应用权限。

在"运行时权限"部分中，选择以下默认运行时权限之一：

- 默认/全局（默认选项）
- 自动授权
- 自动拒绝（谨慎使用）

在"分配本应用程序配置"部分中，选择以下分配选项之一：

- 每人都有应用
- 无人
- 自定义

单击**保存**。

10.10.6.5. 教育

许可证： Gold

适用于：监管的 iOS 9.3+

为领导者和成员配置 Apple 教育有效负载和课堂应用。 下表列出了教育设置：

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
配置类型	选择以下其中一种类型： • 领导者 • 成员
启用此配置	• 选择此选项，以将此配置应用到选定设备。 • 取消选择此选项，以将此配置从所有设备中移除（如果此前应用）。
分发	选择下列分配选项之一： • 所有设备 • 无设备 • 自定义

有关更多信息，请查看**如何创建配置**

10.10.6.6. 全局代理配置

许可证： Silver

全局代理配置可对设备进行设置，以将 HTTP 流量转发至代理服务器。 下表列出了全局代理设置：

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
类型	选择**手动**或**自动**。 如果选择**手动**，您需要代理服务器主机名和端口，以及登录该代理服务器的用户名和密码（可选）。 如果选择**自动**，您可以输入代理自动配置 (PAC) URL。
主机名和端口	如果选择了**手动**，输入该代理服务器的主机名和端口编号。
用户	（可选）用于访问代理服务器的用户名。*
密码	（可选）用于访问代理服务器的密码。
PAC URL	（可选）如果选择了**自动**，可输入定义代理配置的 PAC 文件的 URL。 如果将此设置留为空白，设备使用 Web 代理自动发现协议 (WPAD) 寻找代理。
如果 PAC 无法访问，则允许直接连接	（iOS 7 和更高版本）如果设备因为任何原因无法访问 PAC 文件，选择以允许直接连接。
允许旁路代理访问捕获网络	（iOS 7 和更高版本）选择以允许绕过代理，从而显示捕获网络的登录页面。

> 键入 $ 以查看此字段支持的变量列表（如果有）。

有关更多信息，请查看如何创建配置

10.10.6.7. 全局代理配置 (Android)

> 仅适用于处于设备所有者和 AOSP 模式中的 Android 设备。

全局代理配置可对设备进行设置，以将 HTTP 流量转发至代理服务器。

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 单击**配置**。
3. 点击 **+添加**。
4. 在搜索字段中输入**全局**，然后单击**全局代理**：
   将出现全局代理配置详细信息页面。
5. 在**名称**框中输入配置的名称。
6. 或者，您可以添加有关配置的一些描述。
7. 从**平台**列表中，选择 **Android**。 此时将显示**配置设置**部分。
8. 在类型下，选择**手动**或**自动**。
   - **手动**
     - 输入**主机名**（域名/IP 地址）和**端口**详细信息。
     - 在**添加排除项**下，您可以添加必须在排除列表下的多个主机名（域名/通配符）。
   - **自动**
     - 输入 PAC URL。
9. 单击**下一步**，以配置分配设置，然后单击**完成**。

10.10.6.8. LDAP 配置

LDAP 配置可设置对企业目录的访问。 下表列出了 LDAP 设置：

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
主机名	输入 LDAP 服务器的主机名。*
用户	输入用于访问 LDAP 帐户的用户名。*
密码	输入访问 LDAP 帐号的密码。
使用 SSL	如果您想要使用 SSL 连接至 LDAP 服务器，请选择此项。
搜索设置	至少输入一个帐号条目。 每个条目代表 LDAP 树中的一个节点，由此节点开始搜索。 单击“+”按钮以添加新条目，然后编辑该条目。 条目包含以下值： 说明：解释搜索设置的目的。 范围：**选择基本**、**子树**或**一级**以显示搜索范围。 **基本**仅表示节点级别，**子树**表示节点和所有子节点，**一级**表示节点和一个级别的子节点。 搜索基本：指定节点的概念路径（例如，ou=people、o=mycorp）。
每个 App VPN	**先决条件**：在 LDAP 配置中配置 Per-App VPN 前，配置 Tunnel 或任何 Per-App VPN 配置。 从下拉菜单中，选择预配置的 Per App VPN 配置。 **适用于**：iOS 14+
iOS 10+	
通信服务规则	选择要用来在 LDAP 系统内音频呼叫联系人的默认应用程序。

键入 $ 以查看此字段支持的变量列表（如果有）。

有关更多信息，请查看如何创建配置

10.10.6.9. macOS 服务器配置

使用配置的帐号类型和设置，macOS 服务器配置会定义 macOS 服务器帐号。 此配置允许用户在服务器上激活文件共享。

适用于： iOS 10+

配置 macOS 服务器

步骤

1. 转到**配置 > + 添加**。
2. 选择 **macOS 服务器**配置，以显示**创建 macOS 服务器配置**页面。
3. 输入配置的名称。
4. 输入描述。
5. 输入**端口名称**，以指定服务器地址。
6. 输入**用户名**，以指定用户的登录名。
7. （可选）为用户输入**密码**。
8. （可选）为账号输入**描述**。
9. （可选）在配置的账号下，输入要在为文档字段账号连接服务器时使用的**端口**号。 如果未指定端口号，则会使用默认端口号。
10. 单击**下一步**。
11. 选择此配置的分配水平。

10.10.6.10. Tunnel

Ivanti Tunnel 在 iOS、Android 和 Windows 设备上启用 VPN 功能。 Ivanti Tunnel 与统一端点管理 (UEM) 平台、Standalone Sentry 和 Access 交互，以安全地从企业网络外部访问企业资源。 企业资源可以位于本地或云端。 UEM 平台包括：Ivanti EPMM 和 Ivanti Neurons for MDM。

> 依应用程序配置已在Android Enterprise 设备中弃用。 需要使用应用程序目录中的 Ivanti Tunnel 托管配置。

关于 Ivanti Tunnel 配置

Ivanti Tunnel 的配置是在统一端点管理 (UEM) 平台中创建的。 Ivanti Tunnel 从 UEM 客户端接收配置。 Ivanti EPMM 的客户端是 Mobile@Work，Ivanti Neurons for MDM 的客户端是 Go。

最新文档

如需最新 Tunnel 说明，请访问产品文档。

- Tunnel for Android，请参阅 **Ivanti Tunnel for Android 指南**
- Tunnel for iOS，请参阅 **Ivanti Tunnel for iOS 指南**
- Tunnel for macOS，请参阅 **Ivanti Tunnel for macOS 指南**
- Windows Tunnel，请参阅 **Ivanti Tunnel for Windows 指南**

> Ivanti Tunnel for Windows 已被弃用，现已不受 Ivanti Neurons for MDM 支持。

10.10.6.11. 设置 AppTunnel

AppTunnel 通过在每个应用容器和企业网络间提供应用与应用会话安全来保护应用数据。

本部分包含以下主题：

- 设置 Sentry 使用带有证书的 AppTunnel{
- 上传 Sentry 证书
- 设置应用使用 AppTunnel
- 关于 AppTunnel 服务名称

设置 Sentry 使用带有证书的 AppTunnel

> 首次安装 Standalone Sentry 时，还会安装自签名证书。 Ivanti 强烈建议您将默认证书替换为公开受信任的第三方证书。

先决条件

- AppTunnel 取决于 Sentry 的最新支持版本。 在开始 AppTunnel 设置任务前，请完成 Sentry 安装。
- 如果您要使用 SCEP 身份：
  - 添加本地或外部证书颁发机构。 需要安装 Connector。
  - 添加应用身份证书配置。 这是您在配置 AppTunnel 时将使用的动态分配。

可以使用 X.509 证书配置 ActiveSync 和/或 AppTunnel 进行身份验证，以便使用分配给配置文件的 Sentry 服务器。

步骤

1. 转至**管理员 > Sentry**。
2. 单击 **+ 添加 Sentry 配置文件**。
3. 单击**带有证书的 ActiveSync 和/或 AppTunnel**。
4. 单击**下一步**。
5. 使用下表中的指导，以完成**全局设置**页面。

表格：管理员的全局设置 > Sentry	
设置	**采取何种措施**
名称	输入可识别此配置文件的名称。
描述	输入阐明此配置文件目的的说明。
外部主机名和端口	输入 Sentry 的主机名和端口。
设备 身份验证模式	
使用单个证书进行双因素身份验证	选择 使用单个证书进行身份验证。 如果您尚未上传证书，可在选定选项下方显示的区域中执行此操作。
选择证书	上传设备身份验证所需的组证书： 1. 单击**添加**。 将显示**添加证书**窗口。 2. 在**证书名称**字段中，键入证书的名称。 3. 键入保护 PKCS12 文件的密码。 4. 点击**选择文件**上传组证书。 请确保文件格式为 .p7b、.p12、.pfx、.pem、.der、.crt 或 .cer 文件。
启用证书吊销列表 (CRL)	选择以根据 CA 发布的证书吊销列表 (CRL) 验证设备显示的证书。
默认的未托管设备行为	
允许未托管设备接收电子邮件和数据	如果不想阻止不受 Ivanti Neurons for MDM 管理的设备访问数据，可选择此项。

6. 单击**下一步**。
7. 在 **Sentry 服务器配置**页面中，配置以下字段：
8. 单击**下一步**。

表格：管理员 > Sentry 的 Sentry 服务器配置	
设置	流程
侦听器协议	选择以下任何协议选项： • **仅限 HTTPS** • **仅限 HTTP** • **HTTPS 和 HTTP**
HTTPS 端口	输入 HTTPS 端口号。 如果将侦听器协议选择为“仅限 HTTP”，将不显示此字段。
HTTP 端口	输入 HTTP 端口号。 如果将侦听器协议选择为“仅限 HTTPS”，将不显示此字段。
Sentry TLS 服务器证书/密钥	
使用 Sentry 的自签名证书	选择以使用 Ivanti Neurons for MDM 服务创建的自签名证书，该证书作为此配置文件的一部分发送到 Sentry。 该证书用于 Sentry 和移动设备间的通信。
添加	上传身份验证所需的证书： 1. 单击**添加**。 将显示**添加证书**窗口。 只有取消选择**使用 Sentry 的自签名证书**选项后，才可以看到此选项。 2. 在**证书名称**字段中，键入证书的名称。 3. 键入保护 PKCS12 文件的密码。 4. 点击**选择文件**上传证书。 确保文件格式为 .p12 文件。 5. 单击**添加**。 Sentry TLS 服务器证书/密钥部分会显示所有上传的 Sentry TLS 服务器证书（包含从 Sentry 主页面和其他配置文件上传的证书）。 要选择身份验证所需的 TLS 证书，单击证书旁边的单选按钮。
添加第二个证书	选择以启用第二个证书。 一旦主证书过期，Sentry 会自动切换到保留证书，而无需管理员干预。 Tunnel 已经存储了这两个证书，并且可以匹配其中任何一个，从而确保不间断的连接。
协议	选择所需的入站和出站协议。
密码套件	用于与 Sentry 的 SSL 加密通信的密码。 通常首选强密码。 旧设备可能需要弱密码。 默认选择强密码。 选择您要使用的附加密码。 必须选择至少一个密码。

9. 添加 至少一个已显示的服务。
10. 单击**保存**。

在注册 Sentry 后，将显示在“未配置的 Sentry 服务器”部分的 Sentry 页面中。 要为 Sentry 分配配置文件，单击**操作**列中的**分配**。

上传 Sentry 证书

在创建 Sentry 配置文件时，Ivanti Neurons for MDM 会上传 TLS 服务器证书和组证书。 在 **Sentry 证书**部分中，您也可以从 **Sentry** 页面上传这些证书。

Ivanti Neurons 在上传时验证 Sentry 证书，根据证书中的条件返回以下类型的信息：

条件	信息类型
分支证书不包含任何证书颁发机构的链，或者上传的文件中没有证书颁发机构。	错误
没有可用的根证书颁发机构。	警告
根证书颁发机构未签发中间证书颁发机构的分支证书。	警告

Ivanti Neurons for MDM 还会根据本文中的规则进行验证。

步骤

1. 在 **TLS 服务器证书**部分中，单击**添加**。 将显示**添加证书**窗口。
2. 在**证书名称**字段中，键入证书的名称。
3. 键入保护 PKCS12 文件的密码。
4. 单击**选择文件**，以上传组证书。 请确保文件格式为 .p7b、.p12、.pfx、.pem、.der、.crt 或 .cer 文件。
5. 单击**添加**。 上传的证书会显示在表格中。
6. 要删除 TLS 服务器证书，单击**操作**列中的删除图标。

> 如果任何 Sentry 配置文件中使用了 TLS 服务器证书，则您将无法删除该证书。 如果执行删除操作，系统将显示错误消息。

添加组证书

步骤

1. 在**组证书**部分中，单击**添加**。 将显示**添加证书**窗口。
2. 在**证书名称**字段中，键入证书的名称。
3. 键入保护 PKCS12 文件的密码。
4. 单击**选择文件**，以上传组证书。 请确保文件格式为 .p7b、.p12、.pfx、.pem、.der、.crt 或 .cer 文件。
5. 单击**添加**。

要删除上传的组证书，单击**操作**列中的删除图标。

编辑 Sentry 根证书

管理员可以选择编辑 Sentry 根证书配置的分发。 也可以通过将配置委派给其他空间来向自定义空间管理员提供编辑权限。

1. 转至**配置**。
2. 搜索**Sentry 根证书**。
3. 点击“编辑”图标。
4. 选中与设备或设备组对应的复选框来分发证书。 或清除与设备或设备组对应的复选框。
5. 从“分发摘要”部分中选择以下适用的选项之一：
   - **不适用于其他空间**
   - **适用于其他空间中的设备**
6. （可选）点击复选框**允许空间管理员编辑分发**。
7. 单击**保存**。

8. 随即显示警告消息。 单击**是**进行确认。

设置应用使用 AppTunnel

如需最新 Sentry 说明，请访问产品文档并单击 Sentry。 选择适合您的 Sentry 版本的文档。

关于 AppTunnel 服务名称

AppTunnel 服务定义 AppConnect 应用程序所通过的后端服务。

有关最新说明，请访问产品文档并选择适合 **Sentry** 和 **AppConnect** 版本的文档。

10.10.6.12. Per-App VPN 配置

许可证：Silver

适用于：iOS、watchOS、visionOS 和 tvOS 设备

Per-App VPN 配置定义了以下特定应用的虚拟专用网络访问权限的设置：

- **Per-App VPN 设置**
- **Psec (Cisco)**
- **Cisco AnyConnect**
- **Juniper SSL**
- **NetMotion VPN**
- **F5 SSL**
- **SonicWALL 移动连接**
- **Aruba VIA**
- **自定义 SSL**
- **Palo Alto 网络全球保护**

> Per App VPN 配置取决于应用配置。 Per App VPN 配置将在应用配置设置过程中创建。 在删除或取消分发 Per App VPN 配置时，应用配置会因断开应用与网络连接出现故障。

分配配置

从 Ivanti Neurons for MDM 91 版本开始，全局管理员可以委派空间管理员来为所有设备和自定义分发选项编辑依应用程序 VPN 配置。 对于依应用程序 VPN 配置，可以视需要选择“允许在所有空间中提供此配置”选项。

> 分发更改仅适用于特定空间。 所有其他空间会继续继承默认空间分发设置。

根据适用情况，使用下表中的信息在字段中指定配置设置，然后分发配置：

有关详细信息，请参阅使用配置中的*分发配置*主题。

Per-App VPN 设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
连接类型	选择要配置的 VPN 类型。 其余设置取决于该选项。
按需启用 VPN	选择以对按需建立 VPN 的域和主机名使用该配置。
启用 iOS 规则 （如果选择“按需启用 VPN”，则适用。）	对于 iOS 和 macOS，您可以设置： • 允许或禁止连接的网络规则、允许或忽略的网络规则，以及评价为真的网络。 • 在需要时连接规则允许，或从未允许，评为真的网络连接。 对于网络规则，您可以指定以下参数类型： • DNS 域匹配 • DNS 服务器地址匹配 • SSID 匹配 • URL 字符串探针 • 接口类型匹配 对于连接规则，您可以指定以下参数类型： • DNS 域匹配 • DNS 服务器地址匹配 • SSID 匹配 • URL 字符串探针 • 接口类型匹配 • 域 • DNS 服务器 • URL 探针
已启用按需匹配应用	选择以按需启用 Per App VPN。
启用 5G 网络切片	选择连接到隧道的 **DNN**（网络供应商提供的数据网络名称），以便将隧道定位到特定的蜂窝切片 VPN。 选择**应用程序类别**（由网络提供商提供），确定要建立隧道的蜂窝切片类型。
域	
Safari 域 (iOS)	数组的条目必须指定域，该域会在 Safari 中触发 VPN 连接。 每个条目的格式是 www.apple.com。
iOS 14.0+ 和 macOS 11.0+	
关联域	指定一个或多个关联域。 与其中一个域中的服务器连接会与 Per-App VPN 关联。
已排除域	指定一个或多个排除域。 与其中一个域中的服务器连接会从 Per-App VPN 中排除。

设置	流程
iOS 13+ 和 macOS 10.15+	
邮件域	单击 **+ 添加**，以输入一个或多个将在邮件中触发此 VPN 连接的域。 每个条目的格式是 www.apple.com。
联系人域	单击 **+ 添加**，以输入一个或多个将在联系人中触发此 VPN 连接的域。 每个条目的格式是 www.apple.com。
日历域	单击 **+ 添加**，以输入一个或多个将在日历中触发此 VPN 连接的域。 每个条目的格式是 www.apple.com。
iOS 9 和更高版本	
提供商类型 (iOS 9+)	选择以下其中一个通道提供商： • 应用代理 - 应用层上的隧道流量。 有关应用代理提供商的概述，请查看 Apple 文档。 • 数据集通道 - IP 层上的隧道流量。 有关数据包隧道提供商的概述，请查看 Apple 文档。

IPsec (Cisco)

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
计算机身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
包括用户 PIN	选择此项提示用户输入 PIN。
代理设置	选择**手动**或**自动**以配置代理。 **如果您选择手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 **如果您选择自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

Cisco AnyConnect

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
组	输入要用于验证连接的组。
用户身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果选择**自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

Juniper SSL

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
领域	输入要用于验证连接的验证领域。
角色	输入要用于验证连接的验证角色。
用户身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果选择**自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

NetMotion VPN

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
用户身份验证	**证书**是要使用的用户身份验证方法。 以下字段可用： **凭据**：选择要使用的身份证书。 用户提供的证书仅支持 iOS 设备。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。 选择以下选项： • 启用按需 VPN - 添加建立按需 VPN 的域或主机名。 • 启用 iOS 规则。 • 已启用按需匹配应用。
Safari 域	单击 **+ 添加**，以添加 Safari 域。
提供商类型 (iOS 9.0+)	**数据包隧道**会默认选择为隧道提供商类型。 有关数据包隧道提供商的概述，请查看 Apple 文档。

F5 SSL

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
用户身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果选择**自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

SonicWALL 移动连接

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
登录组或域	输入要用于验证连接的登录组或域。
用户身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果选择**自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

Aruba VIA

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
用户身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果选择**自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

自定义 SSL

设置	流程
标识符	以反向 DNS 格式输入此自定义 SSL VPN 的标识符（例如 com.mycompany.myserver）。
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
自定义数据	输入定义该 VPN 的自定义数据的键值对。
用户身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果选择**自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。
(iOS 9.0+) 在主 VPN 和子 VPN 字典中包含 ProviderType	选择在生成 plist（预定义配置文件）时包含提供程序类型。
提供捆绑标识符	输入 VPN 提供商的捆绑标识符。 您可以使用不同的提供商捆绑标识符为同一个应用程序维护多个应用程序配置。

Palo Alto 网络全球保护

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐号。
自定义数据	输入定义该 VPN 的自定义数据的键值对。
用户身份验证	证书是用户身份验证方法。 选择要在**凭据**字段中使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果选择**自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

键入 $ 以查看此字段支持的变量列表（如果有）。

相关主题：

如何创建配置

10.10.6.13. 单点登录配置

Ivanti Neurons for MDM 使用可扩展 SSO 和可扩展 SSO Kerberos 配置启用可扩展单点登录 (SSO)。 实施需要身份提供商提供的应用扩展，例如 Microsoft Authenticator。 通过可扩展 SSO 实施，用户仅在访问企业资源时需要进行一次身份验证。 后续登录时，系统不会再提示用户进行身份验证。 有关预期身份提供程序设置的信息，请参阅**配置标识提供者**。

本部分包含以下主题：

- **单点登录帐户设置**
- **可扩展单点登录帐户设置**
- **可扩展单点登录 Kerberos 帐户设置**

单点登录帐户设置

适用于：

- iOS 7.0 至 Ivanti Neurons for MDM 支持的最新发布版本。
- visionOS 1.1 至 Ivanti Neurons for MDM 支持的最新发布版本。

使用以下设置，以为 iOS 设备中的任何托管应用和 Apple Safari 浏览器配置基于 Kerberos 的企业单点登录。

> 此配置需要 Tunnel 和 Sentry。 有关详细信息，请参阅 *Tunnel for iOS 指南*中的“使用 Kerberos 设置单点登录”。

设置	描述
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
用户名	输入 Kerberos 主体名称。
Kerberos 领域名称	输入 Kerberos 领域名称。
证书	**针对具备 Gold 证书的 iOS 8：**选择要使用的证书，以更新 Kerberos 凭据。
URL 前缀匹配	为使用此帐号在 HTTP 上进行 Kerberos 身份验证而必须匹配的 URL 前缀。
适用于 SSO 的允许列表应用	从 App Catalog 添加应用，将其加入允许列表，从而进行单点登录。 例如，输入“Safari”，以添加 Apple Safari。 如果使用此类配置未将应用加入允许列表进行单点登录，所有支持 iOS 单点登录的应用可以使用单点登录，包含内置 iOS 应用。

可扩展单点登录帐户设置

适用于：

- iOS 13.0 至 Ivanti Neurons for MDM 支持的最新发布版本。
- macOS 10.15 至 Ivanti Neurons for MDM 支持的最新发布版本。
- visionOS 1.1 至 Ivanti Neurons for MDM 支持的最新发布版本。

使用以下设置，以通过通用扩展类型配置单点登录扩展配置文件，从而使用各种身份验证方法为本机应用和网站启用单点登录。

> 在适用于 macOS 10.15.x 设备的用户渠道中推送配置时，可扩展单点登录无法正常工作。

设置	描述
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。

选择 SSO 类型	选择以下其中一种单点登录类型：
	• **凭据**
	  ◦ 输入一个或多个**主机**名或域名；此类名称可以通过应用扩展进行身份验证。 主机名或域名会以不区分大小写的方式进行匹配，所有已安装的可扩展单点登录负载的所有主机名/域名必须唯一。 以“.”开头的主机是通配符后缀，将匹配所有子域，否则主机必须为精确匹配项。
	  ◦ 输入**领域**名。 此值应使用大写字母正确表示。
	• **重定向**
	  ◦ 输入身份提供商的一个或多个 **URL** 前缀，应用扩展会对其执行单点登录。 URL 必须以 http:// 或 https:// 开头；方案和主机名会以不区分大小写地方式匹配；不允许查询参数和 URL 片段；所有已安装的可扩展单点登录负载的 URL 必须唯一。

扩展标识符	对于为已指定 URL 执行单点登录的应用扩展，输入捆绑标识符。
团队标识符	应用扩展的团队标识符。 此密钥在 macOS 中是必填项，并在其他位置忽略。
自定义数据	输入一个或多个自定义数据作为键值对。
身份验证方法（仅适用于 macOS 13+）	• 密码 • Secure Enclave 用户密钥
注册令牌	输入令牌。 选择任一身份验证方法后，都会启用此字段。
屏幕锁定行为（适用于 iOS 15.0+ 和 macOS 12.0+）	选择下列选项之一： • **取消**：屏幕锁定时，系统将取消身份验证请求。 • **不处理**：屏幕锁定时，身份验证请求将继续进行，无需 SSO。
被拒绝的捆绑标识符（适用于 iOS 15.0+ 和 macOS 12.0+）	对于不使用由此扩展提供的 SSO 的应用，添加多个捆绑标识符。 例如，*com.company.appname.www*。

适用范围：macOS 14.0 至 Ivanti Neurons for MDM 支持的最新发布版本。

设置	描述
账户显示名称	输入在通知和身份验证请求中显示的账户名称。
其他组	输入没有管理员访问权限的组的名称。
管理员组	输入具有管理员访问权限的组的名称。
身份验证方法	从下拉列表中选择一种身份验证方法： • 密码 • Secure Enclave 用户密钥 • 智能卡
授权组	输入组名称的授权权限。
启用授权	选中复选框可为管理员组、授权组或其他组启用授权提示。
启用登录时创建用户	选中复选框可在登录期间使用密码或智能卡作为身份验证方法创建新用户。
登录频率	系统完全登录而非完成刷新前所需的持续时间（以秒为单位）。 默认值为 64,800 秒（18 小时）。 最低值为 3600 秒（1 小时）。
新用户授权模式	从下拉列表中选择一种新用户的授权模式： • 标准：标准用户账户。 • 管理员：系统将账户添加到本地管理员组中。 • 组：系统自动将新用户分组到管理员组、授权组或其他组下。
令牌到用户映射	输入新用户的账户名和全名，以便为他们建立授权映射。
用户授权模式	从下拉列表中选择一种用户授权模式： • 标准：标准用户账户。 • 管理员：系统将账户添加到本地管理员组中。 • 组：系统自动将新用户分组到管理员组、授权组或其他组下。
使用共享设备密钥	选中复选框可为所有用户启用相同的登录和加密密钥。

适用范围：macOS 15.4 至 Ivanti Neurons for MDM 支持的最新发布版本。

设置	描述
允许设备标识符证明	选中复选框以在平台 SSO 认证中包含设备的 UDID 和序列号，从而允许对注册设备进行后端跟踪。

适用范围：macOS 14.0 至 Ivanti Neurons for MDM 支持的最新发布版本。

要查看可扩展单点登录账户设置，请在**身份验证方法**字段选择下拉选项中的**密码**。

设置	描述
FileVault 策略	启用政策以查看以下设置： • 尝试身份验证 • 需要身份验证 选中**需要身份验证**复选框以启用其他配置设置。 • 允许离线宽限期 • 允许身份验证宽限期
登录策略	启用政策以查看以下设置： • 尝试身份验证 • 需要身份验证 选中**需要身份验证**复选框以启用其他配置设置。 • 允许离线宽限期 • 允许身份验证宽限期
解锁策略	启用政策以查看以下设置： • 尝试身份验证 • 需要身份验证 选中**需要身份验证**复选框以启用其他配置设置。 • 允许离线宽限期 • 允许身份验证宽限期 • 允许 TouchID 或监视解锁
身份验证宽限期	输入选择一项策略后，可使用未注册本地账户的时间长度。 如果在一项策略中选中**允许身份验证宽限期**复选框，则字段会变为必填字段。
离线宽限期	输入成功完成平台 SSO 登录并选择一项策略后，可使用离线本地账户密码的时间长度。 如果在一项策略中选中**允许离线宽限期**复选框，则字段会变为必填字段。
非平台 SSO 账户	选择 **+ 添加**可输入不受 FileVault、登录或解锁策略约束的用户名列表。

可扩展单点登录 Kerberos 帐户设置

适用于：

- iOS 13.0 至 Ivanti Neurons for MDM 支持的最新发布版本。
- macOS 10.15 至 Ivanti Neurons for MDM 支持的最新发布版本。
- visionOS 1.1 至 Ivanti Neurons for MDM 支持的最新发布版本。

使用以下设置，以配置通过 Kerberos 扩展执行单点登录的应用扩展。

> 在适用于 macOS 10.15.x 设备的用户渠道中推送配置时，可扩展单点登录 Kerberos 无法正常工作。

设置	描述
基本设置	
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
用户名	输入 Kerberos 主体名称。
领域	输入 Kerberos 领域名称。
证书	选择用于续订 Kerberos 凭据的证书。
URL 前缀	为使用此帐号在 HTTP 上进行 Kerberos 身份验证而必须匹配的 URL 前缀。
高级设置	
允许自动登录	如果为假，不允许将密码保存到钥匙串。 默认情况下，此选项已启用。
延迟用户设置	如果为真，在管理员使用 app-sso 工具启用或收到 Kerberos 质询前，不会提示用户设置 Kerberos 扩展。 此选项适用于 macOS 11 到由 Ivanti Neurons for MDM 支持的最新版本。
需要用户状态	如果为真，需要用户提供触控 ID、面容 ID 或密码访问钥匙串条目。
监视凭据缓存	如果为假，将在下一次匹配 Kerberos 质询或网络状态变更时请求凭据。 如果凭据过期或缺少，将创建新凭据。 此选项适用于 macOS 11 到由 Ivanti Neurons for MDM 支持的最新版本。 默认情况下，此选项已启用。
缓存名称	输入要使用的 Kerberos 缓存的通用安全服务 (GSS) 名称。 此选项现已停用。
域领域映射	输入领域的名称作为键。 该值是映射到领域的 DNS 后缀数组。 单击 **+ 添加**，以添加一个或多个键-值对。
默认领域	如有多个 Kerberos 扩展配置，此属性会指定默认领域。
使用站点自动发现	如果为假，Kerberos 扩展不会自动使用 LDAP 和 DNS，以确定 AD 站点名称。 默认情况下，此选项已启用。
站点代码	输入 Kerberos 扩展应使用的 Active Directory 站点的名称。
复制时间	在 Active Directory 域中输入复制变更所需的时间（以秒为单位）。 在变更后检查密码使用期限时，Kerberos 扩展将使用此内容。 此选项适用于 macOS 11 到由 Ivanti Neurons for MDM 支持的最新版本。 此选项现已停用。
凭据捆绑 ID ACL	单击 **+ 添加**，以添加允许访问票证授予票证 (TGT) 进行身份验证的捆绑 ID 的列表。
在捆绑 ID ACL 中包含受管应用	如果为真，Kerberos 扩展将仅允许受管应用访问和使用凭据。 如果已指定，这是对凭据捆绑 ID ACL 的补充。 此选项适用于 iOS 14 或 Ivanti Neurons for MDM 受支持的更新的版本。
在捆绑的 ID ACL 中包含 Kerberos 应用	如果为 true，Kerberos 扩展允许包括 Ticket Viewer 和 klist 在内的标准 Kerberos 实用程序访问并使用凭据。 在 macOS 12 和更高版本中可用。

设置	描述
自定义用户名标签	输入 Kerberos 扩展中使用的自定义用户名标签，而不是“用户名”，例如，“公司 ID”。此选项适用于 macOS 11 到由 Ivanti Neurons for MDM 支持的最新版本。
帮助文本	输入在 Kerberos 登录窗口底部向用户显示的文本。 可用于显示帮助信息或免责声明文本。 此选项适用于 iOS 14 和 macOS 11 到由 Ivanti Neurons for MDM 支持的最新版本。
凭据使用模式	此设置会影响其他进程如何使用 Kerberos 扩展凭据。 使用以下其中一项： • 始终（默认）- 如果服务主体名称 (SPN) 与 Kerberos 扩展主机数组匹配，将始终使用扩展凭据。 如果调用应用未在 credentialBundleIDACL 中，将不使用该凭据。 • 在未指定时 - 在调用方未指定其他凭据并且 SPN 与 Kerberos 扩展主机数组匹配时，才使用该凭据。 如果调用应用未在 credentialBundleIDACL 中，将不使用该凭据。 • Kerberos 默认值 - 选择凭据的默认 Kerberos 进程；通常使用默认 Kerberos 凭据。 这与关闭此功能相同。（可选）选择**需要适用于 LDAP 的 TLS**。
首选密钥分发中心	添加首选密钥分发中心。 单击 **+ 添加**，添加首选 KDC。
	允许平台 SSO 身份验证回退 - 如果为 True 且“使用平台 SSO TGT”也为 True，则允许用户手动登录。 适用于 macOS 13 及更高版本
	仅执行 Kerberos - 如果为 True，则 Kerberos 扩展程序仅会处理 Kerberos 请求。 适用于 macOS 13 及更高版本。 **使用平台 SSO TGT** - 如果为 True，此配置将使用来自平台 SSO 的 TGT，而不是请求新的 TGT。 适用于 macOS 13 及更高版本。
配置切换到密码模式	如果为 True，允许用户将用户界面切换为“密码”模式。 适用于 macOS 15 及更高版本。
配置切换到智能卡模式	如果为 True，允许用户将用户界面切换到“智能卡”模式。 适用于 macOS 15 及更高版本。
配置以智能卡模式启动	如果为 True，用户界面在“智能卡”模式下启动。 适用于 macOS 15 及更高版本。
身份颁发者自动选择过滤器	筛选可用智能卡的列表。 适用于 macOS 15 及更高版本。
密码设置	
允许密码更改	如果为假，禁用密码更改。 此选项适用于 macOS 10.15 到由 Ivanti Neurons for MDM 支持的最新版本。 默认情况下，此选项已启用。
密码更改 URL	输入在用户发起密码更改时将在用户的默认 Web 浏览器中启动的 URL。 此选项适用于 macOS 10.15 到由 Ivanti Neurons for MDM 支持的最新版本。
允许密码复杂度	如果为 true，密码必须满足 Active Directory 对“复杂”的定义。此选项适用于 macOS 10.15 到由 Ivanti Neurons for MDM 支持的最新版本。

设置	描述
最低密码长度	输入域中密码的最小长度（以字符为单位）。 此选项适用于 macOS 10.15 到由 Ivanti Neurons for MDM 支持的最新版本。
密码到期通知	输入向用户发送密码到期通知之前的天数。 此选项适用于 macOS 10.15 到由 Ivanti Neurons for MDM 支持的最新版本。 默认值为 15 天。
密码过期替换	输入以在此域上使用密码的天数。 对于大部分域，这可以自动计算。 此选项适用于 macOS 10.15 到由 Ivanti Neurons for MDM 支持的最新版本。 （现已弃用此选项）
密码必填文本	输入域的密码要求的文本版本。 仅在未指定 pwReqComplexity 或 pwReqLength 时使用。 此选项适用于 macOS 10.15 到由 Ivanti Neurons for MDM 支持的最新版本。
密码历史计数	输入无法在此域中重复使用的先前密码的数量。 此选项适用于 macOS 10.15 到由 Ivanti Neurons for MDM 支持的最新版本。
密码最小期限	输入在此域中更改密码前的最小期限（以天为单位）。 此选项适用于 macOS 10.15 到由 Ivanti Neurons for MDM 支持的最新版本。
允许同步本地密码	如果为假，禁用密码同步。 如果用户使用移动帐户登录，将不支持此操作。 此选项适用于 macOS 10.15 到由 Ivanti Neurons for MDM 支持的最新版本。
密码要求 RTF 数据	域的密码要求的 RTF 文件格式版本。 适用于 macOS 15 及更高版本。 仅在未指定 pwReqComplexity 或 pwReqLength 时使用。

有关更多信息，请查看**如何创建配置**

10.10.6.14. 网络中继配置

Ivanti Neurons for MDM 可启用负载的网络中继配置，方便用于配置设备或应用程序的中继设置，而无需 VPN 或隧道来访问私有资源。

适用于

- iOS 17.0 至 Ivanti Neurons for MDM 支持的最新发布版本。
- macOS 14 至 Ivanti Neurons for MDM 支持的最新发布版本。
- visionOS 1.1 至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**网络中继**配置。
3. 根据下表配置**网络中继**设置：

设置	描述
名称	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
HTTP/3 中继 URL	指定用作此配置的 HTTP 字段值的 URL 值。 包含 HTTP/2 中继 URL 或 HTTP/3 中继 URL，或者同时包含两者。
HTTP/2 中继 URL	指定用作此配置的 HTTP 字段值的 URL 值。 包含 HTTP/2 中继 URL 或 HTTP/3 中继 URL，或者同时包含两者。
其他 HTTP 标头字段	为相应的标头字段名称指定 HTTP 标头字段值。
证书	从下拉列表中选择您已创建的其中一个身份证书。
原始公钥	指定原始公钥，以在网络连接期间对服务器进行身份验证。
+ 添加	选择**+ 添加**以添加多个网络中继配置。
匹配域	指定域列表，以确定要通过“中继”中的服务器路由哪些连接。
排除域	指定域列表，以确定要避免通过“中继”中的服务器进行哪些连接。
匹配 FQDN（在 iOS 18.4+ 和 macOS 15.4+ 设备上受支持）	指定应通过中继中包含的服务器路由的完全限定域名 (FQDN)（也称为主机名）列表。 任何与此确切 FQDN 或主机名匹配的连接都将使用中继。 如果没有列出 FQDN 和“MatchDomains”，则所有域的流量（与排除的域或排除的 FQDN 匹配的除外）都将路由到中继服务器。
排除 FQDN（在 iOS 18.4+ 和 macOS 15.4+ 设备上受支持）	指定**不应**通过中继中包含的服务器路由的完全限定域名 (FQDN)（也称为主机名）列表。 任何与 FQDN 完全匹配的连接都不会使用中继服务器。 当还指定了“MatchDomains”时，“ExcludedFQDNs”中列出的任何 FQDN 都应该是至少一个 MatchDomain 的子域。 否则，它不会有任何效果。

4. 单击**下一步**，配置分配设置。
5. 选择其中一个分发选项来设置**网络中继**配置。 有关配置分发选项的详细信息，请参阅使用配置。
6. 单击**完成**。

10.10.6.15. iOS 的多用户安全登录

通过多用户 Web 剪辑，用户可以登录和注销在 Ivanti Neurons for MDM 中注册的 iOS 设备。 在用户首次登录时，与该用户关联的配置文件、应用和配置会推送到设备。 在完成工作时，用户可以打开 Web 剪辑并选择“注销”功能；只要配置和应用未分发到无人用户，此操作会将设备分配到无人用户，并移除与初始登录用户关联的配置文件、应用和配置。 在注销后，Web 剪辑会重置，以便下一个用户登录并收到自定义配置、应用和策略。 设备监督不需要使用多用户安全登录功能。 请查看支持知识库文章 **Ivanti Neurons for MDM：适用于 iOS 的多用户安全登录**，以深入了解多用户安全登录功能。

适用于：iOS 设备（不适用于用户注册的设备）

本部分包含以下主题：

- 支持的凭据
- 了解无人用户
- 登录设备
- 正在注销设备

支持的凭据

只有使用用户名和密码，才可以登录多用户安全 Web 剪辑。 多用户安全 Web 剪辑不支持基于 PIN 的注册。

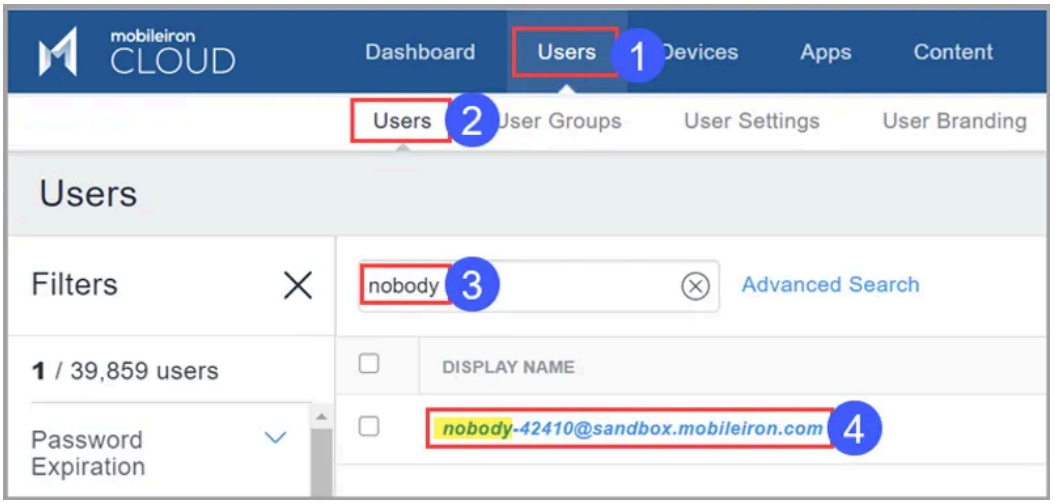
步骤

1. 转至**配置**。
2. 单击**适用于 iOS 的多用户安全登录**。 如果包含多个配置页面，您可能需要使用搜索功能进行查找。 通过选择 **+ 添加**，此配置不可访问。
3. 单击**编辑分发**或关联图标，以将网络剪辑分发到适当设备组。
   
   如果您要将其分发到用户组，您可以创建与用户组绑定的动态设备组。
4. 选择以下其中一个分发选项，并记住您必须始终将网络剪辑分发到无人用户或与无人用户关联的设备组。 默认情况下，不会出现此情况，因此请确保您将其分发到无人用户。
   - 所有设备
   - 无设备（默认）
   - 自定义

单击**保存**。

了解无人用户

在通过 Web 剪辑注销设备时，该设备仍将通过 Ivanti Neurons for MDM 注册到名为“无人用户”的特殊用户。 如果您要在用户注销时将应用和配置从设备中移除，您必须确保这些应用和配置未分发到无人用户。 如果您想要设备保留在用户注销安全登录 Web 剪辑时的特定配置，例如 Wi-Fi，您必须确保这些配置也分发到无人用户。



这表示，您必须留意收到应用和配置的用户组和设备组。 如果您将应用分发到每个人，并且想要在用户注销设备时移除，最佳实践是创建不包含无人用户的用户组。 凭借自定义属性，更轻松地创建一个“多用户”用户组，以及另一个仅包含无人用户的用户组。 您可以从“管理员 > 系统 > 属性”中创建名为“多用户所有者”的用户属性，然后将“是”或“真”值分配到无人用户。 然后，根据属性值，您可以创建用户组和设备组。

登录设备

用户可以登录 iOS 设备，并为自己分配设备。 在登录后，所有相关应用、策略、配置和证书都将推送到设备。

> 出于安全原因，iDP 用户每次登录时都必须重新进行身份验证，即使他们已经登录设备。

注销设备

用户可在使用后注销他/她的 iOS 设备。 在注销后，应用、策略、配置和证书将从设备中移除，并使设备处于用户登录前的状态。 然后，设备将可让其他用户登录。

> 从多用户 Web 剪辑注销之前，先从所有 Microsoft 应用程序注销。

有关详细信息，请参阅多用户登录品牌

10.10.6.16. Android APN 设置配置

通过 Android APN 设置配置，您可以在公用网络上设置设备所需的接入点名称 (APN) 设置。 此配置适用于 Android Enterprise 工作托管设备和带有公司拥有设备上的工作配置文件的托管设备（在 Android 版本 9.0 或支持的更新版本上）。

步骤

1. 转到**配置 > + 添加**。
2. 选择 **Android APN 设置**配置。
3. 输入配置的名称。
4. 输入描述。
5. 在配置设置部分，配置以下选项：
6. 单击**下一步**。

设置	说明
条目名称	键入接入点设置的名称。
接入点名称	键入接入点的名称。
接入点类型	从以下选项中，选择接入点的类型： • **默认** • **DUN** • **IMS** • **紧急** • MMS • **HIPRI** • **CBS** • **MCX** • **SUPL** • **FOTA** • **IA**
MVNO 类型	从以下选项中，选择移动虚拟网络运营商的类型： • **无** • **SPN** • **IMSI** • **GID** • **ICCID**
Bearer	从以下选项中，选择用于数据传输的持有者服务的类型： • **1xRTT** • **CDMA** • **EDGE** • **EHRPO** • **EVDO** • **EVDO A** • **EVDO B** • **GPRS** • **GSM** • **HSDPA** • **HASP** • **HSPAP** • **HSUPA** • **IDEN**

设置	说明
	• **IWLAN** • **LTE** • **NR** • **TD_SCDMA** • **UMTS**
APN 协议	选择 APN 所需的 APN 协议。 以下是可用选项： • **无** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP**（点到点协议） • **非结构化**
APN 漫游协议	选择 APN 所需的 APN 漫游协议。 以下是可用选项： • **无** • **IPV4** • **IPV6** • **IPV4/IPV6** • **NON_IP** • **PPP**（点到点协议） • **非结构化**
启用/禁用 APN	打开 APN 配置。
运营商 ID	输入运营商 ID 的数值。
身份验证类型	从以下选项中，选择身份验证协议的类型： • **无** • **PAP**（密码身份验证协议） • **CHAP**（质询握手身份验证协议） • **PAP 或 CHAP**
用户名	输入登录用户名。
密码	输入登录密码。
确认密码	重新输入密码进行确认。
端口号	输入端口号（介于 1 至 65535 之间的数值）。
代理地址	键入代理地址。

设置	说明
移动国家/地区代码	输入移动国家/地区代码。
移动网络代码	输入移动网络代码。
MMS 代理地址	键入 MMS 代理地址。
MMS 端口号	输入 MMS 端口号（介于 1 至 65535 的数值）
MMS 服务器地址 (mmsc)	键入 MMS 服务器地址

7. 选择下列分配选项之一：
8. 单击**完成**。

- **所有设备**
- 无设备（默认）
- **自定义**

> 如果设备存在具有这些值的现有 APN 配置，将无法为以下字段添加具有相同值的其他 APN 配置：

- 移动国家/地区代码
- 移动网络代码
- 接入点名称
- 代理地址
- 端口号
- MMS 代理地址
- MMS 端口号
- MMS 服务器地址
- 启用/禁用 APN
- MVNO 类型
- APN 协议
- APN 漫游协议

如果已经在设备中手动或由网络运营商配置，Android APN 设置配置将覆盖 APN 设置。

10.10.6.17. VPN 配置

适用于：

- Android（对 Android Enterprise 设备已停用。 需要使用应用程序目录中特定 VPN 的托管配置。）
- Windows
- iOS
- macOS
- tvOS
- visionOS

VPN 配置定义虚拟专用网络访问的设置。

> 此配置支持带自定义分发选项的委派。 有关详细信息，请参阅使用配置中的*分发配置*主题。

步骤

1. 转到**配置** > **+ 添加**。
2. 选择 **VPN** 配置。
3. 输入配置的**名称**。
4. 输入描述。
5. 按照以下描述，配置 VPN 设置。
6. （仅限 iOS 9.0+）在匹配域部分中，单击 **+ 添加**，以输入一个或多个匹配域（例如：company.com）。 在域是其中一个指定域时，使用代理连接。
7. 单击**下一步**。
8. （仅 macOS）在“分发”页面中，选择以下其中一个分发选项：
   - 设备渠道 - 配置对设备中的所有用户有效，即常见选项。
   - 用户渠道 - 配置仅对设备中目前注册的用户有效。
9. 选择此配置的剩余分发选项。
10. 单击**完成**。

VPN 设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
连接类型	选择要配置的 VPN 类型。 其余设置取决于该选项。

协议及其设置如下所示：

- L2TP（Ivanti Go 不支持）

- **PPTP**（Ivanti Go 不支持）
- **IPsec (Cisco)**（Ivanti Go 不支持）
- **Cisco AnyConnect**（Ivanti Go 支持）
- **Juniper SSL**（Ivanti Go 不支持）
- **NetMotion VPN**（Ivanti Go 不支持）
- Pulse Secure（Ivanti Go 支持）
- **F5 SSL**（Ivanti Go 不支持）
- **SonicWALL Mobile Connect**（Ivanti Go 不支持）
- **Aruba VIA**（Ivanti Go 不支持）
- **自定义 SSL**（Ivanti Go 不支持）
- **Palo Alto Networks GlobalProtect**（Ivanti Go 支持）
- **KEv2（仅限 Windows）**（Ivanti Go 不支持）
- **IKEv2**（Ivanti Go 不支持）

L2TP

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
用户身份验证	选择要使用的身份验证方法：**密码**或**RSA SecurID**。
共享密钥	如果初始化连接需要一个共享秘密通行码，则输入共享秘密通行码。
发送所有流量	选择此选项，将此连接用于所有网络流量。 此选项可防止数据泄露，尤其是在公用网络中。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

PPTP

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
用户身份验证	选择要使用的身份验证方法：**密码**或**RSA SecurID**。
加密级别	选择用于连接的数据加密的级别：**无**、**自动**、或**最高（128 位）**。
发送所有流量	选择此选项，将此连接用于所有网络流量。 此选项可防止数据泄露，尤其是在公用网络中。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

IPsec (Cisco)

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
计算机身份验证	选择要使用的身份验证方法：**共享密码/组名**或**证书**。
组名称	共享密码/组名身份验证。 指定要使用的组名。 如果使用混合身份验证，字符串必须以 â€œ[hybrid]â€ 结尾。
共享密钥	共享密码/组名身份验证。 输入共享秘密通行码。
使用混合身份验证	共享密码/组名身份验证。 选择此项可指定混合身份验证，例如，服务器提供证书，客户端提供预共享密钥。
提示输入密码	共享密码/组名身份验证。 指定连接时是否要提示用户输入密码。
凭据	*证书身份验证* 选择要使用的身份证书。
包括用户 PIN	*证书身份验证* 选择此项提示用户输入 PIN。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

Cisco AnyConnect

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
组	输入要用于验证连接的组。
用户身份验证	选择要使用的用户身份验证方法：**密码**或**证书**。 如果您选择**证书**，则以下字段可用： **凭据**：选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

Juniper SSL

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
领域	输入要用于验证连接的验证领域。
角色	输入要用于验证连接的验证角色。
用户身份验证	选择要使用的用户身份验证方法：**密码**或**证书**。 如果您选择**证书**，则以下字段可用： **凭据**：选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

NetMotion VPN

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
用户身份验证	选择要使用的用户身份验证方法：**密码**或**证书**。 如果您选择**证书**，则以下字段可用： **凭据**：选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

F5 SSL

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐号。
用户身份验证	输入要使用的用户身份验证方法：**密码**或**证书**。 如果您选择**证书**，则以下字段可用： **凭据**：选择要使用的身份证书。
代理设置	选择手动配置代理还是自动配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

SonicWALL Mobile Connect

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
登录组或域	输入要用于验证连接的登录组或域。
用户身份验证	选择要使用的用户身份验证方法：**密码**或**证书**。 如果您选择证书，则以下字段可用： **凭据**：选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

Aruba VIA

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
用户身份验证	选择要使用的用户身份验证方法：**密码**或**证书**。 如果您选择**证书**，则以下字段可用： **凭据**：选择要使用的身份证书。
代理设置	选择手动配置代理还是自动配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

自定义 SSL

设置	流程
标识符	以反向 DNS 格式输入此自定义 SSL VPN 的标识符（例如 com.mycompany.myserver）。
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
自定义数据	输入定义该 VPN 的自定义数据的键值对。
用户身份验证	选择要使用的用户身份验证方法：**密码**或**证书**。 如果您选择证书，则以下字段可用： **凭据**：选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

Palo Alto Networks GlobalProtect

> 不适用于 Android 设备。

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐号。
自定义数据	输入定义该 VPN 的自定义数据的键值对。
用户身份验证	选择要使用的用户身份验证方法：**密码**或**证书**。 如果您选择证书，则以下字段可用： **凭据**：选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

IKEv2（仅 Windows）

设置	采取何种措施
服务器	输入 VPN 服务器的主机名或 IP 地址。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

IKEv2

设置	采取何种措施
服务器	输入 VPN 服务器的主机名或 IP 地址。
本地标识符	采用下列格式之一的 IKEv2 客户端标识符： • FQDN • UserFQDN • 地址 • ASN1DN
远程标识符	采用下列格式之一的远程标识符： • FQDN • UserFQDN • 地址 • ASN1DN
计算机身份验证	只有未选择**启用 EAP**时可用。 选择下列选项之一： • 证书 • 共享密钥
EAP 身份验证	只有选择**启用 EAP**时可用。 选择下列选项之一： • 证书 • 用户名/密码
共享密钥	仅当选择共享密钥进行计算机身份验证时可用。 输入用于连接的共享密钥。
凭据	仅当选择证书进行计算机身份验证时可用。 选择要使用的证书。 将发送此证书，进行 IKE 客户端身份验证。 如果使用扩展的身份验证，此证书可用于 EAP-TLS。
启用 EAP	选择此项可启用扩展的身份验证。
账户	仅当选择用户名/密码进行 EAP 身份验证时可用。 输入 VPN 服务器的帐号 ID。
密码	仅当选择用户名/密码进行 EAP 身份验证时可用。 输入 VPN 服务器的密码。
对等体存活检测间隔	选择下列选项之一： • 无（禁用） • 低（每 1 小时发送一次 keepalive） • 中（每 30 分钟发送一次 keepalive） • 高（每 10 分钟发送一次 keepalive）
服务器证书发行方一般名称	（可选）- 服务器证书颁发机构的通用名称，使 IKE 服务器根据证书颁发机构向服务器发送证书请求。
服务器证书一般名称	（可选）- 服务器证书的通用名称，用于验证 IKEv2 服务器发送的证书。

设置	采取何种措施
使用 IP4 和 IP6 子网属性	（可选）选择使用 IP4 和 IP6 子网属性。
启用 IKEv2 移动性和多宿主协议 (MOBIKE)	（可选）默认设置为 0。 MOBIKE（当连接到 Wi-Fi 以及拥有多个 IP 地址的蜂窝链接时，支持多宿主移动设备的能力）已启用。 默认为启用状态。 设置为 1 以禁用 MOBIKE。
启用完美正向加密 (PFS)	（可选）设置为 1 时，会为 IKEv2 连接启用 PFS。 默认设置为 0。
启用 IKEv2 重定向	（可选）默认设置为 0。 如果接收到服务器的重定向请求，将重定向 IKEv2 连接。 默认为启用状态。 设置为 1，以禁用 IKEv2 重定向。
启用 NAT Keepalive	启用网络地址转换保持连接，以防止在 IKE 对等体之间存在 NAT 时在没有任何流量的情况下删除 NAT 条目。
NAT 保持连接间隔	如果启用了 NAT Keepalive，则此项是将为设备发送 Keepalive 数据包的时间（以秒为单位）。
PPK	输入支持 RFC 8784 的 VPN 服务器的后量子预共享密钥 (PPK)。 如果此密钥存在，则必须要有 PPK 标识符。
PPK 标识符	输入 PPK 标识符。
强制要求 PPK	选择下列下拉选项之一： • **强制**：如果服务器支持 RFC 8784 或接受 PPK 标识符中指定的 PPK 标识符，则 VPN 连接将建立成功。 • **非强制**：如果服务器不支持 RFC 8784 或不接受 PPK 标识符中指定的 PPK 标识符，则无法建立 VPN 连接。
加密算法	选择下列选项之一： • **DES** • **3DES** • **AES-128** • **AES-256**（默认） • **AES-128 GCM** • **AES-256 GCM**
完整性算法	选择下列选项之一： • **SHA2-256**（默认） • **SHA2-384** • **SHA2-512**
迪菲-赫尔曼分组	选择下列选项之一： • **1** • **2**（默认） • **5** • **14** • **15**

设置	采取何种措施
	• **16** • **17** • **18**
以分钟为单位的生存期	输入以分钟为单位的 SA 使用时间（密钥更新间隔）。 有效值为 10 到 1440。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

*键入 $ 查看此字段支持的变量列表（如果有）。

有关更多信息，请查看如何创建配置

10.10.6.18. 按需 VPN

适用于：iOS+ 设备

按需 VPN 配置可根据域、主机名等设置 VPN 服务器的访问权。

按需 VPN 设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
连接类型 按需启用 VPN	选择要配置的 VPN 类型。 其余设置取决于该选项。 选择以对按需建立 VPN 的域和主机名使用该配置。
启用 iOS 规则 （如果选择“按需启用 VPN”，则适用。） 提供商类型 (iOS 9+)	对于 iOS 和 macOS，您可以设置： • 允许或禁止连接的网络规则、允许或忽略的网络规则，以及评为真的网络。 • 在需要时连接规则允许，或从未允许，评为真的网络连接。 对于网络规则，您可以指定以下参数类型： • DNS 域匹配 • DNS 服务器地址匹配 • SSID 匹配 • URL 字符串探针 • 接口类型匹配 对于连接规则，您可以指定以下参数类型： • DNS 域匹配 • DNS 服务器地址匹配 • SSID 匹配 • URL 字符串探针 • 接口类型匹配 • 域名 • DNS 服务器 • URL 探针 选择以下其中一个通道提供商： • 应用代理 - 应用层上的隧道流量。 有关应用代理提供商的概述，请查看 Apple 文档。 • 数据集通道 - IP 层上的隧道流量。 有关数据包隧道提供商的概述，请查看 Apple 文档。
EnforceRoutes	启用后，VPN 的非默认路由会覆盖任何本地定义的路由。 • 如果启用 IncludeAllNetworks，系统会忽略 EnforceRoutes 设置 • 在 iOS 14.2 和更高版本中可用。
ExcludeLocalNetworks	如果同时启用 IncludeAllNetworks，则所有本地网络流量都会路由到 VPN 之外。
IncludeAllNetworks	启用后，系统会通过 VPN 路由所有流量。

协议及其设置如下所示：

- IPsec (Cisco)

- Cisco AnyConnect
- Juniper SSL
- NetMotion VPN
- F5 SSL
- SonicWALL Mobile Connect
- Aruba VIA
- 自定义 SSL
- Palo Alto Networks GlobalProtect

IPsec (Cisco)

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
计算机身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
包括用户 PIN	选择此项提示用户输入 PIN。
代理设置	选择**手动**或**自动**以配置代理。 **如果您选择手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 **如果您选择自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

Cisco AnyConnect

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
组	输入要用于验证连接的组。
用户身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 **如果您选择手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 **如果您选择自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

Juniper SSL

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
领域	输入要用于验证连接的验证领域。
角色	输入要用于验证连接的验证角色。
用户身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 **如果您选择手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 **如果您选择自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

NetMotion VPN

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
用户身份验证	证书是用户身份验证方法。 **凭据**：选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 如果您选择**自动**，则以下附加字段可用： **代理服务器 URL**：输入代理的完全限定的 URL。

F5 SSL

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
用户身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 **如果您选择手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 **如果您选择自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

SonicWALL Mobile Connect

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
登录组或域	输入要用于验证连接的登录组或域。
用户身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 **如果您选择手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 **如果您选择自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

Aruba VIA

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
用户身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 **如果您选择手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 **如果您选择自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

自定义 SSL

设置	流程
标识符	以反向 DNS 格式输入此自定义 SSL VPN 的标识符（例如 com.mycompany.myserver）。
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐户。*
自定义数据	输入定义该 VPN 的自定义数据的键值对。
用户身份验证	仅支持证书身份验证。
凭据	选择要使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 **如果您选择手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 **如果您选择自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

Palo Alto Networks GlobalProtect

设置	流程
服务器	输入 VPN 服务器的 IP 地址或主机名。
账户	输入要用于验证连接的用户帐号。
自定义数据	输入定义该 VPN 的自定义数据的键值对。
用户身份验证	证书是用户身份验证方法。 选择要在**凭据**字段中使用的身份证书。
代理设置	选择**手动**或**自动**以配置代理。 **如果您选择手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 **如果您选择自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。

键入 $ 以查看此字段支持的变量列表（如果有）。

有关更多信息，请查看如何创建配置

10.10.6.19. Wi-Fi 配置

适用于：

- Android
- Windows
- iOS
- macOS
- watchOS
- visionOS
- tvOS

本部分包含以下主题：

Wi-Fi 设置

- **WEP、WPA/WPA2/WPA3、任何（个人）设置**
- **WEP 企业、WPA/WPA2/WPA3 企业、任何（企业）设置**
- **iOS、macOS 和 visionOS**

Wi-Fi 设置

Wi-Fi 配置可设置对无线网线的访问。

> 用户可以修改设备上的某些 WiFi 设置。 但是，MDM 服务器可能接收或不接收基于设备 OS 的更改信息。 因此，配置将不会自动重新推送到设备，以使用服务器上的配置覆盖设备上的配置。

> 此配置支持带自定义分发选项的委派。 有关详细信息，请参阅使用配置中的*分发配置*主题。

> 某些特定版本的 Android 设备可能需要管理员输入域和其他信息才能连接到 TLS、TTLS、PEAP 等 (WPA2) 网络。 建议先确保在选定的设备上对 Wi-Fi 配置进行更改，然后再对更多设备进行更改。

> 在早于 94 的任何 Ivanti Neurons for MDM 版本上注册的 Android 14.x 设备的配置将处于“等待安装”状态。 当将 Ivanti Neurons for MDM 升级至 94 而不编辑 Wi-Fi 配置时，配置将保持为“等待安装”状态。 必须启用 EAP_PEAP 的“域”字段并更新配置中的域和证书，以将状态更新为“已安装”。

步骤

1. 转到**配置** > **+ 添加**。
2. 选择 **Wi-Fi** 配置。
3. 输入配置的**名称**。
4. 输入描述。
5. 按照以下描述，配置 Wi-Fi 设置。
6. 单击**下一步**。

7. （仅 macOS）在“分发”页面中，选择以下其中一个分发选项：
    - 设备渠道 - 配置对设备中的所有用户有效，即常见选项。
    - 用户渠道 - 配置仅对设备中目前注册的用户有效。
8. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义。
9. 单击**完成**。

下表列出了 Wi-Fi 设置：

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
服务集标识符(SSID) 自动加入 隐藏的网络	输入应用这些设置的无线网络名称。 该字段区分大小写。 如果设备可自动加入相应的 Wi-Fi 网络则选择该选项。 如果未选择该选项，设备用户必须点击设备上的网络名称以加入该网络。 如果该网络访问未广播，则选择该选项。
禁用强制网络检测(iOS 10+)	管理员可以启用或禁用 Wi-Fi 强制绕过模式。 Apple 检测到存在强制门户网站时，它会打开登录屏幕，请求访问。 您可以禁用强制门户网站检测，要求用户手动启动 Web 浏览器，这会触发强制网络的门户网站登录。 该新的设置在 ISE 强制门户网站阻止登录屏幕弹出（导致用户认为其未连接的设备实际上已经连接到 Internet）时非常有用。
代理设置	选择**手动**或**自动**以配置代理。 如果您选择**手动**，则以下附加字段可用： • **服务器和端口**：输入代理服务器的网络地址和端口号。* • **身份验证**：如果连接代理需要用户名，则输入一个有效用户名。* • **密码**：如果连接代理需要密码，则输入一个有效密码。 要移除添加的主机名，单击“减号”图标。 如果您选择**自动**，则以下附加字段可用： • **代理服务器 URL**：输入代理的完全限定的 URL。
安全类型	选择访问网络所需的安全方法： • 任何(个人) • 任何(企业) • WEP • WEP 企业 • WPA • WPA 企业 • WPA2 • WPA2 企业 • WPA3 • WPA3 Enterprise WPA3/WPA3 企业适用于 iOS 13+。 Windows 支持 WPA、WPA 企业、WPA2 和 WPA2 企业。

WEP、WPA/WPA2/WPA3、任何（个人）设置

设置	流程
密码	（可选）输入密码以访问该网络。 否则，将会提示设备用户输入所需密码以访问网络。

WEP 企业、WPA/WPA2/WPA3 企业、任何（企业）设置

设置	流程
协议	
接受的 EAP 类型	选择可用于访问该网络的 EAP 类型： • TLS • TTLS - 在内部标识字段中，选择其中一个身份验证协议，例如 OS 默认设置、PAP、CHAP、MSCHAP、MSCHAPv2 和 EAP。 • PEAP • LEAP（不受 AMAPI 注册设备的支持） • EAP-SIM • EAP-AKA • EAP-FAST（AMAPI 注册的设备不支持）
EAP-FAST	选择定义验证方法的 EAP-FAST 选项： • **使用 PAC：**选择以便使用代理自动配置 (PAC)。 • **调配 PAC：**选择此项可允许调配 PAC。 否则，仅可使用设备上已调配的 PAC。 该选项仅在您选择“使用 PAC”之后可用。 • **匿名调配 PAC：**选择此项，无需验证服务器即可允许调配 PAC。 该选项仅在您选择“调配 PAC”之后可用。
身份验证	
用户名	指定访问网络所需用户名。 如果保留此处为空，将会提醒设备用户输入所需内容。*
使用每连接密码	选择此项可提示设备用户为每个连接输入密码。 当设备重新加入同一网络时，将会重新提示设备用户重新进行身份验证以加入网络。 AMAPI 注册的设备不支持此选项。
密码	（可选）输入密码以访问该网络。 否则，将会提示设备用户输入所需密码以访问网络。
身份证书	（可选）选择用于身份凭据的证书。 该身份证书配置定义了每个可用的身份凭据。
身份验证证书（仅适用于 Windows 设备）	从以下三个证书存储中选择一个，以便选取连接至 Wi-Fi 网络时使用的证书： • 计算机或用户：如果选择此选项且用户未登录，则将从计算机存储中选取身份验证证书。 如果用户已登录，则将从用户存储中选取特定证书。 • 计算机：如果选择此选项，则将从计算机存储中选取身份验证证书。 • 用户：如果选择此选项，则将从用户存储中选取身份验证证书。 默认选择“用户”选项。
外部身份	（可选）对于 TLS、TTLS、PEAP 和 EAP-FAST，选择该选项可允许设备用户隐藏其身份。 用户的真实姓名仅出现在内部的加密通道中。 此选项可以增加安全性，因为攻击者无法清楚地看到正在进行身份验证的用户名。
域	当 EAP 类型为 TLS 和 TTLS 时受到支持。
信任	
可信证书（不受 AMAPI 注册设备的支持）	选中复选框以从列表中选择多个证书。

设置	流程
受信任服务器证书名称	单击 **+ 添加**，以输入一个或多个受信服务器证书的名称。 （可选）选择**允许信任异常**，以允许用户在对话窗口做出信任决策。

iOS、macOS 和 visionOS

设置	流程
所有版本	
网络类型	如果将该网络视为以下内容，则选择它： • 标准 • 遗留热点 • Passpoint
允许代理 PAC 回退	（可选）如果 PAC 文件不可达，则允许设备直接连接至目的地。
设置模式（可选）	包含要附加连接模式的类型的字符串数组。 • 系统：在用户登录设备前，WiFi 已处于连接状态。 • 登录窗口：在用户登录设备后，WiFi 可以使用。 目前，只有在同时启用系统模式和登录窗口模式后，设置模式才可用。
Passpoint 设置	本部分钟的设置会在您为网络类型选择 Passpoint 时显示。
域名	输入将用于 Passpoint 协调的域名。
连接至漫游合作伙伴 Passpoint 网络	（可选）选择此项可允许连接到漫游服务供应商。
漫游联合组织标识符	（可选）将由 IEEE 分配的标识符输入由 Wi-Fi 配置文件支持的实体。
网络访问标识符领域名称	（可选）输入用于 Passpoint 协调的网络访问标识领域名称。
MCC 和 MNC 对	（可选）输入用于 Passpoint 协调的移动国家码 (MCC) /移动网络码 (MNC) 对。 每个字符串必须正好包含六位数字。
已显示运营商名称	（可选）输入要显示的网络运营商名称。
Cisco QoS 快车道	本部分中的设置应用于 Cisco 快车道配置。 设置包含适用于 L2 和 L3 标记的允许列表应用，以及是否将内置音频/视频服务的音频和视频流量加入允许列表，例如 FaceTime 和 Wi-Fi 通话。
限制 QoS 标记	如果未选择，那么所有应用程序都将在网络支持 Cisco QoS 快车道时使用 L2 和 L3 标记。 如果选择，则会使用显示的**选择应用程序**设置，以便添加您希望为 L2 和 L3 标记包括的应用程序。 未选择的所有应用程序将不会使用 L2 和 L3 标记。
启用 QoS 标记	禁用 L3 标记，并仅为发送到 Wi-Fi 网络的流量使用 L2 标记。 未选择时，系统会认为 Wi-Fi 未与 Cisco QoS 快车道网络相关联。
将 Apple 音频/视频通话加入允许列表	指定是否将内置音频/视频服务的音频和视频流量加入允许列表，例如 FaceTime 和 Wi-Fi 通话。
选择应用	用来添加您希望为 L2 和 L3 标记包括的应用程序。 未选择的所有应用程序将不会使用 L2 和 L3 标记。

设置	流程
iOS 10+	
Cisco QoS 快车道 限制 QoS 标记	本部分中的设置应用于 Cisco 快车道配置。 设置包含适用于 L2 和 L3 标记的允许列表应用，以及是否将内置音频/视频服务的音频和视频流量加入允许列表，例如 FaceTime 和 Wi-Fi 通话。 如果未选择，那么所有应用程序都将在网络支持 Cisco QoS 快车道时使用 L2 和 L3 标记。 如果选择，则会使用显示的**选择应用程序**设置，以便添加您希望为 L2 和 L3 标记包括的应用程序。 未选择的所有应用程序将不会使用 L2 和 L3 标记。
启用 QoS 标记	禁用 L3 标记，并仅为发送到 Wi-Fi 网络的流量使用 L2 标记。 未选择时，系统会认为 Wi-Fi 未与 Cisco QoS 快车道网络相关联。
将 Apple 音频/视频通话加入允许列表 选择应用 **iOS 10.3+ 被监控** 启用 Wi-Fi 允许列表	指定是否将内置音频/视频服务的音频和视频流量加入允许列表，例如 FaceTime 和 Wi-Fi 通话。 用来添加您希望为 L2 和 L3 标记包括的应用程序。 未选择的所有应用程序将不会使用 L2 和 L3 标记。 确定设备允许连接的 WiFi 网络。 如果存在多个 WiFi 配置，则应用最严格的 WiFi 配置。
iOS 14.0+ 和 macOS 15.0+	
禁用 MAC 地址随机选择	在 iOS 14.0+ 和 macOS 15.0+ 中，Apple 更改了设备报告其 Wi-Fi MAC 地址的默认行为，从而会针对新连接报告随机地址，而不是设备的实际 Wi-Fi MAC 地址。 因此，对于使用强制网络门户或筛选 MAC 地址的企业，此功能可能造成意外行为。 通过编辑关联 Wi-Fi 配置并打开此选项（默认设置为假），管理员可以为 Wi-Fi 网络**禁用 MAC 地址随机选择**。 这将使 Wi-Fi 配置重新推送到所有设备。 此选项会在设备设置中显示隐私警告，并表示网络降低隐私保护。 通过设备的设置，设备用户仍可以手动打开或关闭。
Android 11+	
MAC 地址随机化	• 已禁用：用户登录设备前已连接 Wi-Fi。 • 已启用 - 自动：用户登录设备后 Wi-Fi 可用。 • 已启用 - 非永久 • 已启用 - 永久

键入 $ 以查看此字段支持的变量列表（如果有）。

有关更多信息，请查看如何创建配置。

10.10.7. 手机网络配置

本部分包含以下主题：

- APN 配置
- 移动电话
- Cellular Private Network Configuration.htm蜂窝专用网络配置
- iOS 电信预置配置
- eSIM 配置

10.10.7.1. APN 配置

APN 配置会设置设备的蜂窝接入点名称。 对于 iOS 7，使用**蜂窝配置**代替。

APN 设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
接入点名称	输入相应接入点的名称。 该名称通常由提供服务的运营商定义。
访问点用户名	输入为此接入点授予的用户名。*
访问点密码	输入与已输入的用户名相对应的密码。
代理服务器和端口	输入 IP 地址或 URL 以及 APN 代理的端口号。
EnableXLAT464	选中此复选框以启用接入点名称 (APN)。 此选项通过仅支持 IPv6 的网络提供 IPv4 服务。

键入 $ 以查看此字段支持的**变量**列表（如果有）。

有关更多信息，请查看**如何创建配置**。

10.10.7.2. 移动电话

适用于： iOS 7.0+ 和 watchOS 10.0+

本部分包含以下主题：

- **默认 APN 的蜂窝设置**
- **数据 APN 的蜂窝设置**
- **漫游时控制蜂窝访问**
- **控制蜂窝访问**

蜂窝配置可设置设备的蜂窝配置文件。 在运行 iOS 7.0+ 或 watchOS 10.0+ 的设备上配置蜂窝网络设置。 一些公司与授予它们对唯一访问点名称(APN)的访问权限的移动电话运营商签有合约，以实现远程网络访问或特殊计费计划。 有关配置参数，请咨询您的移动电话运营商。

- 任何时候可安装的移动电话配置文件不能超过一个。
- 如果已安装**APN 配置文件**，则无法安装移动电话配置文件。

您可以从**配置的 APN 类型**下拉框中为以下 APN 类型配置蜂窝设置：

- 默认和数据 APN
- 默认 APN
- 数据 APN

对于所有配置，请输入标识配置的名称和可选描述。

默认 APN 的蜂窝设置

默认 APN 设置	流程
APN 名称	输入相应接入点的名称。 该名称通常由提供服务的运营商定义。
APN 身份验证类型	（可选）选择下列选项之一： • CHAP（挑战握手身份验证协议） • PAP（密码身份验证协议）
用户名	（可选）输入用于验证的用户名。
密码	（可选）输入用于验证的密码。

数据 APN 的蜂窝设置

数据 APN 设置	流程
APN 名称	输入相应接入点的名称。 该名称通常由提供服务的运营商定义。
APN 身份验证类型	（可选）选择下列选项之一： • CHAP（挑战握手身份验证协议） • PAP（密码身份验证协议）
用户名	（可选）输入用于验证的用户名。
密码	（可选）输入用于验证的密码。
代理服务器	指定代理服务器。
代理服务器端口	指定代理服务器端口。
10.3+	
允许的协议掩码	选择 IPv4、IPv6 或两者。
国内漫游中允许的协议掩码	选择 IPv4、IPv6 或两者。
漫游中允许的协议掩码	选择 IPv4、IPv6 或两者。

控制在漫游时的蜂窝访问权限

您可以在设备处于漫游状态时，限制部分或所有可管理应用访问蜂窝数据。

步骤

1. 转到 Ivanti Neurons for MDM 主导航菜单中的**配置**选项卡。
2. 单击**+添加**
3. 在搜索字段中输入**网络**，然后点击**网络使用**配置。
4. 选择**不允许所有可管理的应用**复选框，以在漫游时或始终阻止可管理的应用程序访问蜂窝数据。
5. 请保持复选框未选中，才可以通过名称或捆绑 ID 指定受管应用，以避免接受蜂窝数据。
6. 使用应用字段中的下拉菜单，以通过名称或捆绑 ID 搜索应用。

控制蜂窝访问

您可以随时限制部分或全部可管理应用程序对蜂窝数据的访问。 这些应用程序仍可以在受限基础上使用，但它们将无权访问蜂窝数据。

步骤

1. 转到 Ivanti Neurons for MDM 主导航菜单中的**配置**选项卡。
2. 单击**+添加**
3. 在搜索字段中输入**网络**，然后点击**网络使用**配置。
4. 选择**不允许所有可管理的应用**复选框，以阻止可管理的应用程序在任何时候访问蜂窝数据。
5. 也可以取消选中该复选框，指定可管理应用程序，以阻止其接收蜂窝数据。
6. 使用应用字段中的下拉菜单，以通过名称或捆绑 ID 搜索应用。

有关更多信息，请查看**如何创建配置**。

10.10.7.3. 蜂窝专用网络配置

Ivanti Neurons for MDM 让蜂窝专用网络配置负载可以提供有关专用网络部署的设备信息，包括地理位置、Wi-Fi 首选项和网络部署类型。

适用于

iOS 17.0 至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**蜂窝专用网络**配置。
3. 根据下表配置**蜂窝专用网络**设置：

设置	描述
名称	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
首选蜂窝数据	选中复选框可优先启用和使用蜂窝数据（相比 Wi-Fi）。
NR 独立组网	如果蜂窝数据网络采用 NR 5G 独立组网模式，请选中复选框。
数据集名称	指定标识此配置的数据集名称。
版本号	指定数据集的版本号以跟踪系统更新。
越界报警	指定每个地理 ID 的纬度、经度和半径，以在地理位置内部署专用网络。 您可以为专用网络创建包含多达一千个越界报警的列表。

4. 单击**下一步**，配置分配设置。
5. 选择其中一个分发选项来设置**蜂窝专用网络**配置。 有关配置分发选项的详细信息，请参阅使用配置。
6. 单击**完成**。

10.10.7.4. iOS 电信预置配置

iOS 电信预置配置可设置漫游限制和热点限制的默认值。

iOS 电信预置设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
允许设备在漫游时使用语音服务	选择以启用语音漫游。 语音漫游是否可用取决于操作员。
允许设备在漫游时使用数据服务	选择以启用数据漫游。 启用数据漫游即启用设备上的语音漫游。
允许用户启用个人热点	选择以启用个人热点功能。 此功能是否可用取决于操作员。

有关更多信息，请查看**如何创建配置**。

10.10.7.5. 增强 5G 网络切片配置

Ivanti Neurons for MDM 提供增强的 5G 网络切片配置，为 Android 设置 5G 网络切片，由此允许移动网络运营商分配专用的 5G 网段（或“切片”），用于将具有类似需求（例如低延迟或高带宽）的不同应用程序划分到特定切片中，以便更好地优化网络资源。 这使 MDM 管理员和网络提供商能够直接管理切片，以实现更好的应用程序性能。

主要功能

1. **专用网络**：网络切片使不同的应用程序能够使用针对其具体需求定制的网络切片，而不是所有应用程序共享单个网络切片

2. **自定义**：管理员可以根据应用程序的具体要求配置将应用程序分配到特定网络切片的方式，例如，在分配时确保实时通信应用程序的低延迟，或在分配时确保 YouTube 等流媒体服务的高带宽。 专为高性能游戏定义的切片可能优先考虑低延迟，而专为媒体流式传输定义的切片将针对高带宽进行优化。

3. **合作伙伴参与**：此功能通常需要与定义这些切片的网络提供商协作，并向 MDM 管理员告知切片列表及其重要性。

创建增强型 5G 网络切片配置

程序

1. **添加配置**

- 导航到**配置 >> +添加**。 随即将显示**添加配置**页面。
- 在搜索栏中输入**增强型网络切片**以配置增强型网络切片。 随即将显示**创建增强型网络切片配置**页面。
- 点击 **+添加描述**以输入配置的描述。

2. **配置应用程序**

- 在**配置设置 >> 应用程序目录**下，输入所需的应用程序名称。
- 如果在 Play 商店或 App Store 中未提供应用程序，请点击**手动添加**。
- 输入**程序包 ID**，并从下拉菜单中选择适用的**网络切片**。
- 从**选择切片**下拉列表中选择所需的切片。
- 点击**添加**。 应用程序即会显示在所选网络切片下的**配置网络切片**中。
- 要删除应用程序，请点击**配置网络切片**部分下的**删除**。

3. **分发配置**

- 点击**下一步**，选中或取消选中“**启用此配置**”复选框，然后选择分发选项（“所有设备”、“无设备”或“自定义”）。
- 点击**完成**以完成配置。

针对锁定和 Kiosk 的增强型网络切片配置

通过创建增强型 5G 网络切片配置，您可以将设备配置为以受限方式运行，从而确保用户只能访问指定的应用程序和设置。

在以下锁定下，有一个“**启用 5G 网络切片**”复选框：

- **工作配置文件** - 在具有使用 Android Enterprise 版本 12.0 配置的工作配置文件的员工拥有设备上，“启用 5G 网络切片”复选框位于**配置设置 > 工作配置文件锁定设置**。

- **带有工作配置文件的托管设备/公司拥有设备上的工作配置文件** - 在“带有工作配置文件的托管设备/采用 Android 12.0 版本的公司拥有设备上的工作配置文件”下，有一个“启用 5G 网络顺畅”复选框。

这是允许设备使用 5G 网络切片的旧版设置。 它与新的增强型 5G 网络切片配置的相关性如下：

如果对设备应用了上述任何锁定，并且*启用 5G 网络切片*选项**未被**选择，则*增强型 5G 网络切片*配置将失败并出现错误。

示例

- **案例 1**：如果设备锁定未分发且增强型网络切片配置已分发，则增强型配置将激活。
- **案例 2**：如果分发了设备锁定但未选择 5G 复选框 (false)，则增强型 5G 网络配置将出错。
- **案例 3**：如果先分发增强网络切片，然后在启用复选框的情况下锁定设备，则增强网络切片配置将继续工作。 否则，它将出错。

配置详细信息：

- 如果分发了设备锁定并且推送/分发了增强型网络切片配置，则用户必须确保“启用 5G 网络切片”复选框处于启用状态，以防止发生错误。
- 如果未启用复选框，但配置已发送，则它会在设备上出错。

10.10.7.6. eSIM 配置

eSIM 配置使用 RefreshCellularPlans 命令，在设备上配置手机网络。 在将手机网络映射到设备前，管理员必须获取 eSIM 运营商 URL。

适用于：Android 15+、iOS、iPadOS 和 Windows 11

Android 15+ 设备的程序

1. 转到**配置** > **+添加**。
2. 在搜索字段中键入 eSIM，然后单击 **eSIM** 配置。
3. 输入配置的名称和描述。
4. 从**平台**列表中，选择 **Android**。
5. 在**配置设置**部分下，输入**运营商 URL**。
6. **自动启用** - 选择此选项下载 eSIM 配置文件并在设备上自动启用。 如果未选择此选项，将下载 eSIM 配置文件，但不会在设备上自动启用。

> 此选项不适用于工作配置文件模式下的设备。

7. 使用以下分发选项之一选择和分发配置：
   - 所有设备
   - 无设备（默认）
   - 自定义
8. 单击**完成**。

适用于 Android 13+ 设备的 EID

请求 EID 选项现在可在设备详细信息和设备列表页面中使用。 此选项仅支持工作配置文件上兼容 eSIM 的设备、工作托管设备和公司自有设备模式下的工作配置文件。 如果设备已注册，EID 将自动为已注册设备选取，并显示在设备详细信息页面中。 如果不是，此字段将被启用，您可以通过单击**请求 EID** 来请求 EID。 您还可以使用设备列表页面中的**导出为 CSV** 选项导出 EID。

> 在**设备详细信息**页面中，**请求 EID** 选项可用于具有 Ivanti Go R122 或更高版本的 Android 13+ 设备。

保留 eSIM 数据计划（适用于 iOS 11+ Android 15.0+）：当您尝试擦除已注册 eSIM 配置的设备时，**擦除设备**操作提供了一个额外的选项来保留数据计划。 如果选择 **保留 eSIM 数据计划（适用于 iOS 11+ 和 Android 15.0+）**，然后单击**擦除**，则会保留现有的 eSIM 数据计划，同时擦除设备的所有其他数据。 您可以从**设备详情**页面访问此选项，或者通过选择设备，打开**操作**菜单并单击**擦除**来访问此选项。

iOS 和 iPadOS 设备的操作步骤

1. 转到**配置** > **+添加**。
2. 在搜索字段中键入 eSIM，然后单击 eSIM 配置。
3. 输入配置的名称和描述。
4. 选择 **iOS/iPadOS**。
5. 键入运营商 URL。
6. 单击**下一步**。
7. 选择启用此配置选项。

8. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义
9. 单击完成。

Windows 11 设备的操作步骤

1. 转到**配置** > **+添加**。
2. 在搜索字段中键入 eSIM，然后单击 eSIM 配置。
3. 输入配置的名称和描述。
4. 在“选择操作系统”部分中，点击 **Windows**。
5. 在“配置设置”部分的“服务器名称”文本框中，键入运营商 URL（采用 FQDN 格式）。
    - 是 Discovery 服务器 - 选择此项可将服务器标记为可发现。
    - 自动启用 - 选择此项可在下载后在设备上启用配置文件。
6. 单击**下一步**。
7. 选择启用此配置选项。
8. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义
9. 单击**完成**。

将 eSIM 重置为出厂状态（仅适用于 Windows 11 设备）

此选项在所有设备的“设备详细信息”部分下提供。 点击此选项可删除下载到设备上的所有 eSIM 配置文件。

重要说明 - 仅适用于 Windows eSIM 配置

- 设备注册后，**设备详情**部分现会在**支持 ESIM** 下显示设备是否支持 eSIM。 对于支持 eSIM 的设备，相应的 eSIM 标识符详细信息也显示在 **ESIM 标识符**下。
- 在 Ivanti Neurons for MDM 已注册设备被擦除并重新注册后，应从“设备”页面删除该设备的旧记录（状态为“已擦除”），以避免在该重新注册的设备上出现 eSIM 配置的预配问题。
- 将相同的配置重新推送到已下载配置文件的设备，无法再次下载配置文件。 如果管理员希望设备重新下载配置文件，建议先将 eSIM 模块重置为出厂状态，然后推送/重新推送 eSIM 配置。
- 在设备上成功预配 eSIM 配置后，在停用设备之前，管理员应执行 eSIM 擦除操作，以确保从设备上擦除下载的 eSIM 配置文件。
- 如果删除 eSIM 配置，则只会从设备中删除配置。 如果在设备上发现、下载并激活了任何 eSIM 配置文件，则这些 eSIM 配置文件将保持激活状态，直到执行 eSIM 擦除。
- 如果执行 eSIM 擦除操作，则会从设备中删除所有已下载的 eSIM 配置文件。 但是，处于“已安装”状态的 eSIM 配置在设备上保持不变。管理员需要取消分发 eSIM 配置，以便从设备中删除该配置。

10.10.8. 其他配置

本部分包含以下主题：

- 关联域配置
- Android 文件传输配置
- Apple TV 配置
- AirPlay 配置
- AirPlay 镜像
- 浏览器设置
- 为 iOS 配置单一应用模式
- 配置 iOS MDM 配置文件
- 配置 macOS MDM 配置文件
- 内容缓存
- 创建 Android 快捷方式
- 设备名称设置
- 以太网配置 (macOS)
- EMA 服务器集成配置
- 设备壁纸配置
- 锁定屏幕消息配置
- 创建屏幕保护程序配置
- 配置用户的屏幕保护程序
- macOS 系统扩展配置
- 仅限 MAM
- 托管的 Google Play 配置
- 迁移助手设置
- 通知配置
- 打印机设置
- 删除 Bloatware 配置
- Samsung 手机限制配置
- 单应用模式配置
- 开始菜单和任务栏
- 系统更新配置
- Windows 更新管理
- Windows 应用计划
- Windows BIOS 配置
- Windows BitLocker
- Windows 自助服务终端配置

- Windows 许可证配置
- 软件更新推荐节奏配置

10.10.8.1. 关联域配置

许可证： Gold

关联域配置是将应用程序映射到其关联域的词典。 关联域可与可扩展 AppSSO、通用链接和密码自动填充等功能一起使用。

关联域设置如下：

设置	流程
名称	输入用于识别此配置的名称。
应用程序标识符	（必需）与域关联的应用程序标识符。
关联域	（必需）与应用程序关联的域。 每个字符串都采用 "service:domain" 的形式。 域应该是完全限定主机名，例如 www.example.com。
启用直接下载	如果设置为 True，则应直接下载此域的数据，而不是通过 CDN 下载。 此域的权利值必须设置为 service:domain?mode=managed，否则该值将被忽略。 适用于 macOS 11 及更高版本。 **默认值**：False

10.10.8.2. Android 文件传输配置

在 Android 11 中，Google 在应用程序对设备的存储访问上做出了重大更改，这也影响了企业如何将文件发送到这些设备上的特定应用程序。 考虑到这些更改，随着设备升级到 Android 11 及更高版本，许多大型企业都会在将文件分发到设备和应用程序方面遇到挑战。 任何依赖于硬件供应商特定 API 的方法，都会限制企业在运行不同制造商和操作系统版本的不同设备上采用相同的方法。

Ivanti 开发了一种文件传输解决方案，可以打破 Android 版本和硬件供应商方面的限制。 此解决方案依赖于 Android 的标准 *Content-Provider* 功能。 *Content-Provider* 允许 Ivanti 的 Go 应用程序为通过 UEM 推送的每个文件生成唯一的设备上位置。

文件传输配置适用于处于完全托管设备模式的 Android 设备。 通过使用此配置，管理员可以提供传输设备上文件的选项，以便在同一设备允许的不同应用程序之间共享文件。 其他应用程序可以出于任何原因使用这些文件。 其中一个示例用例则是使用 JavaScript 初始化应用程序配置，或者使用 PDF 或视频显示公司信息。 上传到 Ivanti 文件传输配置的每个文件都会在 Ivanti Go 收到相应的配置和关联文件后进行下载。 文件会安全地存储在 Ivanti Go 中。

其他应用程序无法任意访问此处的文件。

应用程序沙箱内的每个下载文件都有唯一位置参考，也称为 *ContentURI* 或 *URI*。 自定义属性用于保留设备上每个文件在服务器上的 ContentURI 值，可以帮助管理员确定文件在设备上的可用性、形成动态设备组，以及按要求使用托管应用程序配置将 ContentURI 传递给目标应用程序等。

> 对于非 Ivanti 应用程序，管理员应咨询第三方应用程序开发人员，了解他们对这种方法的支持，即通常所称的“使用基于 FileProvider 的 ContentURI”。

必备项：

- 添加基于设备的新自定义属性以用于文件传输操作。 对于每项文件传输配置，应创建一个唯一的自定义属性。 每个自定义设备属性只能为每个配置的一个文件存储设备 contentURI（文件位置）。

步骤

1. 转到**配置** > **添加配置** > **文件传输**。 **创建文件传输配置**页面随即打开。
2. 在**名称**框中输入配置名称。
3. 输入配置的**描述**。
4. **配置设置**
   在**要传输的文件**部分中，使用拖放选项或通过**选择文件**选项进行浏览，选择要传输的文件。 默认情况下，文件大小上限为 50 MB。
5. 选择以下一个或多个**下载到设备**选项（可选）：
   - **允许通过按流量计费的网络下载** - 选择此项以在按流量计费的网络上继续下载文件
   - **需要充电** - 选择此项以确保在文件传输过程中对设备进行充电
   - **需要设备空闲** - 选择此项以在文件传输过程中让设备处于空闲状态
6. 使用以下两个选项之一与其他应用程序共享文件
   - **使用 Android 托管应用程序配置进行传输** - 仅当目标应用程序可以使用其托管应用程序配置来使用内容 URI 时才使用此选项。
   - **使用设备上意图进行传输** - 意图是特定于应用程序的。 要使用此选项共享文件，请参阅目标应用程序文档并提供以下意图部分中的信息。 文件可与应用程序共享后，意图即可允许 Ivanti Go 应用程序在设备上广播消息。

使用 Android 托管应用程序配置进行传输

步骤

1. 在**选择基于现有设备的自定义属性以与其他应用程序共享此文件**字段中，输入现有属性名称，例如 **Custom-Filename**。 有关详细信息，请参阅将自定义属性分配到设备。
2. 自定义属性名称应是唯一的新属性，仅用于此文件传输操作。 每个自定义设备属性只能为每个配置的一个文件存储设备 contentURI（文件位置）。
   提供对以下应用程序和/或包名称的访问权限：可从应用程序名称选择器中选择应用程序名称，并添加包名称。

> 这些将是唯一允许访问文件的授权包。

   - **应用程序名称** - 可从应用程序名称选择器中选择应用程序名称。
   - **包名称** - 可在此区域输入捆绑包 ID，例如用分号 (;) 隔开多个包名称。

```
Bash

com.mobileiron.filetransfer.android3。
```

单击**保存**。 新的文件传输配置将显示在"配置"页面上。

配置目标应用程序

步骤

1. 转到**应用程序 > 应用程序目录**。
2. 选择接收文件的目标应用程序。
3. 导航到**应用程序配置 > Android 托管配置**。
4. 创建新的配置或使用现有配置。
5. 应用程序可能具有"清单信息"一类的设置或其他属性，管理员可以在其中定义替换变量并将文件的位置传递给目标应用程序。 以 Ivanti Velocity 应用程序为例，在应用程序配置对话框 > **获取配置 > 清单信息**字段中，输入替换变量。 例如 $Custom-File-Name$。
   选择分发。
6. 单击**保存**。

使用设备上意图进行传输

步骤

1. 在**选择现有设备属性以在意图附加项中传递文件路径**字段中，输入新的自定义属性名称，例如 deviceIntentURI。
2. 自定义属性用于保留每个设备在服务器上的位置 (URI / ContentURI) 值，可以帮助管理员确定文件在设备上的可用性。 有关详细信息，请参阅将自定义属性分配到设备。
   在**提供对特定应用程序或包名称的访问权限**字段中，输入**应用程序名称**或**包名称**，例如 Velocity。

> 这些将是唯一允许访问文件的授权包。

3. 在 Intents-Standard 部分中，提供以下详细信息：
   - **操作类型** - 从下拉列表中选择**启动活动/启动服务**，或根据应用程序选择其他类似选项。 根据目标应用程序开发人员的指引或参考目标应用程序文档，为此字段选择正确的值。
   - **类名称**（可选）- 根据目标应用程序开发人员的指引或参考目标应用程序文档，为此字段选择正确的值。

- **操作** - 根据应用程序将操作设置为：或设置为类似的值。

```
Bash

com.wavelink.nameofapp.action.INSTALL_CONFIG
```

- **类别** - 输入值，用分号 (;) 隔开。
- **MIME 类型**（可选）- 在管理员的主机服务器中，应使用 MIME 类型的应用程序/配置设置 custom.mobileconfig 文件，以便下载设备的 MDM 配置文件并将其安装在设备上。 根据目标应用程序开发人员的指引或参考目标应用程序文档，为此字段选择正确的值。
- **标志**（可选）- 选择要使用的标志数量。 根据目标应用程序开发人员的指引，为此字段选择正确的值。

提供项、类型和值下的 **Intents-Extras** 值。 有关更具体的参数，请参阅 OEM 应用程序文档。 根据目标应用程序开发人员的指引或参考目标应用程序文档，为此字段选择正确的值。

5. 单击**保存**。
6. 在“配置”页面中，选择新的文件传输配置，然后选择**操作** > **应用到标签**。 **应用到标签**对话框随即打开。
7. 选择合适的标签，然后点击**删除**。
   与其他应用程序传输/共享文件只能通过从目标应用程序或设备收集日志来验证。

验证文件下载状态

自定义属性用于保留每台设备上每个文件在服务器上的位置 (ContentURI) 值，可以帮助管理员确定文件在设备上的可用性。

步骤

1. 转到**设备** > **设备**。
2. 选择文件传输配置要部署到的特定设备。
3. 在“设备详细信息”页面中，选择设备，然后选择**操作** > **强制设备签入**。
4. 在“配置”选项卡下，检查文件传输配置显示的状态是否为**已应用**。
5. 在“自定义属性”选项卡下，检查是否显示新自定义属性的名称（例如 Custom-File-Name$）及其相关值。 这里会提供文件在设备上的存储位置信息，也会显示文件已下载到 Ivanti Go 应用程序沙箱中可用的本地设备上。
   与其他应用程序传输/共享文件只能通过从目标应用程序或设备收集日志来验证。

10.10.8.3. Apple TV 配置

许可证： Silver

定义 Apple TV 语言和区域的 Apple TV 配置。

Apple TV 设置如下所示：

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
语言	输入两个字符的语言代码，以指定用户界面语言。
区域设置	输入本地 ID，以指定用户界面的国家或地区/语言组合。

有关更多信息，请查看**如何创建配置**。

10.10.8.4. AirPlay 镜像

许可证：Gold

通过 AirPlay Mirroring 功能，您可以在使用 Apple TV 的显示器上显示 iOS 设备的画面。 Apple TV 和 iOS 设备必须连接在同一 Wi-Fi 网络中。 此功能需要以下设备：

- 设备版本最低 iOS 7 - 被监控
- macOS 10.10 及更高版本 - 受监管
- Apple TV 版本 - 被监控
- AirPlay

> 切换包含的非 iOS 设备管理无法逆转。

本部分包含以下主题：

- 配置 Apple AirPlay
- 在移动设备上设置 AirPlay
- 设置与 Apple TV 配合的监视器
- 将 iOS 设备连接到 Apple TV

配置 Apple AirPlay

有关 AirPlay 配置设置的更多信息，请查看 AirPlay 配置。

程序

1. 转至**配置**。
2. 点击 **+ 添加**。
3. 单击 **AirPlay**。
4. 在相应字段输入配置的名称和描述。
5. 对于所有支持的 iOS 版本，输入设备名称和密码。
6. 单击 **+添加**，以添加其他设备（如需要）。
7. 或者，对于受监督的 iOS 7+ 设备或 macOS 10.10+，将设备 ID 加入允许列表。
8. 单击**下一步**。
9. 选择分配水平。
10. 单击**完成**。

在移动设备上设置 AirPlay

程序

1. 设置 Apple Configurator。
2. 转到**设备 > 设备**。
3. 单击 iOS 设备名称，显示该设备的“详细信息”页面。

4. 单击 ⋮ 图标。
5. 选择 **AirPlay Mirroring**，以显示 AirPlay Mirroring 对话框。
6. 从下拉菜单选择 Apple TV 设备。
7. 输入以秒为单位的扫描时间，指定扫描所选设备的时间限制。
8. 输入 Apple TV 设备的密码。
9. 单击**发送请求**。

设置与 Apple TV 配合的监视器

程序

1. 在连接到 Apple TV 的监视器上，转到**设置 > 配置文件**。
2. 选择 **Ivanti Neurons for MDM Apple Configurator**。
3. 单击**添加配置文件**。
4. 单击 ⋮ 图标。
5. 选择 **AirPlay Mirroring**，以显示 AirPlay Mirroring 对话框。
6. 从下拉菜单选择 Apple TV 设备。
7. 输入以秒为单位的扫描时间，指定扫描所选设备的时间限制。
8. 输入 Apple TV 设备的密码。
9. 单击**发送请求**。

将 iOS 设备连接到 Apple TV

程序

1. 将 Apple TV 设备连接至显示器。
2. 使用 Apple TV Remote，转到**设置 > 帐户 > 家庭共享**，以打开“家庭共享”。
3. **将 iOS 设备**连接到与 **Apple TV 设备**相同的 Wi-Fi 网络。
4. 在 **iOS** 设备上，打开 Remote 应用。
5. 从 **Remote 设置**屏幕启用**家庭共享**。

10.10.8.5. 浏览器设置

使用浏览器设置，您可在 Windows 10 设备上为 Google Chrome、Mozilla Firefox 和 Internet Explorer 配置设置和限制。

此功能需要 Bridge。 请查看 **Ivanti Bridge**，以了解详细信息。

> 请确保，在应用浏览器设置前，在设备上安装浏览器。

要配置浏览器设置：

1. 转到**配置 > + 添加**。
2. 选择**浏览器设置**配置。
3. 输入配置的名称。
4. 输入描述。
5. 在“配置设置”部分中，按照下表描述指定剩余设置。

设置	采取何种措施
浏览器	选择需要设置的浏览器类型： • **Chrome** • **Firefox** • **Microsoft Edge** • **Internet Explorer**
浏览器设置	配置以下选项： **允许浏览器**： • 允许保存密码 • 允许安全浏览模式 • 允许在浏览器中使用过期插件 **Chrome 和 Firefox**： • **允许删除浏览器历史** **Chrome 和 Internet Explorer**： • **允许浏览器打印** • **新标签页 URL** **仅限 Chrome**： • **在书签栏中显示应用快捷方式** • **显示主页按钮** • **允许与 Google 同步数据** • **在 Chrome 关闭时，继续运行后台应用** **仅限 Firefox**： • **允许安装扩展程序** **仅限 Internet Explorer**： • **允许从网站下载数据**
浏览器收藏夹	点击 **+ 添加**。 将显示**添加浏览器收藏夹**窗口。 配置以下字段： • **显示名称**：键入收藏夹的显示名称 • **URL**：键入浏览器收藏夹的 URL。 单击**添加**。 已添加浏览器收藏夹的详细信息将显示在页面上。 在**操作**列中，单击编辑图标，以编辑设置。 要删除浏览器收藏夹，单击删除图标。 **浏览器收藏夹文件夹名称**：键入应列出收藏夹的浏览器收藏夹文件夹的名称。 您也可以通过 CSV 格式添加浏览器收藏夹。 要以 CSV 格式上传： 1. 单击“上传 CSV 文件”。 浏览并选择要上传的 CSV 文件。 2. 单击**上传**。 CSV 文件中的详细信息应通过以下格式添加： • 第一列（显示名称）应指定收藏夹的显示名称。 例如：“购物”。 • 第二列 (URL) 应指定收藏夹的 URL。 例如：“https://amazon.com”。

设置	采取何种措施
网站安全性	配置以下网站安全性设置： **所有网站（Chrome 和 Firefox）** • **阻止 Cookie** • **阻止 Javascript** • **阻止插件** • **阻止弹出窗口** 特定网站（仅限 Chrome） **阻止网站（Chrome 和 Edge）**：添加要阻止的网站。 单击 **+ 添加**。 系统将显示**添加已加入阻止列表的网站**窗口。 在**网站 URL** 中，键入应加入阻止列表的网站 URL。 在**访问**字段中，选择**阻止**，将网站加入阻止列表。 默认选项是**允许**。 单击**添加**。
浏览器扩展程序	**允许的扩展类型（仅限 Chrome）**：选择下列任意选项： • **扩展程序** • **用户脚本** • **主题** • **已封装的应用** • **已托管的应用** • **平台应用** **浏览器扩展源（仅限 Chrome）**： 单击 **+ 添加**，以添加浏览器扩展程序源。 在浏览器扩展程序源添加后，通过单击**操作**列中的相关选项，您可以编辑或删除源。 **强制安装扩展（仅限 Chrome）**： 单击 **+ 添加**，以添加强制安装扩展程序。 在强制安装扩展程序添加后，通过单击**操作**列中的相关选项，您可以编辑或删除源。

6. 单击**下一步**。
7. 选择下列分配选项之一：
   - 所有设备
   - 无设备（默认）
   - 自定义
8. 单击**完成**。

10.10.8.6. 为 iOS 配置单一应用模式

许可证：Silver

单个应用程序模式将 iOS 和 tvOS 设备限制为只能使用指定应用。 例如，您可能要设置仅使用贵组织开发的自定义应用的设备。

程序

1. 转到**配置 > 添加>单一应用模式**。
2. 使用以下指导原则定义应用和相关设置。
3. 单击**下一步**。

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
选择应用	选择用于选择应用的方法： • **从应用程序目录和系统应用：**选择以搜索 Ivanti Neurons for MDM 应用程序目录和系统应用（默认预安装在 Apple 设备上）。 • 输入应用的名称，然后在它显示在应用列表内时选择它。 • **输入绑定 ID：**对于要选择的系统应用， 选择输入唯一标识符。 如果您无法使用 **从 App Catalog 和系统应用**选项找到系统应用，请使用此选项。
禁用触摸	选择此项可禁用触摸屏。
禁用设备旋转	选择此项可禁用设备旋转感应。
禁用音量按钮	选择此项可禁用设备音量按钮。
禁用铃声切换	选择此项可禁用设备铃声切换。
禁用睡眠唤醒按钮	选择此项可禁用设备睡眠/唤醒按钮（设备边框右上角）。
禁用自动锁定	选择此项可防止设备在闲置一段时间后进入睡眠状态。
启用旁白	选择此项可启用旁白屏幕阅读器（辅助功能）。
启用缩放	选择此项可启用缩放（辅助功能）。
启用反色	选择此项可启用反色调整（辅助功能）。
启用辅助触摸	选择此项可启用辅助触控（辅助功能）。
启用语音选择	选择此项可启用语音选择（辅助功能）。
启用单声道音频	选择此项可从立体声切换到单声道音频（辅助功能）。
旁白调整	选择此项可允许设备用户进行旁白调整。
缩放调整	选择此项可允许设备用户进行缩放调整。
反色调整	选择此项可允许设备用户进行反色调整。
辅助触摸调整	选择此项可允许设备用户进行辅助触控调整。

4. 在**分配**屏幕，选择接受此配置的设备组。
5. 单击**完成**。

如果已经将电话拨号器配置为要使用的应用程序，一旦设备进入单应用程序模式，主页按钮就会被激活。

10.10.8.7. 配置 iOS MDM 配置文件

iOS MDM 配置定义对 Ivanti Neurons for MDM 的访问限制。 有两大类 iOS MDM 配置：

- **iOS MDM - 批量配置：**针对由企业购买并且作为批量分发一部分配置的设备。
- **iOS MDM - 逐一配置：** 针对逐一配置的设备。 将不应用于受监管和用户注册的设备。

每一类仅提供一个，也仅允许一个跨过所有空间。

编辑 iOS MDM 配置

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 转至**配置**。
3. 选择您要编辑的 iOS MDM 配置。
4. 点击铅笔（编辑）图标可编辑配置。
5. 根据以下指导原则更改：
6. 单击**完成**。

设置	流程
MDM 访问权限	
允许设备锁定和密码移除	取消选中以免执行通行码合规性设置。
允许设备擦除	取消选中以免执行设备擦除操作。
允许查询网络信息（电话/SIM 号、MAC 地址）	取消选中，将设备排除在网络信息报告的范围之外。 如果取消选中此选项，则设备列表视图和设备详细信息视图将对不再需要报告的网络信息显示不适用。 此外，对于受影响的设备，漫游策略将无法再执行。
配置文件移除密码	
用于移除配置文件的密码	指定密码。 从设备删除配置文件时，系统将提示用户输入密码。
添加所需应用 (iOS 15.0+)	
按查找添加	输入应用名称并在应用商店中搜索应用，然后选择所需应用。 一次仅可添加一个应用。 选择一个应用会禁用其他应用。
手动添加	输入应用的 iTunes ID。

更改仅适用于更改后配置的设备。

10.10.8.8. 配置 macOS MDM 配置文件

macOS MDM 配置定义对 Ivanti Neurons for MDM 的访问限制。 macOS MDM 配置是单独配置，用于逐个配置设备。

程序

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 转至**配置**。
3. 选择您要编辑的 macOS MDM 配置。
4. 点击铅笔（编辑）图标可编辑配置。
5. 根据以下指导原则更改：
6. 单击**完成**。

设置	流程
允许设备锁定和密码移除	取消选中以免执行通行码合规性设置。
允许设备擦除	取消选中以免执行设备擦除操作。
允许查询网络信息（电话/SIM 号、MAC 地址）	取消选中，将设备排除在网络信息报告的范围之外。 如果取消选中此选项，则设备列表视图和设备详细信息视图将对不再需要报告的网络信息显示不适用。 此外，对于受影响的设备，漫游策略将无法再执行。
配置文件移除密码 用于移除配置文件的密码	指定密码。 从设备删除配置文件时，系统将提示用户输入密码。

更改仅适用于更改后配置的设备。

10.10.8.9. 内容缓存

许可证：Gold

适用于：macOS 10.13.4 或支持的更新版本。

配置内容缓存服务，以启用 App Store 软件的本地副本，并使连接的客户端更快地下载软件和应用。

内容缓存配置

程序

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中，键入**缓存**，然后单击**内容缓存**配置。
4. 输入名称并描述配置。
5. 输入内容缓存配置设置。
6. 单击**下一步**。
7. 选择**启用此配置**选项。
8. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义
9. 单击**完成**。

内容缓存配置设置

使用下表中的设置，以配置内容缓存。 有关这些设置的更多信息，请查看 **Apple 文档**。

设置	描述
允许系统自动从缓存清理内容（适用于 macOS 10.15 或支持的更新版本。	允许系统在其他应用需要磁盘空间时自动从缓存清理内容（例如 计算机上的可用磁盘空间不足时）。 默认情况下，此选项已启用。
允许个人缓存	缓存用户的 iCloud 数据。 客户端可能需要一段时间（小时或天），以回应对此设置的更改；但不会立即生效。 默认情况下，此选项已启用。
允许共享缓存 允许自动激活内容缓存 允许自动启用受限缓存（适用于 macOS 10.15.4 或支持的更新版本。	缓存非 iCloud 内容，例如应用和软件更新。 客户端可能需要一段时间（小时、天），以回应对此设置的更改；但不会立即生效。 默认情况下，此选项已启用。 自动激活内容缓存（如果可能），并防止禁用。 自动启用互联网连接共享（如果可能），并防止禁用互联网连接共享。
禁用受限缓存	禁用受限缓存。 禁用受限缓存选项会覆盖允许自动启用受限缓存选项。
缓存限制 数据路径	用于内容缓存的磁盘空间的最大字节数量。 0 值表示磁盘空间不受限。 默认值：0 用于存储缓存内容的目录的路径。 手动更改此设置不会自动将缓存内容从旧位置移到新位置。 要自动移动内容，使用共享首选项的内容缓存窗格。 值必须是（或结尾）/Library/Application Support/Apple/AssetCache/Data。
允许显示提醒（适用于 macOS 10.15 或支持的更新版本。	内容缓存会在屏幕右上角将异常情况（警报）显示为系统通知。
保持设备处于唤醒状态（适用于 macOS 10.15 或支持的更新版本。 **侦听范围** 第一个 IP 地址 上一个 IP 地址	只要打开内容缓存，即可防止计算机进入休眠状态（系统首选项 > 共享 > 内容缓存打开）。 词典数组，用于描述要服务的客户端 IP 地址的范围。 客户端在侦听范围中的第一个 IP 地址。 客户端在侦听范围中的最后一个 IP 地址。
IP 地址类型	选择下列选项之一： • IPv4（默认） • IPv6
仅允许侦听范围	内容缓存仅向侦听范围中的客户端提供内容。
允许与同级和父级侦听	通过整合侦听范围、对等侦听范围和父级，内容缓存会为客户端提供内容。 默认情况下，此选项已启用。

设置	描述
仅允许本地子网	内容缓存仅在相同即时本地网络中向客户端提供内容。 未向内容缓存可访问的其他网络中的客户端提供任何内容。 如果启用此选项，将忽略侦听范围。 默认情况下，此选项已启用。
记录客户端标识	内容缓存会记录请求内容的客户端的 IP 地址和端口号。
父级选择策略	选择以下其中一个策略选项： • 第一个可用 • URL 路径哈希 • 轮循机制（默认） • 随机 • 粘滞可用
父级	此缓存应从下载或上传的其他内容缓存的本地 IP 地址的数组，而非直接从 Apple 下载或上传到 Apple。 单击 **+ 添加**，以添加一个或多个 IP 地址。
仅允许同级本地子网	内容缓存仅与相同即时本地网络中的其他内容缓存对等，而非与使用与设备相同的公共 IP 地址的内容缓存对等。 默认情况下，此选项已启用。
端口	内容缓存接受上传或下载请求的 TCP 端口号。 将端口设置为 0，以选择随机可用的端口。 默认值：0
公共范围	词典数组，用于描述公共 IP 地址的范围，Ivanti Neurons for MDM 服务器应使用范围中的公共 IP 地址将客户端与内容缓存进行匹配。
第一个 IP 地址	服务器在公共范围中的第一个 IP 地址。
上一个 IP 地址	服务器在公共范围中的最后一个 IP 地址。
IP 地址类型	选择下列选项之一： • IPv4（默认） • IPv6

有关更多信息，请查看[如何创建配置](#)。

10.10.8.10. 创建 Android 快捷方式

快捷方式仅适用于使用已加入允许列表的浏览器的自助服务终端模式。 浏览器必须位于锁定和自助服务终端中

配置中列入白名单的浏览器。 快捷方式将出现在 Ivanti Neurons for MDM Kiosk 启动程序中。

步骤

1. 转到**配置**。 **> +添加**
2. 点击 **Android 快捷方式**可显示**创建 Android 快捷方式配置**页面。
3. 在**名称**字段中输入配置的名称。
4. 在**描述**字段中输入配置的描述。
5. 在**标签**字段中输入快捷方式的唯一标签。
6. 在 **URL** 字段中输入快捷方式目标的 URL。
7. 或者，将文件拖放至图标字段，或点击**选择文件**导航到该文件，选择快捷方式的图标。
8. 单击**下一步**。

10.10.8.11. 创建辅助功能设置配置

此配置允许企业在 Apple 设备上限制、更改或配置辅助功能设置。

步骤

1. 转至**配置**。
2. 单击 **+添加**
3. 点击**辅助功能设置配置**。
4. 配置下表中指定的设置：

设置	流程
名称	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
选择其中一个辅助功能设置 **辅助功能设置** 近观远点 近观近点 对比度值 光标大小 鼠标驱动程序初始延迟 鼠标驱动程序最大速度 在键盘选项中启用“慢速键” 为慢速键启用“点击按键声音” 慢速键延迟	• **辅助功能设置**：使用此选项可以配置 macOS 设备上的辅助功能设置。 • **辅助功能设置限制**：使用此选项可以限制对 iOS 设备的辅助功能设置所做的更改。 **配置设置** 缩放设置中的最小缩放级别 缩放设置中的最大缩放级别 在缩放选项中启用“使用滚动手势” 在缩放选项中启用“平滑图像” 指定值 选中复选框 - 在音频选项中启用“闪烁屏幕” 选中复选框 - 在鼠标和触控板选项中启用鼠标键 指定值 选中复选框 - 忽略内置触控板 指定值 指定值 选中复选框 选中复选框 选中复选框
以毫秒为单位指定值	选中复选框
选中复选框 - 以单声道播放立体声音频	选中复选框
在键盘选项中启用粘滞键	选中复选框
启用为粘滞键设置修改键时发出蜂鸣声	选中复选框
为粘滞键启用“在屏幕上显示按下的键”	选中复选框
启用旁白	选中复选框
在显示调节中启用反色	选中复选框

设置	流程
辅助功能限制	**配置设置**
启用粗体文本	选中复选框
启用增加对比度	选中复选框
启用减少运动	选中复选框
启用降低透明度	选中复选框
支持使用动态文本的辅助功能文本大小应用程序	从下拉列表中选择所需选项
启用触摸调节	选中复选框
启用旁白	选中复选框
启用缩放	选中复选框

5. 选择分发选项，并根据适用情况指定所需详细信息。
6. 单击**完成**。

10.10.8.12. 创建屏幕保护程序配置

屏幕保护程序配置允许您添加密码、空闲时间、模块路径和名称等选项。

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 单击**配置**。
3. 点击 **+添加**。
4. 在搜索字段中输入“屏幕”，然后点击**屏幕保护程序**。
   将显示“创建屏幕保护程序配置”详细信息页面。
5. 在此页面上配置设置。 请参阅**屏幕保护程序配置设置**主题中的表格，了解有关值的指南。
6. 单击**下一步**，以配置分配设置，然后单击**完成**。

屏幕保护程序配置设置

设置	流程
名称（必填）	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
密码提示复选框	选中此复选框后，当解锁或停止屏幕保护程序时，系统将提示设备用户输入密码。 （适用于 macOS 10.13 及更高版本）。
密码提示延迟	指定延迟持续时间（以秒为单位）。
登录窗口空闲时间	指定空闲时间（以秒为单位），屏幕保护程序在经过此时间后必须显示。
屏幕保护程序模块的路径	指定屏幕保护程序模块的路径。
屏幕保护程序模块的名称（必填）	输入屏幕保护程序的名称。

有关更多信息，请查看如何创建配置。

10.10.8.13. 配置用户的屏幕保护程序

用户的屏幕保护程序配置允许您添加密码、空闲时间、模块路径和名称等选项。

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 单击**配置**。
3. 点击 **+添加**。
4. 在搜索字段中输入“屏幕”，然后点击**用户的屏幕保护程序**：
   随即将显示“创建用户的屏幕保护程序配置”详细信息页面。
5. 在此页面上配置设置。 请参阅**用户的屏幕保护程序配置设置**主题中的表格，了解有关值的指南。
6. 单击**下一步**，以配置分配设置，然后单击**完成**。

用户的屏幕保护程序配置设置

设置	流程
名称（必填）	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
空闲时间	指定空闲时间（以秒为单位），屏幕保护程序在经过此时间后必须显示。
屏幕保护程序模块的路径	指定屏幕保护程序模块的路径。
屏幕保护程序模块的名称（必填）	输入屏幕保护程序的名称。

有关更多信息，请查看如何创建配置。

10.10.8.14. 设备名称设置

许可证：Silver

默认设备名称配置允许您创建新配置，该配置将在注册时或注册后被推送到设备上，并允许设备命名。 管理员只可定义**受监督 iOS 8 设备**的默认设备名称。 定义默认的设备名称。您可以使用以下变量构建设备名称：

- 设备序列号
- 设备 IMEI
- 设备型号
- Ivanti Neurons for MDM 用户名（仅限本地用户）
- LDAP 组织单元 (OU)
- LDAP 通用名称 (CN)

例如，您可以输入以设备序列号开始，以 LDAP 中定义的用户组织结尾的设备名称 $-$。

默认设备名称设置 (iOS)

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
设备名称	输入默认设备名称的格式，包括可用设备和 LDAP 属性。* 如果生成的设备名称超过 63 个字符，将缩短名称，确保在设备上正确显示。
说明	输入阐明此配置目的的说明。

键入 $ 以查看此字段支持的变量列表（如果有）。

设备名称设置 (Android)

Go app 可以检索 Android 设备名称。 管理员生成“设备详细信息”报告时，将显示实际设备名称而不是设备型号或制造商名称。 如果用户更改设备名称，那么，下一次生成报告时将显示新的名称。 相应设备名称可以在**设备** > **设置** > **设备名称**下查看。

10.10.8.15. 设备壁纸配置

许可证： Silver

设备壁纸配置定义 Android 7.0 设备（处于设备所有者模式）或公司拥有的个人已启用 (COPE) 设备（不含 Android 11 EPO 模式设备）的主屏幕和锁定屏幕的默认壁纸图像。

Android 壁纸设置

定义 Android 设备的默认壁纸图像：

1. 转至**配置**。
2. 单击 **+添加**
3. 单击**设备壁纸**。
4. 单击 Android 图标，以查看 Android 的配置设置部分，并配置以下设置
5. 单击**下一步**

设置	流程
名称	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
上传 Android 壁纸	
为主屏幕和锁定屏幕使用相同的壁纸	选择为两个屏幕上传一个图像。
主屏幕	拖放图像或单击**选择文件**从中选择一个。
锁定屏幕	拖放图像或单击**选择文件**从中选择一个。

6. 选择下列分配选项之一：

- **所有设备**
- **无设备**（默认）
- **自定义**

7. 单击**完成**。

> 上传图像的格式必须是 .jpg 或 .png。

iOS 壁纸设置

可以为 iOS 设备定义默认壁纸图像。

> 此设置仅适用于受监督设备。

1. 转至**配置**。
2. 单击 **+添加**

3. 单击**设备壁纸**。
4. 单击 iOS 图标，以查看 iOS 的配置设置部分，并配置以下设置
5. 单击**下一步**。

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
上传 iPhone 壁纸	
为主屏幕和锁定屏幕使用相同的壁纸	选择该选项为 iPhone 上传单张图像。
主屏幕	拖放图像或单击**选择文件**从中选择一个。
锁定屏幕	拖放图像或单击**选择文件**从中选择一个。
上传 iPad 壁纸	
为主屏幕和锁定屏幕使用相同的壁纸	选择该选项为 iPad 上传单张图像。
主屏幕 锁定屏幕	拖放图像或单击**选择文件**从中选择一个。 拖放图像或单击**选择文件**从中选择一个。

6. 选择下列选项之一：
- **所有设备**
- **无设备**（默认）
- **自定义**
7. 单击**完成**。

> 上传图像的尺寸必须是 640W x 1136H，格式为 .jpg 或 .png。

macOS 壁纸设置

定义 macOS 设备的默认壁纸图像：

1. 转至**配置**。
2. 单击 **+添加**
3. 单击**设备壁纸**。
4. 单击 macOS 图标，查看 macOS 的配置设置部分。
5. 输入桌面图片的路径。
6. 单击**下一步**。
7. 选择下列选项之一：
    - **所有设备**
    - **无设备**（默认）

- **自定义**

8. 单击**完成**

> 您可以根据限制更改壁纸。 如果已启用 macOS 限制配置**允许修改壁纸**，则您可以修改壁纸。

有关更多信息，请查看**如何创建配置**。

10.10.8.16. EMA 服务器集成配置

通过 EMA 服务器集成配置，Windows 10 设备可以链接到配置的 Intel EMA 服务器。 要将设备链接到配置的 Intel EMA 服务器，您应提供原始 EMA 代理的安装目录，并从新 EMA 服务器上传 EMA 代理 .msh 文件。

此功能需要 Bridge。 请查看 **Bridge**，以了解详细信息。

步骤

1. 转到**配置 > + 添加**。
2. 选择 **EMA 服务器集成**配置。
3. 输入配置的名称。
4. 在“配置设置”部分中，单击**选择文件**，以选择 EMA 代理 .msh 文件。

> msh 文件是可从 EMA 服务器下载的代理策略文件。

5. 在原始 **EMA 代理安装目录**字段中，键入安装原始 EmaAgent.exe 文件的位置。
6. 单击**下一步**。
7. 选择下列分配选项之一：
   - 所有设备
   - 无设备（默认）
   - 自定义
8. 单击**完成**。

10.10.8.17. 节能配置

Ivanti Neurons for MDM 可以为负载启用节能配置，方便用于在 Windows 和 macOS 设备上配置节能设置。

适用于：

- Windows 10 至 Ivanti Neurons for MDM 支持的最新发布版本。
- macOS 10.7 至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**节能**配置。
3. 在"选择操作系统"部分，选择 **Windows** 或 **macOS**，然后点击**下一步**。
4. 单击 **+添加描述**，输入配置的简要描述。
5. 针对 Windows，配置以下**节能**设置：
   - 设备使用电池供电
   - 设备已接通电源
6. 配置以下**节能**设置：
   - 台式电脑交流电源节能设置
   - 计算机启动或关闭的计划设置
   - 笔记本电脑交流电源节能设置
   - 笔记本电脑电池节能设置
7. 单击**下一步**，配置分配设置。
8. 选择其中一个分发选项来设置**节能**配置。 有关配置分发选项的详细信息，请参阅使用配置。
9. 单击**完成**。

Windows 节能配置

设备应用新的节能配置或修改现有的节能配置设置后，用户必须重新启动设备才能使更改生效。

设备使用电池供电

设备使用电池供电时，请使用表中的以下节能设置：

设置	描述
开启节能的电池阈值	设备使用电池供电时，输入开启节能的电池电量，可以输入从 0 到 100 的值。 输入表示电池电量的百分比值。 例如，设为 80 时，当电池电量为 80% 或更低时，系统会开启节能模式。 如果不输入值，Ivanti Neurons for MDM 不会更改或更新此设置。 Windows 设备默认设为 70%。
合上盖子时	• **不采取措施**：设备保持开启状态并继续使用电池供电。 • **睡眠**：设备进入睡眠模式，消耗少量电池电量。 计算机仍处于开启状态，打开的应用程序和文件存储在随机存取内存 (RAM) 中。 • **休眠状态**：设备进入休眠模式。 打开的应用程序和文件存储在硬盘上，设备关闭。 • **关机**：设备关闭。 打开的应用程序和文件不保存直接关闭。
选择电源按钮时	• **不采取措施**：设备保持开启状态并继续使用电池供电。 • **睡眠**：设备进入睡眠模式，消耗少量电池电量。 计算机仍处于开启状态，打开的应用程序和文件存储在 RAM 中。 • **休眠状态**：设备进入休眠模式。 打开的应用程序和文件存储在硬盘上，设备关闭。 • **关机**：设备关闭。 打开的应用程序和文件不保存直接关闭。
选择睡眠按钮时	• **不采取措施**：设备保持开启状态并继续使用电池供电。 • **睡眠**：设备进入睡眠模式，消耗少量电池电量。 计算机仍处于开启状态，打开的应用程序和文件存储在 RAM 中。 • **休眠状态**：设备进入休眠模式。 打开的应用程序和文件存储在硬盘上，设备关闭。 • **关机**：设备关闭。 打开的应用程序和文件不保存直接关闭。
打开混合睡眠	• **True**：设备可以进入混合睡眠模式。 打开的应用程序和文件存储在 RAM 和硬盘上。 此模式消耗少量电池电量。 • **False**：防止设备进入混合睡眠模式。

设备已接通电源

设备使用外部电源供电时，请使用表中的以下设置：

设置	描述
开启节能的电池阈值	设备接通电源时，输入开启节能的电池电量，可以输入从 0 到 100 的值。 输入表示电池电量的百分比值。 例如，设为 80 时，当电池电量为 80% 或更低时，系统会开启节能模式。 如果不输入值，Ivanti Neurons for MDM 不会更改或更新此设置。 Windows 设备默认设为 70%。
合上盖子时	• **不采取措施**：设备保持开启状态并继续使用外部电源。 • **睡眠**：设备进入睡眠模式，消耗少量外部电源电量。 计算机仍处于开启状态，打开的应用程序和文件存储在 RAM 中。 • **休眠状态**：设备进入休眠模式。 打开的应用程序和文件存储在硬盘上，设备关闭。 • **关机**：设备关闭。 打开的应用程序和文件不保存直接关闭。
选择电源按钮时	• **不采取措施**：设备保持开启状态并继续使用外部电源。 • **睡眠**：设备进入睡眠模式，消耗少量外部电源电量。 计算机仍处于开启状态，打开的应用程序和文件存储在 RAM 中。 • **休眠状态**：设备进入休眠模式。 打开的应用程序和文件存储在硬盘上，设备关闭。 • **关机**：设备关闭。 打开的应用程序和文件不保存直接关闭。
选择睡眠按钮时	• **不采取措施**：设备保持开启状态并继续使用外部电源。 • **睡眠**：设备进入睡眠模式，消耗少量外部电源电量。 计算机仍处于开启状态，打开的应用程序和文件存储在 RAM 中。 • **休眠状态**：设备进入休眠模式。 打开的应用程序和文件存储在硬盘上，设备关闭。 • **关机**：设备关闭。 打开的应用程序和文件不保存直接关闭。
打开混合睡眠	• **True**：设备可以进入混合睡眠模式。 打开的应用程序和文件存储在 RAM 和硬盘上。 此模式消耗少量外部电源电量。 • **False**：防止设备进入混合睡眠模式。

macOS 节能配置

台式电脑交流电源节能设置

使用以下设置来配置 macOS 桌面设备的交流电源节能设置：

设置	描述
名称	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
电源故障解决后自动启动	启用设备的电源故障解决后自动启动。
闲置以下时间后让硬盘进入睡眠状态	启用复选框可让硬盘在闲置固定的时间间隔后进入睡眠状态，可选择 1 到 180 分钟的间隔。 值为 0 分钟时则表示永远不会让硬盘进入睡眠状态。
闲置以下时间后关闭显示器	启用复选框可让显示器在闲置固定的时间间隔后关闭，可选择 1 到 180 分钟的间隔。 值为 0 分钟时则表示永远不会关闭显示屏。
动态电源 STEP	选中复选框可启用动态电源 STEP。
降低处理器速度	选中复选框可降低处理器速度。
闲置以下时间后让计算机进入睡眠状态	启用复选框可让计算机在闲置固定的时间间隔后进入睡眠状态，可选择 1 到 180 分钟的间隔。 值为 0 分钟时则表示永远不会让计算机进入睡眠状态。
网络访问时唤醒	选中复选框可唤醒计算机以进行网络访问。
调制解调器响铃时唤醒	选中复选框可通过调制解调器响铃唤醒计算机。

计算机启动或关闭的计划设置

使用以下设置来配置 macOS 设备，以计划设备的启动或关闭。

关闭设备设置

选中**关闭设备**复选框，以按照固定的时间间隔关闭设备。

设置	描述
事件类型	从下拉列表中选择一种事件类型： • 睡眠 • 重新开始 • 关闭
时间	选择一周中的一天或多天来计划事件类型。
时刻	选择计划事件类型的时间。

启动或唤醒设备设置

选中**启动或唤醒设备**复选框，以按照固定的时间间隔唤醒设备。

设置	描述
事件类型	从下拉列表中选择一种事件类型： • 唤醒 • 启动/唤醒
时间	选择一周中的一天或多天来计划事件类型。
时刻	选择计划事件类型的时间。

笔记本电脑交流电源节能设置

使用以下设置来配置 macOS 笔记本电脑设备的交流电源节能设置：

设置	描述
电源故障解决后自动启动	启用设备的电源故障解决后自动启动。
闲置以下时间后让硬盘进入睡眠状态	启用复选框可让硬盘在闲置固定的时间间隔后进入睡眠状态，可选择 1 到 180 分钟的间隔。 值为 0 分钟时则表示永远不会让硬盘进入睡眠状态。
闲置以下时间后关闭显示器	启用复选框可让显示器在闲置固定的时间间隔后关闭，可选择 1 到 180 分钟的间隔。 值为 0 分钟时则表示永远不会关闭显示屏。
动态电源 STEP	选中复选框可启用动态电源 STEP。
降低处理器速度	选中复选框可降低处理器速度。
闲置以下时间后让笔记本电脑进入睡眠状态	启用复选框可让笔记本电脑在闲置固定的时间间隔后进入睡眠状态，可选择 1 到 180 分钟的间隔。 值为 0 分钟时则表示永远不会让笔记本电脑进入睡眠状态。
网络访问时唤醒	选中复选框可唤醒笔记本电脑以进行网络访问。
调制解调器响铃时唤醒	选中复选框可通过调制解调器响铃唤醒笔记本电脑。

笔记本电脑电池节能设置

使用以下设置来配置 macOS 笔记本电脑电池节能设置：

设置	描述
电源故障解决后自动启动	启用设备的电源故障解决后自动启动。
闲置以下时间后让硬盘进入睡眠状态	启用复选框可让硬盘在闲置固定的时间间隔后进入睡眠状态，可选择 1 到 180 分钟的间隔。 值为 0 分钟时则表示永远不会让硬盘进入睡眠状态。
闲置以下时间后关闭显示器	启用复选框可让显示器在闲置固定的时间间隔后关闭，可选择 1 到 180 分钟的间隔。 值为 0 分钟时则表示永远不会关闭显示屏。
动态电源 STEP	选中复选框可启用动态电源 STEP。
降低处理器速度	选中复选框可降低处理器速度。
闲置以下时间后让计算机进入睡眠状态	启用复选框可让笔记本电脑电池在闲置固定的时间间隔电池后进入睡眠状态，可选择 1 到 180 分钟的间隔。 值为 0 分钟时则表示永远不会让笔记本电脑电池进入睡眠状态。
网络访问时唤醒	选中复选框可唤醒笔记本电脑电池以进行网络访问。
调制解调器响铃时唤醒	选中复选框可通过调制解调器响铃唤醒笔记本电脑电池。

10.10.8.18. 以太网配置 (macOS)

许可证：Gold

适用于：macOS 10.13+ 或支持的较新版本。

管理员可以配置不同的以太网接口。 下列有效负载可用于配置以太网：

- 全局以太网
- 第一个活动以太网
- 第一个以太网
- 第二个活动以太网
- 第二个以太网
- 第三个活动以太网
- 第三个以太网

> 适用于配置以太网的不同有效负载是默认回退全局、第一个、第一个活动、第二个、第二个活动、第三个和第三个活动以太网接口。 在安装第一个、第一个活动、第二个、第二个活动、第三个和第三个活动以太网接口方面，Apple 存在已知问题。

以太网配置

程序

1. 选择**配置**。
2. 单击 **+添加**
3. 在搜索字段中输入**以太网**，然后选择**以太网**配置。
4. 输入名称并描述配置。
5. 从下拉列表中选择配置设置。
6. 输入**以太网配置设置**。
7. 单击**下一步**。
8. 选择**启用此配置**选项。
9. 选择以下其中一个渠道选项，以应用配置：
    - 设备渠道（最常见）
    - 用户渠道（当前注册用户）
10. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义
11. 单击**完成**。

以太网配置设置

使用下表中的设置，配置以太网。 有关这些设置的更多信息，请查看 **Apple 文档**。

设置	描述
协议	
接受的 EAP 类型	选择可用于访问该网络的 EAP 类型： • 传输层安全性 (TLS)：TLS 是两台连接互联网的计算机之间建立加密会话的协议。 这会验证服务器的身份，并防止黑客拦截任何数据。 • TTLS：在**内部标识**字段中，选择其中一个身份验证协议，例如 OS 默认设置、PAP、CHAP、MSCHAP、MSCHAPv2 和 EAP。 • PEAP • LEAP • EAP-SIM：在 **RAND 的 EAP SIM 号**字段中，从下拉列表中选择 RAND 数量。 • EAP-AKA • EAP-FAST：选择定义身份验证方法的 EAP-FAST 选项： ◦ **使用 PAC**：选择以使用代理自动配置 (PAC)。 ◦ **预配 PAC**：选择以允许预配 PAC。 否则，仅可使用设备上已调配的 PAC。 该选项仅在您选择“使用 PAC”之后可用。 ◦ **匿名预配 PAC**：选择以允许在无需对服务器进行身份验证的情况下预配 PAC。 该选项仅在您选择“调配 PAC”之后可用。
身份验证	**用户名**：指定访问网络所需的用户名。 如果保留此处为空，将会提醒设备用户填写用户名。 • 使用每连接密码：选择以提示设备用户为每连接输入密码。 在设备重新加入相同网络时，将提示设备用户重新进行身份验证，才可以加入网络。 在每次启动连接时，要求输入密码。 • **在连接网络时提示输入一次性密码**：在配置推送到设备时，仅要求输入密码一次。 在每次连接和断开网络时，不要求输入任何密码。 **密码**：（可选）输入访问此网络的密码。 否则，将会提示设备用户输入所需密码以访问网络。 **外部标识**：（可选）对于 TTLS、PEAP 和 EAP-FAST，选择以允许设备用户隐藏身份。 用户的真实姓名仅出现在内部的加密通道中。 此选项可以增加安全性，因为攻击者无法清楚地看到正在进行身份验证的用户名。 **系统模式凭据源标识**：系统模式用于计算机身份验证。 使用系统模式的身份验证将在用户登录计算机前实施。 通常，系统模式会配置为对身份验证提供本地证书颁发机构颁发的计算机 X.509 证书 (EAP-TLS)。
信任	**可信证书：**选中复选框以从列表中选择多个证书。 **受信任的服务器证书名称**：添加证书名称。 • **允许信任异常**：允许用户做出信任决定（通过对话框）。 • **需要 TLS 证书** **允许对 EAP 身份验证使用最大 TLS 版本** **允许对 EAP 身份验证使用最小 TLS 版本** **TLS 受信证书：MobileIron 代理 CA 证书**

有关更多信息，请查看[如何创建配置]。

10.10.8.19. Google BeyondCorp 配置

Ivanti Neurons for MDM 可以与 Google BeyondCorp 集成，实现条件访问。 Ivanti Neurons for MDM 会向 Google BeyondCorp 发送设备合规状态信号。 这可以确保只有符合条件的 N-MDM 设备才能访问 Google Workspace 应用程序。

适用于

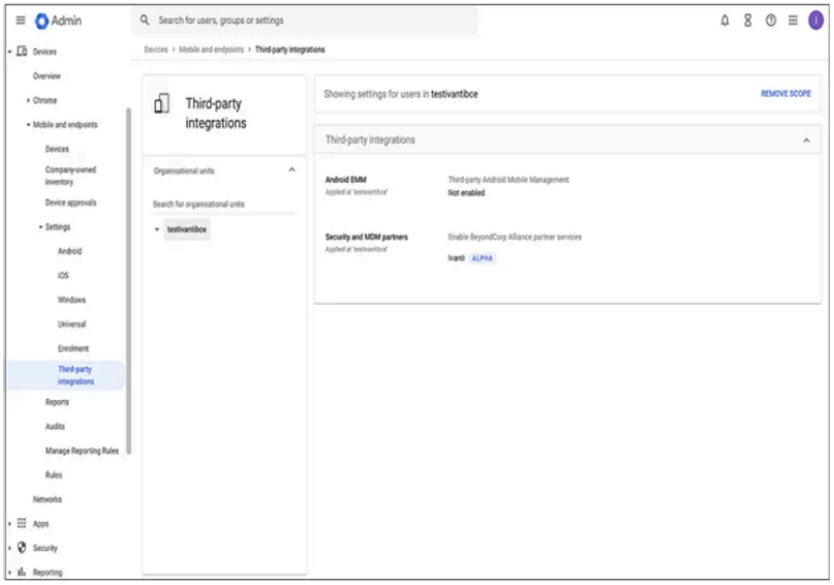
- iOS
- Android
- Windows

先决条件

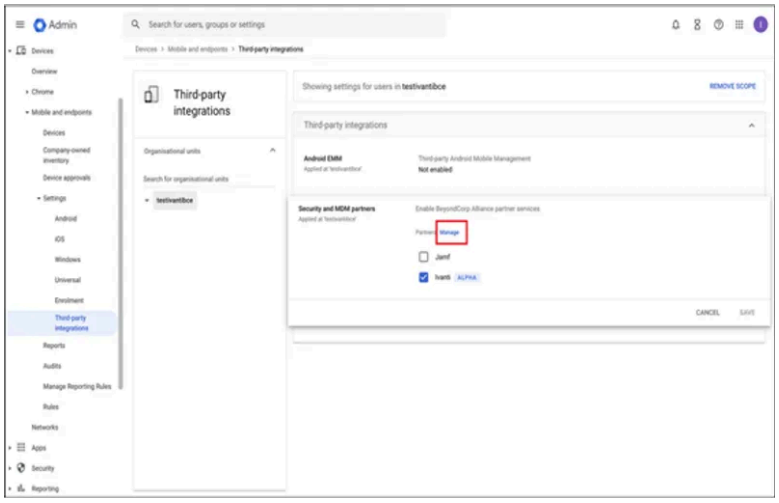
- 针对 Ivanti Neurons for MDM，必须拥有 Ivanti Professional Plus / Premium 许可证。
- 针对 Google，必须拥有 BeyondCorp Enterprise、Google Workspace Enterprise 或 Cloud Identity Premium 许可证。
- 对于 Windows，您必须在设备上安装以下内容：
  - Ivanti Bridge
  - Google Chrome

程序 (Google)

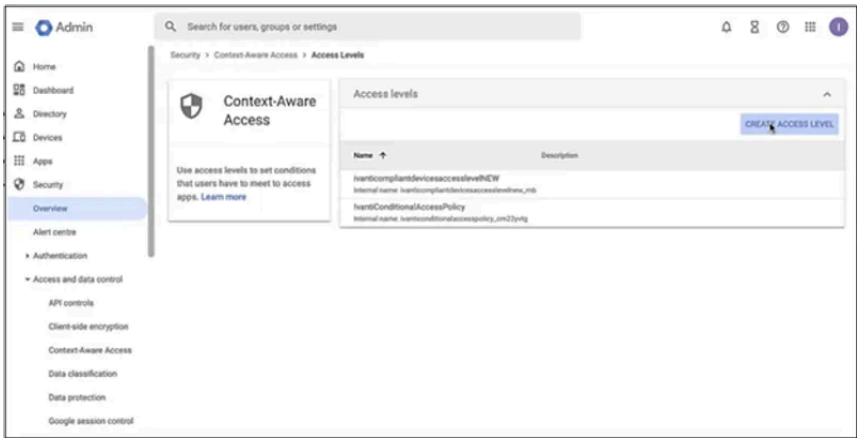
1. 使用管理员凭据登录 **Google 管理员控制台**。
2. 前往**设备** > **移动和端点** > **设置** > **第三方集成**。



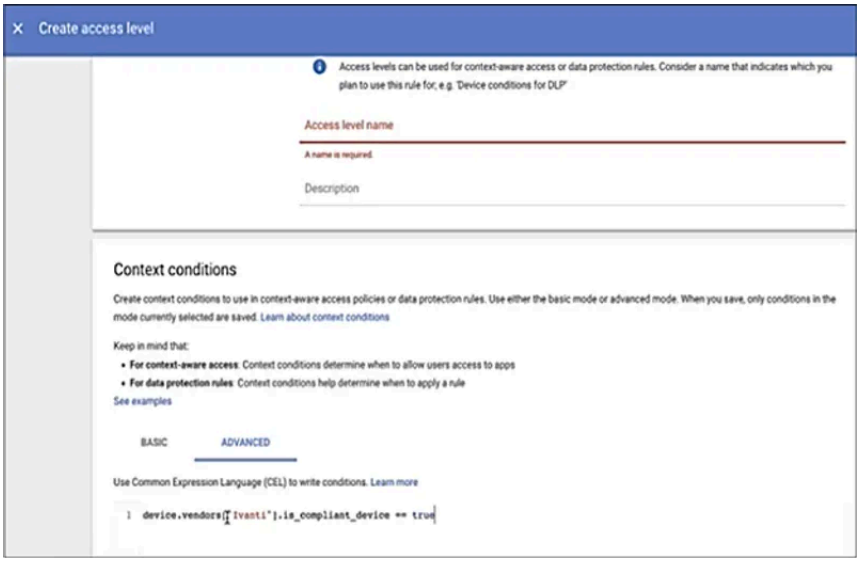
3. 点击**安全和 MDM 合作伙伴** > **管理**。



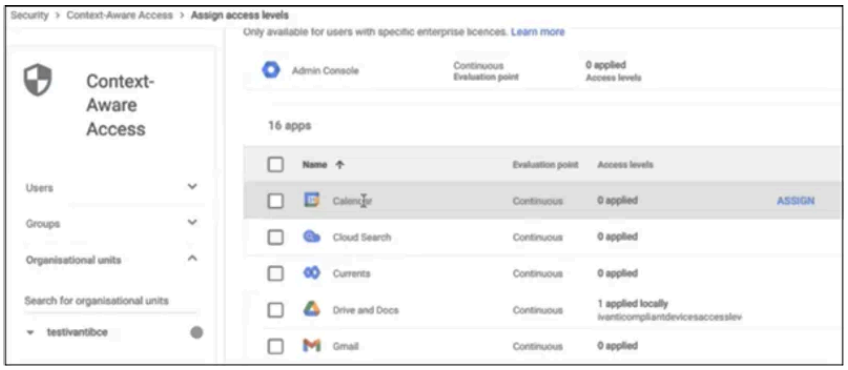
4. 在**管理合作伙伴连接**窗口中，选择 **Ivanti**。
5. 点击**打开连接**。
   系统将重定向到 Ivanti Neurons for MDM 登录页面；输入租户管理员凭据。 登录租户后，系统会显示 **Google BeyondCorp** 已启用且已自动链接到 Google 账户。
6. 在 Google 管理员控制台中，前往**安全** > **上下文相关访问** > **访问级别**。



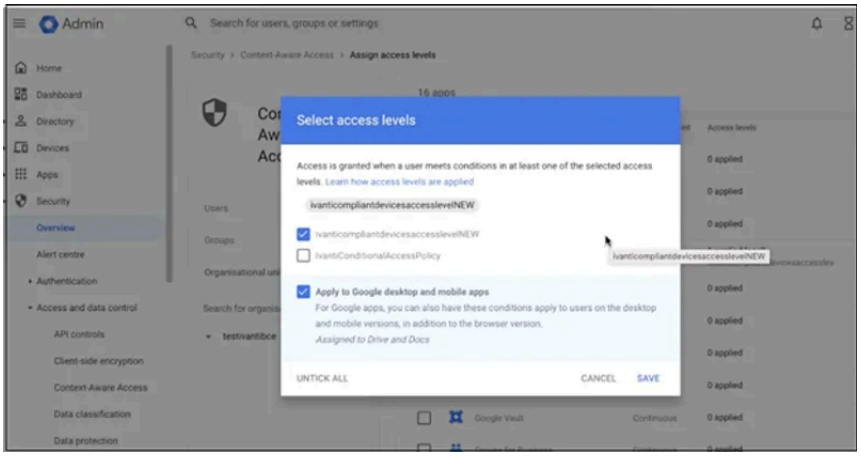
7. 点击**创建访问级别**。
   在“创建访问级别”窗口的“上下文条件”部分下，点击**高级**并提供所需信息。



8. 前往**安全** > **上下文相关访问** > **访问级别**，选择要为其分配策略的应用程序。



9. 单击**分配**。
10. 在**选择访问级别**窗口中，选择要分配的策略并点击**保存**。



完成上述设置后，可以使用 **Google BeyondCorp** 创建合作伙伴设备合规性配置。

程序 (Ivanti Neurons for MDM**)**：

1. 前往**配置** > **添加配置**。

2. 选择**合作伙伴设备合规性**配置。
3. 屏幕上随即显示“创建合作伙伴设备合规性”配置页面。
   输入配置的名称。
4. 在“选择合作伙伴”列表下，选择 **Google BeyondCorp**。
5. 屏幕上随即显示“配置设置”部分。 确保 iOS 和 Android 设备的“报告合规性状态”选项已设为“开启”。
   单击**下一步**。
6. 选择**启用此配置**。
7. 选择**自定义**分发选项
8. 选择**自定义分发**选项下的**用户/用户组**。
9. 在**选择以下选项来分发此配置**部分，从列表中选择用户/用户组。
10. 单击**完成**。

> Google BeyondCorp 服务器可以通过应用程序管理的配置 P 清单唯一地标识每个设备。
> 

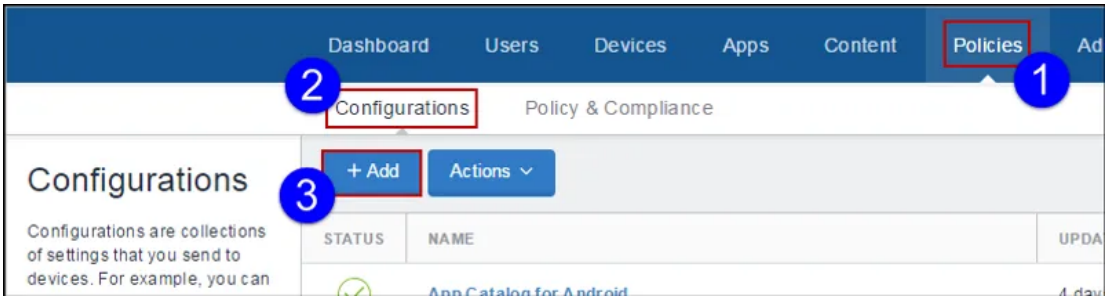
10.10.8.20. 锁定屏幕消息配置

在登录和锁定屏幕上显示消息和资产标记信息。 这适用于使用 iOS 9.3 或支持的更新版本的受监管设备。

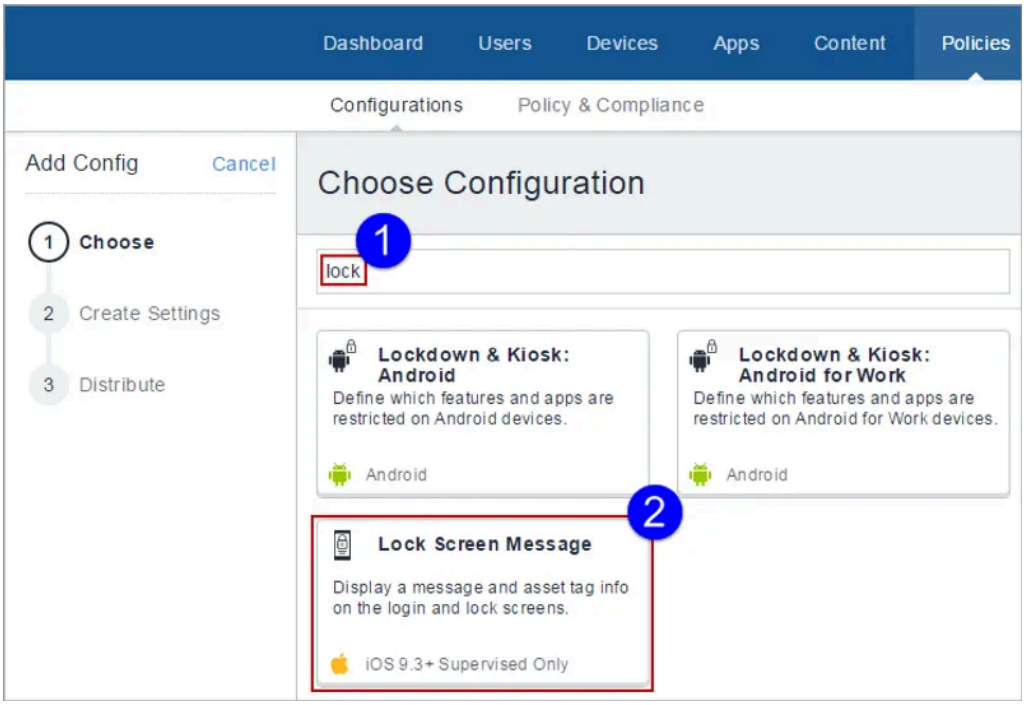
创建锁屏消息配置

程序

1. 选择**配置**。
2. 单击 **+添加**



在搜索字段中键入**锁定**，然后单击**锁定屏幕消息**配置：



将显示锁定屏幕消息配置详细信息页面。
在此页面上配置设置。 请参阅锁屏消息配置设置小节中的表格，了解有关值的指南。

5. 单击**下一步**，以配置分配设置，然后单击**完成**。

锁定屏幕消息配置设置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
锁屏脚注	此文本会显示在登录窗口和锁定屏幕上。
资产标记信息	此文本会显示在登录窗口和锁定屏幕底部。

有关更多信息，请查看**如何创建配置**。

10.10.8.21. 登录窗口配置 - macOS

步骤

1. 登录 Ivanti Neurons for MDM。
2. 前往**配置** > **添加配置**。
3. 点击（或选择）**登录窗口**。
4. 在**名称**字段中，输入登录窗口配置的名称。
5. 点击 **+ 添加说明**添加详细信息。
6. 在**配置设置**部分下，提供以下字段：
    - **管理员主机信息**：输入主机名、IP 地址或 SystemVersion。
    - **允许列表**：系统允许用户登录的用户 GUID 或用户的组 GUID 列表。 星号 ('*') 字符串会指定所有用户或组。
    - **自动登录密码**：输入自动登录密码。
    - **拒绝列表**：系统禁止登录的用户 GUID 或用户的组 GUID 列表。 此列表优先于“AllowList”键中的列表。
    - **登录窗口文本**：输入登录窗口文本。
    - 选中其他选项对应的复选框，例如：
        - **禁用控制台访问**
        - **禁用 FDE 自动登录（FileVault 磁盘加密）**
        - **禁用即时屏幕锁定功能**
        - **显示用户列表时隐藏管理员用户**
        - **仅显示网络和系统用户**
        - **隐藏移动帐户**
        - **显示网络用户**
        - **禁用注销菜单项**
        - **用户登录时禁用关闭电源**
        - **在用户登录时禁用重新启动菜单项**
        - **禁用重启项**
        - **显示名称和密码对话框**
        - **显示其他用户 - 托管**
        - **显示输入菜单**
        - **禁用关机按钮**
        - **禁用“睡眠”按钮**
        - **禁用关机菜单按钮**
7. 单击**完成**。

10.10.8.22. macOS 系统扩展配置

在没有内核级访问权限的情况下，系统扩展配置允许安装扩展类型，例如驱动程序扩展、网络扩展和端点安全扩展。

步骤

适用于：macOS 10.15+

1. 转到**配置** > **+ 添加**。
2. 在搜索字段中，键入**扩展**，然后单击**系统扩展**配置。
3. 输入配置的**名称**和**描述**。
4. 在**允许的系统扩展**下方， **+ 添加允许的团队标识符**和**允许的系统扩展**。
5. 在**允许的系统扩展类型**下方，**+ 添加允许的团队标识符**和**允许的系统类型**。
6. 选中**允许用户覆盖**选项。
7. 单击**下一步**。
8. 选择**启用此配置**选项。
9. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义。
10. 单击**完成**。

> 在 macOS 12 中，RemovableSystemExtensions 允许应用在卸载应用时不经管理员批准即可禁用其系统扩展。

10.10.8.23. 仅限 MAM

通过 Ivanti Neurons for MDM，您可以将 iOS 和 Android 设备指定为 MAM 专用，并向此类设备提供移动应用程序管理 (MAM) 功能。 通过 MAM Only 部署，您可以分发并管理应用，无需管理设备。

仅限 MAM 解决方案 - Ivanti AppStation 替代方案

作为 Ivanti AppStation 的替代解决方案，Ivanti 提供了一种使用 Ivanti Go 客户端的现代且灵活的移动应用程序管理 (MAM) 解决方案，可用于 iOS 和 Android 平台。

新的仅限 MAM 的解决方案引入了集成的应用程序目录和 Ivanti Neurons for MDM Web 剪辑功能，共同满足了 App Station 之前解决的核心用例的要求，为用户和管理员提供了简化、安全和统一的应用程序管理体验。

关键功能

- **应用程序内应用程序目录**：直接在 Go 客户端中托管和分发经过批准的托管应用程序。
- **应用程序配置和更新**：支持应用程序级配置和版本更新，通过 MAM 策略强制执行。
- Ivanti Neurons for MDM**要求**：非常适合无法注册 Ivanti Neurons for MDM 的 BYOD 和承包商场景。

使用 Web 剪辑以便于访问

- **直接访问应用程序目录**：通过 Ivanti Neurons for MDM 部署 Web 剪辑，提供应用程序目录或特定基于 Web 的企业应用程序的快捷方式。
- **自定义应用程序快捷方式**：允许用户从主屏幕快速启动常用资源。

增强的管理和用户体验

- **统一界面**：将应用程序目录、Web 访问和合规性消息组合到一个体验中。
- **简化管理**：无需维护单独的解决方案（即 App Station），降低了复杂性和配置漂移的风险。

灵活性和自定义

- **自定义目录视图**：根据用户角色、地理位置或组织单位自定义应用程序目录内容。
- **使用现有基础设施**：利用您现有的 Ivanti Neurons for MDM/MAM 投资（不需要单独的基础设施）。

支持双重角色用户

Ivanti MAM-Only 解决方案旨在支持现代工作场景，包括具有双重角色的用户：

- **全职员工 - 组织 A**：经由通过 Ivanti Neurons for MDM 部署的 Web 剪辑（例如，Apps@Work)访问企业应用程序。
- **承包商 - 组织 B**：在仅限 MAM 模式下使用 Ivanti Go 客户端安全地访问托管应用程序，而无需在 Ivanti Neurons for MDM 中注册设备。

这使得对必要应用程序的无缝、基于角色的访问成为可能，而不会出现配置文件冲突或设备管理重叠。

迁移指导

Ivanti 强烈建议 App Station 客户计划并执行向基于 Go 客户端的仅限 MAM 解决方案过渡。 有关分步迁移帮助，请参阅以下资源：

- 仅限 Ivanti MAM 解决方案

- **Go 客户端中的应用程序目录配置**
- **创建 Web 剪辑配置**

如果您有任何问题或需要迁移帮助，请联系 **Ivanti 支持**或您的客户成功经理。

10.10.8.24. 托管的 Google Play 配置

管理员可以配置自动更新设置，Google Play 商店可使用此设置更新 Android Enterprise 设备上的应用程序。

要配置自动更新设置：

1. 转到**配置 > + 添加**。
2. 选择**托管的 Google Play** 配置。
3. 输入配置的名称。
4. 输入描述。
5. 在"配置设置"部分，选择一个选项从 Google Play 更新应用程序。

设置	采取何种措施
用户定义	设备用户可以设置自动更新应用维护时段设置，以定义何时更新应用。 1. 在**开始时间**字段中，选择执行应用更新的时间。 2. 在**持续时间**字段中，选择执行更新的持续时间（以小时为单位）。 最小与最大范围介于 1 小时至 24 小时之间。 应用可以在开始时间至选定时段的期间内随时更新。 例如，如果"开始时间"设置为 6PM，"时段"设置为 12hrs，应用可能会在 6PM 至 6AM 之间的时段内随时更新。
无	Google Play Store 从不自动更新设备上的应用程序。
仅 Wifi	Google Play Store 会自动更新设备上的应用程序，但只使用 Wi-Fi，而不是手机连接。
始终	Google Play Store 使用 Wi-Fi 或手机连接自动更新设备上的应用程序。

6. 单击**下一步**。
7. 选择下列分配选项之一：

- 所有设备
- 无设备（默认）
- 自定义

8. 单击**完成**。

10.10.8.25. 迁移助手设置

使用**迁移助手设置**配置受监控设备上的迁移助手设置。 此配置可帮助管理员应用基于策略的一致控件，以管理用户在设备设置或迁移期间传输数据、应用程序和设置的方式。

适用于：

- macOS 26.4+ 受监控设备至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**迁移助手设置**配置。
3. 按照下表配置**迁移助手设置**：

设置	采取何种措施
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
应该进行托管迁移	选中复选框以启用和管理设备的迁移。 切换**推送至设备**按钮，启用设备迁移。
排除的账户	输入要从迁移中排除的账户名称。 切换**推送至设备**按钮，以启用账户排除。
排除的路径	输入要从迁移中排除的路径名称。 切换**推送至设备**按钮，以启用路径排除。
必需路径	输入要包含在迁移中的路径名称。 切换**推送至设备**按钮，启用路径包含。
应迁移安全隐私设置	选中复选框以启用从设备迁移安全隐私设置。 切换**推送至设备**按钮，启用安全隐私设置的迁移。

4. 单击**下一步**，配置分配设置。
5. 选择一个分发选项以设置**迁移助手设置**配置。 有关配置分发选项的详细信息，请参阅使用配置。
6. 单击**完成**。

10.10.8.26. 通知配置

使用通知配置，管理员可以为 iOS 设备安排无提示和可见的通知。 也可以克隆、导出或删除通知配置。

步骤

1. 转到**配置 > + 添加**。
2. 选择**通知**配置。
3. 输入配置的名称。
4. 输入描述。
5. 在配置设置部分，选择**通知计划**选项中的一个或两个：
    - 无提示通知计划 - 无提示通知用于支持由 Ivanti Neurons for MDM 发起的背景设备管理操作。 它们支持自动操作，例如合规性检查、策略更新和应用程序更新，而无需用户交互。 Ivanti Neurons for MDM 在配置的级别向设备发送无提示通知。
    - 可见通知计划 - 当需要用户知晓或操作来维护设备合规性、安全性或功能时，将使用可见通知。 可见通知仅在指定的时间间隔后触发，即使在此期间发生多个操作或事件也是如此。 仅当在可见通知间隔期间未发送无提示通知时，设备上才会显示可见通知。
6. 单击**下一步**。
7. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义
8. 单击**完成**。

MTD 设备的可见通知内容 - 您的设备可能容易受到威胁。 请启动 Ivanti Go 应用程序并检查 Threat Defense 状态。

非 MTD 设备的可见通知内容 - 要接收增强的安全功能并确保最新的保护措施，请在设备启动应用程序，以获得更安全的用户体验。

10.10.8.27. 打印机设置

Ivanti Neurons for MDM 允许您创建打印机配置文件，并将其添加到设备。 此功能需要 Bridge。 请查看 **Bridge**，以了解详细信息。

> 在打印机配置文件发送到设备时，打印机必须处于活动状态，否则无法发现设备。

要为 Windows 设备设置打印机设置配置：

1. 转到**配置 > + 添加**。
2. 选择**打印机设置**配置。
3. 输入配置的名称。
4. 选择 **Windows** 选项。
5. 在**配置设置**部分，配置以下设置：

设置	流程
名称	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
Windows 打印机设置	
共享打印机	如果选择**共享打印机**选项，该打印机将与其他设备共享。配置以下字段： **名称**：输入打印机配置的名称。 **描述**：输入打印机的描述。 **打印服务器**：输入打印服务器的 IP 地址。 **共享打印机名称**：输入打印机名称。
网络附加的打印机	在选择**网络附加**选项时，打印机仅可由附加网络中的设备访问。 配置以下字段： **名称**：输入打印机配置的名称 **描述**：输入打印机的描述。 **打印名称**：输入网络中打印机的名称。 **打印机主机地址**：输入打印机的主机 IP 地址。 **打印机端口号**：选择网络打印机的端口号。 **打印机驱动程序名称**：输入打印机驱动程序的名称。 **打印机驱动程序 URL**：输入打印机驱动程序的 URL。 对于打印机驱动程序，上传包含所需文件的 ZIP 存档。 ZIP 归档必须包含以下文件： • .inf 文件（驱动程序信息） • .cat 文件（目录/签名） • INF 引用的任何其他驱动程序二进制文件（如 .dll、.sys 等）

6. 点击**下一步**。
7. 选择下列分配选项之一：

- 所有设备
- 无设备（默认）
- 自定义

8. 单击**完成**。

要为 macOS 设备设置打印机设置配置：

1. 转到**配置 > + 添加**。
2. 选择**打印机设置**配置。
3. 输入配置的名称。
4. 选择 **macOS** 选项。
5. 在**创建打印机配置**部分中，配置以下设置：

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
配置设置	更新以下字段，并为 macOS 设备设置打印机： • 允许本地打印机 • 默认打印机显示名称 • 页脚字体名称 • 页脚字体大小 • 用户打印机列表 • + 添加打印机

6. 点击**下一步**
7. 选择下列分配选项之一：

- 所有设备
- 无设备（默认）
- 自定义

8. 单击**完成**。

10.10.8.28. 删除 Bloatware 配置

删除 Bloatware 配置允许您选择设备中安装的需要被强制删除的应用程序列表。 先决条件是为此配置设置 Bridge。 请查看 **Bridge**，以了解更多详细信息。

若要运行或卸载应用程序：

1. 在**配置**选项卡中，单击**+添加**。
2. 选择**移除 Bloatware** 配置。 系统将显示**移除 Bloatware 配置**页面。
3. 在**名称**字段中，为配置输入恰当的名称。
4. 单击 **+添加描述**链接，以便为配置添加描述。该字段是可选项。
5. 在**配置设置**部分，选择应删除或卸载的应用程序。 您也可以使用桌面应用程序列表中显示的应用程序名称，在搜索字段中搜索应用程序。

> 在创建**移除 Bloatware** 配置前，应通过转到**应用 > 桌面应用 > 获取应用**来获取应用。 否则，在创建**移除 Bloatware** 配置时，将没有应用可供搜索或选择。

可以删除文件类型 .appx、.appxbundles、.xap 和 .msi，但不能删除 .exe 文件类型。

6. 在高级选项中，配置以下选项：

选项	说明
该配置的运行间隔为	设置运行配置的间隔持续时间（以分钟为单位）。
在登录时运行	选中该复选框，以便在登录时运行配置。
卸载后禁止强制重启	选中该复选框，以防止在卸载应用程序后强制重启。

10.10.8.29. Safari 扩展和设置配置

Safari 扩展程序

Ivanti Neurons for MDM 可用于管理受监管 iOS 和 macOS 设备上的 Safari 扩展。 管理员可有效管理标准和隐私浏览模式的 Safari 扩展。

适用于：

- iOS 18.0 受监管设备至 Ivanti Neurons for MDM 支持的最新发布版本。
- macOS 15.0 受监管设备至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择 **Safari 扩展设置**配置。
3. 根据下表配置 **Safari 扩展设置**的设置：

设置	描述
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
扩展 ID	输入组合的扩展标识符。 例如，*Identifier (TeamIdentifier)*。 为所有扩展名输入 *。 要生成此字符串，请使用代码符号 *-dv <path_to_appex>*。 浏览器扩展位于应用程序捆绑包内的插件文件夹中。 预期格式为 *Identifier (TeamIdentifier)*。对于 macOS 上无法使用的扩展，应用程序开发人员应提供相关信息。
扩展状态	选择下列选项之一： • **允许**：用户可以打开或关闭扩展。 • **始终开启**：扩展对用户始终“开启”。 • **始终关闭**：扩展对用户始终“关闭”。
隐私浏览状态	选择下列选项之一： • **允许**：用户可以在“隐私浏览”模式中打开或关闭扩展。 • **始终打开**：即使在“隐私浏览”模式下，扩展对用户也始终“开启”。 • **始终关闭**：无法使用扩展。
允许的域	输入域或子域的值来授予 Safari 扩展访问。 可以输入多个域或子域的值。 如果在扩展 ID 字段中输入 *，则允许的域设置不适用于设备。
拒绝的域	输入域或子域的值来限制 Safari 扩展访问。 可以输入多个域或子域的值。 如果在扩展 ID 字段中输入 *，则拒绝的域设置不适用于设备。

4. 点击 **+添加**可添加多个**扩展**。
5. 单击**下一步**，配置分配设置。
6. 选择其中一个分发选项来设置 **Safari 扩展设置**配置。 有关配置分发选项的详细信息，请参阅使用配置。

7. 单击**完成**。

Safari 设置

Ivanti Neurons for MDM 可用于管理受监管 iOS 和 macOS 设备上的 Safari 设置。 管理员可有效管理标准和隐私浏览模式的 Safari 扩展。

适用于：

- iOS 26.0+、iPad 26.0+、macOS 26.0+、visionOS 26.0+ 测试版，直至 Ivanti Neurons for MDM 支持的最近发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择 **Safari 扩展和设置**配置。
3. 点击 **Safari 设置**。
4. 根据下表配置 **Safari 设置**的各项设置：

设置	描述
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
配置设置	选择以下选项之一可设置开始页面类型： • **开始**：使用默认的开始页面。 Safari 禁用现有主页。 • **主页**：使用指定的主页 URL。 Safari 将此设置为主页。 • **扩展**：使用 Safari 扩展指定的页面，其标识符为 ExtensionIdentifier。 Safari 禁用现有主页。

5. 单击**下一步**，配置分配设置。
6. 选择其中一个分发选项来设置 **Safari 设置**配置。 有关配置分发选项的详细信息，请参阅使用配置。
7. 单击**完成**。

Safari 隐私设置

Safari 隐私设置允许管理员使用声明性设备管理 (DDM) 为 Safari 中的特定网站定义默认相机和麦克风权限。 此功能可帮助组织集中管理网站隐私权限，并在受管 Apple 设备上提供更一致的浏览体验。

适用于：

- iOS 27.0+ 和 macOS 27.0+，直至 Ivanti Neurons for MDM 支持的最新发布版本。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择 **Safari 扩展和设置**配置。
3. 单击 **Safari 隐私设置**。
4. 根据下表配置 **Safari 隐私设置**的各项设置：

设置	描述
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。

配置设置	• **添加 URL**：输入 URL 以应用设置。
	• **+添加默认值**：指定要应用于此设置的默认值。
	  ◦ 相机 - 允许/拒绝
	  ◦ 麦克风 - 允许/拒绝
	  ◦ 组织理由（必填）

5. 单击**下一步**，配置分配设置。
6. 选择其中一个分发选项来设置 **Safari 设置**配置。 有关配置分发选项的详细信息，请参阅使用配置。
7. 单击**完成**。

10.10.8.30. Samsung 手机限制配置

配置

Samsung 手机限制配置允许您在 Samsung 设备中设置呼叫限制和例外。 这些限制限制了用户可以拨打或接听的电话号码。

适用于：所有具有 Knox SDK 2.0+ 的 Samsung 设备。

若要配置 Samsung 手机限制：

1. 在**配置**选项卡中，单击**+添加**。
2. 选择 **Samsung 手机限制**配置。 将显示 **Samsung 手机限制配置**页面。
3. 在**名称**字段中，为配置输入恰当的名称。
4. 单击 +**添加描述**链接，以便为配置添加描述。该字段是可选项。
5. 在**配置设置**部分，配置以下选项：

   选项

   描述

   来电

   被阻止的号码

   单击“添加”图标，添加号码和 Java 正则表达式来定义来电限制。

   已加入允许列表的号码

   单击“添加”图标，添加号码和 Java 正则表达式，以便为来电定义一组较大的被阻止号码中的允许号码。

   如果没有被阻止的号码，该选项不会有任何效果。

   呼出电话

   被阻止的号码

   单击“添加”图标，添加号码和 Java 正则表达式来定义呼出电话的限制。

   已加入允许列表的号码

   单击“添加”图标，添加号码和 Java 正则表达式，以便为呼出电话定义一组较大的被阻止号码中的允许号码。

   如果没有被阻止的号码，该选项不会有任何效果。
6. 单击**完成**，以便将设置推送到所选设备。

> 当设备被停用时，所有的通话限制都将从设备中删除。

有关更多信息，请查看如何创建配置。

10.10.8.31. 默认浏览器配置 - iOS 和 visionOS

用于更改 iOS 和 visionOS 设备上默认应用程序的设置的配置。

先决条件

- 仅适用于 iOS (18.2+) 和 visionOS 2.2 版本。
- 可在 iOS 设备上通过**设置** - **应用程序** - **默认应用程序**设置这些应用程序。

步骤

1. 在**设备**页面上，注册 iOS (18.2 +) 设备或 visionOS 2.2 设备。
2. 导航至**配置** > **添加配置** > **默认应用程序设置**，以在 iOS 设备上设置默认浏览器。
3. 点击**配置** > **创建设置** > **创建默认应用程序设置配置**
4. 在“配置详情”部分下，提供**名称**和**说明**。
5. 在“配置设置”>“添加应用程序”>“通过查找添加”下，搜索所需的浏览器。 随即显示浏览器列表。
6. 从列表中选择所需的浏览器。
7. 在**创建默认应用程序设置配置**页面中，点击**自定义**将配置分发至特定的设备/设备组或用户/用户组。
8. 在**选择其中一个“自定义分发”选项**下，选择所需的选项以指定将此配置分发至用户/用户组或设备/设备组。
9. 在**全部可用**下选择所需选项以分发此配置。
10. 单击**完成**。

10.10.8.32. 屏幕共享主机设置配置

屏幕共享主机设置配置使管理员能够使用 Ivanti Neurons for MDM 安全地控制跨受管设备的 macOS 屏幕共享功能。 此功能允许指定授权用户、身份验证方法和服务限制，以确保兼容和安全的远程访问。

适用范围：macOS 14.0 至 Ivanti Neurons for MDM 支持的最新发布版本。

开始之前：为了无缝集成**屏幕共享主机设置**配置，用户必须在其设备上启用"**远程管理**"。 在您的设备中，转到**设置** > **远程管理** > **启用远程管理**。

步骤

1. 转到**配置** > **+ 添加**。
2. 搜索并选择**屏幕共享主机设置**配置。
3. 根据下表配置**屏幕共享主机设置**的各项设置：

设置	描述
名称	输入用于识别此配置的名称。
描述	输入阐明此配置目的的说明。
端口基准	输入连接到主机的初始 UDP 端口号。 屏幕共享需要多个连接，因此系统会为每个额外的连接将此值递增 1。这不会改变系统最初用于与主机建立连接的端口号，该端口号始终是 TCP 端口 5900。 **最小端口基准值**：1024 **最大端口基准值**：65535
最大虚拟显示数	您最多可以使用两个虚拟显示器。
防止从主机复制文件	选中复选框以防止用户从屏幕共享主机复制文件。
防止将文件复制到主机	选中复选框以防止用户将文件复制到屏幕共享主机。
防止高性能连接	选中该复选框可防止用户与主机建立高性能连接。

4. 单击**下一步**，配置分配设置。
5. 选择其中一个分发选项来设置**屏幕共享主机设置**配置。 有关配置分发选项的详细信息，请参阅使用配置。
6. 单击**完成**。

10.10.8.33. 单应用模式配置

配置

许可证： Silver

单应用模式配置限制 iOS 设备只使用指定应用。 例如，您可能想将设备设置为仅可使用您的组织自定义的应用。

单应用模式配置

设置	流程
名称	输入用于识别此配置的名称。
说明	输入阐明此配置目的的说明。
选择应用	选择用于选择应用的方法： • **从应用程序目录和系统应用：**选择以搜索 Ivanti Neurons for MDM 应用程序目录和系统应用（默认预安装在 Apple 设备上）。 • 输入应用的名称，然后在它显示在应用列表内时选择它。 • **输入绑定 ID：**对于要选择的系统应用， 选择输入唯一标识符。 如果您无法使用 **从 App Catalog 和系统应用**选项找到系统应用，请使用此选项。
禁用触摸	选择此项可禁用触摸屏。
禁用设备旋转	选择此项可禁用设备旋转感应。
禁用音量按钮	选择此项可禁用设备音量按钮。
禁用铃声切换	选择此项可禁用设备铃声切换。
禁用睡眠唤醒按钮	选择此项可禁用设备睡眠/唤醒按钮（设备边框右上角）。
禁用自动锁定	选择此项可防止设备在闲置一段时间后进入睡眠状态。
启用旁白	选择此项可启用旁白屏幕阅读器（辅助功能）。
启用缩放	选择此项可启用缩放（辅助功能）。
启用反色	选择此项可启用反色调整（辅助功能）。
启用辅助触摸	选择此项可启用辅助触控（辅助功能）。
启用语音选择	选择此项可启用语音选择（辅助功能）。
启用单声道音频	选择此项可从立体声切换到单声道音频（辅助功能）。
旁白调整	选择此项可允许设备用户进行旁白调整。
缩放调整	选择此项可允许设备用户进行缩放调整。
反色调整	选择此项可允许设备用户进行反色调整。
辅助触摸调整	选择此项可允许设备用户进行辅助触控调整。

有关更多信息，请查看[如何创建配置](#)。

10.10.8.34. 软件更新推荐节奏配置

管理员可以选择允许用户查看设备，并将其更新为编号最高（最新）版本或编号较低（最旧）的版本，或同时执行。

适用于：iOS 和 iPadOS 14.5 至 26.0（受监督）

步骤

1. 转到配置 > + 添加。
2. 在搜索字段中，键入软件更新推荐，然后单击软件更新推荐节奏配置。
3. 输入配置的名称和描述。
4. 从下拉列表中，选择所需的配置设置：
    - 提供两个软件更新版本
    - 提供编号较低（最旧）的软件更新版本
    - 仅提供编号最高（最新）的软件更新版本
5. 单击下一步。
6. 选择启用此配置选项。
7. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义。
8. 单击完成。

10.10.8.35. 开始菜单和任务栏

可以为用户定义开始菜单布局，以定义可以安全使用的应用程序并删除不需要的应用程序。 Windows 10 和 11 版本支持不同的功能，因为开始菜单的布局不同。

要设置开始菜单和任务栏配置：

1. 转到**配置 > + 添加**。
2. 选择 **Windows 开始菜单和任务栏**配置。
3. 输入配置的名称。
4. 选择特定于 Windows 的版本。
5. **Windows 10 设备**：
   在**配置设置**部分，配置以下设置：
   设置
   流程
   名称
   输入用于识别此配置的名称。
   描述
   输入阐明此配置目的的说明。**选择标准设备**
   选择在开始菜单和任务栏中配置了应用程序的 Windows 10 设备。
6. 点击**从设备获取开始菜单布局**，并配置以下选项。
7. **设置**
   流程开始菜单和任务栏布局
   选择以下任何选项，以隐藏应用列表。
   - 无
   - 隐藏所有应用列表
   - 隐藏所有应用列表，并在设置应用中禁用“在开始菜单中显示应用列表”
   - 隐藏所有应用列表，移除所有应用按钮，并在设置应用中禁用“在开始菜单中显示应用列表”

开始菜单布局自定义开始菜单
点击**是**可自定义开始菜单和布局参数。**任务栏自定义任务栏**单击**是**，以自定义任务栏**在添加自定义任务栏快捷方式之前，删除现有的已固定任务栏快捷方式**点击**是**可在添加自定义任务栏快捷方式之前，删除现有的已固定任务栏快捷方式。**应用类型**指定应用类型。**应用**指定应用的 ID。
还原
点击**恢复**链接可从原来的 Golden 设备任务栏恢复任务栏。
点击并拖动行中的箭头图标来（向上或向下）移动特定行的位置。
单击删除图标，以删除行。
单击**添加新行**按钮，以添加新行。

8. **Windows 11 设备**
   在**配置设置**部分，配置以下设置：
   设置
   流程
   名称
   输入用于识别此配置的名称。
   描述

输入阐明此配置目的的说明。**选择标准设备**

选择在开始菜单的“已固定”部分配置了应用程序的 Windows 11 设备。**开始菜单和任务栏布局开始菜单和任务栏布局**

选择以下选项之一以查看任务栏中的搜索选项：

- **隐藏**
- **搜索图标**
- **搜索图标和标签**
- **搜索框（默认）**

选择复选框**隐藏任务视图**以隐藏任务视图。**最常用的应用程序**

选择以下选项之一来配置“开始”菜单中最常用的应用程序：

- **不强制在“开始”菜单中显示最常用的应用程序列表。**
- **强制在“开始”菜单中显示最常用的应用程序列表。**
- **强制隐藏“开始”菜单中最常用的应用程序列表。**

默认会选中复选框**允许固定到任务栏**。

选中复选框**隐藏推荐部分**隐藏所有推荐的部分。

由于供应商问题，即使用户注销或登录后，**隐藏推荐部分**复选框也不会对设备产生可见的作用。 目前，您无法隐藏“推荐”部分。**任务栏应用类型**

选择以下选项之一可指定应用程序类型：

- **应用程序用户模型 ID**
- **桌面应用程序链接路径**

应用指定应用程序的 ID 或路径**还原**

点击**恢复**链接可从原来的 Golden 设备任务栏恢复任务栏。

点击并拖动行中的箭头图标来（向上或向下）移动特定行的位置。

单击删除图标，以删除行。

单击**添加新行**按钮，以添加新行。

9. 点击**从设备中获取开始菜单布局**。
10. 从 Golden 设备获取设置后，所有在开始菜单中“已固定”部分中配置的应用程序都会显示出来，供管理员查看。

    点击**下一步**并将配置分发给所有适用的设备和用户组。

> 如果由于供应商的问题，配置未分发，已固定的应用程序将保留原来的配置。 然而，分发新的配置后，将覆盖以前的布局，并应用新的布局。

10.10.8.36. 系统更新配置

管理员可以限制设备用户管理 Android 6.0 设备或受支持更高版本上的系统更新。 此功能仅适用于 Android Enterprise 设备。

要配置：

1. 转到**配置 > + 添加**。
2. 选择**系统更新**配置。
3. 输入配置的名称。
4. 输入描述。
5. 在配置设置部分，配置以下选项：

设置	说明
自动	每当新固件可用时，静默应用系统更新。
延缓	将系统更新安装推迟 30 天。 在 30 天期限结束后，系统将提示设备用户安装更新。
Windowed（当地时间）	安排一段时间以静默应用系统更新。 选择**开始时间**和**结束时间**。
手动操作系统更新 (Android 10+) 不适用于或不支持 Samsung 和 Zebra 设备	选择此选项可在部分设备上手动执行操作系统更新，然后再将更新推送到所有设备。 **固件文件** - 选择**自定义属性**或 **HTTPS URL** 选项。 输入以下详细信息： • 固件位置 - 如果已将**自定义属性**选为固件文件选项，则需要提供用于文件传输的自定义属性。 固件文件可以是自托管，也可以使用文件传输配置上传到 Ivanti Neurons for MDM。 有关详细信息，请参阅**文件传输配置**。 将大于 50 MB 的文件上传到 Ivanti Neurons for MDM 需要附加许可证。 • 描述（选填） • 指纹（必填）- 验证设备上是否已安装预期的操作系统版本。 解压缩 OTA 文件夹并打开 /META-INF/com/android/metadata 文件，即可在 OTA 文件中找到指纹。 搜索与以下条目类似的条目： "post-build=google/xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxxxx:user/release-keys" 在上述条目中，**google/ xxxxx/xxxxxx:13/TQ3A.230805.001.S1/xxxxxx:user/release-keys** 即为指纹，TQ3A.230805.001.S1 是内部版本 ID（内部版本 ID 是指纹中从左往后数，由 / 分隔的第 4 个值）。 • 校验和（选填） **更新设置** → **操作系统更新请求** - 此部分的设置与 Zebra 固件配置相同。 请参阅此表中的 *Zebra 固件配置*部分。 如果选择 **HTTPS URL** 作为固件文件选项，则需要提供以下信息： • 固件位置 - 输入固件的下载路径，无需进行任何身份验证。 描述（选填） • 指纹（必填）- 验证设备上是否已安装预期的操作系统版本。 • 校验和（选填） 除了**操作系统更新请求**部分之外，还有**启动下载请求**和**下载期间条件**部分。 **启动下载请求**和**下载期间条件**部分提供的选项与 **Zebra 固件配置**部分提供的选项相同。 设备在下载后开始系统更新，若在更新期间重新启动设备，更新过程会中止。
冻结期	在一段指定的时间内冻结系统更新。 此选项适用于 Android 9.0 + 设备。 单击**添加冻结期**。 选择冻结期的**开始日期**和**结束日期**。 冻结期不得超过 90 天，您可以添加多个冻结期。 只有在上一个日历结束日期起 60 天后，才能选择下一个冻结期。 要删除冻结期，请单击删除图标。
Zebra 固件配置	选择**配置 Zebra OTA**，升级或更新 Zebra 设备的操作固件（在 Android 版本 8.0 或支持的较新版本上运行）。 这仅适用于设备所有者模式。 若要配置 Zebra OTA 更新，您必须在**管理员 > 固件管理 > Zebra OTA** 中启用 Ivanti Neurons for MDM OTA 服务，且 Zebra 设备必须位于 Ivanti Neurons for MDM 中。 您必须在弹出窗口中输入 Zebra 凭据。 要重新创建凭据，请直接联系 Zebra。

设置	说明
	在选择此选项时，将显示已注册 Zebra 设备的列表。 要选择并将固件应用于设备型号： 1. 在 Zebra 设备的**操作**列中，执行以下任何操作： ◦ **无**：对于该设备型号，将不执行任何操作。 ◦ **完整升级**。 在**选择目标 Zebra 固件**窗口中，选择要应用于设备型号的完整升级固件版本。 **完整升级**流程期间，只需要使用端口 443。 在**搜索**字段中，您可以键入版本号 ID 的字符，根据版本号 ID 搜索升级。 版本号 ID 会按降序排序和显示（顶部显示最新项）。 **修补程序升级**选项**不**适用于 Android 11+ 设备。 2. 配置下列任意选项： **启动下载请求** - Go app 将评估这些条件。 ◦ **电池电量最低要求**：移动滑块，在可用范围内设置电池电量最低要求。 ◦ **需要为设备充电**：选择此选项可在此过程中确保设备处于充电模式。 ◦ **下载时间表**：选择此选项可创建启动下载请求和文件下载的时间表。 ◦ **需要设备空闲**、**需要充电**和**允许通过按流量计费的网络下载**将传递至 Android 下载管理器。Go app 将在上述窗口，按以上参数，将下载请求添加到 Android 下载管理器。 **应用下载计划** - 选择**周几**、**开始时间**和**结束时间**，以计划下载。 系统支持选择多天，以计划下载。 例如，如果选择周六和周日，以及开始和结束时间介于中午 12:00 到晚上 11:00 之间，将仅在选定日的该时段内在 Zebra 设备上执行下载。 在 Go app 中，配置应用到设备后，下载将按计划开始。 没有下载结束时间限制，并且可能会在计划结束时间之后完成。 ◦ 选择**周几**、**开始时间**和**结束时间**，以计划安装固件更新。 如果设备电量低于 32，将推迟安装。 如果未配置更新计划，安装将立即在固件下载完成之后开始。 3. 配置下列任意选项： **下载期间的条件** - 下载管理器将评估这些条件。 您可以根据条件进行选择。 ◦ **需要设备闲置**（默认选中）：在设备闲置时，允许在设备上更新固件。 ◦ **需要充电**（默认选中）：在处于充电模式时，允许在设备上更新固件。 ◦ **允许通过按流量计费的网络下载**：选择此选项可允许使用 Wi-Fi 模式下载。 此选项默认取消选中。 ◦ **需要设备空闲**、**需要充电**和**允许通过按流量计费的网络下载**将传递至 Android 下载管理器。Go app 将在上述窗口，按以上参数，将下载请求添加到 Android 下载管理器。 **允许在指定的"下载时间表"之外继续下载**：选择此选项可允许在指定的下载时间表之外下载。 **操作系统更新请求** ◦ **电池电量最低要求**- 选择此选项可设置请求操作系统更新时必须达到的最低电池电量。 ◦ **需要为设备充电**：选择此选项可在此流程中确保设备处于充电模式。 ◦ **创建计划以在设备上启动操作系统更新** - 选择此选项可设置在设备上启动操作系统更新的计划。 在 Go app 中，配置应用到设备后，下载将按计划开始。 没有下载结束时间限制，并且可能会在计划结束时间之后完成。 单击**应用**。

设置	说明
Samsung e-FOTA 配置	选择**配置 Samsung e-FOTA**，以升级或更新 Samsung 设备的操作固件（Knox 版本 2.7.1 和更高版本）。 这仅适用于公司拥有设备上的工作配置文件的托管设备模式。 如果未注册支持 Samsung e-FOTA 的设备，页面将显示一则消息，即通知此信息。 要配置 Samsung e-FOTA 更新，必须在**管理员 > 固件管理 > Samsung E-FOTA** 中激活 Samsung e-FOTA 许可证。选择此选项后，将显示注册 Samsung 设备列表。 要选择并将固件应用于设备型号： 1. 在 Samsung 设备的**操作**列中，执行以下任何操作： ◦ **最新**：应用最新固件版本。 此选项默认选中。 ◦ **强制执行**：在选择目标 Samsung 固件窗口中，选择要强制应用于（无需用户介入）设备型号的特定固件版本。 在执行此操作时，将在 15 分钟内开始下载固件。 ◦ **目标**：在选择目标 Samsung 固件窗口中，选择应用于设备型号的特定固件版本。 在执行"强制执行"或"目标"操作时，如果未列出设备的固件，页面将显示一则消息，即通知此信息。 2. **启用调试固件**（可选）：在启用**启用调试固件**选项及应用配置时，设备会升级到虚拟固件。 通过 Samsung 设备固件的虚拟固件，管理员可以测试设备中的系统更新配置行为，无需实际修改设备上的任何内容。 要升级到实际固件更新（而非虚拟固件），管理员应在应用配置前确保禁用**启用调试固件**选项 3. 单击**应用**。

6. 单击**下一步**。
7. 选择下列分配选项之一：

- 所有设备
- 无设备（默认）
- 自定义

8. 单击**完成**。

Samsung E-FOTA 配置（已停用）

Samsung E-FOTA 配置已于 2022 年 7 月停用。 因此，新设备将无法使用此配置。 已具有该配置的设备仅可停用此配置。

10.10.8.37. Windows 10 更新管理

作为管理员，如果您想使用 Windows 10 更新管理更新 Windows 10 设备，可以查看和批准该设备报告的更新。 通过使用此功能，您可以防止在设备中安装不必要或未经测试的更新。

更新管理功能要求使用**软件更新**配置对设备进行配置，并启用**需要更新批准**选项。 只有将此配置应用于设备，设备才会报告安装更新并等待批准。

管理更新

1. 转到**管理员> Windows > Windows 更新**。 页面中将显示以下更新详细信息。
   创建日期：创建更新的日期。**标题**：描述更新类型以及知识库文章编号。

> 在单击更新时，将显示说明。

分类：将更新类型分为以下类别之一：

- 关键更新
- 定义更新
- 驱动程序更新
- 安全更新。
- 更新
- 升级
- 更新汇总

分配：为更新执行的分配。 例如，当更新分发到所有设备时，将显示**所有**。

> 如果将更新分配到特定数量的组，则会显示分配的计数。 例如，如果仅对 3 个组执行分配，则显示 3。

2. 此外，您还可以查看更新是否已分发到所需的设备。 以下列中包含的数字表示在不同类别的更新下存在的设备数量：
   - 符合条件的设备
   - 已安装的设备
   - 安装失败的设备
   - 等待重启的设备

点击任意数字后，您将被定向到“设备”页面上的筛选视图，您可在其中了解更新的状态并执行所需的操作。
通过单击更新的复选框，查看更新并选择要分配给设备的更新。

3. 在**操作**下点击**设置分发**。
4. 在**分配 Windows 更新**窗口中，选择以下任何分配选项：
   所有设备：将更新分配给所有设备。
   无设备：保留要分配给设备的更新**自定义**：为指定的设备组分配更新。
5. 单击**保存**。

搜索和过滤更新

您可以根据以下条件搜索和过滤更新：

- 知识库文章 ID
- 配置的分配

根据知识库文章 ID 进行过滤：

1. 在 **Windows 10 更新管理**页面的快速搜索字段中输入知识库 ID（只需在搜索字段中输入数字即可）。
   示例：对于 KB4056892，键入 4056892。 页面上显示与搜索条件匹配的更新。

> 您可以进一步查找有关更新的其他信息，方法是单击**支持**和**更多信息**链接。 指向 Microsoft 网页的**支持**链接为更新提供产品支持信息，指向 Microsoft 网页的**更多信息**显示与更新有关的更多信息，例如知识库文章。

根据配置的分配进行过滤：

在 **Windows 10 更新管理**页面中，根据配置的分发选择以下任意筛选选项：

- **所有**：显示所有更新。
- **已配置**：显示分配给设备的更新列表。
- **未配置**：显示未指定分配的更新列表。

> 已配置和未配置的筛选器基于执行的分发，分发也可以是**无**。

查看设备的更新

要查看特定于设备的详细更新信息：

1. 转至**设备 > 设备**。
2. 单击设备名称可查看详细信息页面。
3. 转至**更新**选项卡。 将显示待处理（由管理员批准更新但未报告为已安装在设备上）、失败和已安装的设备的更新。

> 您还可以在仪表板下的通知页面中看到有关新 Windows 更新的通知。 通知包括通知的创建日期、可用通知的数量以及通知的目的。 Windows 更新通知也在管理员门户的右上角可见。

10.10.8.38. Windows 应用计划

Windows 桌面应用可以是大型应用，并在企业的关键使用时间在网络和服务器上增加额外和扩展负载。 通过 Windows 应用计划功能，您可以计划时间，以在您选择的时间在设备上安装应用，尤其是大型应用。

要配置应用计划：

1. 转至**应用 > 应用目录**。
2. 点击**添加**并选择 Windows 应用程序，然后继续执行**添加应用程序**向导中的后续步骤。
3. 在第 5 步（配置）中，点击**安装应用程序配置设置**以查看**配置设置**页面。
4. 选中**计划安装**复选框。

> **计划安装**复选框仅在启用静默安装时显示。

5. 选择**开始时间**和**结束时间**，以计划安装应用的时间。
6. 选择**开始日期**和**结束日期**，以此计划安装应用程序的日期。

> 您还可以选择以下两项操作之一，以便在错过计划日期时执行：**下次签入时安装**或**不安装**。

7. 选择应用程序配置分发选项：**有应用程序的所有人**、**一律不**或**自定义**。
8. 单击**完成**。

> 需要计划的应用不应添加到 Apps@Work。
> 应用计划不适用于商店应用，因为商店应用不支持静默安装。

10.10.8.39. Windows BIOS 配置

管理员可在 Lenovo 设备上设置 Windows BIOS 设置。 只有注册至少一款支持 BIOS 设置的 Lenovo 设备，才可以设置此配置。

要配置：

1. 转到**配置 > + 添加**。
2. 选择 **Windows BIOS** 配置。
3. 输入配置的名称。
4. 输入描述。
5. 在"选择设备型号"部分中，从下拉列表选择设备型号。
6. 在配置设置部分，配置以下选项：

> 设置列表因注册的特定设备型号的可用内容而异。 有关更多信息，请参阅相应设备的网站。

设置	采取何种 措施
AMT 控制	选择以下任一选项： • **禁用** • **启用**
适应性热管理 AC	选择以下任一选项： • **平衡** • **最大化性能**
适应性热管理电池	选择以下任一选项： • **平衡** • **最大化性能**
始终开启 USB	选择以下任一选项： • **禁用** • **启用**
BIOSPasswordAtBootDeviceList	选择以下任一选项： • **禁用** • **启用**
重新启动时的 BIOS 密码	选择以下任一选项： • **禁用** • **启用**
无人值守启动时的 BIOS 密码	选择以下任一选项： • **禁用** • **启用**
由最终用户执行的 BIOS 更新	选择以下任一选项： • **禁用** • **启用**
Bluetooth 访问权限	选择以下任一选项： • **禁用** • **启用**
启动设备列表 F12 选项	选择以下任一选项： • **禁用** • **启用**

设置	采取何种 措施
启动显示设备	选择以下任一选项： • **DisplayPort** • **扩展坞显示** • **HDMI** • **LCD**
BootMode	选择以下任一选项： • **诊断** • **快速**
启动顺序锁定	选择以下任一选项： • **禁用** • **启用**
BootTimeExtension	选择以下任一选项： • **1** • **10** • **2** • **3** • **5** • **禁用**
已检测到 BottomCover 篡改	选择以下任一选项： • **禁用** • **启用**
CPU 电源管理	选择以下任一选项： • **自动** • **禁用**
计算机被盗追踪服务程序模块激活	选择以下任一选项： • **禁用** • **启用**
数据执行保护	选择以下任一选项： • **禁用** • **启用**
以太网 LAN 访问	选择以下任一选项： • **禁用** • **启用**
以太网 LAN 选项 ROM	选择以下任一选项： • **禁用**

设置	采取何种 措施
	• **启用**
指纹密码身份验证	选择以下任一选项： • **禁用** • **启用**
指纹前桌面身份验证	选择以下任一选项： • **禁用** • **启用**
指纹识别器访问	选择以下任一选项： • **禁用** • **启用**
指纹识别器优先级	选择以下任一选项： • **外部** • **仅限内部**
指纹安全模型	选择以下任一选项： • **高** • **正常**
Fn Ctrl 按键交换	选择以下任一选项： • **禁用** • **启用**
FnKeyAsPrimary	选择以下任一选项： • **禁用** • **启用**
FnSticky	选择以下任一选项： • **禁用** • **启用**
IPv4 网络堆栈	选择以下任一选项： • **禁用** • **启用**
IPv6 网络堆栈	选择以下任一选项： • **禁用** • **启用**
集成相机访问	选择以下任一选项： • **禁用** • **启用**

设置	采取何种 措施
InternalStorageTamper	选择以下任一选项： • **禁用** • **启用**
键盘提示音	选择以下任一选项： • **禁用** • **启用**
锁定 BIOS 设置	选择以下任一选项： • **禁用** • **启用**
存储卡插槽访问	选择以下任一选项： • **禁用** • **启用**
麦克风访问	选择以下任一选项： • **禁用** • **启用**
最低密码长度	选择以下任一选项： • 4 • 5 • 6 • 7 • 8 • 9 • 10 • 11 • 12 • **禁用**
NFFControl	选择以下任一选项： • **禁用** • **启用**
NFC 访问	选择以下任一选项： • **禁用** • **启用**
通过接入 AC 启动	选择以下任一选项： • **禁用** • **启用**

设置	采取何种 措施
PasswordBeep	选择以下任一选项： • **禁用** • **启用**
PasswordCountExceededError	选择以下任一选项： • **禁用** • **启用**
适用于 TPM 清除的实体存在	选择以下任一选项： • **禁用** • **启用**
适用于 TPM 配置的实体存在	选择以下任一选项： • **禁用** • **启用**
快速启动技术	选择以下任一选项： • **禁用** • **启用**
SecureBoot	选择**启用**
安全回滚预防	选择以下任一选项： • **禁用** • **启用**
安全芯片	选择以下任一选项： • **激活** • **禁用** • **启用** • **停用**
智能卡插槽访问	选择以下任一选项： • **禁用** • **启用**
SpeedStep	选择以下任一选项： • **禁用** • **启用**
启动选项键	选择以下任一选项： • **禁用** • **启用**
TXT 功能	选择以下任一选项：

设置	采取何种 措施
	• **禁用** • **启用**
总图形内存	选择以下任一选项： • **256 MB** • **512 MB**
触摸板	选择以下任一选项： • **自动** • **禁用**
TrackPoint	选择以下任一选项： • **自动** • **禁用**
USB30 模式	选择以下任一选项： • **自动** • **禁用** • **启用**
CPU BIOS 支持	选择以下任一选项： • **禁用** • **启用**
USB 端口访问	选择以下任一选项： • **禁用** • **启用**
UEFI Pxe 启动优先级	选择以下任一选项： • **优先 IPv4** • **优先 IPv6**
Vtd 功能	选择以下任一选项： • **禁用** • **启用**
虚拟化技术	选择以下任一选项： • **禁用** • **启用**

设置	采取何种 措施
局域网唤醒	选择以下任一选项： • **仅限 AC** • **AC 和电池** • **禁用** • **启用**
无线 LAN 访问	选择以下任一选项： • **禁用** • **启用**
无线 WAN 访问	选择以下任一选项： • **禁用** • **启用**

7. 单击**下一步**。
8. 选择下列分配选项之一：
   - 所有设备
   - 无设备（默认）
   - 自定义
9. 单击**完成**。

10.10.8.40. Windows BitLocker

作为管理员，通过使用设备 GUID 和恢复密码上传 Excel 文件，您可以为一组加密的 Windows 10 设备批量更新恢复密钥。

上传 Excel 文件批量更新恢复密钥：

1. 转到**管理员 > Windows BitLocker**。
2. 单击**下载示例 csv 文件**，以下载并查看 .csv 文件的示例。
3. 创建并添加 BitLocker 恢复密钥 .csv 文件的记录。
4. 单击**上传恢复密码**
5. 单击**选择文件**，以上传您创建的 .csv 文件。
6. 单击**上传**。 使用此前上传的密钥上传新文件将覆盖旧条目。

> 每次上传最多提交 1000 个记录。 在成功上传后，您可以在特定设备的设备详细信息中查看个人密钥。

10.10.8.41. Windows 自助服务终端配置

使用 Windows 自助服务终端配置，您可以在 Windows 10 设备上配置单个或多个应用程序自助服务终端。 通过应用该配置，自助服务终端用户被限制访问自助服务终端应用程序之外的任何功能。 此配置要求启用 Windows 网桥。

以下是可应用配置的三种模式。

- 单个应用程序
- 多个应用程序（从 Windows 设备获取应用程序列表）
- 多个应用程序（从开始菜单配置中选择现有布局）

> 在进入配置的 Windows 自助服务终端模式前，设备已包含用于 Windows 自助服务终端配置的应用。

要配置 Windows 自助服务终端配置：

1. 转到**配置 > + 添加**。
2. 选择 **Windows 自助服务终端**配置。
3. 输入配置的名称。
4. 输入描述。
5. 在“配置设置”部分中，按照下表描述指定剩余设置。

设置	采取何种措施
选择自助服务终端模式：选择以下 3 个选项中的任意一个。	
单个应用程序	选择此选项可为设备配置单个应用程序自助服务终端模式。 1. 在**选择 Windows 设备（可选）**部分，选择 Windows 10 设备。 单击**从设备获取应用程序**以从设备获取应用程序列表。您选择的设备应该在您的监督下，并且需要签入才能成功获取应用程序数据。要跳过这些步骤，请选择**跳过此步骤。 如果需要，您可以稍后改变主意**复选框。 2. 单击**从提取的应用程序列表添加**，从提取的列表添加应用程序。 3. 单击应用程序**名称**列中的单选按钮，选择单个应用程序。 单击**添加新项**，将新应用程序添加到列表中。 要从列表中删除应用程序，请单击删除图标。
多个应用程序（从 Windows 设备获取应用程序列表）	选择此选项可为设备配置多个应用程序自助服务终端模式。 1. 在**选择 Windows 设备（可选）**部分，选择 Windows 10 设备。 单击**从设备获取应用程序**，从设备获取应用程序列表。 您选择的设备应该在您的监督下，并且需要签入才能成功获取应用程序数据。要跳过这些步骤，请选择**跳过此步骤。 如果需要，您可以稍后改变主意**复选框。 2. 在**自助服务终端应用程序和开始菜单布局**中，单击**从提取的应用程序列表添加**。 将显示**选择自助服务终端应用程序**窗口。 从提取的列表中选择应用程序，然后单击**使用选定的应用程序**。 3. 在“允许其他应用”部分，点击**从提取的应用列表中添加**。 将显示**选择自助服务终端应用程序**窗口。从提取的列表中选择应用程序，然后单击**使用选定的应用程序**。 其他允许的应用被视为 **Kiosk 应用和开始菜单布局**中所选应用的依赖应用。如果没有“允许的应用”，即使应用图标显示在“开始菜单”中，操作系统也不允许运行此应用。 4. 单击**添加新项**，将新应用程序添加到列表中。要从列表中删除应用程序，请单击删除图标。 您可以将列表中的应用程序拖放到列表中的任何位置。 5. 在**多应用程序其他设置**中，选择所需选项： ◦ **隐藏电源按钮** ◦ **隐藏用户平铺** ◦ **隐藏任务栏** 在 Microsoft Windows 11 中，不支持多应用程序 Kiosk 模式选项**隐藏任务栏**。
多个应用程序（从开始菜单配置中选择现有布局）	如果已创建“开始”菜单布局配置，您可以导入该配置，并通过选择该选项将其用于配置多应用模式。 1. 在**选择布局**部分中，选择以前设置为“开始菜单配置”的布局。 具有适用布局参数的先前创建的配置显示在下面的下拉列表中。 2. 在“多应用程序其他设置”中，选择所需选项： ◦ **隐藏电源按钮** ◦ **隐藏用户平铺** ◦ **隐藏任务栏** 在 Microsoft Windows 11 中，不支持多应用程序 Kiosk 模式选项**隐藏任务栏**。

6. 单击**下一步**。
7. 选择下列分配选项之一：

- 所有设备

- 无设备（默认）
- 自定义

8. 单击**完成**。

> 要使配置完全生效，应在应用或更新 Windows 自助服务终端配置后重新启动设备。是否需要第二次重新启动设备，这取决于多应用自助服务终端配置的应用。 第一次登录时可能会丢失一些图标，但在第二次重新启动后，登录时会显示丢失的图标。

应用、删除或更新自助服务终端配置后，必须重新启动设备。 这可以通过设备操作菜单中的重启/关机设备命令来完成。 如果不重启：

- 应用自助服务终端配置后，设备不会自动进入自助服务终端模式。
- 删除应用的自助服务终端配置后，设备不会自动退出自助服务终端模式。
- 设备不会更改正在运行的自助服务终端配置。

如果具有应用的自助服务终端配置的设备接收到更新的配置，该设备上的 Windows 操作系统将删除现有自助服务终端用户，并使用新的自助服务终端配置重新创建新的自助服务终端用户。 当前用户的会话应该随着设备的重新启动而明确结束。

对于多应用自助服务终端配置，最好配置“.lnk”文件，对于单应用自助服务终端配置，最好配置“.exe”文件。 从设备导入的开始菜单配置使用“.lnk”格式。 为“.exe”应用程序手动创建的开始菜单项有时不能显示在根据“.exe”应用程序配置的多应用程序自助服务终端的开始菜单中。

例如，Windows Media Player 可以使用以下“.lnk”文件之一添加到“开始菜单”：

- %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows Media Player.lnk
- %ALLUSERSPROFILE%\Microsoft\\Windows\Start Menu\Programs\Windows Media Player.lnk

如果此应用程序使用以下任一“.exe”文件直接添加，则不会显示相应的图标，即使第一个“.exe”路径在上述“.lnk”文件中内部使用也是如此：

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
- C:\Program Files\Windows Media Player\wmplayer.exe

对于单应用程序自助服务终端配置，您可以向 exe 文件添加参数。 E.g. '%ProgramFiles%\Internet Explorer\iexplore.exe -k www.bing.com'. 但是，在多应用程序配置的情况下，带有参数的 exe 应用程序的图标不会显示在“开始菜单”中。如果在多应用程序自助服务终端配置中需要带有参数的 exe 应用程序，请使用内部带有参数的“.lnk”文件。 “.lnk”在单应用程序自助服务终端配置的情况下不起作用。

多应用程序自助服务终端模式中的依赖关系

在多应用程序自助服务终端模式下，Win32/64 应用程序可能需要添加到“其他允许的应用程序”部分的依赖项。 单应用程序自助服务终端模式不需要“其他允许的应用程序”。

示例 1：对于 Windows Media Player 应用程序，在多应用程序自助服务终端模式下需要以下依赖项：

- C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- %ProgramFiles(x86)%\Windows Media Player\setup_wm.exe

第一个依赖项是从相应的“.lnk”文件调用的应用程序二进制文件。 第二个依赖项是从第一个依赖项调用的一次性向导。

如果没有“允许的应用程序”，即使应用程序图标显示在“开始菜单”中，操作系统也不允许运行此应用程序。

示例 2：对于 Internet Explorer，如果它配置了以下列表中的任何项目，它的图标将显示在“开始菜单”中：

- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Accessories\Internet Explorer.lnk
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Internet Explorer.lnk

- C:\Program Files\internet explorer\iexplore.exe
- %ProgramFiles%\Internet Explorer\iexplore.exe

Internet Explorer 需要以下依赖项：

- C:\Program Files (x86)\Internet Explorer\iexplore.exe
- C:\Program Files (x86)\Internet Explorer\ExtExport.exe
- C:\Program Files (x86)\Internet Explorer\ieinstal.exe
- C:\Program Files (x86)\Internet Explorer\ielowutil.exe

第一个依赖项是仅“.lnk”项需要的应用程序二进制文件，另一个依赖项是一次性向导。 如果没有第一个依赖项，操作系统会阻止具有弹出窗口的应用程序。 如果没有其他依赖项，应用程序会在启动后立即关闭，没有任何来自操作系统的额外通知。

10.10.8.42. Windows 许可证配置

Windows 许可证配置会升级设备上的操作系统，例如将 Windows 10 Pro 升级到 Windows 10 Enterprise。 此外，此配置可激活或更改 Windows 10 桌面设备的产品密钥。

要升级 Windows 许可证：

1. 转到**配置 > + 添加**。
2. 选择 **Windows 许可证**配置。
3. 输入配置的名称。
4. 在**配置设置**部分中，键入 Windows **产品密钥**。
5. 单击**下一步**。
6. 选择下列分配选项之一：
    - 所有设备
    - 无设备（默认）
    - 自定义
7. 单击**完成**。

11. 策略

策略可以定义设备要求，以及设备不符合要求时将产生的后果。 每种策略都由规则和合规性操作（违反规则将产生的后果）组成。 使用**策略**页面可对策略进行选择、设置和分配。

> 使用自动设备登记流程，请注意以下更改：

- 仅对过去 90 天内登记的设备进行评估。
- 在 90 天后和一年前登记的设备上，只会触发强制登记命令。
- 对过去一年内未登记的设备不采取任何行动。

本部分包含以下主题：

- 使用策略
- 自定义策略
- 监控和控制允许的应用程序
- 确定策略的优先级
- Windows 硬件策略

11.1. 使用策略

本部分包含以下主题：

- 实施策略
- 合规性操作
- 查找现有策略
- 添加策略
- 编辑策略
- 删除策略

实施策略

策略可以定义设备要求，以及设备不符合要求时将产生的后果。 每种策略都由规则和合规性操作（违反规则将产生的后果）组成。 使用**策略**页面可对策略进行选择、设置和分配。

以下策略类型可用：

类型	功能
存在安全危险的设备	优先级（1 = 最高） 违反 1 插件受损 2 客户端被篡改 3 未知的设备制造商：未知 4 检测到可疑文件夹：[path] 5 可疑二进制文件位于：[path] 6 文件夹/数据可浏览或文件夹/数据/数据可浏览 7 Found /system/app/Superuser.apk 8 软件包管理器受损 9 发现可疑应用程序：[package] 标记越狱设备 (iOS) 或刷机设备 (Android)。 要查看系统将 Android 设备标记为由于生根而受损的违规原因： 1. 单击**策略**选项卡。 2. 单击**受损设备**链接。 3. 单击**活动违规**选项卡。 4. 检查违规列中的违规原因。 要查看系统将 Android 设备标记为由于生根而受损的违规原因： 5. 单击**策略**选项卡。 6. 单击**受损设备**链接。 7. 单击**活动违规**选项卡。 8. 检查**违规**列中的违规原因。 这将是以下原因之一：
已禁用设备保护/加密（仅限 macOS）	标记未启用通行码或加密的 macOS 设备。
国际漫游	标记可能出现国际漫游费的设备。 设备签入时，状态将刷新。 对于 iOS，服务使用 iOS 设置并报告的漫游标记。 仅第一次违规会触发合规性操作。
MDM/设备管理已禁用	如果设备处于 MDM 已禁用状态，将不会在签入期间对任何其他策略或者配置或应用的增量处理进行评估。
超出合同期限	标记在指定时间范围内与 Ivanti Neurons for MDM 失联的设备。 选择设备在指定小时范围（2-3 至 23-24）或天数内未签入时要执行的操作。
MI 客户端失联（仅限 iOS）	标记在指定时间范围内与 Ivanti Neurons for MDM 失联的 Ivanti Neurons for MDM 客户。 选择客户端在指定小时范围（2-3 至 23-24）或天数内未签入时要执行的操作。 这也适用于通过 iReg 注册的设备。 如果没有客户端，或如果客户端未在规定的时段内签入，策略会将设备标记为不合规。
允许的应用	标记违反关于允许或要求哪些应用规则的设备。
自定义策略	根据您指定的条件和相关操作，创建自定义策略。

合规性操作

可以使用以下合规性操作：

合规性操作	功能
监控	标记 Ivanti Neurons for MDM“设备”页面中的设备。 此操作默认打开。
阻止 将消息发送给用户	如果上次签入详细信息显示某个设备违反了策略，那么之后尝试通过 Sentry 或 Access 访问资源时，此合规性操作将指示 Access 和/或 Sentry 阻止该设备。 • 标记 Ivanti Neurons for MDM“设备”页面中的设备。 • 向设备所有者发送电子邮件。 • 除了现有策略外，**使用合规性策略电子邮件模板**切换功能现在也适用于以下策略： ◦ 数据保护/加密已禁用 ◦ 国际漫游 ◦ MDM/设备管理已禁用 ◦ 超出合同期限 ◦ MI 客户端失联 向设备发送推送通知。
隔离	• 移除设备中的大部分配置。 ◦ 排除：通行码配置、对仅具有 Wi-Fi 功能的设备进行的 Wi-Fi 配置、限制配置 (iOS)。 • 移除所有由 Ivanti Neurons for MDM 安装的应用。 • 移除由 Ivanti Neurons for MDM 分发的所有内容，包括 iBook 和 ePub 文件。 • 阻止对 Ivanti Neurons for MDM 目录的访问。 • 安装其他应用时的推迟提示。 • 阻止访问 AppConnect 已启用的应用。 • 包括支持启用 AppConnect 的应用。 • 如果打开，在隔离设备的个人端暂停个人应用，以表示设备用户需要解决设备的合规性问题，才可以正常使用。 支持配置为公司拥有设备上的工作配置文件的 Android 11+ 设备。
附加隔离操作（可选）：	**阻止新应用下载** - 阻止将任何新应用程序下载到设备。 **托管应用程序** - 从设备中移除 Ivanti Neurons for MDM 管理的应用，并启用“阻止新应用下载”选项，以阻止应用重新在设备上安装。 选择下列选项之一： • **所有应用程序** • **删除以下之外的所有应用程序** - 删除所有应用程序但已添加到应用程序列表中的应用程序除外。 • **委派应用** - 通过查找或手动（使用捆绑 ID 或软件包名称），添加一个或多个应用。 单击**查看应用**选项卡，以查看已添加应用的列表。 阻止 App Store 访问默认隔离操作不再可用。 在特定设备上，由于特定设备限制，因此隔离操作不会将应用从设备中移除。 默认情况下，此选项为选中状态（适用于所有三种情况：所有应用程序、删除以下之外的所有应用程序和指定应用程序）且无法取消选择。 这会阻止应用重新安装到设备。 **移除配置** - 移除设备中的 Ivanti Neurons for MDM 配置。 选择下列选项之一： • **所有配置**

合规性操作	功能
	• **委派配置** - 从列表中选择一个或多个配置，或者进行搜索。 单击**选定配置**选项卡，以查看选定配置的列表。 **推送指定配置** - 作为自定义合规的一部分，分发指定配置。 此列表包含满足以下条件的配置： • 已启用配置 • 非系统配置 • 隔离配置 • 在当前空间中创建或从默认空间委派的配置 有关不可隔离配置的列表，请参阅不可隔离配置。 **移除内容** - 从设备中移除与 Ivanti Neurons for MDM 分发的应用相关联的所有内容和媒体。 **暂停个人应用程序** - 在隔离设备的个人端暂停应用，以表示设备用户需要解决设备的合规性问题，才可以正常使用它。 支持配置为公司拥有设备上的工作配置文件的 Android 11+ 设备。

查找现有策略

您可以使用"策略"页面中的筛选器和搜索功能，以查找一个或多个现有策略。

程序

1. 转到**策略**。
2. 要筛选匹配特定条件的策略列表，单击**筛选器**。
3. 选择一个或多个筛选条件。
4. 要按名称搜索现有策略，请在**搜索**字段中输入策略名称。

添加策略

程序

1. 转到**策略**。
2. 单击 + **添加**（右上角）。
3. 选择一个策略类型。
4. 完成设置。
5. 选择要接收此策略的设备组。

> 您一次可以分发最多 100 个配置文件。

6. 单击**完成**。

编辑策略

程序

1. 转到**策略**。
2. 对于所需策略，单击操作列中的**编辑**（铅笔）图标。
3. 做出更改。

4. 保存更改。

删除策略

程序

1. 转到**策略**。
2. 对于所需策略，单击操作列中的**移除**图标。
3. 单击**是**进行确认。

如果您未看到策略页面，这可能是您没有所需权限。 您需要以下角色之一：

- 设备管理
- 设备只读

有关更多信息，请查看确定策略的优先级。

11.2. 自定义策略

策略

许可证：Platinum

符合条件的设备：Android、iOS、macOS、Windows。

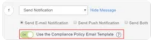
允许您根据您指定的设备和用户属性、部分条件、值和合规性操作来创建自定义策略。

> 在定义自定义策略时，甚至可以使用 Android 安全修补程序级别设置。

添加自定义策略

1. 转到**策略**。
2. 单击 **+添加**
3. 选择**自定义策略**。
4. 为自定义策略提供名称。
5. 如果需要，单击**+ 添加描述**，输入其他详细信息。
6. 使用规则生成器，以定义在条件评估为真时触发操作的条件。 请参阅**了解条件设置**，以了解创建条件的指南。 在规则生成器中选择“用户组名称”属性后，Ivanti Neurons for MDM 管理员控制台会显示重复用户组的数量和相应的 GUID 数量，以便识别重复组。 此外，此规则下方的表会显示重复用户组的列表及其详细信息，例如用户组名称、GUID、来源和可分辨名称 (DN)。
7. 选择在满足指定条件时要采取的其中一个合规性操作（见以下默认操作）。 在其他操作之间添加操作“**等待**”，可提供一种方法，允许设备用户在采取其他操作之前修复设备并使其恢复合规。 例如，您可能需要发送警告消息，并在应用隔离操作之前等待 24 小时。
8. 选择**在设备重新处于合规状态时发送通知**选项（默认关闭）。

- **发送电子邮件通知** - 设备恢复合规时，向设备用户的电子邮件地址发送电子邮件来通知用户。
  - 打开**使用合规策略电子邮件模板**选项，以将您在此处配置的消息插入您按**品牌化电子邮件模板**中的**自定义电子邮件模板**所述配合的策略通知电子邮件模板。 有关概览，请查看**配置和使用策略合规通知电子邮件**。

    
  - 通过包含可选替代变量，您可以自定义消息，以向收件人提供有关策略违反的更多详细信息和其他相关信息。 单击以下属性类型，以显示完整的变量列表：
    - 策略属性包括 $、$ 和 $。
    - 用户属性包括 $、$ 和 $。
    - 设备属性包括 $、$ 和 $。
    - 从**管理>属性**页面创建的自定义设备/用户/LDAP 属性。
- **发送推送通知** - 在设备重新处于合规状态时，向设备发送推送通知。
- **发送推送通知和电子邮件通知** - 同时向设备发送推送通知，向设备用户的电子邮件地址发送电子邮件，并在设备重新处于合规状态时通知。 您可以通过包含可选的替代变量来自定义邮件，以便为收件人提供更多详细信息，如前面发送电子邮件操作所述。

9. 从表中指定以下选项，以便在设备所有者违反策略规则时通知管理员和注册的设备所有者：

选项	描述
主题	输入主题文字。 例如，“您违反了策略！”
正文	根据需要输入消息。 例如，“需要采取行动！”
仅向管理员发送电子邮件通知	选择此选项以仅向管理员发送电子邮件通知。
抄送给管理员	如果您选择了“仅向管理员发送电子邮件通知”选项，则此文本框将不可用。
输入管理员的电子邮件地址	输入管理员的电子邮件 ID。 请用分号 (;) 作为分隔符来添加多个电子邮件地址。
预览电子邮件	点击**预览电子邮件**按钮查看电子邮件地址。

10. 点击**下一步**保存策略详细信息。

默认操作：

1. 单击**是**复选框，确认您了解，如果以前在设备上触发此策略，则添加分层策略将重置以前应用的策略和任何合规性操作。 新的自定义策略将在下一次设备签入时生效。 如果您选择了“停用”操作，请单击**是**，确认您了解无法取消该操作。

- **监控** - 目前，始终选中。 需要 Sentry 版本 9.0.0 或更高版本才能使用分层合规性操作。
- **不进行任何操作**
- **发送通知**
- **发送电子邮件** - 向设备用户的电子邮件地址发送电子邮件，通知用户设备不合规。
  - 如上所述，您可以使用策略通知电子邮件模板。
  - 您可以通过包含可选替换变量来自定义邮件，以便为收件人提供有关违反策略的更多详细信息和其他相关信息。 这为不合规设备的用户提供有关违反策略的相关信息，以便他们采取补救措施。 单击以下属性类型，以显示完整的变量列表：
    - 策略属性包括 $、$ 和 $。
    - 用户属性包括 $、$ 和 $。
    - 设备属性包括 $、$ 和 $。
    - 从**管理>属性**页面创建的自定义设备/用户/LDAP 属性。
- **发送推送通知** - 向设备发送推送通知，告知设备不合规。
- **发送推送通知和电子邮件通知** - 同时向设备发送推送通知，并向设备用户的电子邮件地址发送电子邮件，通知其设备不合规。 您可以通过包含可选的替代变量来自定义邮件，以便为收件人提供更多详细信息，如前面发送电子邮件操作所述。
- **阻止** - 使用 Sentry 阻止托管设备访问电子邮件和启用 AppConnect 的应用。 需要 Sentry 版本 9.0.0 或更高版本，才能使用阻止操作。
- **停用** - 停用设备。 **此操作无法撤消**。 例如，可以通过使用“用户已启用”条件为所有禁用用户退出设备。
- **等待** - 延迟指定时间段（小时数或天数）的操作，以允许用户在设备保持不合规的情况下，执行额外操作之前修复违规。
- **隔离** - 根据以下操作删除对应用、内容和服务器的访问权限：

（可选）附加隔离操作	描述
隔离受管应用	从设备中移除 Ivanti Neurons for MDM 管理的应用，并启用“阻止新应用下载”选项，以阻止应用重新在设备上安装。 选择下列选项之一： • **所有应用程序** • **委派应用** - 通过查找或手动（使用捆绑 ID 或软件包名称），添加一个或多个应用。 单击**查看应用**选项卡，以查看已添加应用的列表。 阻止 App Store 访问默认隔离操作不再可用。 在特定设备上，由于特定设备限制，因此隔离操作不会将应用从设备中移除。
阻止新的应用程序下载	阻止将任何新应用程序下载到设备。 选择下列选项之一： • **所有应用程序** • **委派应用** - 通过查找或手动（使用捆绑 ID 或软件包名称），添加一个或多个应用。 单击**查看应用**选项卡，以查看已添加应用的列表。 阻止 App Store 访问默认隔离操作不再可用。 默认情况下，选择此选项（适用于所有应用和指定应用），且无法取消选择。 这会阻止应用重新安装到设备。
删除配置	移除设备中的 Ivanti Neurons for MDM 配置。 选择下列选项之一： • **所有配置** • **委派配置** - 从列表中选择一个或多个配置，或者进行搜索。 单击**选定配置**选项卡，以查看选定配置的列表。
推送指定配置	作为自定义合规的一部分，分发指定配置。 此列表包含满足以下条件的配置： • 已启用配置 • 非系统配置 • 隔离配置 • 在当前空间中创建或从默认空间委派的配置 有关不可隔离配置的列表，请参阅不可隔离配置。 有关详细信息，请参阅此过程后的推送指定配置 部分。
删除内容	从设备中移除与 Ivanti Neurons for MDM 分发的应用相关联的所有内容和媒体。
暂停个人应用	在隔离设备的个人端暂停应用，以表示设备用户需要解决设备的合规性问题，才可以正常使用。 支持配置为公司拥有设备上的工作配置文件的 Android 11+ 设备。
默认隔离操作 - 始终执行这些操作。	
阻止 App Store 访问	阻止设备通过 Ivanti Neurons for MDM 访问应用商店。
阻止 Content Store 访问	阻止设备通过 Ivanti Neurons for MDM 访问内容商店。
阻止 AppConnect	阻止设备使用 AppConnect 功能。

（可选）附加隔离操作	描述
阻止 AppTunnel	阻止设备上的应用程序通过 AppTunnel 访问内容和服务器。
阻止 ActiveSync	阻止设备通过 ActiveSync 服务器访问电子邮件。

2. 单击**下一步**，配置将应用策略和操作的设备。
3. 单击**完成**。

下表说明当 Ivanti Neurons for MDM 是隔离操作的发起者时在多个 Android 设备上执行的隔离行为：

设备中的指示，确定将哪些隐私配置应用到希望的设备上	隔离行为
在设备管理员模式中的 Samsung 设备通过 Go 客户端应用	• 卸载受管公共和内部应用 • 移除特定配置文件（排除移动威胁防御和其他）
在设备管理员模式中的 Samsung 设备通过 Go 客户端应用 MAM 通过 AppStation 应用	• 不支持卸载或隐藏受管公共和内部应用 • 移除特定配置文件（排除移动威胁防御和其他）
通过 Go 客户端应用程序管理 Android Enterprise	• 隐藏受管公共和内部应用 • 移除特定配置文件（排除移动威胁防御和其他）

推送指定配置

作为自定义合规的一部分，分发指定配置。 配置自定义策略，以在设备不合规时分发一组配置。 在设备状态从不合规更改为合规状态时，作为补救措施的一部分，将设备重置为此前的状态。

> 管理员尝试在“推送指定配置”选项卡中委派非委派配置的自定义策略时出错。

以下是在特定条件下通过自定义策略推送配置的行为：

条件	行为
选择 2 个已设置优先级且类型相同的配置	具有较高优先级的配置将推送到设备。
选择 2 个未设置优先级且类型相同的配置	2 个配置将推送到设备。 可能产生意外行为。
在设备具有类型相同的配置且支持在自定义策略中定义的优先级时 在设备具有类型相同的配置且不支持在自定义策略中定义的优先级时	对于在自定义策略中定义的配置，将具有优先级并推送到设备。 设备中的现有配置将移除，不论优先级如何（即使优先级高于在自定义策略中定义的配置）。 对于在自定义策略中定义的配置，将推送到设备。 设备将显示 2 个配置。 可能产生意外行为。
如果在创建自定义策略后更改配置的优先级	在设备签入时，如果是自定义策略的一部分，将推送具有最高优先级的配置。
在满足 2 个条件时： • 条件 A：当违规设备中的配置作为自定义策略的一部分推送时（其优先级高于设备上类型相同的配置）。 • 条件 B：违规已更正，设备不再处于隔离状态	在自定义策略中定义的配置将移除；设备上其中一个类型相同的配置将在隔离前通过现有设备组的应用进行推送，并将设备还原为原始状态。

在隔离操作中，如果您选择移除配置，以及推送指定配置，请留意以下规则：

- 移除所有配置 + 推送指定配置：在此情况下，移除设备中的所有配置，并将在“推送指定配置”中选择的配置推送到设备。
- 如果两个自定义策略中选择了相同的配置，则删除指定配置（在一个自定义策略中）+ 推送指定配置（在另一个自定义策略中）：由于在两个不同的合规策略中选择了相同的配置，因此将采用最严格的方法，即 从设备中删除这些配置。

您可以将自定义策略从默认空间委派到自定义空间。 对于要委派的自定义策略，在“推送指定配置”选项卡的自定义策略中提及的配置需要委派到空间。

在设备页面中，您可以单击设备的名称，以访问设备详细信息页面。 在“配置”选项卡中，分发方法列表示，推送到设备的配置的分发方法。 分发方法是“设备组”或“合规操作”。

在配置页面中，对于每个配置，Ivanti Neurons for MDM 会显示通过设备组和合规操作收到配置的设备计数。

了解条件设置

下表描述一些可用于构建规则的字段：

UI 字段	描述	可能的值	支持的平台
支持 APNS	此字段表示设备是否可以使用 APNS。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。	iOS/macOS/Android
防网络钓鱼本机状态	此字段显示防网络钓鱼本机状态	可能的运算符： • 等于 • 不等于 可能的值为： • 未启用 • 不适用 • 已启用 • 未知	iOS/Android
防网络钓鱼状态	此字段显示防网络钓鱼状态	可能的运算符： • 等于 • 不等于 可能的值： • 未启用 • 不适用 • 已启用 • 未知	iOS/Android
防网络钓鱼 VPN 状态	此字段显示防网络钓鱼 VPN 状态	可能的运算符： • 等于 • 不等于 可能的值： • 未启用 • 不适用 • 已启用 • 未知	iOS/Android
电池信息	此字段具有以下属性： • 电池电量 - 显示 Android 操作系统报告的当前电池电量 • 电池运行状况状态 - 由 Android 操作系统报告 • 电池充电状态 - 由 Android 操作系统报告	有关可能的值的信息，请参阅使用高级搜索。	Android

UI 字段	描述	可能的值	支持的平台
	• 电池运行状况百分比（特定于 OEM）- 设备（来自支持的设备制造商，如 Zebra）的电池运行状况百分比 • 电池制造日期 (OEM) - 设备（来自支持的设备制造商，如 Zebra）的电池制造日期 • 电池充电循环 (OEM) - 设备（来自支持的设备制造商，如 Zebra）总共完成的充电循环次数		
基带健康状态	此字段指示设备的基带健康状态。	可能的运算符是： • 等于 • 不等于 可能的值是“正常”或“错误”。	iOS 27.0+ 受监控设备
启动令牌可用	此字段表示启动令牌是否对设备可用。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。	macOS
Autopilot 已注册	此字段指示设备是否已注册 Autopilot。	• 等于 • 不等于 可能的值是“是”和“否”。	Windows
Bridge 上次签入	此字段表示客户端 Bridge 上次签入的时间。	可能的运算符是： • 小于 • 少于或等于 • 大于 • 大于或等于 • 在范围内 • 不在范围内 输入 Bridge 上次签入时间的数值。 选择下列持续时间的任意选项： • 小时 • 天 例如：距离 Bridge 上次签入未满 12 小时。	Windows
相机健康状态	此字段指示设备的相机健康状态。	可能的运算符是： • 等于 • 不等于 可能的值是： • 确定	iOS 27.0+ 受监控设备

UI 字段	描述	可能的值	支持的平台
		• 错误 • 非正版（如果不是正版 Apple 组件）	
客户端上次签入	此字段表示客户端的上次签入时间。	可能的运算符是： • 小于 • 大于 输入上次签入时间的数值。 为持续时间选择以下其中任一选项： • 小时 • 天 示例：客户端上次签入不足 12 小时前。	iOS/macOS/Android
客户端已注册	此字段表示已注册客户端的状态。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。	iOS/macOS/Android
存在安全危险	此字段表示设备是否已 Root/存在安全危险。	可能的运算符是： • 等于 • 不等于 可能的值是： • 越狱或 Root • 无安全危险	iOS/Android
当前国家/地区名称	此字段表示对应于设备报告当前连接的移动国家/地区代码 (MCC) 或移动网络代码 (MNC) 的当前国家/地区名称。	可能的运算符是： • 等于 • 不等于 可能的值是表示住宅所在国家/地区名称的下拉列表值。	iOS/macOS/Android
当前 MCC	此字段表示当前移动设备的国家/地区代码	输入要验证的属性值。 可能的运算符是： • 等于 • 不等于	iOS/macOS/Android
当前 MNC	此字段表示当前移动设备的网络代码	输入要验证的属性值。 可能的运算符是： • 等于 • 不等于	iOS/macOS/Android
自定义设备属性	此字段允许将现有的自定义设备属性添加为规则条件以验证其值。	输入要验证的属性值。 可能的运算符是： • 等于 • 不等于 • 包含 • 不包含 值可以是 ASCII 字符串，包括空格和 Unicode 字	iOS/macOS/Android/Windows

UI 字段	描述	可能的值	支持的平台
		符。	
自定义 LDAP 属性	此字段允许将现有的自定义 LDAP 属性添加为规则条件以验证其值。	输入要验证的属性值。 可能的运算符是： • 等于 • 不等于 • 包含 • 不包含 值可以是 ASCII 字符串，包括空格和 Unicode 字符。	iOS/macOS/Android/Windows
自定义用户属性	此字段允许将现有的自定义用户属性添加为规则条件以验证其值。	输入要验证的属性值。 可能的运算符是： • 等于 • 不等于 • 包含 • 不包含 值可以是 ASCII 字符串，包括空格和 Unicode 字符。	iOS/macOS/Android/Windows
数据漫游	此字段使数据漫游能够用作规则条件来验证其值。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。 如果支持的设备未报告有关此字段的信息，则默认值为否。	iOS/Android
设备类型	此字段表示设备型号。	可能的运算符是： • 等于 • 不等于 • 开头为 • 结尾为 可能的值是文本值。	iOS/macOS/Android/Windows
设备类型 (Apple)	此字段代表设备的 Pretty Model 名称。	可能的运算符是： • 等于 • 不等于 • 开头为 • 结尾为 可能的值是文本值。	iOS/macOS
显示健康状态	此字段指示设备的显示健康状态。	可能的运算符是： • 等于 • 不等于 可能的值是：	iOS 27.0+ 受监控设备

UI 字段	描述	可能的值	支持的平台
		• 确定 • 错误 • 非正版（如果不是正版 Apple 组件）	
加密已启用	此字段决定设备加密/数据加密是否已启用。	是 - 设备加密/数据加密已启用。 否 - 设备加密/数据加密未启用。	iOS/Android/Windows
GUID	此字段表示设备 GUID。	可能的运算符是： • 等于 • 不等于 • 开头为 • 结尾为	iOS/macOS/Android/Windows
Face ID 健康状态	此字段指示设备 Face ID 健康状态。	可能的运算符是： • 等于 • 不等于 可能的值是“正常”或“错误”。	iOS 27.0+ 受监控设备
原籍国家/地区名称	此字段表示对应于编程到设备 SIM 或 eSIM 的移动国家/地区代码 (MCC) 或移动网络代码 (MNC) 的住宅所在国家/地区名称。	可能的运算符是： • 等于 • 不等于 可能的值是表示住宅所在国家/地区名称的下拉列表值。	iOS/Android/Windows
Windows 更新失败	该字段确定设备是否不符合最新的更新规则。	是 - 设备不符合最新的更新。 否 - 设备符合最新的更新。	Windows
家用 MCC	此字段表示当前移动设备的国家/地区代码。	输入要验证的属性值。 可能的运算符是： • 等于 • 不等于	iOS/macOS/Android
家用 MNC	此字段表示当前移动设备的网络代码。	输入要验证的属性值。 可能的运算符是： • 等于 • 不等于	iOS/macOS/Android
IMEI	此字段表示第一个 SIM 卡槽的 IMEI 号。	可能的运算符是： • 等于 • 不等于 • 开头为 • 结尾为	iOS/Android/Windows
IMEI2	此字段表示第二个 SIM 卡槽的 IMEI 号。	可能的运算符是： • 等于 • 不等于	Android

UI 字段	描述	可能的值	支持的平台
IMSI	此字段表示 SIM 卡的 IMSI 号。	• 开头为 • 结尾为 可能的运算符是： • 等于 • 不等于 • 开头为 • 结尾为	Android/Windows
机构恢复密钥已启用	此字段指示设备上是否启用了机构恢复密钥。	可能的运算符是： • 等于 • 不等于	macOS
上次签入	通过此字段，您可以通过 MDM 渠道设置与受管设备上次签入时间相关的条件。	可能的运算符是： • 小于 • 大于 • 为空 输入上次签入时间的数值。 为持续时间选择以下其中任一选项： • 小时 • 天 示例：上次签入时间超过 12 小时。	iOS/macOS/Android/Windows
最后修补程序 ID	此字段允许您设置与最后一个修补程序 ID 相关的条件。	可能的运算符是： • 等于 • 不等于 • 小于 • 少于或等于 • 大于 • 大于或等于 • 包含 • 不包含 • 开头为 • 开头不为 • 结尾为 • 结尾不为	Windows
最后修补程序安装于	此字段允许您设置与上次安装的修补程序相关的条件。	可能的运算符是： • 小于 • 大于	Windows

UI 字段	描述	可能的值	支持的平台
定位器服务已启用	此字段表示设备是否已启用设备定位器服务（查找我的手机）。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。	iOS
制造商	此字段允许您设置与设备制造商相关的条件。	可能的运算符是： • 等于 • 不等于 可能的值是： • Samsung • NOKIA • HTC • LGE • Apple Inc	iOS/macOS/Android/Windows
MTD 激活状态	此字段显示 MTD 激活状态	可能的运算符： • 等于 • 不等于 可能的值： • 不适用 • 错误 • 挂起 • 受保护	iOS/Android
MDM 管理	此字段决定设备是否为已启用 MDM/设备管理员。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。	iOS/macOS/Android
MDM 注册类型	此字段指示设备的注册类型。	可能的运算符是： • 等于 • 不等于 可能的值是： • 用户 • 设备 • 受监控 • 无	iOS 27.0+、macOS 27.0+、tvOS 27.0+、visionOS 27.0+ 和 watchOS 27.0+
MDM 返回服务	此字段指示使用应用程序保存的 MDM 返回服务的设备状态。	可能的运算符是： • 等于	iOS 27.0+ 和 visionOS 27.0+

UI 字段	描述	可能的值	支持的平台
		• 不等于 可能的值为 True 或 False。	
多用户模式	此字段指示设备 (iPad) 是否使用多用户模式。	可能的运算符是： • 等于 • 不等于 可能的值是是或否。	iOS 27.0+
近场健康状态	此字段指示设备 NFC 健康状态。	可能的运算符是： • 等于 • 不等于 可能的值是“正常”或“错误”。	iOS 27.0+ 受监控设备
操作系统	此字段表示设备的操作系统类型。	可能的运算符是： • 等于 • 不等于 可能的值是： • macOS • Android • iOS • Windows • visionOS	iOS/macOS/visionOS/Android/Windows
操作系统版本	此字段表示设备的操作系统 Build 版本。	可能的运算符是： • 等于 • 不等于 • 小于 • 少于或等于 • 大于 • 大于或等于 • 包含 • 不包含 • 开头为 • 开头不为 • 不为空 • 为空 • 结尾为 • 结尾不为	iOS/macOS/visionOS/Android/Windows
操作系统版本	此字段表示设备的操作系统版本。	可能的运算符是： • 等于	iOS/macOS/visionOS/Android/Windows

UI 字段	描述	可能的值	支持的平台
		• 不等于 • 小于 • 少于或等于 • 大于 • 大于或等于 • 在范围内 • 不在范围内 可能的值是文本。	
操作系统及版本	此字段表示设备的操作系统和操作系统版本。	可能的运算符是： • 等于 • 不等于 • 小于 • 少于或等于 • 大于 • 大于或等于 • 在范围内 • 不在范围内 可能的值是文本。	iOS/macOS/visionOS/Android/Windows
所有权	此字段表示设备的所有值类型。	可能的运算符是： • 等于 • 不等于 可能的值是： • 用户拥有 • 未设置 • 公司所有	iOS/macOS/Android/Windows
个人恢复密钥已启用	此字段指示是否启用了个人恢复密钥。	可能的运算符是： • 等于 • 不等于	macOS
通行码符合配置文件	此字段表示设备的通行码是否与配置文件相符。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。	iOS/macOS/Android
个人热点已启用	此字段表示个人热点功能是否在设备上启用。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。	iOS

UI 字段	描述	可能的值	支持的平台
		个人热点设置仅在特定运营商下可用。	
手机号码	此字段表示设备手机号码。	可能的运算符是： • 等于 • 不等于 • 包含 • 开头为 • 结尾为	iOS/Android/Windows
公用 IP 地址	此字段显示公用 IP 地址。 如果设备使用 VPN 连接或代理服务器连接到 Ivanti Neurons for MDM，则显示代理 WAN IP 地址。	可能的运算符是： • 在范围内 • 不在范围内 • 不为空 • 为空	Android/ChromeOS
漫游	此字段表示设备的漫游状态。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。	iOS/Android/Windows
安全锁定模式	此字段指示设备是启用还是禁用锁定模式。	可能的运算符是： • 等于 • 不等于 可能的值为 True 或 False。	iOS 27.0+ 和 macOS 27.0+
已阻止 Sentry	指出设备是否被 Sentry 阻止。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。	iOS/macOS/Android/Windows
状态	此字段表示注册状态。	可能的运算符是： • 等于 • 不等于 默认可能的值是“活动”。 在自定义策略中，它通过删除所有其他潜在值将设备状态限制为“活动”，因为设备签入为“活动”、“待停用”和“待擦除”状态时会进行策略评估，并且这些设备将在签入时评估其策略。	iOS/macOS/Android
序列号	此字段表示设备序列号。	可能的运算符是： • 等于 • 不等于 • 开头为 • 结尾为	iOS/macOS/Android/Windows

UI 字段	描述	可能的值	支持的平台
受监控	此字段表示设备是否受管监管。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。	iOS/macOS
补充内部版本	此字段表示设备的补充内部版本。	可能的运算符是： • 等于 • 不等于 • 小于 • 少于或等于 • 大于 • 大于或等于 • 包含 • 不包含 • 开头为 • 开头不为 • 结尾为 • 结尾不为 • 不为空 • 为空	iOS/macOS
补充操作系统/版本额外信息	此字段表示设备的补充操作系统内部版本。	可能的运算符是： • 等于 • 不等于 • 小于 • 少于或等于 • 大于 • 大于或等于 • 包含 • 不包含 • 开头为 • 开头不为 • 结尾为 • 结尾不为 • 不为空 • 为空	iOS/macOS

UI 字段	描述	可能的值	支持的平台
Touch ID 健康状态	此字段指示设备 Touch ID 健康状态。	可能的运算符是： • 等于 • 不等于 可能的值是： • 确定 • 错误 • 不适用（如果是 iPhone）	iOS 27.0+ 受监控设备
用户已启用	此字段表示用户是否已启用。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。	iOS/macOS/Android/Windows
用户组	此字段表示用户组。	可能的运算符是： • 等于 • 不等于	iOS/macOS/Android/Windows
超宽带健康状态	此字段指示设备的超宽带健康状态。	可能的运算符是： • 等于 • 不等于 可能的值是“正常”或“错误”。	iOS 27.0+ 受监控设备
语音漫游	此字段表示语音漫游是否在设备上启用。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。 语音漫游设置仅在特定运营商下可用。 禁用语言漫游也会禁用数据漫游。 如果受支持的设备不报告有关此字段的信息，则默认值为不等于。	iOS
已阻止 Access	指出设备是否已被 Access 阻止。	可能的运算符是： • 等于 • 不等于 可能的值是“是”和“否”。	iOS/macOS/Android/Windows
合规性	指出设备是否合规。	可能的运算符是： • 等于 • 不等于 可能的值有两种，合规与不合规。	iOS/macOS/Android/Windows
已阻止合规性操作	指出是否已阻止设备。	可能的运算符是： • 等于	iOS/macOS/Android/Windows

UI 字段	描述	可能的值	支持的平台
		• 不等于 可能的值是“是”和“否”。	

不可隔离配置

下表显示不可隔离配置的列表：

操作系统	不可隔离配置
Android	• Android 应用目录 • Android 加密 • Android Enterprise • Android Enterprise 应用 • Android Zebra • 反网络钓鱼保护 • Android 工作认证 (Work Challenge) • 设备通行码 • 文件下载 • 锁定和自助服务终端：Android 设备管理模式 • 锁定和自助服务终端：Samsung Knox Standard • 仅限 MAM • 具有工作配置文件/公司拥有设备上的工作配置文件的受管设备 • 工作受管设备（设备所有者） • Samsung 手机限制 • SafetyNet 认证 • 公司拥有设备上的工作配置文件
iOS 和 macOS	• 防钓鱼保护 (iOS) • 应用通知 (iOS) • AppStation 站点 (iOS) • Filevault 恢复密钥 (macOS) • Filevault 2 (macOS) • 全局代理（iOS 和 tvOS） • 主屏幕布局（iOS 和 tvOS） • iOS 应用控制 • iOS 限制 • iOS 软件更新 (iOS) • macOS 防火墙 • macOS 软件更新 • 仅限 MAM (iOS) • MI 客户端隐私 (iOS/macOS) • 网络使用情况 (iOS) • Office 365 帐户创建 (macOS) • 单个应用程序模式（iOS 和 tvOS） • 系统隐私控制 (macOS)

操作系统	不可隔离配置
	• 系统策略受管 (macOS) • 系统策略规则选项 (macOS) • 时间服务器 (macOS) • Web 内容筛选器 (iOS)
Windows	• Windows 应用控制 • Windows 限制DDF（数据定义文件） • Windows 防火墙 • Windows 网络代理 • Windows 限制 • Windows 更新
全部	• Active Directory • 客户端服务 • 移动设备管理 • 移动威胁防御激活 • 移动威胁防御本地操作 • 通行码 • 隐私 • 隐私声明 • ServiceConnect • 同步

如果您未看到策略页面，这可能是您没有所需权限。 您需要以下角色之一：

- 设备管理
- 设备只读

11.3. 监控和控制允许的应用程序

许可证： Silver

要控制在设备上安装何种应用程序，您可以创建允许的应用策略。 此策略也支持 MobileIron Packager (MIP) 内部 macOS 应用。 该策略需包含以下信息：

- {{允许列表应用}}
- {{阻止列表应用}}
- {{所需应用}}
- {{合规性操作}}

如果应用需要并加入阻止列表，针对所需列表进行的应用评估优先。 例如，如果应用 A1 同时位于所需列表和阻止列表，此设备的应用策略评估行为如下：

- 如果在设备上安装 A1，则设备将符合要求。
- 如果在设备上未安装 A1，则设备将不符合要求。

支持的设备

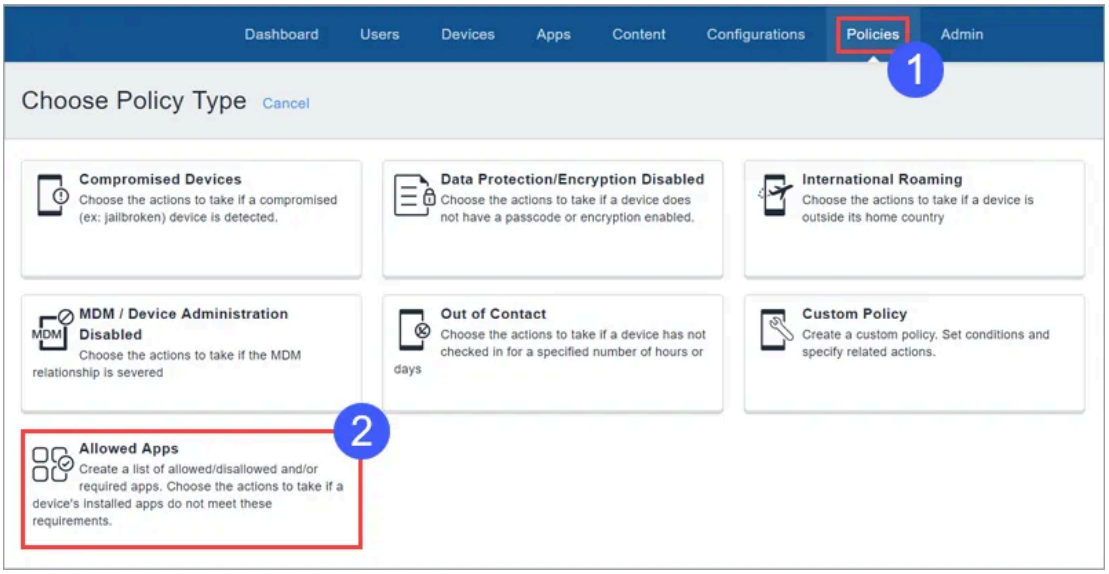
- Android 4.2 或支持的更新版本
- iOS 8.0 或支持的更新版本
- macOS 10.12 或支持的更新版本
- Windows 10 或支持的更新版本。

先决条件

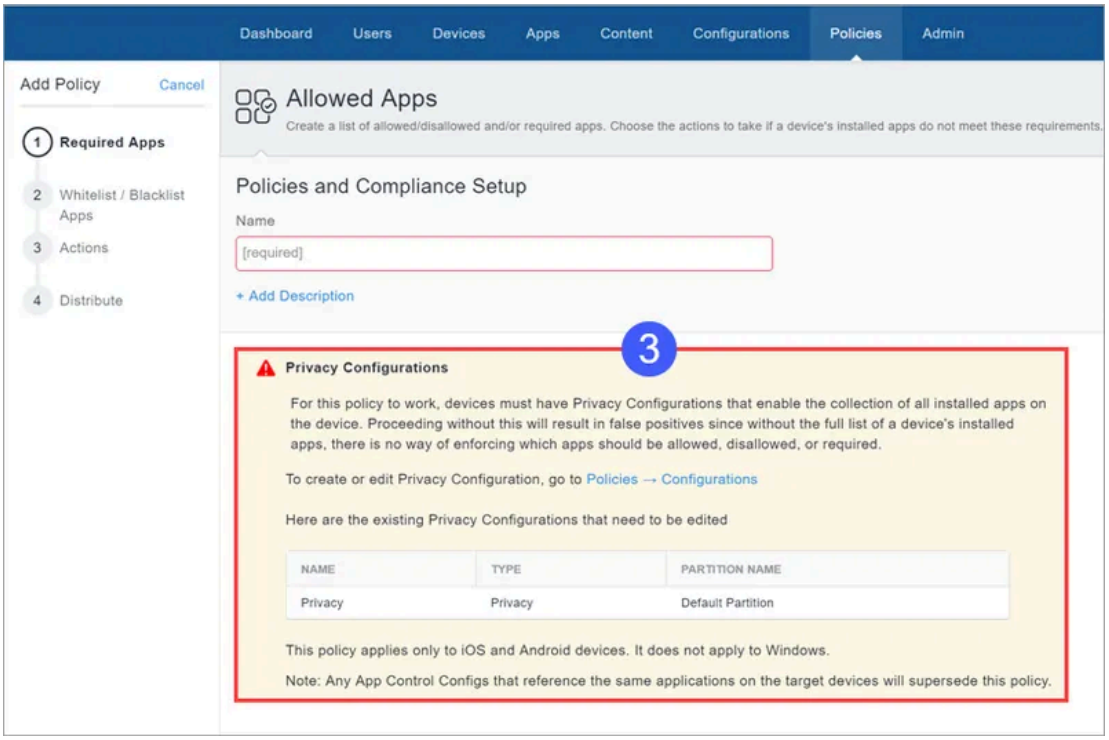
- 分配到设备的隐私配置必须允许收集应用信息，以便允许的应用策略正常运行。 如果您将允许的应用策略应用到某设备，请检查指定到该设备的隐私配置。

如果您不确定受影响的配置：

1. 转到**策略**。



单击**允许的应用程序**。



3. 在**隐私配置**中，请注意需要编辑的配置。
4. 转至**配置**。
5. 有关每个隐私配置，您需要注意：
    1. 选择配置。
    2. 单击**编辑**。
    3. 在**收集应用库存**中，选择**针对设备上的所有应用**。
    4. 单击**完成**。

创建允许的应用策略

先决条件

- 支持 Android Enterprise 访问 Google Play 商店，并将新应用添加到允许的应用策略。

程序

1. 转到**策略**，并单击 **+ 添加**。

2. 单击**允许的应用程序**。

3. 在**名称**字段中，键入此策略的名称。
4. 在**说明**字段中，键入说明策略目的的可选文本。
5. 单击以下其中一个或两个选项卡，选择要加入允许列表或阻止列表的应用：

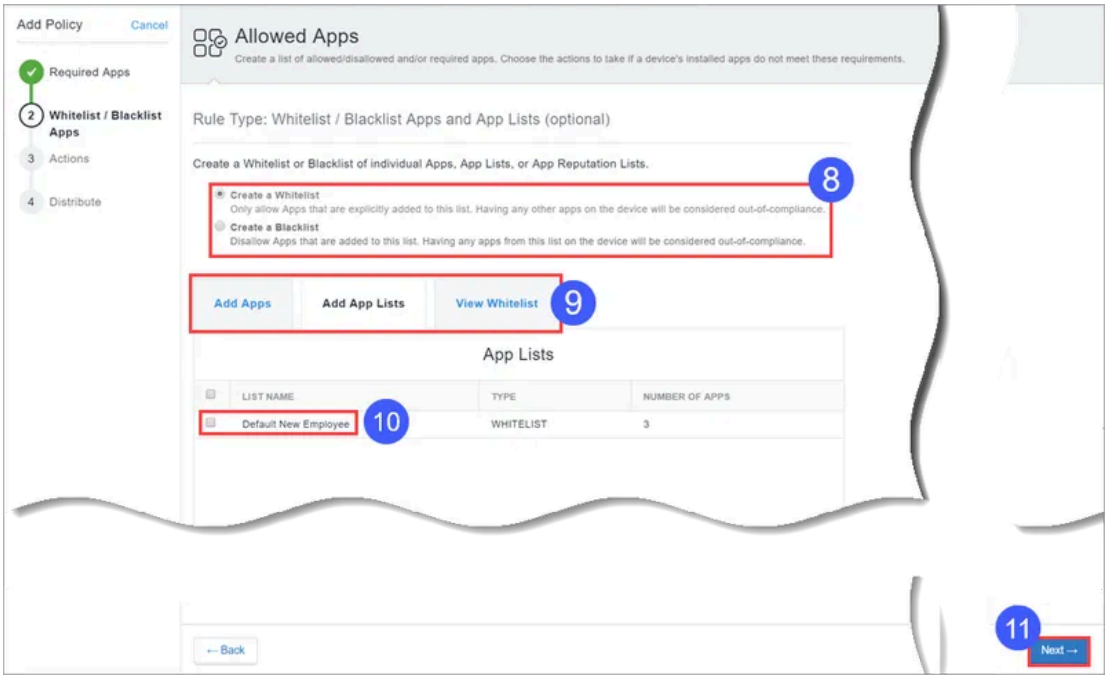
- 单击“按查找添加”，以从 App Store 或 App Catalog 搜索并选择应用。
  请确保支持 Android Enterprise 访问 Google Play 商店。
  
- 点击**手动添加**，通过输入 Android、Windows、iOS 或 macOS 系统应用程序的捆绑包 ID 来选择应用程序。

选择**添加应用列表**选项卡，然后选择所需的应用列表。

6. 使用结果字段来选择必要应用程序或应用程序列表。
7. 单击**下一步**

> 点击**查看所需列表**选项卡，查看您迄今为止选择的应用程序列表。

8. 选择是否创建允许列表或阻止列表。



9. 使用**允许列表/阻止列表应用和应用列表**部分，选择应用和应用列表。

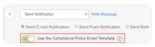
> 无法同时将设备加入允许列表和阻止列表。 创建允许列表表示所有其他应用会加入阻止列表。

10. 使用结果字段来选择必要应用程序或应用程序列表。
    - 选择**添加应用程序列表**选项卡，然后选择希望的应用程序列表。
11. 单击**下一步**。

> 单击**查看允许列表或阻止列表**选项卡，了解迄今为止选择的应用列表。

12. 选择设备不合规时采取的操作：

操作	流程
监控器	当前始终选择。 需要 Sentry 版本 9.0.0 或更高版本才能使用分层合规性操作。
不进行任何操作	选择以便在设备不合规时不采取任何操作。
发送通知	

发送电子邮件	选择以便向设备用户的电子邮件地址发送电子邮件，通知他们设备不合规。
	• 打开**使用合规策略电子邮件模板**选项，以将您在此处配置的消息插入您按品牌化电子邮件模板中的自定义电子邮件模板所述配合的策略通知电子邮件模板。 有关概览，请查看配置和使用策略合规通知电子邮件。
	
	• 您可以通过包含可选替换变量来自定义邮件，以便为收件人提供有关违反策略的更多详细信息和其他相关信息。 这为不合规设备的用户提供有关违反策略的相关信息，以便他们采取补救措施。 单击以下属性类型，以显示完整的变量列表：
	  ◦ 策略属性包含 $、$ 和 $。
	  ◦ 用户属性包括 $、$ 和 $。
	  ◦ 设备属性包含 $、$ 和 $。

发送推送通知	选择以便向设备发送推送通知，告知设备不合规。
发送推送通知和电子邮件通知	选择以便同时向设备发送推送通知，并向设备用户的电子邮件地址发送电子邮件，通知他们设备不合规。 您可以通过包含可选的替代变量来自定义邮件，以便为收件人提供更多详细信息，如前面发送电子邮件操作所述。
等待	选择以便延迟指定时间段的操作，以允许用户在设备保持不合规的情况下，执行额外操作之前修复违规。
阻止	使用 Sentry 阻止托管设备访问电子邮件和启用了 AppConnect 的应用程序。
隔离	选择以根据下表中的操作移除对应用程序、内容和服务器的访问权限。 不允许删除所有应用程序操作。
在设备重新处于合规状态时发送通知	

发送电子邮件	向设备用户的电子邮件地址发送电子邮件，并在设备重新处于合规状态时通知。
	• 如上所述，您可以使用策略通知电子邮件模板。
	• 您可以通过包含可选替换变量来自定义邮件，以便为收件人提供有关违反策略的更多详细信息和其他相关信息。 单击以下属性类型，以显示完整的变量列表：
	  ◦ 策略属性包括 $、$ 和 $。
	  ◦ 用户属性包括 $、$ 和 $。
	  ◦ 设备属性包含 $、$ 和 $。
	  ◦ 从**管理>属性**页面创建的自定义设备/用户/LDAP 属性。

发送推送通知	在设备重新处于合规状态时，向设备发送推送通知。
发送推送通知和电子邮件通知	同时向设备发送推送通知，向设备用户的电子邮件地址发送电子邮件，并在设备重新处于合规状态时通知。 您可以通过包含可选的替代变量来自定义邮件，以便为收件人提供更多详细信息，如前面发送电子邮件操作所述。

如果您有 Platinum 许可证，允许的应用策略支持分层合规操作。

（可选）附加隔离操作	描述
隔离受管应用	从设备中移除 Ivanti Neurons for MDM 管理的应用，并启用“阻止新应用下载”选项，以阻止应用重新在设备上安装。 选择下列选项之一： • **所有应用程序** • **委派应用** - 通过查找或手动（使用捆绑 ID 或软件包名称），添加一个或多个应用。 单击**查看应用**选项卡，以查看已添加应用的列表。 阻止 App Store 访问默认隔离操作不再可用。 在特定设备上，由于特定设备限制，因此隔离操作不会将应用从设备中移除。
阻止新的应用程序下载	阻止将任何新应用程序下载到设备。 选择下列选项之一： • **所有应用程序** • **委派应用** - 通过查找或手动（使用捆绑 ID 或软件包名称），添加一个或多个应用。 单击**查看应用**选项卡，以查看已添加应用的列表。 阻止 App Store 访问默认隔离操作不再可用。
删除配置	移除设备中的 Ivanti Neurons for MDM 配置。 选择下列选项之一： • **所有配置** • **委派配置** - 从列表中选择一个或多个配置，或者进行搜索。 单击**选定配置**选项卡，以查看选定配置的列表。
删除内容	从设备中移除与 Ivanti Neurons for MDM 分发的应用相关联的所有内容和媒体。
暂停个人应用	在隔离设备的个人端暂停应用，以表示设备用户需要解决设备的合规性问题，才可以正常使用。 在公司拥有的设备中，支持配置为公司拥有设备上的工作配置文件的 Android 11+ 设备。
默认隔离操作 - 始终执行这些操作。	
阻止 App Store 访问	阻止设备通过 Ivanti Neurons for MDM 访问应用商店。
阻止 Content Store 访问	阻止设备通过 Ivanti Neurons for MDM 访问内容商店。
阻止 AppConnect	阻止设备使用 AppConnect 功能。
阻止 AppTunnel	阻止设备上的应用程序通过 AppTunnel 访问内容和服务器。
阻止 ActiveSync	阻止设备通过 ActiveSync 服务器访问电子邮件。

单击**下一步**。

14. 配置分配。
15. 单击**完成**。

有关对允许的应用策略设置更高或更低优先级的详细信息，请查看确定策略的优先级。

11.4. 确定策略的优先级

允许的应用策略支持优先级，类似于配置。 优先级用于确定将哪个相同类型的策略分配到多个设备组，以及相同设备显示在多个设备组中的情况。 例如，在以下情况下，策略优先级有助于确定策略分发：

- “必需应用 A”需要分发到设备组 1，
- “必需应用 B”需要分发到设备组 2，
- 用户的设备是两个设备组的成员。

您可以按如下方式确定策略的优先级：

1. 转至**策略 > 策略与合规**。
2. 选择**操作 > 优先级策略**。 如果**操作**未显示，可能没有多个需要优先级的策略。
3. 使用箭头从高（上）到低（下）排列优先级。 锁定图标表示，在不编辑策略中的所有设备分发设置，无法更改策略的优先级。
4. 单击**保存**。

11.5. Windows 硬件策略

Couldn't convert your doc.

12. 管理

通过管理部分，您可以从 Ivanti Neurons for MDM 门户管理用户、设备和配置。 以下部分包含您作为管理员执行的所有任务的列表：

- 系统
- 基础设施
- 设置 (Apple)
- 使用 Windows 设备工作
- 使用 Microsoft Azure 设置
- 与 Google 应用连接
- 使用 ChromeOS 设备
- 固件管理
- 租户暂停
- 管理脚本和文件
- 品牌
- 添加对非 iOS 设备的管理

12.1. 系统

本部分包含以下主题：

- 属性
- 设备清理设置
- GDPR 配置文件
- 通知电子邮件
- 角色管理
- 空间
- 支持管理员
- 管理 > 系统使用通知

12.1.1. 属性

使用“属性”页面执行以下任务：

- 管理可以针对用户、设备和应用程序进行记录的信息类型。
- 查看 Ivanti Neurons for MDM 跟踪的信息的标准类型。

自定义用户属性包括部门或内部 ID 等信息。 每个属性都有一个对应变量，可使用该变量构建组或分发配置。

> 创建用户规则组条件时，如果自定义属性具有数字值，则 Ivanti Neurons for MDM 不支持整数运算。

创建自定义属性

可以在 Ivanti Neurons for MDM 管理门户中创建自定义属性。

步骤

1. 登录到管理门户。
2. 导航到**管理员** > **系统** > **属性**。
3. 在**自定义属性**中，单击 **+ 添加**。
4. 在**属性名称**字段中输入代表属性的文本内容。

> 您输入的文本将用于在**使用情况**字段中创建相应变量。

从以下**属性类型**选项中，选择任何属性类型。

   - **用户**
   - **设备**
   - **应用**
   - **IDP**（有关详细信息，请参阅使用 SCIM 进行用户配置 或 连接 Ivanti Neurons for MDM 与 Entra ID 用户源）

如果属性类型是“设备”，请选择以下**数据类型**选项之一：

   - **数字**
   - **文本**

7. **保留属性**（可选）：仅当属性类型为**设备**时，才可以使用此选项。 选择此选项，即使在设备上执行擦除/停用操作时，也可以保留自定义属性。
8. 单击**添加**。
   在属性页面中，创建的自定义用户属性会显示在**已添加管理员**部分下方。

> 自定义属性组合 $ + $ + $ + ${Static String} 支持任何顺序。

重命名自定义属性

重命名自定义属性将重命名在以下实体中使用的该自定义属性的所有引用：

- 自定义策略

- 用户组
- 设备组
- 应用程序分配过滤器
- 空间

> 任何其他实体（例如策略合规性操作中的配置、邀请电子邮件模板、电子邮件和推送消息等）中的自定义属性的引用将不会更新。

步骤

1. 在**已添加管理员**下方，单击要重命名属性旁边的 **+ 编辑**。
2. 在**属性名称**字段中输入代表属性的新名称。

> 您输入的文本将用于在**使用情况**字段中创建相应变量。

单击**保存**。

删除自定义属性

删除自定义属性还将从所有相关联的用户或设备上删除该属性的值。 该操作不能逆转。

如果在以下任何实体中使用该属性，则不能删除自定义属性：

- 自定义策略
- 用户组
- 设备组
- 应用程序分配过滤器
- 空间

在尝试删除自定义属性前，应先从实体中删除自定义属性。

如果要删除的属性没有引用上述任何实体，单击该属性旁边的**删除**将显示弹出消息，以便确认该操作。 确认该操作，并单击**删除**。

> 以下自定义属性的字段名称在适用的规则生成器中进行排序：

- 自定义 LDAP 属性
- 自定义用户属性
- 自定义设备属性
- 自定义 IDP 属性
- 自定义应用程序属性

查看系统属性

系统属性是您在配置中用作变量的预定义属性。 完整列表在**管理员** > **系统** > **属性**页面的**系统属性**部分中提供。 系统属性包括以下类型的属性：

- 用户属性
- 设备属性
- 电子邮件模板属性

- 系统属性
- 时间戳属性
- Entra ID 自定义用户属性
- 策略属性

用户属性

使用用户属性指定用户相关信息。

密钥	说明
$	部门属性（需要 Entra ID）
$	电子数据交换 - 个人标识符
$	用户的受管 Apple ID
$	sAMAccountName 属性（需要 Active Directory）
$	从可分辨名称中提取的通用名称 (CN) 属性（需要 LDAP）
$	显示名称
$	可分辨名称（需要 LDAP）
$	电子邮件地址的域部分（“@”后面的部分）
$>	电子邮件地址的本地部分（“@”前面的部分）
$	电子邮件地址
$	名字
$	姓氏
$	区域设置
$	从可分辨名称中提取的组织单位 (OU) 属性（需要 LDAP）
$	Kerberos 领域信息（需要 Active Directory）
$	登录 ID 的域部分（“@”后面的部分）
$	登录 ID 的本地部分（“@”前面的部分）
$	登录 ID（电子邮件格式）
$	userPrincipalName 属性（需要 Active Directory）

设备属性

使用设备属性指定移动设备相关信息。

密钥	说明
$	客户端上次签入日期（最近签入 - MDM 或客户端）
$	替代序列号
$	客户端应用使用的标识符
$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $	全局唯一设备标识符 ICCID IMEI2 IMEI IMSI 设备上次签入日期（最近签入 - MDM 或客户端） 内部设备标识符 MDM 使用的标识符 MEID 型号 设备名称 设备电话号码 群集唯一设备标识符 序列号 iOS UDID Wi-Fi MAC 地址 电话号码 2 ICCID 2

创建自定义属性并在托管应用程序配置中引用此属性时，如果属性值得到更新，则托管应用程序配置中引用的属性也会更新，且托管应用程序配置将重新推送给设备。

更新“自定义”或“设备”属性并将配置推送到设备时，Android Kiosk 品牌配置也应更新。

应用程序属性

使用应用程序属性指定应用程序信息，并创建自定义应用程序组。

密钥	说明
$	日期应用程序已添加到 AppCatalog
$	应用程序的名称
$	应用程序操作系统
$	应用程序捆绑或程序包 ID
$	描述应用程序的导入来源
$	描述 iOS 或 macOS 应用程序是否为 VPP

电子邮件模板属性

密钥	说明
$	电子邮件正文
$	电子邮件主题

时间戳属性

可变密钥	说明
$	当前时间戳（自 Epoch 起的毫秒数）

策略模板属性

密钥	说明
$	违规策略名称
$	发送消息后要采取的下一层合规操作（与等待和停用不同）
$	设备处于不合规状态的天数
$	初次触发策略违规时的时间戳（UTC DD-MM-YYYY 格式）
$	规则定义（查询字符串当前的显示方式）

相关主题：

- 将自定义属性分配到用户
- 将自定义属性分配到设备
- 将自定义属性从用户中删除
- 将自定义属性从设备中删除
- 变量

12.1.2. 设备清理设置

设备清理会自动化未使用设备的设备生命周期。 可以停用在指定天数内失联的设备。 可以删除已停用指定天数的设备。 “审计跟踪”页面会捕获“停用设备”、“删除设备”和“删除已擦除的设备”设置。

下表提供了支持设备清理设置的 Android 设备相关信息：

模式	不合规时停用	删除已停用的设备	强制停用或待停用	删除已擦除的设备	删除待擦除的设备
Android 工作配置文件（配置文件所有者）	是	是	是	否	否
设备管理员/公司拥有设备上的工作配置文件	是	是	是	是	是
工作托管设备/带有工作配置文件的 Android 托管设备	否	否	否	是	是

先决条件

您必须拥有系统管理角色权限才能访问此设置。

停用设备

步骤

1.	转到**管理员 > 系统 > 设备清理**。 随即打开“设备清理”页面。
2.	选择**停用设备**。
3.	使用**停用设备**表格指定详细信息。
4.	点击**显示尚未签入的设备列表**。 显示指定天数未签入的设备列表。
5.	点击**立即停用设备**或计划设备停用事宜。
6.	Ivanti Neurons for MDM 管理门户将停用指定设备。
7.	点击**保存**以保存设置。
8.	（可选）如果要更新值，可以点击**重置**，将设置重置为初始设置。

停用设备

字段	说明
选择平台	选择应用设备清理设置所需的平台。 此选项目前仅在**停用设备**和**停用待停用设备**设置中可用。
停用超过以下时间尚未签入的设备（按天计）	天数：默认值为 30 天，允许的上限值为 365 天。
每个会话可停用的设备数量上限	选择 100、500 或 1000（默认值为 100）。
按计划自动停用设备	选中该复选框以根据预先设定的计划停用设备。
停用计划配置	选择以下选项之一可设置停用频率： • **每日 -** 设置为每天停用设备。 • **每周 -** 指定一周中具体在星期几计划停用设备。 • **每月 -** 设置为在每月的第一天停用设备。

删除已停用的设备

步骤

1. 转到**管理员** > **系统** > **设备清理**。 随即打开“设备清理”页面。
2. 选择**删除已停用的设备**。
3. 使用**删除已停用的设备**表格可指定详细信息。
4. 点击**显示停用设备列表**。 显示已停用指定天数的设备列表。
5. 点击**立即删除已停用的设备**或计划设备删除事宜。
6. Ivanti Neurons for MDM 管理门户将删除指定设备。
7. 点击**保存**以保存设置。
8. （可选）如果要更新值，可以点击**重置**，将设置重置为初始设置。

删除已停用的设备

字段	说明
删除停用时长超过以下时间的设备（按天计）	天数：默认值为 30 天，允许的上限值为 365 天。
每个会话可删除的停用设备上限	选择 100、500 或 1000（默认值为 100）
按计划自动删除已停用的设备	选中该复选框以根据预先设定的计划停用设备。
删除计划配置	选择以下选项之一可设置删除频率： • **每日 -** 设置为每天删除设备。 • **每周 -** 指定一周中具体在星期几计划进行删除。 • **每月 -** 设置为在每月的第一天删除已停用的设备。

删除已擦除的设备

步骤

1. 转到**管理员** > **系统** > **设备清理**。 随即打开“设备清理”页面。
2. 选择**删除已擦除的设备**。
3. 使用**删除已擦除的设备**表格可指定详细信息。
4. 点击**显示已擦除的设备列表**。 显示已停用指定天数的设备列表。
5. 点击**立即删除已擦除的设备**或计划已擦除设备的删除事宜。
6. Ivanti Neurons for MDM 管理门户将删除指定设备。
7. 点击**保存**以保存设置。
8. （可选）如果要更新值，可以点击**重置**，将设置重置为初始设置。

删除已擦除的设备

字段	说明
删除擦除时长超过以下时间的设备（按天计）	天数：默认值为 30 天，允许的上限值为 365 天。
每个会话可删除的已擦除设备上限	选择 100、500 或 1000（默认值为 100）
按计划自动删除已擦除的设备	选中复选框以根据预先设定的计划删除已擦除的设备。
删除已擦除的计划配置	选择以下选项之一可设置删除频率： • **每日 -** 设置为每天删除已擦除的设备。 • **每周 -** 指定一周中具体在星期几计划进行删除。 • **每月 -** 设置为在每月的第一天删除已擦除的设备。

删除待擦除的设备

步骤

1. 转到**管理员** > **系统** > **设备清理**。 随即打开“设备清理”页面。
2. 选择**删除待擦除的设备**。
3. 使用**删除待擦除的设备**表格可指定详细信息。
4. 点击**显示待擦除的设备列表**。 显示要擦除指定天数的设备列表。
5. 点击**立即删除待擦除的设备**或计划待擦除设备的删除事宜。
6. Ivanti Neurons for MDM 管理门户将删除指定设备。
7. 点击**保存**以保存设置。
8. （可选）如果要更新值，可以点击**重置**，将设置重置为初始设置。

删除待擦除的设备

字段	说明
删除待擦除时长超过以下时间的设备（按天计）	天数：默认值为 30 天，允许的上限值为 365 天。
每个会话要删除的待擦除设备上限	选择 100、500 或 1000（默认值为 100）
按计划自动删除待擦除的设备	选中复选框以根据预先设定的计划删除已擦除的设备。
删除待擦除的计划配置	选择以下选项之一可设置删除频率： • **每日 -** 设置为每天删除待擦除的设备。 • **每周 -** 指定一周中具体在星期几计划进行删除。 • **每月 -** 设置为在每月的第一天删除待擦除的设备。

停用待停用的设备

步骤

1. 转到**管理员** > **系统** > **设备清理**。 随即打开“设备清理”页面。
2. 选择**停用待停用的设备**。
3. 使用**停用待停用的设备**表格指定详细信息。
4. 点击**显示待停用的设备列表**。 显示要停用指定天数的设备列表。
5. 点击**立即强制停用待停用的设备**或计划待停用设备的停用事宜。
6. Ivanti Neurons for MDM 管理门户将停用指定设备。
7. 点击**保存**以保存设置。
8. （可选）如果要更新值，可以点击**重置**，将设置重置为初始设置。

停用待停用的设备

字段	说明
停用超过以下时间尚未签入的待停用设备（按天计）	天数：默认值为 30 天，允许的上限值为 365 天。
每个会话可停用的待停用设备数量上限	选择 100、500 或 1000（默认值为 100）
按计划自动停用待停用的设备	选中该复选框以根据预先设定的计划停用待停用的设备。
停用待停用的计划配置	选择以下选项之一可设置删除频率： • **每日 -** 设置为每天停用挂起的设备。 • **每周 -** 指定一周中具体在星期几计划停用挂起的设备。 • **每月 -** 设置为在每月的第一天停用挂起的设备。

设备停用后，如果签入发生在很久以前，那么仅考虑将最后一次签入时间用于确定设备删除。 例如，如果设备上次签入是在 30 天前，并且设备今天停用（可能是由于“停用未签入超过（天数）的设备”选项），并且如果“删除停用超过（天）的设备”设置为 30 天，则一旦执行了“删除停用设备”作业，该设备将立即被删除。

12.1.3. GDPR 配置文件

Ivanti Neurons for MDM 管理门户现在包含“GDPR 配置文件”页面，允许您将 GDPR 配置文件分配给用户组。 只能将 GDPR 配置文件分配给用户组，而不能分配给单个用户。

注意以下几点：

- 必须先启用 GDPR 配置文件，然后才能将其分配给特定的用户组。
- 如果禁用 GDPR 配置文件，其将关闭已经分配给用户组的所有配置文件限制。
- 启用 GDPR 配置文件后，某些字段的编辑功能将受到限制或禁用。

GDPR 配置文件分配后隐藏的字段

如果某个用户具有 GDPR 配置文件，则 Ivanti Neurons for MDM 在显示有关该用户的信息时，将默认隐藏以下字段：

- **用户 ID**
- **用户的名称**
- **电子邮件地址**
- **序列号**
- **ICCID**
- **IMSI**
- **MEID**
- **IP 地址**
- **电话号码**
- **IMEI**
- **eSIM 标识符**
- **定位**

> 如果将位置添加到 GDPR 配置文件，则对于已分配 GDPR 配置文件的用户，设备位置字段“上次位置”、“纬度”和“经度”将从设备详细信息中掩去。

启用 GDPR 配置文件

可以启用 GDPR 配置文件，并选择必须在 Ivanti Neurons for MDM 管理门户和设备中隐藏的特定字段。

Procedure程序

	1.	**登录到 Ivanti Neurons for MDM 管理门户。**
2.		**前往管理员 > 系统 > GDPR 配置文件。**
	3.	**点击启用。**

4.	点击编辑（铅笔）图标。

	5.	选择必须隐藏的字段。

6.	单击保存。 所选字段将被掩码处理，并且不会为特定用户显示值。

将 GDPR 配置文件分配给用户组

在启用 GDPR 配置文件后，可以将其分配给特定用户组。

Procedure程序

	1.	登录到 Ivanti Neurons for MDM 管理门户。

	2.	转到用户 > 用户组。

	3.	从列表中选择用户组。

	4.	点击操作下拉列表并选择分配 GDPR 配置文件。 GDPR 配置文件会分配给该特定组的所有用户，并且所有选定的值将在整个管理门户和用户设备中被掩码处理。 由于管理员也在“所有用户”组中，请勿将 GDPR 配置文件分配给“所有用户”组。

12.1.4. 通知电子邮件

许可证： Silver

您可以根据通知的严重性级别配置应接收电子邮件通知的用户的电子邮件地址列表。

通知电子邮件功能是可选的，您可以在需要时打开或关闭该功能。 先决条件是，您应该分配系统管理角色以使用此功能。

1. 选择**管理员 > 系统 > 通知电子邮件**。 将显示**通知电子邮件**页面。
2. 在通知电子邮件设置部分，单击**开启**，启用通知电子邮件功能。
3. 单击**添加收件人**。 显示**添加收件人**弹出框。
4. 在**添加收件人**弹出框，更新以下字段：
    - 收件人电子邮件 ID - 输入要向其发送通知的收件人的电子邮件 ID。
    - 待发送的通知类型 - 通过选择复选框，选择通知类型。 以下是通知类型选项：**重要通知**、**警告通知**、**信息通知**。
5. 单击**确定**。 设置的详细信息显示在表中。
6. 单击**保存**，应用更改。

12.1.5. 角色管理

角色是打包的权限组，允许向管理用户授予一组权限，同时限制他们的访问以控制特定的功能区域。 Ivanti Neurons for MDM 提供一组可分配（或编辑）的系统角色，以及用于创建自定义角色的工具。 您可以根据类别搜索特定权限，并在 UI 中显示与特定角色或权限关联的所有选项。 对于作为依赖权限添加的权限，将为其显示工具提示。

> 对于有权访问 Ivanti Neurons for UEM 和 Ivanti Neurons for MDM 的聚合租户，隐藏“角色管理”页面和关联选项。

共有两类权限可用，因此对应也有两种角色：

- **空间特定角色** - 权限特定于空间，因此仅适用于特定空间。 例如，设备管理、空间中的应用管理。
- **跨空间角色** - 权限本质上适用于所有角色。 示例是租户级设置，例如 MDM 证书、App Catalog 设置。

创建自定义角色

您可以创建自定义跨空间或空间特定角色。 在您选择权限时，将自动选择相关权限。 相应地，分配自定义角色的用户仅可以执行在用户访问设备页面或设备详细信息页面时可用的特定操作（例如停用、擦除）。

应用“查看用户注册 PIN”自定义角色后，用户便可以查看具有相同访问级别或权限较低的其他用户的 PIN，且用户无法为其他用户创建 PIN。

> 新创建的自定义角色无法自动分配到任何人。 租户超级管理员需要将其分配到需要的管理员用户，他们稍后可以根据需要将相同角色分配到其他用户。

步骤

1. 前往**管理员** > **角色管理**。
2. 单击 **+ 添加自定义角色**。
3. 在**创建角色**页面，输入新角色的**名称**。
4. （可选）为新角色添加描述。
5. 在**角色类型**中，选择以下角色类型之一：
   - **跨空间角色**
   - **空间特定角色**
6. 在**权限**下，选择所需的细化权限。
7. 有关管理员和用户权限，请见下表。
   单击**保存**。

下表列出了可用于创建自定义角色的权限、角色和属性：

角色类型	权限类别	细化权限
跨空间角色 **管理员**		
	管理自定义属性	• 添加自定义属性 • 删除自定义属性 • 编辑自定义属性 • 查看自定义属性
	支持管理员	• 添加支持管理员 • 删除支持管理员 • 禁用支持管理员 • 查看支持管理员和显示登录历史
	证书颁发机构	• 添加证书颁发机构 • 删除证书颁发机构
	连接器	• 添加 Connector 日志 • 删除连接器日志 • 查看 Connector • 更新 Connector
	LDAP 管理	• 添加用户/组/OU • 添加服务器 • 浏览服务器 • 删除服务器 • 搜索服务器 • 同步服务器 • 移除用户/组/OU • 查看服务器 此部分中的所有 LDAP 权限需要查看连接器权限。 在您选择其中任何 LDAP 权限时，将在连接器部分中自动选择。
	许可管理	查看许可证
	管理应用程序分发	**更新应用程序分发** 在**管理应用程序分发**下，**更新应用程序分发**权限现在可用于的自定义角色。 默认情况下，具有系统管理角色的用户会自动接收此权限。 应用程序分发页面现在包含**允许空间管理员编辑分发**复选框，该复选框默认为新应用程序版本启用。 分配了自定义角色（具有此新权限）的用户，以及具有应用程序管理角色（没有系统管理访问

角色类型	权限类别	细化权限
		权限）的用户，可以修改此设置。 对于每个应用程序版本，“锁定应用程序分发”设置的可用性将显示在分发页面上，并且现在审计跟踪中会捕获所有缩减范围尝试。
用户		
	用户管理操作	• 查看用户 • 更新用户 • 向用户发送消息 • 将角色附加/分配到用户 • 创建用户 • 删除用户 • 邀请用户 • 查看用户注册 PIN
	分配自定义用户属性	• 删除属性 • 查看属性 • 添加/编辑自定义属性
	用户组	• 查看用户组 • 编辑用户组 • 将角色附加/分配到用户组 • 创建用户组 • 删除用户组
	报告管理	• 创建报告 • 编辑报告 • 运行报告 • 删除报告记录 • 查看报告 • 删除报告 • 下载报告记录
设备中的指示，确定将哪些隐私配置应用到希望的设备上		
	批量注册	• 创建批量注册 • 更新批量注册

角色类型	权限类别	细化权限
空间特定角色		• 将用户分配至批量注册 • 查看批量注册 • 删除批量注册
设备中的指示，确定将哪些隐私配置应用到希望的设备上		
	设备操作	• 将设备分配到用户 • 清除设备激活锁定 • 删除设备 • 禁用设备丢失模式 • 启用设备丢失模式 • 设备强制签入 • 锁定设备 • 解锁设备 • 设备强制注销 • 重新安装设备系统应用 • 重新启动设备 • 计划 iOS 设备更新 • 放弃设备所有权 • 停用设备 • 取消停用设备 • 关闭设备 • 查看设备 • 擦除设备 • 取消擦除设备 • 更新设备操作系统版本 • 通过上传进行批量分配 • 开始 TeamViewer 会话 • 进入自助服务终端模式 • 推出单应用模式
	分配自定	• 添加/编辑设备自定义属性

角色类型	权限类别	细化权限
	义设备属性	• 删除设备自定义属性 • 查看设备自定义属性 此部分中的所有分配自定义设备属性权限需要设备读取权限。 在您选择其中任何分配自定义设备属性权限时，将在设备操作部分中自动选择。
	设备配置	• 排除配置文件 • 推送配置文件 • 推送已排除配置文件 • 出错时重试安装
	设备组	• 添加设备组 • 删除设备组 • 编辑设备组 • 查看设备组
	批量注册	• 创建批量注册 • 更新批量注册 • 将用户分配至批量注册 • 查看批量注册 • 删除批量注册
	应用库存	• 查看应用库存
配置		
	配置	• 查看/导出配置 • 编辑/设置配置优先级 • 添加/克隆配置 • 删除配置
策略		
	策略	• 查看策略 • 编辑/设置策略优先级 • 添加/克隆策略 • 删除策略

要编辑角色，转到管理，角色管理页面，并针对角色名称，单击**操作**下方的编辑图标。 用户无法将跨空间角色编辑为空间特定角色；反之亦然。

相关主题：

- 要为用户分配自定义角色，请参阅**分配角色**。
- 有关默认角色的列表，请查看**用户角色**。
- **使用自定义报告**
- **使用计划的报告**

12.1.6. 空间

本部分包含以下主题：

- 空间
- 管理空间
- 空间示例
- 授权设备
- 授权应用程序

12.1.6.1. 空间

许可证： Silver

空间用于将 Unified Endpoint Management (UEM) 系统分离为独立管理的实体，以进行委派管理。 可以创建空间以反映组织层次结构。 Ivanti Neurons for MDM 支持使用称为“默认空间”的中央管理实体和称为“授权空间”的多个下属管理实体进行单级授权。 每个 UEM 系统都使用默认空间创建。

> 对于有权访问 Ivanti Neurons for UEM 和 Ivanti Neurons for MDM 的聚合租户，隐藏“空间”页面和关联选项。

空间允许授权管理以下系统组件。 目前无法授权用户和用户组。

- 设备
- 配置
- 策略
- 设备组
- 应用
- App Catalog
- Apple App 和图书令牌

当管理员在包含至少一个委派空间的租户上登录 Ivanti Neurons for MDM 管理员门户时，将向管理员显示管理员门户登录推广弹出窗口。 如果委派空间已创建，推广弹出窗口将不会在委派空间创建后及在用户登录期间显示。

全局和授权空间管理员的角色

具有默认空间访问权的相应角色的管理员用户被称为全局管理员。 默认空间的访问权限可以是只读或读写访问权。 具有适当管理角色的全局管理员可以创建授权空间并分配授权管理员来管理它们。 可以分配授权管理员来管理一个或多个授权空间。

在设备和应用选项卡的左上角，空间选择器下拉列表会列出指定管理员可以访问的空间。 要查看和管理空间，使用空间下拉列表，以切换到所需的空间。

除了默认空间之外，全局管理员可以查看并控制所有委派空间。 授权管理员只能查看和控制由全局管理员分配给他们的空间。 全局管理员维护对授权空间的中央控制，而授权管理员可以自主管理授权给他们的空间。 该级别的自主性由授权是从默认空间继承还是复制来决定的。

以下是不同的用户角色和他们可以执行的任务：

在授权空间中继承的应用程序

- 授权时的现有评级或评论将被继承，并对默认空间中的用户可见，包括作者用户名。
- 授权管理员无法删除继承的应用程序的评级/评论。
- 授权管理员可以导出继承的应用程序的评级/评论。
- 授权空间中的用户可以将评级/评论添加到继承的应用程序。
- 授权空间中的用户可以查看用户在默认空间中添加的评级/评论，包括作者用户名。

授权空间中的应用程序（添加，不是继承）

- 只要全局管理员可以从**应用程序 > 目录设置 > 评级和评论**中启用或禁用评论。

- 授权空间中的用户可以添加评级/评论。
- 授权管理员可以删除用户在相同授权空间中添加的评论。
- 其他授权空间中的用户，包括默认空间，无法查看用户在每个授权空间中添加的评级或评论。
- 授权管理员可以导出所有用户添加的评论，包括用户名。

默认空间中的授权应用程序

- 全局管理员可以删除用户在授权空间中添加的评级或评论。
- 全局管理员可以导出所有评级或评论，包括用户在授权空间中添加的评级或评论。
- 默认空间中的用户可以查看用户在授权空间中添加的评级或评论，包括用户名。

授权空间的优先级

UEM 系统中的默认空间始终具有最低优先级。 某个授权空间相对于其他授权空间的优先级由全局管理员设置，可随时更改。 在管理员门户的“管理员”选项卡上的“空间”页面中列出了授权空间的排名，从最高优先级到最低优先级。

通过继承或复制授权

授权管理中的一个关键概念是系统组件是从默认空间继承还是复制。

12.1.6.2. 管理空间

空间使您能够为需要管理的设备组指定不同的管理员（授权管理）。 空间管理员可以定义应用于空间内部设备的{{配置}}和{{策略}}。 创建空间后，您可将每个空间分配给相关或适当的管理员。

此空间页面包括：

- 搜索功能可快速定位空间。
- 用于导航大量空间的分页控件。
- 空间优先级控制，用于管理委派的空间顺序。
- 选择和删除多个空格的选项。

> 无法删除默认空间。

- 空间的字母数字顺序排序。
- 空间选择器中最近查看的空间的列表。
- 在设备、配置、策略和内容页面之间进行持久的空间选择，从而减少在页面之间导航时重新选择空间的需求。

> 用户只能查看分配的空间，而不是所有可用空间。 截至目前，此设置仅适用于**设备**、**设备组**、**应用程序**、**应用程序清单**、**内容**、**配置**、**策略**和**证书管理**模块。 在查看任何这些模块时从空间列表中选择的空间将保存为管理员对该模块的首选默认选项。 将会同时为当前登录会话和未来会话保存这些首选项。

您所创建的空间继承默认空间的所有配置。 因此，您之后在默认空间内创建的任何配置将能够应用到其他空间。 但是，对现有配置所做的更改未被继承。

您创建的空间接收的仅是此时存在于默认空间内的策略副本。 因此，您之后在默认空间内创建的任何策略仅可应用到默认空间中。

创建规则，对空间内的设备进行定义。 这些规则可以使用适用的运算符进行过滤，包括“开头为”、“结尾为”、“包含”、“不包含”、“开头不是”、“结尾不是”、“小于”、“大于”、“在以下范围”、“等于”和“不等于”运算符。 规则可以使用 ANY (OR) 或 ALL (AND) 选项嵌套在一起。 可以使用规则末尾显示的文本审查规则的准确性。

在规则生成器中选择“用户组名称”属性后，Ivanti Neurons for MDM 管理门户会显示重复用户组的数量和相应的 GUID 数量，以便识别重复组。 此外，此规则下方的表会显示重复用户组的列表及其详细信息，例如用户组名称、GUID、来源和可分辨名称 (DN)。

规则可以通过以下内容识别设备：

- 已注册 Entra ID
- 支持 APNS
- 备用序列号（仅限 Android - 适用于设备管理员或设备所有人模式中的 Samsung 设备）
- Android 5G 网络切片已启用
- Android 工作托管设备非 GMS 模式 (AOSP) 已启用
- Android 专用设备
- Android 企业版能力
- 带有工作配置文件的 Android 托管设备
- Android SafetyNet 认证类型
- Android Work 已启用

- Android 安全补丁级别（Android 设备）
- 已启用 Android 工作托管设备（设备所有者）
- Android 工作配置文件已启用
- 公司拥有设备上的 Android 工作配置文件已启用
- 防网络钓鱼本机状态
- 防网络钓鱼状态
- 防网络钓鱼 VPN 状态
- 自动化 Device Enrollment 已注册
- 自动化 Device Enrollment 已启用
- Autopilot 已注册
- Azure 客户端状态代码
- Azure 设备合规性报告时间
- Azure 设备合规性状态
- Azure 设备标识符
- 已阻止 Sentry
- 已阻止 Access
- 启动令牌可用
- 批量配置类型（Apple 配置器或无）
- 载波
- 客户端上次签入
- 客户端已注册
- 合规性
- 已阻止合规性操作
- 当前国家/地区名称（从下拉列表中选择国家/地区名称）
- 当前 MCC
- 当前 MNC
- 自定义设备属性
- 自定义 LDAP 属性
- 自定义用户属性
- 数据漫游
- 设备源
- 设备类型
- 设备类型 (Apple)
- 显示名称
- 加密已启用
- 住宅所在国家/地区名称（从下拉列表中选择住宅所在国家/地区名称）
- 家用 MCC

- 家用 MNC
- IMEI
- IMEI2（仅适用于具有双 SIM 端口的 Android 设备，并且设备必须为 Android 8.0 或更高版本）
- 机构恢复密钥已启用
- IP 地址
- 单应用模式
- 上次签入
- 启用丢失模式
- 仅限 MAM
- 制造商
- MTD 激活状态
- 多用户模式
- 操作系统
- 操作系统版本
- 操作系统及版本
- 所有权
- 个人恢复密钥已启用
- 手机号码
- 已隔离
- 恢复锁定已启用
- 漫游
- Secure Apps 状态
- 序列号
- 状态
- 受监控
- 补充内部版本
- 补充操作系统/版本额外信息
- 解锁令牌可用 (iOS)
- User Enrollment 已注册
- 用户组
- 用户名
- 语音漫游
- macOS 个人恢复密钥已托管
- macOS 恢复密钥类型

> 这些规则仅适用于 **Silver** 及以上级别的许可证。

创建空间

步骤

1. 转到**管理员** > **系统** > **空间**。
2. 单击**创建空间**。
3. 输入空间名称。
4. 为空间配置适当的规则和设置。
5. 单击**保存**。

确定空间的优先级

Ivanti Neurons for MDM 按显示顺序评估空间。

步骤

1. 单击**对空间划分优先级**。
2. 选择空间旁边的向上或向下图标以调整其优先级。
3. 单击**保存**。

删除空间

1. 转到**管理员** > **系统** > **空间**。
2. 使用复选框选择一个或多个空间。
3. 单击**删除**。 提示时确认删除

将管理员分配给空间

步骤

1. 转到**用户**。
2. 搜索将要成为管理员的用户。
3. 单击用户链接，显示详细信息。
4. 选择**操作** > **分配角色**。
5. 选择**设备管理**。
6. 在**设备管理**下，为该管理员选择空间。
7. 单击**完成**。

该管理员登录后，只有已分配空间内的设备、配置和策略可见。

复制配置或策略

如果需要复制配置或策略，您可以进行复制，但有一些不同。 您也可以将复制的配置或策略关联到不同的设备组。 可在空间中复制全部策略。 所有配置可在空间中复制，用户提供的身份证书和 Threat Defense 除外。 在默认空间中，以下配置也在空间之间复制：

- iOS 限制
- Web 剪辑
- 证书
- 通行码

- SCEP（iOS 和 Windows）
- 身份证书（动态生成）

- 配置名称或策略类型应在空间中唯一。 配置或策略的所有其他属性可以复制。
- 配置将复制到您和管理员拥有访问权限的所有空间。 您无需成为全局管理员，即可复制配置。

步骤

1. 转至**配置**或**策略**，具体取决于您要克隆的内容。
2. 单击配置或策略的链接以显示详细信息。
3. 单击**克隆**图标。
4. 在弹出窗口中，输入**名称**和**描述（可选）**。
5. 单击**下一步**。
6. 根据您的要求修改配置或策略。
7. 单击**下一步**。
8. 配置分配。
9. 单击**完成**。

有关更多信息，请查看空间示例。

12.1.6.3. 空间示例

本主题提供了管理员如何使用空间的相关示例。

每个位置的管理员

ACME, Inc. 在北美洲和欧洲设有办事处。 由于语言和时区问题，ACME 希望美国的管理员管理北美洲的设备，德国管理员管理欧洲的设备。

为了设置这些空间，ACME 进行了以下更改：

1. 在 Ivanti Neurons for MDM 中为欧洲用户创建了用户组。
2. 在 Ivanti Neurons for MDM 中为北美用户创建用户组。
3. 采用以下规则创建欧洲空间：
4. 用户组 = 欧洲
   采用以下规则创建北美洲空间：
5. 用户组 = 北美洲
   为合适管理员的每个空间分配设备管理角色。

ACME 现在具有以下空间：

- 欧洲
- 北美洲
- 默认

每个位置每个操作系统的管理员

ACME 规定只有 Android 专家管理 Android 设备。 一个 Android 专家已加入北美洲公司，还有一个已加入欧洲公司。 因此，需要两个新的空间。

为了添加空间，ACME 进行了以下更改：

1. 采用以下规则创建欧洲 Android 空间：
2. 用户组 = 欧洲
   OS = Android
   采用以下规则创建北美洲 Android 空间：
3. 用户组 = 北美洲
   OS = Android
   为合适管理员的每个空间分配设备管理角色。

ACME 现在具有以下空间：

- 欧洲 Android
- 北美洲 Android
- 欧洲
- 北美洲
- 默认

管理层管理员

ACME 管理层决定他们需要特殊管理员的特殊服务。 只有最重要的管理层才会出现在此列表中。

为了添加此空间，ACME 进行了以下更改：

1. 采用以下规则创建管理层空间：
2. 用户名 = jdoe@acme.com
   用户名 = gkunz@acme.com
   用户名 = prizzo@acme.com
   用户名 = fvanhoff@acme.com
   将空间移动到**空间**页面中列表的顶部。
3. 否则，Android 设备管理层将拥有错误的管理员。
   为特殊管理员的空间分配设备管理角色。

ACME 现在具有以下空间：

- 管理层
- 欧洲 Android
- 北美洲 Android
- 欧洲
- 北美洲
- 默认

所有其他设备的管理员

ACME 在日本开设新的办事处时，增加的设备将被分配给默认空间的管理员，直至有人创建日本空间。

12.1.6.4. 授权设备

空间用于将您的设备分离成独立管理的实体。 空间成员由您创建的规则决定。 设备委派允许全局管理员对 UEM 系统中的设备进行分区和独立管理。 当授权设备时，可以将这些设备的访问权限分配给授权管理员的一个子集，从而分配管理员职责。

授权的设备可以分组到设备组和应用于它们的不同自定义配置，而不会影响默认空间或其他空间中的设备。

创建授权设备的规则

您为空间定义的规则会决定哪些设备属于该空间。 一个设备仅可归属于一个空间。 与您所创建的空间规则不匹配的设备，自动归属到默认空间。

1. 如果您希望此定义中包含满足任何规则的设备，请选择**任何**。
2. 如果您希望此定义中包含满足所有规则的设备，请选择**所有**。
3. 从下拉列表中选择以下规则类型之一：
   - **自定义 LDAP 属性：**基于 LDAP 属性的规则。
   - **操作系统**：基于设备操作系统的规则。
   - **用户组**：基于设备用户组的规则（于设备管理服务中定义）。
   - **用户名**：基于与设备关联的用户名的规则。
4. 为选定的规则类型定义标准：
   - **自定义 LDAP 属性：**输入在 LDAP 设置中配置的自定义 LDAP 属性名称。
   - **OS**：选择 Android、 iOS、macOS 或 Windows。
   - **用户组**：在下拉列表中显示的用户组中选择一个组。 这些用户组在**用户 > 用户组**中定义。
   - **用户名**：输入一个用户名。
5. 如要为该空间添加其他规则，请单击上一条规则旁边的“+”。
6. 单击**预览**查看将要分配至空间的设备。
7. 如对空间内的设备满意，请单击**保存**。

与空间规则不再匹配的设备，自动移至下一个匹配空间。 如果设备与现有空间规则不匹配，则该设备会移至默认空间。 例如，从用户组中删除用户会导致用户的设备移动到不同空间。 移至不同空间会导致策略和配置的更改。

12.1.6.5. 授权应用程序

应用委派允许全局管理员在 Ivanti Neurons for MDM 中对应用进行分区和独立管理。 全局管理员可以集中提供和分发公共和内部应用程序，同时保持由授权空间提供的分离和控制。

通过集中分发应用程序，全局管理员可以通过应用程序配置以及应用程序的分发规则来预定义应用程序的管理行为。 然后可以将应用程序授权并提供给授权空间的 App Catalog 用。

然后，授权的应用程序将分发给给定授权空间中的用户。 当授权应用程序时，可以将这些应用程序的访问权限分配给授权管理员的一个子集，从而分配管理员职责。

应用程序授权需要先定义一个或多个授权空间。 授权应用程序时，会将它分配给所有空间。 应用程序授权空间分为：

- 默认空间
- 授权空间

将应用程序添加到授权空间

应用程序可以由授权管理员或全局管理员添加到授权空间。 应用程序仅显示在添加的授权空间的应用程序目录中。 如果您将以前授权的应用程序从“默认空间”添加到“授权空间”，则会导致错误。 在这种情况下，必须首先在默认空间中禁用应用程序继承，以便将其添加到授权空间。 有关更多信息，请查看使用配置中的**添加配置**。

应用程序在授权空间中的分发

从默认空间授权应用程序时，其分发规则将被继承。 该应用程序将分发给分配给授权空间的所有设备，这些设备与应用程序的分发规则相匹配。

全局管理员可以委派空间管理员，并为所有设备和自定义分发选项编辑动态生成的身份证书。

> 分发更改仅适用于特定空间。 所有其他空间会继续继承默认空间分发设置。

> Android 应用程序的应用程序审批设置：不支持针对 Android 应用程序的每个空间进行应用程序审批设置。 自定义空间中批准的应用程序将在所有空间中生效。

> 现有 Android 目录应用程序：在已将公共 Android 应用程序添加到默认空间中的租户上，需要取消委派应用程序，然后才能将该公共应用程序添加到其他非默认空间中。

> Android 企业版应用程序只能由租户级别管理员添加，而**不能**由空间级别管理员添加。 托管 Google Play 在组织级别进行配置，而不是按授权空间进行配置。 因此，新的 Android 企业版应用程序只能在默认空间中获得批准。 授权管理员可以在自己的空间内分配和管理已批准的应用程序，但不能从授权空间内批准或添加新的 Android 企业版应用程序。 所有新应用程序必须首先在默认空间中获得批准，然后才能将其分配给相应的组。

有关更多信息，请查看使用配置中的**添加配置**。

12.1.7. 支持管理员

创建一个临时支持管理员，使服务支持小组可使用您的角色和权限登录。 此用户在 7 天后自动过期，您也可以随时解除其访问权限。 创建支持管理员使得支持小组排除问题更加容易。

创建支持管理员

程序

1. 在**支持管理员**页面，单击**添加支持用户**。
2. 单击**创建用户**，进行确认。

执行此步骤会向设备管理服务支持小组发送电子邮件。

> **显示名称**字段会显示“（已禁用）”，直到支持团队成员激活新帐户为止。激活后，显示名称会显示以下格式：

support-[random_ID]-[your_username]@[your_company].com

创建支持管理员后，选择**管理员 > 支持管理员**会直接打开现有支持管理员列表。 因此，如果需要创建更多支持用户，请直接执行以上第二步。

> 新创建的支持管理员账户默认为只读。 自定义角色不会自动分配，从而降低了意外配置变更的风险。 管理员可以根据需要稍后添加角色和权限。

查看用户历史

在**支持管理员**页面中，单击**用户历史**，以查看支持管理员的登录历史。 支持管理员页面中的登录历史数据仅提供过去 90 天的数据。

启用对支持管理员的访问

程序

1. 在**支持管理员**页面中，单击要删除帐号右侧的**删除**链接。
2. 在出现提示后，单击**删除用户**以进行确认。

暂停对支持管理员的访问

在**支持管理员**页面中，单击要暂停帐号右侧的**禁用**链接。

12.1.8. 管理 > 系统使用通知

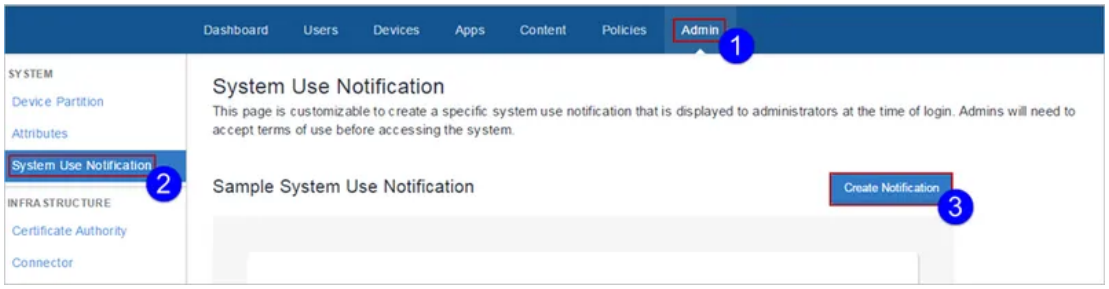
许可证： Silver

使用系统使用通知功能创建在登录时向管理员显示的自定义系统使用通知，并需要管理员在访问系统前接受使用条款。

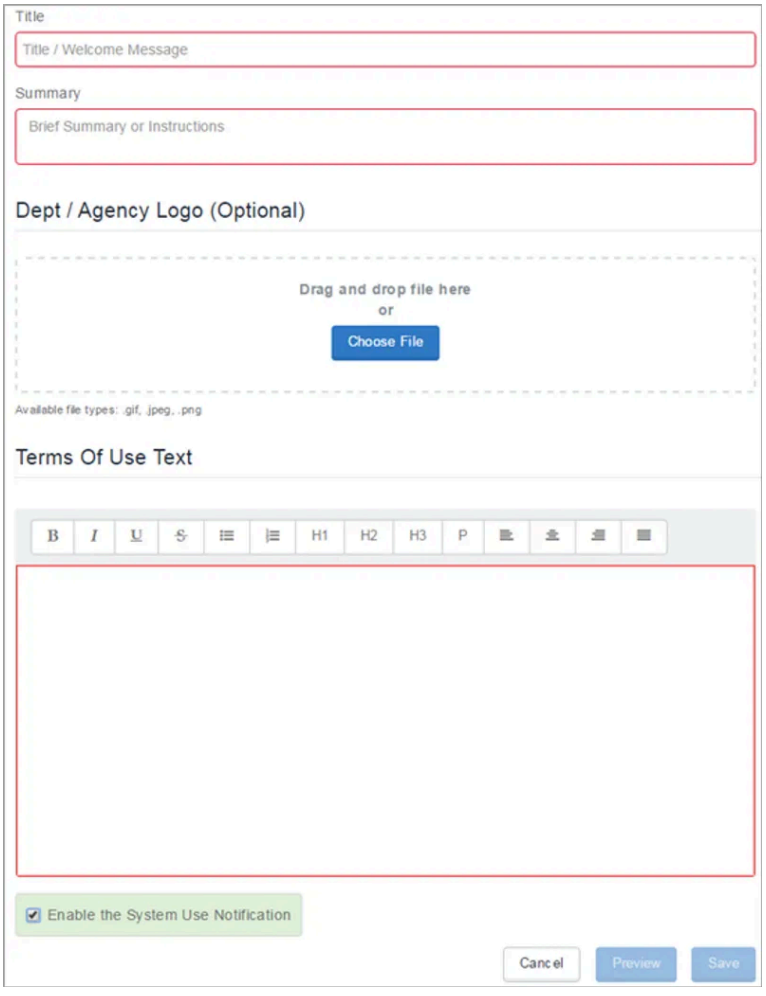
创建系统使用通知

程序

1. 选择**管理 > 系统使用通知**。
2. 单击**创建通知**。



将显示"系统使用通知详细信息"页面。



在**标题**字段中输入标题。

4. 在**摘要**字段中输入摘要或指示。
5. 如果需要，选择徽标。
6. 在**使用条款文本**字段中，输入使用条款文本。 这是管理员在登录时需要接受的文本。
7. 请在**启用系统使用通知**复选框中勾选复选标记，以启用通知。
8. 单击**预览**，以调用系统使用通知预览。
9. 在您对系统使用通知满意时，单击**保存**。

12.2. 基础设施

本部分包含以下主题：

- 访问
- 应用程序列表
- 导出审计跟踪
- 证书管理
- 适用于外部证书授权机构的 SCEP 配置
- 派生凭据提供商
- 连接器
- 使用 Connector 的 httpproxy 命令
- Help@Work
- 基础设施身份
- 配置 LDAP 服务器
- 卫士
- 在 Ivanti Neurons for MDM 和 SCEP 服务器之间启用 Kerberos 身份验证

12.2.1. 访问

适用于：iOS 和 Android 设备。

Access 会保障企业数据的安全，同时在任何设备或应用程序上启用无缝和高效用户体验。 Access 可构建数据边界，这会阻止用户在不安全的设备、应用或云服务上访问企业云服务。

最新文档

访问产品文档并点击 Access，可了解有关 Access 以及如何设置 Access 的更多信息。 选择适合您的 Access 版本的文档。

12.2.2. 应用程序列表

许可证：Silver

您可以创建所需、已加入允许列表和已加入阻止列表应用的列表，以便与 允许的应用策略 一起使用，使用这些列表帮助指定如果设备的已安装应用不符合应用列表隐含的要求应采取什么措施。 创建后无法编辑应用列表，因为允许的应用策略中可以引用应用列表。 同样，您不能删除任何允许的应用程序策略引用的应用程序列表。

创建应用列表

程序

1. 点击**管理员 > 基础设施 > 应用程序列表**。
2. 单击**创建新列表**。
3. 在**应用程序列表名称**框中，输入列表的名称。
4. 选择列表的类型：**白名单**、**黑名单**或**必需**。
5. 在**添加应用程序**部分下，选择应用程序类型：**App Store**、**OS X store**、**Google Play** 或**应用程序目录**。
6. 输入搜索条件来缩小选择范围。
7. 使用复选框选择应用程序。 您可以使用多个搜索并启用多个复选框。
8. 点击**查看应用程序**选项卡，查看您迄今为止选择的应用程序列表。
   单击**保存**。

现在，您可以在配置允许的应用策略时使用此列表。

如果您未看到**应用列表**页面，这可能是您没有所需权限。 您需要以下角色之一：

- 系统管理
- 系统只读

12.2.3. 导出审计跟踪

审计跟踪导出功能用于将所有审计跟踪信息导出并上传到特定的服务器位置。 服务器应该可以从默认端口访问。 用户可以配置审计跟踪导出设置，以便将审计跟踪的存档每天自动上传到特定位置。

> 基于 Linux 和基于 Windows 的 SFTP 服务器支持审核线索导出。

若要配置导出审计跟踪的设置：

1. 选择**管理员 > 基础设施 > 审计跟踪**。 将显示**审计跟踪**页面。
2. 在**审计跟踪**页面中，单击**打开**，启用审计跟踪导出功能。
3. 在**导出**部分，更新以下字段：

功能	描述
导出格式	选择以下审计跟踪数据应导出的任何格式： • **JSON** • **CEF**（常见事件格式） CEF 日志消息包含以下默认值： ◦ 版本：CEF 格式版本号。 版本 25 是当前支持的版本。 ◦ 设备供应商：Ivanti Inc ◦ 设备产品：Ivanti Neurons for MDM ◦ 设备版本：在事件生成时的最新 Ivanti Neurons for MDM 版本。 ◦ 设备事件类 ID：每个跟踪的实体 ID ◦ 名称：每个跟踪的实体名称和操作。 示例：推广分发配置设置创建。 ◦ 严重性：指定事件的重要性。 示例：低。 CEF 日志消息也包含作为以下键值对集合的扩展字段： ◦ CS1 和 CS1Label：审计跟踪元数据，例如 createdAt、entityType、entityName 和 actionType。 ◦ CS2 & CS2Label：执行者信息。 ◦ CS3 和 CS3Label：操作前的状态。 ◦ CS4 和 CS4Label：操作后的状态。 在 CEF 导出中，如果任何字段（例如：CS3 或 CS4 键）超过指定限制，将使用文本"此键的值超过已映射字典键允许的长度"替换实际值。
服务器	将服务器名称输入到导出审计跟踪。
用户	输入用户名，登录服务器。
密码	输入服务器登录密码。
服务器路径	输入服务器的路径，并确保提供的路径存在于服务器上。 示例：/Users/Test/Export。
密钥交换算法	选择用于导出传出 SFTP 配置的审计日志的密钥交换算法列表。 默认选择以下密钥交换算法： • **diffie-hellman-group-exchange-sha1** • **diffie-hellman-group14-sha1** • **curve25519-sha256** • **diffie-hellman-group-exchange-sha256**（默认选中）
密码	选择用于导出传出 SFTP 配置的审计日志的加密密码列表。 默认情况下，选择以下加密密码： • **aes128-ctr** • **aes192-ctr** • **aes256-ctr**（默认选中）
HMAC	选择用于导出传出 SFTP 配置的审计日志的 HMAC 算法列表。 • **hmac-sha1（默认选择）** • **hmac-sha2-256**

功能	描述
	• **hmac-sha2-512**

如果这些字段已经配置，上述字段将处于只读模式。 若要编辑已配置的字段，您应单击**编辑**按钮。 如果管理员已配置 SFTP 导出，所有密钥算法将在升级后选中。

单击**测试连接并保存**，测试服务器连接并保存审计跟踪导出配置。

存档的审计跟踪文件 .zip 文件中能够以 JSON 格式使用。

在保存审核线索导出设置前，请验证所有字段中的配置设置。 如果输入的任何字段值无效，将显示一则错误消息。

在空间中启用设备注册和取消注册的审计跟踪

启用后，系统会记录空间之间的设备移动情况，包括设备注册、设备删除以及空间更新或删除触发的事件。 空间管理员可以识别受影响的设备，按空间和活动类型筛选日志，并将审计记录导出到 CSV。

12.2.4. 证书管理

许可证： Silver

使用证书验证是确保您的移动设备安全的有效方法。 证书比密码更安全，且它们允许您使用单一凭据保护 VPN、无线网络、电子邮件等。 如果您的组织拥有对外部证书颁发机构的访问权，您可使用 Connector 对其进行访问。 如果您的组织无权访问证书颁发机构，则可以将 Ivanti Neurons for MDM 用作证书颁发机构。 您还可以将其用作其他证书颁发机构的中间证书颁发机构。 Ivanti Neurons for MDM 生成的证书称为自签名证书。

- 创建身份证书时，不推荐使用 SHA-1 证书。 您可以选择其他算法。 更新证书时，如果旧的证书使用 SHA-1，则可以使用相同的 SHA-1 算法。 如果早期证书使用 SHA-1 以上的算法，将不允许还原为 SHA-1。
- 在配置本地或外部证书颁发机构期间，选择**缓存** Ivanti Neurons for MDM **上的身份**选项，以将证书与 Ivanti Neurons for MDM 服务一起存储。 清除缓存，以在每次需要时生成证书。
- 将隐式重新颁发证书。
- 为了提高系统效率，管理员创建的配置的证书使用先进先出 (FIFO) 队列离线生成。 在离线生成配置期间，配置状态将在**设备详细信息**页面**配置**选项卡的**状态**列中显示为**等待证书生成**。 生成证书后，配置会移动到**等待安装**状态，并通过自动强制签入，与证书一起推送到设备。
- 在设备停用和擦除时，以及在证书重新生成时，所有证书颁发机构的证书（包含 DigiCert PKI 平台或 GlobalSign 外部证书颁发机构签名的证书）将会撤销。

作为管理员，您可为智能卡登录和自定义对象 ID (OID) 生成 Ivanti Neurons for MDM 证书。 您可为下列身份验证选项生成证书：

  - 客户端身份验证 - 默认启用
  - IPSEC – 可选，管理员可启用
  - 智能卡登录 - 可选，管理员可启用
  - 自定义 OID - 可选，管理员可启用

> 此功能仅适用于下列证书颁发机构：
>
> - 本地证书颁发机构
> - 中间证书颁发机构
> - 外部证书颁发机构 - 在 NDES 服务器中配置 CA 模板的应用策略，支持 IPSEC、智能卡登录和自定义 OID

> 在设备管理、App Station 或其他非 Android Enterprise 模式下，使用 Samsung API 的 Samsung 设备不支持证书管理。 建议根据 Samsung 建议验证到 Android Keystore 的过渡。

有关详细信息，请参阅证书配置。

连接至本地 SCEP 证书颁发机构

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 安装和配置 Connector（**管理员 > Connector**）。 有关详细信息，请参阅 连接器。
3. 前往**管理员** > **基础设施** > **证书管理**。
4. 点击**证书颁发机构**部分下的**添加**。

5. 选择**添加本地 SCEP 证书颁发机构**并点击**继续**：
6. 输入标识配置的名称。
7. 选择以下证书颁发机构类型之一：
    - Microsoft
    - EJBCA
    - 通用 SCEP 服务器
      多数具有静态质询密码的 SCEP 服务器均可使用“通用 SCEP 服务器”选项。

填写显示的表格。

9. 单击**完成**。

创建外部证书颁发机构

如果您想要使用第三方证书颁发机构，选择此选项。

步骤

1. 在**证书管理**页面上，点击**证书颁发机构**部分下方的**添加**。
2. 在“添加证书颁发机构”页面上，在“创建外部证书颁发机构”中，单击**继续**。
3. 选择 GlobalSign 或 DigiCert PKI 平台作为外部证书颁发机构。
4. 填写显示的表单上的剩余字段。
5. 单击**完成**。

查看外部证书颁发机构 的证书

您可以查看证书的详细信息，并上传此证书颁发机构的中间/替代根证书，以替换现有存储的副本。

步骤

1. 在**证书管理**页面的**证书颁发机构**下方，单击外部证书颁发机构旁边的**操作**，并单击**查看证书**。 将显示**查看证书**窗口。
2. 在**查看证书**窗口中，点击**上传证书**。 将显示**上传证书：外部 CA** 窗口。
3. 单击**选择文件**，以选择要上传的证书。
4. 单击**完成**。

创建中间证书颁发机构

- 如果您需要证书，则生成 CSR 并将其提交给签名机构。 一旦您从签名机构收到证书，就请上传该证书。
- 如果您已拥有所需证书，请将其上传。

生成 CSR（证书签名请求）

步骤

1. 在**证书管理**页面的**证书颁发机构**部分下方，单击**添加**
2. 在“添加证书颁发机构”部分中，在“创建中间证书颁发机构”下方，单击**生成 CSR**。
3. 填写显示的表格。
4. 单击**生成**。

5. 将“BEGIN CERTIFICATE REQUEST”和“END CERTIFICATE REQUEST”之间的内容复制到文本文档中。
6. 将文本文件上传到认证机构。
7. 单击**完成**。

上传签名证书

从认证机构收到签名的证书后，便可上传签名的证书。

步骤

1. 在**证书管理**页面的**证书颁发机构**部分下方，查找您生成 CSR 的条目。
2. 在部分下方，选择**操作 > 上传新签名证书**。
3. 单击**选择文件**。
4. 选择新签名证书。
5. 单击**完成**。

上传现有证书

本主题介绍了如何上传签名的证书。

步骤

1. 在**证书管理**页面的**证书颁发机构**部分下方，单击**添加**。
2. 在“添加证书颁发机构”部分中，在“创建中间证书颁发机构”下方，单击**上传现有身份**。
3. 在**名称**字段中，为该证书输入一个可同其他证书区分开的名称。
4. 单击**上传**。
5. 选择证书。
6. 输入证书密码。
7. 单击**上传**。

查看中间证书颁发机构的证书

您可以查看证书的详细信息并获取证书颁发机构的 CRL（证书吊销列表）URL。

步骤

1. 在**证书颁发机构**部分中，单击证书颁发机构旁边的**操作**，并单击**查看证书**。 将显示**查看证书**窗口。
2. 在**查看证书**窗口中，您可以在 **CRL URL** 字段中查看 URL。
3. 单击**复制**将 URL 复制到剪贴板并粘贴到另一个应用程序中。 该 URL 可用于配置 Office 365 接受证书颁发机构颁发的证书。

创建独立的证书颁发机构

如果要创建完全独立的（本地自签名）新证书颁发机构，请选择此选项。

步骤

1. 在**证书管理**页面的**证书颁发机构**部分下方，单击**添加**。
2. 在“添加证书颁发机构”页面上，在“创建独立证书颁发机构”中，单击**继续**。

3. 填写显示的表格。
4. 单击**生成**。

独立证书颁发机构过期通知

如果证书到期日期小于 30 天，则独立（本地）证书颁发机构到期信息现在作为工具提示显示在**到期日期**列下。

如果到期日期少于 365 天，除了发送的通知外，还可以在**仪表板** > **通知**下查看此信息。 选择**到期**作为筛选器。

配置独立证书颁发机构颁发的证书的过期时间

您可以配置独立（本地）证书颁发机构的到期期限。

步骤

1. 在**证书管理**页面的**证书颁发机构**部分下方，单击独立证书颁发机构旁边的**操作**。
2. 单击**编辑**。
   显示**编辑证书颁发机构**窗口。
3. 在客户端证书模板部分的**证书生存期**字段中，以天为单位输入新的到期期限。
4. 单击**保存**。

在本地证书颁发机构颁发的证书即将到期或已到期时，您将收到通知和电子邮件（如果启用，可选）。

- 证书到期日通知 - 在证书到期时段期间的预定间隔生成通知。 第一个通知将在到期前 365 天推送；之后在到期前 180 天、60 天、45 天和 7 天分别推送其他通知。 通过导航到**管理员 > 证书管理 > 操作 > 上传新的签名证书**，您将收到此通知，直到替换证书。
- 关于过期证书的通知 - 您将在证书过期时收到通知。 您将需要更换证书，才可以恢复正常服务。
- 在上传新有效证书时的通知 - 通知将在上传新签名证书时发送。

查看独立证书颁发机构的证书

可以查看证书的详细信息并获取本地证书颁发机构的 CRL（证书吊销列表）URL。

步骤

1. 在**证书管理**页面的**证书颁发机构**部分下方，点击本地证书颁发机构旁边的**操作**，并点击**查看证书**。 将显示**查看证书**窗口。
2. 在**查看证书**窗口中，您可以在 **CRL URL** 字段中查看 URL。
3. 单击**复制**将 URL 复制到剪贴板并粘贴到另一个应用程序中。 该 URL 可用于配置 Office 365 接受本地证书颁发机构颁发的证书。

查看证书颁发机构的 CRL 生存时间

您可以查看并编辑本地或中间证书颁发机构的 CRL 生存时间。

步骤

1. 在**证书管理**页面的**证书颁发机构**部分下方，点击本地证书颁发机构旁边的**操作**，然后点击**编辑**。 显示**编辑证书颁发机构**窗口。
2. 在**编辑证书颁发机构**窗口中，您可以查看 CRL 生存时间值。 最小默认值是 24 小时。 可输入的最大值是 10950 小时。
3. 编辑 CRL 生存时间值，并单击**保存**。

创建云证书颁发机构

如果您想要使用云证书颁发机构，选择此选项。

步骤

1. 前往**管理员** > **基础设施** > **证书管理**。
2. 在**证书管理**页面的**证书颁发机构**部分下，点击**添加**。
3. 在**添加证书颁发机构**页面的**连接到公共信任的云证书颁发机构**下，点击**继续**。
4. 在**名称**框中输入名称。
5. 从以下选项中选择云证书颁发机构：
   - **Atos IDnomic CMS**
   - **DigiCert One PKI 平台**
   - **DigiCert PKI 平台**
   - **Entrust**
   - **GlobalSign**
6. 输入基本 URL 并上传证书数据。
7. 单击**完成**。

对证书使用高级搜索

您可以使用高级搜索选项，以按照规则搜索已签发证书，从而识别和查看满足特定条件的设备。 这些规则可以使用适用的运算符进行构建，包括"开头为"、"结尾为"、"包含"、"不包含"、"开头不是"、"结尾不是"、"小于"、"大于"、"在以下范围"、"等于"和"不等于"运算符。 使用任意（或）或全部（且）选项，规则选项可以全部进行嵌套。 符合规则的已颁发证书会显示在该部分下方。 从 Ivanti Neurons for MDM 76 版开始，所有证书管理模板的运算符必须是标准运算符。 在此版本中，以下模板的运算符将标准化：

- 管理 > 证书管理 > 签发证书 > 高级搜索

对已颁发的证书执行高级搜索

步骤

1. 在**证书管理**页面的**已签发证书**部分中，单击**高级搜索**链接。
2. 如果用户需要匹配其中至少一个规则，单击**任意**；或者，如果证书需要匹配所有规则，单击**全部**。
3. 对于以下属性，创建定义搜索条件的规则：
   - **CA**
   - **配置名称**
   - **到期**
   - **私钥**
   - **操作系统**
   - **序列号**
   - **状态**
   - **使用类型**
   - **用户**
4. （可选）单击 +，以创建其他规则（如果需要）。
5. （可选）单击**保存**，以保存查询。
6. 单击**搜索**。 页面会显示匹配搜索条件的用户列表。

对用户提供的证书执行高级搜索

步骤

1. 在**证书管理**页面的**用户提供的证书**部分下，点击**高级搜索**链接。
2. 如果用户需要匹配其中至少一个规则，单击**任意**；或者，如果证书需要匹配所有规则，单击**全部**。
3. 对于以下属性，创建定义搜索条件的规则：
   - **证书名称**
   - **过期日期**
   - **颁发者**
   - **上传于**
4. （可选）单击 +，以创建其他规则（如果需要）。
5. （可选）单击**保存**，以保存查询。
6. 单击**搜索**。 页面会显示匹配搜索条件的用户列表。

加载已签发证书的搜索查询

查看已保存的搜索查询的列表。

步骤

1. 在**证书管理**页面的**已签发证书**部分中，单击**高级搜索**链接。
2. 单击“文件夹”图标。 显示**高级搜索**窗口。 **加载查询**部分会显示已创建搜索查询的列表。 此部分会显示以下详细信息：
   - **查询名称** - 已加载查询的名称。
   - **查询内容** - 根据定义搜索查询的规则，显示内容。
   - **操作** - 选择对查询执行的操作。
3. 单击**操作**列中的**加载查询**，以查看匹配在已加载查询中定义的条件的已签发证书列表。
   要删除已加载查询，单击删除图标。

> 单击**导出到 CSV**，将搜索结果报告内容下载到 CSV 文件，以便未来参考或分析。

查看已颁发证书的有效期

在**已颁发证书**部分下方，在**过期（天数）**列中，您可以查看证书即将过期的剩余天数（如果在未来 30 天内过期）。 如果证书在过去 30 天内已过期，证书的**过期（以天数为单位）**列会显示从过期之日起的天数。

有关更多信息，请查看[外部证书颁发机构的 SCEP 配置]。

导出到 CSV

可以将证书导出为 CSV 文件，以供后续参考或分析。

程序

1. 在**证书管理**页面，前往以下选项卡之一。
   - **证书颁发机构**
   - **已颁发的证书**

- **用户提供的证书**

2. 点击**导出为 CSV**。
3. 点击**下载**。
4. （可选）点击**删除**可以删除报告。

12.2.5. 适用于外部证书授权机构的 SCEP 配置

此功能支持在 Windows 10 设备上使用外部证书颁发机构的简单证书注册协议 (SCEP) 配置。

> 此配置支持带自定义分发选项的委派。 有关详细信息，请参阅使用配置中的*分发配置*主题。

设置外部证书颁发机构

您必须先设置外部 CA。 如果您拥有外部 CA，则可以跳到下一个部分。

1. 转到**管理员 > 基础设施 > 证书管理**。
2. 点击 **+ 添加**。
3. 输入证书颁发机构的名称。
4. 使用下拉菜单选择 Microsoft 作为**证书颁发机构类型**。
5. 输入 **SCEP URL**。
6. 输入**用户名**和**密码**。
7. 输入**质询 URL**。
8. 单击**保存**。

SCEP 配置

现在您可以继续进行 SCEP 配置。

1. 转到**配置 > + 添加**。
2. 选择 Windows 图标。
3. 选择**身份证书**，以转到**创建身份证书配置**页面。
4. 输入配置的名称。
5. 从**证书分发**下拉菜单的 SCEP 配置列表中，选择**Windows 配置**。
6. 选择外部 CA。
7. 输入证书分配详细信息。
    - 输入主题。 例如：CN=$
    - 从**重试**下拉菜单中，选择重试次数。
    - 从**重试延迟**下拉菜单中，选择每次输入前等待的秒数。
    - 从**密钥长度**下拉菜单中，选择密钥大小。
    - 选择至少一个证书使用选项。
    - 在**验证**字段和下拉菜单中，输入时间长度。
    - 输入 CA 拇指指纹。
    - 转到 SCEP 质询 URL，复制 CA 指纹并将其粘贴到此处，或者点击**从证书创建**... 从可以创建 CA 指纹的位置上传证书。从**哈希算法系列**选项中，至少选择哈希算法。
8. 单击**下一步**。

12.2.6. 派生凭据提供商

在派生凭据提供商页面中，您可以查看用于证书分发的派生凭据提供商列表。 您可以指定应将设置为默认值的派生凭据提供商，并添加您使用的其他自定义派生凭据提供商。

要将派生凭据提供商设置为默认值：

1. 转到**管理员 > 派生凭据提供商**。页面会列出以下派生凭据提供商。
    - **Entrust**
    - **Intercede**
    - **Purebred**
2. 对于要设置为默认项的提供商，请点击**操作**列中的**设置为默认项**。 设置完成后，复选标记图标将显示在该提供程序的**默认提供程序**列下，表明它是默认的凭据提供程序。

要添加自定义派生凭据提供商：

1. 转到**管理员 > 派生凭据提供商**。
2. 单击 **+添加**。
3. 在**名称**列下方的文本字段中，键入派生凭据提供商的名称。
4. 单击**保存**。
   在添加时，此自定义派生凭据提供商作为选项可以在**品牌**字段中选择，并在**身份证书**配置中配置派生凭据分发。

单击**操作**列下方的**删除**，以删除派生凭据提供商。

> 如果您将派生凭据提供商设置为默认值，将无法删除。

12.2.7. 连接器

许可证： Silver

Ivanti Neurons for MDM Connector 提供从 Ivanti Neurons for MDM 服务访问企业资源的权限，例如 LDAP 服务器或证书颁发机构 (CA)。为每个想要访问的资源设置一个 Connector。

如果您使用在 Amazon Web Services (AWS) 中托管的 Microsoft Active Directory 或 LDAP 服务器，您可以在 AWS 中托管 Ivanti Neurons for MDM Connector。 不需要本地 Connector。

Connector 会自动更新到软件的最新版本。

如需最新 Ivanti Neurons for MDM Connector 安装指南，请访问 **https://help.ivanti.com/#106** 并搜索“Connector”。

Connector 托管选项

您可以将 Ivanti Neurons for MDM Connector 本地托管在数据中心或 Amazon Web Services (AWS) 中：

- 如果您在 AWS 中使用 AWS 托管的 Microsoft Active Directory 或自我托管的 Microsoft Active Directory，则在 AWS 中托管 Connector。 在这种情况下，您不需要本地 Connector。
- 要访问本地资源（如 LDAP 服务器或 CA），请在本地部署 Connector。

在 AWS 中托管 Connector

客户可以在 AWS 中托管 Connector，以用于以下 AWS 托管的 Microsoft Active Directory 选项：

- AWS Directory Service for Microsoft Active Directory
- Amazon VPC 中的客户托管的 Microsoft Active Directory

有关 AWS Directory Service for Microsoft Active Directory 的更多信息，请查看**https://aws.amazon.com/directoryservice**。 有关在 Amazon VPC 中托管 Microsoft Windows Server 和 Microsoft Active Directory 的信息，请参阅 AWS 文档。 Ivanti Neurons for MDM Connector 支持 Windows Server 2012、2012 R2、2015。

在 AWS 中设置 Ivanti Neurons for MDM Connector AMI

要设置 Ivanti Neurons for MDM Connector AMI：

1. 使用管理员凭据登录 AWS。
2. 在 AWS 服务页面上，选择**计算**下方的 **EC2**。
3. 展开**图像**并选择左侧窗格中的 **AMI**。
4. 从右侧窗格中的下拉列表中选择**公共图像**。
5. 使用“mobileiron-kocab”等关键字，搜索 Ivanti Neurons for MDM Connector。
6. 从列表选择连接器的最新版本，并单击**启动**。
7. 请访问 https://help.ivanti.com/mi/help/en_us/cld/*<version>*/inst/default.htm，遵循 *Ivanti Neurons for MDM Connector 安装指南*的“在 AWS 中部署 Ivanti Neurons for MDM Connector”部分中与安装 Connector 相关的说明，其中*版本*是正在安装的 Ivanti Neurons for MDM Connector 的版本。例如，对于 74 版本的 Ivanti Neurons for MDM Connector，请访问 https://help.ivanti.com/mi/help/en_us/cld/**74**/inst/default.htm 查找指南。

现场托管 Connector

要在数据中心本地托管 Ivanti Neurons for MDM Connector，请点击**下载 Connector**，然后下载和设置 Ivanti Neurons for MDM Connector。 提取下载的程序包的内容，并按照程序包中包含的“Ivanti Neurons for MDM Connector 安装指南”中的设置说明进行操作。

访问 Connector 日志

您可以从 kocab 服务访问 Connector 日志，以帮助对 Connector 相关问题进行故障排除。 您必须具有系统管理员或系统只读角色。

1. 转到**管理员 > Connector**，以查看“Connector”页面。
   Connector 界面显示 Connector 状态（已启用或已禁用）、Connector 名称、连接（已连接或未连接）、版本号、日志级别、操作（禁用或移除 Connector）。
2. 使用**日志级别**下拉菜单，以选择级别。
   可用日志级别会按照从最低日志级别到最高日志级别的顺序显示在下拉菜单中：
   - 错误
   - 警告
   - 信息
   - 调试
   - 跟踪

信息级别是默认日志级别设置。 如果选择其他日志记录级别，将显示旋转同步图标，并表示正在您选择的日志记录级别上收集信息。 日志级别将在 1 小时后重置为信息级别。 跟踪级别是最高的日志级别设置。 使用此级别，以在所有其他级别上收集所有消息。 同步图标将在请求持续时间内显示。

3. 如果需要，将鼠标悬停在同步图标上，以查看取消图标。 单击取消图标，以取消日志级别更改。
4. 将鼠标悬停在请求图标上，以显示请求信息。 单击请求图标，以从 .zip 文件中的当前日志文件夹请求文件。
   在做出请求时，日志文件已添加到 .zip 文件。 在做出新请求时，上一个请求中的 .zip 文件会删除。
5. 如果需要，将鼠标悬停在请求图标上，该图标将变为取消图标。 单击取消图标，以停止请求。
   如果请求在完成前取消，系统将不显示下载图标，因为上一个日志 .zip 文件已从服务器中删除。 Connector 上的原始日志文件仍可用于请求。
6. 单击下载图标，以下载包含在最新请求期间收集日志文件的日志 .zip 文件。
   日志文件名的格式如下：kocab.log。 下载的 zip 文件名称包含服务器名称、连接版本和时间戳（包含日、月、年）以及如下格式的日期时间：<Connector_Hostname>_<Connector_Version>_<TimeStamp>.zip。 已归档 .zip 文件名的格式如下：kocab.yyyy-mm-dd.0.log.gz。
7. 或者，使用操作**下拉**菜单，以禁用或移除 Connector。

如果您未看到 **Connector** 页面，这可能是您没有所需权限。 您需要以下角色之一：

- 系统管理
- 系统只读

有关更多信息，请查看**将 httproxy 命令用于 Connector**。

12.2.8. 使用 Connector 的 httpproxy 命令

新 klish shell 命令已创建，这有助于编辑 Ivanti Neurons for MDM 安装的 Connector 配置。 使用此命令更改登录信息和其他参数，以配置 Connector。

httpproxy 命令在此版本中已可使用，但存在这些要求。

- klish 外壳

要配置 Connector

1. 登录 klish shell。
2. 输入“？”获取可用 klish shell 命令列表。
3. 输入 **httpproxy**，显示这些参数当前的值：
    1. 已启用
    2. 方案
    3. 服务器
    4. 验证类型
    5. 用户名
    6. 密码
4. 输入 **httpproxy ?**，以查看可与 httpproxy 一同使用的命令列表。
    1. authtype - 将 http 代理的身份验证类型设置为 NONE、BASIC 或 NTLM
    2. 禁用 - 禁用 http 代理
    3. 启用 - 启用 http 代理
    4. 主机 - 设置 http 代理的主机 - 必须为 FQDN 或 IP，http 或 https 均可
    5. 密码 - 设置 http 代理的身份验证密码
    6. 端口 - 设置 http 代理的端口
    7. 方案 - 设置 http 代理的方案 - 必须为 http 或 https
    8. 显示 - 显示当前 http 代理设置
    9. 用户名 - 设置 http 代理的身份验证用户名
5. 使用以上命令列表设置您的 Connector 实例。

12.2.9. Help@Work

许可证：Platinum

支持对象：由 Ivanti Neurons for MDM 支持的 Android 和 iOS 设备

使用 Help@Work for Android/iOS，以为 Android 和 iOS 设备的用户提供远程帮助。 Help@Work for Android/iOS 取决于 TeamViewer QuickSupport 应用。 您将需要 TeamViewer 账号，以使用 Help@Work for Android/iOS。 如果您没有账号，则访问 teamviewer.com，以了解详细信息。

通过允许用户单击按钮寻求帮助并与帮助台客服人员共享屏幕，Help@Work 可以改变 iOS 11.0+ 和 Android 设备的帮助台体验。 用户不用再浪费宝贵时间试图描述问题，而 IT 员工在对设备问题进行故障排除时可以更加高效。 MAM-Only iOS 设备不支持此功能。

> 在自助服务终端模式中，Android 设备所有者设备支持 TeamViewer。

> 如果应用退出或设备重新启动，TeamViewer 启动命令将不复存在。

> 在 Android 设备中，如果未安装 Teamviewer QuickSupport 应用，将提示用户下载该应用。 在 iOS 设备中，应用需要通过 App Catalog 推送，或如果已安装到设备，必须将其转换为托管应用。

> Teamviewer QuickSupport 应用应置于前台，以便会话应用于应用。 无人参与模式需要 TeamViewer Host 应用。

> 对于管理员安装的桌面应用版本，应兼容在客户端设备中安装的 Quicksupport 版本，以支持远程会话。

设置 Help@Work for Android/iOS

以下是一次性设置步骤，适用于推广和分发 Help@Work for Android/iOS：

1. 转到**管理员**选项卡。
2. 在基础设施中，单击 **Help@Work**。
3. **Help@Work** 需要 TeamViewer。 在“激活 TeamViewer”部分中，点击**立即激活**按钮，激活 **TeamViewer 有人参与**或 **TeamViewer 无人参与（仅限 Android）**选项。
4. 查看 TeamViewer 许可协议，然后点击**同意**以继续。 现在，您的 Enterprise 许可证已激活。 这将向 TeamViewer 识别 Ivanti 客户，以便授予访问权限。

> 激活 TeamViewer 后，**移除激活**选项将变为可用。 点击**激活 TeamViewer** 部分下方显示的**移除激活**后，屏幕上将显示**确认移除激活**窗口。 点击**移除激活**可移除 TeamViewer 激活，随后将从所有支持的设备上移除 Help@Work 功能。 但是，以后可以使用现有帐户或其他帐户激活 TeamViewer。

> 如果您想在无人参与模式下删除 **TeamViewer** 帐户，必须取消配置启用了无人参与模式的关联设备。 要取消配置关联设备，必须从关联设备取消分发 **TeamViewer** 应用程序，并执行强制签入。 确保已从所有设备删除 TeamViewer 应用程序，然后从管理员控制台删除绑定的帐户。

将 TeamViewer 应用分发到目标用户，以使用标准应用分发工作流启动远程会话。 此操作仅适用于**有人参与**和**无人参与**模式。 如果管理员要控制设备，TeamViewer 的通用附件或特定于 OEM/型号的附件也需要分发到设备。 请查看应用配置，以了解相关说明。

使用 Help@Work for Android/iOS 开始远程会话

典型的 Help@Work for Android 或 iOS 会话会从最终用户需要帮助开始。

要启动 Help@Work 与用户设备的会话：

1. 在 Ivanti Neurons for MDM 中，转到**设备**。
2. 在设备列表页面中，单击需要支持的设备。
3. 从"操作"菜单中，单击适用于 Android 设备的 **启动 TeamViewer 远程控制**或适用于 iOS 设备的**远程显示**。 您将看到两个选项：
    - 有人参与模式（默认）- 此选项需要安装 **TeamViewer Quick Support** 应用，并将其加入目标设备的白名单。
    - 无人参与模式（仅适用于 Android）- 此选项需要安装 **TeamViewer Host** 应用，并将其加入目标设备的白名单。

> 如要将主机名列入白名单或覆盖内容安全策略，请联系支持团队。

> 无人参与模式选项也适用于 Kiosk 模式。 应从 TeamViewer 集成页面启用。 无人参与远程控制需要在设备上安装 TeamViewer Host 应用，在设备上进行一次性激活，以及一个 MI 附加许可证。 对于一次性激活，当 TeamViewer 主机应用程序首次安装和启动时，系统将显示权限提示。 如果需要的话，管理员可以在安装后使用"自动启动（托管应用程序配置中的设置）"来启动 TeamViewer 应用程序。 许可证数量基于 TeamViewer Host 应用分发进行计算。 如果 TeamViewer Host 应用已分发到设备，则会使用一个无人参与的远程主机会话许可证。 除了 TeamViewer 主机应用程序外，可能还需要其他附加应用程序，并应在 Kiosk 模式或共享 Kiosk 模式中允许。 可能需要其他加载项，具体取决于设备型号和制造商。

> Google Pixel 设备不会保留此权限授予，而且要求对每个会话的权限予以同意。

如果管理员拥有有效 TeamViewer 令牌，桌面客户端将与设备的支持会话一起启动。 否则，管理员需要使用 TeamViewer 登录，并授予权限。

要快速启动移除会话，管理员可以事先登录桌面应用。

安装 TeamViewer

在桌面上安装 TeamViewer 应用，以访问并为用户的远程设备提供支持。 要安装 TeamViewer：

1. 从此处下载适用于 Mac、Windows 或 Android 的 TeamViewer 完整版的安装包：
   https://www.teamviewer.com/en/download/
2. 启动 TeamViewer 安装程序。
3. 选择**基本安装**。
4. 选择**公司/商业用途**。
5. 点击**接受 - 完成**。

请求 TeamViewer 帐号

只有拥有 TeamViewer 帐号，才可以使用 TeamViewer 提供支持。 要获得 TeamViewer 帐号：

1. 转到 https://login.teamviewer.com/。
2. 输入您的电子邮件、名称和密码。

3. 单击**注册**。
4. 使用您在步骤 2 输入的电子邮件帐户，接收 TeamViewer 帐户确认电子邮件。
5. 完成电子邮件中的指示，以激活 TeamViewer 帐户。

确认 TeamViewer 会话 ID

在确定管理员计算机和用户移动设备之间的连接时，TeamViewer 会生成会话 ID。

1. 在生成会话 ID 时，Ivanti Neurons for MDM 使用托管应用配置将其传输到 TeamViewer QuickSupport 应用，然后依次使用此会话 ID 调用设备中的 TeamViewer 客户端。 对于 iOS，会话 ID 将在 30 分钟后到期。
2. 系统将提示用户接受 TeamViewer EULA。

12.2.10. 基础设施身份

本部分包含以下主题：

12.2.10.1. 配置标识提供者

许可证：Silver

配置身份提供程序 (IdP)，对希望使用 Ivanti Neurons for MDM 注册设备、访问此管理门户或访问自助服务门户的用户进行身份验证。 需要本地 LDAP 兼容用户目录。 Ivanti Neurons for MDM 适用于任何兼容 SAML 2.0 的 IdP。 Microsoft Entra ID 身份验证 (Entra ID)、Microsoft ADFS（Active Directory 联合身份验证服务）、Okta、OneLogin、PingOne 和 Ping Identity 的 PingFederate 经验证可与 Ivanti Neurons for MDM 搭配使用。

此前，如果您设置 SAML 身份验证/IdP，SAML 身份验证将用于设备注册和门户身份验证。 现在提供了切换按钮，可以为管理员门户访问和设备注册选择不同的身份验证方法。 免验证切换只适用于设备注册。

设备注册期间，管理员可以绕过身份提供程序选项，向用户提供使用 PIN 进行身份验证而不是使用身份提供程序页面进行身份验证的选项。

概述

- 如果您正在使用 Micorsoft AD 或其他本地 LDAP 目录，您需要设置 Connector，以便将用户连接并导入到 Ivanti Neurons for MDM。 如果您尚未这样做，请设置 Connector 或 **LDAP**。
- 添加 IdP 时，用户身份验证会自动从 LDAP 切换到 IdP。
- 仅允许一个 IdP 提供者。
- 如果您的 IdP 无法访问，请使用 Ivanti Neurons for MDM 租户管理员 (TA) 帐户访问该管理门户并进行故障排除。 TA 是本地账户，无需外部认证。 TA 帐户会在您配置 Ivanti Neurons for MDM 并将信息提供给组织的技术联系人或同等人员时创建。 如果您没有 TA 帐号信息，请联系您的支持代表。
- Ivanti Neurons for MDM 支持 Microsoft Entra ID (Entra ID)，可在 Windows 10 设备注册期间对用户进行身份验证。

> 请使用 IdP 供应商提供的工具设置您的 LDAP 用户身份验证类型。 您的 IdP 身份验证计划将优先于 Ivanti Neurons for MDM 设置。 Ivanti Neurons for MDM 身份验证设置可在此处找到：**用户 > 用户设置 > 设备注册设置 > 设备注册身份验证类型**。

- Apple 设备注册和 Configurator 设备注册不使用 IdP 进行用户身份验证。
- 如要配置身份提供程序以用于注册 Apple Business Manager iOS 和 macOS 设备，必须启用位于**管理员 > Apple > 设备注册 > *编辑设备注册配置文件*的启用自定义注册**和相关 **Ivanti 托管网页**设置。有关详细信息，请参阅**设备注册**：



IdP 设置类型

Ivanti Neurons for MDM 身份页面会指导您设置以下类型的 IdP 提供者：

- **Ivanti Neurons for MDM IdP 设置** - 支持的 Ivanti Neurons for MDM IdP 提供程序包括 Entra ID、OneLogin、Okta 和 PingOne。
- **内部部署 IdP 设置** - 支持的内部部署 IdP 提供商是 ADFS 3.0、PingFederate 8.2.1 和 PingFederate 8.1.3。
- **通用 IdP 设置** - 如果您未使用 Microsoft ADFS、Okta、OneLogin 或 PingFederate，则这是您可以使用的通用设置路径。

配置身份提供者 (IdP)

步骤

1. 前往**管理员** > **身份** > **SAML 身份验证**。
2. 点击身份提供程序设置类型：

- **Ivanti Neurons for MDM IDP 设置**
- **本地 IDP 设置**
- **通用 IDP 设置**

3. 选择对应的 IdP。 如果在步骤 3 中选择了**通用 IDP 设置**，则跳过此步骤，从步骤 5 开始继续操作。
4. 屏幕上将针对您选择的 IdP 显示相应的说明，请按照说明进行操作。
5. 单击**完成**。

> 管理员可以在使用 IdP 进行初始身份验证后，一次性登录长达 2 小时。

设置您可能需要完成的任务

根据您选择的 IdP，系统将指导您前往以下相关页面并完成所需步骤：

IdP	步骤
• Entra ID • Okta • OneLogin • PingOne	• 生成密钥，以上传到 IdP。 • 登录 IdP 并上传生成的密钥。 • 从 IdP 导出元数据文件，并将其导入 Ivanti Neurons for MDM。
• ADSF 3.0 • PingFederate 8.2.1 • PingFederate 8.1.3	• 从 Ivanti Neurons for MDM 下载元数据文件。 • 在 ADFS 上设置“信赖方信任”或在 PingFederate 上设置“SP 连接”，并导入 Ivanti Neurons for MDM 元数据文件。 • 从 IdP 导出元数据文件，并将其导入 Ivanti Neurons for MDM。
• 通用 IdP	1. 从 Ivanti Neurons for MDM 下载元数据文件。 2. 按照 IdP 供应商提供的说明配置 IdP 服务器或服务，使其作为“服务提供程序”与 Ivanti Neurons for MDM 服务通信。这可以包括： 1. 将上面步骤 1 中的元数据文件上传到 IdP。 此配置文件包含的基本信息可以使 Ivanti Neurons for MDM 作为 SAML 2.0 服务提供程序与您的 SAML 2.0 身份提供程序通信。 标准 SAML 2.0 URL、证书和设置包含在元数据文件中。 Ivanti Neurons for MDM 预计 SAML 2.0 兼容 IdP 能够导入和处理从服务提供程序导出的 XML 元数据。 2. 将您的 IdP 配置为使用 RSA-SHA1 签署 SAML 身份验证请求。 有关用于验证身份验证请求的签名证书的信息包括在步骤 1 中下载的元数据文件中。 3. 配置您的 IdP，以便在发送到 Ivanti Neurons for MDM 的 SAML 响应中包含用户名。 指定来自 IdP 的 SAML 响应[名称 ID]元素的用户名。 从 IdP 导出元数据文件，并将其导入 Ivanti Neurons for MDM。 3. （可选）- 在 SAML 身份验证请求中包含用户名：在身份验证请求中包括正在进行身份验证的用户的用户名，并在使用 IdP 进行身份验证时删除其他的用户输入。 如果启用此选项，则身份验证可能失败。 如果确定要进行 IdP 验证，请选择**我了解此更改所产生的影响**选项，并将**在 SAML 身份验证请求中包含用户名**设置切换至**打开**。 对于此设置，Ivanti Access 是经验证的 IdP。

启用本地用户以绕过 IdP 身份验证。

当 IdP 或 Ivanti Neurons for MDM 连接断开并需要从 Ivanti Neurons for MDM 端进行故障排除时，某些管理员需要能够登录到 Ivanti Neurons for MDM，而不必依赖 LDAP 或 IdP 等外部系统进行身份验证。 只有拥有系统管理员角色的本地用户才能绕过 IdP 身份认证。

创建本地用户列表以绕过 IdP 身份验证。

步骤

1. 单击**管理员 > 身份**。

2. 在"绕过 IdP 身份验证的本地用户"部分，单击**+添加用户。**
3. 从仅显示具有系统管理员角色的本地用户的列表中，选择一些用户。
4. 单击**保存**。

> 要从绕过 IdP 身份验证的本地用户列表中删除用户，请单击要删除的条目旁边的删除图标。

如果您未看到身份页面，这可能是您没有所需权限。 您需要以下角色之一：

- 系统管理
- 系统只读

12.2.10.2. 使用 SCIM 进行用户配置

本部分包含以下主题：

- 用户配置
- 从 Ivanti Neurons for MDM 生成令牌
- 更改令牌状态
- 从"审计跟踪"中查看令牌状态
- 在 SCIM 配置中配置属性

用户配置

用户配置使用 SCIM 协议同步 IdP 和 Ivanti Neurons for MDM，并允许部分用户和组同步。 用户配置使用 SCIM 协议自动创建用户和组对象并将来源从 IdP 更新到 Ivanti Neurons for MDM。 就像当前与 Entra ID 和 Okta 的集成，用户和组配置流程是自动进行的；如果在 IdP 中对用户或组进行更改，同样的更改将反映在 Ivanti Neurons for MDM 中。

> 如果用户名在 Ivanti Neurons for MDM 中是唯一的，则可以在身份提供者 (IdP) 中重命名通过 SCIM 配置的用户的用户名。

> 现在可以使用各自的外部 ID 搜索 SCIM 用户和组。

从 Ivanti Neurons for MDM 生成令牌

要开始 IdP 用户配置，请从 Ivanti Neurons for MDM 生成令牌和目标 URL。

> 确保保存令牌和目标 URL。

> 任何时候最多生成 2 个令牌。

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 前往**管理员** > **身份** > **用户配置**。
3. 从下拉列表中选择身份提供程序 (IdP)。
4. 要生成新令牌，请点击**生成**。 随即显示通知消息，请点击**生成**。 新页面随即打开，其中包含令牌和目标 SCIM URL 的详细信息。
5. 单击**复制**，复制令牌或 SCIM URL。
6. 刷新页面。 **用户配置**页面将显示"令牌状态"表格。

更改令牌状态

可以更改现有令牌的状态。

步骤

1. 点击**用户配置 Entra ID** 页面上的**选择**下拉菜单。
2. 点击**选择**对令牌进行以下更改：

- **设置为活动**
- **设置为不活动**
- **续订**
- **移除**

从“审计跟踪”中查看令牌状态

您可以从“审计跟踪”部分查看 SCIM 令牌上发生的操作/事件的日志。 SCIM 令牌可以具有以下状态之一：

- SCIM 令牌已创建 - 已经创建 SCIM 令牌。
- SCIM 令牌已启用 - 已经启用 SCIM 令牌。
- SCIM 令牌已禁用 - 已经禁用 SCIM 令牌。
- SCIM 令牌已更新 - 已经更新 SCIM 令牌。
- SCIM 令牌已删除 - 已经删除 SCIM 令牌。

“详细信息”列还列出了 SCIM 供应商名称 (IDP)，例如 Azure、Okta 等。 这使得与 Ivanti Neurons for MDM 通信变得容易。

在 SCIM 配置中配置属性

本节描述如何在用户配置期间为 IdP 创建自定义和企业属性。

映射属性

建立连接后，可以在 IdP 和 Ivanti Neurons for MDM 之间映射属性。 Ivanti Neurons for MDM 支持以下用户属性：

核心属性

- id
- userName
- displayname
- active
- givenName
- familyName
- emails

> 对于 Entra ID IdP，支持外部 IdP。

允许更新操作的属性列表

- userName
- displayName
- emails
- givenName
- familyName
- active

- urn:ietf:params:scim:schemas:extension:ivanti:2.0:User
- urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

自定义属性

架构 - urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<CustomAttribute123Name>

企业属性

目前仅支持部门属性。

架构 - urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department

12.2.10.2.1. Entra ID IdP 用户配置

本部分包含以下主题：

- 与 Ivanti Neurons for MDM 建立连接
- 配置已分配的用户和组
- 配置所有用户和组
- 验证已分配的用户配置
- Entra ID IdP 用户配置
- 编辑设置
- 配置自定义和企业属性
- 迁移注意事项 - Entra ID 用户源到用户配置 SCIM
- 迁移注意事项 - LDAP 到用户配置 SCIM
- 重要说明 - SCIM

与 Ivanti Neurons for MDM 建立连接

在 Entra ID Enterprise 应用程序中创建用户和组后，您可以在 Entra ID 与 Ivanti Neurons for MDM 之间建立连接。

步骤

1. 登录 Entra ID 门户。
2. 转到**企业应用** > 点击 **+ 创建您自己的应用**。 随即将打开“创建您自己的应用”窗口。
3. 指定应用的名称（**默认：非图库**），然后点击**创建**。 例如，Ivanti Neurons for MDM 用户配置。
4. 转到**配置** > **编辑配置** > **管理员凭据**。
5. 从 Ivanti Neurons for MDM 管理员门户中，复制目标 SCIM URL，并将其粘贴到 Entra ID 门户中的**租户 URL** 字段。
6. 从 Ivanti Neurons for MDM 中复制令牌，并将其粘贴到 Entra ID 门户中的**机密令牌**字段。
7. 执行以下步骤之一：
    - 选择**仅同步已分配的用户和组**。 有关详细信息，请参阅“配置已分配的用户和组”
    - 选择**同步所有用户和组**。 有关详细信息，请参阅“配置所有用户和组”。

    > 为迁移用户选择“同步所有用户和组”选项。

单击**测试连接**。 系统将显示绿色复选标记的弹出窗口，并用于确认连接。

9. 单击**保存**。
10. 从 Entra ID 门户的**配置**页面展开**映射**。
11. 点击**配置 Entra ID 用户**。 随即打开“属性映射”页面。
12. 点击**删除**可删除不支持的属性。

配置已分配的用户和组

Entra ID 与 Ivanti Neurons for MDM 建立连接后，您可以配置用户或组。

> 配置组时，Entra ID 不会向所选的组添加嵌套组的成员。 同步过程中，Entra ID 只向组中添加即时成员和组名，不会添加子组成员。

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 在应用中，转到**用户和组** > 点击 **+ 添加用户/组**。 系统将打开添加分配页面。
3. 从**搜索**字段中搜索用户或组，点击**选择**，然后点击**分配**。 系统将打开用户和组页面。
4. 选择相应的用户或组复选框。
5. 单击**配置**，然后单击**开始配置**。 随即显示成功配置的详细信息。

配置所有用户和组

在 Entra ID 与 Ivanti Neurons for MDM 之间建立连接后，您可以配置用户或组。

步骤

- 单击**配置**，然后单击**开始配置**。 系统将打开页面，其中包含成功配置的详细信息，而用户将配置到 Ivanti Neurons for MDM。

验证已分配的用户配置

在 Entra ID 门户中配置已分配的用户后，验证 Ivanti Neurons for MDM 管理员门户中的配置。

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 转到主菜单下方的**用户**选项卡。 此页面中的用户列表将显示已配置的用户。

> 配置过程可能会花费一个小时。

验证组配置

在 Entra ID 门户中配置组后，验证 Ivanti Neurons for MDM 中的配置。

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 转到**用户**选项卡 > **用户组**。 此页面中的组列表将显示已配置的组。

> 配置过程可能会花费一个小时。

编辑设置

本主题可帮助您配置 Entra ID 设置。

步骤

1. 转到**管理员 > Microsoft Azure > 用户配置 Entra ID**。
2. 点击**生成令牌**并复制令牌。
3. 刷新页面。 Entra ID 设置页面随即打开。

4. 点击**编辑设置**。
5. 设置**自动邀请从 Entra ID 导入的用户** - 管理是否自动邀请从 Entra ID 导入到 Ivanti Neurons for MDM 中的用户通过电子邮件进行注册。
6. 设置**托管 Apple ID** - 此选项默认禁用。 单击切换按钮启用它。 在配置过程中，可以通过以下方式设置受管 Apple ID：
   - **用户电子邮件地址**
     - （可选）选择包含 "appleid" 子域选项以避免与现有 Apple ID 发生冲突。
   - 映射到**自定义属性**

     > 自定义属性应计算为唯一的电子邮件地址。
7. （可选）点击**添加自定义属性** - 指定要应用到设备管理的目录服务中的自定义用户属性。 每个属性随后可被支持变量的配置字段中的 $ 引用。 使用此选项需要在 Entra ID 服务器上实施一致的自定义属性。 如果实施时包含的 Entra ID 服务器未使用此属性，那么依赖此属性的功能可能无法按预期工作。 在**编辑设置**部分的**自定义属性**表格中，**属性类型**列将显示 **IDP** 属性。
8. 修改 Entra ID 设置后，点击保存更改。

配置自定义和企业属性

步骤

1. 前往**管理员** > **身份** > **用户配置**。
2. 在**编辑设置**下，点击 **+ 添加自定义属性**。
3. 在**属性名称**字段（例如 custAttr1）输入名称，然后点击**保存更改**。 该属性会在**管理员** > **系统** > **属性**页面中列出并可供使用。 该属性表示为 IdP 属性，只能执行删除操作。
4. 登录 **Entra ID** 门户。
5. 前往**主页** > **企业应用程序** > 点击 SCIM 应用程序。
6. 在**映射**部分点击**配置 Entra ID 用户**。
7. 选中**显示高级选项**复选框。
8. 点击**编辑 customappsso 属性列表**。
9. 为您在 Ivanti Neurons for MDM UI 中创建的自定义属性输入新条目。
10. 为自定义/企业（部门）属性添加架构，如下所示：
    自定义属性 - **urn:ietf:params:scim:schemas:extension:ivanti:2.0:User:<custAttr1> -** 请参阅第 3 步。
    企业属性 - **urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department**
11. 点击**保存更改**。
12. 点击**添加新映射**，并从下拉菜单中选择“源”属性和“目标”属性。
13. 点击**确定**，然后点击**保存映射**。
14. 前往**主页** > **企业应用程序** > 点击 SCIM 应用程序 > **用户和组**。
15. 点击用户名。 “配置文件”页面随即打开。
16. 确认与属性相关的值是否出现在“配置文件”页面中。
17. （可选）点击 SCIM 应用程序 > 配置 > 按需配置，搜索特定用户，然后点击配置。 验证在前述步骤中执行的新属性映射。
18. 登录到 Ivanti Neurons for MDM 管理门户。
19. 转到**用户** > **用户** > 选择用户。
20. 点击**属性**选项卡，并验证属性值。 属性已映射到特定用户。

迁移注意事项 - Entra ID 用户源到用户配置 SCIM

- 从 Entra ID 用户源迁移到用户配置 Entra ID (SCIM) 时，请选择“同步所有用户和组”。
- 使用 SCIM Entra ID 源更新用户和组之后，返回到 Azure 中的“Azure 配置”页面，通过使用“仅同步已分配的用户和组”选项来设置要由用户配置 Entra ID 进行管理的特定用户和组。
- 同步完成后，可从 Ivanti Neurons for MDM 用户和组列表中删除未在 Azure 中定义的用户和组。
- 开始迁移时，“Entra ID 用户源”页面将仅支持只读访问。

迁移注意事项 - LDAP 到用户配置 SCIM

必备项：

1. 默认选中**启用此 LDAP 服务器**选项。 迁移前必须取消选择此选项。
2. 在 Entra ID 中创建一个企业应用程序，将同步的 LDAP 用户/组（Ivanti 中存在的相同 LDAP 用户/组）添加到 SCIM 应用程序中。 开始配置。

LDAP 迁移到 SCIM 的重要注意事项

- LDAP 不会捕获同步用户/组的所有信息，而 SCIM 会在审计日志中记录用户/组事件。
- 具有自定义属性的 LDAP 用户具有类型定义的 LDAP，而对于 SCIM，则是 IdP。 因此，具有自定义属性的用户从 LDAP 迁移到 SCIM 时，应在 SCIM 应用程序中创建相应的 IdP 自定义属性，然后迁移用户。 如果用户后续想要更新 LDAP 自定义属性，则迁移后 ldap.custom 属性值不会在 MDM 中更新。 IdP 属性值会更新。
- 迁移与一个或多个自定义属性（比如“ldap.custAttr1”）关联的 LDAP 用户，表示 LDAP 设备的注册以及推送到设备的配置（身份证书配置），其 SAN 类型与 LDAP 自定义属性的值相对应。
- 迁移受管 Apple ID 与电子邮件地址关联的 LDAP 用户 - 因此，在从 LDAP 迁移到 SCIM 之前，如果用户希望保留 LDAP 用户的受管 Apple ID 的值，则必须启用 SCIM 设置中的受管 Apple ID 并保存设置。
- 从 LDAP 服务器删除 LDAP 用户后，该用户仍处于活动状态，但该特定同步 LDAP 用户的同步标志不再设为 true。 如果是在 SCIM 中，则删除已配置的用户后，该用户将处于禁用状态。
- 为 SCIM 用户的身份提供程序 (IdP) 配置 SAML 后，来自本地和 LDAP 等各种来源的所有用户都将通过 SAML 进行身份验证。 仅本地用户可添加到例外列表，免去 IdP 身份验证流程。 可以在 SAML 页面的以下位置管理此配置：**管理员** > **身份** > **SAML**。
- 为迁移的 IDP (SCIM) 用户配置 SAML 后，来自本地和 LDAP 等不同来源的其他用户可以免去设备注册（不通过 IDP）。 此设置可在**用户** > **用户设置**下进行管理。
- LDAP 支持用户、组和组织单位，而 SCIM 支持用户和组，但不支持组织单位。
- SCIM 不支持嵌套组配置流程。

重要说明 - SCIM

- 电子邮件地址是配置和迁移用户或成员的必填字段。
- SCIM 提供从 Microsoft Entra ID 到 Ivanti Neurons for MDM 的单向配置。 Ivanti Neurons for MDM 不提供任何同步选项。 如果从 Ivanti Neurons for MDM 删除 SCIM 配置组或用户，请确保也从 Microsoft Entra ID 中删除相应的用户或组。
- 一次只能在 Microsoft Entra ID 的 SCIM 应用程序映射窗口中使用一个属性（源或目标）。 同一来源不能映射到一个特定的目标属性两次。
- 无法使用 SCIM 配置或迁移非活动用户至 Ivanti Neurons for MDM。
- 现在，Ivanti Neurons for MDM 不支持 SCIM 事件通知。
- 迁移或配置持续时间取决于所涉及的用户或组的数量。

- Microsoft Azure 会控制配置间隔，大约为 40 分钟或更长时间。
- 在重新配置期间，Microsoft Entra ID 将仅重试失败的条目。 您可以下载配置日志以验证从 Microsoft Entra ID 配置成功或失败的用户。
- SCIM 中不允许来自不同来源的重复组。
- 从 Microsoft Entra ID 中硬删除配置的用户时，该用户将在 Ivanti Neurons for MDM 中遭到禁用。
- 从 Microsoft Entra ID 中删除配置的用户组时，该组将从 Ivanti Neurons for MDM 中删除，同时属于已删除组的独立成员将遭到禁用并关联到所有用户组。
- 从 Microsoft Entra ID 中硬删除配置组的配置成员时，该成员将在 Ivanti Neurons for MDM 中遭到禁用，但该成员仍与 Ivanti Neurons for MDM 中的该组关联。
- 从应用程序中删除属性（企业属性或自定义属性）映射时，删除的属性值仍会反映在 Ivanti Neurons for MDM 中。
- 当已配置用户的用户属性更新为空白或空值时，更新的属性值不会反映在 Ivanti Neurons for MDM 中。
- 从 Microsoft Entra ID 迁移或更新到 SCIM 期间，如果用户属性 FName 和 LName (name.formatted) 为空，则迁移或更新会失败。
- 如果从 Entra ID 中删除用户，相应的 SCIM API 不会永久删除该用户，而是会执行软删除并将用户状态从活动更改为非活动。 如果要永久删除该用户，请登录 Ivanti Neurons for MDM 管理门户并手动删除非活动/禁用用户。
- 在 Ivanti Neurons for MDM 中已存在具有特定用户 ID 的本地用户时，系统会从 Entra ID 向 MDM 配置具有相同用户 ID 的类似用户，用户源将从“本地”更新为“SCIM Entra ID”。
- 具有“Entra ID Premium P1”订阅的 Entra ID 有权配置要分配和配置的所需组。

12.2.10.2.2. Okta IdP 用户配置

本部分包含以下主题：

- 与 Ivanti Neurons for MDM 建立连接
- 配置用户和组
- 验证已分配的用户配置
- 验证组配置
- 编辑设置
- 在 SCIM 用户配置中配置自定义/企业属性

与 Ivanti Neurons for MDM 建立连接

在 **Okta** 应用程序中创建用户和组后，可以建立 **Okta** 与 Ivanti Neurons for MDM 之间的连接。

步骤

1. 登录 **Okta**。
2. 前往**应用程序** > **应用程序** > **浏览应用程序目录**。
3. 搜索**添加 SCIM 2.0 Test App**（OAuth Bearer 令牌）并安装应用程序。
4. 点击应用程序并前往**配置** > **集成**。
5. 点击**编辑**并提供基本 URL 并粘贴生成的令牌。
6. 单击**保存**。
7. 前往**配置**，然后点击**编辑**。
8. 启用必要的用户操作并点击**保存**。

配置用户和组

Okta 与 Ivanti Neurons for MDM 建立连接后，可以配置用户或组。

步骤

1. 前往**分配** > **分配** > **分配至人员**或**分配至组**。
2. 2. 选择或搜索现有用户或组，然后点击**分配**。
3. 重复此过程即可添加更多**用户**或**组**。
4. 单击**完成**。
5. 选择组并点击**按名称推送组**来保存并同步该组。

验证已分配的用户配置

在 Okta 门户中配置已分配用户后，验证 Ivanti Neurons for MDM 管理门户中的用户配置。

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 前往主菜单下方的**用户**选项卡。 此页面中的用户列表将显示已配置的用户。

验证组配置

在 Okta 门户中配置组后，验证 Ivanti Neurons for MDM 中的配置。

步骤

1. 登录到 Ivanti Neurons for MDM 管理门户。
2. 前往**用户**选项卡，然后点击**用户组**。 此页面中的组列表将显示已配置的组。

编辑设置

本主题可帮助您配置 Okta 设置。

步骤

1. 前往**管理员** > **身份** > **用户配置 Okta**。
2. 点击**编辑设置**。
3. 设置**自动邀请从 Okta 导入的用户** - 管理是否自动邀请从 Okta 中导入到 Ivanti Neurons for MDM 中的用户通过电子邮件进行注册。
4. （可选）点击**添加自定义属性** - 指定要应用到设备管理的目录服务中的自定义用户属性。 然后，可以在支持变量的配置字段中通过 $ 引用每个属性。 使用此选项需要跨 Okta 服务器实现一致的自定义属性。 如果实施中包含的 Okta 服务器不使用自定义属性，那么依赖于自定义属性的功能可能无法按预期工作。 在**编辑设置**部分的**自定义属性**表格中，**属性类型**列将显示 **IDP** 属性。
5. 修改 Okta 设置后，点击**保存更改**。

在 SCIM 用户配置中配置自定义/企业属性

步骤

1. 前往**管理员** > **身份** > **用户配置**。
2. 点击**编辑设置**。
3. 输入自定义属性（例如 custAttr1），然后点击**保存更改**。
4. 在 Okta 门户中，点击**目录** > **配置文件编辑器**。
5. 点击 **SCIM 2.0 Test App（OAuth Bearer 令牌）用户**应用程序。
6. 点击**添加属性**。
7. 添加以下自定义属性值，例如：
    - 显示名称（与 N-MDM 中提供的自定义属性值相同，请参阅第 3 步）。
    - 变量名称：custAttr1
    - 外部名称：custAttr1
    - 外部命名空间：**urn:ietf:params:scim:schemas:extension:ivanti:2.0:User**
    - 用户权限：（读/写）
8. 点击**保存属性**。
9. 点击**配置文件编辑器** > **映射**。 您将看到两个映射部分（SCIM 和 Okta）。
10. 将 N-MDM 中创建的自定义属性映射到 Okta 中定义的属性，并保存映射。
11. 前往**用户**，然后点击所需的用户。
12. 点击**配置文件** > **编辑**即可编辑属性。
13. 前往**应用程序** > **SCIM 2.0 Test App（OAuth Bearer 令牌）**应用程序。

14. 在**分配**选项卡下，点击**分配**并选择**分配至人员**。
    将 SCIM 2.0 Test App（OAuth Bearer 令牌）分配至人员窗口随即显示在屏幕上。
15. 选择所需的用户，然后点击**分配**。
16. 单击**完成**。

验证自定义属性及其在 Ivanti Neurons for MDM 中的映射：

- 前往**用户** > **用户**（任何特定用户）> **属性**。 确保 Okta 映射的自定义属性可在“用户属性”部分下显示。

12.2.11. 配置 LDAP 服务器

许可证： Silver

配置 LDAP 服务器和 Connector 允许您从公司目录中导入用户和组。 您至少安装一个 Connector 后，便可添加一个或多个 LDAP 服务器。

添加 LDAP 服务器意味着配置：

- 同 LDAP 服务器的*连接*
- 查看目标目录数据必需的*搜索条件*
- 要*导入*的目录部分
- 是否在所选目录部分自动*邀请用户*

添加 LDAP 服务器后，您可以返回到此页面**编辑 LDAP 服务器信息**或**更改所选 LDAP 用户**。

> 在配置 LDAP 用户后，必须导入 LDAP 用户。 请参见**导入 LDAP 用户**。
> LDAP 用户名（例如本地用户名）必须全局唯一。 请确认用户没有拥有相同用户名的本地帐户；或者对于拥有多位租户的组织，请确认用户名没有与其他租户关联。

添加 LDAP 服务器

程序

1. 单击 **+ 添加服务器**。
2. 提供以下信息：
3. 单击**测试连接并继续**。

设置	流程
名称	输入用于识别此服务器的名称。
说明	输入阐明此服务器目的的说明。
目录 URL	输入目录的 URL。 使用以下格式之一： ldap://IP address 或 ldaps://IP address 或 示例：ldap://myserver1.mycompany.com:389
用户 ID	输入具有以下特征的账户的用户 ID： • 由 LDAP 服务器管理 • 可以绑定至 LDAP 服务器，并能搜索用户、组和组织单位的子树 这通常是一个具有目录管理员证书（DN 或可分辨名称和密码）的帐号。
密码	输入帐号的密码。
确认密码	重新输入帐号的密码。
目录类型	从所支持的目录列表中选择目录类型。 • Microsoft Active Directory • 打开 LDAP • 其他（与 Open LDAP 兼容）

4. 此步骤验证您目前所提供的信息。

- 如果信息证明有效，则服务会检索 LDAP 命名上下文，用此填写下一页中的一些字段。
- 如果 LDAP URL 无法连接，您可能会继续设置后续步骤。 但这可能会导致功能受限，直到解决连接。

完成剩余设置：

5. 单击**下一步**。

设置	流程
目录故障转移 URL	输入二级目录的 URL。 使用以下格式： ldap://IP address 或 示例：ldap://myserver2.mycompany.com:389
同步间隔	输入每次尝试从 LDAP 服务器同步 LDAP 数据之间的时间段。 默认值为 15 分钟。 一旦您成功同步所有目标 LDAP 数据，并确认您的 LDAP 设置满足您的需求后，考虑增大间隔。
启用同步放弃	如果重新加载的数据集显著下降，选择此项可自动放弃同步数据。 此选项可确保 LDAP 系统上的一部分不正常行为不会对服务造成不必要的破坏性更新，以及从注册设备上移除配置。 如果您打算对 LDAP 设置或 LDAP 服务器进行大改动，请确保未选择此选项。
启用该 LDAP 服务器	选择此项可让您的服务使用此 LDAP 服务器。 如果您想要停用此 LDAP 服务器或将其从服务中移除，请清除此设置。 虽然配置的故障转移至第二个 LDAP 服务器将自动替换此服务器，但使用此选项可使您提前计划并避免在故障转移期间暂时缺少连接性。
在导入用户自动邀请	选择在从 LDAP 服务器导入时自动将邀请发送到用户。
上传 CA 证书	单击**选择文件**，以上载由在此 LDAP 服务器中安装的 CA 颁发的 TLS 证书。 您可以上传多个 CA 证书。
查找参照	仅在使用多林域时适用。 此选项表明当目标域控制器没有请求对象的副本时，您是否要使用备用域控制器。 • 如果您要使用推荐控制器，请选择**跟随**。 • 如果您不使用备用域控制器，请选择**忽略**。 • 目前，**丢弃**选项与**忽略**的效果相同。 选择**遵循**会延迟 LDAP 身份验证。
搜索结果超时	如果您浏览从 LDAP 服务器同步的数据时，发现性能问题或结果不完整，请延长此超时时间。
搜索结果计数	设置为应从 LDAP 服务器中一次返回的最大记录数。 需要更改此设置以提高性能的情况包括： • LDAP 服务器的位置远离高延迟链接，或在高延迟链接之后。 此种情况下，检索大搜索结果比检索小搜索结果所需的时间长，因此定义一个较小的集可使您更快地查看更新数据的子集。 • LDAP 是巨大的，每次搜索均会返回巨大的结果集。 此种情况下，如果性能不是问题，定义一个较大的结果集便能通过较少次的搜索返回所有数据。

> 对于沙盒环境，LDAP 同步间隔不能小于 8 小时。

6. 按照以下指导方针配置与 LDAP 服务器的集成：
7. 单击**浏览**或**搜索**。

设置	流程
组成员格式	选择 **DN** 或 **UID**，以指示是在搜索中使用可分辨名称还是用户 ID。
OU 搜索属性	指定在组织单位级别进行搜索的条件。
基本 DN	输入您希望您的搜索根源或起点所在的起始级别的可分辨名称。 您的选择决定一些其他字段的默认值，如有必要，您可以对其进行更改。
对象 GUID	如有必要，更改默认值以同您的 LDAP 环境匹配。 这是唯一跨越时间和 OU 名称更改识别组织单位的属性。
属性名称	如有必要，更改默认值以同您的 LDAP 环境匹配。
说明	如有必要，更改默认值以同您的 LDAP 环境匹配。
属性 DN	如有必要，更改默认值以同您的 LDAP 环境匹配。
搜索筛选	如有必要，更改默认值以同您的 LDAP 环境匹配。
搜索范围	选择要作为目标的 LDAP 层次结构部分： • **基本**（仅搜索基本条目的级别） • **一级**（搜索基本之下的级别） • **子树**（搜索基本 DN 之下的目录信息树中的 子树）
用户搜索属性	指定在特定目录级别搜索用户的条件。
基本 DN	输入您希望进行搜索的起始级别的可分辨名称。
属性 UID	如有必要，更改默认值以同您的 LDAP 环境匹配。
对象 GUID	如有必要，更改默认值以同您的 LDAP 环境匹配。 这是唯一跨越时间和用户名称更改识别用户的属性。
属性 DN	如有必要，更改默认值以同您的 LDAP 环境匹配。
名字	如有必要，更改默认值以同您的 LDAP 环境匹配。
姓氏	如有必要，更改默认值以同您的 LDAP 环境匹配。
显示名称	如有必要，更改默认值以同您的 LDAP 环境匹配。
电子邮件地址	如有必要，更改默认值以同您的 LDAP 环境匹配。
主体名称	如有必要，更改默认值以同您的 LDAP 环境匹配。
区域设置	如有必要，更改默认值以同您的 LDAP 环境匹配。
成员	如有必要，更改默认值以同您的 LDAP 环境匹配。
搜索筛选	如有必要，更改默认值以同您的 LDAP 环境匹配。
搜索范围	选择要作为目标的 LDAP 层次结构部分：

设置	流程
	• **基本**（仅搜索基本条目的级别） • **一级**（搜索基本之下的级别） • **子树**（搜索基本 DN 之下的目录信息树中的 子树）
受管 Apple ID	选择以同步 LDAP 用户的受管 Apple ID。 • **无** • **模式** - ◦ **用户电子邮件地址** ◦ **userUPN** 或者，选择**包含“appleid”子域**选项，以避免与现有 Apple ID 冲突。
+添加自定义属性	（可选）从目录服务中指定最多 7 个要用于设备管理的自定义用户属性。 每个属性随后可被支持变量的配置字段中的 $ 引用。 **重要信息：**使用此选项需要在所有 LDAP 服务器执行中使用统一的自定义属性。 如果执行中包含的 LDAP 服务器未使用此属性，则取决于该属性的功能可能无法发挥预期作用。
组搜索属性	
基本 DN	输入您希望进行搜索的起始级别的可分辨名称。
对象 GUID	如有必要，更改默认值以同您的 LDAP 环境匹配。 这是唯一跨越时间和组名更改识别组的属性。
属性 DN	如有必要，更改默认值以同您的 LDAP 环境匹配。
属性名称	如有必要，更改默认值以同您的 LDAP 环境匹配。
说明	如有必要，更改默认值以同您的 LDAP 环境匹配。
成员	如有必要，更改默认值以同您的 LDAP 环境匹配。
搜索筛选	如有必要，更改默认值以同您的 LDAP 环境匹配。
搜索范围	选择要作为目标的 LDAP 层次结构部分： • **基本**（仅搜索基本条目的级别） • **一级**（搜索基本之下的级别） • **子树**（搜索基本 DN 之下的目录信息树中的 子树）

8. 确认您的配置返回期望数据。
9. 您可以通过在目中浏览或搜索已知项完成此操作。

单击**下一步**。

删除自定义 LDAP 属性

您可以删除自定义 LDAP 属性，并从关联的用户或设备中删除其值。

程序

1. 转至**管理员 > 属性**。

2. 在**自定义属性**部分，单击应删除的 LDAP 属性旁边的**删除**链接。 将显示“确认”窗口。
3. 点击**删除**确认删除。

> **删除**按钮默认禁用。您应该选中**我了解删除自定义属性不可逆**选项中的复选框，以启用**删除**按钮。

编辑 LDAP 服务器信息

程序

1. 转至**管理 > LDAP**。
2. 在 LDAP 服务器条目中，从**操作**列选择**编辑**图标，以查看“连接 LDAP 服务器”页面。
3. 进行必要更改。
4. 单击**测试连接并继续**。
   如果 LDAP URL 无法连接，您可能会继续设置后续步骤。 但这可能会导致功能受限，直到解决连接。
5. 单击**浏览**或**搜索**。
6. 确认您的配置返回期望数据。
   您可以通过在目中浏览或搜索已知项完成此操作。
7. 单击**完成**。

导入 LDAP 用户

程序

1. 转到**用户**。
2. 单击 **+ 添加 > 从 LDAP 邀请用户**。
3. 在 LDAP 服务器条目中单击**选择用户**。
4. 在“添加 LDAP 用户”页面，在搜索字段中输入用户、小组或 OU 的名称。
5. 要添加新用户或小组，单击您想要添加条目旁边的 **+ 添加**。
6. 单击**下一步**。
7. 选择是否发送邀请：
   - 无邀请
     要在稍后发送邀请，转到**用户 > 用户**并选择**操作 > 发送邀请**，以发送邀请。
   - 全部邀请

单击**完成**。

更新所选的用户、组或组织单位

程序

1. 转至**管理 > LDAP**。
2. 在 LDAP 服务器条目中，从**操作**列选择**管理用户**图标，以查看添加 LDAP 用户页面。
3. 要添加新用户或小组，在搜索字段中输入用户名或小组名。
4. 单击您想要添加条目旁边的 **+ 添加**。

5. 要移除用户、小组或 OU，单击您想要删除条目旁边的移除图标。
6. 单击**完成**。

启用 LDAP 同步丢弃通知

启用 LDAP 同步丢弃通知有助于防止因无意中对 LDAP 环境进行大规模更改而导致的中断。

程序

1. 转至**管理 > LDAP**。
2. 在 LDAP 服务器条目中，从**操作**列选择**编辑**图标，以查看“连接 LDAP 服务器”页面。
3. 选中**启用同步丢弃**复选框。
4. 为重新加载 LDAP 数据的百分比输入值，以触发同步放弃。
5. 单击**测试连接并继续**。
   如果 LDAP URL 无法连接，您可能会继续设置后续步骤。 但这可能会导致功能受限，直到解决连接。
6. 单击**完成**。
7. 在 LDAP 服务器条目中，单击**立即同步**图标。
   从 LDAP 同步到 Ivanti Neurons for MDM 的变化差异超过已设置的放弃百分比时，则会生成“警告”通知。 在更改还原到设置百分比之下的值以后，则会清除通知。

触发器	严重等级	通知类型	组件类型	组件
LDAP 同步放弃	警告	数据同步	LDAP	LDAP 服务器名称
LDAP 同步已恢复	信息	数据同步	LDAP	LDAP 服务器名称

当一个或多个用户记录无法从 LDAP 同步时，将生成部分同步丢弃通知。 在这种情况下，CSV 文件作为附件包含在一起，其中包含无法同步的用户列表。 如果用户由于缺少属性而被丢弃，则缺失属性列表也会包含在导出的 CSV 文件中。

从 LDAP 服务器同步更改

在“LDAP”页面中，单击 LDAP 服务器条目中的**立即同步**图标。

> 如果显示名称超过 128 个字符，LDAP 同步将忽略此类用户，并继续与其他用户或用户组同步。

排除连接至 LDAPS 服务器的故障

若您放在连接至 LDAPS (LDAP over SSL) 服务器时遇到问题，您可能是碰到与证书相关的问题。

要解决此问题：

- 核实您并未在 LDAPS 服务器上使用自签名证书。
- 核实 LDAPS 证书尚未到期或被撤销。 此外，检查主机名是否不匹配。

在验证后，等待自动 LDAP 同步，或在 LDAP 服务器条目中使用**管理员 > LDAP > 立即同步**图标手动同步。

如果您未看到 LDAP 页面，这可能是您没有所需权限。 您需要以下角色之一：

- 系统管理

- 系统只读

12.2.12. 卫士

Sentry 是一个组件，作为移动设备和支持 ActiveSync 功能的电子邮件系统之间的网关使用。 使用 Sentry 控制允许访问电子邮件的设备。 可将它作为可安装在虚拟机上的 ISO 文件进行下载。 组织应考虑使用负载平衡器来维持多个（冗余）Sentry。

许可证： Silver

最新文档

如需最新 Sentry 说明，请访问产品文档并单击 Sentry。

有关最新的 Sentry 安装说明，请选择适当版本的*独立 Sentry 内部部署安装指南*。

有关 Sentry 升级说明，请选择 *Sentry 指南的相应版本*。 请参阅 Sentry 指南中的以下部分：

- 有关使用独立 Sentry System Manager UI 进行升级的说明，请参阅“独立 Sentry 软件更新”。
- 有关使用独立 Sentry 命令行界面 (CLI) 进行升级的说明，请参阅“使用 CLI 升级”。

升级之前，请参阅要升级的版本的独立 Sentry 发行说明。

12.3. Apple 设置

本部分包含以下主题：

- Apple Configurator
- 设备注册
- 配置设置辅助
- 安装 MDM 证书
- 共享 iPad 设备企业版
- 校园教务管理
- 设置 (Apple)

12.3.1. Apple Configurator

可以使用此页面准备 Apple Configurator，以便在 iOS 设备上设置 Ivanti Neurons for MDM 设备管理。 通过 Apple Configurator 可以很轻松地部署大量 iOS 设备。 此外，Configurator 允许管理员使 iOS 设备处于受监控状态，从而实现更高级别的配置和管理功能。 有关 Apple Configurator 的详细信息，请访问 Mac App Store。

基本步骤：

1. 从 Ivanti Neurons for MDM 租户中导出 MDM 配置文件。
2. 将 MDM 配置文件导入 Configurator。
3. 使用 Configurator 将 MDM 配置文件应用至捆绑设备。

定义设备的默认用户

除非您选择其他用户，否则通过 Apple Configurator 配置的设备将分配到 Ivanti Neurons for MDM 中的无人用户：

1. 单击**将配置的设备分配至**字段。
2. 开始输入您要选择的 Ivanti Neurons for MDM 用户的用户名。
3. 下拉菜单中显示该用户名时，将其选中。
4. 单击**保存**。

使用 Apple Configurator 安装应用程序

在使用 Apple Configurator 安装应用程序之前：

- 通过设备配置限制 Apple 应用商店的访问权限。
- 通过设备配置允许应用程序安装。
- Apple Configurator 必须安装在用于配置设备的计算机上。

要使用 Apple Configurator 安装应用程序：

1. 在 Ivanti Neurons for MDM 中，前往**管理员 > Apple Configurator**。
2. 打开注册设备切换开关。
3. 单击下列选项之一：
    - **默认用户的 plist**
    - **具体用户的 plist**- 输入具体用户的用户名或电子邮件 ID。

在 Apple Configurator 中，转至**准备 > 应用。**

5. 转到**准备 > 设置并禁用监督**。
6. 在“更新 iOS”中选择**“从不更新设备”**选项。
7. 单击**准备**（Apple Configurator 底部）。
   在设备签入后，应用程序将在设备上“已安装”的应用程序列表中可见。

使用 UEM 服务器安装应用

要使用 UEM 服务器安装应用：

1. 从“应用程序”选项卡的内部存储上传应用程序。
2. 选择应用。
3. 单击**应用配置**选项卡。
4. 选择**在设备上安装**。
   完成配置设置。
5. 选择**操作 > 强制签入**。

最终用户需要做什么

Apple 要求最终用户至少启动一次 Go，否则 Ivanti Neurons for MDM 位置功能将无法正常运行。 这用于确保最终用户知晓其位置已被追踪。

警告：如果设备使用配置器在单一应用模式中部署，则此方法不可以使用。

如果您未看到**安装 Apple Configurator** 页面，这可能是您没有所需权限。 您需要以下角色之一：

- 系统管理
- 系统只读

12.3.2. 账户驱动型注册

本节适用于账户驱动型用户和设备注册。

支持的设备

- 运行 iOS 15+（针对账户驱动型用户注册）和 iOS17+（针对账户驱动型设备注册）的设备
- 运行 macOS 14+ 的设备
- 运行 visionOS 1.1+ 的设备

先决条件:

账户驱动型用户注册

- Ivanti Neurons for MDM 中使用托管 Apple ID 的用户账户（Apple 商务管理或 Apple 校园教务管理中的用户）。
- 在 **Apple 注册**部分下，从**选择 Apple 注册类型**下拉列表中选择**用户注册**。
- 在**用户 → 用户设置**下，将**设备所有者设置**设置为**开启**，然后选择**用户所有**选项。

账户驱动型设备注册

- Ivanti Neurons for MDM 中使用托管 Apple ID 的用户账户（Apple 商务管理或 Apple 校园教务管理中的用户）。
- 在 **Apple 注册**部分下，从**选择 Apple 注册类型**下拉列表中选择**设备注册**。
- 在**用户 → 用户设置**下，将**设备所有者设置**设置为**开启**，然后选择**公司所有**选项。

适用于 iOS 15+、macOS 14+ 和 visionOS 1.1+ 设备的**账户驱动型用户注册**是专供企业实施 BYOD（自带设备）而设计的注册选项。 帐户驱动的用户注册是 MDM 协议和 Apple 商务管理的用户注册的修改版本；该版本更注重用户隐私，并以企业所需的安全级别进行实施。

适用于 iOS 17+、macOS 14+ 和 visionOS 1.1+ 设备的**账户驱动型用户注册**是专供企业注册公司所有设备/企业设备而设计的注册选项。 账户驱动型用户注册采用 MDM 协议和 Apple 商务管理的用户注册，更注重用户隐私，也更能满足企业的安全要求。 最终用户可以使用“设置”中的“工作账户”功能注册设备。

设置发现服务

如果您的企业有企业域名，例如 acme.com，则您设备的电子邮件 ID 为 devicename@acme.com。

1. 用户输入 username@acme.com 即可登录工作或学校账户，然后设备向 URL 发出 HTTP GET 请求调用：
   https://acme.com/.well-known/com.apple.remotemanagement?user-identifier=user@acme.com
   有关详细信息，请参阅 - https://developer.apple.com/documentation/devicemanagement/discover_authentication_servers
2. 在 acme.com 域上，为 URI - /.well-known/com.apple.remotemanagement 配置重定向规则，将其重定向到以下 URL：
   https://<n-MDM cluster>/.well-known/com.apple.remotemanagement

针对账户驱动型设备注册的简化服务发现

> 适用于 iOS 18.2+、macOS 15.2+ 和 visionOS 2.2+ 设备。

对于账户驱动型注册，当用户输入其组织电子邮件以登录工作或学校账户时，设备首先会搜索组织域中已知的 HTTP 资源，其包含指向 MDM 注册 URL 的链接。

步骤

1. 登录工作或学校账户。
2. 在 **Apple Business Manager** 和 **Apple School Manager** 中验证域 - 仅适用于已在 Apple Business Manager 或 Apple School Manager 中进行验证的域。 如果已验证域，则设备可以向 Apple Business Manager/Apple School Manager 确认以获取备用 MDM 注册 URL。
3. 为 **Mac**、**Apple Vision Pro**、**iPhone** 和 **iPad** 平台类型设置默认 Ivanti Neurons for MDM 分配。
   要设置默认设备分配，请按照下列步骤操作：
   1. 在 **Apple Business Manager** / **Apple School Manager** 中，使用具有管理员或设备注册管理员角色的用户身份登录。
   2. 在侧边栏底部选择您的姓名，选择首选项，然后执行以下操作之一：
      - 选择设备管理服务下方的设备管理服务分配，然后选择默认设备管理服务分配旁边的编辑。
      - 在设备管理服务下选择现有服务，然后在默认设备分配下选择更改。
   3. 如果没有任何其他已配置的设备管理服务，请将所有自动设备分配更改为所选服务，然后选择**保存**。
4. 在 Ivanti Neurons for MDM 控制台上，导航至**管理员** > **Apple** > **设备注册**。 在**设备注册**屏幕中，已添加 **ADDE URL** 和 **ADDE URL SET TIME** 列。

> **首选**：设备检查组织域中的已知 HTTP 资源。

回退选项：如果第一种方法失败，设备会联系 Apple ABM/ASM 以获取 Ivanti Neurons for MDM 指定的其他目标。

5. 在**操作**下，选择**配置 ADDE URL**。
6. 刷新页面。

设备用户说明

本主题介绍设备用户在注册“账户驱动型用户注册”或“账户驱动型设备注册”时需要采取的操作。

步骤

1. 在设备上，按以下步骤之一操作：
   - 对于 **iOS** 设备 - **设置** > **通用** > **VPN**和**设备管理**。
   - 对于 **macOS** 设备 - **系统设置** > **隐私和安全** > **配置文件**。
   - 针对 **visionOS** 设备 - **设置** > **通用** > **VPN** 和**设备管理**。
2. 转到**登录工作或教务帐户**。
3. 键入工作或教务帐户电子邮件地址。 请确保电子邮件地址符合以下格式：
   username@<enterprise domain name>，例如 username@acme.com。
4. 登录页面会自动获取托管 Apple ID，并指导用户完成 iReg 流。 确保输入 Ivanti Neurons for MDM 凭据。
5. 键入工作或教务帐户凭据，并单击**继续**。
6. 在第 2 重身份验证后，设备注册完成。

12.3.3. 设备注册

设备注册是 Apple Business Manager 的一部分，其支持客户批量购买设备，并在激活过程中自动将这些设备注册到 MDM。 如果选择参与，您可以将 Ivanti Neurons for MDM 用作管理这些设备的 MDM 服务器。 有关更多信息，请查看 https://business.apple.com/。

将 Ivanti Neurons for MDM 连接到设备注册

要将 Ivanti Neurons for MDM 用作设备注册的 MDM 服务器，请在 Ivanti Neurons for MDM 中设置 Apple Business Manager 服务器令牌。

对于每个 Apple 商务管理服务器，请在 Ivanti Neurons for MDM 中执行以下操作：

- 测试连接
- 添加设备注册配置文件
- 下载公用密钥
- 设备注册完全同步 - 启动完全同步。 这可能需要一段时间，才可以完成。 在同步完成后，您可以在上次同步列中查看信息。 如果正在进行，您无法启动完全同步。

> Ivanti Neurons for MDM 在 DEP 服务器同步失败时通知管理员，从而更容易识别问题。 如果删除 DEP 服务器，系统也会删除其相关通知。

- 上传新令牌
- 删除

> 现在，**编辑身份验证**和**分配设备注册设备属性**操作对设备注册配置文件可用，而非设备注册（MDM 服务器）。

程序

1. 转到**管理** > **Apple** > **设备注册**。
2. 单击**下载密钥**。
3. 保存 Ivanti Neurons for MDM 密钥。
4. 单击 **business.apple.com**。
5. 使用具有设备注册资格的 Apple 凭据登录。
6. 在 Apple 设备注册站点上：
7. 在 Ivanti Neurons for MDM 中，单击**上传**。
8. 单击**入门指南**。
9. 选择受信电话，以用于对 Apple 服务进行身份验证。
10. 输入发送至所选手机的验证码。
11. 单击**添加 MDM 服务器**。
12. 输入名称，以识别服务使用的虚拟 MDM 服务器。
13. 单击**下一步**。
14. 上传此前下载的公钥。
15. 单击**下一步**
16. 单击**您的服务器令牌**，下载令牌。

17. 单击**完成**。
18. 单击**下一步**。
19. 选择身份验证选项：

- **提示用户注册/登录**

> 不支持使用 visionOS 平台运行的设备。 应使用**跳过用户登录**来注册设备。

> 系统将提示用户输入用户名和密码。 用户可以为密码字段输入密码或 PIN。 对于 macOS 15+ 设备，支持密钥的身份提供者上的 iDP 用户还可使用 **Face ID**、**Touch ID** 或**安全密钥**等其他选项。 可以在**用户** > 用户设置中（与身份验证相关的设置）配置密码和 PIN 首选项。

- **跳过用户登录**

> 对于分配到无人用户（匿名）或定义用户的设备，稍后可从**设备**页面重新分配到特定用户。

选择下列选项之一：

  - **定义一个用户，以便将所有设备分配给**
  - **将所有设备分配给匿名用户**

10. 选定选项会覆盖用户设置下方的选择。

点击**上传**，安装步骤 3 中接收的密钥。

11. 填写显示的表单，以定义设备注册设备的配置文件：
12. 定义设备激活期间用户可以针对下列设置选项跳过哪些步骤：

设置	采取何种措施
名称	输入可识别此设备注册配置文件的名称。
说明	输入配置文件的描述。
部门	输入与此配置文件关联的组织中的部门。
受监控模式 iOS 17+	启用对配置和限制的附加管理控制。 对于 iOS 13+ 和 macOS 10.15+ 设备，此选项会默认启用。 **用于注册的操作系统版本** • **注册时需要具备最低操作系统版本**：管理员可以设置设备注册所需的最低操作系统版本。 如果设备不符合最低操作系统版本条件，系统会提示用户升级到所需版本。 如果用户拒绝升级，将被阻止注册。 **最新版本**：管理员可以为设备注册设置最新的操作系统版本。 如果设备不符合最新操作系统版本条件，系统会提示用户升级到所需版本。 如果用户拒绝升级，将被阻止注册。 **特定版本**：管理员可以设置设备注册所需的最低操作系统版本。 如果设备不符合最低操作系统版本条件，系统会提示用户升级到所需版本。 如果用户拒绝升级，将被阻止注册。 • **最低 iOS 版本**：如果内部版本与“**OSVersion**”键中指定的操作系统版本不一致，则操作系统版本优先。 • **最低内部版本**：如果内部版本与“**OSVersion**”键中指定的操作系统版本不一致，则操作系统版本优先。 如果您输入的内部版本号不正确，则此字段是可选的。 • **消息**：适合显示给用户的软件的说明 如果需要， ◦ 客户端将尽量尝试显示该消息，但可能会 ◦ 因为本地情况而无法显示。 作为惯例，应该添加该消息。 • **将设备添加至 Beta 版程序** **iOS 的测试版程序**：在自动设备注册期间在 iOS 上强制执行测试版软件版本。
macOS 14+	**用于注册的操作系统版本** • **注册时需要具备最低操作系统版本**：管理员可以设置设备注册所需的最低操作系统版本。 如果设备不符合最低操作系统版本条件，系统会提示用户升级到所需版本。 如果用户拒绝升级，将被阻止注册。 **最新版本**：管理员可以为设备注册设置最新的操作系统版本。 如果设备不符合最新操作系统版本条件，系统会提示用户升级到所需版本。 如果用户拒绝升级，将被阻止注册。 **特定版本**：管理员可以设置设备注册所需的最低操作系统版本。 如果设备不符合最低操作系统版本条件，系统会提示用户升级到所需版本。 如果用户拒绝升级，将被阻止注册。 • **最低 macOS 版本**：如果内部版本与“**OSVersion**”键中指定的操作系统版本不一致，则操作系统版本优先。 • **最低内部版本**：如果内部版本与“**OSVersion**”键中指定的操作系统版本不一致，则操作系统版本优先。 如果您输入的内部版本号不正确，则此字段是可选的。 • **消息**：适合显示给用户的软件的说明 如果需要， ◦ 客户端将尽量尝试显示该消息，但可能会 ◦ 因为本地情况而无法显示。 作为惯例，应该添加该消息。 • **将设备添加至 Beta 版程序** **macOS 的测试版程序**：在自动设备注册期间在 macOS 上强制执行测试版软件版本。

设置	采取何种措施
自动下载和安装 iOS 更新	（仅限 iOS 9.0+）如果在设备的**设置 > iTunes 和 App Store** 中选择了“自动下载”选项，即使关闭“设备注册配置文件”选项，操作系统更新也将自动下载，但不会安装。 当系统包含适用于设备注册已注册的受监管设备的 iOS 软件更新配置时，将优先考虑此设置。 此设置中的任何变更将适用于设备注册已注册的受监管设备，甚至无需重置设备。
MDM 可删除	定义用户是否无法在设备注册后从 MDM 取消注册。 此设置不适用于共享 iPad。
MDM 强制	定义用户是否无法在激活过程中跳过 MDM 安装。 对于 iOS 13+ 和 macOS 10.15+ 设备，此选项会默认启用。
不使用备份中的配置文件 允许配对	启用后，当您从备份恢复设备时，设备不会使用此配置文件。 仅适用于 iOS 26+ 和 visionOS 26+ 设备。 （不适用于 iOS 13+ 和 macOS 10.15+）允许主机配对功能，例如 iTunes 同步。 始终允许具备有效配对证书的主机进行配对。
恢复服务 证书 支持电话号码	将**恢复服务**设置为 **True**，以确保在执行**返回服务**操作时保留应用程序。 这允许设备拍摄应用程序的快照，并在“返回服务”过程中提供更快的体验。 如果禁用，设备仍然可以执行“返回服务”，但必须在重新注册过程中再次下载应用程序。 要利用 **Apple Migration ABM** 功能，需要禁用此功能。 如果**恢复服务**设置为 **True**，则无法迁移设备。 仅适用于 iOS 26+ 和 visionOS 26+ 设备。 单击 **+ 添加**以便上传证书。 为设备用户提供可联系帮助的电话号码。
支持电子邮件地址	提供设备用户可以联系以获取帮助的电子邮件地址。
自定义注册	（iOS 13.0+ 和 macOS 10.15+）创建自定义注册 Web 页面。 指定您自己的自定义 Web 页面（Web 视图），以在 Device Enrollment 期间对用户进行身份验证。 使用此页面，以显示自定义信息，例如身份验证类型、品牌化、同意文本和隐私策略。 请在此步骤后查看“*添加自定义设备注册 Web 页面*”部分，以了解更多详细信息。 • 选择**启用自定义注册**，以启用此功能。 • 输入 **URL**，例如 https://mycustomweburl.com。 此 URL 定义自定义 URL 的值，以在 Web 视图中向用户显示。
多用户	(iOS 13.4+) 共享 iPad 企业版 支持企业在多名员工之间共享设备，并仍提供个性化体验。 选择**多用户模式**，以在设备上启用共享 iPad。 有关详细信息，请参阅共享 iPad 企业版。 • 此设置不适用于 Apple 教育。 • 选择**受监管模式**设置，以修改多用户设置。
配额大小	(iOS 13.4+) 共享 iPad 企业版。 该值以兆字节 (MB) 为单位，表示设备中为用户分配的存储空间。 如果该值太小，设备将分配默认配额大小。

设置	采取何种措施
常驻用户	(iOS 13.4+) 共享 iPad 企业版 值表示可在设备上保留或驻留的用户数量。 如果值大于设备支持的最大用户数量的值，MDM 服务器将使用该值（最大用户数量）作为默认值。 管理员可以提供配额大小或常驻用户值。 如果提供两个值，MDM 服务器将使用配额大小作为默认值。
用户会话超时 临时会话超时	(iOS 14.5+) 共享 iPad 企业版 显示用户会话的超时（以秒为单位）。 用户会话将在指定的不活动时段后自动注销。 最小值是 30 秒。 将此值设置为 0 会移除超时，并设置为设备默认超时。 1 至 29 之间的值无效。 在设置时，设备将设置为默认超时。 (iOS 14.5+) 共享 iPad 企业版 显示访客或临时会话的超时（以秒为单位）。 临时会话将在指定的不活动时段后自动注销。 最小值是 30 秒；将此值设置为 0 会移除超时，并设置为设备默认超时。 1 至 29 之间的值无效。 在设置时，设备将设置为默认超时。
仅限临时会话	(iOS 14.5+) 共享 iPad 企业版 若为真，用户仅可看到“欢迎来宾”窗格，并仅以来宾用户身份登录。 若为假，用户可以使用受管 Apple ID 登录（现有行为）。 默认：假
受管 Apple ID 默认域	(iOS 16.0+) 共享 iPad 企业版 指定域列表。 用户可使用 QuickType 键盘在域列表中选择他们的帐户域。
在线身份验证宽限期	(iOS 16.0+) 共享 iPad 企业版 指定用户可以在不连接网络的情况下登录的天数。 如果将该值设置为 0，用户在每次登录时都需要进行在线身份验证。 **默认值**：0
自动锁定时间	(iOS 17.0+) 指定在经过多少时间后设备进入睡眠模式（以秒为单位）。 最小值为 120 秒。
通行码锁定宽限期	指定在经过多少时间后设备用户必须输入设备密码才能解锁（以秒为单位）。 最小值为 0 秒，最大值为 14400 秒。
时区	指定设备必须属于哪个时区。 **例如**：Pacific/Midway

设置选项
• 跳过输入密码 - 选择此选项将自动启用“跳过 Apple Pay”设置和“跳过 Touch ID” • 跳过定位服务 • 跳过从备份还原 • 跳过从 Android“转到 iOS” • 跳过服务条款 • 跳过登录 Apple ID 和 iCloud - 选择此项将自动启用跳过 Apple Pay 设置。 • 跳过触控 ID 设置（仅限 iPhone 5s、6、6+、iPad Air 2、iPad Mini 3）- 选择此项将自动启用跳过 Apple Pay 设置。 • 跳过 Apple Pay 设置（仅限 iPhone 6、6+、iPad Air 2、iPad Mini 3） • 跳过缩放设置 • 跳过 Siri • 跳过 Intelligence（iOS 18+ 和 macOS 15+） • 跳过诊断信息自动发送 • 跳过 Cloud 存储（iOS 10.3+ 和 macOS 10.13.4+） • 跳过显示音调设置（iOS 9+ 和 macOS 10.14+） • 跳过主页按钮灵敏度 • 跳过键盘选择屏幕 • 跳过培训信息屏幕 - 此信息适用于用户教育。 例如：封面、多任务和控制中心。 • 跳过 Apple Watch 迁移的屏幕 • 跳过选择外观屏幕（iOS 13.0+ 和 macOS 10.14+） • 跳过屏幕时间 (iOS 12.0+ & macOS 10.15+) • 跳过隐私（macOS 10.13.4+ 和 tvOS 11.3+） • 跳过启用锁定模式（iOS 17.1+ 和 macOS 14.0+） • 跳过软件更新（iOS 12.0+ 和 macOS 15.4+） • 跳过添加手机计划窗格（iPhone Xs、iPhone Xs Max、iPhone XR） • 在登录页面上显示自定义文本 - 选择此选项，以在文本框中输入自定义文本消息。 此消息将在设备注册设置期间显示在设备的登录页面上，以向最终用户提供任何额外说明，从而在流程期间提供帮助。 • 自动前进设置 - 选择此选项，以便设置助手在设备设置屏幕上自动前进。 默认设置为假。 支持 tvOS 和 macOS 11 及更高版本。 自动前进设置不支持 WiFi 连接，设备应使用以太网进行连接。 • 称谓语 - 跳过称谓语窗格。 (iOS 16+) • 跳过 Liquid Glass 窗格 (iOS 27.0+ & macOS 27.0+)
iOS
• 跳过开始使用窗格 (13.0+) • 跳过 iMessage 和 FaceTime (12.0+) • 跳过 Spoken Language (13.0+) • 跳过还原已完成 (14.0+)

设置选项
• 跳过更新已完成 (14.0+) • 跳过 Safety (16.0+) • 跳过操作按钮设置窗格 (17.0+) • 跳过 Web 内容筛选窗格 (18.2+) • 跳过安全和处理窗格 (18.4+) • 跳过多任务窗格 (26.0+) • 跳过操作系统展示窗格 (26.0+) • 跳过无障碍功能状态窗格 (27.0+)
macOS
• 跳过 iCloud 分析屏幕 • 跳过 True Tone Display 屏幕 (10.13.6+) -（可选）选择此选项可跳过 True Tong Display 窗口。 • 跳过无障碍 (11.0+) • 跳过使用手表解锁 (12.0+) • 跳过启用锁定模式 (14.0+) • 跳过壁纸选择 (14.1+) • 跳过其他设置隐私窗格 (26.0+) • 跳过更新已完成 (26.0+)
tvOS • 跳过 Apple TV 主屏幕布局同步屏幕 • 跳过 Apple TV 提供商登录屏幕 • 跳过点击设置选项 • 跳过 Aerial Screensaver 设置 **macOS 账户设置助手选项** • 跳过管理员账户创建 • 跳过主要设置账户创建 • 以常规用户身份创建主账户（如果未选中，则以管理员身份进行创建） 在设备注册设置期间等待设备配置 • 等到配置和高优先级应用程序推送到设备 - 选择将配置和高优先级应用程序推送到设备，然后再继续其余的设备注册设置步骤。 此设置将禁止最终用户在所需配置和高优先级应用程序推送到设备之前使用设备。 • 时间限制 - 默认时间限制为 3 分钟。 最长时间为 10 分钟。 要启用此功能，在编辑设备注册配置文件时选择**受监管模式**选项。

单击**保存**。

将填充**管理员** > **Apple** > **设备注册**页面中的下表：

设置	采取何种措施
名称 （点击列标题以按字母数字排序。） 使用“搜索”字段搜索此列中的项目	MDM 服务器名称
Apple 帐户名 （点击列标题以按字母数字排序。） 使用“搜索”字段搜索此列中的项目	受管 Apple ID
设备数量	已分配的设备计数
注册配置文件	已分配的设备注册配置文件计数
上次同步时间 （点击列标题以按字母数字排序。）	上次联系时间
令牌到期 （点击列标题以按字母数字排序。）	令牌到期日期

- 当新设备加入“Apple 设备注册”时，Ivanti Neurons for MDM 可能需要 15 分钟才可以发现这些新设备。 随后分配给新设备登记配置文件。 如果您无法将新设备加入设备注册，请转到**仪表板 > 通知**，以查看 Apple 针对设备注册发出的通知。 如果存在任何 EULA 更新，您将通过电子邮件收到详细步骤的通知，以便接受新 EULA。
- 您可以查看租户中存在的所有自定义设备属性，并在注册期间通过 Apple 设备注册将其分配到设备。
- 在共享 macOS 设备中，ListUsers 命令将显示设备上所有本地用户的列表，并且只显示注册设备的用户的上次签入详细信息。

编辑设备注册配置文件

程序

1. 转到**管理** > **Apple** > **设备注册**。
2. 在 Apple 帐户名称列中，查找 Apple 商务管理服务器的名称（您已在 Apple 网站上创建）。
3. 单击注册配置文件列中的数字链接。
4. 对于特定配置文件，选择**操作** > **编辑设备注册配置文件**。
5. 更新并保存配置文件。

- 如果编辑设备注册配置文件，已修改配置文件的设备计数将很快更新。
- 如果您刷新 Apple 站点上的服务器令牌，现有令牌将无效。 但在上传新令牌前，在“设备注册”页面中显示的令牌（含令牌过期日期）仍有效。
- 如果创建或编辑了设备注册配置文件，则可以在“审计试验”部分查看对配置文件所做的更改。 单击“详细信息”下的链接时，可以查看“属性”，以及“之前”和“之后”列下对属性所做的更改。 您可以注意到每个设备注册配置文件的状态为“已创建”（用于新建配置文件）、“已更新”（用于编辑任何现有配置文件）或“已删除”（用于删除任何现有配置文件）。 要筛选审计跟踪下的设备注册配置文件，您需要选择管理系统作为类别，并选择自动化设备注册类型作为类型。

设备注册配置文件包含以下详细信息：

设置	采取何种措施
配置文件名称 （点击列标题以按字母数字排序。）	输入可识别此设备注册配置文件的名称。
描述 （点击列标题以按字母数字排序。）	输入配置文件的描述。
部门 （点击列标题以按字母数字排序。）	输入与此配置文件关联的组织中的部门。
支持电话号码 （点击列标题以按字母数字排序。）	为设备用户提供可联系帮助的电话号码。
设备数量	显示配置文件的设备数量
操作	管理配置文件

管理多个设备注册配置文件

对于每个 Apple 商务管理服务器，您可以创建多个设备注册配置文件。 这样，不同设备组可以收到不同配置。 设备也可以从一个设备注册配置文件移到另一个设备注册配置文件。

程序

1. 转到**管理** > **Apple** > **设备注册**。
2. 在 Apple 帐户名称列中，查找 Apple 商务管理服务器的名称。
3. 单击注册配置文件列中的数字链接。
4. 要创建与选定服务器关联的新设备注册配置文件，单击**创建新配置文件**。 创建并保存配置文件。
5. 要管理每个配置文件，单击**操作**，并选择以下其中一个选项：
   - **设置为默认配置文件** - 将配置文件设置为相同虚拟服务器中的默认配置文件。 新设备注册将收到此默认配置文件。
   - **编辑配置文件** - 更新现有配置文件。
   - **编辑身份验证** - 编辑设备注册身份验证设置。
   - **分配设备注册设备属性** - 管理员可以使用设备的自定义属性，以将其他属性与这些对象关联。 随后可以使用这些属性构建组或分发配置。
   - **删除** - 默认配置文件无法删除。 在删除非默认配置文件时，所有关联设备将重新分配到默认配置文件。

6. 要将已注册设备从相同虚拟服务器中的一个配置文件移到另一个配置文件（而非在不同 Apple 商务管理服务器之间），单击设备数量列中的数字链接。 配置文件的重新分配适用于还未注册的设备。
    1. 要移动 1 个设备，单击特定设备的**分配注册配置文件**，从下拉列表中选择配置文件，并单击**分配**。
    2. 要移动多个设备，选择设备，并单击**操作** > **分配注册配置文件**，从下拉列表中选择配置文件，并单击**分配**。

- 如果编辑设备注册配置文件，已修改配置文件的设备计数将很快更新。
- 如果您刷新 Apple 站点上的服务器令牌，现有令牌将无效。 但在上传新令牌前，在"设备注册"页面中显示的令牌（含令牌过期日期）仍有效。

添加自定义 Device Enrollment Web 页面

适用于：iOS 13.0 和 macOS 10.15，以及支持的较新版本

在 Custom Enrollment 部分中，您可以指定自己的自定义 Web 页面（Web 视图），以在 Device Enrollment 期间对用户进行身份验证。 使用此页面，以显示自定义信息，例如身份验证类型、品牌化、同意文本和隐私策略。

程序

1. 转到**管理** > **Apple** > **设备注册**。
2. 查找您在 Apple 站点上创建的服务器名称。
3. 选择**操作** > **编辑设备注册配置文件**。
4. 在自定义注册部分中，选择**启用自定义注册**。
5. 选择下列选项之一：
    - **MobileIron 托管网页** - 如果注册正在使用身份提供商，例如 Microsoft Active Directory 联合身份验证服务 (ADFS) 或 Okta，重定向到身份提供商 (IDP)。 对于使用基于非 IDP 的身份验证的 Ivanti Neurons for MDM 用户，这也可以重定向到自助服务门户。
    - **自定义 URL** - 输入 URL，例如 https://mycustomweburl.com。 此 URL 定义自定义 URL 的值，以在新 Device Enrollment 设备或擦除的设备的初始设置期间加载的 Web 视图中向用户显示。 使用此字段，以使用身份验证方法定义您自己的身份验证 UI。 在用户经过身份验证后，将下载 MDM 注册配置文件。

自定义 Device Enrollment Web 页面的工作流

此部分会详述自定义 Device Enrollment Web 页面的行为和步骤，以创建自定义 Web 页面（Web 视图）。

当在 **URL** 字段中指定的自定义 Web 页面开始加载时，

- 配置 Web URL 具有 **https** 模式，并且是 **GET** 请求。 Web 页面应使用公开受信的证书。
- 自定义标头 **x-apple-aspen-deviceinfo** 会由启动注册的 Apple 设备附加到 GET 请求。 其中包含 CMS（加密消息语法）信封的 base64 编码，并包括具有设备属性的 plist。 对于初始 POST 请求中基于令牌的 Device_Enrollment 提供的信息，这与其内容相同，并且格式相同。

当自定义 Web 页面随后加载时：

- 在管理员的主机服务器向客户端提供 **custom.mobileconfig** 文件之前，设备用户会与 Web 页面（Web 视图）进行交互。 Ivanti Neurons for MDM 服务器会返回 MDM 配置文件的字节码。 在管理员的主机服务器中，custom.mobileconfi 文件应使用 **application/x-apple-aspen-config** 的 MIME 类型进行设置，这样设备的 MDM 配置文件会下载并安装到设备。

- 为与 Ivanti Neurons for MDM 进行身份验证，Web 页面应包含身份验证用户名和密码凭据。 建议在 Ivanti Neurons for MDM 中创建单独的用户，并将“自定义注册”角色分配给使用 Ivanti Neurons for MDM 服务器 URL 获取 MDM 配置文件的用户（例如，https://micloudDomain.com/c/i/dep/custom.mobileconfig）。
- 为注册设备并从 Ivanti Neurons for MDM 获取 MDM 配置文件，管理员的主机 Web 服务器应对 Ivanti Neurons for MDM 服务器 URL 进行 POST 调用。 在设备点击 GET URL 加载自定义 Web 页面时，也应传输标头 x-apple-aspen-deviceinfo 及设备提供的值。 如果未提供注册用户 ID，设备会注册到无人用户。 以下是额外详细信息：
  - 当设备点击在 Device Enrollment 配置文件中配置的自定义 Web URL 时，管理员的主机 Web 服务器应捕获设备显示的标头“x-apple-aspen-deviceinfo”。
  - 要获取该设备及其相关用户的 MDM 配置文件，管理员的主机 Web 服务器应对标头 x-apple-aspen-deviceinfo 的 Ivanti Neurons for MDM 服务器 URL 进行 POST 调用。 其中应包含基本身份验证，即使用 Ivanti Neurons for MDM 用户 ID 作为请求参数（例如 https://miCloudDomain.com/c/i/dep/custom.mobileconfig?user=name@company.com）。 应为用户分配自定义注册角色。
  - 在管理员的主机 Web 服务器收到字节码后，通过设置响应标头 Content-Disposition = attachment;filename="profile.mobileconfig" 和 Content-Type = application/x-apple-aspen-config，将字节码下载到设备。
- Web 视图会关闭，OS 会尝试安装配置文件，即必须是 MDM 注册配置文件。

> Ivanti Neurons for MDM 不会对返回 MDM 配置文件的用户 ID 进行身份验证。 因此，在请求 MDM 配置文件之前，管理员应对用户 ID 执行必要的身份验证。

对于 iOS，在擦除的设备的初始设置期间，支持此工作流。 对于 macOS，如果在设置助手期间跳过 Device Enrollment，设置助手及配置文件首选项窗格会支持此工作流。

如需创建自定义 Web 页面相关的开发人员信息，请查看以下 Apple 文档参考：

- **Web 视图**
- **通过 Web 视图进行身份验证**
- **实施可查看网站桌面或移动版本的简单 iPad Web 浏览器的示例代码**

编辑设备注册身份验证设置

程序

1. 转到**管理** > **Apple** > **设备注册**。
2. 查找您在 Apple 站点上创建的服务器名称。
3. 选择**操作** > **编辑身份验证**。

移动帐户的启动令牌管理

适用于：macOS 10.15 设备和使用 Apple 教务管理系统或 Apple 商务管理在 MDM 中注册设备的支持的较新版本。

Ivanti Neurons for MDM 支持移动帐户的启动令牌管理。 启动令牌支持移动帐户登录使用 FileVault 的 macOS 设备。 使用此功能，所有登录的移动帐户将自动获取 SecureToken。 在多个用户登录加密计算机时，此功能非常有用。

在受管管理员帐户尝试登录到设备时：

- 对于首次登录，从 MDM 服务器请求启动令牌。
- 如果 MDM 服务器提供启动令牌，设备将为该帐户自动创建 SecureToken。

- 设备会为用户启用 FileVault。

启动令牌可用是在设备详细信息页面中可用的字段，并在创建新设备组或自定义策略时用作筛选器属性。

出于故障排除和验证目的，转到设备的设备详细信息页面。 使用日志页面，以使用基于操作名称设置启动令牌和获取启动令牌的筛选器，缩小设备日志。

使用设备注册设置受管 macOS 管理员帐户

Ivanti Neurons for MDM 支持重置为出厂默认设置或首次激活的设备注册进行注册。 使用设备注册，在 macOS 设备上创建管理员帐户。 Ivanti Neurons for MDM 仅支持 macOS 的可选注册，因此，Ivanti Neurons for MDM 会忽略设备注册配置文件中的 **MDM 强制**字段，因为它仅适用于 iOS 设备。

程序

1. 转到**管理员 > Apple > 设备注册**。
2. 查找您在 Apple 站点上创建的服务器名称。
3. 选择**操作 > 编辑设备注册配置文件**。
4. 从 macOS 账户设置助手选项中选择以下选项之一：
   - **跳过管理员账户创建** - 选择此选项，可禁止创建管理员账户（可见或隐藏）。 取消选择此选项，以在**设置托管的 macOS 管理员帐户**部分中创建管理员帐户（如下所述）。
   - **跳过主设置账户创建** - 选择此选项可以跳过设置 macOS 设备上的主账户。 除了管理员账户之外，没有创建用户账户。 将显示其他部分 - **设置托管 macOS 管理员账户**，以创建托管 macOS 管理员账户。 账户也可以从用户和组中隐藏。
   - **以常规用户身份创建主账户（如果未选中，则为管理员）** - 选择此选项可以创建非管理员标准账户，作为注册的一部分。 管理员仍可以创建管理员账户，并将其推送到设备。 将显示其他部分 - **设置托管 macOS 管理员账户**，以创建托管 macOS 管理员账户。 账户也可以从用户和组中隐藏。

选择上述选项之一后，如果您想创建托管 macOS 管理员帐户，请在**设置托管 macOS 管理员帐户**部分中输入以下详细信息：

- 全名
- 账户名
- 密码
- 确认密码
- （可选）在用户和组中隐藏托管管理员账户

如果您未选择**跳过主要设置帐户创建**，请在**设置主帐户**部分中输入以下详细信息。 通过将托管本地用户简短名称设置为管理员的简短名称，这会增加对托管管理员帐户的用户渠道支持。

- **全名**
- **简短名称**
- （可选）**防止最终用户修改** - 如果全名和/或简短名称拥有替换变量并评估为空，将覆盖此设置。 如果您选择此选项，请确认您了解仅在以下其中一个选项正确设置时，此主管理员帐户设置才适用：
  1. 在身份验证设置视图中选择提示用户注册/登录。
  2. 选择 MobileIron 托管的网页进行注册自定义。

7. 选择**跳过主要设置帐户创建**，以为受管管理员帐户启用用户渠道支持。 您可以将托管本地用户简短名称设置为管理员的简短名称。
8. 单击**保存**。

更改本地 macOS 管理员账户密码

对于设置助手在设备注册期间创建的本地 macOS 管理员帐户，管理员可以更改其本地密码。

适用于：macOS 10.11 或支持的较新版本。

程序

1. 转到**设备**。
2. 单击与设备相关联的用户名，查看设备详细信息页面。
3. 从操作菜单中，单击**设置 macOS 管理员密码**。此外，选择一个或多个设备，也可以在设备列表页面中执行此操作。
4. 输入密码。
5. 单击**保存**。

导出到 CSV

Ivanti Neurons for MDM 允许将已注册的设备导出到 CSV 文件。

程序

1. 转到**管理** > **Apple** > **设备注册**。
2. 点击**设备数量**列下的特定设备计数链接。
3. 点击**导出到 CSV** 选项，可将设备列表和相关详细信息导出到 CSV 文件。 报告就绪后，您将收到下载或删除报告的提示消息。 您还将收到一封电子邮件，其中包含下载报告的链接。
4. 点击**下载**。
5. （可选）点击**删除**可删除报告。

12.3.4. 测试版注册

如果设备受监管且运行 iOS 18、iPadOS 18、macOS 15 或更高版本，Ivanti Neurons for MDM 可以在稍后时间自动远程注册设备。 如有必要，可以从 Beta 版程序中删除受监督设备，并限制用户手动注册。 这样用户就无需执行手动步骤，并且可以在整个 Beta 版测试生命周期中简化流程。

先决条件

- “设备注册”是“Beta 版注册”的必要条件。 有关“设备注册”的详细信息，请参阅**设备注册**。
- 若要在无需 Apple 帐户的情况下提供 AppleSeed for IT Beta 版，Apple Business Manager 或 Apple School Manager 的管理员必须登录 AppleSeed for IT 门户，并代表其组织针对当前 Beta 版测试期间接受条款和条件。

将 Ivanti Neurons for MDM 连接到“Beta 版注册”

要将 Ivanti Neurons for MDM 用作“Beta 版注册”的 MDM 服务器，请在 Ivanti Neurons for MDM 中设置 Apple Business Manager 或 Apple School Manager 服务器令牌。

“Beta 版注册”部分

名称	说明
组织名称	组织名称。
上次同步时间	执行同步的日期和时间。
状态	同步的状态。
“Beta 版注册”令牌同步	单击**同步**以同步新的可用测试版注册令牌以进行测试版更新。

12.3.5. 配置设置辅助

可以使用配置设置辅助选择在 iOS 和 macOS 设备设置期间要跳过或包括的设置屏幕。

步骤

1. 登录 Ivanti Neurons for MDM 管理控制台。
2. 转至**配置**。
3. 选择**设置辅助**。
4. 点击铅笔（编辑）图标。
5. 选中复选框，在设备上跳过特定设置屏幕。
6. 单击**完成**。
7. 选择**设备渠道**。
8. 选择**所有设备**。 “设置辅助”配置将推送到设备，“设备详细信息”页面下方的“配置”选项卡显示已安装状态。
9. 登录设备。 系统将跳过所有初始设置屏幕。

12.3.6. 安装 MDM 证书

您必须请求并安装 Apple MDM 证书，以管理 iOS 设备。 您还需要每年对此证书更新一次。 （接近到期日期时，用于创建证书的 Apple 帐户将收到 Apple 网站发送的通知。）使用“MDM 证书”页面来添加或更新此证书。

获取并安装 MDM 证书

程序

1. 使用 **MDM 证书**页面，从 Ivanti Neurons for MDM 租户下载证书签名请求 (CSR)。
2. 将 CSR 上传至 Apple，以创建新证书。
3. 在 Apple 网站，添加说明证书用途的节点。 该节点在更新证书时将对您有所帮助。
   保存更新后的证书。
4. 为 Ivanti Neurons for MDM 租户安装证书。

审查 MDM 证书

程序

1. 单击**更新证书**。
2. 从 Ivanti Neurons for MDM 租户下载证书签名请求 (CSR)。
3. 将 CSR 上传至 Apple，以更新对应的证书。
4. 在 Apple 网站上，确认您更新正确的证书。 将不同的证书上传到 Ivanti Neurons for MDM 将自动停用所有注册的 iOS 设备。
   为 Ivanti Neurons for MDM 租户安装证书。

如果您上传错误的证书，将收到警告。

如果您未看到**安装 MDM 证书**页面，这可能是您没有所需权限。 您需要以下角色之一：

- 系统管理
- 系统只读

12.3.7. 共享 iPad 设备企业版

共享 iPad 设备企业版适用于在 Apple Business Manager 中创建的受管 Apple ID 以及 iOS 13.4 或支持的更新版本。

- 共享 iPad 设备支持企业在多名员工之间共享设备，同时仍然提供个性化体验。
- 员工可以使用受管 Apple ID 登录，以便加载其需要的数据，包括其邮件帐户、文件、iCloud 照片库、应用数据和更多信息。
- 数据存储在 iCloud 中，因此员工可以登录到属于该组织的任何共享 iPad 设备。

共享 iPad 设备可用于医疗、零售和工业应用。 例如，医生和护士可以共享一台 iPad 设备，因为他们可以安全地访问专为其设计的用户配置文件。 在零售店中，授予一线工作者对产品信息、资源、专业知识的访问权限，以为客户提供服务和更卓越的购物体验。

工作方式

- iPad 设备将添加到 Apple Business Manager 中，并使用打开共享模式的自动注册配置文件进行注册。
- 员工使用公司提供的受管 Apple ID 和密码登录共享 iPad 设备。 Apple 商务管理的管理员可以手动为用户创建账户，或者将账户创建与身份提供程序（如 Entra ID）关联。
- 每个用户在登录到共享 iPad 设备时都可以拥有自己的自定义配置文件。 管理员可以根据用户的角色、职责和部门来分发应用。
- 用户可以在共享 iPad 设备上以访客用户身份登录。 默认情况下，访客用户登录处于启用状态。 访客用户不需要使用受管 Apple ID 和密码登录。 可以禁用访客用户登录，在 **iOS 限制**配置中，将**允许共享 iPad 的访客会话**选项设置为 **False** 即可。
- 转到 Ivanti Neurons for MDM **> 设备**，点击共享 iPad 设备名称，然后点击**用户**选项卡查看设备上的用户列表及其详细信息（如受管 Apple ID、以字节计可用数据、以字节计已使用数据、有数据要同步到 Ivanti Neurons for MD）。
- 转到**日志**选项卡，从筛选器选择**报告用户列表**操作，以查看其他用户详细信息。
- 共享 iPad 设备中的访客用户登录名与 Ivanti Neurons for MDM 访客用户管理不同。 来宾用户帐户在 Ivanti Neurons for MDM 中默认禁用。 要在共享 iPad 设备中管理访客用户，请启用访客用户帐户。
- 共享 iPad 设备上的控制中心提供屏幕录制功能。
- Ivanti Neurons for MDM 支持受管 Apple ID 的替换变量，即 `${managedAppleID}`。 系统属性部分和设备属性部分会显示此系统变量。
- Ivanti Neurons for MDM 限制管理员更改过去登录到共享 iPad 设备的常驻用户以及当前登录的用户的受管 Apple ID。 如果您尝试更改受管 Apple ID，则会显示一条错误消息，指出由于用户正在使用共享 iPad 设备，因此无法更改用户的受管 Apple ID。
- 至于 **Apple App 和图书**，将根据基于设备的许可证在共享 iPad 设备上安装 App 和图书，无论是否选择基于设备的许可证。

先决条件

请确保满足下列先决条件：

- 共享 iPad 设备需要受管 Apple ID。 管理员可以手动创建账户，或者与身份提供程序（如 Entra ID）关联。
- 共享 iPad 设备必须包含 iOS 13.4 或支持的较新版本。
- 设备必须关联 Apple Business Manager 帐户。
- 设备必须具有至少 32 GB 的存储容量。

注意以下几点：

- Ivanti Neurons for MDM 限制共享 iPad 设备的某些配置（如密码），因为 Apple 不支持它们。 此类配置不会推送到设备（设备 > 单击设备名称链接 > 配置选项卡）。

- 密码配置不适用于共享 iPad 设备，因为它们需要与密码而非密文关联的受管 Apple ID。 Ivanti Neurons for MDM 管理门户的解锁操作不会清除共享 iPad 设备上的密文。
- 在将 iOS 限制配置分发到共享 iPad 设备期间，选择设备通道或用户通道。 您可以分发单独配置，并强制实施仅适用于设备或用户渠道的限制。
- Ivanti Neurons for MDM 会验证过期帐户，并停用所有者是过期帐户的设备。 但是，对于共享 iPad 设备，设备所有者是最后登录的用户，可能不是合法所有者。 如果所有者帐户过期，Ivanti Neurons for MDM 会将共享 iPad 设备从停用名单中排除。
- 共享 iPad 设备不支持 Go for iOS 客户端。
- 用户无法在共享 iPad 设备上执行停用和擦除等操作。 只有管理员可以从 Ivanti Neurons for MDM 管理门户执行停用和擦除操作。
- 管理员无法从 Ivanti Neurons for MDM 管理门户更改共享 iPad 设备的所有者。
- 共享 iPad 设备不支持零登录。
- 启用 ListUsers 命令时，所有受管用户 ID 及其签入时间都会显示在**管理员**选项卡下的“设备注册”（Apple Business Manager 的一部分）中。

配置共享 iPad 设备

您可以设置共享 iPad 设备并配置设置。

步骤

1. 转到**管理** > **Apple** > **设备注册**。
2. 通过使用自动设备注册配置文件注册设备，将设备添加到 Apple 商务管理。 有关此过程的信息，请查看设备注册。
3. 在设备注册设置中，启用：
   - **受监控模式**。
   - **共享 iPad 设备企业版**下的**多用户模式**。
4. （可选）创建本地用户帐户。 该设备将注册到此用户。 对此用户进行身份验证仅在注册期间发生一次。
5. 重置共享 iPad。

> 注册过程仅在重置后开始。 将设备注册并配置为共享 iPad 设备需要几分钟的时间。

6. 合法所有者会分配到注册设备的用户帐户。 管理员可以从**设备**页面更改法定所有者。
7. 在设备登录屏幕上，输入用户的受管 Apple ID 凭据。
   - 与 macOS 设备类似，您可以通过设备和用户通道在共享 iPad 设备上推送配置。
   - 用户替换变量不能替代通过设备渠道推送的配置（包括受管应用配置）。
   - 如果共享 iPad 设备中的登录用户不是托管用户 - 受管 Apple ID 不属于 Ivanti Neurons for MDM 管理门户中的任何用户，则该设备不会分配给任何人。 用户不受管理，管理员无法从 Ivanti Neurons for MDM 推送用户渠道配置。
   - 默认情况下，禁用由 Ivanti Neurons for MDM 创建的默认来宾用户。 访客用户登录时，不会将设备分配给任何用户，且用户不受管理。 如果访客用户必须受管理，则必须启用 Ivanti Neurons for MDM 创建的默认访客用户，且在访客用户登录后将设备分配给默认访客用户。 然后，用户即会受管理。
   - 设备所有者信息显示在 Ivanti Neurons for MDM > **设备**页面和设备日志（设备详细信息页面 > **日志**）中。

管理共享 iPad 的合法所有者

您可以从设备列表页面使用共享 iPad 设备的电子邮件 ID 搜索和查看其合法所有者。 您可以通过将现有合法所有者重新分配给新的合法所有者来更改共享 iPad 设备的合法所有者。 如果非共享 iPad 设备的合法所有者被重新分配，则 Ivanti Neurons for MDM 忽略该分配。

程序

1. 转到**设备**。
2. 点击齿轮图标，选择**法定所有者**列并将其添加至设备列表页面。
3. 选择共享 iPad 设备。
4. 单击**操作 > 分配到合法所有者**。

向共享 iPad 设备的合法所有者发送电子邮件

您可以向共享 iPad 设备的合法所有者发送电子邮件。

步骤

1. 转到**设备**。
2. 单击共享 iPad 设备的名称。
3. 单击**电子邮件**图标。
4. 撰写电子邮件。
5. 单击**发送**。

使用多用户模式属性

您可以在 Ivanti Neurons for MDM 中使用共享 iPad 设备的“多用户模式”属性。

步骤

1. 在**设备**页面中，使用**多用户模式**属性。
2. 点击**高级搜索**并创建规则，使用**多用户模式**属性查找设备。
3. 在**设备 > 设备组**页面中，使用**多用户模式**属性为共享 iPad 设备创建动态设备组。 例如，您可以将此组用作分发筛选器，以分发配置。
4. 在**策略**页面中，使用**多用户模式**属性为共享 iPad 设备创建自定义策略。
5. 在**应用 > 分发筛选器**中，使用**多用户模式**属性限制可以安装的应用数量。

- 对于 Apple 校园教务管理设备，Ivanti Neurons for MDM 不支持多用户模式。 不建议启用设置，并将设备注册配置文件推送到 Apple 校园教务管理设备。
- iOS 多用户安全登录配置不适用于共享 iPad 设备。

从共享 iPad 设备中删除用户

您可以从共享 iPad 设备中删除一个用户或多个用户帐户。 在“用户列表”选项卡中，将为当前登录用户显示**活动**标签。 删除选项不适用于共享 iPad 设备上当前登录的用户。 可以从**设备**或**用户**选项卡删除用户。

从“设备”选项卡删除用户

步骤

1. 转到**设备**选项卡 > **设备详细信息**。
2. 转到**用户**选项卡。 随即显示用户列表。
3. 点击**删除所有用户**。
4. 点击“**-**”减号可删除特定用户。
    - （可选）在**删除用户**窗口中，选择**强制删除用户，即使有数据要同步到 Ivanti Neurons for MDM** 选项，并点击**是**。

> 选择**强制删除用户，即使有数据要同步到 Ivanti Neurons for MDM** 会强制删除该用户，即使数据尚未同步到 Ivanti Neurons for MDM 管理门户。

从“用户”选项卡删除用户

步骤

1. 转到**用户**选项卡。
2. 选择一位或多位用户，转到**操作**下拉菜单，点击**删除**。 随即显示确认消息。 确认后，系统会将删除用户命令发送到设备。
3. 转到设备详细信息中的**设备日志**，并验证是否已将删除用户命令发送给共享 iPad 设备的选定用户。

从共享 iPad 设备中注销用户

管理员可以从共享 iPad 设备注销用户。

步骤

1. 在**设备**页面中，选择一个共享 iPad 设备。
2. 从**操作**菜单中，选择**强制注销**。 一个弹出窗口提示对于将用户从共享 iPad 设备注销进行确认。
3. 单击**确定**，批准强制注销。

12.3.8. 校园教务管理

许可证： Gold

适用于：监管的 iOS 9.3+

Apple School Manager 是一项 Apple 云服务，旨在帮助教育机构提供相关服务，包括在 Apps and Books 中购买应用、通过“Apple 设备注册”注册 iPad，以及创建托管 Apple ID。 Ivanti Neurons for MDM UEM 解决方案与 Apple School Manager 全面集成，并提供无缝方式来全面管理为教师和学生指定的 iPad，从而充分利用 School Manager 生态系统和 Classroom 等应用。

> 不支持 Apple 图书。

配置校园教务管理

1. 转到**管理员 > 校园教务管理**。
2. 如果关闭，单击**设置教育**选项。
3. 选择下列选项之一：
   - **与 Apple School Manager 帐户同步以导入学校信息**：
     1. 转到**管理员 > Apple > 设备注册**，以下载贵组织的密钥文件。
     2. 将密钥文件上传到 Apple 校园教务管理帐户，以生成加密密钥。
     3. 从 Apple School Manager 下载加密密钥，并将密钥上传到 Ivanti Neurons for MDM（**管理员 > Apple > 设备注册**）。

        > 现有 Apple 设备注册帐户可以重复用于 Apple 教育。 Apple 可让您选择升级您的设备注册帐户，以在访问 Apple 校园教务管理时包含教育功能。 有关升级指示，请访问 https://support.apple.com/en-in/HT206960。

        在接受加密密钥时，将显示**立即同步**按钮。

     4. 单击**立即同步**，开始与 Apple 校园教务管理同步数据。
   - **从 CSV 文件导入数据**：
     1. （可选）单击**下载 CSV 模板 ZIP 文件**，以下载包含所有数据类型模板的 zip 文件。
     2. 单击**选择文件**...
     3. 添加以下 6 个 CSV 文件：
        - 学生数据文件 (students.csv)
        - 名册数据文件 (roster.csv)
        - 员工数据文件 (staff.csv)
        - 班级数据文件 (classes.csv)
        - 课程数据文件 (courses.csv)
        - 位置数据文件 (locations.csv)

        > 在将其上传前，您每次必须选择所有 6 个 CSV 文件。

        单击**上传**。

     4. （可选）如果 CSV 文件需要修改，请在此前更新的所有 6 个文件中保留所有必要数据。 请进行必要编辑，并重新将其上传。

从**课堂**和**个人**选项卡搜索数据。

> 个人（学生和教职人员）也将显示在 Ivanti Neurons for MDM 的**用户**页面中。

5. 为学生和教职人员将用于教育的设备创建两个设备组，如下所示：
    1. 转到**管理员 > 自定义属性**。
    2. 为将用于动态创建托管设备组的学生和员工创建自定义属性。
    3. 转至**设备 > 设备**。
    4. 单击**添加 +**。
    5. 为每个使用将此前创建为筛选器的自定义属性的学生和员工，创建一个动态托管设备组。
6. 使用**操作 > 分配到用户**选项，将注册设备从**设备**页面分配到学生和员工。
7. 通过添加**配置 >** 教育负载，创建领导者（员工）配置和成员（学生）配置。
8. 将领导者（员工）和成员（学生）配置分配到员工和学生设备组。
   此分配将推送这些配置，并在各自设备上安排证书。

> 在**管理员 > School Manager** 页面上，如果没有为班级名称显示值，则将从班级系统源标识符和课程标识符字段派生值。 这些字段在 Apple 校园教务管理或 CSV 文件中是可选字段。 但推荐始终输入值，因为值组合会在缺少班级名称时用作默认标识符。

将教室应用推送到老师

使用课堂应用，教师（领导者）可以管理以下情景：

- 教室管理功能可远程控制 iPad 和应用。
- 可创建班级组。
- 可让老师查看该组的学生成员。
- 可让教师为该组的学生发送内容。
- 对学生能够查看的应用和内容予以限制。

可以从 Apple App Store 推送 Classroom 应用。

步骤

1. 转到**应用 > App Catalog** 页面。
2. 单击 **+ 添加**按钮。
3. 依据 Apple 搜索并选择教室应用。
4. 单击**下一步**。
5. 输入类别和描述。
6. 单击**下一步**。
7. 将应用分配到此前创建的老师设备组。
8. 在“应用配置”页面中，配置应用设备。
9. 单击**完成**。

禁用校园教务管理

禁用校园教务管理将擦除所有当前数据。 在执行此操作时，请谨慎小心。

1. 转到**管理员 > 校园教务管理**。
2. 如果开启，单击**设置教育**选项。
3. 单击**是**。

12.3.9. 设置 (Apple)

管理员可为 Apple 设备配置、启用、禁用多个设置。

静默注册（仅适用于 macOS）

适用于 macOS 设备的静默注册锁定为已启用。 这应用于租户中的所有新设备注册，并由 Mobile@Work 1.4 和/或更高版本提供支持。

常规设置

禁用设备协调 - 如果管理员希望再次注册同一设备，现在可以保留设备条目。 默认未选中此选项。 选择此选项以保留停用设备详细信息。

> 未启用禁用设备协调时，如果以同一用户重新注册设备，将创建新条目。 否则，将使用新的注册信息更新设备条目。

配置文件设置

如果未安装 MDM 配置文件，管理员可以启用或禁用向最终用户发送电子邮件，以及向 macOS 和 Go for iOS 客户端发送通知。 MDM 配置文件通知功能会默认启用。

程序

1. 转到**管理员 > 设置**。
2. 选择或取消选择**如果未安装 MDM 配置文件，向用户发送电子邮件并向客户端发送通知**选项。
3. 在 1 至 4 之间选择最大电子邮件/通知数量。
4. 单击**保存**。

自动化设备注册的 OS 更新（仅限 iOS）

管理员可以为自动设备注册打开 iOS 操作系统更新。 如果启用此选项，设备注册设备将使用软件更新配置，而不是设备注册配置文件中的计划 OS 更新设置。

此选项默认禁用，不论何种情况，使用设备注册配置文件中的计划 OS 更新设置。 打开此设置是永久设置，并且无法关闭。 此设置将移除所有可用设备注册配置文件中的计划 OS 更新设置。

> 受监管的非设备注册设备会使用软件更新配置。

程序

1. 转到**管理员 > 设置**。
2. 选择或取消选择**使用自动设备注册的软件更新配置**选项。
3. 单击**是**进行确认。
4. 单击**保存**。

多用户安全登录

通过在“管理 > Apple > 设置”下方“**多用户安全登录**”中选择“**在用户注销后清除通行码**”选项，当用户从 iOS 共享设备上的多用户安全登录 Web 剪辑中注销时，管理员可以清除设备密码。

限制配置的优先级设置

通过在**管理 >Apple > 设置**下方**限制配置的优先级设置**部分中，选择 **iOS 限制配置**或 **macOS 限制配置**选项，管理员可以为多个 iOS 和 macOS 限制配置启用优先级。 此选项默认禁用。 有关优先级工作原理的详细信息，请查看**确定配置的优先级**。

程序

1. 转到**管理 > Apple > 设置**。
2. 在**限制配置的优先级设置**部分中，选择 **iOS 限制配置**或 **macOS 限制配置**选项。
3. 单击**保存**，以启用优先级。 系统将显示“**限制配置的优先级设置（iOS 或 macOS）已启用**”横幅。 在优先级**已批准**前：
   - **编辑分发摘要（如适用）**：在启用优先级设置时，选定限制配置的分发摘要将默认从“**应用于其他空间中的设备**”更改为“**按最高优先级应用于其他设备空间中的所有设备**”。
   - **默认优先级按创建顺序进行分配**：对于选定限制类型配置，现有默认优先级将按创建顺序进行分配。
   - **暂停管理配置**：在批准优先级前，暂停管理选定限制配置（例如，iOS 限制配置）。

> 在启用优先级后，只有在批准后，才会处理对限制实施的任何更改。 在批准前，管理员可以在**配置**部分中编辑限制配置的分发、分发摘要或优先级。

4. 选择**批准**选项，以使优先级生效。
5. 单击**保存**。

> 在取消选择 iOS 或 macOS 限制配置选项时，**批准**选项不可用，更改会立即应用。

在优先级设置禁用时，优先级与配置无关。 如适用，所有限制配置推送到设备（在下次设备同步时）。

- **分发摘要（如适用）：在对限制配置禁用优先级设置时，分发摘要将从按最高优先级应用于其他设备空间中的所有设备或按最低优先级应用于其他设备空间中的所有设备更改为“应用于其他空间中的设备”。**
- **未分配优先级**：将对选定限制配置移除已分配的优先级

12.4. 使用 Windows 设备工作

本部分包含以下主题：

- 配置 Windows Autopilot 配置文件
- 针对 Windows Autopilot 配置文件的审计跟踪
- TenantLockdown CSP
- ADMX (GPO) 浏览器
- 配置应用库存间隔
- 硬件库

12.4.1. 配置 Windows Autopilot 配置文件

Windows Autopilot 是一项 Microsoft 功能，可帮助管理员设置和预配置新设备，从而为业务做好准备。 借助 Autopilot 功能，可以快速可靠和无缝地配置 Windows 桌面或 HoloLens2 设备。 此外，Autopilot 功能可以帮助执行以下任务：

- 自动将设备加入 Entra ID (Entra ID)
- 将设备自动注册到 MDM 服务
- 根据设备的配置文件，创建并将设备自动分配到配置组
- 自定义注册体验
- 应用配置和策略
- 安装必需应用

先决条件

要在 Windows Autopilot 页面上进行操作，请查看 Ivanti Neurons for MDM 合作伙伴步骤和 Azure 许可要求。 只有满足以下先决条件，Autopilot 功能才能正常运行：

- **与使用 Autopilot 相关的 Azure 许可要求**：请查阅“Windows Autopilot 许可要求”。
- **Azure Windows Autopilot 设备注册**：请查阅“Windows Autopilot 注册概述”。
- **经销商将设备添加到客户账户**：请查阅“通过在新设备上使用 Windows Autopilot 配置文件使客户获得获得自定义的即装即用体验”。

附加要求

1. 集成 Entra ID 租户和 Ivanti Neurons for MDM。 有关详细信息，请参阅使用 Microsoft Azure 设置。
2. 请确保您拥有 Ivanti Neurons for MDM 和 Entra ID 管理员账户。
3. 要利用自助部署配置文件，请先创建一个假用户，以便在 Ivanti Neurons for MDM 中注册无用户自助部署设备。
4. 从 Entra ID 主域创建并同步虚拟用户 fooUser@Entra IDPrimaryDomain.com。

> 创建和同步虚拟用户无需使用 Microsoft 许可证。

5. Entra ID 中的“自定义域名”页面将显示 Entra ID 环境的主域。
6. 确保用户可以注册设备并且未被禁用。 例如，如果主域是 contoso.com，则生成的用户将为 fooUser@contoso.com。 如果主域是 contoso.onmicrosoft.com，则生成的用户将为 fooUser@contoso.onmicrosoft.com。
7. 如需通过 SCIM 将用户添加到 Ivanti Neurons for MDM 中，请在 Entra ID 中编辑用户详细信息并添加电子邮件地址。 一般来说，电子邮件地址与 UPN 相同。
8. 确保所有用户（包括 fooUser）都存在于 Azure 和 Ivanti Neurons for MDM 中。
9. 管理员可以使用 Microsoft Store for Business 或 Ivanti Neurons for MDM 创建 Autopilot 配置文件。 如需使用 Ivanti Neurons for MDM 创建配置文件，管理员需要具备 Entra ID 全局管理员和 Intune 管理员权限。

> 管理员需要拥有 Azure P1 或 P2 许可，同时需要具备 Ivanti Neurons for MDM Secure UEM 或 Secure UEM Premium 许可证。 管理员不需要具备 Intune 许可证。

> 在 Neurons for MDM 中，创建 Autopilot 配置文件的功能需要用到适用于 Autopilot 的 Microsoft Graph API，这些 API 仍处于测试阶段。

Autopilot 注册模式

在根据设备使用情况将设备与特定用户配置文件组关联后，您可以配置 Autopilot 注册模式，允许用户快速开始使用设备。 Ivanti Neurons for MDM 提供以下 Autopilot 注册模式：

- 自部署模式
- 用户驱动（预配置模式）
- 用户驱动

自助部署 Autopilot 模式 - 自助部署 Autopilot 设备注册模式通过绕过初始设备设置并推送设备安全启动所需的所有必要配置文件，确保为用户无缝部署企业设备。 此模式可保护硬件，将设备连接到企业网络，并使用虚拟用户 ID 将设备注册到 Entra ID (Entra ID)、MDM 服务和 Ivanti Neurons for MDM 管理员门户，并在用户登录前将所有必要的配置文件推送到设备。 在强制性配置文件推送到设备后，设备将重启并显示登录界面，以供企业用户开始使用。 对于可用作自助服务终端的设备或数字签名的设备，您可以使用自部署模式。

用户驱动型预配置配置文件模式 – 管理员创建用户驱动型预配置配置文件后，系统会立即将该配置文件分配给用户组，同时设备硬件 ID 会上传并分配给 Entra ID 组。 设备将与用户驱动的预配置配置文件关联。 管理员使用此模式设置设备，然后将设备移交给企业用户。

步骤

请按照预配置部署的步骤进行操作：

1. 将新硬件设备连接到 LAN，并按 Windows 按钮五次。
2. 设备将显示问题提示。 选择 Windows Autopilot 配置选项，并单击“继续”。 Entra ID 检测到用户驱动型预配置配置文件模式后，所有基本配置设置都会部署到设备中。 将显示 Windows Autopilot 配置屏幕。
3. 单击“继续”。 设备会继续操作并保护硬件，将设备连接到企业网络，并使用虚拟用户 ID 将设备注册到 Entra ID (Entra ID)、MDM 服务和 Ivanti Neurons for MDM 管理员门户，同时在用户登录前将所有必要的配置文件推送到设备并显示确认消息。
4. 现在，您可以将设备移交由用户。 在用户登录设备时，用户 ID 会注册到 Ivanti Neurons for MDM 管理门户，并附上设备详细信息。

在用户登录设备前，将自动推送以下配置：

身份证书

Wi-Fi

Windows Hello For Business

Windows 限制

> 其余配置处于待处理状态，将在用户使用电子邮件地址登录设备后进行推送。

> 在自助部署和用户驱动（预配置）模式下的 Autopilot 注册流程中，分配的 .MSI 和 .EXE 应用程序将安装在设备上，以便完成注册流程。 在 Autopilot 注册流程中安装 .MSI 和 .EXE 应用程序时，如果安装过程中应用程序报告或无法报告，则 Autopilot 进程将完成，同时“重新封装”按钮将启用。

创建 Windows Autopilot 用户配置文件

在配置 Entra ID (Entra ID) 用户源并将用户和 Entra ID 用户组与 Ivanti Neurons for MDM 租户同步后，您可以创建 Autopilot 配置文件。

步骤

1. 登录 Ivanti Neurons for MDM 管理员门户。
2. 转到**管理员 > Microsoft Azure > Windows 设备管理**。

> 如果 Entra ID 用户源未配置，则**添加**按钮将被禁用。 您需要使用 **Microsoft Azure** 部分下的 **Windows 设备管理**选项来配置用户源。

3. 单击**添加**。
   屏幕将显示**添加 Windows Autopilot 配置文件**页面。
4. 在**名称**框中，输入配置文件名称。
5. 使用此过程下方的表，完成**配置文件设置**。
6. 单击**下一步**。
   屏幕上将显示包含所有 Entra ID 设备组的新页面。
7. 选择一个或多个必须向其分配 Autopilot 配置文件的 Entra ID 设备组。
8. 您也可以创建 Entra ID 设备组，并向这个新创建的组分配 Autopilot 配置文件。 请参阅**创建 Entra ID 设备组**获取详细信息。
   如需将 Autopilot 配置文件分配到所有 Entra ID 组，请选择**分配到所有 Entra ID 组**选项。

> 鉴于 Microsoft 的局限性，您无法将多个配置文件分配到“所有组”。

9. 单击**完成**。

设置	说明
设备类型	根据设备，选择以下两个选项中的其中一项： • **Windows PC** • **HoloLens** - 在选择此选项时，默认部署模式应设置为**自部署**模式。 在极个别情况下，使用 Autopilot 注册 HoloLens 2 设备时，注册可能会在“设置设备进行工作”屏幕上卡住。 在极个别情况下，用户必须按电源按钮关闭并打开设备。 然后，设备将显示登录屏幕，用户应在其中输入 Entra ID 凭据完成注册。
部署模式	• **自部署**：在此模式中，设备部署会在用户很少或未参与的情况下完成。 • **用户驱动**：管理员可以使用此选项选择注册模式，从而在将设备移交用户前为用户配置新设备。
用户帐户类型	• **管理员**：如果用户在设备部署后需要完全控制权限，选择此选项。 • **标准**：如果用户在设备部署后需要对基本选项的授权，选择此选项。
语言	默认情况下，语言将特定于操作系统。 您可以从列表更改为不同语言。
将所有目标设备转换为 Autopilot	选择此选项，将已分配组中的所有设备转换为 Autopilot。
允许预配置	选择此选项，使用正常注册过程为 Autopilot 注册设备。 在选择**自部署**选项时，此选项不可用。
自动配置键盘	如果**语言**选项设置为与默认值不同的值，选择**是**，跳过键盘选择。
设备名称模板	输入要在设备注册过程中使用的模板名称。
Microsoft 软件许可条款	您仅可在用户驱动的部署模式中显示或隐藏此选项。
隐私设置	您仅可在用户驱动的部署模式中显示或隐藏此选项。
更改帐户选项	只有在用户驱动的部署模式中并且用户帐户类型是标准类型时，您才可以显示或隐藏此选项。

Windows 设备管理

管理员可以使用新选项“Windows 设备管理”来配置租户中的 Autopilot 功能。 如果用户采用 Entra ID 环境，利用此选项可以更轻松地实现与 Ivanti Neurons for MDM 的集成。

要访问此选项，请转到**管理员** > **Microsoft Azure** > **Windows 设备管理**。

此集成会授权 Ivanti Neurons for MDM 管理设备、Autopilot 配置文件，检查 Windows 设备合规性并验证 Azure 租户。

相关主题

- TenantLockdown CSP

创建 Entra ID 设备组

管理员可以在需要时，在“Entra ID 设备组”部分中创建 Entra ID 设备组。 必须在“设备合规性”部分下配置 Entra ID 租户验证后，才能创建 Entra ID 设备组。

步骤

1. 前往**管理员** > **Microsoft Azure** > **Entra ID 设备组**。
2. 屏幕上将显示 **Entra ID 设备组**页面。
   点击**添加**。
3. 屏幕上将显示**组设置**页面。
   提供以下详细信息：
   - 组名称
   - 组描述
   - 成员身份类型
     - 静态设备 - 管理员将在**将成员分配到组**窗口中获得可用静态设备的列表。 选择所需设备，然后点击**保存**。
     - 动态设备 - 管理员必须在**动态查询**窗口中选择特定条件。

系统将创建新的 Entra ID 设备组，管理员可以将设备添加到新创建的组中。

> 在创建动态组后，设备将在一段时间后列在特定设备组的“设备”选项卡下方。

编辑 Autopilot 设备

用户可以在 Ivanti Neurons for MDM 管理门户中编辑 Autopilot 设备。

先决条件

确保满足以下先决条件：

- IT 管理员用户应具有 Azure 全局管理员和 Intune 管理员权限。
- 只有设置用户后才能设置用户友好名称。
- 设备名称一旦完成设置便无法取消设置。

步骤

1. 登录 Ivanti Neurons for MDM 管理门户。
2. 转到**管理** > **Windows** > **Autopilot**。 Autopilot 设备选项卡会列出 Autopilot 设备。
3. 单击**编辑**（铅笔图标）。 系统将显示编辑页面。
4. 编辑以下详细信息：
   - **用户**
   - **用户友好名称**
   - **设备名称**
   - **组标记**

单击**保存**。 设备详细信息将更新。

删除 Autopilot 设备

用户可以从 Ivanti Neurons for MDM 管理门户删除 Autopilot 设备。

1. 登录 Ivanti Neurons for MDM 管理门户。
2. 转到**管理** > **Windows** > **Autopilot**。 Autopilot 设备选项卡会列出 Autopilot 设备。

3. 单击**删除**。 设备详细信息将删除。

12.4.2. 针对 Windows Autopilot 配置文件的审计跟踪

审计跟踪将跟踪在 Ivanti Neurons for MDM 中的所有实体上执行的所有活动。 这些活动包括添加、删除、更新新设备等。

有关详细信息，请参阅审计跟踪。

管理员可以在 Autopilot 模式下注册的所有 Windows 设备上使用审计跟踪执行以下活动：

Autopilot 配置文件

- 创建
- 编辑
- 删除
- 将配置文件分配到组

Autopilot 设备

- 上传 CSV
- 编辑
- 删除

12.4.3. TenantLockdown CSP

借助 TenantLockdown CSP 功能，管理员可以将所有 Windows 设备锁定到租户。 要使用此功能，设备必须使用 Autopilot 选项注册。 此配置可在设备级完成。

在 Autopilot 自部署和用户驱动的模式中，管理员可将设备直接锁定到租户。 这在设备丢失或被盗时非常有用。 对于此类情况，即使设备重置，用户也将强制连接到租户，自部署模式不支持本地帐户创建。 但如果需要在用户驱动的模式中阻止帐户创建，在 Autopilot Profile 配置过程中，管理员必须在**更改帐户选项**设置中启用**隐藏**选项。

通过创建 Windows 限制配置，并在**其他限制**下方选择**需要用户在设备设置期间连接到网络（需要 Autopilot 配置文件）**选项，管理员可以启用 TenantLockdown CSP。

要将设备从 TenantLockdown CSP 中移除，管理员必须手动将设备从组中移除，或更改限制。

12.4.4. ADMX (GPO) 浏览器

使用 ADMX (GPO) 浏览器，您可以查看 GPO 设置；这些设置将根据租户中存在的 ADMX 对象进行组织。 您可以搜索和查看默认的 ADMX 对象，还可以添加（上传）自定义 ADMX 文件，该文件提供基于 XML 的结构，以定义 GPO 设置的显示

要上传自定义 ADMX 对象：

1. 选择**管理员 > ADMX (GPO) 浏览器**。 将显示 **ADMX (GPO) 浏览器**页面。
2. 单击**附加**。 将显示**附加自定义 ADMX (GPO) 对象**窗口。
3. 单击**选择文件**，选择要上传的 ADMX 文件。

> 确保 ADMX 文件是 zip 文件。

4. 单击**附加**。 将显示表示成功上传的确认消息。

> 解压 zip 文件后，请确保根文件夹包含 *.admx* 扩展名文件。

搜索 GPO 设置

在 ADMX (GPO) 浏览器中，您可以通过点击左侧窗格中 GPO 层次结构树内的相关组件来搜索并选择 GPO。 GPO 层次结构树表示策略设置的路径。 您也可以通过在搜索字段中键入 GPO 名称或 ADMX 文件名搜索特定 GPO 设置。 所选 GPO 设置的详细信息显示在右侧窗格中。

12.4.5. 配置应用库存间隔

对于多个应用来源类型库存，您可以设置 Windows 10 应用库存收集间隔。 在隐私配置设置为从设备收集所有应用时，使用间隔。

1. 导航至**管理员 > 应用库存间隔**。
2. 对于以下应用来源类型，从下拉列表中，选择用于收集应用库存的间隔（以小时为单位）。
   - **非 App Store 库存间隔**
   - **App Store 库存间隔**
   - **系统库存间隔**
   - **Win32 库存间隔**
     收集 Windows 应用程序清单的间隔选项为 **24** 到 **48** 小时之间。 默认值是 **24** 小时。

12.4.6. 硬件库

您可以从 Windows 10 设备启用收集硬件信息。 使用 Bridge 检索硬件库详细信息。

1. 导航到**管理员 > 硬件清单**。
2. 启用选项**启用收集硬件库**。
3. 在**库存间隔**, 中，选择收集硬件库的频率。 以下是可用选项：
    - **一天一次**（默认）
    - **一周一次**
    - **每 30 天**

在启用硬件库选项时，您可以在设备详细信息页面上查看**硬件**选项卡中的设备硬件详细信息。

12.5. 使用 Microsoft Azure 设置

本部分包含以下主题：

- 使用 Microsoft Azure
- Entra ID Windows 10 统一端点管理设置
- 分配 Entra ID UEM 应用程序
- 连接 Ivanti Neurons for MDM 与 Entra ID 用户源
- Azure 租户
- 管理员 > Microsoft Azure > Office 365 应用保护

12.5.1. 使用 Microsoft Azure

可使用 Microsoft Azure 设置 Ivanti Neurons for MDM，以便您的用户在 Windows 桌面设备和运行 Windows 10 的平板设备上实现无缝注册。 按照下面的步骤来配置和连接您的实例。

本部分包含以下主题：

- 设置 Entra ID 账户
- 在 Entra ID 上创建用户
- 将 Entra ID 连接到适用于 Windows 10 设备的 UEM
- Windows 设备的多用户支持

设置 Entra ID 账户

设置 Entra ID：

1. 转至https://azure.microsoft.com/en-in/pricing/purchase-options/，以购买 Azure 账户。
2. 使用现有 Hotmail 或 Outlook.com 账户，或者创建新账户并注册为新用户。
3. 使用其中一种付款选项和以下验证步骤，购买 Azure 账户。
4. 要求 Microsoft 将 Ivanti Neurons for MDM 租户加入允许列表。
5. 使用您在步骤 2 中使用的同一 Hotmail 或 Outlook.com 账户，以管理员身份登录 Entra ID，地址为 https://manage.windowsazure.com/https://manage.windowsazure.com/。
6. 转到**域**选项卡。
   系统将为您的帐户创建默认域 TestMiBGLRoutlook.onmicrosoft.com，而创建的任何用户将属于此域。 如果需要，您可以重新创建自定义域。

在 Entra ID 上创建用户

在 Entra ID 上创建用户：

1. 转到活动目录 - > **默认目录 - > 用户**。
2. 选择“添加用户”选项 - > 选择贵组织中的新用户。
3. 输入用户名。 单击下一步**(→)**。
   系统将显示**用户配置文件**页面。
4. 添加用户信息，例如姓名并显示名称。
5. 使用下拉菜单，为用户分配适当角色。
6. 生成临时密码。
   第一次登录时，需要用户更改此密码。

将 Entra ID 连接到适用于 Windows 10 设备的 UEM

连接 Entra ID 与 UEM：

1. **转到管理员 > Microsoft Azure > 使用 Entra ID 的 Windows 注册和合规性。**
2. 完成 Entra ID Windows 10 统一端点管理设置一节中描述的 UEM 设置步骤。
3. 完成 Azure 门户中的分配 Entra ID UEM 应用程序设置。

4. 在 Ivanti Neurons for MDM 管理员门户中，输入您的 Entra ID 账户域名，接着点击“连接 Azure 门户”，然后选中复选框。
5. 在成功登录后，接受并同意 MobileIron AD 租户验证应用验证 Ivanti Neurons for MDM UEM 应用是否已正确设置。 系统将显示一则消息，并表示连接成功。

适用于 Windows 10 设备的 Microsoft Passport for Work

Windows Hello for Business 已替换 Microsoft Passport for Work。 有关更多信息，请查看 Windows Hello for Business 配置。

Windows 设备 Entra ID 注册

先决条件

必须在 Ivanti Neurons for MDM 中注册用户。

连接您的域以在 Windows 10+ 设备上注册用户。

1. 点击**加入 Entra ID**。
2. 输入用户名和密码。
3. 单击**登录**。
4. 接受 EULA。
5. 单击**创建 PIN**。
   - 如果您已启用 Microsoft Passport for Work PIN 复杂性，则系统将会提示您根据配置策略设置复杂 PIN。
   - Entra ID 对用户进行身份验证，并将 JWT（JSON Web 令牌）下载到设备。
   - 设备现已注册。
   - 通过验证的设备联系用户。
6. 输入并确认 PIN。
7. 单击**确定**。

Windows 设备的多用户支持

对于 Windows 10 Entra ID 注册设备，Ivanti Neurons for MDM 支持多用户功能。 此功能包含将 VPN、WiFi、默认电子邮件客户端配置文件和证书等一些配置文件推送到个人用户，而非设备。 此外，对于登录用户，也支持分发内部和公共应用。 Entra ID 新用户每次登录设备时，Ivanti Neurons for MDM 不仅会评估设备，还会评估用户。 如果用户是新用户，Ivanti Neurons for MDM 将更新该用户的设备。 如果用户是设备上的现有用户，将评估自上次登录后需要更新对设备和用户设置进行的任何更改。

Ivanti Neurons for MDM 管理员门户会报告登录设备的 Entra ID 用户的详细信息。 在用户注销设备及第二个用户登录设备时，设备详细信息页面会更新第二个用户的详细信息。

使用 UEM 设置 Microsoft Store for Business

Microsoft Store for Business 是 Microsoft 作为 Azure 的一部分提供的门户。 管理员可以登录此门户，购买应用程序并将其分发到所有托管设备。 Ivanti Neurons for MDM 可以使用 Microsoft Store for Business 进行设置，以通过设置以下步骤在 Ivanti Neurons for MDM 管理员门户中管理应用程序。

步骤 1：在 Microsoft Azure 门户中注册 Entra ID 应用程序

1. 打开第一个浏览器并登录 Microsoft Azure 门户 (https://portal.azure.com/https://portal.azure.com/)。
2. 在左侧窗格中单击**应用程序注册**。

3. 单击 **+ 新建应用程序注册**。
4. 输入以下信息将 MobileIron 注册为 Azure 应用程序。
   - **名称：**输入 MobileIron 应用程序的名称。（此字段必须至少包含 4 个字符。）
   - **应用程序类型：**选择 Web 应用程序/API
   - **登录 URL：**输入用户访问登录 MobileIron 的 URL 设备（必填）。
5. 单击**创建**，添加应用程序并返回 Azure 主页。
6. 转到“设置”并创建新密钥。

步骤 2：将应用程序添加为管理工具

1. 在 Microsoft Store for Business 设置中，单击“管理
2. 分发设置”
3. 在添加管理工具中，激活创建的应用程序。

连接管理员门户中的账户

1. 转到**管理员 > Microsoft Azure > 适用于企业的 Microsoft Store**。
2. 在步骤 1 的**注册 Entra ID 应用程序**中，选中复选框**是，我已完成此步骤**。
3. 在步骤 2 **添加管理工具**中，选中复选框**是，我已完成该步骤**。
4. 在步骤 3“连接账户”中，更新以下字段：
   - Entra ID 域
   - 应用程序标识符
   - 应用程序键
   - 同步间隔（小时）
5. 单击**连接**。您将看到一条确认消息，表明 MobileIron Store for Business 已成功设置。
6. 单击**同步应用程序**。成功同步后，状态显示为**应用程序已成功同步**。

当 Microsoft Store for App被推至设备时，应用程序详细信息可在设备详细信息中的**已安装的应用程序**选项卡下找到。 从设备报告的每个 Microsoft Store for Business 应用程序，可以在**源**列中标识为 **Microsoft Store for Business**。

12.5.2. Entra ID Windows 10 统一端点管理设置

若要设置 Windows 10 统一端点管理设置 (UEM)：

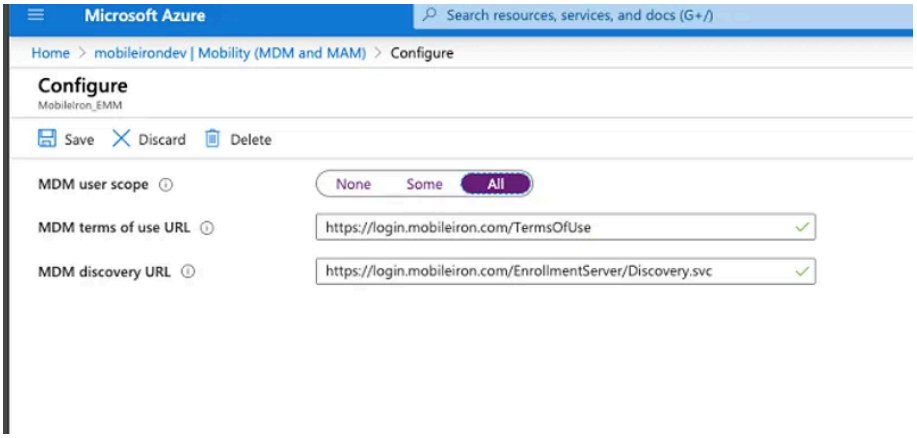
1. 请以管理员身份登录 https://portal.azure.com/，然后选择 Entra ID。
2. 在左侧面板中选择“移动性（MDM 和 MAM）”，然后单击**+ 添加应用**。

3. 从应用库中选择 MobileIron_UEM 应用，然后单击**添加**。


12.5.3. 分配 Entra ID UEM 应用程序

完成分配用户设置：

1. 点击步骤 2 中，您在 **Entra ID Windows 10 统一端点管理设置**中创建的 MobileIron UEM 应用程序。
2. 在 MDM 用户范围中，将其分配到自定义用户组，或者选择**全部**。



12.5.4. 连接 Ivanti Neurons for MDM 与 Entra ID 用户源

要使用 Entra ID (Entra Id)，您必须使用您的 Microsoft Entra ID 账户详细信息配置 Ivanti Neurons for MDM。 您需要现有的已配置 Microsoft Entra ID 账户。 此解决方案不需要本地连接器或 LDAP。

本部分包含以下主题：

- 用例
- 使用 Entra ID
- Entra ID 设置

用例

对于以下任一用例，您都可以连接 Ivanti Neurons for MDM 与 Entra ID：

- 使用 Microsoft Office 365
- 设置 Microsoft Entra ID、Microsoft ADFS 或其他 SAML 2.0 身份提供程序 (IdP) 以进行用户身份验证
- 将 Microsoft Entra ID 设置为您的用户源
- 同步来自 Microsoft Entra ID 的用户并开始使用。 您的 Entra ID 域中的所有用户和组都将同步到您的 Ivanti Neurons for MDM 实例
  如果 Entra ID 同步由于以下原因出错，系统将在**通知**页面中显示通知：
  - Entra ID 服务无法访问
  - 所有用户属性未与 Entra ID 同步
  - 部分用户属性未与 Entra ID 同步
- 目前不支持具有多个 IdP 的环境。
- 如果您使用的用户源并非 Microsoft Entra ID，则可以使用本地账户或 LDAP 中的源用户。 这需要设置 Ivanti Neurons for MDM Connector 以访问本地 LDAP 资源。
- 目前不支持仅在用户身份验证时使用 Microsoft Entra ID，也不支持针对用户目录使用内部 LDAP。

使用 Entra ID

要使用 Entra ID，请通过以下方法之一设置身份提供程序以进行用户身份验证：

- 要将 Microsoft Entra ID 用作用户源并用于用户身份验证，请将 Entra ID 设置为您的 IdP。 转到**管理员 > 身份 > Ivanti Neurons for MDM IdP 设置**，然后从菜单中选择 **Entra ID**。
- 要将 Microsoft Entra ID 用作用户源，并使用 ADFS 进行用户身份验证，请将 ADFS 设置为您的 IdP。 转到**管理 > 身份 > 内部 IdP 设置**并从菜单中选择 ADFS。
- 要使用 SAML 2.0 IdP 而不是 Entra ID，并使用 ADFS 进行用户身份验证，请转到**管理 > 身份 > 通用 IdP 设置**，然后按照页面上的说明进行操作。

有关详细信息，请参阅配置标识提供者。

Entra ID 设置

本主题可帮助您配置 Entra ID 设置。

步骤

1. 转到**管理员 > Microsoft Azure > Entra ID 用户源**。
2. 指定以下详细信息：
    1. **Entra ID 名称**。
    2. **同步间隔** - 修改 Ivanti Neurons for MDM 从您的 Entra ID 同步用户数据的频率。
    3. **启用此 Entra ID** - 使用此选项可启用或禁用 Entra ID 实例。
    4. 选择**自动邀请从 Entra ID 导入的用户** - 管理是否自动邀请从 Entra ID 导入到 Ivanti Neurons for MDM 中的用户通过电子邮件进行注册。
    5. 选择**托管 Apple ID** - 选择此选项可同步 Entra ID 用户的托管 Apple ID。
        - **无**
        - **模式** -
            - **用户电子邮件地址**
            - **userUPN**
            - （可选）选择包含 "appleid" 子域选项以避免与现有 Apple ID 发生冲突。
    6. （可选）点击**添加自定义属性** - 指定要应用到设备管理的目录服务中的自定义用户属性。 每个属性随后可被支持变量的配置字段中的 $ 引用。 使用此选项需要在 Entra ID 服务器上实施一致的自定义属性。 如果实施时包含的 Entra ID 服务器未使用此属性，那么依赖此属性的功能可能无法按预期工作。

修改 Entra ID 设置后，点击**保存**。

12.5.5. Azure 租户

本部分包含以下主题：

- 要求
- 将 Intune 许可证应用于设备用户
- 将 MobileIron 添加为合规合作伙伴
- 在 Microsoft Endpoint Manager 中创建条件访问策略
- 将 Microsoft Azure 连接到 Ivanti Neurons for MDM
- 创建合作伙伴设备合规性策略
- 从 Ivanti Neurons for MDM 向 Azure 报告设备状态
- 取消配置 Azure 租户

12.5.5.1. Azure Tenant Requirements

本节介绍使用 Microsoft Azure 租户设置 Ivanti Neurons for MDM。

要求

Microsoft

Ivanti Neurons for MDM 客户必须拥有 Microsoft Intune 的有效订阅，并将 Microsoft Intune 许可证分配给设备用户。

MobileIron

- Ivanti Neurons for MDM - Ivanti Neurons for MDM 75 版本到由 MobileIron 支持的最新版本。
- 其他许可 - Azure 设备合规性是一款 Premium 产品，并且可用于 **Secure UEM Premium** 和 Platinum 客户。 对于现有客户，Platinum 许可证足以。
- Go for iOS（客户端）或 Go for Android（客户端）版本 75.0 到 MobileIron 支持的最新版本。

支持多个版本 Ivanti Neurons for MDM

如果有多个 Ivanti Neurons for MDM 连接到相同的 Azure 租户，请断开所有 Ivanti Neurons for MDM 的连接，或从特定（单个）Ivanti Neurons for MDM 禁用 Entra ID 合规性集成的合规性策略，这样就不会将设备数据上传到 Azure

> 请确保先禁用合规性策略，然后再将 Ivanti Neurons for MDM 断开连接。

Ivanti Neurons for MDM 管理员进程

对于 Ivanti Neurons for MDM 管理员，该流程：

1. 管理员将 Intune 许可证应用于设备用户。 请查看**将 Intune 许可证应用于设备用户**。
2. 管理员登录 Azure 门户。
3. 管理员将 MobileIron 添加为 Azure 合规合作伙伴。 请查看**将 MobileIron 添加为合规合作伙伴**。
4. 管理员会为应用创建条件访问策略。 请查看**在 Microsoft Endpoint Manager 中创建条件访问策略**。
5. 管理员设置 MobileIron 与 Azure 之间的连接。 请参阅**将 Microsoft Azure 连接到 Ivanti Neurons for MDM**。
6. 管理员在 Ivanti Neurons for MDM 中创建设备合规性策略。 请查看**创建合作伙伴设备合规性策略**。
7. 条件访问策略生效。 根据设备是否合规，授予或拒绝对应用的访问权限。

> Ivanti 建议管理员对每个 Microsoft 应用运行测试。

12.5.5.2. 将 Intune 许可证应用于设备用户

- 如果出现以下情况，不得使用此功能：
  - 您正在更改用户或管理用户可能会变更的情况
  - 设备由多个用户拥有
- Ivanti 建议您不执行分配到用户，并且不将设备合规性配置分发到多用户设备，例如：
  - 使用安全登录 WebClip 的设备
  - 共享 iPad 设备
  - Android 自助服务终端模式设备

Ivanti Neurons for MDM 许可要求

设备合规性是一款 Premium 产品，并且可用于 Secure UEM Premium 和 Platinum 客户。 对于现有客户，Platinum 许可证足以。

将批量许可证分配到设备用户

要将许可证批量分配到现有设备用户：

基于组的分配

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-groups-assign

基于 PowerShell 的分配

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. 将 MobileIron 添加为合规合作伙伴

先决条件

- 安装 Microsoft Intune 许可证。 请查看将 Intune 许可证应用于设备用户。
- 在 Microsoft Azure 中创建用户
- 在 Microsoft Azure 中创建组

程序

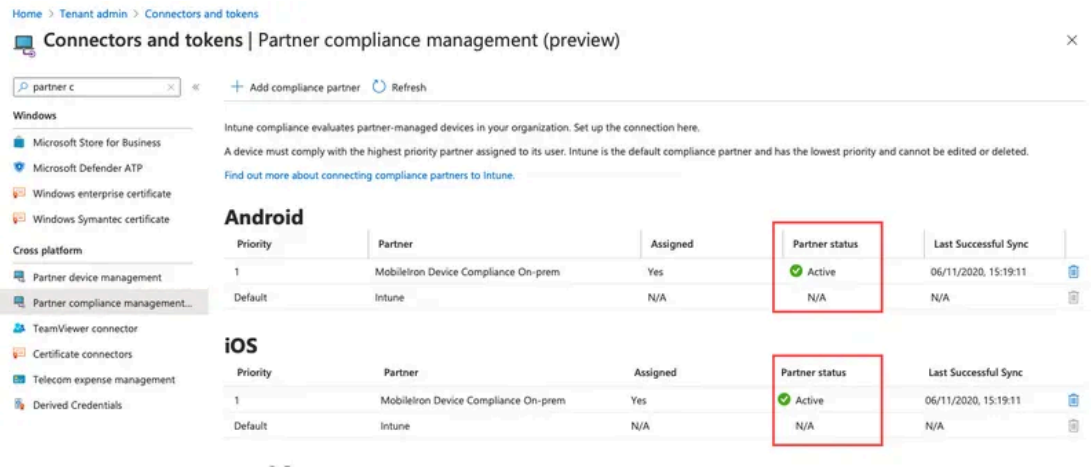
1. 登录：https://endpoint.microsoft.com。
2. 在 Microsoft Endpoint Manager 管理中心页面的左面板中，单击 租户管理员。 单击 Connectors 和 Tokens > 合作伙伴合规性管理。

3. 在搜索字段右侧，单击 + 添加合规合作伙伴。

4. 在“概况”选项卡中，从合规合作伙伴字段的下拉列表中选择 MobileIron Device Compliance Cloud。

5. 在平台字段中，选择 iOS 或 Android，然后单击下一步。
6. 单击分配选项卡。 在“分配对象”下拉列表中，选择合规性状态适用的用户/设备用户组。 选择拥有许可证的用户/组。

7. 选择下一步。
8. 单击创建。 合作伙伴合规性管理页面会显示新合规合作伙伴。



12.5.5.4. 在 Microsoft Endpoint Manager 中创建条件访问策略

程序

1. 登录 Microsoft Endpoint Manager https://endpoint.microsoft.com。
2. 在 Microsoft Endpoint Manager 管理中心页面中，转到主页 > 端点安全性 > 条件访问。
3. 单击策略，然后单击 + 新建策略。

4. 输入条件访问策略的名称。

5. 在分配中，单击以将策略分配到用户和组。

6. 单击 Cloud 应用或操作，然后单击选择。 搜索并选择需要保护的应用。

7. 单击“条件”，然后单击设备平台。 选择适当的设备平台。

8. 在新建条件访问策略页面 > 访问控制中，单击授予，并访问和阻止选择。

9. 要启用新策略，单击打开。

10. 单击创建。

12.5.5.5. 将 Microsoft Azure 连接到 Ivanti Neurons for MDM

程序

1. 登录 Ivanti Neurons for MDM，然后前往**管理员** > **Microsoft Azure**。
2. 在左侧导航窗格中，单击 **Microsoft Azure** > **设备合规性**。
3. 在“连接帐户”部分下，提供以下详细信息：
   - **Azure 租户 ID** - 在 Microsoft Azure 实例中查找。
   - **注册 URL（可选）** - 如果设备未通过 MDM 注册，设备用户将被指向此 URL 进行注册。 在配置时，使用 HTTPS 格式。 如果您在组织中托管页面以重定向设备用户获取注册信息，请在此处添加该链接。
   - **修正 URL（可选）** - 如果设备不合规，设备用户将被指向此 URL 进行修正。 在配置时，使用 HTTPS 格式。 如果您在组织中托管页面以重定向设备用户获取修正信息，请在此处添加该链接。
4. 单击**连接账户**。 Azure 租户验证对话框打开。

> 当前已与 Azure 连接的租户如果想要为 macOS 设备添加设备合规性，则必须断开账户连接并重新建立连接。

5. 在“Azure 租户验证”对话框中，单击步骤 1 中的**链接**。
6. **登录**。
7. 查看权限，然后单击**接受**。

> 如果登录后页面提示您重新登录，请关闭浏览器选项卡/窗口。

8. 返回至 Ivanti Neurons for MDM。 在“连接 Azure 帐户”对话框中，选中**我表示同意**复选框。 单击**确认**。

- 要编辑帐户，单击**编辑帐户**。
- 要将帐户断开连接，单击**将帐户断开连接**。 有关其他说明，请查看取消配置 Azure 租户。
- 日志会记录添加、编辑和取消激活帐户的所有活动。

12.5.5.6. 创建合作伙伴设备合规性策略

在 Ivanti Neurons for MDM 中创建合作伙伴设备合规性策略并施加所需的标签。 合作伙伴合规性策略将设备合规性状态报告给 Azure 或 BeyondCorp，以实现有条件的访问。

适用于

- iOS
- Android
- Windows

先决条件

必须设置 Azure 租户 ID 或 Google BeyondCorp ID。 有关 Azure 合作伙伴设备合规性的详细信息，请参阅**将 Microsoft Azure 连接到 Ivanti Neurons for MDM**。



程序

1. 登录 Ivanti Neurons for MDM，前往**配置**。
2. 点击**添加**并搜索**合作伙伴设备合规性**配置。
3. 在**创建合作伙伴设备合规性配置**页面上输入以下详细信息：

个项目	说明
名称	输入名称。
+ 添加描述	输入说明。
选择合作伙伴	选择 **Microsoft Azure 合规性**。 或 **Google BeyondCorp 合规性 - Beta 版**。
配置设置 将 iOS、macOS 和 Android 设备的合规性状态报告给 Azure	默认切换为“打开”。 如果没有看到此字段，则需要设置 Azure 租户 ID。 如果已启用“报告 iOS、macOS 和 Android 设备的合规性状态”选项，并且合规性策略应用于客户端，则客户端将在设备的“设置”下显示“Microsoft 365 Access”。 在以下情况，报告设备的合规性状态： • 设备不合规 • 设备合规 • 设备重新合规性 • 24 小时已过。 如果状态没有更改，则每周/每 7 天发送一份报告。
将 iOS、macOS、Android 和 Windows 设备的合规性状态报告给 Google BeyondCorp	默认切换为“打开”。 在以下情况，报告设备的合规性状态： • 设备不合规 • 设备合规 • 设备重新合规性 • 24 小时已过。 如果状态没有更改，则每隔 24 小时发送一份报告。

4. 单击**下一步**。

5. 默认选择**启用此配置**。
6. 选择配置的分发级别。 有关配置分发的详细信息，请参阅**添加配置**。
7. 单击**完成**。

12.5.5.7. 从 Ivanti Neurons for MDM 向 Azure 报告设备状态

出现以下情况时，Ivanti Neurons for MDM 会报告设备库存和合规性状态。

- 设备上的合规性状态变化
- 设备上的库存变化
- Ivanti Neurons for MDM 会每周一次报告合规性和库存状态

根据在合规性策略中选择的操作，发送以下设备状态：

操作 （最严格的操作适用）	Ivanti Neurons for MDM 发送的内容
阻止电子邮件、AppConnect 应用、隔离	设备不合规
发送警报	对 Azure 合规
停用设备	从 Azure 平台移除的设备数据

设备详细信息页面

要查看有关设备的 Azure 信息，转到设备详细信息页面。 字段及其可能的值的描述：

字段	说明
Azure 设备标识符	Microsoft 向 iOS 或 Android 设备报告的设备 ID。 例如：007c8232-9489-4074-9b35-345b16f0a72d。 Ivanti Neurons for MDM 会收到此设备 ID，因为设备用户需要注册到 Microsoft Authenticator 应用，才可以使用此功能。 如果无法检索设备 ID，此字段留空。
Azure 设备合规性状态	在 Azure 中列出设备的合规性状态。 可能的值： • 进行中 • 成功 • 失败
Azure 客户端状态代码	表示设备是否连接到 Azure。 可能的值： • Success - 可检索设备 ID。 • Internal_Error - 客户端或服务器端出现无法恢复的错误。 • Workplace_Join_Required - 设备需要注册。 设备用户可以缓解此状态。 • Interaction_Required - 需要交互登录。 设备用户可以缓解此状态。 • Server_Declined_Scopes - 未向一些范围授予访问权限。 • Server_Protection_Policies_Required - Intune 条件访问策略会保护请求的资源。 • User_Canceled - 设备用户通过在 Web 浏览器中点击“完成”或“取消”按钮取消 Web 身份验证会话。 • Account_logged_out - 帐户已注销。
Azure 设备合规性报告时间	Ivanti Neurons for MDM 向 Microsoft Intune 报告设备合规性状态的时间。 空白字段表示以下其中一项内容： • 功能禁用 • Ivanti Neurons for MDM 已收到数据，但尚未调用 Microsoft API • 出现错误，例如 user_Cancelled 或内部错误

12.5.5.8. 取消配置 Azure 租户

如果启用多个版本的 Ivanti Neurons for MDM 以使用相同的 Azure 租户，请从所有版本的 Ivanti Neurons for MDM 取消配置。 如果单个 Ivanti Neurons for MDM 需要停止使用 Azure，您可以仅对该 Ivanti Neurons for MDM 禁用合作伙伴合规性策略。

如果管理员在 Ivanti Neurons for MDM 中执行断开连接操作，Ivanti Neurons for MDM 会停止向 Azure 报告设备库存和合规性状态。

先决条件

- 请确保所有设备为不受管
- 请确保所有设备为不合规

程序

Microsoft

1. 登录 Microsoft Azure。
2. 转到 Intune > 条件访问。 请确保禁用条件访问策略。

Ivanti Neurons for MDM

1. 登录 Ivanti Neurons for MDM，前往 管理员。
2. 在左侧导航窗格中，单击 Microsoft Azure > iOS 和 Android 的设备合规性。
3. 单击将帐户断开连接。

4. 单击是。

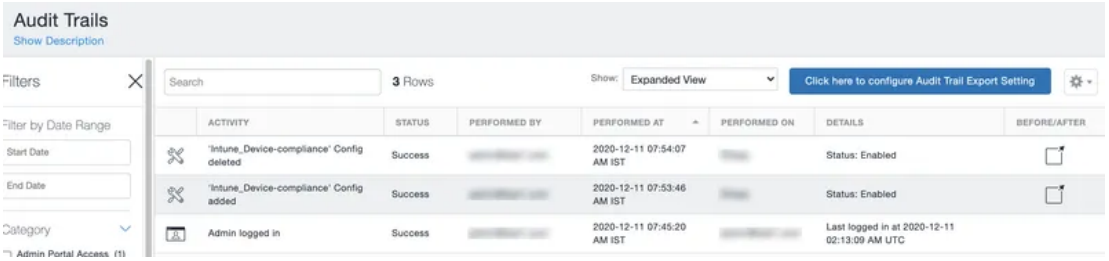
从 Azure 中停用设备

在设备停用时，Ivanti Neurons for MDM 会向 Azure 报告设备不再受管，并且不合规。

Azure 将在 90 天后删除已停用的设备条目。

日志会记录 Azure 帐户活动

日志会记录所有活动。



12.5.6. 管理员 > Microsoft Azure > Office 365 应用保护

许可证：Gold

您可以设置 Office 365 应用程序保护策略来帮助保护公司的数据。 这些策略使用 Microsoft 图形 API 为 Microsoft Office 365 应用程序强制执行数据丢失防护（DLP）控制。 其中一些 Graph API 允许管理员对使用 Graph SDK 的本机 iOS 和 Android 应用执行应用保护。

使用此功能可执行以下策略：

- 防止用户从 Office 365 应用程序打印。
- 防止出站数据从 Office 365 应用程序共享。
- 强制执行 Office 365 应用程序的 PIN。
- 从 Office 365 应用程序禁用联系人同步。

使用 Office 365 应用程序保护的先决条件

在使用 Office 365 应用程序防护之前，您必须拥有：

- 有效的 MobileIron 许可证。
- Office 365 应用保护功能已在 Ivanti Neurons for MDM 中启用
- Intune 订阅或包含 Intune 的 Microsoft EMS 订阅。
  - 每次对应用策略的使用都需要许可证，但启用和测试集成仅需要一个许可证。
- 可在移动设备上访问 Office 365 应用程序的有效 Office Enterprise 或 Business 订阅。
- 一个或多个 Office 365 应用程序。
- 已将您的 Active Directory 用户同步到 Entra ID。
- One Drive for Business 安装在设备上，以保护Word、Excel 和 PowerPoint 中的数据。 这不是强制性的。
- 访问 Microsoft Azure 门户 (https://portal.azure.com/)，以配置 Intune 应用保护策略。
- Intune Company Portal 应用安装在 Android 设备上。
  设备用户无需登录，但必须在设备上安装此应用程序才能保护设备上的数据。 当用户登录到应用程序时，保护将适用。

将 MobileIron 注册为 Azure 应用程序

本主题介绍如何使用 Ivanti Neurons for MDM 软件注册和存储 Azure 租户凭据，并远程管理适用于 Android 和 iOS Office 365 应用的 Microsoft Azure 云中的应用保护策略。 虽然没有必要，但您可以打开两个浏览器来执行以下过程中的步骤。 使用第一个浏览器登录到 Microsoft Azure 门户。 使用第二个浏览器登录 Ivanti Neurons for MDM 管理门户。

Microsoft Azure 门户的过程

> Microsoft 可能会随时更改 Azure 门户用户界面。 这些说明会假定您熟悉 Microsoft Azure 门户，并可在将 MobileIron 注册为 Azure 应用时实施必要调整。

1. 打开第一个浏览器并登录到 Microsoft Azure 门户（https://portal.azure.com/）。
2. 在左侧窗格中单击**应用程序注册**。

3. 单击 **+ 新建应用程序注册**。
4. 输入以下信息将 MobileIron 注册为 Azure应用程序。
    - **名称：**输入 MobileIron 应用程序的名称。 （此字段必须至少包含 4 个字符。）
    - **应用程序类型：**选择 Web 应用/API
    - **登录 URL：**输入用户访问登录 MobileIron 的 URL 设备（必填）。

单击窗格底部的**创建**，添加该应用并返回到 Azure 主页。

6. 在 Azure 主页上单击新创建的 MobileIron 应用程序。
7. 返回 Azure 主页，为 MobileIron Azure 应用程序分配权限。
8. 要为新创建的 MobileIron 应用设置所需的 API 权限，单击应用注册中的应用名称。
9. 单击 **API 权限** > **添加权限**。
10. 在 **Microsoft Graph > 委派权限 > 设备管理应用** 部分中，选择 **DeviceManagementApps.Read.All** 权限，并点击**保存**。 默认情况下，已为该应用启用 user.Read 权限。
11. 要授予访问权限，单击**授予管理员对 MobileIron 的同意**。
12. 请对 Ivanti Neurons for MDM 管理员门户执行以下过程。

Ivanti Neurons for MDM 管理门户的操作流程

1. 打开第二个浏览器并登录 Ivanti Neurons for MDM 管理门户。
2. 转到**管理员 > Microsoft Azure > Office 365 应用保护**。
3. 将**应用程序 ID** 粘贴到 Ivanti Neurons for MDM 管理门户中。
4. **步骤**
    1. 转至 Azure 门户。
    2. 选择 MobileIron 应用 > **属性**。
    3. 复制**应用程序 ID**。
    4. 返回管理员门户中的**管理员 > Microsoft Azure > Office 365 应用保护**。
    5. 将其粘贴到**应用程序 ID** 字段。

将**应用程序密钥**（客户端密钥）粘贴到 Ivanti Neurons for MDM 管理门户中。

5. **步骤**
    1. 转至 Azure 门户。
    2. 选择 MobileIron 应用程序。
    3. 单击**密钥**，然后在**密钥说明**中输入名称，并在**持续时间**中选择到期时间段。
    4. 单击**保存**并复制**密钥**的值。
    5. 返回管理员门户中的**管理员 > Microsoft Azure > Office 365 应用保护**。
    6. 将其粘贴到**应用程序密钥**（客户端密钥）字段中。

将**租户 ID** 粘贴到 Ivanti Neurons for MDM 管理门户中。

6. **步骤**
    1. 转至 Azure 门户。

2. 点击左侧窗格中的 Entra ID，然后点击“属性”。
3. 复制目录 ID。
4. 返回管理员门户中的**管理员 > Microsoft Azure > Office 365 应用保护**。
5. 将其粘贴到**租户 ID** 字段。

输入您的 Intune 管理员**用户名**和**密码**。

- Azure 帐户应拥有全局管理员权限或受限管理员 + Intune 服务管理权限。
- Ivanti 建议仅使用 Intune 服务管理权限创建本地 Azure 帐户。 Microsoft 不支持与身份提供商联合的用户帐户，以通过 Graph API 进行身份验证。

单击**验证并保存**。
如果提交日期不正确，则会显示错误消息。

Office 365 应用程序保护策略

在配置 Microsoft Graph 凭据后，转到**应用 > Office 365 应用保护**，以为不同用户组添加适用于 iOS 或 Android 设备的新 Office 365 应用保护策略。

应用程序策略**选项卡中的应用程序 > Office 365 应用程序保护**页面将显示这些策略。 此策略列表提供表格详细信息，例如更新的时间戳、平台、分配的应用程序和部署的用户组。

为 iOS 设备添加 Office 365 应用程序保护策略

程序

1. 转至**应用程序 > Office 365 应用程序保护**。
2. 单击**应用程序策略 > + 添加**。
3. 为该策略输入**名称**和可选**说明**。
4. 在选择操作系统下，单击 **iOS**。
5. 在**数据重新定位**下，从以下设置和选项中进行选择：
   - 防止 iTunes 和 iCloud 备份
   - 允许应用程序将数据传输到其他应用程序 - 所有应用程序（默认）、策略管理应用程序、无
   - 允许应用程序从其他应用程序接收数据 - 所有应用程序（默认）、策略管理应用程序、无
   - 防止“另存为”
   - 限制使用其他应用程序剪切、复制和粘贴 - 任何应用程序（默认）、阻止、策略管理应用程序、通过粘贴进行管理的策略
   - 限制 Web 内容显示在托管浏览器中
   - 加密应用程序数据 - 设备被锁定时（默认）、设备被锁定且存在打开的文件时、设备重新启动后、使用设备设置
   - 禁用联系人同步
   - 禁用打印
6. 在**访问**下，从以下设置和选项中进行选择：
   - 需要 PIN 才能访问
   - 重置 PIN 之前的尝试次数（默认值为 5）
   - 允许简单的 PIN

- PIN 长度（默认为 4）
- 允许指纹而不是 PIN (iOS 8+)
- 管理设备 PIN 时禁用应用程序 PIN
- 要求公司凭据才能访问
- 阻止托管应用程序在越狱或根源设备上运行
- （分钟）后重新检查访问要求
  - 超时 - 必须是介于 1 和 65535 之间的值（默认值为 30）
  - 离线 - 宽限期必须介于 1 和 65535 之间（默认值为 720）
  - 应用程序数据擦除之前的离线间隔（天） - 必须是介于 1 和 65535 之间的值（默认值为 90）

要求最低的 iOS 操作系统

- 要求最低的 iOS 操作系统（仅限警告）
- 需要最低应用程序版本
- 要求最低应用程序版本（仅限警告）
- 需要最低 Intune 应用程序保护策略 SDK 版本

单击**下一步**。

8. 选择并分配将应用此策略的应用程序。
9. 单击**下一步**。
10. 选择将应用此策略的用户组。
11. 单击**完成**。

为 Android 设备添加 Office 365 应用程序保护策略

步骤

1. 转至**应用程序 > Office 365 应用程序保护**。
2. 单击**应用程序策略 > + 添加**。
3. 为该策略输入**名称**和可选**说明**。
4. 在选择操作系统下，单击 **Android**。
5. 在**数据重新定位**下，从以下设置和选项中进行选择：
   - 防止 Android 备份
   - 允许应用程序将数据传输到其他应用程序 - 所有应用程序（默认）、策略管理应用程序、无
   - 允许应用程序从其他应用程序接收数据 - 所有应用程序（默认）、策略管理应用程序、无
   - 防止“另存为”
   - 限制使用其他应用程序剪切、复制和粘贴 - 任何应用程序（默认）、阻止、策略管理应用程序、通过粘贴进行管理的策略
   - 限制 Web 内容显示在托管浏览器中
   - 加密应用程序数据
   - 启用设备加密时禁用应用程序加密
   - 禁用联系人同步

- 禁用打印

6. 在**访问**下，从以下设置和选项中进行选择：
   - 需要 PIN 才能访问
   - 重置 PIN 之前的尝试次数（默认值为 5）
   - 允许简单的 PIN
   - PIN 长度（默认为 4）
   - 允许指纹而不是 PIN (Android 6+)
   - 管理设备 PIN 时禁用应用程序 PIN
   - 要求公司凭据才能访问
   - 阻止托管应用程序在越狱或根源设备上运行
   - （分钟）后重新检查访问要求
     - 超时 - 必须是介于 1 和 65535 之间的值（默认值为 30）
     - 离线 - 宽限期必须介于 1 和 65535 之间（默认值为 720）
     - 应用程序数据擦除之前的离线间隔（天） - 必须是介于 1 和 65535 之间的值（默认值为 90）
   - 拦截屏幕截图和 Android 助手
   - 要求最低的 Android 操作系统
   - 要求最低的 Android 操作系统（仅限警告）
   - 需要最低应用程序版本
   - 要求最低应用程序版本（仅限警告）
   - 需要最低 Intune 应用程序保护策略 SDK 版本
7. 单击**下一步**。
8. 选择将应用此策略的应用程序。
9. 单击**下一步**。
10. 选择将应用此策略的用户组。
11. 单击**完成**。

修改 Office 365 应用程序保护策略

程序

1. 转至**应用程序 > Office 365 应用程序保护**。
2. 单击**应用程序策略**。
3. 单击您要修改的策略的名称。
4. 在策略详细信息页面上，单击**编辑**。
5. 修改策略配置设置。
6. 单击**下一步**。
7. 修改将应用此策略的应用程序列表。
8. 单击**下一步**。
9. 修改将应用此策略的用户组。

10. 单击**完成**。

删除 Office 365 应用程序保护策略

程序

1. 转至**应用程序 > Office 365 应用程序保护**。
2. 单击**应用程序策略**。
3. 在**操作**列下，针对要删除的策略名称，单击删除图标。
4. 单击**是**进行确认。

Office 365 应用程序配置

转至**应用程序 > Office 365 应用程序保护**页面，在**应用程序配置**选项卡中，为不同的用户组添加、修改或删除 Office 365 应用程序配置。 在这些应用程序配置中，管理员可以添加键值对列表。 并将配置分配给一个或多个 Office 365 应用程序。 “应用程序配置”选项卡列出具有表格详细信息的配置，例如更新的时间戳、分配的应用程序和部署状态。

添加 Office 365 应用程序配置

程序

1. 转至**应用程序 > Office 365 应用程序保护**。
2. 单击**应用程序配置 > + 添加**。
3. 为该配置输入**名称**和可选**说明**。
4. 输入键值对。
5. 单击**下一步**。
6. 选择将应用此配置的应用程序。
7. 单击**下一步**。
8. 选择将应用此配置的用户组。
9. 单击**完成**。

修改 Office 365 应用程序配置

程序

1. 转至**应用程序 > Office 365 应用程序保护**。
2. 单击**应用程序配置**。
3. 单击您要修改的配置的名称。
4. 在配置详细信息页面上，点击**编辑**。
5. 或者，单击**应用程序分配**或**用户组分配**选项卡。 单击**编辑**仅修改这些设置，并单击**保存**。
6. 修改策略配置设置。
7. 单击**下一步**。
8. 修改将应用此配置的应用程序列表。
9. 单击**下一步**。
10. 修改将应用此配置的用户组。

11. 单击**完成**。

删除 Office 365 应用程序配置

程序

1. 转至**应用程序 > Office 365 应用程序保护**。
2. 单击**应用程序配置**。
3. 在**操作**列下，单击要删除的配置名称的移除图标。
4. 单击**是**进行确认。

使用 Office 365 应用程序的用户不合规

管理员可以查看不合规行为的用户及其设备列表。 使用此页面可擦除此类已标记设备上的任何 Office 365 应用程序。

擦除 Office 365 应用程序

程序

1. 转至**应用程序 > Office 365 应用程序保护**。
2. 单击**不合规用户**。
3. 执行以下操作之一：
   - 从列表中选择用户，然后单击**擦除 Office 365 应用程序**。
   - 单击该用户的名称，以显示不符合应用程序要求的设备列表。 在**操作**列下，单击特定设备的**擦除 Office 365 应用**图标。
   - 单击该用户的名称，以显示不符合应用程序要求的设备列表。 单击特定设备的名称，以查看列出的应用，以及捆绑 ID/软件包名称和标记原因。 单击**擦除 Office 365 应用程序**。
4. 单击**是**，确认操作。

或者，执行以下步骤：

1. 转到**用户**。
2. 单击用户名以显示用户详细信息页面。
3. 单击**操作 > 擦除 Office 365 应用程序**。
4. 选择需要擦除 Office 365 应用程序的设备。
5. 单击**确定**，确认操作。

取消对 Office 365 应用程序的擦除请求

程序

1. 转到**用户**。
2. 单击用户名以显示用户详细信息页面。
3. 单击 **Office 365 保护**选项卡。
4. 在**选择报告类型**下拉框中，选择**擦除请求**报告，以便显示相应的信息。
5. 选择需要取消擦除请求的设备。 只能选择具有“待定擦除”状态的设备。
6. 单击**取消擦除**。

7. 单击**确定**，确认操作。

具有 Office 365 应用程序保护的用户的应用程序报告

管理员可以选择以下报告之一来查看具有 Office 365 应用程序保护的用户列表及相关信息：

- 应用程序策略报告
- 应用程序配置报告
- 擦除请求

应用报告中的信息包括捆绑 ID/软件包名称、设备名称、设备类型、策略或配置（部署到设备）、状态（已同步、已同步但过期或未同步）以及上次签入时间。 可以将应用程序报告中的信息导出为 CSV 文件，以供日后参考或分析。

“擦除请求”报告中的信息包括显示名称、用户名、设备名称、设备类型和擦除状态（擦除待定或擦除完成）。

执行以下步骤以查看其中一个报告：

1. 转到**用户**。
2. 单击用户名以显示用户详细信息页面。
3. 单击 **Office 365 保护**选项卡。
4. 在**选择报告类型**下拉框中，选择其中一个报告，以显示相应的信息。
5. （可选）在“擦除请求”报告页面中，选择需要取消擦除请求的设备，然后单击**取消擦除**。 只能选择具有“待定擦除”状态的设备。
6. （可选）单击**导出为 CSV**，将报告内容下载到 CSV 文件中，以供日后参考或分析。

12.6. 与 Google 应用连接

本部分包含以下主题：

- 受管 Google Play 帐户（Android Enterprise 帐户）
- Android 设备注册
- Android 管理 API
- Google Apps API
- 管理员 - Android Enterprise

12.6.1. 受管 Google Play 帐户（Android Enterprise 帐户）

许可证：Silver

需要受管 Google Play 帐户，才可以支持 Android Enterprise 设备的使用和配置。 您不必再使用 Google Apps Directory Sync (GADS) 或使用 Google 账户注册设备。

重要：如果您已设置 Android Enterprise，则必须先停用这些设备，才可以使用该功能。

使用已托管 Google Play 帐户配置 Android Enterprise

步骤

1. 登录 Ivanti Neurons for MDM 门户。
2. 前往**管理员 > Google > Android Enterprise**。
3. 在**托管的 Google Play 帐户**中，单击**授权 Google**，以便显示 **Google Play for Work** 页面。
4. 输入您的 **Google Play 帐户电子邮件 ID**。
5. 单击**入门指南**。
6. 接受 Android Enterprise 协议。
7. 单击**确认**。
8. 单击**完成注册**。
   Android Enterprise 已配置部分显示以下信息：
   - **状态**
   - **管理员电子邮件**
   - **企业类型**
   - **Google Enterprise ID**

在 Android Enterprise 使用受管 Google Play 帐户进行设置，每个用户注册的设备数量会受到限制。 要克服此局限性，请在创建新用户时选择**Android Enterprise 设备帐户**选项，启用此帐户附带的 Android Enterprise 工作受管设备注册，并自动分配 Google 设备帐户。

设备账户用于 COSU（一次性）部署（例如，使用自助服务终端模式）。 拥有设备账户的用户可能拥有有限的 Google Play 访问权限。

有时，受管 Google Play 帐户或令牌出于多种原因过期，例如身份验证令牌过期，或将删除的帐户或企业。 在此类情况下，Google Play 服务将通过广播操作通知客户端；通过移除现有帐户并添加包含从 UEM 服务器获取的新令牌的帐户，该操作将触发客户端重新配置设备。

如果帐户重新配置因为旧帐户无法移除或在重新配置时尝试次数过多而失败，将通知用户通过停用客户端或对设备执行出厂重置来重新开始，具体取决于设备是处于工作配置文件模式还是受管设备模式。

将现有的托管 Google Play 账户迁移到托管 Google 域账户 (BTE)

此功能可将 Android Enterprise 账户和设备从**托管 Google Play 账户**迁移到**托管 Google 域账户**。

迁移包括：

- 账户升级
- 设备迁移

先决条件

- 设备必须以工作托管设备或工作配置文件模式注册；在公司拥有设备上的工作配置文件 (WPCOD) 模式下注册的设备必须运行 Android 12 或更高版本。
- 设备被分配有效的公司或商业电子邮件 ID。

> 如果设备已分配给非公司电子邮件 ID，管理员必须重新分配有效的公司电子邮件 ID，以使设备有资格进行迁移。

升级 Android Enterprise 账户

将 Android Enterprise 账户从托管 Google Play 账户升级到托管 Google 域账户。

程序

1. 前往**管理员** > **Google** > **Android Enterprise**。
2. 单击**升级账户**。
3. 使用有效的公司或商业电子邮件 ID 登录。
4. 完成升级过程。
5. 刷新页面。

应用设备迁移配置

程序

1. 导航到配置。
2. 选择 **Android Enterprise：从托管 Google Play 到托管 Google 账户的设备迁移**配置 > **编辑** > **下一步** > **所有设备或自定义** > **缓慢推出分发** – 默认情况下，**手动推出**选项已选中 > 从下拉列表**选择摘要中的自定义设备百分比（缓慢推出）**或**选择摘要中的所有设备**进行选择。
3. 单击**完成**。

完成设备迁移

程序

1. 在设备上，当提示“添加工作账户”时点击**继续**。
2. 验证**公司电子邮件 ID**。
3. 输入**密码**。
4. 如果可用，请完成**双因素身份验证 (2FA)**。
5. 完成账户设置流程。

验证迁移

在设备上

1. 打开 **Google Play** 商店。
2. 确认账户类型已从工作账户更改为公司域账户。

在管理员控制台中

- 要查看**Android Enterprise：从托管 Google Play 到托管 Google 账户的设备迁移**配置状态，请导航至**设备** > **设备** > **设备详细信息** > **配置** > **Android Enterprise：从托管 Google Play 到托管 Google 账户的设备迁移**。 确保配置状态处于已安装状态。

监控迁移状态

管理员可以使用以下方法跟踪迁移（**已迁移至托管 Google 账户**）进度：

- **设备详细信息** – 查看每台设备迁移状态
- **高级搜索** – 筛选已迁移和未迁移设备
- **设备组** – 对迁移和非迁移的设备进行分组

这些选项有助于识别需要进一步操作的设备。

采用托管 Google 域账户 (BTE) 的新注册

Android Enterprise 可以使用**托管 Google 域账户**进行配置，无论是否具有 Google 身份验证。

程序

1. 登录门户。
2. 前往**管理员** > **Google** > **Android Enterprise**。
3. 在**托管 Google Play 账户**下，单击**授权**。
4. 输入您的**公司**或**企业电子邮件 ID**，然后单击**下一步**。
5. 选择**创建新绑定于..** 在**选择绑定选项**页面中。
6. 单击**确认**。 将显示**跳过**和**启用**选项。

- **跳过** – 在没有身份验证的情况下继续
- **启用** – 在有身份验证的情况下继续

Android Enterprise 部分显示以下信息：

- **状态**：显示连接状态。
- **管理员电子邮件**：显示公司或商业电子邮件 ID。
- **企业类型**：显示企业类型。
- **Google 身份验证设置**：根据身份验证要求显示否/是。
- **Google Enterprise ID**：显示唯一的 Google Enterprise ID。
- **企业名称**：显示企业名称。

12.6.2. Android 设备注册

在 Android 设备注册期间，如果您需要用户提供的电话许可才能完成注册（需要报告 IMEI、电话号码和其他电话标识符），您可以配置此选项。 配置时，系统将提示设备用户授予允许 Go 客户端访问设备标识符的权限。

> 此配置仅适用于 Android 版本高于 6.0 的所有 Android 设备的新注册。

1. 选择**管理员 > Google > 注册**。
2. 选择**注册期间需要 Android 设备标识符（工作配置文件和设备管理员）**。
3. 单击**保存**。

有关遗失模式的更多信息，请参阅**管理遗失模式下的 Android 设备**

12.6.3. Android 管理 API

Android 管理 API (AMAPI) 是 Google 提供的云平台 API，用于将 Google Android UEM 功能集成到 Ivanti Neurons for MDM。 在 Android Enterprise 设置中，您可以启用 Android 管理 API 框架以管理 Android Enterprise 设备，无需将客户端应用安装到适用于设备管理的设备。 目前，不支持将 Go app 推送给设备的其他功能，如 MTD 等。

在设置中配置 Android Enterprise 帐户时，您将可以启用并使用 Android 管理 API 框架。 在启用后，您可以：

- 添加注册配置文件，以将 QR 码用于设备注册。
- 出于特定目的，为已注册设备创建专用设备配置（企业拥有的单用途或 COSU）。

目前，只有在运行 Android 版本 9 或更高版本并且安装 Google Play 和在专用模式中配置的设备，才支持 Android 管理 API。 企业专用模式也称为企业拥有的一次性 (COSU) 模式，并且属于其中一种设备所有者模式。 此功能也支持以下设备操作：

- 锁定
- 重新启动
- 同步到服务器
- 擦除

设备签入计划于定期（每小时）实施。 但如需立即采取措施，使用设备详细信息页面中的设备操作“同步到服务器”。 AMAPI 设备不会将强制签入发送到 Ivanti Neurons for MDM。 在设备有活动时，执行库存更新。

启用 Android 管理 API

要启用 Android 管理 API，请转至**管理员 > Android Enterprise > 授权 Google（需要有效的 Google 地址）> 已启用 Android Enterprise**。

已启用的 Android 管理 API 功能的状态（**是**表示已启用，**否**表示已禁用）也会显示在“设备详细信息”页面中。

> COSU 目前不支持 GSuite 帐户。

添加注册配置文件

对于使用 QR 码扫描或令牌的字母数字字符串注册的 Android 设备，需要创建注册配置文件。 仅在 Android 管理 API 启用时，才可以创建注册配置文件。 您也可以创建与注册配置文件关联的自定义设备属性。

1. 选择**管理员 > Android Enterprise > 注册配置文件**。
2. 在**注册配置文件 - 企业拥有的专用设备**窗口中，配置以下设置。
3. 单击**保存**。 **配置文件摘要**窗口会显示以下令牌详细信息：

设置	说明
名称	输入可标识此注册配置文件的名称。
描述	输入阐明此注册配置文件目的的描述。
用户名 **令牌有效性**	输入有效用户名的前几个字母，并从显示的匹配结果中选择一项。 有效用户名可以来自本地用户或 LDAP 用户。 注册配置文件会标记使用配置文件中的 QR 码进行注册的设备，以显示为属于创建注册配置文件的用户的设备。 对于令牌 QR 码扫描进行身份验证，输入其有效期的天数。 输入的数字应介于 1-30 之间。 如果您在过期后使用令牌或注册配置文件，设备会重置。
自定义设备属性	在操作列中，单击 **+ 添加新内容**，以添加与注册配置文件关联的自定义设备属性。 1. 在**属性名称**列中，从下拉列表选择自定义设备属性。 2. 在**值**列中，输入自定义属性的值。 3. 单击**保存**。 表会显示已添加的自定义设备属性。 要删除，单击操作列中的**删除**选项。 自定义属性只能在创建配置文件时添加到注册配置文件中。 属性字段无法在配置文件创建后编辑。

- 名称
- 说明
- 用户名
- 令牌创建日期
- 令牌到期日期
- 令牌值
- QR 代码
- 自定义设备属性

> 如果在注册后的 10 分钟时段内未获取适当的设备配置，设备将重置。 在此情况下，您应使用注册令牌/QR 码重新注册

在创建注册配置文件时，将列在**注册配置文件**页面中。 在**操作**列中，您可以执行以下任意操作。

- 单击查看图标，以在配置文件摘要窗口中查看注册配置文件的详细信息。 此窗口也会显示 QR 码。
- 单击编辑图标，以编辑注册配置文件的详细信息。

> 您仅可编辑令牌有效性。 无法编辑其他属性。

单击删除图标，以删除注册配置文件。

创建 COSU 配置

通过 Android Enterprise 或专用设备（企业拥有的单用途或 COSU）配置，管理员可以配置可用于特定目的的专用设备。COSU 配置已分发到工作托管设备（设备所有者模式），以在自助服务终端模式中仅向用户提供一个应用。 不支持公司拥有设备上的工作配置文件中的设备。

使用此配置，管理员可以配置设备，以将应用固定到屏幕；这样，自助服务终端模式用户无法取消固定此应用，并导航离开应用到设备的其他屏幕，或在设备上使用任何其他应用。

通过在"高级选项和应用配置"中选择"在设备上安装"选项，其他应用也可以在 AMA 设备上强制安装；但在自助服务终端应用通过配置固定到屏幕时，您将无法与其进行交互。 对于多应用自助服务终端，建议使用工作托管设备（设备所有者模式）的自助服务终端功能。 此功能将对应用和设备设置提供更多控制，并且也可以扩展到多用户模式。

通过按需查看各种选项，管理员可以更改配置，例如允许系统导航，以及通过 Google DPC 使用推送到最终用户的设备的其他应用。

为用户分配的优先级确定 COSU 配置。 优先级最高的配置会用于将策略配置推送到 Google。 COSU 配置会应用于已定义空间中的设备。 如果在默认空间中定义，将委派到其他空间。

要配置：

1. 转到**配置 > + 添加**。
2. 在**锁定和自助服务终端：Android Enterprise 配置**中，单击**专用设备（企业拥有的单用途或 COSU）**。
3. 输入配置的名称。
4. 输入描述。
5. 通过单击相关选项卡，您可以配置以下设置：

- **应用设置**
- **通用锁定**
- **自助服务终端自定义**
- **系统设置**

下表会提供可配置字段的详细信息：

设置	说明
应用设置	
应用名称	通过键入应用名称，或键入应用名称的首字母，选择要在设备上固定的应用，直到您在下拉列表中看到所需的应用。 如果您未在下拉列表中看到所需的应用，请确保要部署的应用是 Play Store 中的可用公共/私人应用，并且已添加到 App Catalog。 此字段是必填字段。 如果您未在此字段中选择要添加的应用，将不允许创建配置。 您仅可添加公共和私人应用。 无法添加内部应用和 Web 应用（私人）。
通用锁定	
保持屏幕开启	对于需要保持开启状态的设备，将电池配置为插入模式。 选择以下任一选项： • **AC** - 电源是交流充电器 • **无线** • **USB** - 电源是 USB 端口 • **任意** - 电源来自交流充电器或 USB 端口，或者无线充电器。
自助服务终端自定义	
自定义状态栏	选择以下任意选项，以自定义目标设备中的状态栏： • **通知和系统信息已启用** - 在状态栏中显示系统信息和通知。 • **仅启用系统信息** - 仅在状态栏中显示系统信息。
自定义系统导航	选择以下任意选项，以指定在 kiosk 模式中对导航功能（主页和概览按钮）的访问权限： • **已启用** - 启用主页和概览按钮导航。 如果选择此选项，用户可以导航到指定应用外部。 • **已禁用** - 禁用主页和概览按钮导航。 • **仅限主页按钮** - 仅启用主页按钮导航. 所有这些选项提供返回按钮。
启用全局操作	选择以在自助服务终端模式中启用全局操作。 通过此选项，控制与电源按钮关联的重启和关机功能。
启用系统错误对话框	选择以在自助服务终端模式中启用崩溃或无响应应用的错误对话框。
系统设置	
系统更新设置	配置以下设置，以管理系统更新： • **系统更新** - 选择所需的系统更新类型。 ◦ **自动** - 在更新可用时立即自动安装。 ◦ **推迟** - 自动安装最多推迟 30 天。 ◦ **窗口化** - 在每日维护时段内自动安装。 设置维护时段的开始和结束时间。 在设备上安装的更新可能会因支持的功能集、Android 版本和在设备上安装的 Google DPC 版本而异。

设置	说明
	• **冻结期** - 在冻结期期间设置设备时，将阻止所有传入系统更新，并且不会安装。 单击**添加冻结期**，以设置冻结期的**开始日期**和**结束日期**。 在设备冻结期结束时，将应用正常更新行为。 如果结束日期在开始日期前，冻结期将在当年和下一年之间延长。 冻结期可以设置为最多 90 天。 2 个连续冻结期必须间隔至少 60 天。

6. 单击**下一步**。
7. 选择下列分配选项之一：

- **所有设备**
- **无设备**（默认）
- **自定义**

8. 单击**完成**。

管理 AMAPI 设备中的应用

在将 COSU 配置分发到设备时，应用将推送并固定到 AMA 设备的屏幕。 无论 COSU 配置是否推送到设备，都可以管理在 AMA 设备上安装的应用。 以下是这些设备中的应用管理的详细信息：

- 仅支持公共私人应用；不支持内部应用和 Web 剪辑。
- 仅在安装设置启用“在设备上安装”或“静默安装”选项时，才可以推送应用。 在未启用其中任意选项的情况下，设备或设备的 Play Store 将不会显示分配到用户/设备的应用，以进行任何用户操作。
- 支持的应用配置是托管 Google Play 和工作托管设备 (Android for Work) 设置。 支持应用程序的托管配置，包括对 OEMConfig 应用程序的托管配置的支持。

> 安装和卸载配置的完成时间可能会有所不同，具体取决于 Google（消息服务）发送的关于是否已执行所需操作的通知。

- 现在，Go app 将默认作为 AMA 设备注册的一部分进行安装。 在注册过程中，应用程序将固定到屏幕，并将于设置完成后在后台运行。

> 除了基于制造商、操作系统版本和安全补丁级别的设备注册要求强制实施之外，不支持其他策略。 支持“设备允许列表”功能，该功能仅允许列入允许列表的设备注册 Ivanti Neurons for MDM。

管理 AMAPI 设备上的应用程序反馈支持

可以在 AMAPI (COSU) 设备上管理应用程序反馈支持。 当设备在 AMAPI (COSU) 模式下完成注册后，托管应用程序配置将直接从 Google 推送到 Ivanti Neurons for MDM，无需 Go app 进行任何干预。 可以通过**设备详细信息 > 安装的应用程序 > 查看反馈**在设备级别查看托管应用程序反馈信息，或者也可以在“应用程序配置反馈”选项卡下的应用程序目录中导航至特定的 Android 应用程序，在单个应用程序级别查看托管应用程序反馈信息，以便了解所有设备的总体报告。 有关应用程序反馈机制的信息，请参阅同步和获取应用反馈。

AMAPI 局限性

AMAPI 目前具有以下限制：

- 仅支持专用设备（COSU 模式）。

支持的配置

AMAPI 支持以下配置：

- 应用分发（单个或多个应用）
- 应用的托管应用配置推送到设备
- Wi-Fi 配置
- Android 企业锁定专用 (COSU) 配置
- Always-on VPN 配置

12.6.4. Google Apps API

由于协议中的限制阻止设备支持由单点登录 (SSO) 触发的外部身份验证服务重新定向，因此利用 SSO 验证 Google Apps 服务用户访问权的 Google 客户可能无法通过 Exchange 将用户连接至电子邮件、联系人和日历。 通过创建和管理 ActiveSync 连接的帐户密码，此服务可解决此问题。

先决条件

在尝试配置 Google Apps API 特性前，您需要：

- 管理员访问 https://console.developers.google.com/. 上的账号。
- 管理员访问 https://admin.google.com. 上的账号。

启用 Google Apps API 功能

程序

1. 选择**管理员 > Google > Google Apps API**。
2. 单击左侧标签 1 处矩形底部的**步骤 1：Google Dev**。
3. 步骤 1：“Google Dev”页面出现。
   按照“步骤 1：Google Dev”页面出现的指示操作，然后单击**完成**。
4. 单击中间标签 2 处矩形底部的**步骤 2：Google Admin**。
5. 步骤 2：“Google Admin”页面出现。
   按照“步骤 2：Google Admin”页面出现的指示操作，然后单击**完成**。
6. 在右侧标签 3 处矩形的**输入 Google 管理员用户名称**字段中，输入 Google 管理员用户名称。
7. 在同一矩形中，单击**选择文件**，上传您在步骤 1 中下载的 JSON 文件。
8. 单击**保存**。
9. 如果您未看到 Google Apps API 页面，这可能是您没有所需权限。 您需要以下角色之一：
   - 系统管理
   - 系统只读

12.6.5. 管理员 - Android Enterprise

许可证：Silver

- Email+、Docs@Work 和 Web@Work 等支持 Android Enterprise 的Ivanti, Inc生产力应用程序需要黄金许可证。
- Tunnel for Android Enterprise 需要铂金许可证。

Android Enterprise 支持使用和配置 Android Enterprise 应用程序。 Android Enterprise 用户可以从应用程序目录以及通过 Google Play 查看和安装应用程序。

如果您是新客户，默认情况下，应用程序分配设置为按设备。 您不能更改此设置。 对于升级客户，您可以选择按用户或按设备分配应用程序。 此外，对于升级客户，默认情况下会选择按用户分配应用程序。 许多用户有多个设备。 如果用户有多个设备，当应用程序分配设置为“按设备”时，您可以在每个设备上提供不同的应用程序集。

本部分包含以下主题：

- 配置 Android Enterprise
- 配置 Android Enterprise 工作配置文件

配置 Android Enterprise

1. 在 Ivanti Neurons for MDM 门户中，点击**管理员 > Google > Android Enterprise**。
2. 选择下列选项之一：
   - **托管 Google Play 帐户：**针对非 G Suite 订阅企业，此方法允许用户注册 Android Enterprise，而无需发送任何个人信息（向 Google 发送电子邮件地址）。 Ivanti Neurons for MDM 将通过 Google 自动提供和管理用户。 系统会要求您使用 Google 管理员帐户授权 Android Enterprise。
   - **托管 Google 帐户：**针对订阅了 G Suite 的企业，此方法允许用户使用其 Google 帐户注册 Android Enterprise。 每位用户都必须拥有 Google 帐户才能注册 Android Enterprise。

按照屏幕上的说明完成配置过程：

4. 对于自动方法，这包括：
   - 启用 UEM API 并创建企业凭据。
   - 通过授权整合的所有者来登录 Google。 这应该是 IT 账户，而不是个人账户。
   - 通过拖放您的服务账户 JSON 客户端 ID 来设置您的凭据。

对于替代方法，这包括：

   - 请参阅以下部分中的客户端 ID，并将其添加到 Google 管理门户。
   - 在 Google 管理门户中查找您的 MDM 令牌，并在 Google Cloud Console 中查找您的服务帐户。
   - 在 Ivanti Neurons for MDM 中，输入您的 MDM 令牌、企业 Google 域和企业管理员电子邮件地址以连接到 Google 服务。
   - 在 Ivanti Neurons for MDM 中，拖放您的服务帐户 JSON 客户端 ID。
   - 在 Ivanti Neurons for MDM 中点击**授权**，授权 Ivanti Neurons for MDM 查看和/或管理 Google 用户。

Ivanti Neurons for MDM 用户界面会指导您完成这些步骤。

用于绑定 Ivanti Neurons for MDM 与托管 Google 帐户的客户端 ID

在管理控制台中添加客户端 ID 为**140561810807-tiiglke17laibbrt5darupmvo4ae7cbj.apps.googleusercontent.com**，将 Ivanti Neurons for MDM 租户与受管 Google 帐户绑定。

配置 Android Enterprise 工作配置文件

1. 在 Ivanti Neurons for MDM 门户中，前往**配置**。
2. 点击 **+ 添加**。
3. 选择**锁定和自助服务终端：Android Enterprise** 配置。
4. 输入配置名称和说明。
5. 单击**工作配置文件**锁定类型。
   选择您要应用到目标设备中的**锁定设置**。
   重要：当用户使用"设置"中的"添加账户"添加 Google 账户时，Google 身份验证服务器会检查是否将该账户的域注册为 UEM 托管的域。请确认，是否选中**对 Android 设备强制实施 UEM 策略**。 如果是，GO 客户端会自动安装或更新（如果尚未在设备中安装）和启动。 在用户完成整个注册过程后，系统会提示用户创建工作配置文件，Google 帐户会自动迁移到该工作配置文件。

12.7. 使用 ChromeOS 设备

本部分包含以下主题：

- ChromeOS 和 Ivanti Neurons for MDM
- 向 ChromeOS 设备分发 Android 应用程序
- ChromeOS 蓝图配置
- 设备操作
- 常见问题解答
- 建议的评估步骤

12.7.1. ChromeOS 和 Ivanti Neurons for MDM

ChromeOS 是基于 Linux 的操作系统，由 Google 创建和发布。 Ivanti Neurons for MDM 支持 Android、Windows、iOS 和 macOS 设备。这种支持现在也已扩展到 ChromeOS 设备。 Ivanti Neurons for MDM 为配置和管理 ChromeOS 设备提供统一且简单的移动管理解决方案。Ivanti 为 ChromeOS 设备提供统一、简单且功能丰富的解决方案，类似于 Ivanti Neurons for MDM 上针对 iOS、Android、Windows 和 Mac 的管理工作流。 管理员可以从**管理员 > Google > ChromeOS 管理**使用简单集成，直接连接 Ivanti Neurons for MDM 与 Google Cloud（也称为 Google 管理控制台）。

先决条件

1. 必须具有托管 Google 管理员帐户。
2. 必须在 Google 管理控制台上导入 LDAP 用户和 OU。 Ivanti Neurons for MDM 仅支持从 LDAP 源导入的 OU。 不支持本地 OU。
3. 管理员必须已经将组织单位（用户组）同步到 Ivanti Neurons for MDM。 可以通过配置 LDAP 服务器和添加组织单位来完成此操作。

授权 Google

在 Google 管理控制台上可用的 ChromeOS 设备不能直接注册到 Ivanti Neurons for MDM。 相反，这些设备将注册到 Google，其相关信息会在 Google 和 Ivanti Neurons for MDM 之间同步。 管理员必须授权 Google 导入设备并执行其他操作，比如分配应用程序和配置等。

步骤

1. 转到**管理员 > Google > ChromeOS 管理**。
2. 点击**授权 Google**。
3. 选择要授权的 Google 管理员帐户。
4. 点击**继续**接受提供所需服务的权限。
   屏幕上显示 **ChromeOS 设置成功**确认消息。 也可以在确认信息下找到域信息。

从 Google 同步 ChromeOS 设备

管理员必须从 Google 管理控制台同步 ChromeOS 设备。 初次使用 Google 管理控制台访问 ChromeOS 设备时，管理员必须在“ChromeOS 管理”页面使用“立即同步”选项手动同步设备。

> 初次手动同步设备后，后续同步将每小时自动进行一次。

删除 Google 管理员控制台与 Ivanti Neurons for MDM 的集成

删除集成将撤销我们从 Google 收到的 Google 资源访问 OAuth 令牌。 此操作将删除 ChromeOS 设备、与蓝图配置和应用程序配置关联的清单，以及注册元数据。 蓝图配置和上传的应用程序不会被删除。

如果租户注册未删除，您可以提交票证排查问题。

步骤

1. 转到**管理员 > Google > ChromeOS 管理**。
2. 在 ChromeOS Ivanti Neurons for MDM 注册部分下，点击**删除**。
   屏幕上将出现一个弹出窗口，询问您是否要继续执行删除操作，同时提示您继续操作将删除与此集成关联的所有设备。 选择**确定**。

12.7.2. 向 ChromeOS 设备分发 Android 应用程序

管理员可以通过应用程序目录将 Android 应用程序分发给 ChromeOS 设备。

先决条件

1. 必须配置 Android Enterprise。 有关设置 Android Enterprise 的详细信息，请参阅**设置 Android Enterprise**。
2. Android 应用程序必须位于应用程序目录中。
3. 分发 Android 应用程序和 ChromeOS 蓝图配置前，请确保 ChromeOS 设备 (Chromebook) 用户属于用户组（也称为组织单位）。

确定 Android 应用程序后，需要按照与分发任何其他应用程序类似的流程来分发该应用程序。 分发 Android 应用程序时，请确保选择要向其分发应用程序的用户组，然后在设备上执行静默安装。

> 如果现有的 Android 应用程序部署设置为分发到设备/设备组或用户，则必须将分发更改为基于用户组。 如果该应用程序已在使用中，则此操作可能会影响现有部署。 建议先在全新的应用程序上执行此操作。

> 安装设置允许管理员控制最终静默安装，并且需要将应用程序推送到 ChromeOS 设备。 此处必须选择用户组。

12.7.3. 添加和分发 ChromeOS 扩展应用程序

管理员可以将 ChromeOS 扩展应用程序添加至应用程序目录，并将这些应用程序分发到 ChromeOS 设备。

步骤

1. 前往**应用程序** > **应用程序目录**。
2. 点击 **+ 添加**。
3. 从列表中选择 **ChromeOS**。 屏幕上会显示**添加 ChromeOS 应用程序详细信息**页面。
4. 提供以下详细信息：**应用程序名称** - ChromeOS 扩展应用程序的名称、**扩展 ID** - 可以从 Chrome Web Store 获取此信息。
5. 单击**下一步**。 屏幕上会显示**应用程序配置**页面。 您可以选择将在下一次设备签入时立即实施的即时更新，或您可以选择在新版本可用时自动更新应用。
6. 选择其中一个应用程序分发选项，并提供所需的详细信息。

> ChromeOS 应用程序分发仅适用于 LDAP 用户组。

确定 ChromeOS 扩展应用程序后，需要按照与分发任何其他应用程序类似的流程来分发该应用程序。 分发 ChromeOS 扩展应用程序时，请确保选择要向其分发应用程序的用户组，然后在设备上执行静默安装。

> 安装设置允许管理员控制最终静默安装，并且需要将应用程序推送到 ChromeOS 设备。 此处必须选择用户组。

您可以编辑有关 ChromeOS 扩展应用程序的信息，或从应用程序目录中删除 ChromeOS 扩展应用程序。 必须遵循与编辑或删除应用程序目录中的任何其他应用程序类似的流程。

编辑 ChromeOS 扩展应用程序

1. 转到**应用程序 > 应用程序目录 > 详细信息**。
2. 点击**编辑**。 进行所需更改，然后点击**保存**。

有关删除应用程序的详细信息，请参阅从应用程序目录删除应用程序。

12.7.4. ChromeOS 蓝图配置

ChromeOS 蓝图配置具有以下设置：

- 设备设置
- 用户和浏览器设置
- 托管访客会话设置

可以在特定用户组（也称为组织单位）上应用 ChromeOS 配置。 如果尝试分发 ChromeOS 蓝图配置，将只有“用户组”部分可用，并且与授权 Google 管理控制台关联的所有 LDAP 用户组都将列于该部分中。 可以选择一个或多个列出的组，然后应用配置。

步骤

1. 转到**配置 > 添加**。
2. 选择“操作系统”部分下的 **Google ChromeOS**。 屏幕上显示 **ChromeOS 蓝图配置**选项卡。
3. 点击 **ChromeOS 蓝图**。 屏幕上显示**创建 ChromeOS 蓝图配置**页面。
4. 在**名称**框中输入配置名称。
5. 您可以在“配置设置”下，根据需要修改设备设置、用户和浏览器设置和托管访客会话设置，并打开“推送到设备”按钮以应用修改的设置。
6. 单击**下一步**。
7. 选择**自定义**分发选项。

> 仅 LDAP 用户组可用于分发配置。

> 如果要向所有人分发配置，将只能针对 Ivanti Neurons for MDM 和 Google 管理控制台中可用的 LDAP 用户组进行分发。

选择一个或多个组，然后点击**完成**。

> 如果取消分发已分发的设置，将不会恢复应用的设置。

> 可以在 ChromeOS 蓝图配置中上传文件。

12.7.5. 设备操作

ChromeOS 设备支持以下操作：

- **擦除** - 擦除操作会删除设备上的所有数据，设备会重置为出厂设置。 有关详细信息，请参阅**擦除设备**。
- **锁定** - 锁定操作会限制您对设备进行任何操作。 有关详细信息，请参阅**锁定设备**。
- **解锁** - 解锁操作会释放设备以供进一步使用。 有关详细信息，请参阅**解锁设备**。

12.7.6. 常见问题解答

本节列出了在 Ivanti Neurons for MDM 上使用 ChromeOS 设备时可能会遇到的一些常见问题。

- Chromebook 管理与其他操作系统有何不同？
- 目前，Google 只允许基于 LDAP 用户组的配置分发，管理员应该确保在使用配置或应用程序时，基于 LDAP 用户组进行分发。
  ChromeOS 设备管理不支持本地用户组和设备组。
  管理 ChromeOS 设备需要 Ivanti 的哪些许可？
- ChromeOS 设备应具有 Chrome Enterprise Upgrade 或 Chrome Education Upgrade 等许可证。 这些许可证可以作为硬件的一部分从经销商处购买，也可以单独购买。 有关详细信息，请参阅 Google 文档。 要开始使用 Chrome 设备管理，需要 Ivanti Secure UEM（统一端点管理）许可。
  移动威胁防御 (MTD) 或类似的解决方案是否可用？ 是否需要单独的 MTD 许可证？
- 当前在产品中不可用，请参阅当前限制。 我们将通过常见问题解答和发布公告，提供更多有关功能变化的信息。
  为什么“配置和应用程序”选项卡不像其他设备那样具有详细信息？
- 由于配置分发给用户组，且并非基于登录的用户进行应用，因此目前配置不会显示在设备详细信息中。 应用程序遵循相同的分发逻辑，也具有相同的限制。 我们将通过常见问题解答和发布公告，提供更多有关限制变化的信息。
  ChromeOS 目前支持多少种配置？
- 对于 ChromeOS，我们减少了可用的配置磁贴数量，并减少了与配置相关的管理任务。 我们将此配置称为“ChromeOS 蓝图”。 在这些设备上，ChromeOS 蓝图支持近 700 种配置。 有关配置选项，请参阅 Google 文档。
  如何轻松管理适用于所有设备的单个配置？
- 管理员可以直接克隆现有配置，并针对各自的用户组进行修改（如果需要）。 无需从零开始。
  如何向 Chrome 设备添加 VPN 配置？
- 可以使用 Android 应用程序完成此操作，而不是使用本地 VPN。
  这些设备是否支持包括停用和擦除在内的设备操作？
- 企业 Chromebook 始终由组织管理，且此类设备上的数据被视为已经达到完全组织化程度。 请记住：
  - 阻止停用
  - 允许擦除
  - 允许锁定
  - 允许解锁
  - 其他操作 – 不支持

就硬件而言，Ivanti 支持哪些 Chromebook？

- Ivanti 本就支持 Google Cloud 设备管理解决方案支持的设备。 Ivanti 目前尚未公布 Ivanti 解决方案支持的具体硬件列表。
  哪个 Chrome 操作系统版本受到支持？
- Google Cloud 只支持 ChromeOS 的最新稳定版本，由于后端集成的缘故，Ivanti 支持与 Google 支持的模型相同。
  由于这是首次发布该功能，可以列出当前有哪些限制吗？

对于新 Chrome 操作系统支持，我们正在努力为客户提供其期待的功能。 以下是管理员应该注意的一些限制：

- Chrome 操作系统扩展（浏览器应用程序）目前不支持分发（作为“应用程序”）。
- 目前不支持 Android 应用程序的托管应用程序配置。
- Wi-Fi 配置 API 于近期发布，目前不受支持。
- 目前不支持证书分发。

- 目前不支持分发 Ivanti Go（原 MobileIron Go）Android 应用程序。
- 目前不支持 Ivanti Tunnel (VPN) 应用程序。
- 目前不支持空间和空间委派。
- 目前不支持移动威胁防御解决方案。
- 这些设备支持 Ivanti 零登录解决方案，被归类为非托管设备。
- 不完全支持策略操作。

12.7.7. 建议的评估步骤

建议采用以下步骤来验证解决方案：

1. 创建一个单独的 OU（用户组），该 OU 在目录源（例如 Active Directory）中有测试用户。 此操作可以避免对有效的组织单位产生任何影响。
2. 在 Ivanti、Google 和目录源 (LDAP) 之间同步用户。 验证用户组中是否有“测试 OU”。
3. 按照上述步骤，将 Ivanti Neurons for MDM 与 Google 集成。
4. 创建 ChromeOS 蓝图配置，并仅将其分发给“测试 OU”用户组。
5. 启动 Chromebook（即装即用或之前已注册）。 确保其显示在设备列表中。
6. 验证 ChromeOS 蓝图设置在设备上是否可用。
7. 按照类似于 Android 应用程序分发的步骤操作。

12.8. 固件管理

本部分包含以下主题：

- 正在注册 Zebra OTA 服务
- Samsung E-FOTA 许可证管理（已停用）

12.8.1. 正在注册 Zebra OTA 服务

在注册到 Zebra OTA（无线）服务时，您可以启用 Zebra OTA 配置，以接收并更新注册到 Ivanti Neurons for MDM 的 Zebra 设备的固件详细信息。

程序

1. 前往**管理员 > 基础设施 > Zebra OTA**。 随即显示 **Zebra OTA 服务**页面。
2. 在**链接到 Zebra OTA 服务**下，点击**开始**。
3. 输入 Zebra OTA 凭据登录，并按照步骤请求批准使用 Zebra 服务。
4. 单击**完成验证**，以确认连接到 Zebra 服务。 在连接确认时，Zebra OTA 服务页面将显示成功注册状态。

要撤销注册，请点击**操作**列下的**撤销**。 **撤销**操作将从现有配置中删除所有 Zebra OTA 配置。 要使用 Zebra OTA 重新注册，单击**刷新**。 刷新操作不会影响现有配置。

在注册后，您可以启用 Go 客户端在设备所有者模式中收到和应用于 Zebra 设备（在 Android 版本 8.0 或支持的更新版本上运行）的 Zebra 固件配置。 在应用配置时，系统将下载固件，并按照配置中的计划安装到设备。 有关启用 Zebra 固件配置的更多信息，请查看系统更新配置。

在完成固件更新时，在“设备”页面上的**系统更新**列中，您可在 Zebra 设备中查看固件更新状态。 以下是可能状态：

- **未知** - 客户端或 OS 不支持
- **最新** - 设备具有最新的可用更新
- **待处理** - 系统更新配置已应用，但未下载或应用更新
- **正在下载** - 系统更新正在下载到客户端
- **可用** - 系统更新目前对设备可用
- **错误** - 下载或安装出错。

“设备”页面中的 **Zebra 补丁版本**列显示设备的 Zebra 补丁信息。

> 运行 Android 11 及以上版本的设备不支持 **Zebra 修补程序版本**，仅支持 **Zebra 完整升级**。

12.8.2. Samsung E-FOTA 许可证管理（已停用）

Samsung E-FOTA 服务已于 2022 年 7 月停用。 请参阅 Samsung 公告了解详细信息。

> 从现在开始，您将无法配置 Samsung E-FOTA 服务。 但是，如果您已有 E-FOTA 配置，可通过导航至**管理员** > **固件管理** > **Samsung E-FOTA** 并点击**停用**选项来停用配置。

12.9. 管理脚本和文件

管理员可以管理可在配置中使用并推送到设备的脚本和文件。

本部分包含以下主题：

所有脚本

文件

12.9.1. 所有脚本

适用于：macOS 和 Windows 设备

在**管理 > 脚本和文件 > 所有脚本**页面中，Ivanti Neurons for MDM 允许具有系统管理角色的用户创建或上传和管理可用于配置并分发到设备的脚本。 您可以将自定义属性与脚本关联，并将结果值分配到配置的设备。 使用审计跟踪查看脚本更改的日志，使用设备详细信息页面查看执行结果。

您可以写入配置设备中任何设置的脚本。 例如，您可以运行脚本：

- 强制设备用户每月更改密码
- 在闲置时间达到 5 分钟后锁定屏幕
- 配置安全 Wi-Fi 网络。

本部分包含以下主题：

- 添加脚本
- 修改脚本
- 使用脚本变量（适用于 Windows 和 macOS）
- 测试脚本
- 验证脚本执行结果

添加脚本

您可以创建或上传 bash 脚本（适用于 macOS）和 ps1 脚本（适用于 Windows）的存储库。 此存储库可以在配置中使用，以选择脚本并分发，从而按照配置中的指定计划在设备上执行。

例如，您可以创建要在设备上执行的 Shell 脚本。 如果必要，您可以使用封装程序。 不支持从 Shell 脚本执行二进制文件。

> Ivanti 强烈建议您在设备上运行之前测试 Shell 脚本，以确保鲁棒性和质量。 本地运行脚本，并修复产生的任何错误。

程序

1. 转到**管理员 > 脚本 > 所有脚本**。
2. 单击 **+添加**
3. 输入脚本的名称和说明。
4. 在平台类型下，选择 macOS 或 Windows。
5. 选择以下**脚本类型**之一：
    - **bash**
    - **zsh**
    - **python**
    - **swift**
    - **ps1**
6. 选择**以 root 身份运行**选项，以在设备上以 root 身份运行脚本。 默认情况下，此选项被清除。
7. 在**脚本编辑器**中，您可以在文本框中键入、拖放或复制并粘贴脚本。

8. 或者，单击**从脚本导入代码**，以拖放现有脚本文件，或单击“选择文件”，以浏览并选择要上传到 Ivanti Neurons for MDM 的脚本文件。 这将替换脚本编辑器中的任何现有脚本。 此操作无法撤消。 单击**导入**。 已上传脚本中的代码将显示在脚本编辑器中。
9. （可选）在**可用自定义属性**部分中，选择一个或多个显示的设备自定义属性，以将其与脚本关联。 自定义属性可用于将结果脚本执行值分配到已配置设备的设备自定义属性。 单击**自定义属性的示例代码**，以使用脚本中的自定义属性查看示例代码。
10. 单击**保存**。

脚本中的自定义属性名称应小写。 如果在任何脚本中引用自定义属性，该属性无法移除。 在您修改自定义属性（例如名称）时且如果与脚本关联，您应对关联脚本实施相应的更改。

修改脚本

编辑或移除脚本：

1. 转到**管理员 > 脚本 > 所有脚本**。
2. 在脚本的**操作**列中，单击编辑或删除操作的相应图标。
3. 请按照屏幕中的指示，以完成操作。

在脚本（内容、名称、描述）更改时，与该脚本关联的所有配置会再分发到设备。

使用脚本变量（适用于 Windows 和 macOS）

在脚本存储库中定义和存储脚本输入，例如环境和替换变量。 在 Mobile@Work for macOS 脚本配置或 Ivanti Bridge for Windows 脚本和操作配置中，根据链接的脚本，相关脚本变量将根据需要可供使用。 对于 macOS，此功能需要 **Mobile@Work for macOS** 1.71.0 到 Ivanti Neurons for MDM 支持的最新版本。 对于 Windows，此功能需要 **Ivanti Bridge**。

每次运行脚本时，使用变量以不同的值运行脚本。 例如，管理员可以创建一个脚本，使用 $ 环境变量作为脚本变量，并将其与 Mobile@Work for macOS 脚本配置或 Windows 配置相关联。 当配置已分发并安装在每个用户设备上时，Ivanti Neurons for MDM 会为每个设备发送不同的注册用户电子邮件地址，以采取特定措施。 Ivanti Neurons for MDM 管理门户支持自定义变量。

若要添加脚本变量：

1. 转到**管理员 > 脚本 > 所有脚本**。
2. 在脚本输入部分，单击 **+ 添加**。
3. 在“添加脚本输入 - 环境变量”弹出页面中，输入以下详细信息：
    - 要显示的标签 - 此文本将作为标签显示在 Mobile@Work for macOS 脚本配置页面中。 例如，输入 OS 文件夹，输入 Apache 编号等。
    - 环境变量名称 - 例如，JAVA_HOME、OS_VERSION 等。 在将配置详细信息发送到目标设备时，Ivanti Neurons for MDM 会使用值替代脚本变量，因为这些值会保存在数据库中。
    - 环境变量默认值 - 例如，1024、bin/java、$ 等。 输入变量将在管理员上传或编辑的脚本中使用。 另请参见以下备注。

在预览区域，查看环境变量的值将如何在配置页面中显示为脚本输入。

5. 单击**保存**。

这样，只有标签和默认值可用于配置，而不是环境变量名称，从而提供抽象层。

- 字母数字值（例如 1024、bin/java、root@localhost）或系统属性（例如 $）可以作为环境变量的值。
- 在部署期间，环境变量的值可在配置页面上修改或删除。
- 如果未提供环境变量的值，请确保在脚本部署期间提供值。 否则，空值将传递到脚本。

- 在设备上分发并安装脚本配置后，在**管理 > 脚本和文件 > 所有脚本**页面中编辑环境变量不会影响与脚本关联的现有配置。 另请参见 Mobile@Work for macOS 脚本配置。 对于 Windows，请参阅 Ivanti Bridge for Windows 脚本和操作配置。

编辑脚本变量

要修改脚本变量，请单击变量旁边的编辑（铅笔）图标并保存更改。

如果脚本配置引用具有脚本变量的脚本，编辑现有脚本变量的标签也将反映在脚本配置中。 但是：

- 脚本变量默认值的更改不会反映在现有配置中。
- 对于脚本变量默认值的更改，将反映在使用先前脚本创建的任何新配置中。

删除脚本变量

要删除脚本变量，请单击该变量旁边的删除（减号）图标并确认。

新创建的脚本变量或删除现有的脚本变量甚至会反映在现有的配置中。

测试脚本

在设备上测试脚本之前，在调试工具中快速测试运行脚本，无需保存脚本。

先决条件

- 对于 macOS，此功能需要 Mobile@Work for macOS 1.67 到 Ivanti Neurons for MDM 支持的最新发布的版本。
- 对于 Windows，此功能需要 Ivanti Bridge for Windows 脚本和操作配置。

程序

1. 转到**管理员 > 脚本 > 所有脚本**。
2. 在脚本编辑器中，添加或导入脚本。
3. 如果租户拥有多个空间，选择空间。
4. 在测试脚本部分，选择 **macOS** 或 **Windows** 作为平台。
5. 在**查找设备**文本字段中，查找并选择测试脚本的设备。 设备可以按序列号、用户名、设备名称和 OS 版本搜索。
6. 单击**立即测试**。 这样，对于环境变量可以进行添加、编辑和删除，并且可在该状态下测试脚本（甚至不保存所做的更改）。 对于 **Windows** 脚本，屏幕上会出现一个弹出窗口，脚本执行将开始，您可以在一段时间后从设备详细信息日志选项卡中查看状态。
7. 单击**保存**。
8. 对于 macOS，等待脚本推送并在设备上执行。
9. 在脚本输入（包含环境变量详细信息）、脚本输出和自定义属性部分中，查看已发布的测试结果。 还会显示环境变量的默认值。

验证脚本执行结果

查看脚本执行结果的日志：

1. 转到**设备**。
2. 单击设备的名称。
3. 单击**日志**选项卡。
4. 在显示脚本执行操作的行中，您可以验证以下信息：
    - 详细信息列中的脚本名称。

- 状态列中的脚本执行状态。
- 日期列中的脚本执行日期和时间。
- 脚本执行日志（设备日志 plist）（通过单击操作列中的眼睛图标）。

使用筛选器，以显示**脚本执行**行。 这些行中的日志包含标准输出的输出 (plist) 和脚本的标准错误。

6. 使用筛选器，以显示**脚本执行结果处理**行。 这些行中的日志包含结果处理方式的详细信息 (plist)。
   - 如果脚本没有与其关联的任何自定义属性，没有要处理的任何结果。 已筛选行的列表不显示此类脚本。
   - 如果脚本包含与其关联的自定义属性，且如果为预期格式，将映射结果中的自定义属性，状态显示为成功。 在**属性**选项卡中，您可以验证映射的自定义属性及其值。
   - 如果脚本包含与其关联的自定义属性，且如果不是预期格式，将不映射结果中的自定义属性，状态显示为错误。
   - 如果结果格式正确，但并非所有关联的自定义属性会在结果中发送，状态将显示为错误。
   - 如果脚本变量随脚本一起发送，脚本执行结果处理日志将包括脚本变量的详细信息 (plist)。

相关主题：

- Mobile@Work for macOS 脚本配置
- 如何创建配置
- Ivanti Bridge for Windows 脚本和操作配置

12.9.2. 文件

适用于：macOS 设备

Ivanti Neurons for MDM 允许具有系统管理角色的用户创建或上传以及管理用于配置和分发到设备的文件。

程序

1. 转到**管理** > **脚本和文件** > **文件**。
2. 在**文件**页面中，单击 **+添加**。
3. 在**创建文件**窗口中，输入以下详细信息：
    1. 在**名称**字段中，输入一个名称以标识文件。
    2. 在**说明**字段中，输入说明以阐明此文件的目的。
    3. 在**上传文件**窗格中，单击**选择文件**以上传 .zip 文件。 或者，您可以从设备中拖放文件。
4. 单击**保存**。
   新添加的文件将显示在**文件**页面上。

编辑文件

1. 转到**管理** > **脚本和文件** > **文件**。
2. 选择要编辑的文件，然后单击**编辑**。
   此时会出现**编辑文件**窗口。
3. （可选）您可以编辑**名称**和**描述**字段。
4. 在**上传文件**窗格中，单击**选择其他文件**以上传 .zip 文件。 或者，您可以从设备中拖放文件。
5. 单击**更新**。

删除文件

要删除现有的**文件**，请导航到**管理** > **脚本和文件** > **文件**，选择要删除的所有文件，然后单击 **+ 删除**。

如果**文件**与配置相关联，Ivanti Neurons for MDM 将显示**警告消息**，**“无法删除文件，因为它正被其他策略使用。”**

12.10. 品牌

本部分包含以下主题：

- 管理员 > Apple 应用目录（品牌化）
- 将 Android App Catalog 品牌化
- 管理员 > Android 自助服务终端加印品牌
- 品牌化电子邮件模板
- 自助门户
- 自助门户（品牌化）
- 多用户登录 (Webclip) 品牌加印
- 组织

12.10.1. 管理员 > Apple 应用目录（品牌化）

许可证：Gold

您可以对 Apple {{App Catalog}} 进行品牌化，以使 iPhone、iPad 和 Mac 设备的最终用户更加熟悉其外观。 您可以在 Apple App Catalog 中自定义以下项目：

- 应用图标（PNG，360px 方形）
- 应用名称
- 应用横幅图像 (PNG, 360x64)
- 文本颜色

> 共有两种访问 Apple App Catalog 的模式：独立 App Catalog和集成 App Catalog。 独立 App Catalog 可在 iPhone、iPad 和 Mac 设备上使用。 集成应用程序目录可在 iOS 和 Mac 设备上使用。

为 Android App Catalog 加印品牌

此页面的变化会影响主屏幕、初始屏幕和应用主屏幕。 步骤对独立 App Catalog 和集成 App Catalog 相似。

步骤

1. 在 **Apple App Catalog 品牌化**页面上，单击**自定义**（右上角）。
2. 在**应用图标**部分中，将徽标文件拖放到虚线框，或者单击**选择文件**，以从文件系统中选择。 应用图标会显示在 iOS 主屏幕上
3. 在**应用名称**部分中，编辑 **App Catalog 名称**文本，以更改在初始屏幕上显示的标签。
4. 名称和图标会应用于主屏幕横幅。 要更改自定义横幅图像，取消选择**将名称和图标应用于主屏幕横幅**选项。 随即将显示**应用横幅图像**部分。
5. 要更改应用横幅图像，将新横幅图像文件拖放到虚线框，或者单击**选择文件**，以从文件系统中选择。 应用横幅图像会显示在应用主屏幕的顶部栏中。
6. 在**文本颜色**部分中，单击十六进制颜色代码框，以选择颜色，或者输入十六进制颜色代码，以分配到文本和图标。 这将应用于初始屏幕、应用名称、横幅和操作按钮的文本上。
7. 单击**保存更改**。

您输入的 App Catalog 名称将同时应用于 Android、iOS 和 macOS。

12.10.2. 将 Android App Catalog 品牌化

许可证：Gold

您可将 Android {{App Catalog}} 品牌化，以使最终用户更加熟悉外观。 您可以在 Android 应用目录中自定义以下项：

- 目录徽标（PNG，360x64）
- 目录名称
- 操作栏颜色
- 快捷方式图标
- 快捷方式名称

为 Android App Catalog 加印品牌

程序

1. 在 **Android App Catalog 品牌化**屏幕中，单击**自定义**（右上角）。
2. 要更改 App Catalog 徽标，则将日志文件拖放到虚线框中，或单击**选择文件**，以从文件系统中进行选择。
3. 单击**操作栏颜色**字段以显示可从中选择颜色的调色板，或者输入代表您喜欢颜色的十六进制数字。
4. 编辑**应用目录名称**文本，更改该目录的标签。
5. 您输入的 App Catalog 名称将同时应用于 Android、iOS 和 macOS。
   要更改快捷方式图标，将图标文件拖到虚线框中，或单击**选择文件**，以从文件系统中选择。
6. 编辑**快捷方式名称**文本，以为应用快捷方式更改标签。
7. 单击**保存更改**。

12.10.3. 管理员 > Android 自助服务终端加印品牌

许可证：Silver

您可以在 Android 自助服务终端页面上加印品牌，使最终用户更熟悉其外观。 您可以自定义以下项：

- 横幅徽标 (PNG, 840x114) 或文本
- 横幅边框颜色
- 横幅背景颜色
- 屏幕背景颜色
- 屏幕背景图像 (1280x800)
- 屏幕背景样式

Android 自助服务终端屏幕加印品牌

程序

1. 导航到**管理员>Android 自助服务终端**。
2. 在**自助服务终端模式加印品牌**页面上，单击**创建品牌**。
3. 在**名称**字段中，输入自助服务终端模式加印品牌的名称。
4. 如果您想要关闭横幅，请取消选中**启用顶部横幅。**
5. 单击**横幅背景颜色**字段以显示可从中选择颜色的调色板，或者输入代表您喜欢颜色的十六进制数字。
6. 单击**横幅边框颜色**字段以显示可从中选择颜色的调色板，或者输入代表您喜欢颜色的十六进制数字。
7. 选择**图像/徽标**或**文本**以设置横幅内容。
8. 如果您已选择**图像/徽标**，请拖放图像文件或单击**选择文件**从中选择一个。
9. 如果您已选择**文本**，请键入您想要在横幅中显示的文本。
10. 单击**背景**选项卡。
11. 单击**背景颜色**字段以显示可从中选择颜色的调色板，或者输入代表您喜欢颜色的十六进制数字。
12. 要更改背景图像：
13. a. 删除默认图像。
    b. 拖放首选图像或点击**选择文件**从中选择一个。
    c. 选择首选布局。
    单击**保存更改**。
    创建的自助服务终端模式加印品牌显示在**自助服务终端模式加印品牌**页面中。 要进一步编辑自定义品牌，请单击**操作**列中的“编辑”图标。 要删除自定义品牌化，单击删除图标。 在删除自定义自助服务终端品牌化时，使用该品牌化的配置将还原为默认品牌化。

12.10.4. 品牌化电子邮件模板

您可以对最终用户电子邮件邀请进行品牌化，以使最终用户更熟悉其外观。 单击**还原默认设置**，以清除自定义。

您还能够以所有支持的语言自定义以下电子邮件模板：

- **最终用户邀请** - 邀请用户连接设备，以获取对应用和配置的访问权限。
- **密码重置通知** - 系统会在本地帐户的密码过期之前 7 天和 24 小时发送提醒电子邮件。 这不适用于 LDAP 账户。
- **注册确认** - 在用户完成注册后发送的电子邮件。 您可以使用此注册确认，感谢用户注册并将其定向到更多学习资源。
- **策略合规通知** - 在设备不合规时发送的电子邮件。

本部分包含以下主题：

- 预览和测试电子邮件模板
- 自定义消息标题
- 自定义电子邮件模板
- 支持的电子邮件变量

预览和测试电子邮件模板

您可以预览和测试电子邮件模板。 测试允许您根据模板将电子邮件发送到您指定的电子邮件地址。

若要预览和测试电子邮件模板：

1. 单击**管理员**。
2. 在电子邮件模板中，单击**最终用户邀请**、**密码重置通知**、**注册确认**或**策略合规通知**。
3. 单击与您希望预览和测试的电子邮件模板相关联的**预览和测试**链接。
4. 在渲染的模板窗格中查看渲染的模板。
5. 指定测试电子邮件地址（向其发送测试电子邮件）。
   如果您指定的电子邮件地址属于当前用户，则测试电子邮件将代替大多数电子邮件模板变量的值，从而为用户体验电子邮件提供非常准确的思路。 但测试电子邮件不会替代 Ivanti Neurons for MDM 在生成实际电子邮件邀请时生成的变量。
6. 单击**发送测试电子邮件**。

自定义消息标题

1. 单击**管理员**。
2. 单击**电子邮件模板**。
3. 单击与要编辑电子邮件模板关联的**编辑**图标链接（在操作列中）。
4. 根据需要，对**电子邮件显示名称**、**发件人电子邮件地址**、**回复电子邮件地址**和**设置 SMTP 电子邮件配置**进行新的设置。
5. 如果自定义发件人和收件人电子邮件地址，建议您将电子邮件中继服务加入允许列表，确保电子邮件垃圾邮件过滤服务不会屏蔽电子邮件。 请查看本文档，以了解更多信息。
   单击**保存**。
6. 查看电子邮件模板的预览，并单击**保存**。

使用 SMTP 配置

已添加**设置 SMTP 电子邮件配置**，方便管理员为出站通知配置自己的电子邮件服务器集成。

1. 前往**管理员 > 品牌 > 电子邮件设置**，启用**设置 SMTP 电子邮件配置**选项。
2. 更新以下字段：
    - SMTP server
    - SMTP 服务器端口
    - 协议
    - 用户名
    - 密码
3. 点击**测试**发送测试邮件，随即将显示**测试邮件**弹出画面。
4. 输入邮件的**收件人**姓名和**正文**，然后点击**保存**。

> 如果凭据不正确，则会显示错误消息。

5. 点击**保存**

下表总结了 SMTP 配置窗口中的字段和描述：

字段	说明
SMTP 服务器	指定 Ivanti Neurons for MDM 服务器要使用的 SMTP 服务器的 IP 地址或完全限定主机名。
SMTP 服务器端口	指定为 SMTP 服务器配置的端口。
协议	如果您要配置的 SMTP 服务器是受保护服务器，即使用 SMTPS 协议，则选择 SMTPS 按钮。 否则，请选择 SMTP。
用户名	输入 SMTP 身份验证所需的用户名。
密码	输入 SMTP 身份验证所需的密码。

自定义电子邮件模板

1. 选择**管理 > 品牌化 > 电子邮件模板**。
2. 选择要编辑的模板、**最终用户邀请**、**密码重置通知**、**注册确认**或**策略合规通知**。
3. 单击您想要自定义电子邮件模板旁边的编辑笔图标。

4. 编辑主题行（如果需要）。
5. 在正文窗格中，编辑包含 HTML 元素的电子邮件模板，以自定义消息内容。



您可以使用显示在电子邮件正文右侧的变量。 请参见支持的电子邮件变量。

6. 单击**预览**，在您创建令人满意的迭代时预览电子邮件模板。
7. 在您准备保存模板时，单击**预览**。 这将呈现预览并提供保存功能。



8. 如果您对预览满意，则单击**保存**。

自定义用户邀请中已加入允许列表和阻止列表的内容

在**最终用户邀请**中自定义用户邀请电子邮件模板时，共有一组允许加入允许列表的 HTML 标记和属性。 此外，对于用户邀请不允许的字符串，也存在阻止列表，用于阻止跨站点脚本 (XSS) 漏洞。

仅允许您在邀请电子邮件中使用已加入允许列表的标记和属性。 下表列出已加入允许列表的标记，以及允许的相应属性。

> 部分已加入允许列表的标记（如 <big>）不应有任何已加入允许列表的属性，因此显示为空。

已加入允许列表的标记	已加入允许列表的属性
<big>	[]
<img>	["id","label","editable","height","border","src","style","width", "align", "class","cellpadding","alt","title","data-max-width","data-default"]
	[]
<singleline>	["label"]
<tbody>	[]
<!DOCTYPE>	[]
<h1>	["style"]
<h2>	["style"]
<hr>	["noshade","style"]
<h3>	[]
<body>	["style", "class", "bgcolor", "paddingwidth", "paddingheight", "offset", "toppadding", "leftpadding", "lang","link","vlink","border","cellspacing","cellpadding"]
<title>	["id"]
<head>	[]
	["style","class","width","align","id"]
 	[]
<path>	["d"]
	["style"]
<html>	["xmlns","xmlns:mso","xmlns:msdt"]
	["start"]
<table>	["class","width","border","cellspacing","cellpadding","style","height","bgcolor", "align","background"]
<a>	["href","style","target","rel","class","title"]
<b>	[]
<o:p>	[]
<svg>	["xmlns","class","viewbox","width","height","role","aria-labelledby"]
	[]

已加入允许列表的标记	已加入允许列表的属性
	[]
<i>	[]
<label>	["style"]
<td>	["valign","width","height","class", "cellpadding", "cellspacing","border","bgcolor","align", "style","colspan","id"]
<p>	["style","class","align"]
<u>	[]
<meta>	["name","content","http-equiv","charset"]
<multiline>	["label"]
<style>	["type","id"]
	["style"]
<tr>	["style"]
	["style","class","lang"]
<font>	["color"]

以下是自定义用户邀请不允许的已加入阻止列表的字符串列表。

- Script, @import, ¼script¾, script>, <script, <script>, </script>, javascript, alert(, moz-binding, expression(, +ADw-SCRIPT+AD4-,+ADw-/SCRIPT+AD4-, xml:base
- 特殊字符，并搜索 javascript 或脚本
- 包含 "url=" 未区分大小写的元内容属性
- 未包含 .svg 的 img src。
- 包含 "\00" 的属性值

如果以上任何已加入阻止列表的字符串在最终用户邀请的 HTML 内容中使用，将在单击**预览**时显示错误消息。 此错误消息列出最终用户邀请不允许的 HTML 内容。 编辑并移除不允许的 HTML 内容，然后单击**预览**，以继续更多操作。

> 不允许保存包含已加入阻止列表的 HTML 内容的已编辑模板。

支持的电子邮件变量

Ivanti Neurons for MDM 会提供一些可用于自定义电子邮件模板的变量。

最终用户邀请变量

变量	说明
$	用户激活 URL - 这是围绕 $ 文本的超链接。
$	群集注册 URL - 未在默认模板中找到，但间接引用（通过$ 变量）。
$	产品品牌名称 - 此内容在默认模板的标题中定义为 <title> 标记。
$ ${message:$ ${message:$ }	公司徽标 URL - 这是默认模板中的一个图像 - 它指向 Mobilelron CDN 中的图像 更新**用户品牌**设置会更改 **$** 引用的值。 注册用户设备标题。 电子邮件邀请标题。
${message:$ }	用户在设备中的确认。
${message:$ }	电子邮件邀请开始使用文本。
${message:$ } ${message:$ } ${message:$ }	登录和注册说明。 电子邮件和应用会推送到设备信息。 注册信息（如果用户未在设备中，即包含群集注册 URL）。
${message:$ }	包含公司网站标签的电子邮件邀请页脚。
$	公司网站标签 - 未在默认模板中找到，但间接引用（通过 $ 变量）。

密码过期通知变量

变量	说明
$	密码重置 URL。
$	产品品牌名称 - 此内容在默认模板的标题中定义为 <title> 标记。
$ ${message:$} ${message:$}	公司徽标 URL - 这是默认模板中的一个图像 - 它指向 MobileIron CDN 中的图像 更新**用户品牌**设置会更改 **$** 引用的值。 密码到期通知标题。 密码到期通知介绍段落。
${message:$}	密码重置 URL 名称。
${message:$} $	包含公司网站标签的电子邮件邀请页脚。 公司网站标签 - 未在默认模板中找到，但间接引用（通过 $ 变量）。

注册确认变量

变量	描述
$	产品品牌名称 - 此内容在默认模板的标题中定义为 <title> 标记。
$	公司徽标 URL - 这是默认模板中的一个图像 - 它指向 MobileIron CDN 中的图像 更新**用户品牌**设置会更改 **$** 引用的值。
${message:$}	注册确认标题。
${message:$}	注册确认介绍段落。

策略合规变量

变量	说明
$	通过策略中的发送电子邮件合规操作，在主题行中输入的内容将替换此变量。
$	通过策略中的发送电子邮件合规操作，在消息部分中输入的内容将替换此变量。
$	产品品牌名称 - 此内容在默认模板的标题中定义为 <title> 标记。
$ ${message:$} $	公司徽标 URL - 这是默认模板中的一个图像 - 它指向 MobileIron CDN 中的图像 更新**用户品牌**设置会更改 **$** 引用的值。 包含公司网站标签的电子邮件邀请页脚。 公司网站标签 - 未在默认模板中找到，但间接引用（通过 $ 变量）。

自定义用户属性变量

在以下条件下，管理员可以使用**自定义用户属性**作为自定义电子邮件模板中的电子邮件变量：

- 自定义用户属性在**管理员>属性**页面上。
- 管理员**为用户分配了自定义用户属性**，为每个用户的自定义用户属性指定了值。

12.10.5. 自助门户

注册邀请中包括跳转至自助门户的链接。 最终用户可使用此门户执行以下任务：

- 锁定
- 解锁
- 查看位置（如果隐私配置中已启用）
- 擦除
- 停用
- 更改帐号信息（名称、密码、电子邮件地址）
- 强制签入
- 添加加密和签名证书

要注册其他设备，最终用户需单击自助门户内显示的注册门户链接。

如果最终用户忘记自助门户的 URL，请将其发送到 **https://mydevices.mobileiron.com/user/login.html**。 对 iOS 用户而言，考虑为自助门户创建 **Web 剪辑配置**。

上传签名和加密证书

您可以允许最终用户在“用户提供的证书”配置中的“自助服务门户”中上传其电子邮件签名和加密证书。 可以使用“用户提供的证书”配置来配置此设置。 配置后，最终用户可以上传其电子邮件签名和加密证书。

1. 在**我的证书**中，单击**添加证书**。 将显示**添加证书**窗口。
2. 更新以下字段：

字段名称	说明
证书类型	选择要上传的证书类型。 选项有： • **加密证书** • **签名证书** 这些选项从 Ivanti Neurons for MDM 管理员门户创建。 查看身份证书配置了解更多信息。
要上传的证书	单击**选择文件**，选择要上传的证书文件。 确保该文件是 PKCS12 格式。
密码	输入用于文件的密码。

3. 单击**上传**。

上传后，您可以在显示以下详细信息的表中查看证书列表。

字段名称	说明
证书名称	将证书的类型指定为**加密**或**签字**。
颁发者	颁发证书的详细信息。
上传于	上传证书的日期。
过期日期	证书的到期日期。
操作	您可以执行以下操作： • **编辑证书** - 编辑证书详细信息。 • **清除私钥** - 从证书包 (PKCS#12) 中删除私钥。 • **删除证书** - 从 Ivanti Neurons for MDM 服务器删除证书。

当用户上传证书配置时，服务器重新推送正在使用证书的配置。

> 用户删除和清除私钥不会重新推送配置。

有关更多信息，请查看自助门户品牌化。

12.10.6. 自助门户（品牌化）

许可证： Silver

您可以利用您组织的徽标，自定义自助门户。 如果您并未添加您的徽标，自助门户将显示默认服务徽标。

对自助服务门户进行品牌加印

程序

1. 在“自助门户品牌”屏幕中，点击**自定义**（右上角）。
2. 将徽标文件（PNG，182x34）拖放到虚线框，或单击**选择文件**，从文件系统中选择。
3. 单击**保存更改**。

12.10.7. 多用户登录 (Webclip) 品牌加印

通过添加新的标题和 Webclip 图标，自定义 iOS 的多用户安全登录。

程序

1. 转到**管理 > 多用户登录 (Webclip)**。
2. 在多用户登录 (Webclip) 屏幕中，单击**自定义**。
3. 将日志文件拖动到虚线框中，或者单击**选择文件**，从文件系统中进行选择。
4. 要更改标签，请编辑**安全登录**文本。
5. 要更改 webclip 图标，请将 webclip 文件拖放到虚线框中，或者单击**选择文件**以从文件系统中选择它。
6. 预览更新并单击**保存更改**。

对于 iPhone 和 iPod touch 设备，创建测量 120 x 120 像素或 60 x 60 像素（标准分辨率）的图标。

对于 iPad 设备，创建测量 152 x 152 像素或 76 x 76 像素（标准分辨率）的图标。

有关更多信息，请查看 **iOS 的多用户安全登录**。

12.10.8. 组织

您可以为组织提供品牌名称，或通过在每个主题中包含租户特定的标识符（例如客户名称）来个性化系统警报电子邮件主题行。 如果不更新组织名称，组织屏幕将显示默认值。

组织品牌化

程序

1. 在组织屏幕的**名称**字段中输入所需的名称。
2. 要添加前缀，请单击**编辑**并启用选项**在所有系统生成的电子邮件中添加组织名称前缀，例如许可证到期**。
3. 单击**保存**，应用您的更改。

12.11. 添加对非 iOS 设备的管理

许可证：Gold

您目前正在使用已针对 iOS 设备进行优化的 Ivanti Neurons for MDM 版本。 本部分介绍如何切换以允许管理非 iOS 设备。 切换后，您也将能够管理以下设备：

- Android 5.0 或支持的更新版本
- Windows 10+

切换包含的非 iOS 设备管理无法逆转。

要切换为包含非 iOS 设备：

1. 单击**管理 > 允许平台**。
2. 单击**允许所有平台**按钮。
3. 勾选**我知道此操作无法撤销**，以确认您知道且了解此操作不能撤销。
4. 单击**允许所有平台**按钮。

13. 程序包

本部分包含以下主题：

- 升级
- Secure UEM 和 Secure UEM Premium 程序包
- 旧版 Bronze、Silver 和 Gold 程序包
  - Silver
  - Gold
  - 白金
- 用于预览/测试的沙箱

Secure UEM 和 Secure UEM Premium 程序包

Secure UEM 和 Secure UEM Premium 程序包提供以下功能：

	Secure UEM	Secure UEM Premium
Device management and security		
Easy on-boarding	✓	✓
Multi-OS security and management	✓	✓
Secure email gateway	✓	✓
App distribution and configuration	✓	✓
Mobile application management (MAM)	✓	✓
Scale IT operations		
Helpdesk tools	✓	✓
Reporting	✓	✓
Secure connectivity		
Per app VPN		✓
Conditional Access		✓
Secure productivity		
Secure email and personal information management (PIM) app		✓
Secure web browsing		✓
Secure content collaboration		✓
Mobile app containerization		✓
Derived Credentials		✓
Zero Sign-On		
Passwordless user authentication (single app)		✓

这些程序包可能随时发生变更。 请联系 Ivanti 销售人员确认当前方案。

旧版 Bronze、Silver 和 Gold 程序包

本节介绍旧版 Bronze、Silver 和 Gold 程序包。 打包方案已升级至 Secure UEM 和 Secure UEM Premium 方案。

Bronze

Bronze 程序包中提供 Ivanti Neurons for MDM 基本功能。 您可以通过以下方式展开Bronze程序包：

- 添加更多设备
- 添加 Silver
- 添加 Gold
- 添加“白金”

这些添加扩展了您的移动解决方案，而且超越了基本设备配置。

如果管理员有兴趣在其默认禁用的租户上启用一个或多个按需功能，他们可以联系支持。

Silver

升级至 Silver 会添加以下功能：

- **LDAP 和 Connector：**支持将企业目录和证书颁发机构添加到 Ivanti Neurons for MDM。
- **Sentry：**支持电子邮件访问控制。
- **空间：**支持为需要管理的设备指定不同的管理员（授权管理）。
- **监管模式：**细粒度级别配置的设备级别支持，包括单应用模式。
- **自助门户品牌：**在自助门户中使用您的徽标。
- **证书颁发机构：**将 Ivanti Neurons for MDM 用作证书颁发机构。
- **静默应用安装/卸载：**自动部署和移除移动设备中的应用。
- **应用允许列表/阻止列表/所需应用**：监控并控制在设备上安装的应用。
- **Web 内容筛选器**：将网站允许列表/阻止列表策略应用于所有 Web 浏览器。
- **Apple 特有功能：**启用/限制 AirPlay、AirDrop iOS 壁纸分配和 Apple TV。
- **开放式管理：**控制哪些移动应用可以打开哪些企业内容。
- **Apple App 和图书：** 向设备分发移动应用许可证，并在设备停用时，回收并重新分配这些许可证。
- **Android 企业版 (Android for Work) 支持**
- **设备注册：** 支持客户批量购买设备，并在激活过程中自动将 Apple 设备注册到 MDM。
- **Per App 配置：**大规模部署配置的移动应用，最终用户几乎无需执行任何操作。
- **第三方 Per App VPN：**现在，VPN 安全是即时、无形且特定于移动应用。
- **策略分层操作**
- 应用分发筛选器
- **审计跟踪**
- **Android 自助服务终端模式：**支持配置 Android 设备在自动服务终端模式下运行。
- **Android 自助服务终端加印品牌：**设备在自动服务终端模式下运行时，更改自助服务终端屏幕显示的背景和横幅。
- **使用图形 API 实现的 Office 365 数据丢失防护 (DLP)**：通过图形 API 实施 Office 365 应用程序的 DLP 控件。

Gold

升级至 Gold 后，除了拥有 Silver 提供的特性外，其还将具备以下特性：

- **单点登录：**用户进行一次身份验证并自动登录到其他企业移动应用。
- **iOS 和 Android 应用目录自定义品牌化：**在 App Catalog 中显示您的公司徽标。
- **增加的内容限制：**50 个文件，每个文件 25 MB
- **AppConnect for iOS：**获得并配置启用了 AppConnect 的应用。
- **AppTunnel for iOS：**获得应用与企业资源的连接。
- **Docs@Work for iOS：**赋予用户查看、存储和共享文档的能力。
- **iOS 8 基于证书的单点登录**

- **iOS 8 iBook/ePub 管理**
- **macOS 支持**
- **用户加印品牌**
- **带 AppConnect 的 Mobile Application Management (MAM)**
- **派生证书**
- **Windows 10（包括 Bridge）支持**

白金

升级至 Platinum 后，除了拥有 Gold 提供的特性外，其还将具备以下特性：

- **Tunnel：**配置特定应用对企业数据的访问。
- **Help@Work**
- **监控器**
- **ServiceConnect（ServiceNow、Splunk）**

用于预览/测试的沙箱

在购买 **Premium Plus** 支持时，Ivanti Neurons for MDM 客户可以获得沙盒租户以预览和测试新版本，然后再正式投入使用。

13.1. 升级

本部分包含以下主题：

- 升级许可证
- 请求升级
- 从之前版本升级

升级许可证

Bronze 软件包提供了基本功能。 您可以通过以下方式展开Bronze程序包：

- 添加更多设备
- 添加 Silver
- 添加 Gold
- 添加“白金”

这些添加扩展了您的移动解决方案，功能超过基础设备配置。

请求升级

程序

1. 从管理员下拉菜单中选择**升级选项**。
2. 单击**请求升级/添加设备**（右上角）。
3. 选择您要添加的选项并输入您的手机号码。

公司代表将会在 24 小时内与您联系以获得详细信息。

从之前版本升级

在从上一个版本升级时，**编辑设备注册配置文件**页面中的设置将不会保留。 在升级前，请注意您的选项设置。

- 如果在升级前启用**跳过使用 Apple ID 登录 iCloud**，则**跳过 Apple Pay 设置**将在升级后启用。
- 如果在升级前启用**跳过输入通行码**，则**跳过触控 ID** 和**跳过 Apple Pay 设置**将在升级后启用。

程序

1. 在升级完成后，返回**编辑设备注册配置文件**页面，编辑设备注册配置文件，以还原所需的设置。
2. 单击**保存**。

升级后，会影响若干配置设置。

- 推广选项设置为**关**。
  安装设置设为**否**。
  不在 App Catalog 中显示选项已不再选中。
  在 Android Samsung Knox 上静默安装设置为“假”。

iOS 管理旗标设置为：

- 备份至 iCloud。

- 取消注册时删除。

这些 iOS 管理标志设置可以为每个应用单独选择。

应用设置：

- 应用设置现在称为配置。
- 所有其他应用程序设置保持升级之前的状态。

有关更多信息，请查看软件包。

14. 设备许可证

Ivanti Neurons for MDM 基于设备的许可证定义您可以注册的设备数量、您可以配置并分发给设备的内容数量，以及可以使用哪些功能。 如果达到设备的限制，“管理员”页面上会显示一个红色三角形。 如果达到内容的限制，服务会阻止您添加更多内容并显示一条消息，提示您已达到限制。

14.1. 租户暂停

Ivanti Neurons for MDM 可能会暂停通过评估许可证或生产许可证访问租户。 在评估周期到期时或已超过使用允许时，评估许可证可能会暂停。 在订阅周期到期时或已超过使用允许时，生产许可证可能会暂停。 Ivanti Neurons for MDM 将在续订许可证或购买额外许可证时恢复已暂停的租户，以避免超额使用。

在租户许可证暂停时：

- 现有的注册设备继续正常运行。
- 管理员无法登录管理员门户。
- 新设备无法注册。
- 对租户的 API 访问被阻止。
- 最终用户可以继续访问自助门户。

租户暂停操作和错误消息

暂停操作	错误	错误消息已显示	定位
最终客户集成 API 访问已阻止。	API 调用失败。	拒绝访问。 您的评估许可证已过期。 请续订许可证，以重新启用 API 访问。 请联系您的系统管理员，以了解详细信息。	API 错误 401。
已阻止新设备注册。	注册屏幕上会显示一条错误消息。	无法注册您的设备。 系统许可证已过期。 请联系您的系统管理员，以了解详细信息。 此前登记的设备将继续正常工作。	遵循密码验证。
管理员被阻止登录管理员门户。	登录屏幕上会显示一条错误消息。	无法登录。 您的许可证已失效。 请更新您的许可证，以重新获取管理员门户网站的访问权限，并登记新设备。 此前已登记的设备将继续正常操作。 请联系您的销售代表，以更新您的许可证。 请注意，管理员密码将在 1 年（365 天）后过期。	遵循密码验证。

15. 打开支持票证

访问 **Ivanti 支持门户**，打开支持票证。

16. 第三方属性

Ivanti Neurons for MDM 包含由第三方开发的组件。 您可以在此处查看列表。

17. Apps@Work

从 Ivanti Neurons for MDM 83 版本开始，可从 Go 应用过渡到 Apps@Work 本地体验。 对于新创建的租户，不会在默认情况下为通过 iReg 或客户端安装的 iOS 设备分发 Apps@work Webclip 配置。 管理员必须为通过 iReg 或客户端注册的设备手动分发 webclip 配置。 注意以下几点：

Ivanti Neurons for MDM**管理门户**：

- 默认情况下，只有新租户才会获得分发到 iOS 设备的“适用于本地客户端的 App Catalog”配置。
- 对于现有租户，默认情况下，系统不会分发 Apps@Work 本地应用。
- 管理员必须向设备推送“适用于本地客户端的 App Catalog”配置，从而在本地 Appstore 中获得 Apps@Work。

客户端：

- Go 应用现在将显示 Apps@Work 选项卡。
- “适用于本地客户端的 App Catalog”配置拥有适用于本地客户端的 App Catalog 身份证书和 App Station 身份证书。
  Ivanti Neurons for MDM 使用“适用于本地客户端的 App Catalog”配置推送证书。

Apps@Work 功能

Apps@Work 选项卡具有以下功能：

- 从 Go 应用访问 Apps@Work 选项卡
- 搜索
- 安装应用 - 按钮状态
- 特别推荐应用和横幅
- 应用更新通知
- 应用更新通知

从 Go 应用访问 Apps@Work 选项卡

- 系统在 Go app 中为 Apps@Work 添加了一个新选项卡。
- Apps@Work 中有两个默认选项卡 -“所有应用”和“类别”。
- “所有应用”选项卡按字母顺序列出所有应用。
- “类别”选项卡仅显示其中有应用的类别。
- 每个类别都会显示其中包含的应用数量。
- “类别”下的 MyApps 是包含所有已安装应用的列表项。 MyApps 将始终是第一个类别，其余类别按字母顺序排列。
- 如果没有安装应用，MyApps 列表将显示“无”。
- 点击某个类别时，特定于该类别的所有应用都会列出，且显示“安装”选项。 向导会指引您分别安装每个应用，或者您也可以点击“安装所有”，以安装该类别中的所有应用。 系统会提示您允许安装每个应用。

搜索

- 点击搜索（镜片）图标搜索以下项：
  - 新版本 - 搜索栏中没有输入任何文本时，会显示新版本的应用列表

- 输入任何文本，然后搜索字段会动态预测和显示匹配的应用。
- 搜索结果计数显示为子标题
- 可以点击“安装”按钮安装应用，无需导航到详细信息页面。

安装应用 - 按钮状态

- 由于应用安装需要服务器处理请求，并将应用下推到设备，“安装”按钮将不会实时显示进度
- “安装”按钮的状态变化顺序：安装 > 已请求 > 已安装。
- 系统首次显示警报消息，表明已请求安装。
- 点击“已请求”按钮时也会显示警报。
- “已安装”状态不是按钮。

特别推荐应用和横幅

- 根据管理员配置，“特别推荐”选项卡可见。
- 没有更新可用时，“特别推荐”选项卡即为默认登录页面。
- “特别推荐应用”横幅在横幅中显示一个应用。
- “特别推荐应用”包含所有特别推荐应用的列表。

应用更新通知

- 有任何可用应用更新时，Go 会发出通知。 通知不显示应用名称。
- 在点击应用更新通知后，您将被重定向至 Apps@Work 中的“所有应用”页面。
- 在 Go 应用中，Apps@Work 选项卡图标将显示徽章计数，以反映有待处理更新的应用数量。
- 在 Apps@Work 选项卡中，“可用更新”子部分将显示在“所有应用”选项卡下，并显示可进行更新的应用数量。
- 每个需要更新的应用都将显示红点图标。

设置 - 我的设备

- “我的设备”选项卡现已移动到“设置”下。
- 在点击应用更新通知后，您将被重定向至 Apps@Work 中的“所有应用”页面。
- 在 Go 应用中，Apps@Work 选项卡图标将显示徽章计数，以反映有待处理更新的应用数量。
- 在 Apps@Work 选项卡中，“可用更新”子部分将显示在“所有应用”选项卡下，并显示可进行更新的应用数量。
- 每个需要更新的应用都将显示红点图标。

18. 在 Ivanti Neurons for MDM 和 SCEP 服务器之间启用 Kerberos 身份验证

可以使用 Kerberos 身份验证在 Ivanti Neurons for MDM 和 SCEP 之间进行通信。 以下部分讨论如何在 SCEP 服务器和 Ivanti Neurons for MDM 上启用 Kerberos 身份验证。

> 此功能将在 Ivanti Neurons for MDM 连接器 93 版本可用时正常工作。

预配置步骤

1. 检查 SCEP 服务器上 SCEP 服务正在使用哪个服务账户。
2. 在 SCEP 服务器上，检查服务账户是否为本地 IIS_USRS 组的成员。
3. 在正在配置的 CA 服务器证书模板上，检查服务账户是否具有注册权限。

配置 Windows 服务器

1. 在域控制器上运行以下命令：
   setspn -s http/<SCEP-SERVER-FQDN> <domain>\<service account>
2. 在 **Active Directory 用户和计算机**中，点击服务账户的**委派**选项卡：
   1. 在**信任此用户并仅将其委派给特定的服务**下，选择**仅使用 Kerberos**。
   2. 点击**添加**并添加 SCEP 服务器名称。
   3. 选择 HTTP 服务。
   4. 单击**确定**。
3. 在 IIS 服务器上执行以下操作，以确保使用应用程序池凭据来解密 Kerberos 票证：
   1. 检查 SCEP 应用程序池是否在您之前验证的服务账户下运行。
   2. 要启用 useAppPoolCredentials，请在 Microsoft SCEP 管理员 (mscep_admin) 或 Microsoft SCEP (mscep) 网页上，选择**配置编辑器 > System.webServer > 安全性 > 身份验证 > Windows 身份验证**，并将值设置为 useAppPoolCredentials=True。
4. 通过选择**身份验证 > 匿名身份验证**并点击**禁用**，在 Microsoft SCEP 管理员网页 (mscep_admin) 上禁用**匿名身份验证**。
5. 在 Windows 身份验证高级设置中禁用内核模式身份验证。

> 确保使用**协商**作为身份验证服务中的第一个选项。

6. 在 Windows 身份验证高级设置网页中禁用内核模式身份验证。
7. 重新启动 IIS 服务。

配置 Kerberos

此部分讨论如何在 Ivanti Neurons for MDM 服务器上配置 Kerberos。

配置 Ivanti Neurons for MDM 中的 Kerberos 设置

导航到**管理员 > 基础设施 > Kerberos**，按表中所示输入以下设置：

UI 部分	择
Active Directory 的 Kerberos 领域	IVANTI.COM
相应的密钥分发中心 (KDC) 服务器	kdc.ivanti.com
服务用户凭据	用户@领域 例如： serviceuser@IVANTI.COM
用于与 Microsoft AD 证书服务进行出站通信的域（主机名不区分大小写，并且必须以 .ivanti.com 或 .IVANTI.COM 结尾） SCEP 或 NDES 服务器：还可以使用主机名，例如：ndes.ivanti.com 或 scep.ivanti.com	

针对现有证书颁发机构的 Microsoft SCEP 证书注册配置启用 Kerberos 身份验证

执行以下步骤以针对现有证书颁发机构启用 Kerberos 身份验证：

1. 在 Ivanti Neurons for MDM 中，选择**管理员 > 基础设施 > 证书管理**。
2. 使用**外部**选项选择证书颁发机构类型。

> 这些外部证书颁发机构类型应表示为 Microsoft。

3. 从**操作**下拉菜单中，选择**编辑**。
4. 在**编辑外部 CA** 窗口中，选中**首选 Kerberos 身份验证**复选框以启用 Kerberos 身份验证。

针对新证书颁发机构的 Microsoft SCEP 证书注册配置启用 Kerberos 身份验证

执行以下步骤以针对新证书颁发机构启用 Kerberos 身份验证：

1. 在 Ivanti Neurons for MDM 中，选择**管理员 > 基础设施 > 证书管理**。
2. 选择**+添加**选项。
3. 在**添加证书颁发机构**窗口中，选择**连接到本地 SCEP 证书颁发机构**选项。
4. 单击继续。
5. 在**添加外部证书颁发机构**窗口中，执行以下步骤：
    1. 从**证书颁发机构类型**下拉列表中选择 **Microsoft** 选项。
    2. 选中**首选 Kerberos 身份验证**复选框以启用 Kerberos 身份验证。
    3. 填写所有必填字段。
    4. 单击**完成**。

19. Ivanti Neurons for MDM 127 管理员指南

2026 年 9 月

作为现代的移动安全性方法，Ivanti Neurons for MDM 在高度可扩展和易于更新的安全基础设施中提供了统一端点管理 (UEM) 解决方案，该基础设施支持全球数百万台设备。

{{如果语言不可用}}

新增功能摘要

以 PDF 格式查看

视频

20. Welcome

21. Welcome CSH

22. Windows 更新管理

作为管理员，如果您想使用 Windows 更新管理更新 Windows 设备，可以查看和批准该设备报告的更新。 通过使用此功能，您可以防止在设备中安装不必要或未经测试的更新。

更新管理功能要求使用**软件更新**配置对设备进行配置，并启用**需要更新批准**选项。 只有将此配置应用于设备，设备才会报告安装更新并等待批准。

管理更新

1. 转到**管理员 > Windows 更新**。 页面中将显示以下更新详细信息。
   创建日期：创建更新的日期。**标题**：描述更新类型以及知识库文章编号。

> 在单击更新时，将显示说明。

分类：将更新类型分为以下类别之一：

- 关键更新
- 定义更新
- 驱动程序更新
- 安全更新。
- 更新
- 升级
- 更新汇总

分配：为更新执行的分配。 例如，当更新分发到所有设备时，将显示**所有**。

> 如果将更新分配到特定数量的组，则会显示分配的计数。 例如，如果仅对 3 个组执行分配，则显示 3。

2. 此外，您还可以查看更新是否已分发到所需的设备。 以下列中包含的数字表示在不同类别的更新下存在的设备数量：
   - 符合条件的设备
   - 已安装的设备
   - 安装失败的设备
   - 等待重启的设备

点击任意数字后，您将被定向到“设备”页面上的筛选视图，您可在其中了解更新的状态并执行所需的操作。
通过单击更新的复选框，查看更新并选择要分配给设备的更新。

3. 在**操作**下点击**设置分发**。
4. 在**分配 Windows 更新**窗口中，选择以下任何分配选项：
   所有设备：将更新分配给所有设备。
   无设备：保留要分配给设备的更新**自定义**：为指定的设备组分配更新。
5. 单击**保存**。

搜索和过滤更新

您可以根据以下条件搜索和过滤更新：

- 知识库文章 ID
- 配置的分配

根据知识库文章 ID 进行过滤：

1. 在 **Windows 更新管理**页面的快速搜索字段中输入知识库 ID（只能在搜索字段中输入数字）。
   示例：对于 KB4056892，键入 4056892。 页面上显示与搜索条件匹配的更新。

> 您可以进一步查找有关更新的其他信息，方法是单击**支持**和**更多信息**链接。 指向 Microsoft 网页的**支持**链接为更新提供产品支持信息，指向 Microsoft 网页的**更多信息**显示与更新有关的更多信息，例如知识库文章。

根据配置的分配进行过滤：

在 **Windows 更新管理**页面，根据配置的分配选择以下任何过滤选项：

- **所有**：显示所有更新。
- **已配置**：显示分配给设备的更新列表。
- **未配置**：显示未指定分配的更新列表。

> 已配置和未配置的筛选器基于执行的分发，分发也可以是**无**。

查看设备的更新

要查看特定于设备的详细更新信息：

1. 转至**设备 > 设备**。
2. 单击设备名称可查看详细信息页面。
3. 转至**更新**选项卡。 将显示待处理（由管理员批准更新但未报告为已安装在设备上）、失败和已安装的设备的更新。

> 您还可以在仪表板下的通知页面中看到有关新 Windows 更新的通知。 通知包括通知的创建日期、可用通知的数量以及通知的目的。 Windows 更新通知也在管理员门户的右上角可见。